MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: ABECS – ASSOCIAÇÃO BRASILEIRA DAS EMPRESAS DE CARTÕES DE CRÉDITO E SERVIÇOS

CPF/CNPJ: 42.159.244/0001-61

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos

titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados. Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS **IMPORTANTE:** Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	O art. 48 da Lei 13.709/18 (“LGPD”) determina que o controlador deverá comunicar à ANPD e aos titulares de dados a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Depreende-se, portanto, do texto legal que não é qualquer incidente de segurança que deve ser reportado à ANPD ou aos titulares, mas apenas aqueles que de fato possam causar risco ou dano relevante aos titulares. Entendemos que um incidente de segurança pode acarretar risco ou dano relevante se de fato houver probabilidade elevada de que o que os titulares venham a sofrer danos concretos à sua integridade física ou moral, como dano físico, discriminação, danos materiais relevantes, roubo de identidade, fraude, significativos danos à sua reputação.

	Para avaliar se o risco ou dano é de fato relevante, deve-se considerar alguns critérios, como: • a natureza e sensibilidade do conjunto de dados afetados sob a responsabilidade do controlador, considerando aqueles que podem de fato acarretar os danos relevantes; • volumetria dos dados afetados; • natureza, categoria e quantidade de titulares de dados afetados; • a probabilidade concreta de se materializar o dano e o seu potencial lesivo (gravidade); • o tipo de incidente e circunstâncias que influenciam os impactos/gravidade, como se os dados pessoais já estavam expostos ou publicamente acessíveis e medidas tomadas para reverter ou mitigar os efeitos do incidente. Definir o que é considerado risco ou dano relevante não é tarefa trivial e deve ser avaliado no contexto de cada caso. A título exemplificativo, um incidente envolvendo dados pessoais sensíveis pertinente ao estado de saúde de titulares tende a gerar uma possibilidade de dano mais elevado se comparado ao vazamento de endereços de e-mail. Um incidente envolvendo dados pessoais que já foram expostos ou que já estejam acessíveis publicamente, por exemplo, mas não se limitando, em alguma mídia social, não tem o condão de gerar risco ou dano aos direitos e liberdades do titular. Além disso, medidas de reversão, contenção ou mitigação dos efeitos do incidente podem mitigar o risco ou dano de modo que não sejam relevantes. Assim, é necessário considerar o contexto e os impactos do incidente ao avaliar a relevância dos riscos e danos aos titulares de dados.
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	Entendemos que a severidade do incidente deva ser subdividida em categorias, considerando probabilidade de materialização do risco e gravidade, mas que não é necessário ou adequado subdividir o risco ou dano relevante em mais categorias, pois a nova divisão pode tornar a avaliação de riscos do incidente mais complexa, confusa e burocrática. Por exemplo, pode-se considerar a gravidade/severidade do incidente como:

	1. Baixo: os titulares dos dados não serão afetados ou poderão encontrar alguns inconvenientes. 2. Médio: os titulares dos dados podem encontrar inconvenientes mais significativos. 3. Alto e muito alto: probabilidade de resultar em alto risco de dano real relevante a um indivíduo. Nessa linha, incidentes de risco baixo e médio não seriam considerados como passíveis de acarretar riscos ou danos relevantes e, portanto, não devem ser objeto de notificação à ANPD ou aos titulares de dados. Apenas os incidentes de alto risco seriam passíveis de notificação, considerando os impactos relevantes comprovados aos titulares dos dados, mas sem necessidade de nova classificação em categorias apenas para os riscos e danos relevantes.
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	No caso do risco ao titular, a ocorrência do incidente de segurança pode vir a gerar um dano ao titular, ou seja, existe uma probabilidade da materialização do risco. Os riscos devem ser relevantes apenas se houver grande probabilidade de resultar em danos reais e relevantes a um indivíduo. No caso do dano ao titular, a ocorrência do incidente de segurança, comprovadamente gerou dano relevante ao titular, ou seja, dano é o risco relevante concretizado.
O que deve ser considerado na avaliação dos riscos do incidente?	Há diversas metodologias para avaliar a severidade do incidente e se este pode acarretar riscos ou danos relevantes aos titulares, como abordaremos em item específico deste documento. De qualquer forma, sugerimos considerar alguns aspectos nessa avaliação, como: • Contexto de Processamento de Dados: aborda o tipo de dados afetados, juntamente com vários fatores vinculados ao contexto do processamento e o nível de criticidade. • Facilidade de Identificação: determina com que facilidade a identidade dos titulares pode ser deduzida dos dados envolvidos no incidente e se esses dados podem ser usados de forma a causar dano ao titular, impactando na avaliação da severidade do incidente. • Circunstâncias do Incidente: aborda as circunstâncias específicas do incidente, que estão relacionadas ao tipo de incidente, incluindo principalmente a perda de segurança dos dados afetados (confidencialidade), bem como qualquer intenção maliciosa envolvida e outras

	circunstâncias que podem influenciar os impactos/gravidade, como se os dados pessoais já estavam expostos ou publicamente acessíveis e medidas tomadas para reverter ou mitigar os efeitos do incidente, assim como os mecanismos de mitigação, identificação e controle existentes e observados pelas entidades envolvidas. No contexto da avaliação de riscos do incidente, pode-se levar em consideração os pontos que mencionamos na resposta à primeira pergunta deste documento, quais sejam: • a natureza e sensibilidade do conjunto de dados afetados sob a responsabilidade do controlador, considerando aqueles que podem de fato acarretar os danos relevantes; • volumetria dos dados afetados; • natureza, categoria e quantidade de titulares de dados afetados; • a probabilidade concreta de se materializar o dano e o seu potencial lesivo (gravidade); • o tipo de incidente e circunstâncias que influenciam os impactos/gravidade, como se os dados pessoais já estavam expostos ou publicamente acessíveis e medidas tomadas para reverter ou mitigar os efeitos do incidente. Ainda, importante considerar, a comprovação da materialização do incidente de segurança, ou seja, o incidente de segurança sob responsabilidade do controlador, os dados pessoais ou a possibilidade de a exposição dos dados ser materializada, com risco de dano ao titular. Ademais, deve ser considerado se o uso a ser feito dos dados comprometidos no incidente pode de fato gerar risco ou dano relevante ao titular, inclusive se os dados já estavam expostos anteriormente ou acessíveis publicamente bem como as medidas adotadas para mitigar os riscos do incidente. De antemão, a ocorrência de um incidente não deve ser considerada uma falha na obrigação de zêlo das empresas. Nenhuma entidade, pública ou privada, tem condições de garantir a segurança absoluta do tratamento de dados. A segurança dos dados é uma atividade complexa, que requer o monitoramente contínuo, bem como processos internos bem estruturados. Há diversas ameaças externas, sendo que o grau de sofisticação das atividades não lícitas é cada dia maior.

	Não é recomendável que a regulação dos incidentes aborde o tema de forma enumerativa e exaustiva. Afinal, as ameaças são mutáveis e estão constantemente em evolução, as tecnologias e serviços dispostos de forma legítima aos titulares avança, bem como há diversas possibilidades de incidentes. Assim, uma regulação que aborada o tema de forma consisente, porém flexível, é altamente recomendável de forma a acompanhar a evolução das tecnologias e atividades empresariais. Deve-se levar em conta, também, os custos e procedimentos necessários, bem como a probabilidade e a gravidade dos riscos em relação aos direitos e liberdades dos titulares. Por fim, importante ressaltar que as instituições devem ter flexibilidade para adotar ou adaptar as metodologias, critérios, considerações específicas, perfil de risco e avaliação.
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	O artigo 48 já traz informações suficientes para a comunicação de incidentes à ANPD. Aproveitamos para recomendar a exclusão da possibilidade de notificação do incidente à ANPD por operadores, como constou do formulário de comunicação de incidentes de segurança à ANPD, disponibilizado por esta Autoridade. Entendemos que o operador de dados não deve notificar incidentes, pois esta é uma obrigação do controlador dos dados.
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	Importante ressaltar que a investigação de um incidente de segurança é complexa e nada trivial, considerando que pode haver um lapso temporal entre a descoberta de um incidente e o efetivo envolvimento e atuação das áreas e pessoas necessárias, além da complexidade para buscar e avaliar evidências e os impactos do incidente. Assim, um prazo muito exíguo para comunicação do incidente não será factível de cumprir. Entendemos que um prazo razoável para comunicação de incidentes à ANPD seria de, no mínimo, 5 (cinco) dias úteis a contar da finalização da análise do incidente que possibilite que o controlador

	tenha razoável grau de certeza de que um incidente de segurança de fato ocorreu sob a responsabilidade do controlador, comprometeu a segurança dos dados e pode acarretar risco ou dano relevante aos titulares de dados pessoais, mas ressaltamos que referido prazo pode ser maior. Desta forma, a ANDP será informada de maneira mais apropriada sobre o incidente, evitando-se, assim, comunicações excessivas, prematuras e sem conteúdo relevante à ANPD que podem desviar o foco da autoridade para temas efetivamente relevantes. Não recomendamos a contagem do prazo em horas, mas em dias úteis, dada a dificuldade prática de identificar com certeza o horário em que houve o razoável grau de certeza a respeito do incidente por parte do controlador. Não recomendamos usar o prazo de comunicação previsto na lei do cadastro positivo, de 2 (dois) dias úteis a contar da ciência do incidente de segurança, pois: • o prazo é muito exíguo; • não há clareza do que seria considerada "ciência do incidente", ressaltando a necessidade de que o início do prazo de notificação não deve ser contado a partir do conhecimento do fato, mas após análises que permitam ao controlador ter razoável grau de certeza sobre o incidente e seus riscos; • a obrigação de comunicação de incidentes prevista no cadastro positivo tem aplicação restrita apenas aos gestores de bancos de dados do cadastro positivo, ao passo que a obrigação de comunicação de incidentes previstas na LGPD é bem mais ampla e aplicável a todos os setores.
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	Entendemos que a comunicação ao titular deve ser feita de forma tempestiva, a partir da finalização da análise do incidente que possibilite que o controlador tenha razoável grau de certeza de que um incidente de segurança de fato ocorreu sob a responsabilidade do controlador, comprometeu a segurança dos dados e pode acarretar risco ou dano relevante aos titulares de dados pessoais. Caso seja definido um prazo específico para a comunicação do incidente aos titulares, referido prazo deveria ser, no mínimo, de 5 dias úteis, mas podendo ser maior do que este prazo, sempre contado

	a partir da finalização da análise do incidente mencionada no parágrafo anterior. Entretanto, importante considerarem a possibilidade de que a comunicação do incidente aos titulares não precise ser realizada no mesmo prazo de notificação à ANPD, podendo ocorrer após a notificação realizada à ANPD, ou mesmo após orientação da ANPD nesse sentido, considerando as características e efeitos do incidente. A comunicação aos titulares dos dados sobre o incidente de segurança deve conter as informações relevantes sobre o incidente: • breve informação sobre a ocorrência do incidente, com a indicação da natureza dos dados pessoais afetados; • informação sobre as medidas utilizadas para a proteção dos dados e as utilizadas ou a serem adotadas para mitigar os efeitos do incidente; • os riscos relacionados ao incidente; • eventuais medidas que o titular pode ou deve adotar para resguardar os seus dados, prevenir fraudes e proteger sua privacidade; • Informação de um canal para contato, em caso de necessidade de esclarecimento de dúvidas. Entendemos não ser necessário informar aos titulares todos os detalhes ou informações técnicas relacionadas ao incidente que sejam informadas à ANPD, conforme descrito no art. 48º.
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	A forma de comunicação ao titular dos dados vai depender da extensão do incidente e dos meios que o controlador considere mais efetivos para tal comunicação, a depender do seu relacionamento com o titular e dos dados de contato de que dispõe. A comunicação direta e individualizada ao titular é preferível, a menos que exija um esforço ou custo desproporcionais ou o controlador não disponha das informações de contato do titular. É possível usar outros meios para realizar a comunicação, como publicações em website, redes sociais, nota à imprensa, comunicados, informações em centrais de atendimento/ouvidoria.

	Entretanto, ainda que a ANPD possa determinar a ampla divulgação do fato em meios de comunicação, caso seja necessário para salvaguardar os direitos dos titulares, conforme previsto na LGPD, recomendamos que a norma não regule ou limite as formas de comunicação em nenhum caso, bem como não determine uma forma específica de comunicação, ficando a critério do controlador escolher os meios para tal comunicação.
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	Como a LGPD determina a obrigatoriedade de comunicação do incidente à ANPD e aos titulares apenas se o incidente de segurança puder acarretar risco ou dano relevante aos titulares, os incidentes que não possam resultar em alto risco de dano real a um indivíduo não devem ser comunicados. De qualquer forma, destacamos situações especificas que poderiam ser consideradas como exceção para a comunicação à ANPD: • Os danos ou riscos do incidente foram mitigados ou revertidos, inclusive pela adoção de medidas subsequentes pelo agente, de modo que não mais há alto risco ou dano provável de se materializar; • Situações pontuais envolvendo número limitado de titulares e de dados pessoais, de acordo com as circunstâncias do incidente; • Quando os dados pessoais já estiverem acessíveis publicamente; • O responsável pelo tratamento tiver aplicado medidas de proteção adequadas, tanto técnicas como organizativas, e essas medidas tiverem sido aplicadas aos dados pessoais afetados pela violação de dados pessoais, especialmente medidas que tornem os dados pessoais incompreensíveis para qualquer pessoa não autorizada a acessar esses dados ou que não possam ser lidos ou utilizados, tais como a criptografia, sendo que neste caso entende-se que não haveria alto risco ou dano relevante aos titulares; • Incidentes que envolvam controlador ou processador com terceiro de confiança submetido a segredo profissional ou obrigação de confidencialidade, sem que tenha havido comprometimento relevante dos dados. Neste caso também não haveria risco ou dano relevante aos titulares.

Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	O Titular não deve ser informado sobre todo e qualquer incidente. As comunicações devem ocorrer em casos de risco alto e se não tiver sido contido pelos agentes de tratamento antes que um dano ou risco elevado possa ser efetivado. Além dos casos mencionados acima em que não seria necessário comunicar a ANPD sobre o incidente e também ao titular, sugerimos também considerar como exceções da obrigatoriedade de comunicar especificamente o titular: • Quando contatar os titulares implicar em esforço desproporcional, como quando os dados de contato tiverem se perdido em resultado da violação ou nunca tiverem sido conhecidos pelo agente de tratamento; e • Situações em que a divulgação possa causar impacto adverso ou colocar em risco a investigação ou possibilidade de mitigação dos efeitos do incidente.
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	Fazemos referência aos nossos comentários à pergunta “O que deve ser considerado na avaliação dos riscos do incidente?” indicados acima, que podem também ser considerados para a avaliação da gravidade do incidente.
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	Existem diversas metodologias para avaliação da gravidade de um incidente de segurança, como os exemplos mencionados neste item: • A metodologia da ENISA (*European Union Agency for Cybersecurity*), com algumas adaptações considerando o cenário do setor financeiro, pode ser usada para a análise de gravidade do incidente de segurança (“Recommendations for a methodology of the

	assessment of severity of personal data breaches", ENISA, disponível em https://www.enisa.europa.eu/publications/dbn-severity); • ISO 27001 • ISO 27701 • ISO 29100 • NIST (Computer Security Incident Handling Guide – NIST. Disponível em https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf) De qualquer forma, entendemos que métodos específicos podem não ser eficientes em todos os casos e que é necessário haver flexibilidade para que o controlador adote ou adapte metodologias que façam sentido de acordo com as suas avaliações internas, atividades e a própria evolução dos cenários envolvendo incidentes de segurança e proteção de dados. Finalmente, é essencial que a ANPD submeta à consulta pública eventuais critérios ou metodologia que venha a adotar para a avaliação da gravidade de um incidente de segurança, para que possam ser conhecidos e debatidos com os diversos ***stakeholders*** envolvidos, dado o seu impacto significativo para os agentes de tratamento e titulares de dados pessoais.
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	A LGPD, em seu artigo 48, § 2º. e seus incisos, determina que a ANPD poderá, caso seja necessário para salvaguardar os direitos do titular, determinar a adoção de providências ao controlador, tais como a ampla divulgação do fato em meios de comunicação e medidas para reverter ou mitigar os efeitos do incidente. De modo geral, quaisquer providências e medidas técnicas ou organizacionais que venham a ser determinadas pela ANPD aos controladores após a comunicação do incidente de segurança devem observar o disposto no art. 55-J, § 1º. e 2º., da LGPD: *§ 1º Ao impor condicionantes administrativas ao tratamento de dados pessoais por agente de tratamento privado, sejam eles limites, encargos ou sujeições, a ANPD deve observar a exigência de*

	mínima intervenção, assegurados os fundamentos, os princípios e os direitos dos titulares previstos no art. 170 da Constituição Federal e nesta Lei. *§ 2º Os regulamentos e as normas editados pela ANPD devem ser precedidos de consulta e audiência públicas, bem como de análises de impacto regulatório.* Observado o disposto acima, eventuais providências e medidas técnicas ou administrativas reativas ou preventivas devem ser necessárias, razoáveis, previamente conhecidas e factíveis de serem implementadas, levando em consideração as medidas já adotadas pelo controlador, o contexto do tratamento e do incidente e os impactos das medidas a serem determinadas não só na segurança dos dados, mas na própria atividade do controlador. Alguns exemplos de medidas são solicitar que o controlador elabore e implemente plano de ação de remediação do incidente, a solicitação de evidências do tratamento do incidente, detalhando as medidas reativas e preventivas factíveis e razoáveis para que se possa prevenir a repetição do incidente, caso seja possível. Além disso, a atuação orientadora e educativa da ANPD junto aos controladores é importante para o eventual aperfeiçoamento de processos internos que possibilitem um ambiente organizado e seguro para o tratamento de dados pessoais. Importante ressaltar que as providências e medidas técnicas e administrativas a serem determinadas pela ANPD não devem se confundir necessariamente com as sanções previstas na LGPD. A aplicação de sanções deve ser precedida do devido processo administrativo.
No momento, não temos sugestões de normativo.	

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: ASSOCIAÇÃO BRASILEIRA DAS EMPRESAS DO MERCADO DE FIDELIZAÇÃO - ABEMF

CPF/CNPJ: 21.473.443/0001-70

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS **IMPORTANTE:** Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	O risco ou o dano relevante ao titular não deve ser mensurado pelo número de indivíduos potencialmente afetados, mas, sim, pela natureza dos dados pessoais envolvidos e, cumulativamente, o tipo de incidente. Devem, ainda, ser consideradas a probabilidade de se materializar o dano, bem como seu potencial lesivo (gravidade). A título exemplificativo: um incidente envolvendo dados pessoais sensíveis pertinente ao estado de saúde de titulares tende a gerar uma possibilidade de dano mais elevado se comparado ao vazamento de endereços de e-mail que sejam públicos. Possível classificação de incidentes por tipo: • Violação de Confidencialidade: quando há uma divulgação ou acesso não autorizado ou acidental dos dados pessoais; • Violação de Integridade: quando há uma alteração não autorizada ou acidental dos dados pessoais;

	• Violação de Disponibilidade: quando há uma perda não autorizada ou acidental dos dados pessoais. Um incidente envolvendo dados pessoais que já estão disponíveis em meios públicos, por exemplo, em alguma mídia social não tem o condão de gerar risco aos direitos e liberdades do titular.
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	Não, mas deve ser divido o risco do dano. Quando um tratamento há risco, deve-se considerar, dentre outras medidas adotadas, aquelas que o controlador e/ou operador implementou para mitigá-lo. Dessa forma, de acordo com o grau de segurança e soluções tecnológicas adotadas, há que se falar em alteração da taxatividade do dado em, inicialmente, nível alto para nível médio ou baixo. Quando referido tratamento acarreta dano ao titular, este deve ser classificado, diferentemente do risco, em nível alto, médio ou baixo, de acordo com o tamanho do dano que o titular sofreu ou venha a sofrer de forma comprovada. Há que se falar em entender de forma palatável o dano claro sofrido, isso porque, de acordo com cada titular de dado, o dano em um vazamento de e-mail, por exemplo, pode ser menos impactante do que outro (quando o e-mail de um deles é público, por exemplo). O nível “baixo” deve ser associado a um incidente que não há impacto ao Titular dos dados e, assim, deve ser considerado não relevante. Sobre o risco/dano baixo, não há motivo para criar uma categoria adicional considerando seu possível impacto.
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	O risco refere-se à probabilidade de uma ameaça explorar determinada vulnerabilidade, ou seja, quando se trata de risco, o dano ainda não ocorreu (ou o risco ainda não foi materializado). Por sua vez o dano é o impacto negativo materializado ao titular dos dados, ou seja, quando um incidente de segurança da informação ocorreu e comprovadamente ocasionou dano ao titular.
O que deve ser considerado na avaliação dos riscos do incidente?	O risco deve considerar a probabilidade e a gravidade de se materializar o dano, assim como os mecanismos de mitigação, identificação e controle existentes e observados pelas entidades de tratamento envolvidas.

	De antemão, a ocorrência de um incidente não deve ser considerada uma falha na obrigação de zêlo das empresas. Nenhuma entidade, pública ou privada, tem condições de garantir a segurança absoluta do tratamento de dados. A segurança dos dados é uma atividade complexa, que requer o monitoramente contínuo, bem como processos internos bem estruturados. Há diversas ameaças externas, sendo que o grau de sofisticação das atividades não lícitas é cada dia maior. Não é recomendável que a regulação dos incidentes aborde o tema de forma enumerativa e exaustiva. Afinal, as ameaças são mutáveis e estão constantemente em evolução, as tecnologias e serviços dispostos de forma legítima aos titulares avança, bem como há diversas possibilidades de incidentes. Assim, uma regulação que aborda o tema de forma consistente, porém flexível, é altamente recomendável de forma a acompanhar a evolução das tecnologias e atividades empresariais. Devem ser considerados a natureza dos dados afetados, os serviços/produtos envolvidos, a forma como os dados foram tratados, o tipo de tecnologia e processamento utilizados para o tratamento, bem como aqueles que poderão ser utilizados para, se e quando possível, afastar ou minimizar o risco. Deve-se levar em conta os cutos e procedimentos necessários, bem como a probabilidade e a gravidade dos riscos em relação aos direitos e liberdades dos titulares.
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	As informações indicadas no referido artigo são suficientes.
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	Considerando que pode haver um lapso temporal entre a descoberta de um incidente e o efetivo envolvimento das áreas e pessoas responsáveis, é recomendável um prazo de até 10 (dez) dias úteis para a comunicação de incidentes de nível alto ou médio. Sugere-se o prazo de 10 dias úteis para o controlador notificar à ANPD sobre um incidente, contados a partir do momento em que ele efetivamente verificar que, (i) o incidente envolve dados pessoais; (ii) a organização noticiante é a controladora da respectiva base de dados pessoais objeto do incidente e (iii) a análise do score do incidente leve a conclusão de que há risco ou dano aos titulares de dados. Ou seja, uma vez confirmado o incidente de forma inequívoca, o controlador deveria ter o

	prazo de 10 (dez) dias úteis contados desta confirmação para compilar as informações exigidas pela LGPD (e posterior regulamentação) a fim de comunicar o incidente à ANPD. Desta forma, a ANDP será informada de maneira mais apropriada sobre o incidente, evitando-se, assim, comunicações excessivas e sem conteúdo relevante à ANPD que podem desviar o foco da autoridade para temas efetivamente relevantes. Prazo útil para a identificação inicial mais efetiva sobre o que de fato ocorreu e se e quais dados pessoais foram afetados. Incidentes de nível baixo não geram impactos negativos ao Titular, portanto não é necessário que o Controlador notifique a ANPD ou o Titular, apenas registre o incidente formalmente em seu processo interno. Observação: Sugerimos que o Operador possa comunicar diretamente a ANPD somente se o incidente ocorrer sob sua gestão, sua responsabilidade e vinculado a este, desde que o Controlador do dado não comunique no prazo legal determinado.
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	• Prazo para informar: 10 (dez) dias úteis • Informações que devam constar: • a descrição da natureza dos dados pessoais afetados; • a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; • os riscos relacionados ao incidente; • as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo. • Eventual atitude requerida ou sugerida ao titular.

	Observação: O Operador poderá comunicar os titulares diretamente somente se o incidente ocorrer sob sua gestão, sua responsabilidade e vinculado a este, bem como desde que o Controlador do dado não tenha comunicado no prazo legal determinado.
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	Por meios eletrônicos, preferencialmente por e-mail ou meio diverso determinado na política de privacidade, caso este dado seja de conhecimento do Controlador. Caso este dado seja comprometido ou esteja indisponível, é recomendado que o Controlador comunique em algum de seus canais que comprovadamente o titular terá acesso.
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	Quando o incidente de segurança for classificado como “baixo”, ou seja, quando o incidente não gerar impacto ao Titular dos dados, bem como quando for classificado como “alto” ou “médio”, mas que com o plano de ação, não gerou qualquer impacto ao titular.
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	O Titular não deve ser informado sobre todo e qualquer incidente. As comunicações devem ocorrer em casos de risco alto e se não tiver sido contido pelos agentes de tratamento antes que um dano possa ser efetivado. Exemplos de casos que não requerem comunicação: (i) em um caso de incidente envolvendo dados pessoais encripitados, se a chave para desencripitação não estiver comprometida, os dados pessoais não serão atingidos pelo incidente e os Titulares não precisam ser informados; (ii) houve um incidente, mas o controlador, tempestivamente, tomou todas as providências para conter qualquer dano. Não obstante o acima indicado, o Titular deve ser notificado se e quando for necessária uma ação ou omissão por parte dele. Por exemplo, incidente envolvendo o vazamento de senhas, será requerido ao Titular que troque suas senhas.

Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	Os critérios que devem ser considerados envolvem a análise do impacto quando a base de tratamento for o legítimo interesse, a classificação e criticidade dos dados, as medidas adotadas após o incidente, e o dano causado ao titular.

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA:

ABERT – ASSOCIAÇÃO BRASILEIRA DE EMISSORAS DE RÁDIO E TELEVISÃO

CPF/CNPJ: 34.055.368/0001-79

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos

titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS

IMPORTANTE: Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.

TÓPICO/QUESTÃO	CONTRIBUIÇÃO/INSTITUIÇÃO
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	A ABERT parabeniza a ANPD e todo seu corpo técnico pelo trabalho realizado até o momento e pela ampla abertura conferida à participação social por meio da presente Tomada de Subsídios, que franqueia aos mais variados atores a apresentação de contribuições logo nas primeiras etapas do processo normativo, antes que a Autoridade já tenha dado por superada as etapas de projeção de cenários e avaliação de impactos. A experiência europeia, apoiada, em grande parte, nos pareceres do *Working Party 29*[1], relaciona uma série de fatores a serem considerados na avaliação dos riscos e danos que emergem de incidentes envolvendo dados pessoais. Há, ainda, a metodologia elaborada pela ENISA (Agência da União Europeia para a Segurança das Redes e da Informação)[2], que ao sopesar outros tantos fatores, sugere uma gradação de *severidade* para incidentes. Ambos os documentos são valiosos e serão abordados em maior detalhe mais abaixo.

[1] Ou "*Grupo de Trabalho estabelecido pelo art. 29*".

[2] Do inglês *European Union Agency for Network and Information Security*

	Antes disto, vale destacar a importância de a ANPD selecionar critérios a serem fixados na regulamentação, que sirvam de base para avaliação da relevância dos incidentes, mas sem perder de vista que tais critérios, por mais claros que sejam, não serão suficientes, *per se*, para que os agentes regulados tenham absoluta segurança a respeito da necessidade de comunicar um incidente à própria Autoridade e, eventualmente, também aos titulares dos dados pessoais afetados. Vários serão os casos em que a análise das especificidades de cada incidente será necessária para que se alcance tal juízo. É evidente que se pode pensar em estabelecer '*gatilhos*' taxativos em alguns casos limítrofes, isto é, aqueles claramente irrelevantes, como uma violação de integridade de um pequeno número de cadastros de ex-clientes, contendo apenas nome e e-mail e sem impacto para prestação de dado serviço; ou, pelo contrário, aqueles evidentemente relevantes, tal qual o acesso não autorizado a grandes quantidades de dados pessoais bancários. Mas quaisquer outras situações demandarão maior cautela e um exame do caso concreto. Em exemplo: tende-se a acreditar que incidentes que acarretem risco de ou a efetiva exposição de dados tomados pela LGPD como sensíveis, como opção religiosa, devam ser classificados como relevantes. No entanto, tal relevância obviamente não existiria na situação em que o indivíduo ou um dado grupo já tivesse tornado pública esta opção religiosa. Tal exemplo, meramente hipotético, demonstra a dificuldade intrínseca que existe na criação de *gatilhos* taxativos e de *enforcement* punitivo, quando estamos lidando com incidentes de segurança envolvendo dados pessoais. Tais incidentes são absolutamente incertos em termos de extensão e forma, podendo ocorrer em contextos completamente diversos e ter consequências mais ou menos graves a depender das circunstâncias do caso concreto. Nesse sentido, por mais que a missão da norma regulamentadora seja esclarecer os comandos contidos na LGPD, conferindo-lhes maior densidade, a ABERT entende que não se pode pretender aplicar apenas critérios objetivos que desconsiderem as circunstâncias específicas de cada incidente, especialmente com viés sancionador: é preciso dar espaço aos agentes para ponderação destes critérios vis-à-vis as circunstâncias do caso concreto, especialmente se considerarmos que a LGPD e os referidos critérios serão normas transversais, isto é, aplicáveis a vários setores de atividade econômica, marcados por suas peculiaridades, práticas e diferentes riscos à proteção de dados inerentes.

	Mais ainda, seria salutar que estes critérios fossem fornecidos aos agentes de tratamento como uma referência, mas que a eles também fosse fornecido um canal de comunicação direta com a ANPD, para que, em caso de dúvidas, possam trocar informações com a autoridade e buscar assim, com mais segurança, um entendimento sobre a necessidade de comunicação, não só à própria ANPD como também aos titulares dos dados afetados pelo incidente, nos termos do art. 48, § 1º. Uma outra medida educativa que seria bastante proveitosa seria a publicação, pela ANPD, de documentos de trabalho contendo exemplos hipotéticos de incidentes de segurança, suas respectivas classificações em termos de capacidade de geração de riscos ou danos aos titulares, e consequente necessidade de notificação da ANPD e/ou dos titulares afetados. A ideia seria dar mostras da aplicação prática dos critérios adotados, dando aos agentes mais previsibilidade e segurança jurídica quanto à atuação da ANPD, a exemplo do que foi feito recentemente pelo EDPB (European Data Protection Board)[3]. Feitas estas considerações, segue-se à experiência europeia, mencionada inicialmente. O *Working Party 29* (WP 29) recomenda, em suas Orientações sobre a Notificação de Incidentes[4], que os seguintes fatores sejam considerados ao avaliar riscos e danos: (i) O tipo de violação – segundo o Parecer n º 03/2014 do WP 29, que acaba servindo de completo às Orientações neste ponto, as violações podem ser enquadradas em três diferentes categorias: • "Violação de confidencialidade" - onde há uma divulgação não autorizada ou acidental de, ou acesso a, dados pessoais. • "Violação de integridade" - onde há uma alteração não autorizada ou acidental de dados pessoais.

[3] *Guidelines 01/2021 on Examples regarding Data Breach Notification*. Disponível para consulta em 18 de março de 2021 em https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf.

[4] Orientações sobre a notificação de uma violação de dados pessoais ao abrigo do Regulamento (UE) 2016/679, revistas e adotadas pela última vez em 6 de fevereiro de 2018. Ratificadas pelo *European Data Protection Board* (EDPB) em 25 de maio de 2018. Disponíveis para consulta em 18 de março de 2021 em https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052.

- "Violação de disponibilidade" - onde há uma perda acidental ou não autorizada de acesso ou destruição de dados pessoais.

(ii) A natureza, sensibilidade e volume dos dados pessoais;
(iii) Facilidade de identificação de indivíduos;
(iv) Gravidade das consequências para os indivíduos;
(v) Características especiais do indivíduo;
(vi) Características especiais do controlador de dados; e
(vii) O número de indivíduos afetados;

A ENISA em suas *Recomendações para uma Metodologia de Avaliação da Severidade de Incidentes*[5], estabelece fórmulas para *scoring* dos ditos incidentes, de acordo com tabela reproduzida logo abaixo. A partir deste *scoring* as Autoridades dos países europeus e os controladores envolvidos podem estabelecer a necessidade de comunicar um determinado incidente à própria Autoridade ou também aos titulares.

Severity of a data breach		
SE < 2	Low	Individuals either will not be affected or may encounter a few inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).
2 ≤ SE < 3	[illegible]	Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).
3 ≤ SE< 4	High	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by banks, property damage, loss of employment, subpoena, worsening of health, etc.).
4 ≤ SE	Very High	Individuals may encounter significant, or even irreversible, consequences, which they may not overcome (financial distress such as substantial debt or inability to work, long-term psychological or physical ailments, death, etc.).

[5] Disponível para consulta em 18 de março de 2021 em https://www.enisa.europa.eu/publications/dbn-severity

	A ABERT entende que tais critérios adotados na experiência internacional, em adição possivelmente à questão do volume de dados afetados, são excelente parâmetro e podem servir de referência à ANPD para a regulamentação do tema, indicando ao mercado quais incidentes poderão ser considerados como capazes de acarretar risco ou dano relevante ao titular. Como explicitado acima, contudo, é fundamental que, uma vez definidos tais critérios, a ANPD faça seu *enforcement* de forma em princípio não punitiva, dando espaço aos agentes para aplicá-los de boa-fé e levando em consideração o caso concreto, haja vista, conforme demonstrado, que a capacidade de geração de danos dos incidentes pode variar imensamente a depender das circunstâncias de cada caso. Assim, sanções, se cabíveis, deverão ser aplicadas apenas nos casos de omissão muito graves ou de erros reiterados que tenham levado à efetiva ocorrência do incidente.
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	Para efeitos do art. 48 da LGPD, entendemos ser recomendável que a Autoridade siga no sentido de criar um sistema de avaliação capaz de identificar quais incidentes são relevantes o suficiente para que sejam comunicados (i) à própria Autoridade e (ii) não só a ela, como também aos titulares. Isto é, a regulamentação deve ser capaz de deixar claro, dentro possível, quando o risco ou dano será relevante o suficiente para comunicação à ANPD e quando ele será ainda mais relevante a ponto de justificar comunicação aos titulares. O regime organizado pelos arts. 33 e 34 da GDPR segue neste sentido: segundo o art. 33, em caso de incidentes de segurança, o agente deve notificar a autoridade *"a menos que a violação dos dados pessoais não seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares"*. Já a notificação aos titulares é devida *"quando for suscetível de implicar um **elevado** risco para os direitos e liberdades das pessoas singulares"* (grifo nosso). Os parâmetros propostos pela ENISA, mencionados no item 1 acima, fornecem interessante referência para a distinção entre os diferentes níveis de riscos ou danos que podem ser causados por cada incidente. Assim como sugestão, o nível "baixo" poderia dispensar qualquer

	notificação; o nível “médio” poderia exigir a notificação apenas à ANPD; já os níveis “alto” e “muito alto” poderiam exigir a notificação tanto à ANPD quanto aos próprios titulares afetados. Outro ponto a ser considerado (sobretudo sopesando a resposta ao item 3), em que o nível do risco se leva pelos fatores probabilidade x consequências (impactos), recomenda-se, também, que sejam considerados os *níveis das consequências*, como **por exemplo**: *Baixa: Acesso corporativo indevido envolvendo dados que não possibilita a identificação do respetivo titular.* *Média: Acesso corporativo indevido envolvendo dados pessoais que possibilita a identificação do titular.* *Alta: Vazamento de dados pessoais possibilitando a identificação do titular.* *Muito Alta: Vazamento de dados sensíveis possibilitando a identificação do titular.*
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	No plano conceitual, risco e dano podem ser definidos, em linhas gerais, respectivamente, como a possibilidade de ocorrência de um sinistro e a materialização desse sinistro, causando perdas materiais ou morais. Em maior detalhe, como esclarece, Camila do Vale Jimene, *in* LGPD: Lei Geral de Proteção de Dados comentada[6]: (i) Risco: trata-se da combinação da probabilidade de um evento vir a ocorrer e suas consequências é a ideia de correr perigo. De acordo com a doutrina de Maria Helena Diniz, risco é: 1. Possibilidade da ocorrência de um perigo ou sinistro causador de dano ou de prejuízo, suscetível a acarretar responsabilidade civil na sua reparação. 2. Medida de danos ou prejuízo potenciais, expressa em termos de probabilidade estatística

[6] LGPD: Lei Geral de Proteção de Dados comentada/ coordenadores Viviane Nóbrega Maldonado e Renato Opice Blum. – 2. ed. rev., atual. e ampl. São Paulo: Thomson Reuters Brasil, 2019.

de ocorrência e de intensidade ou grandeza das consequências previsíveis. 3. Relação existente entre a probabilidade de que uma ameaça de evento adverso ou acidente determinado se concretize com o grau de vulnerabilidade do sistema receptor de seus efeitos[7].

(ii) Dano relevante: trata-se efetivamente do prejuízo expressivo sofrido. Conforme Marcus Cláudio Acquaviva, dano significa:

Do latim *damnu*, prejuízo, perda. Prejuízo sofrido pelo patrimônio econômico ou moral de alguém. O dano pode ser material, também chamado de real, quando atinge bem economicamente apurável; ou moral, quando macula bens de ordem moral, como a honra[8].

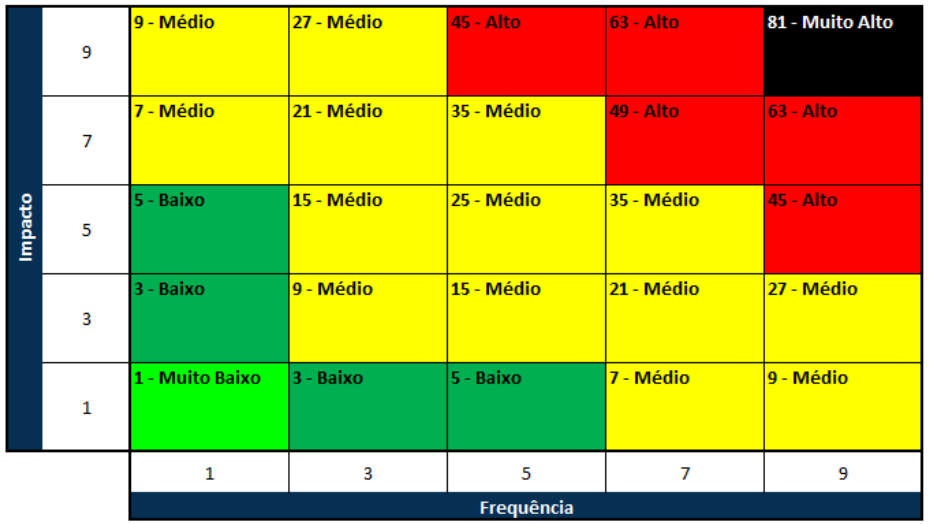
A ABERT entende que a diferenciação entre esses conceitos é útil para fins de responsabilização dos agentes em relação ao incidente ocorrido. A geração de simples risco de dano não suscita a responsabilização do agente; já se o agente causa efetivo dano ao titular, ele fica obrigado a repará-lo, nos estritos termos do art. 42 da LGPD.

Tal diferenciação contudo não agrega muito à questão da obrigação de notificar. Primeiro, porque a regra geral é que ambas as situações – incidentes que causam risco de dano e incidentes que causam efetivo dano – geram tal obrigação, nos termos do art. 48 da LGPD; segundo porque há uma dificuldade prática nesta constatação, já que estamos tratando do titular na sua individualidade, e tal questão – i.e., se o incidente causou ou não um dano efetivo à sua esfera de direitos – é algo que depende de discussão e produção de provas no caso a caso. É preciso se levar em conta ainda hipótese de que o dano pode se materializar tempos depois do incidente, de modo que o agente de tratamento não tem como antecipar sua ocorrência no momento da decisão sobre se notifica ou não notifica a ANPD e/ou o titular.

Nesse sentido, a sugestão é que a regra continue sendo de obrigação de notificação tanto de incidentes que gerem risco de dano relevante quanto de incidentes que gerem efetivo dano relevante, estando esta obrigação sujeita às gradações gerais de severidade propostas nas respostas às questões nº 1 e 2 acima.

[7] DINIZ, Maria Helena. *Dicionário jurídico*. São Paulo: Saraiva, 1998. V. 4. p. 215.

[8] ACQUAVIVA, Marcus Cláudio. *Dicionário jurídico brasileiro Acquaviva*. 9. Ed. Ver., atual. e ampl. São Paulo: Ed. Jurídica Brasileira, 1998. p. 421.

O que deve ser considerado na avaliação dos riscos do incidente?	Vide resposta às questões nº 1 e 2. Adicionalmente, recomenda-se considerar uma matriz dos níveis das consequências e a probabilidade de ocorrência dos eventos, sendo certo que eventual reincidência de evento acarretará em um aumento do nível de risco. 
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	Entendemos que o §1º do art. 48 esteja em linha com a experiência internacional e que reúna um conjunto de informações adequado para que a ANPD e o agente de tratamento possam dar bom encaminhamento às providências relacionadas com incidentes, tanto para sua apuração quanto para sua remediação. Ainda, poderiam ser constar na notificação: *- Nível do impacto do incidente (de acordo com a matriz de impacto adotado pela empresa);*

	- Ação imediata; *- Análise de causa raiz;* *- Plano de ação direcionado em atender a causa raiz;* *- Prazo para conclusão dos planos.*
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	Em primeiro lugar, indispensável debater qual seria o momento inicial a partir do qual (termo *a quo*) tal prazo passaria a correr. Nesse sentido parece inevitável que o prazo, seja qual for sua extensão, deve transcorrer a partir do momento em que o agente de tratamento tiver tomado conhecimento da gravidade do incidente. O termo de 72 horas, estabelecido pela a regulação europeia[9], nos parece um bom parâmetro, sendo certo que ele não deve ser peremptório: deve ser cabível a apresentação de razões que justifiquem o decurso de um período mais extenso entre o conhecimento da gravidade do incidente e a comunicação à Autoridade. Considerada a miríade de incidentes que podem vir a ser enfrentados e a impossibilidade de se estabelecer uma metodologia de avaliação de relevância que traga sempre respostas precisas quanto à existência ou não de riscos suficientes a justificar uma comunicação, a estipulação de um prazo geral não peremptório de 72 horas surge como uma solução regulatória equilibrada.
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	Acreditamos que a regulamentação deve se concentrar em estabelecer prazos não peremptórios, como exposto na resposta anterior, para comunicação à ANPD, sendo certo que, nos casos em que, tão logo seja possível identificar um alto risco para os titulares ou graves danos já consumados, os agentes de tratamento deverão comunica-los sem atrasos indevidos. Nesse sentido é o regime organizado pelo art. 34 da GDPR[10].

[9] Art. 33 Notification of a personal data breach to the supervisory authority

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. 2Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

[10] Art. 34 Communication of a personal data breach to the data subject

1.When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

2.The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).

	Quanto às informações a serem prestadas ao titular, a ABERT sugere que elas se restrinjam àquelas estabelecidas nos incisos I, III, IV e VI do art. 48, §1º – tais informações serão suficientes para dar um bom panorama ao titular quanto ao ocorrido e permitir tomem providências necessárias para mitigar os riscos, bem como que exerçam seus direitos, se assim o quiserem. As demais informações são técnicas e/ou procedimentais e não são de interesse do titular, devendo constar apenas da comunicação à ANPD. Será importante apenas que, na comunicação com os titulares, os agentes de tratamento se preocupem em usar uma linguagem clara e preferencialmente não-técnica, de modo a se garantir que os titulares tenham pleno entendimento do ocorrido quando receberem a notificação. Tal ressalva está estabelecida também no GDPR, no seu art. 34, item 2. Não obstante, antes de formalizar o comunicado junto ao titular, entende-se oportuno concluir as seguintes atividades: - *Identificação do nível de impacto do incidente;* - *Ação imediata;*
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	Como já exposto por ocasião das respostas apresentadas a perguntas anteriores, a LGPD é uma lei transversal, que perpassa vários setores de atividade econômica, chegando, inclusive, a interferir na prestação de serviços públicos. Cada uma dessas atividades, marcada por relações de atacado ou varejo, pela oferta de produtos ou serviços, tem suas especificidades e diferentes canais de contato com o consumidor. Um provedor de serviço por meio de um aplicativo de internet pode ter, a depender do aplicativo em questão, meios para se comunicar diretamente e de modo eficaz com os titulares a partir de mensagens sobrepostas à interface usual do próprio aplicativo. Uma concessionária de carros de altíssimo luxo pode não ter um aplicativo como ferramenta de contato com os consumidores, mas optar por ligações, seguidas de e-mails. A princípio, nenhuma dessas soluções é, por si só, superior à outra. A depender do mercado em que se estiver tratando e da relação entre controlador e titular, um mesmo meio de comunicação pode ser mais ou

	menos eficaz. Por essa razão, a ABERT entende que não seria recomendável tentar traçar, de antemão, em regulamento uma forma especifica mais adequada para comunicação com os titulares. O Regulador deve, sim, ocupar-se de verificar se, de fato, os titulares estão cientes da comunicação que lhes foi dirigida, requerendo, em caso de baixa eficácia, alterações no meio originalmente escolhido pelo controlador envolvido em no incidente. Nesse contexto, a comunicação pública (ou ampla divulgação em meios de comunicação, referida no art. 48, §3º), referida na pergunta que ora se responde, deve ser vista como mais uma alternativa, a ser empregada caso necessário e quando se revelar a mais adequada para o caso concreto. O relevante, como se expôs, é assegurar que o titular seja efetivamente notificado e cientificado do ocorrido, sendo menos importante a forma ou o meio pelo qual essa notificação é viabilizada. Assim, a regulamentação pode até listar meios de notificação a serem adotados pelos agentes de tratamento, mas deverá fazê-lo, se for o caso, de forma exemplificativa, não exaustiva, fornecendo aos agentes apenas referências que os orientem quando diante de um incidente que demande sua comunicação aos titulares dos dados.
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	Em linha com o exposto na resposta às questões 1 e 2 acima, a ABERT entende que os agentes de tratamento poderão ser dispensados da obrigatoriedade de notificar nos casos em que o incidente de segurança seja considerado de severidade “baixa”, considerando a gradação proposta pela ENISA, reproduzida acima. Em tais situações, o incidente será considerado incapaz de gerar risco de danos aos titulares ou capaz de gerar danos apenas desprezíveis, como aborrecimentos que podem ser superados fácil e rapidamente. Ao ver da ABERT, nessas situações, os custos da notificação – tanto de elaboração e envio, sob a perspectiva do agente de tratamento, quanto de recebimento e processamento, sob a perspectiva da ANPD, não compensam seus benefícios, vis-à-vis os baixos ou inexistentes riscos que geram. A esse respeito das exceções à obrigatoriedade de notificar, as Orientações nº 01/2021 do *European Data Protection Board*[11]

[11] *Guidelines 01/2021 on Examples regarding Data Breach Notification*. Disponível para consulta em 18 de março de 2021 em https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf.

	são de especial valia para orientar o presente debate, fornecendo uma série de exemplos práticos de incidentes que de fato não demandam a referida notificação.
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	Vide resposta às questões 1 e 2.
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	Vide resposta às questões 1 e 2 acima. Adicionalmente, pode-se considerar, também, os demais frameworks de segurança da informação, por exemplo ISO 27001/ 27002 (itens 16.1.1, 16.1.4, 16.1.5).
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	
SUGESTÃO DE NORMATIVO, SE HOUVER	

Art. Xxxx ....
Art. Xxxx ....

A

CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

ABES – ASSOCIAÇÃO BRASILEIRA DAS EMPRESAS DE SOFTWARE

CPF/CNPJ: 57.004.897/0002-20

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS IMPORTANTE: Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	A base da análise deve ser semelhante à utilizada na GDPR, onde um dano seria considerado relevante se houvesse desvio de utilização, dano financeiro, reputacional ou físico ao titular. No entanto, esta análise pode ser demasiado subjetiva. Neste contexto, o RIPD poderia auxiliar nesta avaliação. Na eventualidade de incidentes ocorridos em processos que tivessem um RIPD com riscos bem estabelecidos, seria mais fácil identificar os casos onde houvesse risco de dano relevante.
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	O site da ANPD em seu documento "Comunicação de Incidentes de Segurança" (https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca), define INCIDENTE como sendo "*qualquer evento adverso, confirmado ou sob suspeita, relacionado à violação na segurança de dados pessoais*". Ao considerarmos essa redação em conjunto com o texto do art. 48 da LGPD, qualquer ocorrência envolvendo segurança da informação, confirmada ou não, com potencial para causar dano relevante, deveria ser comunicada à autoridade. Deste modo, sugerimos alterar a definição de INCIDENTE que consta do site da ANPD de modo a considerar apenas os casos confirmados e não aqueles ainda não confirmados com potencial de dano. Seria prudente inferir a relevância e o impacto do incidente a partir da análise do risco a ele associado. Para conferir maior tangibilidade a esta avaliação, recomendamos considerar as respostas às seguintes perguntas para, a partir delas, aplicar uma gradação ao incidente que possa representar sua relevância (Score).

	• A informação pode ser facilmente relacionada à um individuo? • O dado está em formato legível acessível ou necessita de técnicas/conhecimentos especiais para fazê-lo? • Este dado pode ser usado de forma maliciosa para causar dano ao titular? • Está limitado à um pequeno grupo ou um grande número de titulares? • O objeto do incidente contém dados pessoais sensíveis? • Qual a natureza das atividades do controlador envolvido no incidente? • São dados financeiros ou de saúde? • Os dados vazados podem causar dano financeiro, físico ou reputacional? Adicionalmente a Autoridade poderia se valer do guia sobre incidentes da EDPB (https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf), utilizando exemplos semelhantes aos lá descritos e associar níveis de dano para cada um deles. Este material ajudaria Controladores a identificar quais processos acarretariam mais riscos ao titular, e consequentemente causariam mais danos em caso de incidentes.
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	Vide resposta acima
O que deve ser considerado na avaliação dos riscos do incidente?	Quando falamos de incidente, falamos necessariamente de seu dano ou impacto. A avaliação da relevância do incidente será determinada pelo Score resultante das respostas às perguntas mencionadas acima a fim de estipular objetivamente o grau de dano aos titulares.
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	A lista que consta do art. 48 já é suficiente.
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	Após a confirmação de um incidente, e caso seu Score indique que houve impacto relevante, a comunicação do incidente poderia acontecer em duas etapas: 1- O Controlador teria um prazo de 72h para enviar, exclusivamente à ANPD, uma Comunicação Preliminar descrevendo os aspectos relevantes do Incidente. 2- Após o envio da Comunicação Preliminar, o Controlador teria o prazo de 10 dias úteis para

	aprofundar a investigação do ocorrido, enviando à ANPD e aos Titulares o Relatório Complementar, cujo conteúdo incluiria as informações constantes do §1º do art. 48.
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	Tal como foi abordado no item anterior, uma vez constatado o incidente, caso o Score indique a necessidade da notificação, esta será feita inicialmente à Autoridade, em até 72h, por meio da Comunicação Preliminar. Após a investigação detalhada do incidente, caso se confirmem as hipóteses constantes da Comunicação Preliminar, ANPD e Titulares devem ser comunicados por meio do Relatório Complementar, em até 10 dias úteis. Com relação à comunicação dos Titulares, todos os itens devem ser incluídos tal como especifica o §1º do art. 48 da LGPD.
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	Se o número de titulares afetados pelo incidente for inferior a um determinado número, a notificação deve ser individualizada. Adicionalmente, se for muito difícil encontrar as informações de contato de todos os Titulares ou se o número de indivíduos afetados atingir um limite onde seja muito caro ou trabalhoso notificá-los individualmente, ou se a notificação precisar ser comunicada com urgência devido ao alto risco, deve ser feito um comunicado à imprensa ou postagens na Internet. Essa prática se assemelha ao conceito de “notificação substituta” que é utilizado em lei do Estado da Califórnia-EUA, onde os indivíduos são notificados diretamente, a menos que certas condições sejam atendidas (Ref . Civil Code - CIV DIVISION 3. OBLIGATIONS [1427 - 3273.16] (Heading of Division 3 amended by Stats. 1988, Ch. 160, Sec. 14.) PART 4. OBLIGATIONS ARISING FROM PARTICULAR TRANSACTIONS [1738 - 3273.16] (Part 4 enacted 1872.) TITLE 1.8. PERSONAL DATA [1798 - 1798.78] (Title 1.8 added by Stats. 1977, Ch. 709.) CHAPTER 1. Information Practices Act of 1977 [1798 - 1798.78] (Chapter 1 added by Stats. 1977, Ch. 709.)

	ARTICLE 7. Accounting of Disclosures [1798.25 - 1798.29] (Article 7 added by Stats. 1977, Ch. 709.)) Segue um exemplo da Lei de Notificação de Violação de Dados da Califórnia, onde os valores deveriam ser adequados à realidade brasileira: Aplica-se a Notificação Substituta, se a pessoa ou empresa demonstrar que o custo para realizar a notificação ultrapassaria duzentos e cinquenta mil dólares ($ 250.000), ou que a classe afetada de pessoas sujeitas a serem notificadas exceda 500.000, ou a pessoa ou empresa não tenha informações de contato suficientes. A notificação de substituição consiste de: (A) Aviso por e-mail quando a pessoa ou empresa tiver um endereço de e-mail para as pessoas em questão. (B) Publicação conspícua, por um período mínimo de 30 dias, do aviso na página do site da Internet da pessoa ou empresa, se a pessoa ou empresa mantiver um. Para os fins deste subparágrafo, postagem conspícua no site da Internet da pessoa ou da empresa significa fornecer um link para o aviso na página inicial ou na primeira página significativa após entrar no site da Internet em um tipo maior do que o texto ao redor, ou em tipo contrastante, fonte ou cor ao texto circundante do mesmo tamanho, ou destacada do texto circundante do mesmo tamanho por símbolos ou outras marcas que chamem a atenção para o link. (C) Notificação em grandes mídias.
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	Conforme nossa sugestão para a adoção de um Score que indique a relevância do incidente, a decisão sobre comunicação ou não dependerá inteiramente do resultado desse Score.
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	Vide resposta anterior.
Quais são os possíveis critérios a serem adotados pela ANPD na análise	A própria análise de risco do RIPD ou a gradação baseada nas perguntas propostas no item 2 desde formulário.

da gravidade do incidente de segurança? (art. 48, §2º)	
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	a) Gestão de riscos (ISO 31000), b) ISO 27005, c) Documento do ENISA (https://www.enisa.europa.eu/publications/dbn-severity) e d) Guia sobre incidentes da EDPB (https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf).
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	As sugestões de providências devem estar alinhadas com as características do incidente identificado. Considerando que houve um incidente em um determinado processo, e este processo havia sido submetido à uma análise de risco, e os riscos foram identificados e mitigados pela implementação de controles e algum destes controles falhou, ocasionando o incidente, a Autoridade deve concentrar suas recomendações orbitando neste contexto: Revisão dos riscos já mapeados, identificação de novos riscos, controles implementados, controles adicionais a implementar, etc.
Outras sugestões:	Se uma organização evidenciar que implementou todas as salvaguardas técnicas, administrativas e físicas necessárias, tendo feito tudo sob seu controle e ainda foi violada, então deve haver algum tipo de isenção de penalidades para eles (desde que também sigam procedimentos de notificação). As penalidades devem ser reduzidas, mitigadas ou isentas.

Colocando-nos à disposição para quaisquer esclarecimentos.

Atenciosamente,

Rodolfo Fücher
Presidente Executivo
ABES – Associação Brasileira das Empresas de Software
Por um Brasil mais digital e menos desigual

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: ABINEE - Associação Brasileira da Indústria Elétrica e Eletrônica

CPF/CNPJ: 62.510.318/0001-70

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS **IMPORTANTE:** Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	Um incidente pode acarretar risco ou dano relevante ao titular, dependendo do volume e da natureza dos dados, bem como da gravidade e da probabilidade de se concretizar. Podemos citar três critérios para avaliar o risco ou dano como relevante: 1) A **gravidade,** que representa a magnitude de um risco ou dano. Depende essencialmente do nível de identificação dos dados pessoais e do nível de consequências dos potenciais impactos; 2) A **probabilidade,** que representa a viabilidade de ocorrer um risco ou dano. Depende essencialmente do nível de vulnerabilidades dos ativos de suporte que enfrentam o nível de recursos das fontes de risco para explorá-los; e 3) O **contexto,** que representa a amplitude de um risco ou dano. Depende essencialmente de quantos titulares são afetados, do eventual impacto econômico, bem como do tempo necessário para ser efetivamente mitigado. A decisão sobre a possibilidade de um incidente acarretar risco ou dado ao titular deverá ser feita individualmente pelo controlador dos dados, considerando o contexto e as especificidades de cada

<table>
<tr><td></td><td>atividade empresarial. A ANPD deve evitar estabelecer normas prescritivas e que definam, de antemão, tais situações.</td></tr>
<tr><td>O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?</td><td>A partir dos critérios mencionados acima, entendemos que riscos ou danos devem ser subdivididos em categorias de gravidade, facilitando a identificação daqueles que devam ser considerados como relevante:
- Impacto muito elevado para os titulares dos dados.
- Elevado impacto para os titulares dos dados.
- Impacto moderado para os titulares dos dados
- Nenhum ou muito pouco impacto para os titulares dos dados

Via de regra o incidente entendido como sendo de risco baixo não deve ser considerado relevante para fins de comunicação à ANPD. Incidentes de segurança são efeitos corriqueiros e esperados e a implementação de todas as medidas técnicas e organizacionais possíveis para que eles sejam evitados não irá, necessariamente, eliminá-los.</td></tr>
<tr><td>Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?</td><td>O risco e os danos devem ser distinguidos de acordo com o nível de gravidade do incidente abaixo:

<table>
<tr><th>Classificação</th><th>Nível de Gravidade</th><th>Critérios</th><th>Prioridade do Incidente Correspondente</th></tr>
<tr><td rowspan="2">Relevante</td><td>Crítico</td><td>Impacto muito elevado para os titulares dos dados</td><td>Um Incidente que cause uma interrupção completa, real ou potencial, da prestação de serviços e aos usuários / clientes / ambiente de produção crítico ou operação comercial. Os usuários / clientes não podem utilizar um ou mais serviços essenciais pré-definidos até que a prestação de serviços seja restaurada.
Não há uma solução imediata.</td></tr>
<tr><td>Maior</td><td>Elevado impacto para os titulares dos dados</td><td>Um Incidente que cause uma interrupção ou degradação significativa, real ou potencial, da prestação de serviços e aos usuários / clientes / ambiente de produção crítico ou operação comercial.</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td>
<table>
<tr><td></td><td></td><td></td><td>Um plano de contingência permitirá que os afetados atinjam uma funcionalidade aceitável durante o evento.</td></tr>
<tr><td></td><td>Médio</td><td>Impacto moderado para os titulares dos dados</td><td>Um incidente que causa a incapacidade de trabalho a muitos usuários / clientes. Embora o impacto imediato seja moderado, o risco de aumento do impacto é aparente, tornando-se possivelmente relevante.</td></tr>
<tr><td>Irrelevante</td><td>Menor</td><td>Nenhum ou muito pouco impacto para os titulares dos dados</td><td>Um Incidente que provoque uma interrupção ou degradação mínima da prestação de serviços aos usuários / clientes, ao seu ambiente de produção ou à sua operação comercial.</td></tr>
</table>

Recomendamos que a ANPD não considere o volume detitulares afetados como um critério para avaliar a gravidade do incidente em termos de sua qualificação de risco.. Dependendo do contexto e das especificidades da atividade empresarial do controlador, o número de usuários afetados não é um indicador que reflete de forma apropriada os danos reais ou a probabilidade de danos que um indivíduo possa sofrer em razão de um incidente de segurança. Empresas que oferecem serviço a consumidor final poderá ter uma gama enorme de titulares de dados mas o eventual incidente de segurança de um dado corriqueiro, tal como o endereço de email, não necessariamente implica que aquele incidente seja de alto risco ou relevância.</td></tr>
<tr><td>O que deve ser considerado na avaliação dos riscos do incidente?</td><td>Conforme mencionado anteriormente, deve ser considerado:
O volume e a natureza dos dados envolvidos;
A gravidade;
A probabilidade; e
O contexto da atividade do controlador, da coleta e dos dados possivelmente afetados.
Importante notar que nem todo o incidente de segurança se concretiza em risco ou dano ao titular de dados pessoais (destacamos essa questão na pergunta abaixo sobre eventuais exceções da obrigatoriedade de notificação).</td></tr>
</table>

Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	As informações listadas no §1º do art. 48 já são suficientes. Sugerimos que a ANPD elabore um formulário simplificado para permitir a agilidade na submissão da comunicação pelos controladores de dados pessoais.
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	Entendemos ser razoável que os controladores possam informar a ANPD sobre um incidente de segurança em até 30 dias após a sua confirmação. O prazo atualmente previsto na GDPR, assim como aquele utilizado como referência no formulário divulgado pela ANPD, é demasiadamente escasso e impraticável para o levantamento das informações fixadas na lei como relevantes. Nesse sentido, sugerimos que a ANPD considere uma notificação preliminar, com informações pouco detalhadas para que o controlador indique à ANPD que pode ter havido um incidente de segurança que gere riscos ou danos aos titulares – essa notificação simplificada sim em um prazo de 48 ou 72 horas e aceite que a comunicação prevista na LGPD possa ser enviada no prazo de 30 dias a contar da notificação prévia. Tal prazo alargado permitirá que os controladores tenham efetivo conhecimento do incidente de segurança ocorrido e possam trazer ao conhecimento da Autoridade um exercício efetivo sobre os potenciais riscos ou danos aos titulares identificados, assim como o conjunto de medidas de mitigação que tenham sido mapeadas. Essa notificação escalonada já é hoje utilizada no ordenamento brasileiro, a exemplo de situações envolvendo a ANVISA. Ela estipula um prazo inicial de 72h para pré-notificação e depois mais um prazo de 60 dias para preencher todas as 10 etapas do formulário (investigação/análise da causa raiz)[1].
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que	Após notificar a ANPD, o controlador deverá ter até 30 dias para analisar e avaliar os riscos e danos atrelados ao incidente de segurança confirmado, conforme os critérios que apresentamos acima, bem como para identificar as medidas de mitigação pertinentes.

[1] https://www.gov.br/anvisa/pt-br/centraisdeconteudo/publicacoes/servicosdesaude/notas-tecnicas/nota-tecnica-n-05-2019-gvims-ggtes-anvisa.pdf

informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	Entendemos que a definição da forma mais adequada para a realização da comunicação do incidente aos titulares deve ser definida pelas empresas e organizações de modo que seja possível uma avaliação caso a caso, considerando a natureza da atividade da empresa, o contexto da coleta e do próprio incidente de segurança, a natureza dos dados pessoais objeto do incidente, o volume dos dados, dentre outros. • Se o número de titulares afetados for inferior a um determinado número, a notificação pode ser individualizada. • Se for muito difícil encontrar as informações de contato de todos os titulares envolvidos, ou se o número de titulares afetados atingir um limite onde seja muito trabalhoso notificá-los individualmente, a organização pode optar por criar avisos em seus respectivos sites, ou até mesmo optar pela divulgação do fato em outros meios de comunicação.
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	Caso o incidente de segurança identificado e confirmado pelo controlador não apresentar características de gravidade, probabilidade e contexto consideradas pertinentes de um "risco ou dano relevante", conforme os critérios que listamos acima, entendemos que o controlador poderá optar por não informar a ANPD. Além disso, entendemos também não ser necessária a obrigatoriedade da notificação de casos em que medidas de segurança apropriadas forem implementadas. Por exemplo, de acordo com a Lei de Proteção de Dados da Irlanda[2], o controlador não é obrigado a notificar um incidente de segurança quando ele tiver implementado medidas de proteção tecnológica e organizacional adequadas que foram aplicadas aos dados pessoais afetados pela violação de dados pessoais, em particular quando as referidas medidas, incluindo a criptografia, tornam os dados pessoais ininteligíveis para qualquer pessoa que não esteja autorizada a acessá-lo, ou até mesmo quando tiver tomado medidas em

[2] http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/print.html

	resposta à violação de dados pessoais que garantem que o elevado risco para os direitos e liberdades do titular em causa decorrente da violação já não é provável de se concretizar.
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	O incidente com nível de gravidade classificado como menor (nenhum ou muito pouco impacto para os titulares dos dados) não deve ser informado aos titulares dos dados. Na prática uma super notificação de incidentes de segurança aos titulares, ou mesmo notificações muito detalhadas poderão ter o efeito contrário ao desejado, tornando tais comunicações corriqueiras e sendo tratadas pelos titulares de maneira relevante.
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	Ver a resposta à pergunta 1 e a tabela apresentada à pergunta 3.
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	Sim, entendemos que a metodologia de gestão de risco seja a mais recomendada, a qual foi amplamente explorada nos seguintes documentos: • ISO 31000:2009 Risk management — Principles and guidelines • ISO/IEC 27035-2:2016 Information Technology — Security Techniques — Information Security Incident Management • NIST Special Publication 800-61, Revision 2, Computer Security Incident Handling Guide. A gestão de risco é um elemento central do princípio de responsabilidade e prestação de contas, fazendo com que as organizações maximizem os benefícios potenciais do tratamento de dados, ao mesmo tempo em que reduz de forma mais eficaz quaisquer impactos negativos potenciais sobre os titulares de dados, na medida em que prioriza a identificação e a análise de riscos, bem como a tomada de decisões que sejam escalonáveis e proporcionais aos fatos e contextos nas quais o controlador está inserido.

Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	Tendo em vista que a LGPD é estruturada na premissa de gestão de risco por parte dos agentes de tratamento de dados pessoais e a lei optou por uma abordagem bastante ampla no sentido de que as organizações devem adotar medidas técnicas e administrativas para o seu cumprimento e segurança dos dados não nos parece adequado que a ANPD venha a fixar as medidas de maneira prescritiva no texto normativo. Deverá ficar a cargo de cada organização a fixação das medidas mais apropriadas ao seu contexto fático. Cumpre lembrar que ainda que haja um incidente de segurança, não necessariamente a organização deixou de implementar medidas técnicas e administrativas compatíveis com os princípios e premissas fixados na LGPD. Eventuais sugestões de providência irão depender do incidente de segurança da informação identificado e da estrutura do controlador, exigindo uma análise de caso a caso e até mesmo recorrência de um incidente de segurança de determinada natureza dentro da organização.
Outras Questões – Formulário de Notificação	Entendemos que o formulário disponibilizado no site da ANPD tem caráter transitório. No entanto, gostaríamos de pontuar algumas questões que achamos que precisam ser endereçadas na versão final do documento: 1) De acordo com o artigo 48 da LGPD, o controlador é o único agente de tratamento responsável por comunicar a ANPD sobre incidentes de segurança. Sendo assim, recomendamos que seja excluída a pergunta onde o notificante poderia se identificar como operador, presumindo que ele seja naturalmente o controlador; 2) No momento da comunicação, o controlador dificilmente terá a visibilidade de todos os tipos de dados pessoais afetados, pois esse levantamento será realizado durante o processo de análise e avaliação de riscos. Portanto, sugerimos que ao perguntar qual a natureza dos dados afetados, tenham apenas duas opções: i) dados pessoais; e ii) dados pessoais sensíveis; 3) O formulário atual exige que o notificante apresente um número de CPF ou de CNPJ. Exigir essas informações pode impedir que empresas estrangeiras não estabelecidas no país, mesmo que sujeitas à LGPD, submetam notificações de incidentes de segurança;

	4) No momento da notificação, entendemos que seja fundamental que o controlador indique apenas as medidas de segurança que foram adotadas para mitigar os riscos ou danos atrelados ao incidente de segurança em questão. Isso porque é de nosso entendimento que todas as medidas técnicas e organizacionais de segurança compõem a estrutura de gestão de risco e são, portanto, muito complexas para serem apresentadas exaustivamente em uma comunicação
SUGESTÃO DE NORMATIVO, SE HOUVER	
Art. Xxxx	
Art. Xxxx	

ABIPAG

Associação Brasileira de Instituições de Pagamentos

São Paulo, 24 de março de 2021

À

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

Esplanada dos Ministérios – Bloco C – 2º andar – Brasília – DF

Por e-mail: consultapublica@anpd.gov.br

Ref.: Tomada de Subsídios nº 2/2020

1. A **Associação Brasileira de Instituições de Pagamentos ("ABIPAG")**, inscrita no CNPJ sob o nº 26.425.404/0001-10, tem a missão institucional de representar instituições entrantes no mercado de meios de pagamentos eletrônicos, tais como instituições de pagamento, credenciadoras e emissoras de moeda eletrônica, e instituições financeiras na modalidade sociedade de crédito direto, sobretudo em prol da promoção da livre concorrência, livre iniciativa e isonomia no mercado.

2. Por se tratar de um tema de extrema relevância aos seus associados e respectivos clientes – usuários finais recebedores de transações de pagamento –, a ABIPAG vem, respeitosamente, à presença da Autoridade Nacional de Proteção de Dados ("**ANPD**"), apresentar suas contribuições à Tomada de Subsídio nº 2/2020, referente à regulamentação do dever de comunicação de incidentes de segurança que possam acarretar risco ou dano relevante aos titulares, nos termos do § 1º do art. 48 da Lei Geral de Proteção de Dados Pessoais ("**LGPD**").

3. Inicialmente, a ABIPAG gostaria de enaltecer a iniciativa de V.Sas., por se preocuparem em estabelecer, desde o início do processo de regulamentação da LGPD, um diálogo aberto com a sociedade, de maneira a proporcionar um ambiente de maior segurança jurídica, possibilitando que o respeito aos direitos dos titulares dos dados pessoais caminhe *pari passu* com as políticas públicas que objetivam o desenvolvimento e crescimento econômico e a transformação digital do país, o que está em linha, aliás, com os comandos da Lei nº 13.874/2019, que instituiu a Declaração de Direitos de Liberdade Econômica.

4. A ABIPAG ressalta, neste sentido, que embora seja importante promover o alinhamento das regras nacionais sobre incidentes de segurança envolvendo dados pessoais àquelas já adotadas em outros países, não se pode perder de vista as características específicas do mercado brasileiro. E nesse sentido, deve-se evitar que a proteção de dados pessoais no Brasil se oriente por formalismos que acabem por prejudicar a competitividade empresarial e a própria eficiência da ANPD no exercício de suas atribuições.

5. Por este motivo, a ABIPAG manifesta desde logo sua concordância com o posicionamento externado por esta Autoridade em sua Nota Técnica nº 3/2021/CGN/ADPD,[1] ao anotar a necessidade da construção de limites claros que permitam distinguir incidentes de segurança que possam trazer riscos ou danos relevantes – justificando a movimentação das máquinas privada e pública – daqueles cuja ameaça, se houver, poderia ser desconsiderada, eis que sem potencial danoso. Tais limites, na avaliação da ABIPAG, deverão ser claros para garantir maior segurança jurídica aos controladores e auxiliar na redução do estoque de notificações a serem enviados à Autoridade.

6. Ao mesmo tempo em que não se deve deixar de realizar, na maior extensão possível, os comandos da LGPD, é medida de rigor que a ANPD elabore uma norma com critérios proporcionais e razoáveis, alinhada com as melhores práticas regulatórias, de forma a (i) evitar o aumento dos custos regulatórios para os agentes de tratamento de dados, o que prejudicaria em maior grau os *players* entrantes e/ou de menor porte, e (ii) assegurar um grau de eficiência à Autoridade, para que não seja obrigada a despender recursos financeiros e humanos no processamento de notificações relacionadas a incidentes cujo potencial danoso seja baixo. Esta "justa medida" é, aliás, reportada como um dos problemas que as autoridades supervisoras de países europeus vêm sofrendo, conforme bem pontuado no *Report from the Multistakeholder Expert Group on the GDPR evaluation*[2].

7. Dado o processo de amadurecimento do tema no Brasil e do papel educativo da ANPD, que busca instituir no país uma verdadeira cultura de proteção de dados, sugere-se que, neste primeiro momento, a ANPD concentre seus esforços na elaboração de diretrizes gerais, a serem explicitadas por meio de *soft laws*, a exemplo de guias de boas-práticas e manuais, bem como

[1] Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-imagens/sei_00261-000098_2021_67-nt-ts-incidente.pdf.
[2] Disponível em https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=21356.

na resposta a consultas, que serviriam de balizas para estruturação de procedimentos internos visando a dar cumprimento às determinações legais.

8. Por fim, para fins da elaboração de regulamentos como o que ora se debate, entende-se ser fundamental não só a **realização de uma análise de impacto regulatório**, conforme já previsto no § 3º do art. 55-J, XXIV, da LGPD, mas também de um **juízo de proporcionalidade**, guiando-se pelos critérios de adequação, necessidade e proporcionalidade em sentido estrito, de modo a verificar, respectivamente, se determinada medida proposta é adequada e necessária para o atingimento do fim proposto, se o objetivo não pode ser promovido de outra maneira com menores riscos à livre concorrência e ao desenvolvimento econômico, bem como se os motivos que a fundamentam têm o peso suficiente para justificá-la.

9. Nesse sentido, importante que a regulação da ANPD tenha como foco negócios que representam grande risco aos seus usuários, uma vez que tratam grande volume de dados e que, por terem elevado poder econômico, têm condições de garantir que todos os mecanismos necessários à proteção aos direitos dos titulares de dados sejam respeitados e de arcar com ônus regulatório proporcional ao risco que representam. Chama-se atenção, por exemplo, para as grandes empresas de tecnologia, as BigTechs, que, apesar de contarem com tamanho poder econômico, que lhes dão maior capacidade de evitar que aconteçam, têm protagonizado incidentes relevantes no tratamento de dados.

10. Feitas estas considerações preliminares, a ABIPAG apresenta a seguir, em formulário próprio anexo, suas contribuições às questões propostas pela ANPD, com o intuito de colaborar para o aprimoramento do ambiente regulatório no País.

11. Sendo o que servia para o momento, a ABIPAG agradece mais uma vez a oportunidade de se manifestar, reforçando seu compromisso com a promoção da livre concorrência, livre iniciativa e isonomia do mercado, e coloca-se à disposição para quaisquer esclarecimentos e informações adicionais que se façam necessários.

Atenciosamente,

ABIPAG – ASSOCIAÇÃO BRASILEIRA DE INSTITUIÇÕES DE PAGAMENTOS

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2/2021

NOME DA INSTITUIÇÃO: ASSOCIAÇÃO BRASILEIRA DE INSTITUIÇÕES DE PAGAMENTOS - ABIPAG

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS **IMPORTANTE:** Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	De início, ressalta-se que um dos desafios regulatórios colocado perante a ANPD é justamente o de encontrar a justa medida, i.e., a opção proporcional, que assegure grau de proteção dos titulares de dados, sem, no entanto, erguer barreiras regulatórias que inviabilizem a realização da atividade econômica. Nesta linha, a ABIPAG reitera que a ANPD deveria se preocupar em privilegiar, sempre que possível, uma abordagem educativa, concentrando esforços neste primeiro momento na edição de *soft laws*, a exemplo de guias de boas-práticas e manuais, bem como na resposta a consultas, que serviriam de balizas para estruturação de procedimentos internos visando a dar cumprimento às determinações legais. Com relação ao dever de comunicação quanto a incidentes de segurança, a ABIPAG avalia que as experiências internacionais sobre o tema são um norte inicial importante e que deveriam ser levadas em conta, em certa medida, para a determinação de critérios para a identificação de incidentes com relevante potencial lesivo ao titular. Destacam-se, nesse sentido, as diretrizes da União Europeia sobre DPIA e notificação de violação de dados, a legislação e diretrizes australianas e as diretrizes espanholas. Na mesma linha, é importante que ANPD considere as dificuldades já experimentadas em outros países para atendimento das regras sobre incidentes de segurança. Dentre tais dificuldades, destacam-se algumas daquelas mencionadas pelo *Multistakeholder Expert Group to Support the Application of Regulation (EU) 2016/679*[3], resumidas a seguir:

[3] Multistakeholder Expert Group to Support the Application of Regulation (EU) 2016/679. Disponível em https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=41708.

	• **Dificuldade para identificar o momento em que se tem ciência de um incidente de segurança**. Muitas vezes há demora (i) para se identificar, com grau razoável de certeza, a ocorrência de um incidente de segurança e (ii) para mensurar o seu potencial lesivo, o que pode resultar, por consequência: (a) na notificação de todos os incidentes de segurança envolvendo dados pessoais, sobrecarregando as autoridades supervisoras; ou (b) no atraso do alcance de um grau razoável de certeza sobre a lesividade do incidente de segurança e, por temor de eventuais sanções, na sua não notificação às autoridades supervisoras. • **O *threshold* para notificação de incidentes de segurança é relativamente baixo e a interpretação sobre o potencial lesivo dos incidentes não é uniforme entre os Estados Membros**. Por conta disso, as empresas tendem a notificar incidentes que não deveriam ser levados ao conhecimento das autoridades, a fim de evitar sanções, fazendo com que as autoridades supervisoras sejam obrigadas a lidar com inúmeras notificações. • **Necessidade de *guidelines* para garantir uma melhor compreensão dos requisitos relacionados a incidentes de segurança**. Por meio de diretrizes, deveriam ser promovidos / esclarecidos, por exemplo, (i) interpretações sobre as diferentes formas de contagem de prazo para comunicação do incidente, exemplificando, inclusive, as circunstâncias em que tal prazo poderia ser ampliado, e (ii) critérios claros sobre como identificar os incidentes de segurança que não demandam notificação, de modo a reduzir o volume de tais notificações às autoridades supervisoras. A ABIPAG entende que, na regulamentação a ser editada, caberia à ANPD definir, logo na abertura, o que viria a ser "incidente de segurança" para fins da LGPD, de modo a dar maior segurança jurídica, facilitando a identificação dessas ocorrências, de modo a se ter, com rapidez, uma mensuração de eventuais riscos ou danos causados aos titulares. Em linha com o quanto sugerido em guia recentemente disponibilizado pela autoridade[4], entende-se que essa definição deverá abarcar, além do evento adverso relacionado à segurança

[4] Disponível em: https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca.

	em si[5], o elemento dados pessoais (isto porque, como se sabe, a Lei não busca tutelar qualquer incidente, mas somente daqueles envolvendo acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito de **dados pessoais**). Além dos aspectos destacados acima, considera-se que, com relação aos critérios que demandariam a notificação de um incidente nos termos da LGPD, deveria ser considerado o seguinte: ● **Categorias de dados pessoais envolvidos no incidente de segurança**: a ABIPAG acredita que, a depender da categoria dos dados pessoais objeto do incidente, o dano poderá ser de menor grau, sendo, portanto, um fator fundamental na avaliação da relevância do incidente de segurança. Tal avaliação envolveria perguntas do tipo: o O incidente envolve apenas dados pessoais cujo acesso público à informação é facilitado, a exemplo de dados cadastrais (i.e., nome, e-mail e números de identidade) e/ou dados disponíveis em bases públicas? o O incidente alcança dados pessoais que adentram em aspectos de personalidade e/ou que ingressem no âmbito da proteção à intimidade (v.g. utilizados para avaliação / *scoring* de perfil pessoal, profissional, de consumo, de crédito, de saúde etc)? o O incidente alcança dados pessoais sensíveis e/ou protegidos por sigilo legal (sigilo bancário, sigilo das comunicações etc.)? ● **Facilidade de identificação dos titulares envolvidos no incidente de segurança**: o dano poderá ser considerado como irrelevante caso o controlador adote técnicas que dificultem e/ou inviabilizem a identificação do titular (v.g., caso utilizados métodos de pseudonimização), o que poderia tornar desnecessária a notificação do incidente.

[5] De acordo como CERT.br, um incidente de segurança pode ser definido como "qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores". Disponível em: https://cartilha.cert.br/glossario/#i.

	● **Circunstâncias do incidente de segurança**: é importante que se proceda à análise das circunstâncias do incidente para avaliar o potencial de exposição dos titulares a um alto, médio ou baixo risco, o que englobaria questionamentos do tipo: ○ Qual é a extensão do incidente em termos de (i) volume de dados e (ii) quantidade de titulares atingidos? ○ O incidente alcança dados pessoais tratados sem que os titulares tenham ciência de quem é o controlador e/ou da finalidade do tratamento? ○ O incidente envolve dados pessoais de grupos de titulares considerados vulneráveis pela legislação brasileira (e.g., crianças, adolescentes, idosos)? ● **Natureza do risco ou dano que o incidente de segurança pode causar ao titular**: considera-se importante que o controlador avalie, por conta e risco, as consequências que possam decorrer do incidente de segurança (v.g., acesso não autorizado a contas, transações fraudulentas, discriminação etc.). ● **Severidade/relevância do risco ou dano aos titulares**: adotando-se uma abordagem similar às da ENISA e AEPD, a ABIPAG sugere que a relevância do risco ou dano seja avaliada a partir da seguinte metodologia: Baixa relevância: incidentes (i) capazes de causar meros transtornos e aborrecimentos aos titulares e, portanto, representem baixa probabilidade de expor o agente de tratamento à responsabilização civil, a multas administrativas ao dano reputacional e ao litígio; e que (ii) em caso de concretização dos danos, seriam de baixo impacto pecuniário e/ou reputacional (e.g., exclusão de dados cadastrais, causando a perda do tempo útil para reinserção de tais dados).

	Média relevância: incidentes (i) capazes de causar mais do que meros transtornos e aborrecimentos aos titulares, pois trariam inconvenientes significativos, apesar de superáveis, e, portanto, representem alguma probabilidade de expor o agente de tratamento à responsabilização civil, a multas administrativas, ao dano reputacional e ao litígio; e que (ii) em caso de concretização dos danos, seriam de médio impacto pecuniário ou reputacional (e.g., danos morais, negação de acesso a serviços, despesas adicionais). Alta/Altíssima: incidentes (i) capazes de causar consequências significativas ou até mesmo irreversíveis, sendo impossível ou extremamente difícil sua superação, e, portanto, representem alta ou altíssima probabilidade de expor o agente de tratamento à responsabilização civil, a multas administrativas, ao dano reputacional e ao litígio, sendo; e que (ii) em caso de concretização dos danos, seriam de alto impacto pecuniário ou reputacional (e.g., perda de emprego, intimações judiciais, fraude ideológica ou financeira, inclusão em cadastros de inadimplentes, piora da saúde, danos psicológicos ou físicos de longo prazo, morte).
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	Conforme mencionado na resposta anterior, a ABIPAG sugere que a relevância dos riscos ou danos seja considerada a partir de três categorias, a partir das quais seria possível avaliar a sua relevância para fins de comunicação: ● Baixo risco (dano irrelevante): incidentes que (i) representem baixa probabilidade de expor o agente de tratamento à responsabilização civil, a multas administrativas, ao dano reputacional e ao litígio, sendo capazes de causar meros transtornos e aborrecimentos aos envolvidos; e que (ii) em caso de concretização dos danos, seriam de baixo impacto pecuniário ou reputacional (e.g., exclusão de dados cadastrais, causando a perda do tempo útil para reinserção de tais dados); ● Médio risco (dano pode ser relevante): incidentes que (i) representem alguma probabilidade de expor o agente de tratamento à responsabilização civil, a multas administrativas, ao dano reputacional e ao litígio, sendo capazes causar mais do que meros transtornos e aborrecimentos aos

	indivíduos, pois trariam inconvenientes significativos, apesar de superáveis; e que (ii) em caso de concretização dos danos, seriam de médio impacto pecuniário ou reputacional (e.g., danos morais, negação de acesso a serviços, despesas adicionais); ● Alto/Altíssimo risco (dano relevante): incidentes que (i) representem alta ou altíssima probabilidade de expor o agente de tratamento à responsabilização civil, a multas administrativas, ao dano reputacional e ao litígio, sendo capazes de causar consequências significativas ou até mesmo irreversíveis, sendo impossível ou extremamente difícil sua superação; e que (ii) em caso de concretização dos danos, seriam de alto impacto pecuniário ou reputacional (e.g., perda de emprego, intimações judiciais, inclusão em cadastros de inadimplentes, piora da saúde, danos psicológicos ou físicos de longo prazo, morte).
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	Em linhas gerais, risco é a possibilidade de ocorrer um dano, podendo este ser graduado conforme sugerido nas respostas anteriores. No contexto da LGPD, o risco ao titular também está relacionado com os princípios da prevenção (art. 6º, VIII) e da precaução (art. 6º, VII e X). Isto porque a Lei dispõe que os agentes de tratamento devem adotar medidas para evitar riscos (precaução) e danos concretos (prevenção) ao titular, sem, contudo, gerar qualquer direito à reparação pela mera exposição do indivíduo a tais riscos. Por outro lado, o dano pode ser entendido como a efetiva lesão de um bem jurídico, podendo esta lesão ser patrimonial ou moral, bem como individual ou coletiva. Nos termos do art. 42 da LPGD, o dano é o fundamento/elemento essencial da responsabilidade civil. Sem ele, não há o que se falar em dever de reparar o titular. Para que o dano seja constituído, deverá ocorrer um prejuízo ao titular dos dados pessoais em decorrência de violações à legislação de proteção de dados pessoais.
O que deve ser considerado na avaliação dos riscos do incidente?	Além dos critérios já mencionados nas respostas anteriores, sugere-se que a ANPD considere os seguintes critérios: ● Contexto da coleta e do incidente de segurança; ● Atividade empresarial exercida pelo controlador;

	● Probabilidade dos riscos se concretizarem; ● Boa-fé do controlador; ● Período de exposição; ● Concretização ou não do dano; e ● Medidas técnicas e administrativas adotadas para se evitar o dano ou seu agravamento.
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	Inicialmente, a ABIPAG ressalta ser fundamental que a ANPD diferencie em seu regulamento sobre incidentes de segurança a natureza da comunicação a ser repassada à autoridade daquela a ser enviada aos titulares, de caráter informativo / *press release*. Neste sentido, para compartilhamento das informações relacionadas a incidentes de segurança à autoridade, sugere-se a elaboração de um formulário eletrônico simplificado, que poderia ser preenchido por completo ou, na impossibilidade, de modo parcial com posterior complementação/modificação, em formato similar àquele adotado pelas autoridades francesa e espanhola. De modo geral, considerando as experiências estrangeiras, as seguintes informações poderiam/deveriam estar contempladas em tal formulário: ● Identidade e informações de contato do controlador (em linha com os formulários da OAIC/Austrália, OAG/Califórnia, EUA, CNIL/França, ICO/Reino Unido, AEPD/Espanha, etc.); ● Identidade e informações de contato do encarregado (em linha com os formulários da ICO/Reino Unido, AEPD/Espanha, etc.); ● Descrição do incidente de segurança (em linha com os formulários da OAIC/Austrália, OAG/Califórnia, EUA, CNIL/França, ICO/Reino Unido, AEPD/Espanha, etc); ● Descrição da natureza dos dados pessoais afetados (art. 48, § 1º, I, LGPD); ● Informações sobre os titulares envolvidos (art. 48, § 1º, II, LGPD); ● Indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados (art. 48, § 1º, III, LGPD); ● Indicação dos riscos relacionados ao incidente (art. 48, § 1º, IV, LGPD);

	• Motivos da demora, no caso de a comunicação não ter sido imediata (art. 48, § 1º, V, LGPD); e • Medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo (art. 48, § 1º, VI, LGPD); e • Método de comunicação dos titulares afetados (em linha com os formulários da OAIC/Austrália, AEPD/Espanha, etc). Além disto, deveria ser franqueado aos controladores a possibilidade de inserção de eventuais informações adicionais que entendam relevantes para compor a comunicação.
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	A ABIPAG acredita que a maior dificuldade dos agentes de tratamento de dados no que se refere a este tema, em especial daqueles de médio e pequeno porte, está nos custos e no prazo para averiguação de possíveis incidentes de segurança e para o levantamento de todas as informações necessárias. Isto porque, como se sabe, grande parte das empresas não possui recursos para contratação de um funcionário e/ou assessoria especializada para o exercício desta função e, consequentemente, o prazo para a solução de demandas acaba sendo mais extenso se comparado às empresas de grande porte. Neste sentido, bem como considerando as dificuldades apontadas por empresas estrangeiras, mencionadas na resposta à primeira questão, sugere-se que a ANPD considere as experiências internacionais e, ao mesmo tempo, estabeleça um prazo razoável e proporcional ao atual nível de maturidade de proteção de dados do mercado brasileiro – na medida do possível, em até 72 (setenta e duas) horas a partir do conhecimento do incidente, em conformidade com o art. 33 do GDPR –, para uma notificação completa ou, na impossibilidade devidamente justificada, parcial, sendo que o restante das informações poderiam ser encaminhadas pelo controlador assim que possível, de modo semelhante ao que ocorre na França[6] e na Espanha[7]. Além disto,

[6] "*Si vous ne pouvez pas fournir toutes les informations requises dans ce délai car des investigations complémentaires sont nécessaires, vous pouvez procéder à une notification en deux temps [..]*" Disponível em https://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles.

[7] "*If, at the time of notification, it was not possible to fulfil the requirement to provide all the necessary information, as detailed in the section of this guide on Notification, the information should be provided gradually, as quickly as possible and without delay*". Disponível em https://www.aepd.es/sites/default/files/2019-09/Guide-on-personal-data-breach.pdf.

	recomenda-se que o prazo fixado pela ANPD possa ser ampliado em determinadas situações (e.g., dificuldades técnicas, caso fortuito, força maior), mediante simples justificativa, conforme prevê o art. 48, § 1º, V, da LGPD. Por fim, assim como ocorre na Europa[8], ressalta-se que eventuais leis ou regulamentos específicos dispondo de modo diferenciado sobre prazos ou procedimento para notificação de incidentes de segurança por determinadas categorias de agentes de tratamento de dados pessoais deverão se sobrepor às regras gerais estabelecidas pela ANPD, em razão do princípio da especialidade. É o caso, por exemplo, do Decreto nº 9.936/2019, que determina, em seu art. 18, § 1º, ser de 2 (dois) dias úteis o prazo para comunicação de incidentes sofridos pelos gestores de banco de dados a que se refere a Lei nº 12.414/2011 (Lei de Cadastro Positivo). Porém, mesmo nestas hipóteses, recomenda-se que o prazo indicado pela norma seja considerado para realização de uma notificação completa ou parcial, podendo as demais informações necessárias serem encaminhadas em momento posterior, de modo a padronizar os procedimentos adotados pela ANPD.
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	Reitera-se as contribuições ao item anterior, sugerindo-se que a ANPD considere as experiências internacionais e, ao mesmo tempo, estabeleça um prazo razoável e proporcional considerando o atual nível de maturidade de proteção de dados do mercado brasileiro, que poderia ser de até 72 (setenta e duas) horas a partir do conhecimento do incidente, desde que este prazo possa ser ampliado em determinadas situações (e.g., dificuldades técnicas, caso fortuito, força maior, necessidade de maior prazo para levantamento de informações precisas e/ou tomada de providências determinadas pela ANPD), mediante simples justificação, conforme prevê o art. 48, § 1º, V, da LGPD) previsão do Art. 48 § 2º, I. e ii). Ressalta-se, porém, que a comunicação da ANPD e do titular não deverá ocorrer, necessariamente, de forma concomitante.

[8] O Art. 95 da GDPR dispõe que "*This Regulation shall not impose additional obligations on natural or legal persons in relation to processing in connection with the provision of publicly available electronic communications services in public communication networks in the Union in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC*". De acordo com o guia da autoridade do Reino Unido, as regras previstas na *Directive 2020/58/EC* "*takes the place of UK GDPR breach reporting obligations. You don't need to take any separate action to comply with the UK GDP*R". Disponível em https://ico.org.uk/for-organisations/guide-to-pecr/communications-networks-and-services/security-breaches/.

	Considerando as experiências estrangeiras mencionadas no item anterior, entende-se que as seguintes informações deveriam ser comunicadas ao titular: ● Identidade do controlador; ● Informações de contato do encarregado; ● Descrição simplificada e acessível do incidente de segurança; ● Descrição da natureza dos dados pessoais afetados (art. 48, § 1º, I, LGPD); ● Informações sobre os titulares envolvidos (art. 48, § 1º, II, LGPD), sendo que a comunicação em si, quando individualizada, já atenderia a esta exigência; ● Indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados (art. 48, § 1º, III, LGPD), de forma simplificada e acessível à leitura dos titulares envolvidos; ● Indicação dos riscos relacionados ao incidente (art. 48, § 1º, IV, LGPD); ● Motivos da demora, no caso de a comunicação não ter sido imediata (art. 48, § 1º, V, LGPD); e ● Medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo (art. 48, § 1º, VI, LGPD); ● Medidas recomendadas pelo controlador a serem adotadas pelo titular de modo a reduzir os riscos. Além disso, é recomendável à autoridade permitir que os controladores insiram eventuais informações adicionais que entendam relevantes para compor a comunicação.
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	A ABIPAG entende que a ANPD deveria orientar-se pelo princípio administrativo da finalidade, dando liberdade às empresas para que estabelecem os mecanismos eficazes de comunicação, abstendo-se, correlatamente, de estabelecer formalidades capazes de incrementar o custo da operação comercial das empresas, a exemplo de exigência de comunicação via postal, por telefone etc.

	Portanto, sugere-se que a ANPD adote as regras similares àquelas estipuladas pela autoridade espanhola[9] e conceda ao controlador o direito de escolher o método de comunicação dos incidentes aos titulares que entender ser mais eficaz e apropriado, podendo optar, inclusive, pela forma (i) direta, via e-mail, telefone, SMS ou outros canais de comunicação, eletrônicos ou não, ou (ii) indireta, por meio de avisos em seu site corporativo ou notas à imprensa, quando o custo da notificação direta for excessivo ou não for possível entrar em contato com todos os titulares afetados, desde que tal comunicação não tenha caráter confidencial e/ou sensível, considerando as técnicas disponíveis à época e a capacidade tecnológica do agente. Na hipótese de análises casuísticas, constate-se a insuficiência destes métodos para o atingimento dos resultados determinados na Lei, caberia, então, à ANPD, convocar o agente econômico / controlador do tratamento para com ela transacionar, tomando compromissos específicos visando ao aperfeiçoamento dos seus procedimentos internos.
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	A ABIPAG sugere que a ANPD se inspire nas regras estabelecidas pela autoridade espanhola e estabeleça as seguintes exceções à obrigatoriedade de informar a ANPD: ● Exceções relacionadas às microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais com fins econômicos, que serão objeto de discussão em processo de regulamentação específico; ● Quando o controlador puder demonstrar que o incidente de segurança não tem o condão de acarretar risco ou dano relevante aos titulares envolvidos (e.g., incidentes envolvendo dados cadastrais de um número reduzido de titulares; incidentes envolvendo dados pessoais que já eram públicos); ● Quando o controlador tomar medidas técnicas adequadas previamente ao incidente de segurança, de modo a torná-los ilegíveis para indivíduos não autorizados a acessá-los (e.g., criptografia);

[9] *Agencia Española de Proteccion de Datos* (AEPD). *Guide on personal data breach management and notification*. Disponível em https://www.aepd.es/sites/default/files/2019-09/Guide-on-personal-data-breach.pdf.

	• Quando o controlador puder demonstrar que adotou medidas técnicas adequadas após o incidente de segurança que atenuem total ou parcialmente o potencial impacto sobre os titulares e que não há mais a possibilidade de um risco relevante (e.g., identificar o incidente e imediatamente implementar medidas contra o indivíduo que acessou os dados pessoais, antes que qualquer ação pudesse ser por ele adotada); e • Quando a comunicação à ANPD implicar esforço técnico ou organizacional desproporcional.
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	Reitera-se as contribuições ao item anterior, de modo a sugerir que a ANPD se inspire nas regras estabelecidas pela autoridade espanhola e estabeleça as seguintes exceções à obrigatoriedade de informar os titulares: • Exceções relacionadas às microempresas, empresas de pequeno porte, *startups* e pessoas físicas que tratam dados pessoais com fins econômicos, que serão objeto de discussão em processo de regulamentação específico; • Quando o controlador puder demonstrar que o incidente de segurança não tem o condão de acarretar risco ou dano relevante aos titulares envolvidos (e.g., incidentes envolvendo dados cadastrais de um número reduzido de titulares; incidentes envolvendo dados pessoais que já eram públicos); • Quando o controlador tomar medidas técnicas adequadas previamente ao incidente de segurança, de modo a torná-los ilegíveis para indivíduos não autorizados a acessá-los (e.g., criptografia); • Quando o controlador puder demonstrar que adotou medidas técnicas adequadas após o incidente de segurança que atenuem total ou parcialmente potencial impacto sobre os titulares e que não há mais a possibilidade de um risco relevante; e • Quando a comunicação aos titulares implicar esforço técnico ou organizacional.

	Além disso, mesmo que se conclua pela obrigatoriedade da notificação dos titulares, em determinados casos tal medida poderia em algum grau comprometer os resultados de uma investigação em andamento, de forma que se recomenda à ANPD a previsão de que tal comunicação possa ser adiada também nessa hipótese.
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	Além dos critérios já mencionados nas respostas anteriores, o art. 48, § 3º, da LGPD dispõe que a análise da ANPD deverá considerar a eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços.
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	De início, destaca-se que a ANPD deverá garantir o sigilo das informações relacionadas às investigações de incidentes de segurança, conforme prevê o art. 55-J, XXIV, § 5º, da LGPD, de forma a não prejudicá-la/comprometê-la, bem como para proteger os agentes de eventuais impactos reputacionais desnecessários/desproporcionais. Ademais, em linha com o procedimento adotado pela CNIL, a ABIPAG acredita que a autoridade poderia avaliar, preliminarmente, se o incidente de segurança foi notificado corretamente, isto é, se o controlador encaminhou as informações necessárias dentro do prazo legal (ou com a devida justificativa para o atraso). No mérito, a ANPD deveria se limitar a avaliar (i) se o incidente de segurança notificado pelo controlador de fato acarreta risco ou dano relevante ao titular; (ii) caso afirmativo, se o controlador notificou corretamente os titulares envolvidos e implementou ou vem implementando medidas técnicas adequadas. Em relação ao item (i), sugere-se à autoridade a adoção de metodologia similar àquela elaborada pelo Comitê Central de Governança de Dados , conforme disponível em seu Guia de Boas Práticas para implementação da Lei Geral de Proteção de Dados na Administração Pública Federal.
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos	Entende-se que as medidas técnicas e administrativas a serem eventualmente determinadas pela ANPD variarão conforme o caso concreto, dentre as quais poderão envolver a solicitação de informações e/ou evidências adicionais, a determinação de adoção de protocolos específicos e razoáveis para mitigar ou

controladores após a comunicação do incidente de segurança?	solucionar o incidente, entre outras (a exemplo daquelas descritas no item 8 do guia elaborado pela autoridade espanhola já mencionado anteriormente). Por fim, a ANPD também poderia exercer seu papel educativo e recomendar aos controladores, em especial aqueles de médio e pequeno porte, a elaboração de / melhoria em seus procedimentos, adoção de *action plans* ou planos de resposta a incidentes de segurança, de modo a incrementar o grau de maturidade de proteção de dados pessoais no Brasil.
SUGESTÃO DE NORMATIVO, SE HOUVER	
Art. Xxxx	
Art. Xxxx	

***

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: ABRACICLO – Associação Brasileira dos Fabricantes de Motocicletas, Ciclomotores, Motonetas, Bicicletas e Similares

CPF/CNPJ: 48.752.885/0001-01

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS **IMPORTANTE:** Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	• Tipo de incidente (confidencialidade – diferente alguém que não devia acessou – disponibilidade – perdeu um hard drive com diversos dados) • Natureza, sensibilidade e volume de dados • Facilidade de identificação dos titulares (criptografia, pseudo ou anonimização) • Gravidade das consequências aos titulares • Características dos titulares (Crianças, idosos) • Aspectos da organização/setor (ex. hospital vs. montadora) • Volume de titulares afetados • Medidas tomadas para reverter ou mitigar as consequências do incidente. • Possíveis intenções de quem perpetrou o ataque (se for ataque) • Dados já expostos/publicamente acessíveis ou dados confidenciais Sugestão: recomendação de metodologias amplamente aceitas como a da *European Union Agency for Network and Information Security* - ENISA como parâmetro (recomendada pela EDBP), porém permitindo a liberdade de definição pelas organização sobre qual metodologia seguir (Recomendações para uma metodologia de avaliação da gravidade dos incidentes de segurança - *Recommendations for a Methodology of the Assessment of Severity of Personal Data Breaches*),

O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	Entendemos que os riscos ou danos podem ser definidos conforme as seguintes categorias: (i) baixo; (ii) médio; (iii) alto; e (iv) muito alto. Neste contexto, entendemos que somente os riscos/danos altos ou muito altos devem ser considerados relevantes e, portanto, passíveis de comunicação. Para definição destas categorias, é importante que seja realizada a avaliação da gravidade e da probabilidade.
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	Dano consiste no risco concretizado.
O que deve ser considerado na avaliação dos riscos do incidente?	Vide critérios listados no item "*Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?*".
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	Entendemos como suficientes as informações listadas na LGPD, sendo critério do Controlador adicionar mais informações que sejam pertinentes, conforme o caso concreto.
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	Primeiramente, é essencial definir quando começa a contar o prazo. Nossa sugestão é que seja considerado o prazo a partir de quando, razoavelmente e considerando as circunstâncias, se possa afirmar que ocorreu um incidente envolvendo dados pessoais. Se envolve um Operador, sugerimos que seja contado da data em que o Operador informar o Controlador (ou este ficar sabendo por outros meios) – sendo essencial que o Operador informe o Controlador de forma razoavelmente imediata (sendo papel do Controlador definir se entende como um risco/dano alto, passível de notificação). Em relação à definição do "prazo razoável", é essencial que sejam definidos parâmetros objetivos. Analisando, como exemplo, a legislação europeia, vemos que se tem um prazo inicial para notificar que, na prática, é reconhecidamente impossível em diversas circunstâncias, para uma investigação apropriada, razão pela qual se possibilita uma notificação faseada/parcial, conforme o andamento da investigação interna. O diálogo e troca de experiência com a Senacon pode ser especialmente interessante em relação aos prazos de notificação à ANPD e aos titulares afetados. Por exemplo, no contexto de atividades de *RECALL*, que foi alvo de diversas discussões jurídicas em relação ao seu prazo para notificação, a legislação traz o prazo "imediato", o que, na prática, se mostrou impossível (dado que, para se estabelecer a necessidade de recall, é necessário de fato aferir a real necessidade do recall,

	evitando inclusive dar causa à prejuízos aos próprios consumidores). Diante disso, o tema foi levado ao judiciário de forma recorrente ao longo dos anos, causando insegurança jurídica para as empresas e consumidores afetados. Em 2019, estabeleceu-se a Portaria de Recall, MJSP 618/2019, com dois prazos distintos, a depender da ciência do fornecedor: (i) a comunicação de investigação de recall sobre produtos ou serviços com possível nocividade ou periculosidade; e (ii) a comunicação de recall no caso de conhecimento da nocividade ou periculosidade do produto ou serviço. A Portaria também borda a situação em que o fornecedor toma conhecimento da possibilidade de nocividade e periculosidade de produtos ou serviços. Nesta circunstância, há o dever legal de comunicação à Senacon em vinte e quatro horas sobre o início das investigações. O prazo para a conclusão das investigações é de dez dias úteis, com a possibilidade de prorrogação, a depender do caso concreto. Ao final deste período, o fornecedor deve formalizar o recall ou apresentar as razões pelas quais não será necessário fazê-lo. Importante destacar que a Senacon poderá conceder prazo adicional para conclusão da investigação, desde que o fornecedor demonstre a necessidade para tal. Por fim, reiteramos a importância do prazo ser definido em dias úteis ao invés de através de horas, para garantir maior clareza às partes envolvidas, inclusive permitindo a condução fluída das investigações.
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	Conforme mencionado anteriormente, entendemos ser saudável haver uma previsão de notificação à ANPD de forma preliminar, com notificação aos Titulares somente após razoável definição dos riscos ou aferição do incidente e findo o prazo investigativo (considerando o esforço operacional, inclusive de notificação aos titulares envolvidos, bem como visando evitar um risco de pânico desnecessário). Importante notar que, caso o incidente se mostre suficientemente grave para justificar a notificação aos titulares no curso da investigação, isso deve ser realizado sem atrasos indevidos. Em relação ao conteúdo da comunicação ao titular dos dados, entendemos ser relevantes as seguintes informações: (i) descrição da natureza dos dados pessoais afetados, para que o titular dos dados tenha conhecimento dos dados pessoais expostos; (ii) riscos relacionados ao incidente de segurança, de forma que o titular dos dados esteja ciente dos riscos e danos decorrentes do incidente; e (iii) forma de contato do DPO ou outro ponto de contato com quem mais informações possam ser obtidas, devendo essas serem as únicas informações obrigatórias para a comunicação com o titular dos dados. Ainda, considerando o momento de conscientização da população, seria

	interessante recomendar que o Controlador inclua informações específicas de ações paliativas a serem tomadas para o titular se proteger (quando cabível). Entendemos que o Titular não deve receber informações técnicas e detalhadas, que serão enviadas à ANPD, sob pena de se sobrecarregar o titular com mais informações do que o necessário ao seu correto entendimento. Assim, é necessário possibilitar ao controlador certa discricionariedade na definição das informações a serem fornecidas visando garantir a transparência (sem ocasionar excesso de informações e potencial fadiga informacional).
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	A comunicação deve ser preferencialmente realizada de forma direta ao Titular, utilizando-se dos dados de contato tratados pelo controlador. Apenas nos casos de inviabilidade do Controlador contatar os titulares de forma direta e individual, a comunicação poderá ser realizada através de divulgação na mídia pelo Controlador.
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	Nas hipóteses de risco ou dano não considerado relevante. Também entendemos que a regulamentação da ANPD deve excluir da obrigatoriedade de comunicação os incidentes que tiveram seu risco ou dano remediado ou razoavelmente mitigado, que envolvam dados pessoais protegidos (criptografados, pseudoanonimizados, por exemplo) ou que envolvam dados pessoais que acessíveis publicamente sem grandes riscos aos titulares em relação ao incidente.
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	Casos em que ainda não seja possível, dentro do prazo estabelecido, aferir a extensão do dano ao titular, durante investigações em andamento ou quando identificado que não há risco relevante ou dano efetivo ao titular (pânico desnecessário), torna-se desnecessário informar os titulares e a ANPD. Importante destacar que, após a vigência do GDPR, na União Europeia, autoridades de proteção de dados reportaram o excesso de notificações de incidentes, que prejudicam a efetividade da proteção de dados e a própria atuação da autoridade. Dessa forma, é salutar que a ANPD utilize este aprendizado internacional para evitar sobrecarga inadequada de suas próprias atividades, criando formas de “filtrar” com efetividade os critérios para ser informada sobre incidentes. Como exemplo, a ICO criou um quiz de autoavaliação que ajuda as Organizações a definirem se o incidente é ou não passível de notificação (https://ico.org.uk/for-organisations/report-a-

	breach/personal-data-breach-assessment/). Fonte de consulta sobre sobrecarga da ICO em temas de incidentes: https://www.pinsentmasons.com/out-law/news/ico-warns-over-reporting-data-breaches
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	• Natureza • Sensibilidade • Volume • Cases similares pelo mundo (benchmarks de posturas de autoridades de outros países e de autoridades brasileiras de temas correlatos) e as consequências sofridas por titulares • Demonstração, boa-fé, critérios qualificadores (paralelo com parágrafo 1º, art. 52)
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	Os controladores devem ter a liberdade de definir sua metodologia para graduação da severidade do incidente de segurança, considerando seu setor de atuação, porte e critérios próprios, bem como o volume e sensibilidade de dados pessoais tratados. Não obstante, existem frameworks como o da ENISA, mencionado anteriormente, que poderão apoiar as definições.
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	• Acompanhamento/Recomendações do Plano de Resposta ao Incidente, com base na comunicação preliminar realizada; • Implementações de contramedidas e ações educativas (conforme o caso) a fim de evitar a repetição do incidente; • Proposição de ações de minimização de danos aos titulares de dados (ex. caso Equifax – envolveu benefícios aos titulares, como monitoramento de crédito).
COMENTÁRIO ADICIONAL. Sobre o formulário	• Apenas o Controlador tem o dever legal de notificar incidente à ANPD e ao titular; • Sobre o campo “Dados do Notificante”, entendemos desnecessário, sendo adequado somente informar os dados do Encarregado ou Responsável Legal.

SUGESTÃO DE NORMATIVO, SE HOUVER
ARTICLE 29 DATA PROTECTION WORKING PARTY. **Guidelines on Personal data breach notification under Regulation 2016/679**. European Data Protection Board. **Guidelines 01/2021 on Examples regarding Data Breach Notification** ENISA **Recommendations for a methodology of the assessment of severity of personal data breaches**

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: Associação Brasileira de Medicina Diagnóstica – ABRAMED

CPF/CNPJ: 10.327.378/0001-58

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS **IMPORTANTE:** Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	Entendemos que um incidente deve ser enquadrado como relevante, quando o tratamento de dados pessoais acarretar riscos às liberdades civis e aos direitos fundamentais. Acreditamos que a Autoridade Nacional (ANPD) deve disciplinar e estabelecer critérios de forma clara, objetiva, descrevendo a materialidade do dano e as formas de mitigações técnicas empregadas e esperadas para remediação de incidentes, para que os agentes de tratamento adotem padrões na análise de risco de seus processos assistenciais, de negócio, apoiando, inclusive, na elaboração do relatório de impacto à proteção de dados pessoais. Consideramos que um risco será relevante, quando: • As atividades de tratamento usem métodos não recomendáveis ou contrários às boas práticas adotadas pelo seu segmento de atuação na economia no momento do tratamento; • Os agentes de tratamento realizem processos de tratamentos de dados que sejam contrários aos princípios e diretrizes da Lei Geral de Proteção de Dados Pessoais; • O Controlador dos dados pessoais identificar um alto risco no processo de tratamento e não adotar medidas de mitigação destes riscos.

	• O incidente ocasionar significativas ou irreversíveis consequências aos titulares de dados; Como critérios à ANPD sugerimos: o tipo de dado se pessoal ou sensíveis, quais foram as medidas de remediação adotadas posteriormente ao incidente, qual o real efeito do incidente para o titular de dados, qual a probabilidade de o titular de dados sofrer algum dano por conta do incidente, qual a chance de terceiros utilizarem indevidamente os dados objetos do incidente. As previsibilidades de materialização de um risco devem ser pautas por critérios de avaliação de riscos inerentes a um determinado processo bem como critérios de avaliação da vulnerabilidade (maior ou menor nível de proteção) dos controles aplicados a este processo na organização**.**
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	Sim, acreditamos que a adoção de categorias de risco ou dano auxiliará na identificação da criticidade do incidente e, por consequência, a quais medidas mitigadoras e corretivas devem ser priorizadas pelos agentes de tratamento. Características que poderão ser adotadas para identificar o risco ou o dano: <u>Alto</u>: • Quando o incidente resultar em consequências significantes comprovadas para um titular dos dados; • Nos casos em que os agentes de tratamento realizem processos de tratamentos de dados que sejam contrários aos princípios e diretrizes da Lei Geral de Proteção de Dados Pessoais; <u>Médio</u>: • Incidente que possa ocasionar constrangimento e afetar direitos fundamentais dos titulares de dados

	Baixo: • Nos casos em que o incidente não possibilite constrangimento relevante ao titular, resultando em mero dissabor cotidiano; • Quando o incidente possibilitar o acesso a dados pessoais e informações que são possíveis de serem obtidas em portais e banco de dados públicos. Por fim, julgamos que risco e danos classificados como baixos não deverão ser notificados à ANPD, por não ser um tema de interesse social, o alto volume de demandas e solicitações e possível incidentes pontuais poderão ser solucionados
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	Consideramos que risco é o efeito da incerteza de um evento que pode ocorrer na persecução dos objetivos (International Organization for Standardization, 2009). De acordo com o RGPD, na implicação (75), o risco é descrito da seguinte forma (Council of the European Union, 2016): *"O risco para os direitos e liberdades das pessoas singulares, [...], poderá resultar de operações de tratamento de dados pessoais suscetíveis de causar danos físicos, materiais ou imateriais, …"* Assim, resta claro que, muitas vezes, podemos ter um processo de baixo risco com alta probabilidade de dano, dependendo da forma de exposição dos dados e a sua utilização. Inclusive, esse é um tema extremamente relevante para o setor da saúde que lida no dia a dia com alto volume de processos de tratamento de dados sensíveis. Portanto, muitas vezes estaremos lidando com dados que possam resultar em alto dano ao titular mesmo que o risco seja baixo ou mitigado pelos agentes de tratamento. Desta maneira, fundamental que se analise as particularidades inerentes aos serviços de saúde, e que se defina os conceitos de dano e risco com clara e nítida separação. Assim, somente os incidentes que possuírem cumulativamente a probabilidade de risco alto e dano alto deverão ser notificados à ANPD e aos titulares de dados.

O que deve ser considerado na avaliação dos riscos do incidente?	• A probabilidade do risco, devendo ser observado as práticas e as características de setores específicos, de acordo com o Artigo 55-J, XXIII, da LGPD; • O nível de vulnerabilidades dos controles identificadas no processo de tratamento de dados; • Se foram realizas medidas efetivas para mitigar os riscos identificados;
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	Entendemos que as informações listadas pelo artigo em análise são suficientes para demonstrar o processo e quais são os riscos e os danos do incidente em questão. A comunicação é apenas um primeiro contato, tendo em vista que ANPD solicitará informações complementares ou, inclusive, determinar as medidas previstas no parágrafo segundo do artigo 48. O prazo de 2 (dois) dias pode não ser factível para que uma Organização tenha uma visão macro do incidente deixando de fornecer informações relevantes a análise.
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	Tendo em vista que, a notificação visa identificar a necessidade de adotar medidas mitigadoras e possibilitar transparência do incidente, sugerimos no mínimo 5 (cinco) dias úteis contados da data de conhecimento dos fatos.
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	Entendemos que o titular deve ser comunicado posteriormente à ANPD a depender do incidente para que a comunicação seja efetiva e não gere "pânico" ao titular, não entendemos que seria eficaz a comunicação de todo o detalhamento relacionado no §1º do art. 48 por conter um caráter estritamente técnico e poderia, assim, inviabilizar o entendimento do titular sobre o incidente. Sugerimos que seja considerado situações em que somente a ANPD deve ser comunicada ou somente o titular. Sendo assim, sugerimos que conste na comunicação os itens I, II e VI do § 1º do art. 48, pois em nosso entendimento já são suficientes para esclarecer o incidente para os titulares. Ademais, sugerimos que a comunicação seja realizada após o levantamento de dados que componham uma informação objetiva e íntegra com as ações de adequação já definidas para que o titular entenda a dimensão do problema e o que foi executado pela empresa

Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	Via de regra, entendemos que a comunicação deverá ser realizada de forma individual e direta, por canais que possibilitem registrar o recebimento da mensagem que o Controlador endereçará ao titular, como o envio de e-mail, ligação telefônica com gravação da conversa, dentre outros. Porém, na hipótese de o incidente ocasionar risco ou dano para um elevado número de titulares, acreditamos que deverá ser admitida a notificação através de canais públicos, como a página do Controlador na internet, o envio de nota oficial à imprensa e demais canais de comunicação que os seus titulares sejam impactados.
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	Entendemos que aos incidentes qualificados como risco baixo e baixa probabilidade de dano ao titular do dado não devem ser notificados à ANPD, nos termos do §7° do Artigo 52.
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	Incidentes qualificados com risco baixo e baixa probabilidade de dano ao titular do dado
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	Consideramos que os critérios devem estar atrelados aos níveis de riscos e danos identificados e classificados como: alto, médio ou baixo. Assim, a gravidade sempre estará atrelada a critérios claros e objetivos, possibilitando maior previsibilidade e transparência aos agentes de tratamento. Avaliar natureza, sensibilidade, dano à privacidade conforme direitos fundamentais previstos na LGPD, volume de titulares afetados e dimensão (territorial).
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	Metodologias adotadas pelas organizações, que estejam embasadas em melhores práticas de mercado como por exemplo: ISO 31000 — Risk management; https://www.nist.gov/; European Union Agency for Network and Information Security (ENISA): Recommendations for a methodology of the assessment of severity of personal data breaches, Para questões de volumetria, o da Commission Nationale de L'Informatique et des Libertés (CNIL): Methodology for Privacy Risk Management.
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem	Sugerimos que a ANPD sugira ações educativas aos controladores com prazo factível para implementação. Autoridade deve avaliar extensão do incidente, pessoas envolvidas e dados

determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	envolvidos para verificar forma de definir gravidade e definir valor da multa, observada a proporcionalidade e análise de risco e dano efetivamente materializado.
SUGESTÃO DE NORMATIVO, SE HOUVER	
Art. Xxxx	
Art. Xxxx	

CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: ASSOCIAÇÃO BRASILEIRA DE MEDICINA DE GRUPO - ABRAMGE
CPF/CNPJ: 61.642.401/0001-30

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS **IMPORTANTE:** Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	O objetivo do processo de avaliação é identificar incidentes que representem um risco relevante para o titular dos dados e, portanto, exigirão notificação ao titular e à ANPD. A definição recomendada de um incidente classificado como de risco relevante é "o acesso não autorizado a dados pessoais que materialmente compromete a segurança, confidencialidade ou integridade dos dados pessoais **e** que o Controlador de Dados acredita razoavelmente que causará perda ou dano ao indivíduo". Danos ao indivíduo devem incluir danos financeiros (por exemplo, roubo de identidade) ou danos à reputação. Uma avaliação de quatro fatores deve ser usada para avaliar a gravidade do risco representado por um incidente e se este poderá ser classificado como de risco relevante, conforme a seguir: 1. A natureza e extensão dos dados pessoais envolvidos; 2. A pessoa ou organização que recebeu ou obteve acesso aos dados de forma não autorizada; 3. A probabilidade do dano ao titular dos dados, incluindo se as informações pessoais foram adquiridas ou visualizadas; e 4. Até que ponto os fatores atenuantes ou controles (como criptografia) que podem diminuir o risco estavam em vigor. A avaliação de quatro fatores acima é aplicada para avaliar o risco de incidentes envolvendo informações de saúde no mercado de saúde nos Estados Unidos e está introjetada desde 2013. Referências: Privacy Act 1988 da Austrália. Disponível em: **https://bit.ly/3cNqgZN** Breach Notification Rule do HIPAA Diretrizes sobre Notificação de Violação de Dados Pessoais – Regulamento 2016/679 (Working Party 29)

O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	O método recomendado para conduzir uma avaliação de risco de quatro fatores, conforme a seguir: 1. A natureza e extensão dos dados pessoais envolvidos; 2. A pessoa ou organização que recebeu ou obteve acesso aos dados de forma não autorizada; 3. A probabilidade do dano ao titular dos dados, incluindo se as informações pessoais foram adquiridas ou visualizadas; e 4. Até que ponto os fatores atenuantes ou controles (como criptografia) que podem diminuir o risco estavam em vigor. Cada fator deverá ser avaliado como risco alto, médio ou baixo e, em seguida, deve-se estabelecer um perfil de risco geral para o incidente e concluir se ele se qualifica como um risco relevante. Os requisitos de comunicação ao titular dos dados e à ANPD devem se concentrar em incidentes que representam um risco relevante, definidos como "o acesso não autorizado a dados pessoais que comprometa materialmente a segurança, confidencialidade ou integridade dos dados pessoais **e** que o Controlador de Dados razoavelmente acredita que causarão perda ou dano ao indivíduo". Danos ao indivíduo devem incluir danos financeiros (por exemplo, roubo de identidade) ou danos à reputação. Referência: *Breach Notification Rule* do HIPAA Diretrizes sobre Notificação de Violação de Dados Pessoais nos termos do Regulamento 2016/679 (*Working Party 29*)
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	A definição recomendada de um incidente de risco relevante é "o acesso não autorizado a dados pessoais que materialmente compromete a segurança, confidencialidade ou integridade dos dados pessoais **e** que o Controlador de Dados acredita razoavelmente que causará perda ou dano ao indivíduo". Danos ao indivíduo devem incluir danos financeiros (por exemplo, roubo de identidade) ou danos à reputação.
O que deve ser considerado na avaliação dos riscos do incidente?	O objetivo do processo de avaliação é identificar incidentes que representem um risco relevante para o titular dos dados e, portanto, exigirão notificação ao titular e à ANPD. A definição recomendada de um incidente classificado como de risco relevante é "o acesso não autorizado a dados pessoais que materialmente compromete a segurança, confidencialidade ou integridade dos dados pessoais **e** que o Controlador de Dados acredita razoavelmente que causará perda ou dano ao indivíduo". Danos ao indivíduo devem incluir danos financeiros (por exemplo, roubo de identidade) ou danos à reputação. Uma avaliação de quatro fatores deve ser usada para avaliar a gravidade do risco representado por um incidente e se este poderá ser classificado como de risco relevante, conforme a seguir : 1. A natureza e extensão dos dados pessoais envolvidos; 2. A pessoa ou organização que recebeu ou obteve acesso aos dados de forma não autorizada;

	3. A probabilidade do dano ao titular dos dados, incluindo se as informações pessoais foram adquiridas ou visualizadas; e 4. Até que ponto os fatores atenuantes ou controles (como criptografia) que podem diminuir o risco estavam em vigor. Conforme descrito acima, a interação entre esses quatro fatores deve ser avaliada no contexto de cada incidente. Certamente, a natureza dos dados pessoais - dados financeiros ou de saúde, por exemplo - terá maior probabilidade de resultar em danos ao indivíduo. No entanto, os fatos específicos associados aos outros fatores da avaliação de quatro fatores podem reduzir significativamente o risco de um incidente. Referência: *Breach Notification Rule* do HIPAA Diretrizes sobre Notificação de Violação de Dados Pessoais nos termos do Regulamento 2016/679 (*Working Party 29*
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	As informações solicitadas no §1º, do artigo 48, da LGPD são suficientes. A ANPD deve reconhecer que informações detalhadas sobre um incidente, incluindo o número de titulares de dados afetados, podem levar tempo. Portanto, o fornecimento de um detalhamento completo pode não ser possível no relatório inicial enquanto a investigação não for concluída.
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	A comunicação à ANPD deve ser realizada “sem demora injustificada” e somente quando o Controlador de Dados tiver confirmado que o incidente se classifica como de risco relevante. O risco relevante deve ser definido como "o acesso não autorizado a dados pessoais que materialmente compromete a segurança, confidencialidade ou integridade dos dados pessoais **e** que o Controlador de Dados acredita razoavelmente que causará perda ou dano ao indivíduo". Se um prazo específico for necessário, deve ser de pelo menos 30 dias a partir da data de identificação e confirmação do risco relevante. A ANPD deve permitir prorrogações mediante apresentação de justificativa plausível. Idealmente, a comunicação à ANPD poderia ser feita ao mesmo tempo que a comunicação ao titular dos dados para apoiar relatórios consistentes e a capacidade de conduzir uma investigação completa para que um Controlador de Dados possa ter certeza dos detalhes relevantes. Referência: Diretrizes sobre Notificação de Violação de Dados Pessoais nos termos do Regulamento 2016/679 (*Working Party 29*): Notification to the competent supervisory authority is required unless a breach is unlikely to result in a risk to the rights and freedoms of individuals.
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem	A comunicação ao titular dos dados deve ocorrer sem atrasos injustificados ou o mais rápido possível após a confirmação de que o incidente de segurança é classificado como de **risco relevante**, conforme disposto na Consideranda 86, do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016. Assim, a fim de ter um termo objetivo, um prazo razoável seria dentro de 30 dias da confirmação do

constar dessa comunicação? As mesmas do §1º do art. 48?	incidente, considerando o tempo dispendido para a realização da apuração e investigação do incidente. O risco relevante é definido como “o acesso não autorizado a dados pessoais que materialmente compromete a segurança, confidencialidade ou integridade dos dados pessoais **e** que o Controlador de Dados acredita razoavelmente que causará perda ou dano ao indivíduo”. O Regulador deve prever exceções a este prazo com base nas necessidades de aplicação da lei.
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	A melhor forma de comunicar um incidente a um titular dos dados deve ficar a critério da escolha do controlador, conforme o meio que considerar mais eficaz diante da situação concreta. Conforme previsto no *Breach Notification Rule* do HIPAA e em alguns estados americanos, como Colorado, Delaware, Illinois e Washington. frisamos a importância dessa liberdade de escolha para utilizar o meio mais adequado, considerando que as seguradoras podem estar com os dados para contato defasados devido ao término do vínculo com o Titular e o decurso do tempo, bem como quando a volumetria de comunicações individuais a ser realizado envolver grande número de Titulares. Para tanto, a comunicação pode ser estabelecida diretamente e de forma individualizada com o titular de dados afetado, por meio de avisos nos canais de comunicação oficiais da organização ou de anúncio publicitário, de forma coletiva. Nessa linha, sugerimos alguns critério objetivos: (i) Para incidentes de risco relevantes envolvendo mais de 100.000 (cem mil) indivíduos ou quando os custos de notificação possam ultrapassar R$ 1.000.000 (um milhão de reais), o Controlador de Dados deve ter a opção de escolher um mecanismo de "aviso alternativo" (por exemplo, um aviso no site do Controlador de Dados ou por meio da mídia); (ii) Quando um incidente exigir a notificação ao titular dos dados e envolver 500 ou mais titulares dos dados que não possam ser razoavelmente identificados, o aviso alternativo deve ser considerado como apropriado. Referência: Colorado: Colo. Rev. Stat. § 6-1-716. Delaware: Del. Code tit. 6, § 12B-101 et seq. Illinois: 815 Ill. Comp. Stat. 530/5, 530/10, 530/12, 530/15, 530/20, 530/25. Washington: 1071-S.PL.
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	A ANPD deve exigir notificação apenas para incidentes que representem risco relevante. Incidente de risco relevante é “o acesso não autorizado a dados pessoais que materialmente compromete a segurança, confidencialidade ou integridade dos dados pessoais **e** que o Controlador de Dados acredita razoavelmente que causará perda ou dano ao indivíduo”. Danos ao indivíduo devem incluir danos financeiros (por exemplo, roubo de identidade) ou danos à reputação. A ANPD deve exigir que as organizações mantenham registros de seus incidentes, avaliações de riscos e comunicações aos indivíduos. No entanto, incidentes de baixo risco são comuns e relatá-los à ANPD desviaria a atenção dos incidentes de alto risco que terão maior impacto sobre os titulares de dados brasileiros. Além disso, de acordo com a Autoridade de Proteção de Dados Irlandesa (DPC IE), independentemente da classificação do risco, não deveria ser obrigatória a comunicação de incidente de segurança à ANPD nos

	seguintes casos: a) quando da implementação de medidas de proteção técnicas e organizacionais adequadas para os dados pessoais afetados pelo incidente, em particular medidas que tornam os dados pessoais ininteligíveis para qualquer pessoa que não esteja autorizada a acessá-los, como criptografia; b) quando o controlador tomar medidas subsequentes que garantam a eficaz mitigação do risco para os direitos e liberdades dos titulares dos dados. Desse modo, incidentes que não forem comunicados à ANPD serão devidamente documentados pelas instituições, incluindo relatório de impacto à proteção de dados pessoais, a fim de que seja comprovado o cumprimento dos preceitos da LGPD. Tal prática está de acordo com os padrões globais de privacidade, incluindo a GDPR (artigo 33).
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	Os titulares dos dados só devem ser notificados quando a avaliação de risco de quatro fatores indicar um risco relevante. De acordo com a Autoridade de Proteção de Dados Irlandesa (DPC IE), independentemente da classificação do risco, os cenários a seguir também devem ser considerados como casos de exceção ao dever de comunicação ao titular dos dados por não representar risco relevante para o titular dos dados: a) quando da implementação de medidas de proteção técnicas e organizacionais adequadas para os dados pessoais afetados pelo incidente, em particular medidas que tornam os dados pessoais ininteligíveis para qualquer pessoa que não esteja autorizada a acessá-los, como criptografia; b) quando o controlador tomar medidas subsequentes que garantam a eficaz mitigação do risco para os direitos e liberdades dos titulares dos dados; c) quando a comunicação individual envolver um esforço desproporcional, ou seja, quando o tempo e o custo para a comunicação forem desproporcionais em relação ao volume de dados pessoais tratados pela instituição. Incidentes envolvendo dados pessoais na esfera pública (por exemplo, números de telefone ou endereços comerciais); d) Incidentes envolvendo a divulgação a um destinatário não intencional, mas confiável (por exemplo, envio de uma receita médica para a farmácia incorreta); e f) Os incidentes que não forem comunicados aos Titulares serão devidamente documentados pelas instituições, incluindo relatório de impacto à proteção de dados pessoais, a fim de que seja comprovado o cumprimento dos preceitos da LGPD. Tal prática está de acordo com os padrões globais de privacidade, incluindo a GDPR (artigo 33).

Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	Uma avaliação de quatro fatores deve ser usada para avaliar a gravidade do risco representado por um incidente e se este poderá ser classificado como de risco relevante, conforme previsto no *Breach Notification Rule* do HIPAA e também contemplados, de forma similar, nas Diretrizes sobre Notificação de Violação de Dados Pessoais nos termos do Regulamento 2016/679 (*Working Party 29*). A ver: 1. A natureza e extensão dos dados pessoais envolvidos; 2. A pessoa ou organização que recebeu ou obteve acesso aos dados de forma não autorizada; 3. A probabilidade do dano ao titular dos dados, incluindo se as informações pessoais foram adquiridas ou visualizadas; e 4. Até que ponto os fatores atenuantes ou controles (como criptografia) que podem diminuir o risco estavam em vigor. A definição recomendada para classificar o incidente como de risco relevante é "o acesso não autorizado a dados pessoais que materialmente compromete a segurança, confidencialidade ou integridade dos dados pessoais **e** que o Controlador de Dados acredita razoavelmente que causará perda ou dano ao indivíduo". Danos ao indivíduo devem incluir danos financeiros (por exemplo, roubo de identidade) ou danos à reputação.
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	Uma avaliação de quatro fatores deve ser usada para avaliar a gravidade do risco representado por um incidente e se este poderá ser classificado como de risco relevante, conforme previsto no *Breach Notification Rule* do HIPAA e também contemplados, de forma similar, nas Diretrizes sobre Notificação de Violação de Dados Pessoais nos termos do Regulamento 2016/679 (*Working Party 29*). A ver: 1. A natureza e extensão dos dados pessoais envolvidos; 2. A pessoa ou organização que recebeu ou obteve acesso aos dados de forma não autorizada; 3. A probabilidade do dano ao titular dos dados, incluindo se as informações pessoais foram adquiridas ou visualizadas; e 4. Até que ponto os fatores atenuantes ou controles (como criptografia) que podem diminuir o risco estavam em vigor. A definição recomendada para classificar o incidente como de risco relevante é "o acesso não autorizado a dados pessoais que materialmente compromete a segurança, confidencialidade ou integridade dos dados pessoais **e** que o Controlador de Dados acredita razoavelmente que causará perda ou dano ao indivíduo". Danos ao indivíduo devem incluir danos financeiros (por exemplo, roubo de identidade) ou danos à reputação.
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	A ANPD deve esperar que os Controladores de Dados já tenham tomado ou estejam em processo de tomar as medidas adequadas para mitigar o risco de um incidente no momento da comunicação. As possíveis investigações de acompanhamento podem incluir se o Controlador de Dados identificou a causa raiz e tomou medidas para prevenir futuros incidentes dessa natureza. Os controles sugeridos podem variar e compreender uma ampla gama de controles de segurança em potencial, dependendo da causa raiz, desde a garantia de patches de software apropriados até o treinamento e conscientização dos funcionários para controles de acesso aprimorados.

	Não obstante, ressaltamos que a importância de prever o direito do Controlador de Dados de realizar auditorias no Operador de Dados, desde que respeitados os seus respectivos segredos comerciais e industriais. Apesar de não estar expressamente previsto na LGPD, tal direito pode ser inferido do artigo 42, que estabelece a responsabilidade aos agentes de tratamento, bem como do artigo 46, que estabelece o dever de implantar medidas de segurança aos agentes de tratamento. Assim, considerando a responsabilidade maior atribuído ao Controlador de Dados, deveria haver a previsão de auditar o Operados de Dados nas orientações elaboradas pela ANPD.
Sugestões de ajustes ao "Formulário de comunicação de incidente de segurança com dados pessoais à Autoridade Nacional de Proteção de Dados (ANPD)"	Sugestões em relação ao "Formulário de comunicação de incidente de segurança com dados pessoais à Autoridade Nacional de Proteção de Dados (ANPD)" - Campo "Para comunicação parcial": Sugerimos que com o preenchimento do Formulário seja gerado um número de protocolo para o acompanhamento e atualização da comunicação, conforme o *Security Incident Notification Form da United Kingdom Information Commissioner Office* (ICO). - Campo "Agente de tratamento": O artigo 48 da LGPD, seguindo os padrões globais de privacidade, sobretudo o Artigo 33 do GDPR, dispõe que o controlador deve comunicar a ANPD e o Titular sobre a ocorrência de incidente de segurança. Ocorre que a utilização da expressão "agente de tratamento" dá abertura para a possibilidade de o operador notificar à ANPD, o que não é recomendável. - Campo "Dados do agente de tratamento": sugerimos criar o campo "desconhecido", caso não tenha as informações. - Campo "Dados do notificante": Solicitamos esclarecimentos a respeito deste campo, tendo em vista que até o momento existe a obrigatoriedade de nomeação de um Encarregado de Dados para todas as instituições e que o preenchimento deste tipo de comunicação deveria ser feito por ele. - Campo "Descreva de forma resumida como o incidente de segurança com dados pessoais ocorreu": Sugerimos a adição das seguintes opções padrão para a descrição da natureza do incidente: (i) Dispositivo perdido ou roubado (criptografado); (ii) Dispositivo perdido ou roubado (não criptografado); (iii) Papel perdido ou roubado; (iv) Divulgação (não autorizada); (v) Descarte inadequado de papel; (vi) *Phishing*; (vii) *Malware*; (viii) Publicação online não intencional; (ix) Segurança de rede comprometida; (x) Violação de segurança do site; (xi) *E-waste* - dados pessoais presentes em dispositivo obsoleto; (xii) Outros. - Campo "Quando o incidente ocorreu": Recomendamos adicionar uma nova pergunta para que seja possível compreender se o incidente ainda está "ativo": O incidente está em andamento? ( ) sim ( ) não. Além disso, é necessário distinguir a diferença entre "não tenho conhecimento" e "não tenho certeza".

	- Campo “Descreva como a organização teve ciência do incidente de segurança”: Recomendamos fornecer as seguintes opções para o controlador de dados: (i) Notificação por um titular dos dados; (ii) Notificação por um terceiro; (iii) Auditoria / teste de sistema; (iv) Notificação por um processador de dados; (v) Funcionário (auditoria / teste fora do sistema); (vi) Outro (descreva). - Campo “Qual a natureza dos dados afetados?”: Recomendamos que o formulário seja atualizado para a conter a divisão entre “dados pessoais” e “dados sensíveis”, assim, seguir com os tipos de dados, incluindo: (i) Dados pessoais cadastrais (nome, telefone, e-mail e endereço); (ii) Desconhecidos até o momento. - Campo “Qual a quantidade de titulares afetados?”: Recomendamos fornecer opções adicionais para controladores de dados: (i) Número real conhecido (em seguida, forneça o número real); (ii) Número aproximado conhecido (forneça o número aproximado); (iii) Número desconhecido. - Campo “Qual a categoria dos titulares afetados?”: Solicitamos que esclareçam a diferença entre clientes e consumidores. Caso não haja diferença prática, sugerimos a exclusão de uma das categorias. Além disso, o termo gera confusão, pois “pacientes” são “clientes”. Também é necessário esclarecer a definição de “usuários”. - Campo “O agente de tratamento realizou relatório de impacto à proteção de dados pessoais?”: Recomendamos excluir esta questão devido à sua importância em relação à outra documentação. - Campo “Os titulares foram comunicados sobre o incidente de segurança com dados pessoais?”: Recomendamos excluir a opção “não sei” e adicionar as seguintes opções para que a comunicação seja realizada de modo mais assertivo: (i) Estamos no processo de comunicar os Titulares; (ii) Sim, eles já foram comunicados; (iii) Não, mas estamos planejando comunicá-los; (iv) Ainda não decidimos se faremos a comunicação ou não.
SUGESTÃO DE NORMATIVO, SE HOUVER	
Não se aplica.	

São Paulo, 23 de março de 2021.

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: ABRANET – ASSOCIAÇÃO BRASILEIRA DE INTERNET

CPF/CNPJ: 01.699.656/0001-07

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS

IMPORTANTE: Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.

TÓPICO/QUESTÃO	CONTRIBUIÇÃO/INSTITUIÇÃO
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	De forma geral, desconsiderando-se a classificação do risco/dano, sugere-se que um incidente pode acarretar risco ou dano ao titular quando o tratamento de dados subjacente não fornecer a segurança que o titular dele poderia esperar, considerando-se as seguintes circunstâncias: (1) o modo pelo qual é realizado; (2) o resultado e os riscos que razoavelmente dele se esperam; (3) as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado. Esta sugestão segue exatamente conforme o disposto no art. 44 da LGPD. Nesse sentido, a ANPD estabeleceu em seu site alguns critérios que elencam para levar em consideração se o incidente pode causar risco ou dano relevante: "*a probabilidade de risco ou dano relevante para os titulares será maior sempre que o incidente envolver dados sensíveis ou de indivíduos em situação de vulnerabilidade, incluindo crianças e adolescentes, ou tiver o potencial de ocasionar danos materiais ou morais, tais como discriminação, violação do direito à imagem e à reputação, fraudes financeiras e roubo de identidade. Da mesma forma, deve-se considerar o volume de dados envolvido, o quantitativo de indivíduos afetados, a boa-fé e as intenções dos terceiros que tiveram acesso aos dados após o incidente e a facilidade de identificação dos titulares por terceiros não autorizados.*" < https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca > Sugerimos acrescentar a esses itens: (i) considerando que os cuidados com as credenciais de acesso são de responsabilidade do titular, casos de *phishing*, compartilhamento de senhas ou semelhantes, o risco ou dano

	não deve ser considerado como relevante, tendo em vista não ser culpa do Controlador; o mesmo se aplica no caso de o titular reaproveitar credenciais e ocorrer vazamento dessas credenciais. Se o vazamento não foi responsabilidade do Controlador, mas as credenciais forem utilizadas nos serviços/produtos do Controlador, o risco ou dano não pode ser considerado como relevante, tendo em vista a culpa do vazamento não ter sido do Controlador, mas do titular, por ter reaproveitado as credenciais em mais de um serviço/produto; (ii) para o contexto de avaliação de risco, para evitar falta de padronização de atributos em uso, é recomendado utilizar como base algum modelo e padrão de-facto, preferencialmente globalmente aceito (como a ISO27005, ISO31000, COSO eRM ou similares). Importante observar queo mesmo vale para incidentes (utilizar fases, classificações e modelos internacionalmente aceitos, neste caso, preferencialmente os consumidos pelos CERTs (BR), CSIRTs ou mesmo o FIRST). Além dos pontos acima, a ANPD deve considerar, cumulativamente: o volume de dados envolvido; o quantitativo de indivíduos afetados; a boa-fé e as intenções dos terceiros que tiveram acesso aos dados após o incidente; a facilidade de identificação dos titulares por terceiros não autorizados.
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	É importante haver uma métrica para aferir os riscos considerando a probabilidade de acontecer a violação X o impacto se acontecer a violação, nesse sentido segue sugestão de classificação. • Baixo (não relevante. Sem necessidade de comunicar a ANPD ou titulares): cumpra os seguintes requisitos: (i) envolvam dados que, isoladamente, não permitam a identificação dos titulares, tais como IP (sozinho, que não sejam IPs públicos e sem outras informações), gênero, localização geográfica geral, data de nascimento e dados mascarados ou parcialmente mascarados que não permitam a identificação do titular; (ii) dados de identificação que estejam mascarados e/ou criptografados; e (iii) envolvam dados correspondentes a 30% ou menos da base de dados do Controlador • Médio (não relevante. Sem necessidade de comunicar a ANPD ou titulares): cumpra os seguintes requisitos:

	(i) envolvam dados que, isoladamente, não permitam a identificação dos titulares, tais como IP (sozinho, que não sejam IPs públicos e sem outras informações), gênero, localização geográfica geral, data de nascimento e dados mascarados ou parcialmente mascarados que não permitam a identificação do titular; e (ii) envolvam dados correspondentes a 30% a 50% da base de dados do Controlador • Alto (relevante): cumpra os seguintes requisitos: (i) envolvam dados que permitam a identificação dos titulares, tais como Nome, CPF, RG, endereço postal, independentemente da porcentagem de dados afetados do Controlador; **e/ou** (ii) envolvam dados pessoais sensíveis, conforme definido na LGPD, independentemente da porcentagem de dados afetados do Controlador, desde que tais dados não estejam mascarados e sejam passíveis de associação a seus titulares; **e/ou** (iii) envolvam dados correspondentes a acima de 50% da base de dados do Controlador.
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	Para que seja considerado "dano ao titular" é necessário que dano material ou moral tenha de fato ocorrido ao titular dos dados. Enquanto nenhum dano de fato ocorrer, seria classificado como "risco". Exemplos: (i) havendo vazamento de nome, CPF e RG do titular, entrará na categoria de "risco" até que o titular seja afetado, como, por exemplo, tentativa ou realização de fraude financeira e/ou roubo de identidade. (ii) se fotos eróticas/sensuais vazarem por invasão a sistema de nuvem e se tornarem públicas na internet, se caracterizaria o dano moral automaticamente.
O que deve ser considerado na avaliação dos riscos do incidente?	Na avaliação dos riscos do incidente é importante que seja considerado, além dos pontos listados na resposta à primeira pergunta: (i) se houve adulteração do dado do titular; (ii) quem é o autor do fato que gerou o incidente; (iii) possibilidade de verificação de origem e remediação e se possível, reversibilidade, do incidente; e (iv) a concretização ou não do dano.
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	Entende-se que as informações já listadas no artigo 48 §1º da Lei 13.709/2018 já seriam suficientes.
Qual o prazo razoável para que controladores informem a ANPD sobre	Sugere-se a adoção do prazo de 5 (cinco) dias úteis.

o incidente de segurança? (art. 48, §1º)	
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	Sugere-se a adoção do prazo de 5 (cinco) dias úteis, porém contados da comunicação à ANPD.
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	Se envolver dados que permitam a identificação dos titulares, a comunicação deve ser direta e individual, salvo no caso de incidentes com milhões de usuários, no qual não é possível comunicar a todos diretamente, nesse caso se aplicaria a comunicação pública
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	Sugere-se que incidentes de classificação de risco/dano “baixa” e médio, nossa sugestão de classificação acima prescindam de comunicação à ANPD.
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	Sugere-se que incidentes de classificação de risco/dano “baixa” e médio, nossa sugestão de classificação acima prescindam de comunicação aos titulares, ademais se os dados alvo do incidente não permitirem a identificação dos titulares, não seria necessário comunicá-los.
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	Vide sugestão de classificação acima.
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	Recomenda-se a adoção da metodologia prevista no documentoISO27001, e os demais modelos apresentados ao longo deste documento (CERTs, CSIRTs, FIRST e IRM – Incident Response Methodology) ajudam mensurar o problema de acordo com as fases listadas. Adicionalmente, FAIR ajuda aproximar o contexto de Incidentes com o de Riscos, OCTAVE pode ser utilizado para uma abordagem mais ágil.

Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	Recomenda-se a adoção da metodologia prevista no documento ISO27001.
SUGESTÃO DE NORMATIVO, SE HOUVER	
Art. Xxxx	
Art. Xxxx	

Associação Brasileira dos Terminais Portuários

Filiada à:
CNT
Confederação Nacional do Transporte

CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: ASSOCIAÇÃO BRASILEIRA DOS TERMINAIS BRASILEIROS - ABTP

CPF/CNPJ: 32.323.149/0001-06

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regularmente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS

IMPORTANTE: Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.

TÓPICO/QUESTÃO	CONTRIBUIÇÃO/INSTITUIÇÃO
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	**A ANPD deve considerar risco ou dano de risco ao titular quando o incidente, efetivamente, expuser ou comprometer a privacidade, a honra e/ou a integridade do titular, ou, ainda, a integridade e/ou disponibilidade dos seus dados pessoais, especialmente os sensíveis, com risco de ocasionar fraude e/ou dano material frente aos princípios da LGPD e à política de proteção de informação da organização, com possibilidade de monetização por terceiros.**
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	**Níveis (categorias) sugeridos:** **1) Crítico: vazamento nacional e/ou internacional de dados pessoais sensíveis com possibilidade comprovada de monetização por terceiros;** **2) Alto: vazamento nacional e/ou internacional de dados pessoais comuns com possibilidade comprovada de monetização por terceiros;** **3) Médio: vazamento nacional e/ou internacional de dados pessoais comuns sem possibilidade de monetização por terceiros;** **4) Baixo: vazamento nacional de dados pessoais comuns sem possibilidade de monetização por terceiros.** **- Riscos Nível 1 e 2 não são aceitáveis, devendo ser endereçados de forma proativa, na medida e proporção possíveis por parte da organização, considerando a razoabilidade dos custos e investimentos frente ao retorno na mitigação do risco. Deve-se, neste caso, haver plano de controle preventivo e medidas corretivas positivadas;** **- Riscos Nível 3 são "toleráveis", desde que a organização tenha mapeado medidas de mitigação, incluindo controle preventivo e rotina de monitoramento periódico dos processos onde estes riscos se apresentam;**

	- Riscos de Nível 4 são "não relevantes", desde que a organização tenha mapeado medidas de mitigação e correção, podendo incluir rotina de monitoramento periódico dos processos onde estes riscos se apresentam, por exemplo.
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	**Risco: Situação hipotética que pode acarretar danos ao titular.** **Dano: Efeitos decorrentes da materialização do risco.** **Nesse sentido, cita-se o exemplo abaixo:** **Risco: Armazenamento dos dados em plataforma externa, gerenciada por terceiros, que não atenda aos requisitos e princípios previstos na LGPD, podendo resultar em: i) acesso não autorizado; ii) divulgação não autorizada; iii) destruição de dados; iv) perda dos dados; vi) alteração indevida dos dados; e viii) tratamento ilícito ou inadequado.** **Dano: exposição, vazamento, perda, roubo, modificação indevida, indisponibilidade dos dados.**
O que deve ser considerado na avaliação dos riscos do incidente?	**Conforme definido nos manuais de boas práticas de avaliação de riscos, definidos através das normas ABNT NBR ISO31000 e ABNT NBR ISO/IEC 31010, devem ser levados em consideração:** **1) Probabilidade de ocorrência do risco de incidente, considerando-se os fatores de vulnerabilidades existentes nos processos, a eficácia dos controles existentes no processo, bem como o histórico de incidentes dentro do contexto interno e externo avaliado;** **2) Consequências da concretização do risco de incidente, considerando os impactos de imagem, legais, financeiros e operacionais para o Controlador/Operador e para o titular dos dados.**
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	**O plano de governança pré-estabelecido como medida de proteção dos dados dos titulares com a descrição do incidente, incluindo a indicação do processo de tratamento e sua base legal, bem como sua extensão do – *i.e.*, seus impactos e implicações.**
Qual o prazo razoável para que controladores informem a ANPD sobre	**Prazo de 72 horas, conforme previsto na GDPR.**

o incidente de segurança? (art. 48, §1º)	
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	**O prazo deve ser de até 72h, em paralelo ao comunicado oficial à ANPD.** **Assim, deve ser encaminhada comunicação por e-mail ao titular, contendo o tipo de dado vazado e como ocorreu o incidente, esclarecendo os métodos de tratamento pré-estabelecido para a privacidade dos dados, assim como as medidas de mitigação dos possíveis danos previstos e, por fim, a confirmação da comunicação à ANPD para os procedimentos de colaboração com a investigação pelo órgão.**
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	**Como forma de evitar danos e prejuízos ainda maiores, sugerimos que a comunicação seja direta e individual (por e-mail, via postal ou outro), endereçada pelo Encarregado. Ainda, a possibilidade de publicação de Nota Pública somente deverá ser utilizada em caso de vazamento em massa e diante da impossibilidade de identificar os titulares.**
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	**Em casos de risco ou dano de Nível 3 ou 4, de acordo com as categorias propostas pela Associação nas sugestões acima, oportunidade na qual cabe informar apenas ao(s) titular(es), no prazo de 72 horas, observados os requisitos do Art. 48, parágrafo primeiro e em conformidade ao princípio da transparência.** **Ainda, deve ser considerada exceção se o incidente ocorreu diretamente por culpa exclusiva do titular dos dados sem envolvimento ou prejuízo a terceiros.**
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	**Em caso de incidente ocorrido diretamente por culpa exclusiva do titular dos dados sem envolvimento ou prejuízo a terceiros.** **Ainda, deve-se considerar o tratamento indevido ocorrido internamente na empresa sem que tenha ocorrido vazamento da informação para fora da incorporação.**
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	• **Nível (categoria) do risco ou dano, conforme sugestão acima, considerando a natureza dos dados envolvidos no incidente e seus respectivos – e eventuais – impactos e implicações;**

	● Extensão da exposição da privacidade, honra e/ou integridade do titular; **● Histórico da organização no que se refere a incidentes de segurança (reincidência);** **● Histórico de incidentes de mesma natureza, fora da organização;** **● Nível de Governança da organização frente a proteção de dados pessoais;** **● Nível de maturidade da organização em controlar e mitigar os riscos de incidente de segurança;** **● Agilidade e proatividade da organização para notificar à Agência e o titular, quando aplicável, mitigar os dados e, se possível, reverter eventuais prejuízos causados;** **● Necessidade de análise do caso concreto, diante da gravidade do fato, a penalidade a ser aplicada, o porte e o ramo de atividade da empresa;** **Além disso, devem ser considerados algumas questões que podem auxiliar na definição, de maneira assertiva, sobre a gravidade do incidente no caso concreto, tais como:** **a) O titular solicitou acesso dos seus dados pessoais para revisão e atualização?** **b) Os dados pessoais foram protegidos contra acesso não autorizado? De que forma?** **c) Há mecanismos de controles para realizar a coleta de dados pessoais, armazenamento e descarte?** **d) O vazamento ocorreu por qual(is) servidore(s) de dados?** **e) A empresa deverá informar o mapeamento de dados e sistemas evidenciando que os servidores estavam protegidos por uma rede segura.** **f) Como medida preventiva, deve entregar o relatório de impacto comprovando que as informações estavam associadas ao mapeamento de dados.** **g) Existe firewall ativo e configurado para atender a segurança dos dados?** **h) Existe antivírus corretamente configurado e atualizado para impedir ataques?** **i) Existe controle de acesso de rede com mecanismos de política de senha implementado com parâmetros mínimos de segurança?** **j) Todos os sistemas operacionais foram atualizados com correção para impedir vulnerabilidade na rede?** **k) Os compartilhamentos de informações possuem permissões explícitas configuradas para permitir apenas o acesso dos usuários relevantes a eles e não utilizar grupos?** **l) Foram realizadas anualmente análises de vulnerabilidades de segurança com especialistas para garantir que o ambiente e processo resistam a um ataque real?**
Existe alguma metodologia recomendada para a análise de	**Gestão de Riscos baseada na ISO 31000**

gravidade do incidente de segurança? Se sim, qual(is)?	
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	**Apresentação de planos de ação para correção de eventuais falhas que resultaram no incidente e, ainda, que contemplem preferencialmente ações preventivas e planos de gestão de mudança com intuito de tornar a proteção de dados intrínseca as atividades do controlador.**
SUGESTÃO DE NORMATIVO, SE HOUVER	
Art. Xxxx	
Art. Xxxx	

Associação Brasileira dos Terminais Portuários – ABTP

Jesualdo Silva

Diretor-Presidente

ANPD Autoridade Nacional de Proteção de Dados

CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO: AJINOMOTO DO BRASIL IND. E COM. DE ALIMENTOS LTDA.

CNPJ: 46.344.354/0001-54

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS **IMPORTANTE:** Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	O *European Data Protection Board* (EDPB), ao se posicionar sobre o tema, orienta que na avaliação se considerem os seguintes critérios: a) O tipo do incidente e em qual nível ele pode afetar o indivíduo; b) A natureza, sensibilidade e o volume dos dados pessoais envolvidos. c) Facilidade com que os indivíduos podem ser identificados. d) Gravidade das consequências para o titular de dados. e) Características especiais do titular de dados. f) Características especiais do controlador. g) O número de indivíduos afetados. Os critérios acima permitem que a ANPD conheça a gravidade do incidente tendo, desta forma a capacidade de determinar qual a probabilidade de dano aos titulares e qual a extensão do dano que pode vir a ser causado aos titulares de dados atingidos. Outros fatores que podem ainda ser acrescentados à lista: a) se o incidente foi interno ou externo; b) nível de confidencialidade dos dados violados; e c) efetividade da contenção do incidente. European Data Protection Board. Guideline on Personal data breach notification under Regulation 2016/679. Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052.

<table>
<tr>
<td>O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc.)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?</td>
<td>
O framework NIST 800 - 37 define que o nível de risco é obtido em função da probabilidade da ocorrência de um evento adverso e o impacto proveniente desta ocorrência. Dessa forma é possível subdividir o risco em níveis. Padronizar os itens que compõem essa função (probabilidade x impacto) é algo recomendável.

A European Union Agency for Cybersecurity (ENISA) descreve uma metodologia para encontrar o nível de risco envolvido em um incidente de segurança de dados, apoiada em três critérios base, de forma a calcular a gravidade do incidente.

As variáveis são as seguintes:

(1) Contexto do tratamento de dados – que considera o tipo do incidente e outras características contextuais do evento;
(2) A facilidade de identificação do indivíduo atingido pelo incidente; e
(3) Circunstâncias do incidente, que se preocupa com as questões de segurança na ocorrência do incidente.

Resumidamente a partir dessas variáveis pela aplicação da fórmula: Gravidade = Contexto do tratamento de dados x Facilidade de identificação + Circunstâncias do incidente é possível atribuir um valor para o risco dentre os níveis baixo, médio, alto e muito alto.

Para aplicar a fórmula é preciso que as variáveis Contexto do tratamento de dados, Facilidade de Identificação e Circunstâncias do incidente tenham seus valores conhecidos previamente. Isso é possível a partir da criação de tabelas em que se atribuem scores a situações específicas para serem utilizadas nessas situações.

Utilizando o modelo acima descrito, é possível criar uma tabela de scores da seguinte maneira:

<table>
<tr><td>Gravidade < 2</td><td>Baixo</td><td>Indivíduos não seriam afetados ou enfrentariam poucas inconveniências.</td></tr>
</table>
</td>
</tr>
</table>

<table>
<tr>
<td></td>
<td>
<table>
<tr><td>2<=gravidade<3</td><td>Médio</td><td>Indivíduos podem ter problemas significantes</td></tr>
<tr><td>3<=gravidade<4</td><td>Alto</td><td>Indivíduos podem enfrentar problemas significantes e dificuldades sérias.</td></tr>
<tr><td>4<=gravidade</td><td>Alto Risco</td><td>Indivíduos podem enfrentar problemas irreversíveis.</td></tr>
</table>

Adotando essa metodologia, riscos baixos, com baixa probabilidade de dano, não seriam considerados relevantes.

NIST 800-37r2. Disponível em: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

Recomendations for a methodology of the assessment of severity of personal data breaches Disponível em: https://www.enisa.europa.eu/publications/dbn-severity
</td>
</tr>
<tr>
<td>Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?</td>
<td>O framework NIST 800-37 define o risco como a medida em que uma entidade é ameaçada por uma circunstância ou evento potencial.

No contexto do Código Civil brasileiro dano é toda lesão que causa prejuízo.

Assim, risco e dano, no contexto de incidentes de segurança de dados, são conceitos que se complementam, mas não se confundem. Enquanto o risco representa a probabilidade de o dano ocorrer, o dano representa a consequência da concretização do risco.

Nesse sentido o Information Comissioner's Office (ICO) define que os riscos relativos à privacidade se relacionam à exposição ou utilização indevida dos dados pessoais do titular de dados, ou seja, é o potencial risco da ocorrência de consequências negativas para o titular caso ele tenha a segurança dos seus dados violada. Já o dano pode vir a ser uma consequência da exposição indevida. Dessa forma, a existência do risco não implica necessariamente na existência do dano.</td>
</tr>
</table>

	Os critérios para avaliação do risco devem considerar o potencial de dano que o incidente pode vir a causar ao titular do dado. Dentre os danos possíveis, existem os danos morais, materiais e/ou físicos. Assim, as consequências de um incidente de segurança de dados pessoais, que seria o dano, podem ser, mas não se resumem a: perda do controle dos dados pessoais, limitação ao exercício de direitos, discriminação, roubo de identidade ou fraude, perdas financeiras, danos reputacionais ou ainda outras desvantagens econômicas ou sociais que possam causar preocupações aos indivíduos. NIST 800-37r2. Disponível em: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf *Personal data breaches.* Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/
O que deve ser considerado na avaliação dos riscos do incidente?	A ICO orienta que na avaliação dos riscos do incidente deve-se observar as possíveis consequências do evento, ou seja, como e em que grau o incidente pode afetar os indivíduos envolvidos e qual a probabilidade dessas consequências acontecerem. O EDPB ao se posicionar sobre o tema, orienta que na avaliação se considerem os seguintes critérios: a) O tipo do incidente e em qual nível ele pode afetar o indivíduo; b) A natureza, sensibilidade e o volume dos dados pessoais envolvidos. Nesse ponto, atenção especial deve ser dada para incidentes que envolvam dados sensíveis nos termos da lei. Em regra, quanto maior a sensibilidade do dado, maior o dano que sua exposição indevida pode causar ao titular dos dados. Ainda nesse ponto, também é preciso avaliar o contexto da violação, quanto mais informações sobre o mesmo titular forem expostas, maior o risco do dano se concretizar e também maior o risco de ser um dano relevante. c) Facilidade com que os indivíduos podem ser identificados. Existe diferença no impacto causado por um incidente envolvendo dados criptografados e incidentes envolvendo dados em texto plano. No primeiro caso certamente a probabilidade de que haja dano ao titular do dado é menor do que no segundo caso. d) Gravidade das consequências para o titular de dados. Quando um incidente envolver a exposição indevida de dados pessoais que possam resultar em roubo de identidade ou fraude, em riscos à integridade física ou psíquica, humilhação ou prejuízo à reputação a probabilidade de dano será alta e se o dano se concretizar será grave, logo impactará na valoração do risco,

	atingindo um grau muitas vezes catastrófico. Ainda na análise desse critério deve-se incluir a temporalidade do dano. Dadas as características do meio digital em que grande parte dos incidentes acontecem, o dano poderia perpetuar-se no tempo tornando-o mais grave. e) Características especiais do titular de dados. Outro fator que contribui para a gravidade do incidente é o envolvimento de indivíduos vulneráveis. No Brasil, por força da própria LGPD e do Estatuto da Criança e do Adolescente fariam parte desse grupo crianças e adolescentes. f) Características especiais do controlador. A própria natureza do negócio que exige o tratamento de dados pessoais interfere na análise do risco de o incidente causar um dano relevante. Negócios que atuam de forma preponderante com dados sensíveis por si só já tem um nível de risco elevado; g) O número de indivíduos afetados. Esse critério tem influência relativa na construção do valor do risco. Obviamente, incidentes envolvendo um grande número de indivíduos gera a desconfiança de que o dano será automaticamente relevante. Entretanto, pequenos incidentes com dados especialmente sensíveis podem causar impactos catastróficos na vida dos titulares de dados atingidos. Nesse caso, é preciso ponderar em conjunto, a natureza dos dados expostos e o contexto em que o incidente ocorreu. Adotar todos os critérios elencados na avaliação dos riscos do incidente possibilitará uma visão ampla do contexto em que o evento ocorreu. Dessa forma, será mais assertiva a abordagem na contenção ou mesmo mitigação dos danos provenientes do evento. EDPB - Guideline on Personal data breach notification under Regulation 2016/679. Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052.
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	Outras informações que, se informadas pelos controladores, subsidiariam a ANPD: a) Tipo do incidente; b) Características do incidente: violação da confidencialidade, da disponibilidade ou da integridade dos dados. Essas informações subsidiariam a ANPD na análise do contexto em que o incidente ocorreu e também sobre a sua gravidade.
Qual o prazo razoável para que controladores informem a ANPD sobre	O prazo de 72 horas nos parece razoável para o primeiro comunicado para a ANPD, desde que efetivamente compreendido o que ocorreu e suas consequências. Analisando a legislação

o incidente de segurança? (art. 48, §1º)	comparada, temos que Regulamento Europeu e a Lei do Uruguai preveem 72 horas após o conhecimento do vazamento como prazo para realização do comunicado. Regulamento Europeu - https://gdpr-info.eu/ Lei do Uruguai - https://www.impo.com.uy/bases/leyes/18331-2008/29
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	Idealmente a comunicação aos titulares deve ser realizada somente após a confirmação de três condições: a) o incidente envolveu dados pessoais; b) o incidente representa realmente um risco relevante ou um dano relevante, e c) após a correta identificação de quem são os indivíduos atingidos. Não há um prazo exato para que se tenha conhecimento dessa informação, mas ela deve ser feita o mais brevemente possível, sem atrasos injustificados. Em relação ao comunicado para os titulares ele deve conter: a) Indicação da data que a empresa teve conhecimento da ocorrência do incidente; b) Se o incidente ocorreu no ambiente do controlador ou em um parceiro; c) Uma breve narrativa da ocorrência contemplando o tipo do incidente e quem são os titulares atingidos; d) Medidas que foram tomadas para solucionar ou mitigar as consequências do incidente; e) Quais dados foram afetados; f) Quais os riscos concretos para o titular dos dados pessoais e qual a gravidade do risco; g) Eventuais medidas adotadas para mitigar os possíveis prejuízos para o titular dos dados; h) Orientações sobre medidas que o titular pode adotar para evitar maiores prejuízos; e i) Dados de contato para que o titular possa obter maiores informações. O conteúdo sugerido para o comunicado é mais completo do que aquele sugerido no contexto do Regulamento Europeu. O *Guideline on Personal data breach notification under Regulation* 2016/679 do EDPB orienta que a comunicação aos titulares dos dados pessoais deve conter as seguintes informações: a) Descrição da natureza do incidente; b) O nome e o contato do DPO/ Encarregado ou outro contato; c) A descrição das consequências do incidente; e

	d) A descrição das medidas tomadas ou propostas pelo controlador para resolver o incidente e mitigar efeitos adversos, se necessário. Informações mais detalhadas possibilitam aos titulares compreender o alcance do incidente e quais medidas podem tomar para saber mais sobre o evento bem como para mitigar consequências derivadas do incidente. European Data Protection Board. Guideline on Personal data breach notification under Regulation 2016/679. Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052.
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	A modalidade de comunicação a ser adotada depende do contexto que envolve o incidente. Incidentes com um alto nível de gravidade (probabilidade de dano alta ou muito alta) devem ser comunicados diretamente aos titulares por canais que permitam esse contato, como o e-mail, por exemplo. Entretanto, quando o incidente envolver um grande número de pessoas e o risco de dano envolvido não for alto ou muito alto, pode ser feito divulgado via comunicação pública. É necessário ainda considerar o nível de esforço que a organização terá que realizar para comunicar o incidente aos titulares de dados, para não inviabilizar o próprio negócio. Não faz sentido, por exemplo, ter de obter dados pessoais complementares para fazer a notificação.
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	O *Guideline on Personal data breach notification under Regulation* 2016/679 do EPDB orienta que a notificação das autoridades supervisoras não seria necessária nas seguintes situações: a) Quando o incidente não resultar em risco para os direitos e liberdades dos titulares de dados pessoais; e b) Quando os dados estiverem em formatos ininteligíveis para partes não autorizadas. Seguindo esse entendimento, incidentes envolvendo dados pessoais já disponíveis publicamente em listas públicas não exigiriam notificação para a ANPD bem como a exposição de dados criptografados sem que a chave de segurança tenha sido violada também não devem ser notificados. Acrescente-se a isso situações de incidente internos, como por exemplo, acessos indevidos, por eventuais falhas no controle de acessos, envolvendo os próprios colaboradores da organização, por ocorrerem em ambiente restrito e com baixo potencial de dano ao titular dos dados pessoais também não mereceriam ser notificados para a ANPD.

	Guideline on Personal data breach notification under Regulation 2016/679 - EDPB. Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052.
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	O Guideline on Personal data breach notification under Regulation 2016/679 do EPDB orienta que a comunicação aos titulares dos dados não é necessária nas seguintes situações: a) Quando os dados expostos estão protegidos de tal forma que não podem ser lidos; b) Quando imediatamente após o incidente o controlador conseguiu mitigar o alto risco tornando improvável a ocorrência de danos ao titular dos dados; c) Quando o esforço a ser adotado para fazer o comunicado é desproporcional. No contexto da LGPD, faz sentido aplicar as mesmas exceções. Seria possível acrescentar à lista de exceções incidentes com baixo risco de dano aos titulares, como destacado anteriormente. Guideline on Personal data breach notification under Regulation 2016/679 - EDPB. Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052.
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	Para garantir o tratamento isonômico para todas as organizações, a ANPD deve adotar uma metodologia que permita compreender a probabilidade do dano aos titulares de dados pessoais atingidos pelo incidente. Nesse sentido, aplicar a metodologia adotada pela ENISA, anteriormente mencionada, utilizando as variáveis **Contexto do tratamento de dados, Facilidade de identificação e Circunstâncias do incidente** a partir de scores previamente determinados permite contemplar todos os fatores envolvidos no incidente. Inclusive se a organização adotava boas práticas de segurança da informação antes do evento ocorrer, fator contido na variável **Circunstâncias do incidente**.
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	ISO 27.000, em especial ISO/IEC 27035-1 — Information Security Incident management, onde há uma referência para priorização e categorização de incidentes de segurança da informação. Recommendations for a methodology of the assessment of severity of personal Data Breaches – The European Union Agency For Network and Information Security (ENISA). Disponível em: https://www.enisa.europa.eu/publications/dbn-severity.

Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	O cabimento das medidas sempre dependerá da análise do cenário em que o incidente ocorreu. Incidentes internos, por exemplo, demandariam treinamentos de reciclagem em segurança da informação, enquanto incidentes externos demandariam realização de testes de vulnerabilidades. De toda forma, algumas medidas devem sempre ser implementadas após um incidente: a) Registro da ocorrência com todos os detalhes pertinentes; b) Monitoramento do ambiente para evitar novos incidentes; c) Treinamentos de segurança da informação e proteção de dados; d) Análise de segurança das tecnologias incorporadas ao negócio (hardware e softwares); e e) Revisão do plano de gestão de incidentes.
SUGESTÃO DE NORMATIVO, SE HOUVER	

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: ANA LIZ VIEIRA SOARES

CPF/CNPJ: [redacted]

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS **IMPORTANTE:** Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	**Quando causar algum tipo de discriminação ao titular dos dados, ou ainda violar direitos fundamentais previsto na Constituição Federal e os direitos do Titular descritos na própria Lei de Proteção de Dados causando danos graves ou irreversíveis.** **Fundamentação: Art.5° da CF elenca um extenso rol de direitos e garantias fundamentais, dentre os quais a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas.**
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	**Sim. Risco leve, moderado e Alto. A distinção do risco deve ser feita com base na categoria dos dados (Dados comuns/ Sensíveis) e levando em consideração também a pessoa que é o titular dos dados (Adulto/Crianças e Adolescentes), e por fim a forma como estão sendo tratados os dados, se estão sendo respeitados os direitos dos titulares e se o tratamento aplicar os princípios previstos na Lei de Proteção de Dados. Deve se avaliar ainda, se existe algum controle de risco ou plano de contingência em caso de vazamento de dados e danos aos titulares.**
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	**Risco ao titular- É a probabilidade de um evento acontecer, seja ele uma ameaça, quando negativo, ou oportunidade, quando positivo devido a tratativa dos dados. Ex: Violação dos seus direitos ou algum tipo discriminação.** **Dano ao Titular- Quando o risco se concretiza em forma ação/evento causando danos morais ou materiais ao titular dos dados.**

O que deve ser considerado na avaliação dos riscos do incidente?	**Origem dos dados/Categoria (Comum/Sensíveis)/Responsáveis pelo tratamento dos dados/Base legal/Violação dos Princípios/Plano de Contingência existente para coibir ou sanar possíveis incidentes dos dados tratados.**
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	**Origem dos dados/Fluxo dos dados/Categoria/Forma de tratamento/Responsáveis pelo tratamento dos dados/Plano de contingência.**
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	**48 horas, sendo esse prazo razoável para passar todas as informações necessárias para Agência Reguladora.**
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	**24 horas, Levando em consideração que o titular dos dados é parte mais vulnerável e devido ao aumento no índice de fraudes e golpes que estão ocorrendo a todo instante, assim, o quanto mais rápido comunicar o titular, menos risco terá do mesmo cair em possíveis golpes ou fraudes devido ao vazamento dos dados.**
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	**Comunicação direta e Individual- Quando se tratar de dados sensíveis e de Crianças e Adolescentes.** **Comunicação Publica – Dados Comuns, Públicos e identificáveis.**
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	**Apenas quando ameaça de risco for sanada a tempo. Quaisquer outras situações envolvendo os dados deve ser comunicado Agência, se possível solicitando orientações para tratativa dos dados.**
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	**Apenas quando ameaça de risco for sanada a tempo. Quaisquer outras situações envolvendo os dados deve ser comunicado ao titular, mostrando desta forma boa-fé e transparência na tratativa dos dados.**
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de	**Violação dos direitos do Titular/Princípios/Base Legal/Plano de Contingência/ Analise Preliminar do Risco/ Segurança da Informação.**

segurança? (art. 48, §2º)	
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	**Técnica de Incidentes Críticos- É uma** técnica qualitativa**, para** identificar falhas **e** condições inseguras **que podem contribuir para a ocorrência de acidentes reais ou potenciais. A técnica tem como** objetivo **a** detecção de incidentes críticos e o tratamento dos riscos **que os mesmos representam. Para isso utiliza-se de uma equipe de entrevistados representativa dentre os principais departamentos da empresa, procurando representar as diversas operações da mesma dentro das diferentes categorias de risco.**
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	**Investigar a causa do Incidente, Reavaliar Programa de Adequação, Treinar todos os envolvidos na tratativa dos dados a cada incidente ocorrido, mostrando novas tratativas ou reforçando as medidas que estão sendo adotadas corretamente.**
SUGESTÃO DE NORMATIVO, SE HOUVER	
Art. Xxxx	
Art. Xxxx	

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL - ANAC

CPF/CNPJ: 07.947.821/0001-89

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS **IMPORTANTE:** Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	**1) Quando um incidente pode acarretar risco ou dano relevante ao titular?** Um dano pode ser causado pela perda ou destruição de informações que são imprescindíveis para o titular, como o histórico escolar de um aluno de faculdade, informações de saldo e extrato bancário de um correntista, dentre outros. Um risco pode ser gerado por um vazamento de informações pessoais que permitam a um terceiro realizar fraudes se passando pelo titular. Tal vazamento pode se potencializar, quando este terceiro, se passando pelo titular, exercer direitos previstos pela LGPD junto à controladores, obtendo mais dados pessoais. **2) Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?** A análise quantitativa com base nos critérios de probabilidade e impacto tem sido amplamente realizada. Embora a sugestão destes critérios seja óbvia, a determinação de seus valores não o é, o que se torna ainda mais difícil em função de as análises de incidentes envolvendo dados pessoais seja recente, embora o termo privacidade não.
O risco ou dano relevante deveria ser subdividido em mais categorias (ex.	**1) O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)?**

Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	Com certeza, pois possibilitaria classificá-los melhor e priorizá-los. **2) Como distinguir os níveis?** Para eliminar subjetividade, seria recomendável a utilização de uma fórmula. Os dados seriam classificados em categorias ou níveis (financeiro, acadêmico, familiar etc) e cada categoria teria um peso. A quantidade de dados de cada categoria seria multiplicada pelo peso da categoria, e esses produtos seriam somados. O valor desta soma seria comparado com uma faixa, que definiria assim o nível correspondente. Cabe ressaltar que a distinção dos níveis deve levar em conta o titular do dado. **3) Risco ou dano baixo deve ser considerado relevante ou não relevante?** Não relevante. A prioridade devem ser os riscos médios e altos (necessário definir a matriz de risco).
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	**1) Como distinguir o risco ao titular do dano ao titular?** Sendo dano o mal, prejuízo, ofensa material ou moral causada por alguém a outrem, deve-se analisar em relação ao incidente se a consequência já ocorreu ou se ela irá ocorrer. Assim, tendo a consequência ocorrido já configura o dano e caso contrário ela deve ser considerada risco. **2) Como esses conceitos se relacionam?** A concretização de um risco pode levar a um dano.
O que deve ser considerado na avaliação dos riscos do incidente?	**1) O que deve ser considerado na avaliação dos riscos do incidente?** O que deve ser considerado na avaliação dos riscos do incidente dependerá da metodologia que a Autoridade utilizar. A título de exemplo, seguem as etapas que compõem o processo de Gestão de Riscos de Tecnologia da Informação e Comunicações da ANAC: I - Definições Preliminares; II - Análise/Avaliação dos Riscos de TIC; III - Plano de Tratamento dos Riscos de TIC; IV - Aceitação de Risco de TIC; V - Implementação do Plano de Tratamento dos Riscos de TIC; VI - Monitoração e Análise Crítica; VII - Melhoria do Processo de GRTIC; VIII - Comunicação do Risco de TIC.

Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	**1) Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?** Entende-se que não há necessidade de informação adicional.
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	**1) Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)** Estabelecer um prazo sem condições de ser cumprido, acaba provocando uma falta de comprometimento em o perseguir. Por mais absurdo que pareça, muitas empresas não vão conseguir reunir as informações solicitadas antes de um mês. Um caminho factível seria a empresa comunicar o vazamento à ANPD em até 2 dias após conhecimento do incidente, e o fazer com os detalhes que já possui, que com certeza serão mínimos neste momento. Se em 15 dias a empresa ainda não tiver conseguido levantar todas as informações, enviar um relatório parcial com as informações já disponíveis. E um prazo final de 1 mês para o envio de todas as informações solicitadas.
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	**1) Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º)** Pelos motivos expostos na resposta anterior, um mês.
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	**1) Qual a forma mais adequada para a realização da comunicação do incidente aos titulares?** Comunicação por mídia eletrônica (correio eletrônico, SMS etc). **2) A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?** Preferencialmente direta e individual para evitar gerar mais riscos ao titular. Em casos específicos, podem ser admitidas comunicações coletivas ou públicas.

Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	**1) Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?** As exceções da obrigatoriedade de informar a ANPD são as situações que não geram riscos ou geram baixo risco ao titular.
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	**1) Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?** As exceções da obrigatoriedade de informar a ANPD são as situações que não geram riscos ou geram baixo risco ao titular.
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	**1) Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)** Risco de dano à imagem ou reputação Risco de prejuízo financeiro
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	**1) Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?** Entende-se que a gravidade do incidente de segurança é subjetiva e deve ser analisada caso a caso.
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	**1) Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?** Elaboração de relatório de diagnóstico do incidente, definição de um plano de ação para restaurar a situação inicial prévia ao incidente, elaboração de relatório de acompanhamento (status report) da implementação de ações de correção e definição de ações de contingência e mitigação para o risco.

SUGESTÃO DE NORMATIVO, SE HOUVER	
Art. Xxxx	
Art. Xxxx	

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: ANAHP – Associação Nacional dos Hospitais Privados

CPF/CNPJ: 04.832.584/0001-12

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS **IMPORTANTE:** Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	Entendemos que um incidente deve ser enquadrado como relevante, quando o tratamento de dados pessoais acarretar riscos às liberdades civis e aos direitos fundamentais. Acreditamos que a Autoridade Nacional (ANPD) deve disciplinar e estabelecer critérios de forma clara, objetiva, descrevendo a materialidade do dano e as formas de mitigações técnicas empregadas e esperadas para remediação de incidentes, para que os agentes de tratamento adotem padrões na análise de risco de seus processos assistenciais, de negócio, apoiando, inclusive, na elaboração do relatório de impacto à proteção de dados pessoais. Consideramos que um risco será relevante, quando: • As atividades de tratamento usem métodos não recomendáveis ou contrários às boas práticas adotadas pelo seu segmento de atuação na economia no momento do tratamento; • Os agentes de tratamento realizem processos de tratamentos de dados que sejam contrários aos princípios e diretrizes da Lei Geral de Proteção de Dados Pessoais; • O Controlador dos dados pessoais identificar um alto risco no processo de tratamento e não adotar medidas de mitigação destes riscos.

	• O incidente ocasionar significativas ou irreversíveis consequências aos titulares de dados; Como critérios à ANPD sugerimos: o tipo de dado se pessoal ou sensíveis, quais foram as medidas de remediação adotadas posteriormente ao incidente, qual o real efeito do incidente para o titular de dados, qual a probabilidade de o titular de dados sofrer algum dano por conta do incidente, qual a chance de terceiros utilizarem indevidamente os dados objetos do incidente. As previsibilidades de materialização de um risco devem ser pautas por critérios de avaliação de riscos inerentes a um determinado processo bem como critérios de avaliação da vulnerabilidade (maior ou menor nível de proteção) dos controles aplicados a este processo na organização**.**
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	Sim, acreditamos que a adoção de categorias de risco ou dano auxiliará na identificação da criticidade do incidente e, por consequência, a quais medidas mitigadoras e corretivas devem ser priorizadas pelos agentes de tratamento. Características que poderão ser adotadas para identificar o risco ou o dano: <u>Alto</u>: • Quando o incidente resultar em consequências significantes comprovadas para um titular dos dados; • Nos casos em que os agentes de tratamento realizem processos de tratamentos de dados que sejam contrários aos princípios e diretrizes da Lei Geral de Proteção de Dados Pessoais; <u>Médio</u>: • Incidente que possa ocasionar constrangimento e afetar direitos fundamentais dos titulares de dados <u>Baixo</u>:

	• Nos casos em que o incidente não possibilite constrangimento relevante ao titular, resultando em mero dissabor cotidiano; • Quando o incidente possibilitar o acesso a dados pessoais e informações que são possíveis de serem obtidas em portais e banco de dados públicos. Por fim, julgamos que risco e danos classificados como baixos não deverão ser notificados à ANPD, por não ser um tema de interesse social, o alto volume de demandas e solicitações e possível incidentes pontuais poderão ser solucionados
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	Consideramos que risco é o efeito da incerteza de um evento que pode ocorrer na persecução dos objetivos (International Organization for Standardization, 2009). De acordo com o RGPD, na implicação (75), o risco é descrito da seguinte forma (Council of the European Union, 2016): *"O risco para os direitos e liberdades das pessoas singulares, [...], poderá resultar de operações de tratamento de dados pessoais suscetíveis de causar danos físicos, materiais ou imateriais, …"* Assim, resta claro que, muitas vezes, podemos ter um processo de baixo risco com alta probabilidade de dano, dependendo da forma de exposição dos dados e a sua utilização. Inclusive, esse é um tema extremamente relevante para o setor da saúde que lida no dia a dia com alto volume de processos de tratamento de dados sensíveis. Portanto, muitas vezes estaremos lidando com dados que possam resultar em alto dano ao titular mesmo que o risco seja baixo ou mitigado pelos agentes de tratamento. Desta maneira, fundamental que se analise as particularidades inerentes aos serviços de saúde, e que se defina os conceitos de dano e risco com clara e nítida separação. Assim, somente os incidentes que possuírem cumulativamente a probabilidade de risco alto e dano alto deverão ser notificados à ANPD e aos titulares de dados.

O que deve ser considerado na avaliação dos riscos do incidente?	• A probabilidade do risco, devendo ser observado as práticas e as características de setores específicos, de acordo com o Artigo 55-J, XXIII, da LGPD; • O nível de vulnerabilidades dos controles identificadas no processo de tratamento de dados; • Se foram realizas medidas efetivas para mitigar os riscos identificados;
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	Entendemos que as informações listadas pelo artigo em análise são suficientes para demonstrar o processo e quais são os riscos e os danos do incidente em questão. A comunicação é apenas um primeiro contato, tendo em vista que ANPD solicitará informações complementares ou, inclusive, determinar as medidas previstas no parágrafo segundo do artigo 48. O prazo de 2 (dois) dias pode não ser factível para que uma Organização tenha uma visão macro do incidente deixando de fornecer informações relevantes a análise.
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	Tendo em vista que, a notificação visa identificar a necessidade de adotar medidas mitigadoras e possibilitar transparência do incidente, sugerimos no mínimo 5 (cinco) dias úteis contados da data de conhecimento dos fatos.
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	Entendemos que o titular deve ser comunicado posteriormente à ANPD a depender do incidente para que a comunicação seja efetiva e não gere "pânico" ao titular, não entendemos que seria eficaz a comunicação de todo o detalhamento relacionado no §1º do art. 48 por conter um caráter estritamente técnico e poderia, assim, inviabilizar o entendimento do titular sobre o incidente. Sugerimos que seja considerado situações em que somente a ANPD deve ser comunicada ou somente o titular. Sendo assim, sugerimos que conste na comunicação os itens I, II e VI do § 1º do art. 48, pois em nosso entendimento já são suficientes para esclarecer o incidente para os titulares. Ademais, sugerimos que a comunicação seja realizada após o levantamento de dados que componham uma informação objetiva e íntegra com as ações de adequação já definidas para que o titular entenda a dimensão do problema e o que foi executado pela empresa
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em	Via de regra, entendemos que a comunicação deverá ser realizada de forma individual e direta, por canais que possibilitem registrar o recebimento da mensagem que o Controlador endereçará ao titular, como o envio de e-mail, ligação telefônica com gravação da conversa, dentre outros.

determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	Porém, na hipótese de o incidente ocasionar risco ou dano para um elevado número de titulares, acreditamos que deverá ser admitida a notificação através de canais públicos, como a página do Controlador na internet, o envio de nota oficial à imprensa e demais canais de comunicação que os seus titulares sejam impactados.
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	Entendemos que aos incidentes qualificados como risco baixo e baixa probabilidade de dano ao titular do dado não devem ser notificados à ANPD, nos termos do §7° do Artigo 52.
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	Incidentes qualificados com risco baixo e baixa probabilidade de dano ao titular do dado
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	Consideramos que os critérios devem estar atrelados aos níveis de riscos e danos identificados e classificados como: alto, médio ou baixo. Assim, a gravidade sempre estará atrelada a critérios claros e objetivos, possibilitando maior previsibilidade e transparência aos agentes de tratamento. Avaliar natureza, sensibilidade, dano à privacidade conforme direitos fundamentais previstos na LGPD, volume de titulares afetados e dimensão (territorial).
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	Metodologias adotadas pelas organizações, que estejam embasadas em melhores práticas de mercado como por exemplo: ISO 31000 — Risk management; https://www.nist.gov/; European Union Agency for Network and Information Security (ENISA): Recommendations for a methodology of the assessment of severity of personal data breaches, Para questões de volumetria, o da Commission Nationale de L'Informatique et des Libertés (CNIL): Methodology for Privacy Risk Management.
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	Sugerimos que a ANPD sugira ações educativas aos controladores com prazo factível para implementação. Autoridade deve avaliar extensão do incidente, pessoas envolvidas e dados envolvidos para verificar forma de definir gravidade e definir valor da multa, observada a proporcionalidade e análise de risco e dano efetivamente materializado.

SUGESTÃO DE NORMATIVO, SE HOUVER	
Art. Xxxx	
Art. Xxxx	

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2/2021

NOME DA INSTITUIÇÃO: Associação Nacional dos Bureaus de Crédito

CNPJ: 23.681.486/0001-76

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS	
IMPORTANTE: Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	O risco é a probabilidade/possibilidade de uma determinada ameaça ou dano se concretizar, enquanto o dano é a materialização do risco indicado. Em relação aos critérios a serem considerados, encontram-se descritos nas respostas aos itens seguintes.
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	O dano, por si só, deve ser subdividido em níveis como baixo, médio, alto e significativo. **Nível baixo** aquele que pode gerar inconvenientes e aborrecimentos no cotidiano dos titulares e que podem ser superados sem esforços significativos (mudança de senha, envio de documentos comprobatórios de identidade etc) ou quando os dados objeto do incidente são idênticos àqueles que já foram objeto de incidente anterior recente. Não coloca em risco a integridade física do titular e é improvável que traga impactos econômicos e morais permanentes ou significativos. **Nível médio** aquele que pode gerar aborrecimentos razoáveis também no cotidiano dos titulares e que pode ser superado apesar de requerer esforços razoáveis (acesso negado a determinado serviço urgente ou emergencial, custo com autenticação de novos documentos, exclusão de um registro indevido em cadastro de inadimplentes etc). Da mesma forma, não coloca em risco a integridade física do titular e é improvável que traga impactos econômicos e morais permanentes ou significativos.

	Nível alto aquele que pode gerar inconvenientes expressivos que podem ser superados com esforço significativo (dano patrimonial, perda de emprego ou relacionamentos afetivos, agravamento de saúde mental, etc.). Aqui, é possível que haja impactos econômicos e morais a curto prazo. **Nível significativo** aquele que pode causar graves consequências e, em alguns casos, até mesmo irreversíveis (morte, impossibilidade de retorno à atividade laboral, danos físicos ou mentais a longo prazo, etc). Aqui, é possível que haja impactos econômicos e morais a longo prazo ou permanentes. Além disso, apesar de a quantidade de dados afetados ser importante, esse não deve ser o único critério utilizado para obrigatoriedade da comunicação, mas sempre em conjunto com a categoria de informações que sejam objeto de eventual incidente de segurança, além da vinculação aos níveis de danos mencionados acima. Considerando o disposto acima, o termo 'relevante' e a consequente necessidade de comunicação à ANPD e aos titulares seriam apenas aplicáveis nos casos em que há dano de nível alto e/ou significativo.
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	O risco é a probabilidade/possibilidade de uma determinada ameaça ou dano se concretizar, enquanto o dano é a materialização do risco indicado. Em relação ao risco, recomenda-se também considerar a probabilidade de materialização, que pode ser subdividida em remoto, possível, provável e muito provável. **Remota (inferior a 35%):** probabilidade remota de concretização do risco, considerando que a empresa utiliza as melhores práticas de segurança da informação. **Possível (de 36% a 65%):** possível concretização do risco, considerando que, apesar de serem adotadas técnicas razoáveis de segurança da informação, a empresa não considera o tratamento de dados como prioridade e está mais suscetível a ataques e incidentes. **Provável (de 66% a 90%):** probabilidade alta de concretização do risco, considerando que a empresa possui poucos mecanismos de segurança da informação e não considera o tratamento de

	dados como prioridade, estando vulnerável a ataques e incidentes. **Muito provável (91% a aproximadamente 100%):** probabilidade significativa de concretização do risco, considerando que a empresa realiza tratamento de dados pessoais e não possui mecanismos de segurança da informação, estando completamente vulnerável a ataques e incidentes.
O que deve ser considerado na avaliação dos riscos do incidente?	- Critérios, regras, sistemas e procedimentos de segurança adotados pela Companhia, inclusive certificações e assegurações; - Categoria de dados pessoais tratados; - Quantidade de dados pessoais e titulares afetados; - Qualidade, como, por exemplo, atualidade dos dados afetados e consequente capacidade de gerar danos aos titulares; - Existência e implementação de Plano de Gestão de Crises em caso de incidentes; - Publicização anterior dos dados pessoais objeto de um incidente em razão de incidente anterior, obrigação legal, regulatória ou contratual ou decisão de negócios de terceiro, e os danos concretos que podem advir da nova publicização; - Governança das atividades de tratamento de dados e mapeamento dos riscos dela decorrentes, com a implementação das respectivas medidas de mitigação;
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	Entendemos que as informações listadas no referido artigo da LGPD são suficientes. Conforme orientações prévias da ANPD, publicadas no dia 22 de janeiro de 2021, comunicação realizada via peticionamento eletrônico, com disponibilização de formulário no site da ANPD.
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	Sugere-se que, uma vez confirmada, pelo controlador, a ocorrência do incidente, este informe a ANPD em até 2 (dois) dias úteis.

Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	Sugere-se que os controladores informem os titulares o quanto antes uma vez confirmada a ocorrência do incidente, recomendando-se, como prazo máximo, 5 (cinco) dias úteis após a referida confirmação. As informações a serem fornecidas aos titulares devem ser suficientes para que eles compreendam o ocorrido, as ações tomadas pelo controlador para conter eventuais prejuízos e as medidas que deve adotar para se prevenir em relação a potenciais danos. Diante disso, sugere-se que devem descrever a natureza dos dados pessoais afetados (inc. I), os riscos relacionados ao incidente (inc. IV), as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo (inc. VI), sem comprometer a própria segurança da operação do controlador, e as medidas que o titular pode adotar para prevenir-se contra danos decorrentes do uso indevido de seus dados.
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	A comunicação deve ser realizada de forma eficiente e adequada a cada caso. Preferencialmente deve ser individualizada, se possível, por quaisquer canais disponíveis, como e-mail, SMS ou carta. Caso não seja possível o contato direto ou se trate de quantidade expressiva de titulares a serem comunicados, pode-se considerar também a notícia em meios de comunicação em massa, como rádios, jornais e televisão.
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	Todos os casos em que houver dano de nível baixo ou médio, conforme descrições mencionadas nas respostas anteriores.
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	Todos os casos em que houver dano de nível baixo ou médio, conforme descrições mencionadas nas respostas anteriores.
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	**-** Critérios, regras, sistemas e procedimentos de segurança adotados pela Companhia, inclusive certificações e asseguraçõ̃es; - Categoria de dados pessoais tratados; - Quantidade de dados pessoais afetados; - Qualidade, como, por exemplo, atualidade dos dados afetados e consequente capacidade de

	gerar danos aos titulares; - Existência e implementação de Plano de Gestão de Crises em caso de incidentes; - Publicização anterior dos dados pessoais objeto de um incidente em razão de incidente anterior, obrigação legal, regulatória ou contratual ou decisão de negócios de terceiro, e os danos concretos que podem advir da nova publicização; - Governança das atividades de tratamento de dados e mapeamento dos riscos dela decorrentes, com a implementação das respectivas medidas de mitigação.
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	Há algumas metodologias para a análise de gravidade de incidente de segurança, devendo ser adotada aquela mais adequada para a empresa eventualmente impactada. A título de exemplo, citamos a ISO 27035 – Gerenciamento de Incidentes de Segurança da Informação.
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	Acompanhamento das ações de correção e apresentação de relatório de investigação pelo controlador, preferencialmente com procedimentos atestados por terceiro.
Outros temas considerados relevantes	À ANPD, a restrição da publicidade do conteúdo da investigação enquanto estiver em curso, de modo a possibilitar o bom andamento das análises realizadas pelo próprio controlador e por terceiro qualificado para tal procedimento.
SUGESTÃO DE NORMATIVO, SE HOUVER	
Art. Xxxx	
Art. Xxxx	

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: ANDRÉ FELIPE FOGAÇA LINO (OAB/SP 234.168)

CPF/CNPJ: [redacted]

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS	
IMPORTANTE: Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	Todas as respostas sugeridas a seguir tem como base nosso trabalho, como advogado, em empresas que comercializam planos de saúde (corretoras de planos). Para essa questão, o incidente acarreta risco quando terceiros recebem informações da ficha de saúde do usuário, para a contratação do plano de saúde, e que trazem informações sensíveis, como comorbidades, por exemplo. Neste caso, a ANPD deve avaliar se tais fichas de saúde, por exemplo, disponibilizadas na relação das operadoras de planos de saúde com seus usuários, são consideradas como portadoras de dados sensíveis e qual tratamento, e responsabilidades, serão reguladas sobre tal documento.
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	Especificamente quanto a dados sensíveis, como o são aqueles que envolvem a condição de saúde dos usuários de planos de saúde, são de risco ou dano alto, sem ter necessidade de distinção.
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	Se tais dados podem ser divulgados ou não entre as operadoras de plano de saúde, diretamente, ou se corretoras podem ter acesso ou devam colher tais dados junto ao cliente final.
O que deve ser considerado na avaliação dos riscos do incidente?	O destinatário da informação, se ele foi usado para apenas determinar a sinistralidade do paciente ou se para definir a contratação ou declínio do contrato de plano de saúde.

Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	Transferência da informação da declaração de saúde sem autorização entre operadoras.
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	72 horas
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	72 horas
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	Nunca por comunicação pública, por envolverem dados sensíveis, mas por comunicação pelo canal da operadora de plano de saúde com o consumidor.
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	Não vejo exceção, por ser dado sensível.
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	Se o vazamento das informações se deu apenas entre operadoras, sem divulgação para corretoras ou mesmo terceiros que possam usar os dados para estatísticas sobre sinistralidade ou outros fins (publicidade, por exemplo, para contratar determinado plano de saúde porque “aceitam” aquele paciente com determinada comorbidade).
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	

Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	
SUGESTÃO DE NORMATIVO, SE HOUVER	
Art. Xxxx	
Art. Xxxx	

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: Associação Nacional dos Fabricantes de Veículos Automotores ("ANFAVEA")

CPF/CNPJ:[43.054.493/0001-55]

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS **IMPORTANTE:** Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
	Inicialmente, cabe ressaltar que a maioria dos tópicos abordados pela Consulta Pública deve ser objeto de regulamentação por meio dos instrumentos jurídicos adequados. **Os aspectos não regulados da Lei Geral de Proteção de Dados ("LGPD") deveriam ser objeto de decreto presidencial** e defini-los exclusivamente por meio de Consulta Pública pode não ser o caminho mais apropriado do ponto de vista legal. Assim, independente de mérito, entendemos que se trata de um ponto que deve ser considerado.
1. Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	O Art. 48 da LGPD estabelece que "*o controlador deverá notificar a Autoridade Nacional de Proteção de Dados ("ANPD") e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares*". Concentramos a análise dessas definições em dois elementos: **(i)** na interpretação do tema em outras jurisdições, especialmente sob a ótica do GDPR (União Europeia – "UE") (conforme seus Considerandos 75 e 76) e **(ii)** no ordenamento jurídico brasileiro e nas definições existentes de risco e dano (tanto na legislação quanto na jurisprudência). **No âmbito do GDPR (EU)**

	(75) "*O risco para os direitos e liberdades das pessoas naturais , cuja* ***probabilidade*** *e* ***gravidade*** *podem ser variáveis, poderá resultar de operações de tratamento de dados pessoais* ***suscetíveis de causar danos físicos, materiais ou imateriais****, em especial: quando o tratamento possa dar origem à discriminação, roubo da identidade ou fraude, a perdas financeiras, prejuízos para a reputação, perdas de confidencialidade de dados pessoais protegidos por sigilo profissional, à inversão não autorizada da pseudonimização, ou a quaisquer outros prejuízos importantes de natureza econômica ou social; quando os titulares dos dados possam ficar privados dos seus direitos e liberdades ou impedidos de exercerem o controle sobre os seus dados pessoais; quando forem tratados dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas e a filiação sindical, bem como dados genéticos ou dados relativos à saúde ou à vida sexual ou a condenações criminais e infrações ou medidas de segurança conexas; quando forem avaliados aspectos de natureza pessoal, em particular análises ou previsões de aspectos que digam respeito ao desempenho no trabalho, à situação econômica, à saúde, às preferências ou interesses pessoais, à confiabilidade ou comportamento e à localização ou às deslocações das pessoas, a fim de definir ou fazer uso de perfis; quando forem tratados dados pessoais relativos a pessoas naturais vulneráveis, em particular crianças; ou quando o tratamento incidir sobre uma grande quantidade de dados pessoais e afetar um grande número de titulares de dados.*" (76) "*A probabilidade e a gravidade dos riscos para os direitos e liberdades do titular dos dados deverão ser determinadas com base na* ***natureza, âmbito, contexto e finalidades do tratamento de dados****. Os riscos deverão ser aferidos com base numa avaliação objetiva, que determine se as operações de tratamento de dados implicam risco ou risco elevado*. " **No ordenamento jurídico brasileiro** No direito brasileiro, dano é toda lesão a um bem juridicamente protegido, que gera prejuízo de ordem patrimonial ou extrapatrimonial. Nesse sentido, o Art. 186 do Código Civil prevê que "*aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito".* **Portanto, para que se configure um dano passível de indenização, mais do que a lesão a direito, deve haver prejuízo concreto que resulte diretamente de ação ou omissão voluntária, negligência ou imprudência do agente.** Alinhada com esse conceito, a LGPD prevê em seu Art. 48 que "*[o] controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares*". Logo, não é qualquer evento que cause danos (ou tenha potencial de

	causá-los) que enseja a notificação de incidente prevista na legislação de proteção de dados, mas é, na verdade, o evento que efetivamente ocasiona (ou tem a potencialidade de ocasionar) prejuízo significativo ao titular dos dados. Essa ideia não é nova no ordenamento jurídico brasileiro. Tanto a doutrina, como a jurisprudência, caracteriza como dano moral a situação sofrida de forma intensa e duradoura a ponto de violar, efetivamente, algum dos direitos da personalidade previstos no Código Civil. Nesse sentido, destaca-se recente precedente do Superior Tribunal de Justiça: > "O direito à compensação de dano moral, conforme a expressa disposição do art. 12 do CC, exsurge de condutas que ofendam direitos da personalidade (como os que se extraem, em *numerus apertus*, dos arts. 11 a 21 do CC), bens tutelados que não têm, *per se*, conteúdo patrimonial, mas extrema relevância conferida pelo ordenamento jurídico, quais sejam: higidez física e psicológica, vida, liberdade (física e de pensamento), privacidade, honra, imagem, nome, direitos morais do autor de obra intelectual. Nessa linha de intelecção, como pondera a abalizada doutrina especializada, mero dissabor, aborrecimento, mágoa, irritação ou sensibilidade exacerbada estão fora da órbita do dano moral, porquanto, além de fazerem parte da normalidade do nosso dia a dia, no trabalho, no trânsito, entre os amigos e até no ambiente familiar, tais situações não são tão intensas e duradouras, a ponto de romper o equilíbrio psicológico do indivíduo". (RECURSO ESPECIAL Nº 1.406.245, Ministro Luis Felipe Salomão, DJe 10/02/2021) Além disso, esse é o conceito que tem sido adotado por outros órgãos reguladores no Brasil. Por exemplo, o Art. 35-C, §1 da Instrução CVM 505/2011 prevê que "*o intermediário deve, tempestivamente, comunicar à SMI e aos órgãos de administração a ocorrência de incidentes relevantes que afetem seus sistemas críticos e tenham impacto significativo sobre os clientes*". Logo, no contexto da Comissão Monetária de Valores, para ser notificado, o incidente deve não só afetar sistemas críticos, como também apresentar impacto significativo aos clientes. Isso porque no dia a dia de qualquer agente de tratamento de dados, diversos eventos atípicos e não esperados podem ocorrer. No entanto, não são todos esses eventos que geram (ou podem gerar) impacto significativo na esfera de direitos de terceiro. **Logo, para que seja passível de notificação, nos termos do Art. 48 da LGPD, o incidente deve ter o condão de causar, em concreto, prejuízos intensos e duradouros de ordem patrimonial ou extrapatrimonial aos titulares de dados.**

	O risco, por sua vez, é um evento futuro e incerto que pode vir a ocasionar dano relevante aos titulares dos dados (como será detalhado na Questão 3 abaixo). Em linha do que determina o Considerando 76 da GDPR (mencionado acima), para analisar o risco de um incidente, deve-se avaliar dois fatores: a probabilidade que o evento aconteça e a gravidade do impacto, caso se materialize. Essa análise deve observar critérios objetivos, que levem em consideração a natureza, o escopo o contexto e as finalidades do tratamento. Nesse sentido, encontra-se na experiência nacional definição similar de risco. A Portaria Nº 42/2019, que estabelece a Política de Gestão de Riscos e Controles Internos (PGRCI) da Agência Nacional do Petróleo, Gás Natural e Biocombustíveis (ANP) define risco como "*evento interno ou externo cuja ocorrência possa causar impacto no cumprimento dos objetivos organizacionais; um evento de risco pode decorrer de um ou mais elementos e ter origem advinda de fontes associadas a pessoas, eventos externos, tecnologia, processos, sistemas ou infraestrutura física/organizacional, ou então ser decorrente de outro evento de risco, caracterizando um encadeamento de riscos*" (Art. 2º, X). **Assim, entende-se que a ANPD deve adotar definição similar de modo que seja notificável o incidente que cause, ou possa vir a causar, dano relevante aos titulares dos dados, observando critérios objetivos, que levem em consideração a natureza, o escopo o contexto e as finalidades do tratamento. Na mesma esteira, entende-se que a ANPD deve expressamente dispor, no regulamento do art. 48 da LGPD que, nos casos de risco baixo ou muito baixo conforme a contribuição abaixo apresentada, que se confia será acolhida, fica expressamente dispensada a notificação dos incidentes de segurança à autoridade e aos titulares de dados pessoais afetados.**
2. O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	A ocorrência de incidentes de segurança dos mais variados tipos dentro de qualquer organização não necessariamente importa em risco ou prejuízos aos titulares de dados pessoais, uma vez que há múltiplos níveis de gravidade. Um incidente de segurança pode estar associado ao comprometimento das operações do negócio, por exemplo, e não absolutamente a uma ameaça à segurança das informações. Sendo assim, entendemos que a melhor prática é que o risco ou dano relevante seja subdividido em categorias (por exemplo, muito baixo, baixo, médio, alto).

	Riscos médios e altos poderão ser considerados como "riscos relevantes" para os fins do Art. 48 da LGPD. Incidentes de segurança de muito baixo e baixo risco devem ser isentos de comunicação à ANPD e aos titulares dos dados. Especialmente os incidentes que envolvem riscos altos devem ser notificados aos titulares dos dados, conforme Questão 10 abaixo. A metodologia mais conhecida, que foi desenvolvida para a avaliação dos riscos relacionados a incidentes de segurança, é a emitida pela Agência da União Europeia para a Cibersegurança (*European Union Agency for Network and Information Security* - ENISA) chamada "Recomendações para uma metodologia de avaliação da gravidade dos incidentes de segurança" (*Recommendations for a Methodology of the Assessment of Severity of Personal Data Breaches*), que foi desenvolvida especialmente para incidentes de segurança envolvendo dados pessoais. Além disso, o GDPR (EU) menciona em seu Considerando 75 alguns exemplos de incidentes que podem causar riscos aos titulares de dados, conforme mencionado acima. Considerando os documentos acima, a experiência europeia e o estudo de incidentes no Brasil, podemos sugerir a adoção dos seguintes critérios: • **Muito baixo:** O controlador entende que os titulares dos dados não estarão sujeitos a consequências (por exemplo, incidentes com dados criptografados em que o controlador acredita que os invasores não têm capacidades técnicas para quebrar a criptografia ou vazamento de dados pseudonimizados em que a reidentificação do titular por terceiros seja razoavelmente inviável); • **Baixo:** Os titulares dos dados podem encontrar alguns inconvenientes, que serão superados sem problemas (por exemplo, necessidade de gastar tempo para reintroduzir informações no caso de perda de dados de uma plataforma, recebimento de correspondência não solicitadas (por exemplo spams), mero aborrecimento causado por informações recebidas ou solicitadas - Medo de perder o controle sobre os dados - Sensação de invasão de privacidade sem dano real ou objetivo (por exemplo, intrusão comercial), etc.); • **Médio:** Os titulares dos dados podem encontrar inconvenientes mais significativos, mas que serão capazes de superar apesar de algumas dificuldades (por exemplo, negativa de acesso a serviços, pequenas despesas extras, inadimplências de pagamento (recusa de acesso a serviços administrativos ou comerciais), perda de oportunidades de conforto (cancelamento de lazer, compras, férias, rescisão uma conta online), doenças psicológicas menores, mas

	objetivas (difamação, reputação), problemas de relacionamento com conhecidos pessoais ou profissionais (por exemplo, imagem, reputação manchada, perda de reconhecimento), etc.); • **<u>Alto</u>:** Os titulares dos dados podem enfrentar consequências significativas, que possivelmente serão capazes de superar, embora com sérias dificuldades ou mesmo irreversíveis, que podem não ultrapassar (apropriação indébita de fundos ou outras perdas financeiras, negativação indevida, danos materiais, vazamento de dados sensíveis que podem causar discriminação, perda de oportunidade de emprego, score de crédito, dificuldades financeiras como dívidas substanciais, oportunidades perdidas, direcionadas, únicas e não recorrentes (por exemplo, empréstimo residencial, recusa de estudos, estágios ou emprego) incapacidade de trabalhar, doenças físicas ou psicológicas permanentes ou de longo prazo (etc.)
3. Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	**Risco**: Considerando que os controladores devem comunicar à ANPD e aos titulares dos dados assim que tomarem conhecimento de um incidente de segurança e que, algumas vezes, não conhecem todos os elementos ou fatos do caso, entendemos que "risco" deve ser definido como "a medida ou o potencial de um evento causar danos, tanto morais como materiais". Ao avaliar um risco, deve-se levar em consideração a **probabilidade** e a **gravidade** de eventuais efeitos adversos em relação aos direitos e liberdades dos titulares dos dados. Isso significa que nem todos os incidentes de segurança comunicados causarão necessariamente danos aos titulares dos dados e, portanto, não implicarão em direito à indenização. Recomenda-se a adoção em caráter supletivo os critérios de riscos estabelecidos na ISO 31.000, que foi publicado em 13 de novembro de 2009, fornecendo um padrão internacional e maduro sobre a implementação da gestão de risco. **Danos**: consistem efetivamente nos prejuízos sofridos, ou seja, os danos materiais e morais causados pelo incidente de segurança em si. Esta definição já existe na legislação brasileira. Os danos não podem ser presumidos. Deve haver uma conexão real entre o incidente de segurança e um dano material ou moral comprovado. Existem vários precedentes favoráveis (ainda que majoritariamente de primeira instância) que estabelecem que, para causar danos morais, o incidente de segurança deve levar à violação efetiva dos direitos da personalidade (privacidade, honra, imagem, respeito à integridade mental). A mera insatisfação, aborrecimento, tristeza, irritação ou sensibilidade não seriam suficientes para ensejar direito à indenização ao titular dos dados. Citamos alguns exemplos: Processos: 9008154.75.2019.813.0024, 9008416.25.2019.813.0024 e

	9072615.90.2018.813.0024 – Juizado Especial Cível MG; e Processo nº 1067242-26.2018.8.26.0002 – TJSP
4. O que deve ser considerado na avaliação dos riscos do incidente?	As considerações abaixo tiveram como base principalmente a experiência na UE e o que já foi publicado pela ANPD. Conforme recomendado pelo WP29 em suas Orientações sobre a notificação de uma violação de dados pessoais ao abrigo do Regulamento (EU) 2016/679 e pelo EDPB em suas Diretrizes sobre Exemplos de Notificação de Incidentes de Segurança (*Guidelines on Examples regarding Data Breach Notification*), os critérios a serem levados em consideração ao avaliar os riscos são: 1. tipo de incidente de segurança (classificação em relação ao ocorrido, tal como divulgação indevida de informações, perda de dados, vazamento, quebra de confidencialidade, acesso indevido, interrupção, etc) 2. natureza e sensibilidade dos dados pessoais 3. facilidade de identificação dos titulares 4. gravidade das consequências para os titulares 5. características especiais dos titulares (incidentes envolvendo vulneráveis, como crianças ou idosos) 6. características especiais do controlador (por exemplo, controladores sujeitos a outros sigilos) 7. o número de titulares afetados e o volume de dados objeto do incidente. Ademais, além dos critérios acima, o fato de um incidente de segurança representar a violação de uma outra lei ou ato normativo (além da LGPD), também deveria ser considerado pela ANPD, ao analisar a gravidade do incidente de segurança, pois isso pode ser um indicativo de que os riscos associados ao incidente de segurança são altos (por exemplo, nos casos em que há uma violação da Lei de Sigilo Bancário - Lei Complementar nº 105/2001 ou do Código de Ética Médica).
5. Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	O Art. 48, §1º da LGPD estabelece que a comunicação a ser enviada pelo controlador deve conter, no mínimo, os seguintes elementos: (i) a descrição da natureza dos dados pessoais afetados; (ii) as informações sobre os titulares dos dados envolvidos; (iii) a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; (iv) os riscos relacionados ao incidente de segurança; (v) os motivos da demora, no caso de a

	comunicação não ter sido imediata; e (vi) as medidas que foram ou que serão adotadas pelo controlador para reverter ou mitigar os efeitos do incidente de segurança. Além disso, quando a ANPD publicou a Consulta Pública em pauta, também publicou um guia preliminar sobre incidentes de segurança, onde estabeleceu, dentre outras coisas, as informações que devem ser incluídas nas comunicações de incidentes de segurança. Na ocasião, a ANPD detalhou e expandiu a lista de informações dispostas no Art. 48, §1º, propondo que os seguintes elementos também devem constar nas comunicações: (i) data e hora da detecção do incidente; (ii) data e hora do incidente e sua duração; (iii) circunstâncias em que ocorreu a violação de segurança de dados pessoais (por exemplo, perda, roubo, cópia, vazamento, dentre outros); (iv) descrição dos dados pessoais e titulares dos dados afetados, incluindo a natureza e conteúdo dos dados pessoais, categoria e quantidade de dados e de titulares afetados; (v) resumo do incidente de segurança com dados pessoais, com indicação da localização física e os meios de armazenamento; (vi) possíveis consequências e efeitos negativos sobre os titulares dos dados afetados; (vii) medidas de segurança, técnicas e administrativas preventivas tomadas pelo controlador de acordo com a LGPD; (viii) resumo das medidas implementadas até o momento para controlar os possíveis danos; (ix) possíveis problemas de natureza transfronteiriça; (x) outras informações úteis às pessoas afetadas para proteger seus dados ou prevenir possíveis danos. **A lista de informações estabelecida pela LGPD, juntamente com os complementos propostos pela ANPD, fornece à ANPD e, quando aplicável, aos titulares de dados, um nível satisfatório de informações, que permitiriam à ANPD iniciar a investigação e, aos titulares dos dados, entender até que ponto eles foram ou podem vir a ser afetados pelo incidente de segurança. As informações que devem ser fornecidas ao titular dos dados são abordadas na Questão 7.** **No que se refere às informações sobre a data e hora do incidente de segurança e sua duração entendemos que estas deveriam ser opcionais, uma vez que, em alguns casos, a determinação dessas informações é difícil ou, até mesmo, impossível. Como exemplo, podemos citar o GDPR (UE), que não exige que tais informações sejam incluídas na comunicação.** **Além disso, solicitamos à ANPD que esclareça e forneça aos controladores mais detalhes a respeito de alguns dos itens propostos no guia mencionado, uma vez que algumas das informações exigidas são de difícil entendimento (por exemplo, "resumo do incidente de segurança, incluindo a indicação da localização física, os meios de armazenamento" e "problemas de natureza transfronteiriça").**

	Enfatizamos que, apesar da definição da lista do conteúdo que deve ser incluída em uma comunicação de incidentes de segurança, na prática, é provável que mais informações sejam fornecidas pelo controlador à ANPD no curso da investigação de incidente de segurança, desde que tais informações sejam necessárias.
6. Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	O Art. 48, §1º da LGPD prevê que os controladores devem informar à ANPD sobre o incidente de segurança em um prazo razoável, sem estabelecer (i) um prazo exato que deva ser observado; e (ii) a partir de qual momento tal prazo passa a ser contado. Ao publicar a Consulta Pública em pauta, a ANPD estabeleceu o prazo temporário de 2 (dois) dias úteis, contados a partir do momento em que o controlador tome conhecimento do incidente de segurança para que as entidades o comunicassem à ANPD. A ANPD se pronunciou sobre esse assunto com antecedência, dada a sua criticidade. O referido prazo foi proposto com base no Decreto nº 9.936/2019, que regulamenta a Lei Federal nº 12.714/11, que disciplina a formação e a consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. O Art. 18, I e §1º do Decreto determina que o gestor do banco de dados deverá comunicar a ANPD, no prazo de 2 (dois) dias úteis, em caso de incidente de segurança envolvendo dados pessoais. Para fins de referência, o Art. 33 do GDPR (UE) estabelece que os controladores devem comunicar à autoridade nacional competente sobre o incidente de segurança sem demora injustificada e, sempre que possível, em até 72 horas após ter tido conhecimento do mesmo, enquanto o Art. 26-D da Lei de Proteção de Dados Pessoais de Cingapura determina que os controladores devem comunicar à autoridade de Cingapura assim que possível, mas em no máximo 3 (três) dias corridos, após o controlador fazer a avaliação de que o incidente de segurança deve ser comunicado. **Quanto ao marco para início da contagem, assim como no GDPR (UE), parece razoável que o prazo seja contado a partir do momento em que o controlador toma conhecimento do incidente de segurança, desde que a nossa sugestão no parágrafo a seguir seja aceita pela ANPD**. Admitir outros momentos de início da contagem do prazo que dependem de elementos subjetivos – como o da Lei de Proteção de Dados Pessoais de Cingapura – possivelmente abriria espaço para muitas

	discussões sobre se o prazo foi cumprido ou não pelo controlador, caso o controlador tentasse adotar mecanismos para estendê-lo etc. **Acreditamos que também é importante que a ANPD permita que a primeira comunicação seja apresentada de forma preliminar. Isso porque, na prática, às vezes os controladores não serão capazes de reunir todas as informações solicitadas no §1º do Art. 48 da LGPD no prazo de 02 dias. As informações disponíveis no momento da comunicação dependerão das diferentes circunstâncias de cada incidente de segurança. Seria importante esclarecer que a notificação preliminar será realizada com o máximo de informações que foi possível levantar dentro do prazo de notificação.** Assim, permitir que os controladores complementem a comunicação após o prazo, é fundamental para garantir que os interesses dos titulares dos dados sejam respeitados, sem criar uma obrigação demasiado onerosa para os controladores. Entendemos que esta abordagem vai ao encontro do entendimento da ANPD, uma vez que, ao publicar a Consulta Pública em pauta, publicou também um guia preliminar sobre incidentes de segurança, no qual afirma que a comunicação deve conter uma série de informações, incluindo "*indicação se a notificação é completa ou parcial. Em caso de comunicação parcial, indicar que se trata de uma comunicação preliminar ou de uma comunicação complementar*". Além disso, no Brasil, Agência Nacional do Petróleo, Gás Natural e Biocombustíveis ("ANP") adota a ideia de uma comunicação inicial e preliminar e uma comunicação posterior com mais detalhes em caso de incidentes de petróleo. A Resolução ANP nº 44 de 22/12/2009 estabelece o procedimento para comunicação de incidentes, a ser adotado pelos concessionários e empresas autorizadas pela ANP a exercer as atividades da indústria do petróleo, do gás natural e dos biocombustíveis, bem como distribuição e revenda. Essa Resolução prevê uma comunicação faseada: (i) comunicação inicial do incidente, que deve ser imediata e (ii) relatório detalhado do incidente, apresentado em 30 dias, prorrogável mediante fundamentação técnica. Do mesmo modo, a CVM também já prevê esse modelo de comunicação faseada para incidentes de segurança cibernética, na Instrução CVM 505/2011. De acordo com esse instrumento normativo (Art. 35-I), o intermediário deve apresentar comunicação preliminar de forma tempestiva e, em um segundo momento, relatório completo. O inciso V, §1º do Art. 48 da LGPD, estabelece que a comunicação incluirá informações sobre os motivos do atraso na comunicação, quando aplicável. Isso nos leva a crer que o legislador reconheceu que, em algumas circunstâncias, o controlador não terá todas as informações necessárias para

	comunicar à ANPD, o que pode gerar demora na comunicação. No mesmo sentido, o GDPR (UE) prevê a possibilidade de uma comunicação por fases. O Considerando (85) afirma que "*Se não for possível efetuar essa comunicação no prazo de 72 horas, a comunicação deverá ser acompanhada dos motivos do atraso, podendo as informações serem fornecidas por fases sem demora injustificada*". É importante destacar que a possibilidade de comunicar a ANPD de forma preliminar é necessária e deve se estender a todos os controladores, independentemente de seu tamanho, estrutura e atividades. **Com base no exposto acima, recomendamos o prazo de até 03 (três) dias úteis para uma comunicação inicial e preliminar e aplicação de um prazo de até 30 (trinta) dias para apresentação do relatório completo, prorrogável mediante fundamentação técnica.**
7. Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	O Art. 48, §1º da LGPD prevê que os controladores devem informar à ANPD e aos titulares dos dados a respeito de qualquer incidente de segurança que possa resultar em dano ou risco relevante para o titular dos dados. A LGPD estabelece que tal comunicação deverá ser apresentada em prazo razoável, sem estabelecer (i) um prazo exato que deva ser observado; e (ii) a partir de qual momento tal prazo passa a ser contado. Além disso, ao contrário de outras leis (como o GDPR [UE] e a Lei de Proteção de Dados Pessoais de Cingapura), a LGPD (i) não reconhece a possibilidade de realizar a comunicação sobre o incidente somente à ANPD, sem notificar o titular dos dados, dependendo do caso concreto; e (ii) não prevê prazos diferentes para essas comunicações. No entanto, acreditamos que seria recomendável abordar essas comunicações de diferentes perspectivas, pois seus objetivos fundamentais são distintos**. As diferenças entre a comunicação à ANPD e a comunicação ao titular dos dados podem se dar, por exemplo, aos prazos aplicáveis, aos cenários que requerem a comunicação à ANPD, aos cenários que requerem a comunicação aos titulares dos dados e sobre qual conteúdo é relevante para o titular dos dados, entre outros.** Isso porque o objetivo da comunicação ao titular dos dados é informar sobre um incidente de segurança relevante e, também, fornecer algumas recomendações para viabilizar que o titular dos dados tome as precauções necessárias para evitar maiores riscos ou danos. Nesse sentido, a comunicação aos titulares dos dados deve contemplar informações claras sobre o incidente de segurança e as recomendações para mitigar potenciais efeitos adversos. Neste sentido, **na prática, às vezes os controladores não serão capazes de reunir todas as informações necessárias para fornecer clareza suficiente ao titular dos dados sobre o incidente de segurança com**

	recomendação dos próximos passos a serem tomados para proteger os dados dentro do prazo proposto (ou seja, 2 (dois) dias úteis contados a partir do momento em que o controlador tomou conhecimento do incidente de segurança). O fornecimento de informações genéricas e imprecisas, apenas para cumprir o prazo de 2 (dois) dias úteis, pode gerar desinformação e pânico entre os titulares dos dados, o que pode ser, na prática, mais prejudicial do que útil. Além disso, alinhamentos prévios com a ANPD podem ajudar a garantir uma comunicação adequada aos titulares dos dados. Para referência, a estreita cooperação entre o controlador e as autoridades nacionais em relação à comunicação ao titular dos dados é abordada no GDPR (UE), uma vez que se afirma que a comunicação aos titulares dos dados deverá ser efetuada logo que razoavelmente possível, em estreita cooperação com a autoridade nacional e em cumprimento das orientações fornecidas por esta ou por outras autoridades competentes, como as autoridades de aplicação da lei (*law enforcemenet authorities*) (Considerando 86). A título de exemplo, o Considerando 86 do GDPR (UE) também prevê que "*a necessidade de atenuar um risco imediato de dano exigirá uma pronta comunicação aos titulares dos dados, mas a necessidade de aplicar medidas adequadas contra incidentes de segurança recorrentes ou similares poderá justificar um período mais alargado para a comunicação*". **Dito isso, sugerimos a adoção de diferentes regimes de comunicação à ANPD e aos titulares dos dados, com prazos diferenciados**. A comunicação adequada ao titular dos dados deve ser enviada após (i) a coleta de todas as informações necessárias para fornecer um cenário claro ao titular dos dados com as medidas correspondentes a serem tomadas para proteger os dados envolvidos no incidente de segurança; e (ii) após alinhamentos prévios com a ANPD, quando necessário, que possam fornecer orientações relevantes para garantir a devida comunicação ao titular dos dados. Os itens (i) e (ii) devem ser realizados dentro de um prazo razoável. A fim de reiterar o argumento de que prazos diferentes são pertinentes, o Art. 33 do GDPR (UE) estabelece que o controlador deve, sem demora injustificada e, sempre que possível, até 72 horas após ter tomado conhecimento do mesmo, comunicar o incidente de segurança à autoridade nacional, enquanto o Art. 34 estabelece que o controlador deve comunicar ao titular dos dados sobre o incidente de segurança sem demora injustificada, mas nenhum outro prazo ou parâmetro específico é mencionado. **Portanto, o nível de informações e a definição da forma mais adequada de comunicar aos titulares dos dados são mais importantes do que o cumprimento de um prazo específico (como o de comunicar à ANPD, pelo menos preliminarmente), uma vez que qualquer**

	comunicação precipitada sem informação ou deliberação suficiente pode ser mais prejudicial do que benéfica para os titulares dos dados. Além disso, as Orientações sobre a notificação de uma violação de dados pessoais ao abrigo do Regulamento (UE) 2016/679 preveem que "(...) *O Considerando 88 [declara] que a comunicação de um incidente deve "levar em conta os legítimos interesses das autoridades de aplicação das leis nos casos em que a divulgação precoce de informações possa dificultar desnecessariamente a investigação das circunstâncias do incidente de segurança". Isso pode significar que, em determinadas circunstâncias, sempre que se justifique e mediante o aconselhamento das autoridades de aplicação das leis, o responsável pelo tratamento pode atrasar a comunicação do incidente aos titulares dos dados até que isso não prejudique essas investigações. No entanto, os titulares de dados ainda precisariam ser informados imediatamente após esse período*. " Em relação ao conteúdo da comunicação ao titular dos dados, reiteramos que as informações mais relevantes são as seguintes: (i) descrição da natureza dos dados pessoais afetados, para que o titular dos dados tenha conhecimento dos dados pessoais expostos; (ii) riscos relacionados ao incidente de segurança, de forma que o titular dos dados esteja ciente dos riscos e danos aos quais ele/ela possa estar sujeito(a) em decorrência do incidente de segurança; (iii) recomendações para mitigar potenciais efeitos adversos, a fim de permitir que o titular dos dados tome as precauções necessárias; (iv) nome e detalhes de contato do DPO ou outro ponto de contato com quem mais informações possam ser obtidas, **devendo essas serem as únicas informações obrigatórias para a comunicação com o titular dos dados**. **Isso porque o titular dos dados não precisa receber informações tão detalhadas e técnicas como a ANPD, sendo o envio de informações em excesso e demasiadamente complexas para os titulares mais prejudicial do que benéfico na prática. Neste sentido, o controlador pode ter uma discricionariedade na definição das informações a serem fornecidas de modo a dar segurança aos titulares e se comunicar de forma clara e acessível a todos, independentemente do conhecimento sobre o tema. Assim, sugerimos que as informações listadas nos itens (i) a (iv) acima sejam as únicas obrigatórias para a comunicação ao titular, devendo o controlador analisar a pertinência de incluir outras na notificação ao titular conforme o caso concreto.**
8. Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre	**A forma mais adequada de comunicar os titulares dos dados sobre o incidente de segurança pode variar, dependendo das características do caso concreto.**

direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	Entende-se que a comunicação individualizada aos titulares de dados afetados é preferível, na medida em que fornecerá aos titulares de dados informações precisas sobre como foram afetados pelo incidente de segurança, bem como sobre as medidas mitigadoras de risco já adotadas pelo controlador, e sobre aquelas medidas mitigadoras adicionais que podem ser adotadas diretamente pelo titular, por exemplo a troca de senha ou a configuração de autenticação em dois fatores. Entende-se que, via informação individualizada aos titulares de dados pessoais afetados, estes terão acesso a informações objetivas e qualificadas sobre como foram afetados pelo incidente, e medidas mitigadoras pertinentes. Além disso, a informação individualizada terá mais atenção do titular se comparada a mensagem generalista divulgada na grande mídia. Ainda nesse tocante, como a matéria objeto da presente consulta pública consiste, justamente, em incidentes de segurança envolvendo dados pessoais, na maioria dos casos o controlador dos dados objeto de incidente tem em mãos ao menos dados pessoais para contato com os titulares de dados afetados - o que lhe viabiliza enviar informe individual e qualificado aos titulares de dados afetados por determinado incidente. Nos casos em que o controlador (i) é capaz de identificar claramente a identidade de todos os titulares de dados envolvidos; e (ii) dispõe dos dados de contato de tais titulares de dados, poderia ser analisada a possibilidade da realização de uma comunicação direta. A título exemplificativo, as Orientações sobre a notificação de uma violação de dados pessoais ao abrigo do Regulamento (UE) 2016/679 estabelecem que "*exemplos de métodos de comunicação transparente incluem o envio direto de mensagens (por exemplo, e-mail, SMS, mensagem direta), banner de notificação em websites proeminentes, comunicações postais e anúncios em destaque nos meios de comunicação impressos*." **Não obstante, reconhece-se que em certas hipóteses uma comunicação direta e individualizada nem sempre será possível**. Dependendo do número de titulares de dados que foram afetados ou da relação atual entre o controlador e o titular (por exemplo, caso o incidente de segurança envolva dados pessoais de titulares de quem o controlador não possua informações de contato atualizadas), a forma mais adequada de comunicar poderá, nos casos em que inviável comunicação individual qualificada, ser uma comunicação pública por meio de *press release*, publicação na internet, dentre outros. Para referência, esta possibilidade residual (isto é, para os casos de inviabilidade ou esforço desproporcional de envio de comunicação individual qualificada) é aceita no GDPR (UE). O Art. 34 (3)c do GDPR (UE) permite a adoção de uma comunicação pública ou medida semelhante através da qual os titulares são informados de maneira igualmente eficaz nos casos em que a comunicação envolve um esforço desproporcional.

	Em síntese, a forma de comunicar o titular dos dados sobre o incidente de segurança deve ser verificada em relação ao caso concreto, podendo a ANPD estabelecer alguns critérios para orientar essa análise (como os critérios mencionados acima). Sendo preferível, sempre que viável, a realização de informação direta, individual e qualificada aos titulares de dados pessoais afetados.
9. Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	**O controlador só deve comunicar à ANPD aqueles incidentes de segurança que possam impor risco ou dano relevante ao titular dos dados,** de acordo com a metodologia e os critérios sugeridos na questão 2 (*O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?)* e na questão 12 (*Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?)*
10. Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	**Existem jurisdições (por exemplo, no contexto da GDPR) que tratam separadamente o que desencadeia a obrigação de informar a autoridade nacional e o que desencadeia a obrigação de comunicar o titular dos dados.** O Art. 33 do GDPR (UE) estabelece que o controlador deve notificar o incidente de segurança à autoridade nacional, a menos que seja improvável que o incidente de segurança resulte em risco para os direitos e liberdades dos titulares de dados. **Ou seja, o que leva ao dever de notificar à autoridade nacional é o fato de que o incidente de segurança pode gerar risco.** Por outro lado, o Art. 34 do GDPR (UE) estabelece que o titular dos dados deve ser notificado quando um incidente de segurança for suscetível a resultar em um alto risco para os direitos e liberdades dos titulares dos dados. **Isso significa que, para fins de notificação do titular dos dados, o incidente deve ter um risco maior do que um ocorrido que exige apenas notificação para a autoridade nacional. Seguindo** o parâmetro europeu descrito acima, entendemos **que devem haver algumas exceções à obrigação de informar os titulares dos dados sobre um incidente de segurança, uma vez que o titular dos dados nem sempre deve ser informado da mesma forma que a autoridade nacional.** Como o objetivo fundamental de uma comunicação ao titular dos dados deve ser fornecer informações a fim de conscientizá-lo e permitir que ele tome as medidas necessárias para mitigar os riscos relevantes, na hipótese em que o incidente de segurança ocorreu, mas que foi rapidamente

	controlado a ponto de qualquer risco ou dano ser mitigado ou, em outra ocasião, na qual é improvável que o risco ou dano se materialize, por exemplo deveriam ser tratados como exceções à obrigatoriedade de informar ao titular. Como exemplo citamos o Art. 34(3) do GDPR (UE) que isenta o controlador da obrigação de notificar o titular dos dados quando (i) o controlador implementou medidas de proteção técnica e organizacional adequadas para proteger os dados pessoais antes do incidente de segurança, em particular aquelas que tornam os dados pessoais ininteligíveis para qualquer pessoa que não esteja autorizada a acessá-los, como criptografia ou tokenização; (ii) o controlador tomou medidas subsequentes que garantem que o alto risco para os direitos e liberdades dos titulares dos dados não é mais provável de se materializar (por exemplo, o controlador identificou rapidamente o incidente de segurança e tomou medidas imediatas contra o indivíduo que acessou dados pessoais antes de ser capaz de fazer qualquer coisa com os dados em questão). A fim de reiterar o argumento de que a comunicação ao titular dos dados deve ser tratada separadamente da comunicação à ANPD, é importante destacar **que o envio de comunicações desnecessárias ao titular dos dados (por exemplo, notificação sobre um incidente de segurança que não imponha um alto risco ao titular dos dados) pode causar desinformação e pânico. Além disso, se o titular dos dados começar a receber várias comunicações do controlador sobre incidentes de segurança, pode resultar em uma "fadiga de comunicação desnecessária" (*unnecessary communication fatigue*), em que o titular dos dados pode perder a sensibilidade sobre quando tal comunicação é realmente importante. Nesse caso, os titulares dos dados podem acabar ignorando ou não entendendo quando devem adotar algumas medidas de proteção para mitigar alguns riscos relevantes.** A Legislação de Proteção de Dados Pessoais de Cingapura também reconhece a possibilidade de comunicar à autoridade nacional e não ao titular dos dados sobre um incidente de segurança. Neste caso, o Art. 5(3) da Regulação sobre Notificação de Incidente e Dados da Lei de Proteção de Dados Pessoais de Cingapura estabelece que, quando o controlador não pretende comunicar nenhum indivíduo afetado sobre um incidente de segurança que deve ser comunicado à autoridade nacional, o controlador deve especificar os motivos para não comunicar o titular dos dados. **Assim, entendemos que a melhor prática seria no sentido de que a obrigatoriedade de comunicação ao titular, à exemplo do previsto na GDPR deveria ocorrer quando um incidente de segurança for suscetível a resultar em um alto risco para os direitos e liberdades dos**

	titulares dos dados, aplicando-se, também, as exceções ao dever de informação aos titulares de dados pessoais afetados por incidente, conforme as excludentes nesse sentido previstas no artigo 34(3) da GDPR, acima descritas.
11. Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	O Art. 48, §2º da LGPD estabelece que a ANPD é responsável por apurar a gravidade do incidente de segurança. **Em linha com nossos comentários à questão 4 acima, nossos comentários se respaldam principalmente na experiência da União Europeia.** O Considerando (76) do GDPR estabelece que "*a gravidade do risco (...) deverá ser determinada por referência à natureza, âmbito, contexto e finalidades do tratamento de dados*.". Além disso, conforme recomendado pelo WP29 nas Orientações sobre a notificação de uma violação de dados pessoais ao abrigo do Regulamento (UE) 2016/679, os critérios a serem levados em consideração ao avaliar os riscos são: 1. tipo de incidente de segurança 2. natureza e sensibilidade dos dados pessoais 3. facilidade de identificação de indivíduos 4. gravidade das consequências para os indivíduos 5. características especiais do indivíduo 6. características especiais do controlador 7. o número de indivíduos afetados e o volume de dados objeto do incidente. Por fim, além dos critérios acima, o fato de um incidente de segurança também representar uma violação de outro regulamento, também deveria ser considerado pela ANPD ao analisar a gravidade do incidente de segurança, pois isso pode ser um indicativo de que os riscos associados ao incidente de segurança são altos (por exemplo, nos casos em que há uma violação da Lei de Sigilo Bancário (Lei Complementar nº 105/2001) ou do Código de Ética Médica).
12. Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	A metodologia mais conhecida, que foi desenvolvida para a avaliação dos riscos relacionados a incidentes de segurança, é a emitida pela Agência da União Europeia para a Segurança das Redes e da Informação (*European Union Agency for Network and Information Security* - ENISA), chamada

	"Recomendações para uma Metodologia de Avaliação da Gravidade dos Incidentes de Segurança" (*Recommendations for a Methodology of the Assessment of Severity of Personal Data Breaches*), que foi adaptada para incidentes de segurança envolvendo dados pessoais.
13. Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	O Art. 48, §2º, II, da LGPD estabelece que, após notificada, a ANPD poderá determinar que o controlador adote medidas para reverter ou mitigar o efeito do incidente de segurança. **Entendemos que as medidas a serem determinadas pela ANPD dependerão das circunstâncias de cada incidente de segurança.** Apresentamos alguns exemplos de medidas que podem ser impostas aos controladores com o único propósito de orientação, sendo importante enfatizar que uma lista exaustiva de medidas a serem determinadas pela ANPD não seria praticável, uma vez que não há como abordar satisfatoriamente todos os cenários possíveis que podem ser delineados na prática. Exemplos: ● Solicitar ao controlador a realização de auditorias (físicas e de TI); ● Solicitar ao controlador para implementar processos que podem limitar os danos se incidentes de segurança semelhantes ocorrerem no futuro; ● Solicitar que o controlador atualize o software e as medidas de segurança, como senhas e controles de acesso; ● Solicitar ao controlador que envolva terceiros para conduzir as medidas para mitigar os danos e conter os incidentes de segurança; ● Solicitar ao controlador que atenda melhor às condições contratuais ao envolver terceiros no tratamento de dados pessoais; ● Solicitar ao controlador para aumentar a conscientização sobre questões de proteção de dados entre colaboradores, parceiros comerciais e prestadores de serviços; ● Solicite ao controlador que tome medidas antes dos titulares dos dados (como fornecer orientações mais práticas sobre as medidas que os titulares dos dados podem adotar para proteger seus dados pessoais que foram sujeitos ao incidente de segurança); ● Fornecer serviços de monitoramento de crédito para titulares de dados afetados.
	Outro(s) problema(s) relevante(s):

	● Notificação de incidente de segurança por operador: Quando a ANPD publicou a Consulta Pública em pauta, também publicou (i) um guia preliminar sobre incidentes de segurança onde estabelecia que “embora a responsabilidade e a obrigação pela comunicação à ANPD sejam do controlador, caso excepcionalmente sejam apresentadas informações pelo operador, serão devidamente analisadas pela ANPD”; e (ii) um formulário de comunicação de incidente de segurança com um campo a ser marcado pela entidade notificadora para informar se é o controlador ou operador. O Art. 48, §1º é claro ao estabelecer que o controlador deve notificar à ANPD sobre o incidente de segurança. Nesse sentido, entendemos que a ANPD não pode estimular ou permitir que os operadores notifiquem à ANPD, pois isso seria ilegal. O controlador é a única entidade responsável pelo tratamento e capaz de avaliar a gravidade de um incidente de segurança e examinar os impactos potenciais que um incidente de segurança pode causar aos titulares dos dados.
SUGESTÃO DE NORMATIVO, SE HOUVER	
Art. Xxxx	
Art. Xxxx	

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: Armando Baltazar Palla de Medeiros

CPF/CNPJ: [redacted]

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS	
IMPORTANTE: Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	**Quais dados foram vazados (com foco nos dados produzidos pela organização), o formato em que estes dados estavam (doc, xls, pdf, txt) e a quantidade de dados vazados.**
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	**O risco deve ser dimensionado com base nas possibilidades de uso em fraudes e contratação de serviços e aquisição de produtos. Baixo: dados de relacionamento com a instituição (contas de água, luz, telefone, compras de bens de consumo e serviços geris); Médio (dados que necessitam serem completados pelo titular para a execução de fraude e dados que possam elevar os custos em contratações – ex: planos de saúde e histórico de compra de medicamentos): CPF, nome, nome de mãe, medicamentos comprados. Alto (dados que servem para validação do usuário em serviços com operações completas em meios digitais): fotos de documentos, foto pessoais, outros tipos de biometrias (servem de validação para fraudes digitais), telefone e e-mails.**
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	**O risco é a possibilidade de prejuízo ao titular provocado pelos dados vazados, o dano é a comprovação de uso dos dados para fraudes e vendas de serviços indesejados ou não solicitados.**
O que deve ser considerado na avaliação dos riscos do incidente?	**A possibilidade de uso destes dados, dividida nos seguintes grupos: fraudes, propostas de serviços e de venda de produtos, risco de sequestro (renda e endereço).**

Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	**No primeiro momento há a suspeita de vazamento de dados, a instituição precisará analisar a possibilidade do vazamento ter realmente acontecido, neste caso um prazo máximo de 10 dias e previsão para solução da falha que não deve passar de outros 10 dias, sob o risco da aplicação ficar suspensa até a efetivação das correções.**
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	**Prazo de 5 dias após a comunicação geral. Deve conter os tipos de dados vazados, nunca o conteúdo dos dados vazados (este conteúdo deve ter a iniciativa do titular coma escolha do meio em que deve ocorrer), além de ser enviada ao titular por todos os meios de comunicação disponíveis (e-mail, telefone, correio)**
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	**Os meios são: e-mail, telefone, correio. A comunicação pública deverá ser feita de forma genérica sem identificação direta do titular ou de sua região. Discordo das últimas divulgações informando a região atingida, pois quem quiser agir em determinada região terá seu trabalho de localização dos alvos facilitado.**
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	**Ao meu ver não devem haver exceções quanto a informações a ANPD, as exceções possíveis seriam relacionadas a publicidade, quando a mesma ficaria dispensada quando a quantidade de titulares atingida for pequena, sem prejuízo da comunicação aos titulares atingidos. Ex: falha identificada, porém sem comprovação de vazamento de dados (isto pode partir da própria organização ou de profissionais de TI do "bem".**
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	**Nos casos em que a empresa tenha sido alertada da falha, mas os dados não tenham efetivamente vazados.**
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	**Quantidade de titulares afetados, tipo de dados vazados, possibilidade do uso dos dados vazados, idade dos dados (dados recentes ou novos serão mais críticos).**

Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	**Sim, análise de logs das aplicações e dos acessos aos servidores de internet das organizações. As aplicações deverão ter seus logs ativados para todas as operações disponibilizadas aos usuários incluindo as consultas e emissão de relatórios. As organizações deverão manter estrutura para extração dos dados dos logs das aplicações e servidores de internet**
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	**Informar os fornecedores de serviços de segurança e de aplicativos com o qual o controlador mantém os serviços e aplicações atingidos (quando uma falha é identificada em um controlador, outros controladores poderão estar sujeitos as mesmas falhas). Isto facilitará identificar previamente problemas em outras organizações usuárias dos mesmos fornecedores que ainda não tenham relatado problemas. Desta forma a ANPD poderá ser proativa em relação as problemas relacionados, entendo que esta informação também deverá estar no Relatório de impactos.**
SUGESTÃO DE NORMATIVO, SE HOUVER	
Art. Xxxx	
Art. Xxxx	

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: ASBZ Advogados

CPF/CNPJ: 13.113.349/0001-81

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS **IMPORTANTE:** Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	Entendemos que um incidente é aquele que pode acarretar risco ou dano relevante ao titular em casos de ameaça às liberdades civis e aos direitos fundamentais do titular do dado. É possível caracterizar os incidentes baseados no impacto causado, tal como a recomendação da CNIL: um **evento** é um incidente de vazamento sem impactos; um **incidente** corresponde a um incidente com impactos isolados; um **evento danoso** é um incidente com impactos significativos e imediatos para um ou mais titulares e uma **crise** é um incidente com consequências mais duradouras e significantes para um ou mais titulares. (fonte: https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf) Com essa nomenclatura, a partir de um **evento danoso** seria possível constatar a presença de risco ou dano relevante ao titular em nosso entendimento. Na prática, alguns exemplos que podem gerar esses riscos são: incidente com (quaisquer dos) dados pessoais sensíveis, dados pessoais de vulneráveis, como crianças e adolescentes, dados financeiros que podem gerar fraudes financeiras ou dado pessoal que possa resultar em roubo de identidade. Os dados pessoais sensíveis podem causar danos muito significativos, como discriminação e segregação, devendo ser manuseados cautelosamente.
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como	Sim, entendemos que seria mais adequado e assertivo se houvesse uma subdivisão do risco ou dano relevante, tal como a proposta acima da CNIL em relação aos incidentes.

distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	Para distinguir os níveis, entendemos necessário verificar a sua natureza e a gravidade do risco/dano ao titular dos dados, o que pode ser feito de acordo com a quantidade de dados envolvidos no incidente (quanto mais dados, mais grave) e na relevância dos dados no incidente, o que resultará no entendimento do impacto. Risco baixo, por essa metodologia, deveria ser considerado não relevante.
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	O risco ao titular consiste na **probabilidade de acontecer a utilização/divulgação indevida de seus dados pessoais após um incidente de segurança**, cuja utilização/divulgação ainda não tenha se concretizado ou não seja sabida no momento da comunicação do incidente. Por exemplo, a perda de um dispositivo USB com dados pessoais não criptografados é um risco. O dano, por outro lado, advém da **concretização na probabilidade, ou seja, quando de fato é de conhecimento que o incidente teve consequências** como, por exemplo, a exposição de um CPF e eventual roubo de identidade. O dano ao titular acaba sendo algo muito mais concreto e fácil de identificar. Utilizando da responsabilidade civil – sem adentrar ao mérito de responsabilidade subjetiva ou objetiva –, quando há um dano concreto, é possível identificar os três elementos ensejadores da responsabilidade: ação/omissão, nexo causal e dano. Ao se falar de risco, este estaria muito mais relacionado ao campo da dúvida, da possibilidade. Até o momento em que não seja possível identificar um titular que efetivamente tenha sofrido consequências diretas do incidente, estaríamos diante de mero risco.
O que deve ser considerado na avaliação dos riscos do incidente?	Entendemos que a avaliação do risco ou dano porventura ocasionados aos titulares deverá ser feita caso a caso. Ao conduzir essa avaliação, devem ser levados em consideração os “riscos às liberdades civis e aos direitos fundamentais”. Para as atividades em que o relatório de impacto (RIPD) seja elaborado, os riscos nele mencionados podem servir como um ponto de início para essa avaliação. Ao avaliar um risco, a **probabilidade** e a **gravidade** dele acometer/ferir direitos e liberdades dos titulares deve ser considerada. Em seguida, o risco deve ser avaliado mediante critérios objetivos. No caso de um incidente real, o evento já ocorreu e, portanto, o foco do controlador restringe-se somente ao impacto, ou gravidade, do ponto de vista dos titulares de dados.

	Com base no histórico e na relevante importância e experiência do Working Party 29 (WP29), acreditamos que os critérios por eles estabelecidos para avaliação de risco seriam de grande contribuição para fazer a análise sugerida neste tópico, quais sejam: **1**. tipo de violação **2**. natureza, sensibilidade e volume dos dados pessoais **3**. facilidade de identificação de indivíduos **4**. gravidade das consequências para os indivíduos **5**. características especiais do indivíduo **6**. características especiais do controlador de dados **7**. o número de indivíduos afetados
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	Entendemos que podem ser de grande valia para a Autoridade, até para verificar a gravidade do incidente, ter conhecimento do **número estimado** de titulares afetados em um incidente. Além disso, pode ser válido determinar que sejam incluídos todos os **dados de contato do encarregado** do controlador que está comunicando o incidente. Por fim, acreditamos ser benéfico permitir que sejam anexadas eventuais imagens/representações gráficas da estrutura de um incidente e para explicações mais aprofundadas.
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	Entendemos como razoável o prazo corrido de 72h para a comunicação do controlador à ANPD sobre a ocorrência de incidentes de segurança após seu conhecimento. Entretanto, importante destacar que, neste primeiro momento, – até mesmo por estarmos falando do início da aplicação da lei no Brasil, de uma cultura de proteção de dados ainda em construção e, também, das diferenças socioeconômicas existentes no país, que podem influenciar no período de detecção e comunicação do incidente – nem sempre os controladores terão todas as informações necessárias sobre o ocorrido, dentro dessas 72h iniciais, pelo que um prazo adicional pode ser necessário. Assim, entendemos ser necessário dividir a comunicação em 2 momentos: ➢ No primeiro deles (dentro de 72h do conhecimento do incidente), o controlador deveria, sem prejuízo de repassar todas as informações, comunicar o que consta dos incisos I e II do art. 48, §1º da LGPD: (I) a descrição da natureza dos dados pessoais afetados e (II) as informações sobre os titulares envolvidos; ➢ Após esse prazo inicial (72h do conhecimento do incidente), o controlador, caso necessário, teria mais 5 dias corridos (ou 120h) para repassar as informações constantes dos demais incisos do

	art. 48, §1º: (III) a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial, (IV) os riscos relacionados ao incidente; (V) os motivos da demora, no caso de a comunicação não ter sido imediata; e (VI) as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo. Com esse modelo "faseado" é possível até que o controlador tenha conhecimento, após a primeira notificação, de que o incidente na verdade não ocorreu (por exemplo, o USB que se pensava perdido estava indevidamente guardado em uma gaveta que não a de origem), o que diminuiria o impacto de fornecer a integralidade de informações em um primeiro momento e direcionar esforços da ANPD para uma apuração que não se faria necessária.
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	Entendemos que a comunicação aos titulares de dados deva ser feita o quanto antes. Seguindo a recomendação anterior, em que estimamos um prazo total de 7 dias para que o controlador consiga obter todas as informações necessárias sobre o ocorrido e comunicar à ANPD, entendemos que esse mesmo prazo poderia ser aplicado no caso de comunicação aos titulares, principalmente tendo em vista que as informações a serem repassadas seriam as mesmas. Sem prejuízo, o titular deve ser informado também em até 72h sobre a detecção do incidente e que seus dados pessoais podem ter sido envolvidos em um incidente. Com relação às informações a serem repassadas aos titulares, além daquelas previstas no 48, §1º da LGPD, entendemos que o controlador deva proceder, sempre que possível e necessário, com uma recomendação ao titular de dados afetado, para mitigar potenciais efeitos adversos (por exemplo, "acesse seu perfil em nosso site e confirme/atualize seus dados" ou, ainda, "acesse seu perfil e troque sua senha" etc), além dos dados de contato do encarregado para sanar eventuais dúvidas dos titulares.
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota	O incidente de segurança deve, sempre que possível, ser comunicado **diretamente aos titulares afetados**, a menos que isso envolva um esforço altamente desproporcional, ocasião em que um comunicado na mídia – desde que com amplo alcance territorial e em, pelo menos, dois meios, visando dar publicidade ao ato – também poderá ser considerado. De toda forma, como a LGPD já deixa à discricionariedade da ANPD determinar a ampla divulgação do fato em meios de comunicação (art. 48, § 2º, I), entendemos que essa comunicação pública só deverá ser feita com o aval da ANPD.

à imprensa, publicação na internet etc.)?	Entendemos, ainda, que nos casos em que o incidente demande uma conduta do titular (por exemplo, troca de senha de acesso ou atualização cadastral), para mitigar potenciais efeitos adversos, a comunicação deve ser prioritariamente direta e individual, para que o titular consiga adotar tais medidas o quanto antes.
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	Segundo a lógica apresentada na primeira pergunta e recomendada pela CNIL para caracterizar os incidentes baseados no impacto causado, um **evento** seria a única exceção para a não obrigatoriedade de comunicação (fonte: https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf). De toda forma, acreditamos que, mesmo nesses casos, ao tornar esse tipo de notificação como opcional seria benéfico para o aculturamento da proteção de dados no Brasil e para que seja desenvolvida uma relação mais estreita entre controladores e ANPD.
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	Na mesma linha da pergunta anterior, somente o **evento** seria passível de não ser informado ao titular. Assim como no item anterior, mesmo nesses casos, consideramos que tornar esse tipo de notificação como opcional seria benéfico.
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	Entendemos que a ANPD deva levar em conta os tipos de dados envolvidos no incidente de segurança e a projeção do impacto imediatamente sentido pelos titulares de dados envolvidos. Ainda, importante verificar se a empresa envolvida tem, de fato, uma cultura de proteção de dados enraizada (com políticas, treinamentos, etc.) ou se os esforços para adequação à legislação foram mínimos. Caso sejam constatados que foram mínimos, é possível se presumir que a empresa não teve preocupação em atender nem mesmo aos princípios da legislação, tais como a finalidade, necessidade, segurança e prevenção, o que automaticamente aumenta a gravidade do incidente.
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	As Autoridades de Proteção de Dados da Grécia e da Alemanha, em colaboração com a ENISA, desenvolveram uma metodologia para avaliação da gravidade dos incidentes de segurança violação de dados. O documento afirma que os principais critérios para análise da gravidade de uma violação de dados pessoais seriam: a) Data Processing Context (DPC) - Contexto do tratamento de dados pessoais: consiste na análise dos tipos de dados envolvidos no incidente (devendo ser classificados em uma das seguintes categorias: dados pessoais, dados referentes a comportamento (comportamentais), dados financeiros e dados pessoais sensíveis); b) Ease of Identification (EI) - Facilidade de identificação dos titulares que tiveram seus dados envolvidos no incidente (aqui seria importante analisar se os dados identificam diretamente o indivíduo ou se o torna identificável, necessitando do complemento de outros dados); c) Circumstances of breach (CB) - Circunstâncias específicas do incidente, incluindo a perda de segurança dos dados violados (confidencialidade, integridade e disponibilidade).

	Fonte: https://www.enisa.europa.eu/publications/dbn-severity O Working Party 29, por sua vez, na Guideline WP 250, sugere a seguinte metodologia: a) Identificação do tipo de violação: uma divulgação de informações médicas para terceiros não autorizados e uma perda de informações médicas, por exemplo, tem consequências diversas; b) Natureza, sensibilidade e volume dos dados pessoais: os dados envolvidos são sensíveis ou "comuns"? os dados podem causar algum risco físico ou financeiro ao titular (exemplo: endereço de casa, extrato de rendimentos)? c) Facilidade de identificação de pessoas únicas: quão fácil será para um terceiro que tenha acesso aos dados identificar pessoas específicas ou combinar os dados com outras informações para identificar pessoais? Quanto mais simples for a identificação, maior será a gravidade; d) Gravidade das consequências para as pessoas: deve se ter em conta a permanência das consequências para as pessoas; e) Características especiais das pessoas únicas: um incidente envolvendo dados relativos a crianças ou vulneráveis tem maior gravidade; f) Características especiais do responsável por tratamento: por exemplo, se a envolvida for uma organização médica, existe uma maior ameaça para os titulares em comparação a um mailing list; e g) Número de pessoas afetadas: quanto mais pessoas estão sendo afetadas, maior é a gravidade. Fonte: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	Entendemos que é de extrema importância que, além de a empresa controladora adotar medidas adicionais de segurança para proteção de dados pessoais, deva também realizar ou apoiar campanhas públicas de conscientização sobre melhores práticas para privacidade, ajudando na conscientização de outras empresas e também dos cidadãos.

SUGESTÃO DE NORMATIVO, SE HOUVER
Art. Xxxx ....
Art. Xxxx ....

Oficio_nº010_2021 Brasília, DF, 24 de março de 2021.

Ao Senhor
WALDEMAR GONÇALVES ORTUNHO JUNIOR
Diretor-Presidente da Autoridade Nacional de Proteção de Dados (ANPD) da Presidência da República

Ref.: Tomada de Subsídios ANPD nº 02/2021 - Regulamentação da aplicação da LGPD

Prezado Senhor,

Observando a publicação da Tomada de Subsídios ANPD/PR nº 2/2021, a **Federação das Associações das Empresas Brasileiras de Tecnologia da Informação – FEDERAÇÃO ASSESPRO** apresenta a seguir suas considerações quanto à regulamentação da comunicação de incidentes de segurança, especialmente com foco no prazo para tais comunicações.

Da comunicação de incidentes de segurança

O art. 48, parágrafo 1º da LGPD atribui ao controlador a obrigação de comunicar à ANPD e aos titulares a ocorrência de incidente de segurança que possa acarretar risco ao dano relevante.

A orientação preliminar dada pela ANPD foi no sentido de recomendar que tais comunicações sejam feitas no prazo de até 2 dias úteis, em conformidades com as informações disponibilizadas no sítio eletrônico da entidade.[1] Tal prazo foi fixado levando em consideração o disposto no Decreto nº 9936/2019, que trata especificamente sobre bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito.

Sugerimos que a ANPD reavalie o referido prazo, que nos parece muito curto para a realidade brasileira na qual, infelizmente, a cultura de proteção de dados ainda não está devidamente enraizada na grande maioria das empresas e o nível geral de maturidade em segurança da informação é relativamente baixo.

Cabe lembrar que o artigo 33 do RGPD (Regulamento Geral de Proteção de Dados), aplicável na União Europeia, prevê o prazo de 72 horas para a realização da notificação de incidentes de segurança. E mesmo no bloco europeu, que possui uma longa tradição de proteção de dados, as organizações ainda enfrentam dificuldades em cumprir tal prazo. Uma pesquisa junto ao sítio eletrônico https://www.enforcementtracker.com/ revela que pelo menos 4% de todos as multas já aplicadas no âmbito do RGDP referem-se ao descumprimento do prazo de notificação obrigatória.

[1] https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca

[redacted]

Nesse sentido, sugerimos que a ANPD avalie:

(i) a revisão do prazo de 2 dias úteis constante de suas orientações preliminares; ou

(ii) estabelecer um prazo diferenciado em favor de empresas de menor porte.

Sendo o que se apresentava, despedimo-nos reforçando a nossa disponibilidade de contribuir com a construção de arcabouço regulatório adequado para o desenvolvimento ecossistema digital brasileiro baseado em dados.

Respeitosamente,

ITALO NOGUEIRA
Presidente FEDERAÇÃO ASSESPRO

A Federação Assespro

A ASSESPRO é uma entidade sem fins lucrativos, regida por seus Estatutos Sociais, criada com o intuito de representar de forma distinta e empreendedora, empresas privadas nacionais produtoras e desenvolvedoras de software, produtos e serviços de tecnologia da informação, telecomunicações e internet. Fundada em 1976, a ASSESPRO é a legítima e a mais antiga entidade empresarial do Setor. Ao longo dessas quatro décadas, a entidade vem defendendo os interesses das empresas nacionais e a indústria nacional de TI.

Hoje com mais de 2.500 empresas associadas e conveniadas por meio de suas 13 entidades regionais, a ASSESPRO assume cada vez mais esta posição de representante do setor junto aos governos municipais, estaduais e Federal, junto a sociedade, e também perante as instituições de ensino, com o objetivo de integrar a comunidade acadêmica com a empresarial e contribuir para formação de pessoal capacitado para as demandas do mercado.

[redacted]

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: AUDITSAFE AUDITORIA E CONSULTORIA EM RISCOS CORPORATIVOS LTDA.

CPF/CNPJ: 07.698.985/0001-10

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS **IMPORTANTE:** Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	**Considerações AuditSafe**: Avaliar riscos de médio e alto impacto que possam acarretar danos graves aos titulares, não deixando de avaliar as medidas protetivas e controles que possam mitigar os riscos de baixo impacto, mas que fazem parte da gestão de riscos da controladora ou operadora.
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	**Considerações AuditSafe :** I – Risco Improvável (Não relevante) – improvável que a violação resulte em risco - para os direitos e liberdades das pessoas singulares. Baixo Risco - a notificação da violação não é obrigatória. II- Risco Possível - que a violação possa resultar em danos físicos, materiais ou não materiais - às pessoas. Médio Risco - a notificação à autoridade supervisora é obrigatória. III – Risco Provável - que a violação provavelmente resultará em um alto risco para os direitos e liberdades dos indivíduos. (Provável materialização do risco). – Alto Risco - a notificação à autoridade supervisora é obrigatória.
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	**Considerações AuditSafe:** O Risco é uma combinação de probabilidade e o impacto do incidente. O dano é quando o incidente ou vulnerabilidade mapeado como risco, de fato acontece, gerando a violação e/ou o prejuízo. Nesse sentido, torna-se fundamental que o Relatório de análise de impacto esteja contemplando um conjunto de informações da controladora ou processadora sobre os riscos,

	planos de resposta a incidentes, planos de recuperação ao dano, controles já existentes e análises dos riscos que a organização mapeou como médios e altos.
O que deve ser considerado na avaliação dos riscos do incidente?	**Considerações AuditSafe:** Descrição do risco, probabilidade, impacto, criticidade ou classificação do risco, vulnerabilidade, ameaça, controles aplicados para mitigar os riscos, risco residual, responsáveis, o ativo impactado.
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	**Considerações AuditSafe:** Notificações de fornecedores ou parceiros que não estão em conformidade com a Lei e não se comprometem a auxiliar e informar sobre o tratamento / ciclo de vida dos dados do controlador.
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	**Considerações AuditSafe:** Obter um critério dependendo da gravidade a ser estabelecido pela ANPD. Possivelmente em até 10 dias, devido a urgência do incidente e violação dos dados pessoais. Entendemos um prazo razoável para conseguir contato, levantamento de informações, análise dos fatos, disponibilidade dos recursos e elaboração da notificação. Considerar análise quanto ao prazo de 72 horas (3 dias), definido pela GDPR em seu Artigo 33º, Notificação de uma violação de dados pessoais à autoridade de controle. Neste caso, o prazo passaria a contar, após o controlador ter tido conhecimento do vazamento.
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	**Considerações AuditSafe:** Obter um critério dependendo da violação ou dano ao titular estabelecido pela ANPD. Considerar análise quanto ao prazo de 5 dias para que os controladores informem os titulares de dados sobre o vazamento de dados, considerando que a comunicação deve ser realizada a partir do momento em que o controlador identifique que o incidente pode causar prejuízos ao titular dos dados. As informações constantes para comunicação devem ser suficientes.
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	**Considerações AuditSafe:** Entende-se que a forma direta e individual é sempre adequada. Depende da gravidade do dano ao titular associado à preservação da confidencialidade das informações ou dados pessoais. Considerar análise quanto à forma direta e individual, podendo ser que por e-mail seria a melhor forma. A depender do incidente, considerando o volume de dados vazados e nível de impacto junto aos titulares, entende-se como uma boa prática o controlador se retratar publicamente.

Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	**Considerações AuditSafe:** Riscos e/ou Danos improváveis e não relevantes aos direitos e/ou liberdade dos titulares de dados pessoais.
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	**Considerações AuditSafe:** Riscos e/ou Danos improváveis e não relevantes aos direitos e/ou liberdade dos titulares de dados pessoais.
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	**Considerações AuditSafe:** Podemos citar a ISO 27005 e 27002 como base dos riscos de segurança e os possíveis controles de segurança. Podemos citar a estrutura de riscos (matriz e análises de riscos) da controladora e da operadora. Podemos citar outras bases legais dependendo do negócio da controladora que possam interferir nas análises e avaliações de proteção de dados e dos titulares. Risco de imagem, reputação, vida ou prejuízo financeiro dos titulares dos dados, devido ao incidente de segurança.
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	**Considerações AuditSafe:** Como a gravidade do incidente está associada com o core business das empresas, gestão dos riscos e com os requisitos legais, podemos citar a ISO 31000 para uma gestão de riscos adequada, assim como a ISO 27005.
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	**Considerações AuditSafe:** Para as medidas técnicas e administrativas citamos os Sistemas de Gestão da ABNT/ IEC - ISO 27005, 27001, 27701, além de outras melhores práticas internacionais como NIST, PCI, que contemplam controles necessários para mitigar os riscos de segurança da informação e proteção de dados pessoais.
Tópico AuditSafe: No caso incidente relacionado a dados pessoais de criança ou adolescente, quais seriam as orientações quanto à comunicação a ser enviada ao titular? Deve ser efetuado algum tipo de comunicação diferenciada?	**Considerações AuditSafe:** Caso o controlador tenha os dados do responsável legal, o comunicado poderia seguir ao mesmo. No caso desta inexistência, deveria ser avaliado comunicado geral por meio público.
Tópico AuditSafe: Quais seriam as orientações quanto à comunicação aos titulares, afetados por incidente, quando em parte do cadastro não constar endereço eletrônico (e-mail) ou	**Considerações AuditSafe:** Considerar que, de acordo com a gravidade do incidentes, deve-se haver esforço do controlador em que o titular receba a comunicação para estar prevenido de ocorrências, tais como consequentes de um vazamento de dados sensíveis.

endereço de correspondência? O Controlador deve enviar comunicado individual apenas aos que possuem algum endereço? Ou o Controlador pode optar por enviar um comunicado único em meios públicos?	
SUGESTÃO DE NORMATIVO, SE HOUVER	
Art. Xxxx	
Art. Xxxx	

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: Grupo Financeiro BMG

CPF/CNPJ: 61.186.680/0001-74

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS	
IMPORTANTE: Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	Um incidente poderá acarretar risco ou dano relevante ao titular quando houver limitação, perda de controle sobre seus dados pessoais, a limitação de seus direitos, incidência de discriminação, fraudes ocasionadas através da utilização indevida dos dados pessoais, perdas financeiras, ou qualquer outra desvantagem econômica ou social significativa para os titulares.
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	Incidentes devem ser comunicados a menos que não resultem em risco aos direitos dos titulares, levando em consideração o tipo de incidente, a natureza, sensibilidade e volume de dados pessoais envolvidos no incidente. O que os dados potencialmente podem revelar sobre o indivíduo também deve ser considerado. Riscos ou danos baixos devem ser considerados irrelevantes, se após análise acurada houver a conclusão de pouca probabilidade em resultar prejuízos ao titular.
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	O risco e dano ao titular se relacionam na medida em que a análise do risco deve ser realizada previamente ao tratamento, considerando todos os princípios da lei e da natureza dos dados pessoais e finalidade pretendida. O dano torna-se evidente quando o incidente expõe a proteção da vida do titular.
O que deve ser considerado na avaliação dos riscos do incidente?	Tipo de incidente, natureza e sensibilidade dos dados pessoais, facilidade para identificar os indivíduos à partir dos dados comprometidos, severidade das consequências para os titulares, se há indivíduos vulneráveis (ex; crianças) a natureza e o papel do Controlador e de suas atividades (ex. um hospital que trata grande volume de dados sensíveis), o número de indivíduos envolvidos no incidente

Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	Contato do DPO ou outro contato que possa fornecer outras informações sobre o incidente, descrição das prováveis consequências do incidente.
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	Em até 72 horas após a ciência do incidente, se factível. (Controlador possuir um razoável indício que o incidente de segurança ocorreu)
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	O titular deve ser comunicado o mais rápido possível e em prazo razoável após o conhecimento do incidente de segurança, em até 72 horas após comunicar à ANPD, se necessário for. Devem ser informados sobre a natureza do incidente de segurança envolvendo dados pessoais, e ao menos os contatos do DPO ou pessoa que possa informar sobre o ocorrido, a descrição das prováveis consequências, descrição das medidas adotadas ou propostas para enfrentar o incidente,
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	A comunicação deve ser feita em linguagem acessível e clara aos titulares, através de mensagens diretas para esse fim, tais como SMS, e-mail, site ou meio de comunicação conhecido e amplo. A comunicação feita apenas em sites/blogs corporativos ou apenas em nota à imprensa pode não ser muito efetiva.
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	Incidentes envolvendo dados pessoais criptografados e de provável impossibilidade de uso (ex. backup de arquivo criptografado armazenado em uma chave USB que é roubado), Incidentes que apontam baixo risco para o titular, após realização de avaliação de impacto.
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	Comprovação que o Controlador implementou medidas técnicas para mitigar o risco (ex. criptografia), adoção de medidas para garantir a não materialização de riscos altos ao titular, esforço desproporcional para comunicar a cada titular individualmente (ex. vazamentos em massa)
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	Volumetria dos dados pessoais tratados, sensibilidade dos dados, medidas técnicas adotadas previamente para mitigar o risco de ocorrência de incidentes, escopo do tratamento de dados.

Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	Verificar se a organização elaborou os documentos necessários (ex. Data mapping, Avaliação de legítimo interesse, DPIA se aplicável) avaliação se as medidas técnicas foram implementadas (ex. backup, criptografia, atualização de sistemas, dois fatores de autenticação, controle rígido de acessos, auditorias sistemáticas)
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	Avaliação do impacto para o titular e dosimetria das sanções previstas na LGPD proporcionais ao dano causado.
SUGESTÃO DE NORMATIVO, SE HOUVER	
Recital 85, GDPR	
Article 29 - Guidelines on Personal data breach notification	
Artigo 33, GDPR.	
Artigo 34, GDPR.	
Guide to data protection – personal data breaches - ICO	
Artigo 33 (2), GDPR.	
Artigo 24, GDPR	

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: Baptista Luz Advogados

AUTORES: Fernando Bousso; Odélio Porto Júnior; Matheus Botsman Kasputis; Rafaela Marcondes Sobrinho; Adriane Loureiro Novaes.

CPF/CNPJ: 07.007.640/0001-72

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS

IMPORTANTE: Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.

TÓPICO/QUESTÃO	CONTRIBUIÇÃO/INSTITUIÇÃO
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	**1. Considerações Iniciais** **1.1. Definição de Incidente de Segurança de Informação** Antes de se analisar os riscos e danos acarretados por um incidente, é importante que a ANPD estabeleça a definição de "*incidente de segurança da informação*" que a agência utilizará. A área da ciência da computação apresenta definições variadas sobre o que seria um incidente de segurança da informação. Uma das definições tradicionais da área é a tríade de princípios "CIA" que define segurança da informação como sendo a preservação da (**i**) confidencialidade, (**ii**) disponibilidade e (**iii**) integridade da informação. Esta é, inclusive, a definição utilizada pela ISO 27000 sobre sistemas de gestão de incidentes de segurança da informação.[1] A redação do artigo 46 da LGPD, apesar de não citar diretamente os princípios da CIA, define indiretamente o conceito de incidente de segurança da informação com um conceito derivado desses princípios[2], na medida em

[1] "3.28 information security: preservation of confidentiality (3.10), integrity (3.36) and availability (3.7) of information". THE INTERNATIONAL ORGANIZATION FOR STANDARDIZATION (ISO**). ISO/IEC 27000:2018(E)**. 2018. p.4.

[2] "Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito". Lei Geral de Proteção de Dados (LGPD) – Lei nº 13.709/2018.

	que as ações listadas no artigo 46 remetem à violação de um ou mais dos princípios da tríade. Por exemplo, a destruição ilícita de um dado afeta a sua disponibilidade e integridade; já um acesso indevido com publicação não autorizada afeta a confidencialidade da informação. Também nesse sentido, a definição de "segurança da informação" do NIST estadunidense - agência governamental não regulatória para promoção da inovação tecnológica – utiliza ambos os elementos destacados acima na sua definição, qual seja: "*a proteção da informação e dos sistemas de informação contra acesso não autorizado, uso, divulgação, interrupção, modificação ou destruição, a fim de garantir a confidencialidade, integridade e disponibilidade*"[3]. / Recomendação Portanto, é recomendável que a ANPD esclareça quais pressupostos serão utilizados para definir e analisar um incidente de segurança da informação, o que pode ser feito, por exemplo, por meio de materiais orientativos e normas administrativas. 1.2. Fundamentos para a Compreensão de um Incidente Devemos considerar como premissa fundamental para o debate deste tema que não existem sistemas que sejam absolutamente seguros – o que não implica dizer que medidas proporcionais de segurança devam deixar ser adotadas. Este fundamento decorre da própria natureza das tecnologias e de sua implementação, sendo de fácil verificação que diversas organizações ao redor do globo - sejam multinacionais, Estados ou organizações da sociedade civil, de tamanhos e capacidade financeira distintas - já foram atingidas por diferentes tipos de incidentes de segurança da informação.

[3] "The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability." ESTADOS UNIDOS. National Institute of Standards and Technology (NIST). **Computer Security Resource Center – Glossary**. Acesso em: 15/03/2021. Disponível em: <https://bit.ly/3eI8eek>

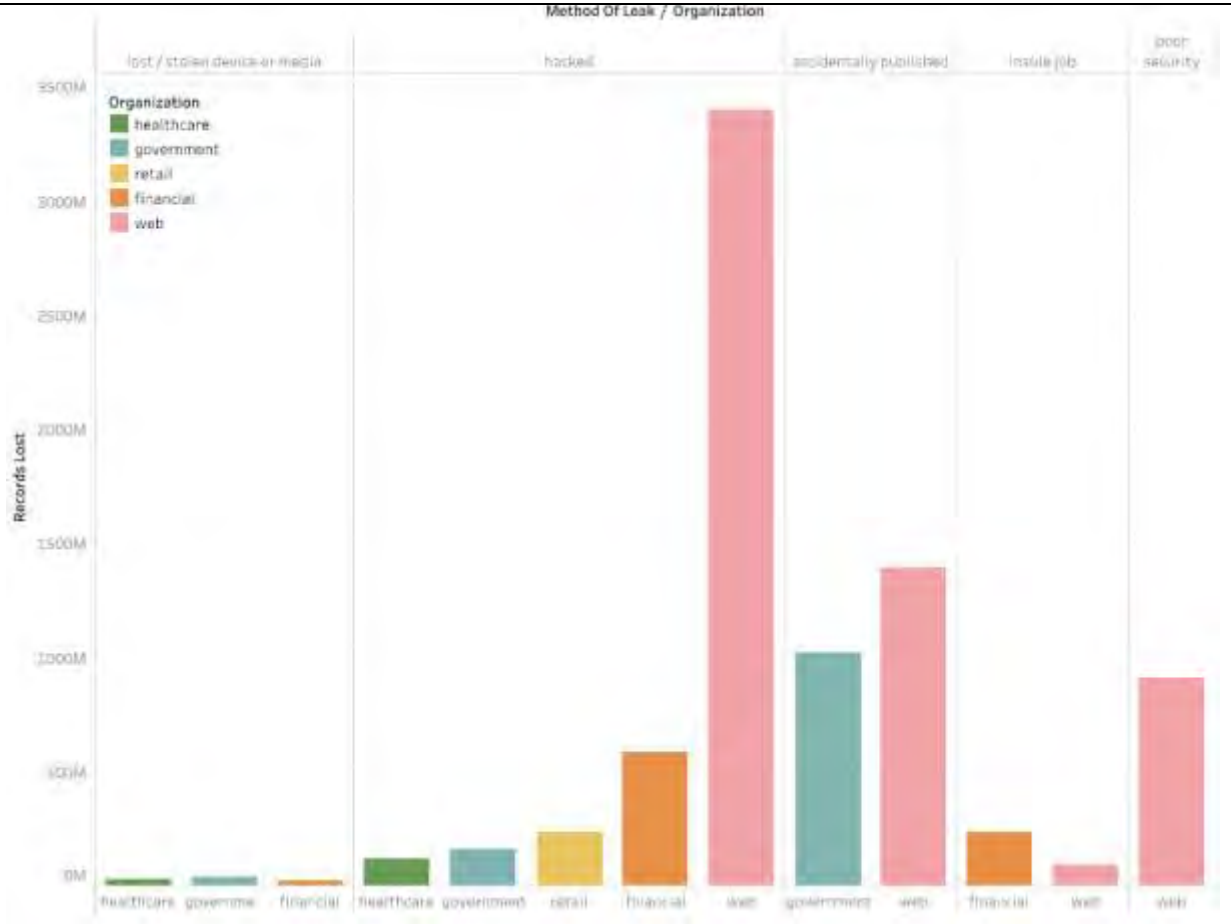


Fig. 1 - O número de dados afetados por tipo de incidente e organização, entre 2004 e 2017, da base de dados World's Biggest Data Breaches.[4]

As técnicas de invasão a sistemas de informação são caracterizadas pelo seu desenvolvimento constante; sendo utilizadas por uma gama de agentes distintos, sejam Estados-Nação, organizações criminosas ou mesmo indivíduos, e por motivos diversos (p. ex. ganho econômico, exposição do alvo, motivações pessoais etc.).[5] Assim, a capacidade de previsão de risco de incidentes é dificultada de forma expressiva por essas características, o que deve ser levado em consideração pela ANPD.

[4] LIU, Liyuan; HAN, Meng; WANG, Yan; ZHOU, Yiyun. **Understanding Data Breach: A Visualization Aspect**. Conference: The 13rd International Conference on Wireless Algorithms, Systems, and Applications. 2018. p. 887. Acesso em: 16/03/2021. Disponível em: <https://bit.ly/2No2Qlf>.
[5] UNIÃO EUROPEIA. European Union Agency for CyberSecurity (ENISA).

É necessário que os incidentes sejam analisados tendo como base a sua natureza complexa. Nesse sentido, após analisar técnica e juridicamente uma série de casos de incidentes de segurança da informação, incluindo os respectivos litígios e processos administrativos que se seguiram, a pesquisadora sobre o tema Josephine Wolff esclarece que:

> "Diferentes tipos de organizações - de desenvolvedores de software a administradores de sistemas e formuladores de políticas públicas - são capazes de influenciar e intervir apenas em diferentes estágios de um incidente de segurança da informação. O fato de que cada defensor individual possui um escopo limitado de atuação é crucial para entender quais responsabilidades de segurança da informação eles podem razoavelmente e realisticamente assumir.
>
> Quando analisamos (e relatamos ou litigamos) incidentes de segurança que obtiveram êxito, muitas vezes nossa inclinação é agarrar-se ao primeiro ponto de acesso [de um hacker] ou ao ponto de acesso mais fácil de ser compreendido (p. ex. o e-mail de phishing [...] a rede sem fio desprotegida), e insistir que a simples defesa desse único ponto teria feito toda a diferença (p. ex. autenticação de dois fatores ou limitação de tentativas de logins [...]).
>
> Mas essa perspectiva simplifica demasiadamente a realidade muito mais complexa de que um incidente de segurança se desenvolve de forma gradual e crescente; bem como ofusca as ações de defesa limitadas e o ambiente desafiador em que os defensores individuais de um ataque operam na prática." (JOSEPHINE WOLFF, 2018, tradução nossa)[6]

/ Recomendação

Desse modo, é recomendável que a ANPD busque preparar seu corpo técnico a fim de ter a real dimensão da complexidade que envolve a investigação e entendimento de um incidente de segurança da informação. Principalmente para que a atribuição de responsabilidades seja feita de forma proporcional, e seja fomentado um ambiente de cooperação entre os agentes de tratamento e a ANPD. A complexidade técnica dos incidentes exige tal ação conjunta para se evitar e mitigar os danos aos titulares.

* * * *

[6] "*Different types of organizations and defenders – from software developers to system administrators to policymakers – are able to influence and intervene at very different stages of security breaches. Each individual defender limited scope of control that is crucial for understanding which defensive responsibilities they can reasonably and realistically be expected to assume. When we talk about (and report on and litigate) successful security incidents, too often our inclination is to latch onto the first or the most easily understood point of access – the phishing email […] the unprotected wireless network – and harp on the simple line defense that seems like it would have made all the difference – two factor authentication, or rate limiting logins […] But that perspective oversimplifies the much more complicated narrative of the gradual, escalating capabilities acquired by perpetrators, as well the much more limited and challenging environment in which individual defenders operate*". WOLFF, Josephine. **You'll See This Message When It Is Too Late - The Legal and Economic Aftermath of Cybersecurity Breaches**. 1ª edição (versão Kindle): The MIT Press. 2018. Capítulo 1, Loc 470 de 6938.

2. Definição de Risco e Dano

Neste tópico será feito uma síntese sobre o conceito de risco conforme ele tem sido utilizado e debatido na União Europeia, em relação à GDPR; e nos EUA (abordado no item 4). A partir desses subsídios são feitas algumas ponderações sobre como a ANPD pode tomar como base os cenários estrangeiros para a regulação no Brasil.

2.1. União Europeia

2.1.1. Risco

A GDPR define risco ao titular por meio de conceitos amplos e pela utilização de alguns exemplos no texto legal. O Considerando (75) da lei estabelece que há risco quando as operações de tratamento forem "*suscetíveis de causar danos físicos, materiais ou imateriais*", citando como como exemplos àqueles que puderem ocasionar:

i) Discriminação;
ii) Roubo da identidade;
iii) Perdas financeiras;
iv) Dano à reputação,
v) Perda de confidencialidade de dados protegidos por sigilo profissional;
vi) Reversão da pseudonimização;
vii) Prejuízos econômicos ou sociais; e
viii) Privação de direitos, liberdades, e do controle sobre os dados.

Também poderá haver risco quando o tratamento envolver dados sensíveis[7]; dados relacionados a aspectos de natureza pessoal (p. ex. desempenho no trabalho, situação econômica, saúde, interesses pessoais, confiabilidade, comportamentos, localização e deslocamentos, a fim de se fazer uso de perfis); dados pessoais de vulneráveis, em particular crianças; e quando houver o tratamento de grande quantidade de dados pessoais que afetem muitos titulares.

Já o Considerando (76) da GDPR esclarece que os riscos aos titulares devem ser avaliados em relação à (i) probabilidade de ocorrerem e (ii) gravidade do risco gerado; considerando a natureza, escopo, contexto e finalidade da atividade tratamento.[8]

[7] Artigo 9º, GDPR: "origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, ou a filiação sindical, bem como o tratamento de dados genéticos, dados biométricos para identificar uma pessoa de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou orientação sexual de uma pessoa."
[8] Considerando (76), GDPR: "A probabilidade e a gravidade dos riscos para os direitos e liberdades do titular dos dados deverá ser determinada por referência à natureza, âmbito, contexto e finalidades do tratamento de dados. Os riscos deverão ser aferidos com base numa avaliação objetiva, que determine se as operações de tratamento de dados implicam risco ou risco elevado."

	Em 2017 a Working Party 29 (WP29)[9] elaborou um guia geral de orientações sobre notificações de incidentes de segurança da informação.[10] [11] O documento busca orientar de forma mais concreta como deve ser feita a análise de risco para verificar a necessidade de notificação; explicando em mais detalhes certos critérios legais, e utilizando casos exemplificativos. Nesse sentido, a WP29 lista os seguintes critérios em adição ao estabelecido na Diretiva 95/46 (substituída pela GDPR):[12] i) Tipo de incidente Este item não é muito desenvolvido no guia, sendo utilizado apenas alguns exemplos com base na tríade de princípios CIA. Assim, uma violação da confidencialidade de dados de saúde, a princípio, ofereceria maiores riscos em relação a mera perda dos mesmos. ii) Natureza, sensibilidade e volume dos dados Além de avaliar o tipo de dado (p. ex. dados financeiros, de saúde etc.), o agente deve também considerar como os dados afetados pelo incidente podem ser combinados com outros e o possível dano resultante da combinação. Por fim, a WP29 alerta para o fato de que o fator volume de dados não pode ser analisado isoladamente, pois poucos dados sensíveis podem acarretar um nível alto de dano ao titular. iii) Facilidade de identificação dos titulares Além de verificar o grau de facilidade de se identificarem os titulares pelos dados afetados, o agente de tratamento também deve considerar como esses dados podem ser combinados com outros (p. ex. dados publicamente disponíveis) para permitir a identificação; e verificar se os dados afetados estavam criptografados de forma adequada. iv) Gravidade das consequências Apesar deste critério já estar elencando na GDPR, o Guia da WP29 cita alguns exemplos práticos. Ela esclarece que o agente de tratamento deve considerar se os danos aos titulares podem ter um caráter permanente ou de longo prazo. É importante destacar que a entidade considera que apresentam baixo risco os casos em que os dados são indevidamente compartilhados com fornecedores/parceiros. v) Características dos titulares

[9] A Working Party 29 era uma entidade pública consultiva da União Europeia, formada por representantes das autoridades de proteção de dados de cada um dos membros da EU. Com a entrada em vigor da GDPR ela foi substituída pela European Data Protection Board (EDPB).
[10] O guia da WP29 sobre notificação de incidentes de segurança da informação foi ratificado pela European Data Protection Board (EDPB). Ver: ARTICLE 29 DATA PROTECTION WORKING PARTY. **Guidelines on Personal data breach notification under Regulation 2016/679**. 18/EN - WP250 rev.01. 2018. p.23. Acesso em 17/03/2021. Disponível em: <https://bit.ly/30SnhtO>
[11] Este guia foi posteriormente revalidado pela European Data Protection Board.
[12] *Ibid*. pp 24-26.

O guia apenas destaca que determinados indivíduos possuem características pessoais que podem potencializar os riscos de um incidente, como no caso de crianças.

vi) Características do controlador
O guia apenas destaca que, a depender da natureza das atividades do agente de tratamento, pode haver automaticamente um risco maior no incidente, como no caso de instituições de saúde.

vii) Quantidade de indivíduos afetados
A WP 29 apenas alerta para o fato de que, geralmente, quanto maior o número de titulares maior o risco, mas que também poucos ou apenas um indivíduo pode ser afetado de forma grave.

Apesar das orientações elaboradas pela antiga WP29, a European Data Proctection Board (EDPB) considerou que, mesmo sendo ainda válidas, elas seriam insuficientes para orientar os agentes de tratamento de forma mais concreta. Assim, em 2021 foi lançando uma versão prévia para consulta pública de um guia de notificação de incidentes baseado em casos práticos específicos (p. ex. ransomware, exfiltração de dados, roubo de equipamentos, etc).[13] A par disso, pode-se inferir que a EDPB reconhece que a GDPR apenas fornece critérios abstratos para avaliação dos riscos gerados por um incidente, sendo necessário que os reguladores intervenham com orientações de cunho mais prático aos agentes de tratamento.

Adicionalmente, a WP29 esclarece que a definição da análise de risco de um incidente pode ser mais bem compreendida quando comparada à análise de risco feita em um Relatório de Impacto à Proteção de Dados[14] (*Data Protection Impact Assessment* - DPIA). Em relação a diferença entre uma análise de risco de incidente (para notificação) e um DPIA, a WP29 esclarece que a avaliação de um incidente se aplica apenas depois que ele ocorreu, enquanto em um DPIA são analisados cenários hipotéticos sobre os diferentes riscos acarretados pelo tratamento, incluindo, mas não se limitando a incidentes de segurança.

2.1.2. Dano
O texto legal da GDPR não define parâmetros específicos para análise do dano ao titular. Os trechos que tratam de dano, apenas mencionam alguns fatos decorridos de um incidente de segurança que podem gerar dano aos titulares, sejam eles físicos, materiais ou imateriais (p. ex. roubo de identidade, fraude, dano à reputação etc.) - conforme já listados neste documento (ver item 2.1.1).[15]

[13] "However, due to its nature and timing, this guideline did not address all practical issues in sufficient detail. Therefore, the need has arisen for a practice-oriented, case-based guidance that utilizes the experiences gained by Supervisory Authorities since the GDPR is applicable". UNIÃO EUROPEIA. Draft: **Guidelines 01/2021 on Examples regarding Data Breach Notification**. Acesso em: 17/03/2021. p. 4. Disponível em: <https://bit.ly/3cIKQun>.
[14] Art.5º, XVII, LGPD.
[15] Considerandos 75, 85, GDPR.

A falta de parâmetros específicos na GDPR parece se justificar pelo fato de o conceito de dano já ser tema de outras áreas do direito, principalmente em relação à responsabilidade civil. Este entendimento é reforçado ao se verificar o Considerando 146, o qual estabelece que o conceito de dano deve ser interpretado com base na jurisprudência do Tribunal de Justiça da União Europeia e os objetivos das GDPR, sem prejuízo aos tipos de danos previstos no direito dos países membros da UE.[16]

Assim, pode se inferir que o conceito de risco se refere aos cenários hipotéticos/possíveis em que um ou mais tipos de danos podem se concretizar em relação às normas de proteção de dados pessoais.

2.2. Estados Unidos – Risco e Dano

2.2.1. Contexto

Na jurisprudência estadunidense, os tribunais também têm discutido como definir os conceitos de risco e dano relacionados a violação de dados (*data breaches*). A definição de dano é importante nos EUA especificamente porque ela é também um dos requisitos processuais para que uma pessoa possa iniciar um processo nas cortes federais (*standing*[17]), de acordo com a Constituição[18] e a jurisprudência estadunidenses. Ou seja, a conceituação de "dano" no direito dos EUA refere-se tanto ao direito material (qual o dano sofrido pelo titular, e em qual medida) como também ao direito processual (se a pessoa pode ou não iniciar um processo).[19]

2.2.2. Entendimento dos Tribunais

Apesar de não haver um consenso sobre os conceitos, parte dos tribunais federais (*federal courts*) têm diferenciado as noções de risco (*risk*) e dano (*harm*). Por exemplo, no caso *Reilly v. Ceridian Corp*, a empresa Ceridian prestava serviços de pagamento de folha e, em 2009, sofreu um incidente de segurança da informação no qual, potencialmente, houve acesso aos dados pessoais de 27.000 empregados.[20] Não foi possível confirmar tecnicamente se os dados foram acessados ou copiados.[21]

---

[16] "The concept of damage should be broadly interpreted in the light of the case-law of the Court of Justice in a manner which fully reflects the objectives of this Regulation. This is without prejudice to any claims for damage deriving from the violation of other rules in Union or Member State law.". Considerando 146, GDPR.

[17] 'Legitimidade para propor a ação". CASTRO, Marcílio Moreira de. **Dicionário de Direito, Economia e Contabilidade – Português-Inglês - Inglês Português**. Rio de Janeiro: Editora Forense. 2013. p. 238.

[18] ESTADOS UNIDOS. **Constituição dos Estados Unidos**. Artigo III. Acesso em:18/03/2021. Disponível em: <https://bit.ly/3qXpoH7>.

[19] The "case or controversy" clause of Article III of the Constitution imposes a minimal constitutional standing requirement on all litigants attempting to bring suit in federal court. In order to invoke the court's jurisdiction, the plaintiff must demonstrate, at an "irreducible minimum," that: (1) he/she has suffered a distinct and palpable injury as a result of the putatively illegal conduct of the defendant; (2) the injury is fairly traceable to the challenged conduct; and (3) it is likely to be redressed if the requested relief is granted. The United States Department of Justice. Civil Resource Manual. Acesso em:12/03/2021. Disponível em: <https://bit.ly/3rCQ4hz>

[20] ESTADOS UNIDOS. United States Court of Appeals for the Third Circuit. Reilly v. Ceridian Corp – No. 11-1738. 27/10/2011. p.3. Acesso em: 12/03/2021. Disponível em: <https://bit.ly/2PXzCKW>.

[21] *Ibid.*

	Os titulares possivelmente afetados foram notificados pela Ceridian sobre o possível tratamento indevido e, em 2010, parte do atingidos iniciaram uma ação coletiva contra a empresa alegando: (a) risco maior de sofrerem roubo de identidade; (b) prejuízo financeiro pela necessidade de contratarem serviços de monitoramento de crédito; e (c) estresse emocional com a situação.[22] Na segunda instância a Corte Recursal do 3º Circuito[23] confirmou o entendimento de que o caso configurava apenas uma alegação hipotética de dano futuro, por se basear numa mera especulação de que o hacker teve acesso e copiou as informações.[24] Até que se comprovasse que os dados foram usados de forma ilícita não seria possível afirmar que houve dano.[25] Desse modo, a corte entendeu que os apelantes não tinham legitimidade por falta de comprovação de dano. Conforme observa Solove e Citron, a maioria das cortes federais dos EUA tem se posicionado de forma semelhante ao caso *Reilly v. Ceridian Corp*, no qual a alegação de um possível dano futuro (p. ex. maiores chances de fraude ou roubo de identidade) ocasionado por incidente de segurança da informação é considerada demasiadamente especulativa.[26] Desse modo, percebe-se que a jurisprudência majoritária dos EUA diferencia as noções de risco e dano, considerando o primeiro como uma possiblidade de ocorrência de um dano. Assim, por exemplo, no caso de um acesso indevido a dados pessoais, a configuração de dano dependeria da comprovação de que aqueles dados foram utilizados de forma ilícita em um caso concreto (p. ex. fraude econômica). Noutro sentido, algumas cortes federais têm entendido que o risco gerado por um incidente de segurança seria "substancial" o suficiente para configurar o requisito de dano (*harm*) para que um autor tenha legitimidade processual (*standing*) em uma corte federal.[27] Nessa linha de raciocínio, contudo, os conceitos de risco e dano tendem a se confundir pois um "risco substancial" seria considerado um tipo de dano. Por fim, importante notar que esse caso exemplifica que nem sempre é possível averiguar detalhadamente as consequências de um incidente de segurança da informação, o que demonstra que a complexidade técnica do tema precisa ser levada em consideração - conforme já mencionado no item 1.2 deste documento - a fim de se evitar reducionismos que são comuns, principalmente quando a mídia reporta sobre incidentes de segurança. / Recomendação

[22] *Ibid*. p.4.
[23] United States Court of Appeals for the Third Circuit.
[24] *Ibid*. p.7.
[25] "Unless and until these conjectures come true, Appellants have not suffered any injury; there has been no misuse of the information, and thus, no harm.". *Ibid*. p.7.
[26] "Much like Reilly, the majority of courts have ruled that injuries from data breaches are too speculative and hypothetical, too reliant on subjective fears and anxieties, and not concrete or significant enough to warrant recognition". SOLOVE, Daniel J.; e CITRON, Danielle Keats. **Risk and Anxiety: A Theory of Data Breach Harms**). GWU Legal Studies Research Paper No. 2017-2. 2017. p. 741. Acesso em:11/03/2021. Disponível em: <https://bit.ly/2ONEzFs>.
[27] "In those cases, plaintiffs were found to have suffered actual, not hypothetical, injuries where hackers stole personal data from inadequately secured systems […]". *Ibid*, p. 742.

	Risco Conclui-se, portanto, que a análise de risco de um incidente na União Europeia é determinada pelos critérios abstratos de (**i**) probabilidade e (**ii**) gravidade do risco(s) originado pelo incidente. Apesar de tanto a redação da GDPR como as orientações institucionais da WP29/EDPB buscarem dar maior concretude a como esses critérios devem ser utilizados, ainda faltam orientações mais claras sobre o tema. Após realizarmos um paralelo com a definição de risco na União Europeia e com os EUA, é importante que ANPD estabeleça critérios de avaliação mais concretos para que os agentes possam determinar quais são as situações que exigem notificação; ainda mais ao se considerar que o disposto na LGPD sobre risco ("*risco ou dano relevante aos titulares*"[28]) é mais genérico que o estabelecido na GDPR. Ademais, recomenda-se que também sejam elaboradas orientações mais práticas, sendo uma solução possível a elaboração de análise de casos específicos de incidentes de segurança, em modelo semelhante ao que vem sendo elaborado pela EDPB. Desse modo, recomenda-se que a ANPD considere a proporcionalidade entre os riscos do incidente e as medidas técnicas e administrativas previamente adotadas pelos agentes de tratamento, para evitá-los e/ou mitigá-los. Assim, a análise deve partir de um **enfoque contextual** e não de uma simples constatação sobre a ocorrência ou não de um incidente. **Dano** Em relação ao dano**,** verificou-se que os seus parâmetros de avaliação não são especificados na GDPR, sendo o termo utilizado para definir o conceito de risco. Raciocínio semelhante é encontrado na jurisprudência dos EUA que diferencia o risco do dano pela comprovação de que este último ocorreu, sendo o risco um mero cenário possível/hipotético de dano acarretado por um incidente. Considera-se tal diferenciação adequada e elevado parâmetro a ser seguido pela ANPD.
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? **Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?**	**3. Categorias de Dano e Risco** **3.1. Risco** A LGPD é uma norma baseada na noção de risco (risk-based approach), a qual impõe aos agentes de tratamento o dever de avaliar os riscos relacionados ao uso de dados pessoais, a fim de que possam evitá-los e ou mitigá-los de forma proporcional. Desse modo, é intrínseco à ideia de análise de risco a necessidade de subdividi-lo em categorias/graus distintos.

[28] Art. 48, LGPD.

	Por exemplo, a Agência Espanhola de Proteção de Dados Pessoais defende que o risco pode ser classificado e definido como baixo, médio, alto e super alto, considerando os seguintes parâmetros: volume de dados pessoais, tipo de dados pessoais, impacto ou exposição dos dados pessoais[29] **3.2. Dano** O conceito de dano comporta raciocínio semelhante pois, não se parece razoável considerar, por exemplo, que o dano acarretado por um incidente de violação de confidencialidade com dados sensíveis afete da mesma forma um titular que teve um comprovante de escolaridade da sua pré-escola exposto. Ainda, quando se considera que ANPD tem a competência de aplicar sanções administrativas, as mesmas deverão ser aplicadas se utilizando o critério da proporcionalidade/razoabilidade, o qual é pacificamente reconhecido pela doutrina e jurisprudência do direito administrativo.[30] Assim, a não avaliação do risco e do dano por meio de graus/categorias distintas impede inclusive o adequado exercício dos poderes sancionatórios da ANPD.
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	**4. Distinção entre Risco e Dano** De forma simples, considerando interpretações internacionais sobre o tema (ver **item 2**), o risco se refere à possibilidade de um dano ocorrer. Já o dano é a materialização de tal risco, ou seja, no caso em questão, é o efetivo prejuízo para o titular decorrente do incidente, como, por exemplo: fraude, clonagem do cartão de crédito, danos reputacionais, dentre outros. Esses conceitos se relacionam à medida que o risco é abstrato e o é dano concreto. O risco é anterior ao dano. Existir um risco não significa que o dano vai ocorrer, porém, quanto mais alto o risco, maior é a chance da ocorrência do dano e vice-versa. Ver **item 5**.
O que deve ser considerado na avaliação dos riscos do incidente?	**5. Critérios de Risco** **5.1. União Europeia** Conforme já apontado no **item 2** deste documento, baseado na regulação europeia, para a devida avaliação dos riscos do incidente pode-se considerar como critérios: **i)** Probabilidade de o dano(s) ocorrer;

[29] Guia para la gestión y notificación de brechas de seguridad. Agencia Española de Protección de Datos. pp. 53. Disponível em: < https://www.aepd.es/sites/default/files/2019-09/guia-brechas-seguridad.pdf> Acesso em 12/03/2021.
[30] Ver art. 2º, Parágrafo Único, VI, da Lei nº 9.784.

ii) Gravidade do possível dano;
iii) Tipo de incidente;
iv) Natureza, sensibilidade e volume dos dados;
v) Facilidade de identificação dos titulares;
vi) Características dos titulares;
vii) Características do agente de tratamento; e
viii) Quantidade de indivíduos afetados.

Ver itens 1 e 2.

5.2. Espanha

O guia de gestão e notificação de incidentes da Agência Espanhola de Proteção de Dados Pessoais, propõe, em seu Anexo III[31], a utilização de fórmula matemática para o cálculo do risco e da necessidade de informar a autoridade e os titulares. A fórmula atribui um peso para os fatores para (i) a quantidade de dados afetados (p. ex. menos de 100; entre 1k e 100k); (ii) categoria dos dados (sensíveis ou não); e (iii) nível de exposição dos dados acarretado pelo incidente (p. ex. dados foram tornados públicos):

"Riesgo = P (Volumen) x Impacto (Tipología x Impacto)"

Entendemos que esta fórmula poderá ser utilizada como referência pela ANPD na elaboração de seus critérios de avaliação de risco.

5.3. Medidas de Segurança da Informação

Uma vez que a resposta de um incidente de segurança envolve conjuntamente ações de investigação, contenção e mitigação desde a detecção, a autoridade deve considerar os esforços empreendidos pelo agente para evitar e/ou reduzir a extensão e os efeitos do incidente – e não apenas a capacidade de evitar a vulnerabilidade. Em outras palavras, o agente que reage proativamente e em tempo hábil a um incidente reforça sua presunção de boa-fé e deve ser recompensado por isso; ao passo que situações opostas (e.g. negligência, conduta omissiva) também devem ser tratadas como tais. A ocorrência de um incidente não se traduz automaticamente no entendimento de que não foram adotadas medidas de segurança adequadas pelo agente de tratamento.

Dois outros pontos de destaque referem-se ao fato de ser (i) comum em muitos incidentes haver mais de um agente de tratamento envolvido, devido à complexidade das cadeias de tratamento de dados, principalmente quando da utilização de sistemas de informação de terceiros (p. ex. serviços de cloud; licenciamento de software etc.); e (ii) a realidade técnica de que incidentes de segurança são complexos e multicausais.

[31] ESPANHA. Agencia Española de Protección de Datos (AEPD). Guia para la gestión y notificación de brechas de seguridad. Anexo III. Acesso em 12/03/2021. Disponível em: <https://bit.ly/3lxveOA>

Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	**6. Espanha** A Agência Espanhola de Proteção de Dados Pessoais disponibiliza, ao final de seu guia sobre incidentes de segurança, um modelo de formulário com as informações que devem constar em uma notificação de incidente à autoridade[32]. Tal formulário é bastante completo e pode ser utilizado como modelo por outras jurisdições. Se compararmos às informações exigidas pela lei brasileira, verifica-se que as informações constantes do modelo espanhol de notificação à autoridade são mais detalhadas e permitem uma avaliação melhor do incidente ocorrido, tendo em vista, por exemplo, que detalha não só os riscos, mas também as possíveis consequências concretas daquele incidente (como danos à reputação do titular dos dados). O modelo espanhol abarca todas as informações exigidas pela lei brasileira (descrição da natureza dos dados pessoais afetados, informações sobre os titulares envolvidas etc.), porém exige maiores detalhamentos para uma melhor avaliação da autoridade. Seguem abaixo as informações que, para a autoridade espanhola, devem constar em uma notificação de incidente à autoridade:[33] **i) Dados do encarregado de proteção de dados pessoais** **ii) Identificação do responsável pelo tratamento – controlador** **iii) Identificação do operador dos dados pessoais** **iv) Informações temporais do incidente (data de notificação, meios de detecção, eventual justificação de notificação tardia etc.)** **v) Sobre o incidente:** • Resumo do incidente; • Tipo do incidente: de confidencialidade (acesso não autorizado), de integridade (alteração não autorizada), de disponibilidade (perda dos dados pessoais); • Por qual meio se materializou o incidente (exemplos: malware; dispositivo perdido ou furtado/roubado; dados pessoais enviados a alguém equivocadamente; phishing; hacking etc.);

[32] AEPD. **Guia para la gestión y notificación de brechas de seguridad**. pp. 48-52.
[33] *Ibid*. pp. 22 e 23.

	• Contexto da ocorrência do incidente (interno por ação intencional; interno por ação não intencional; externo por ação intencional; externo por ação não intencional; outros); e • Medidas tomadas antes do incidente para a proteção dos dados pessoais. vi) Sobre os dados pessoais afetados • Categorias de dados pessoais (dados básicos; dados sobre infrações ou condenações penais; credenciais de acesso ou identificação; dados bancários; dados de contato; dados de localização; outros); • Categorias especiais de dados (religião, saúde; origem racial; afiliação sindical; dados genéticos; dados biométricos; opinião política; vida sexual; outros); e • Número aproximado de dados pessoais afetados. vii) Sobre os titulares afetados • Perfil dos titulares afetados (clientes, estudantes, usuários, pacientes, empregados, outros); • Número aproximado de titulares afetados. viii) Possíveis consequências • Nos casos de incidente de confidencialidade: divulgação a terceiros/divulgação na internet; enriquecimento de outras bases de dados; dados podem ser tratados para outro fim; outras; • Nos casos de incidentes de integridade: dados foram modificados de modo que não podem ser recuperados; dados foram modificados e usados para outro fim; outras; • Nos casos de incidentes de disponibilidade (impossibilidade de prestação de um serviço aos interessados; deterioração das condições de prestação de um serviço aos interessados; outras); • Natureza do impacto potencial aos titulares (perda do controle sobre seus dados pessoais; falsificação de identidade; danos à reputação; limitação dos direitos; fraude; discriminação; danos materiais; perda da confidencialidade de dados protegidos por segredo de negócio; outros); • Severidade das consequências aos titulares (baixa, média, alta, muito alta); e • Medidas tomadas para solucionar os incidentes e minimizar o impacto aos titulares dos dados pessoais. ix) Comunicação aos titulares • Os titulares foram comunicados a respeito do incidente? Se sim: em que data, quantos titulares foram informados; meios ou ferramentas de comunicação. Se ainda não: data em que serão informados. Se a comunicação não será feita: justificativa para não os informar. • Se titulares foram informados, anexar documento que comprove.

	x) Implicações internacionais - Existem sujeitos de outros países afetados pelo incidente? Se sim, quais países? **xi) Documentos anexos** **** **7. França** A autoridade francesa de proteção de dados pessoais, a *Commission Nationale de L'informatique et des Libertés* (CNIL), destaca que lhe devem ser notificadas as seguintes informações[34]: **i)** a natureza da violação; **ii)** as categorias e o número aproximado de pessoas envolvidas; **iii)** as categorias e o número aproximado de arquivos afetados; **iv)** as prováveis consequências da violação; **v)** as medidas tomadas para mitigar e/ou limitar as consequências negativas do incidente; **vi)** se aplicável, a justificativa de ausência de notificação à autoridade e/ou aos titulares dos dados pessoais envolvidos; e **vii)** os motivos de atraso na notificação à autoridade, quando aplicável. Ao compararmos os elementos exigidos na notificação da CNIL, verificamos que há uma certa convergência com a notificação espanhola. O que pode indicar que a par de um núcleo específico de determinadas perguntas, eventuais requisições das autoridades irão variar em relação a documentos técnicos ou de risk assessment dos agentes de tratamento relacionados ao incidente.
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	**8. Critérios para o Prazo** **8.1. Contagem** A contagem do prazo deve se iniciar com a confirmação do incidente pela empresa. Ou seja, a suspeita de que houve um incidente necessita de uma verificação adequada antes de que seja necessário notificação à ANDP. Posicionamento semelhante foi adotado pela WP29 ao esclarecer em suas *guidelines* que um incidente deve ser informado apenas após haver um grau razoável de certeza de que ele ocorreu.[35] Este critério também evita com que a ANPD seja notificada de forma excessiva pelos agentes de tratamento.

[34] CNIL. **Les violations de données personnelles**. Disponível em <https://bit.ly/3lsgrEu>. Acesso em 18/03/2021.

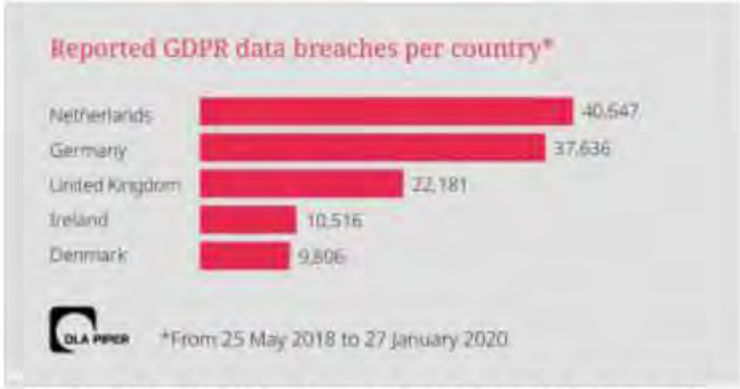
[35] "WP29 considers that a controller should be regarded as having become "aware" when that controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised. ARTICLE 29 DATA PROTECTION WORKING PARTY. **Guidelines on Personal data breach notification under Regulation 2016/679.** pp 10-11.

	Conforme a Agência Espanhola de Proteção de Dados, o prazo de 72 horas estabelecido pela GDPR refere-se à primeira notificação à autoridade após a ciência do incidente. Ainda, se, no momento da notificação, não for possível fornecer todas as informações necessárias, exigidas pela lei, isso poderá ser feito posteriormente, de forma gradual e em diferentes fases. Quando a comunicação não for possível no prazo estabelecido em lei, ela deverá ser feita da mesma forma, mas justificando o motivo da demora[36]. **8.2. Prazo de Notificação** Entendemos que uma notificação pode ser dividida entre parcial e complementar. Assim, após a confirmação da ocorrência do incidente, o agente de tratamento pode realizar uma notificação parcial à ANPD, enquanto realiza as medidas adequadas de investigação e mitigação. Considerando a natureza complexa dos incidentes de segurança da informação (ver **item 1.2**), pode ser inviável tecnicamente exigir em todos os casos uma avaliação completa do incidente na primeira notificação – em alguns casos não é possível nem mesmo compreender totalmente um incidente – por isso a importância de notificações parciais.
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) **Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?**	**9. Espanha** De acordo com o guia de incidentes de segurança da Agência Espanhola de Proteção de Dados Pessoais, a comunicação aos titulares dos dados pessoais deve ser feita em linguagem clara e simples, e deve conter, no mínimo, os seguintes elementos[37]: • Dados de contato do encarregado de proteção de dados pessoais ou um canal de contato onde o titular possa obter mais informações; • Descrição geral do incidente e do momento em que ocorreu; • Resumo das medidas adotadas desde o momento do incidente para controlar possíveis danos; e • Outras informações úteis aos titulares para proteger os seus dados pessoais ou prevenir possíveis danos. Ainda, de acordo com o referido guia, para verificar a necessidade de comunicação dos titulares dos dados pessoais, diversos fatores devem ser levados em consideração, como os seguintes[38]: • Quais são as obrigações legais e contratuais; • Quais são os riscos decorrentes da perda dos dados pessoais: p. ex. danos materiais, danos reputacionais etc.;

[36] Guia para la gestión y notificación de brechas de seguridad. Agencia Española de Protección de Datos. p. 53. Disponível em: <https://www.aepd.es/sites/default/files/2019-09/guia-brechas-seguridad.pdf>. Acesso em 12/03/2021.
AEPD. **Guia para la gestión y notificación de brechas de seguridad**. p. 43.
[38] *Ibid.*

	• Se existe risco razoável de falsificação de identidade ou fraude (em razão do tipo de informação afetada e levando em consideração se a informação foi pseudonimizada ou criptografada); e • Até que ponto a pessoa afetada pode evitar ou mitigar possíveis danos posteriores. As sugestões acima podem ser utilizadas como parâmetros pela ANPD na análise de um documento de comunicação aos titulares feito por uma empresa. Sobre o prazo para a referida comunicação, diferente do indicado no **item 8** acima, importante que os titulares sejam notificados após a confirmação da ocorrência, e não também para os casos de mera suspeita, e apenas nos casos em que tal comunicação se faz necessária (ver **item 12**).
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? **A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?**	**10. Forma da Comunicação** A comunicação deve, preferencialmente, ocorrer de forma direta, seja por telefone, e-mail, SMS, correio etc., prevalecendo meio de comunicação usualmente praticado pela empresa com o titular. A notificação indireta (p. ex. por meio de avisos públicos em sites, blogs corporativos ou comunicados na imprensa) deve ser utilizada quando (**i**) os custos de uma notificação direta forem excessivos para a empresa em questão ou (**ii**) quando não seja possível entrar em contato com os titulares afetados (por exemplo, porque são desconhecidos ou os dados de contato estão desatualizados). Caso não se verifique nenhuma dessas situações, deve-se privilegiar a comunicação direta. Nesse mesmo sentido é o guia de incidentes de segurança da Agência Espanhola de Proteção de Dados Pessoais[39].
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	**11. União Europeia** A legislação europeia determina que não será necessária comunicação à autoridade quando o controlador puder demonstrar que o incidente de proteção de dados pessoais não trará risco relevantes aos direitos e às liberdades fundamentais dos titulares (e.g. os dados pessoais já se encontravam publicamente disponíveis e sua divulgação não representou nenhum risco adicional ao titular dos dados). **/ Recomendações** A ANPD pode seguir no mesmo sentido elencado acima, de acordo com a redação expressa na LGPD, uma vez que há situações de incidentes que não acarretam risco ou dano relevante aos titulares (p. ex. dados criptografados que tornem os dados afetados pelo incidente ininteligíveis).

[39] Idem.

	A notificação excessiva é uma questão com a qual a ANPD deve estar atenta no processo de elaboração das normas sobre o tema. As autoridades de proteção de dados pessoais da União Europeia têm enfrentado essa questão, conforme mostram os dados da pesquisa quantitativa abaixo:  **Fig. 2** – As 5 autoridades de proteção de dados da EU que mais receberam notificações de incidentes.[40] Assim, os critérios de notificação devem buscar filtrar os casos realmente necessários de serem notificados a fim de proteger os direitos dos titulares.
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	**12. União Europeia** No direito europeu, somente há necessidade de informar os titulares dos dados afetados pelo incidente em situação de alto risco às pessoas afetadas. Quando a comunicação aos titulares puder comprometer o resultado de uma investigação em curso, a comunicação poderá ser adiada, mas com a supervisão da autoridade. Além disso, mesmo nas hipóteses de alto risco ao titular dos dados, as autoridades de proteção de dados destacam algumas situações excepcionais em que pode ser dispensada a comunicação, quais sejam: • Os dados pessoais afetados pelo incidente foram submetidos a medidas de segurança técnica e administrativa adequadas para garantir que os dados pessoais não sejam compreensíveis por pessoas ou sistemas não autorizados, seja, por exemplo, por meio do uso criptografia prévia, minimização no uso dos dados, acesso a ambientes de teste sem dados reais etc.; • Detectado o incidente, o agente de tratamento tomou as medidas necessárias para garantir que o risco alto aos direitos e às liberdades dos titulares dos dados não deva mais se concretizar;

[40]DLA PIPER. **DLA Piper GDPR data breach survey: January 2020**. p. 6. Acesso em:18/03/2021. Disponível em: <https://bit.ly/3tr8OkG>.

	• A comunicação aos titulares dos dados exigiria um esforço desproporcional do agente de tratamento, a nível técnico e administrativo, por exemplo, quando os dados de contato foram perdidos em razão do incidente; quando um novo processo deva ser desenvolvido para realizar a comunicação; ou se requer dedicação excessiva de recursos internos para a identificação dos titulares afetados / **Recomendações** LGPD somente dispõe como exceção à obrigatoriedade de notificação aos titulares os casos que não acarretam risco ou dano relevante aos titulares.[41] A ANPD, contudo, deverá regulamentar tal norma, trazendo critérios e casos específicos de dispensa de comunicação, as quais podem se basear no diploma europeu, conforme narrado acima. Outro critério interessante de ser considerado é que os titulares sejam notificados após a confirmação da ocorrência, e não também para os casos de mera suspeita. Precauções nesse sentido evitam com que o titular possa ser excessivamente notificando, e que desse modo, não consiga discernir as situações mais críticas que possam exigir a tomada de precauções de sua parte (p. ex. troca de senha, realização de back-ups, etc).
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	**13. Espanha** A Agência Espanhola de Proteção de Dados (AEPD) estabelece critérios detalhados para se determinar o risco de um incidente e as tomadas de decisões subsequentes. Conforme guia publicado AEPD, para a gestão de um incidente de segurança, deve-se determinar o perigo potencial do incidente e estimar a magnitude do impacto potencial sobre os indivíduos, o que simplesmente reflete os comandos da GDPR[42]. Para esta avaliação, também deve se recorrer à análise de risco/avaliação de impacto realizada antes do início das atividades de tratamento. A periculosidade/gravidade do incidente, conforme a Agência Espanhola, dependerá dos seguintes fatores[43]: **i) Categoria ou o nível de criticidade da segurança dos sistemas afetados:** • Crítico (afeta dados valiosos, grande volume e em pouco tempo). • Muito alto (capacidade de afetar dados valiosos, em quantidade considerável). • Alto (capacidade de afetar dados valiosos). • Médio (capacidade de afetar um volume considerável de dados). • Baixo (pouca ou nenhuma capacidade de afetar um volume considerável de dados). **ii) Natureza, sensibilidade e categoria dos dados pessoais afetados:** • Dados de baixo risco: dados de contato, de educação, familiares, profissionais, dados biográficos.

[41] Art. 48, LGPD.
[42] Considerando 76, GDPR.
[43] AEPD. **Guia para la gestión y notificación de brechas de seguridad**. p. 22.

- Dados de comportamento: localização, trânsito, hábitos e preferências.
- Dados financeiros: transações, posições, receitas, contas, faturas.
- Dados sensíveis: dados de saúde, dados biométricos, dados relacionados à vida sexual etc.

iii) Dados legíveis/ilegíveis:

- Dados protegidos por meio de algum sistema de pseudonimização, por exemplo, criptografia ou hash.

iv) Volume de dados pessoais:

- Expresso em quantidade (registros, arquivos, documentos) e/ou em períodos de tempo (uma semana, um ano etc.).

v) Facilidade de identificação dos indivíduos:

- Facilidade com que se pode deduzir a identidade de indivíduos envolvidos na violação

vi) Severidade das consequências aos indivíduos:

- Baixa: as pessoas não serão afetadas ou poderão encontrar alguns inconvenientes que poderão superar sem problemas (irritações, aborrecimentos etc.).
- Médio: as pessoas podem encontrar inconvenientes significativos, que serão capazes de superar, apesar de algumas dificuldades (custos adicionais, negação de acesso a serviços comerciais, medo, falta de compreensão, estresse, pequenos males físicos etc.).
- Alto: as pessoas podem enfrentar consequências importantes, que podem ser capazes de superar, porém com sérias dificuldades (danos materiais, perda de emprego, intimações judiciais, deterioração da saúde etc.).
- Muito alto: as pessoas podem enfrentar consequências graves e até irreversíveis, que não poderão superar (exclusão ou marginalização social, dificuldades financeiras como dúvidas consideráveis ou incapacidade de trabalhar; doenças psicológicas ou físicas a longo prazo, morte etc.).

vii) Características especiais dos indivíduos:

- Se afetam indivíduos com características ou necessidades especiais.

viii) Número de indivíduos afetados:

- Dentro de uma escala determinada, por exemplo, mais de 100 indivíduos.

ix) Características especiais do controlador dos dados pessoais:

- Com base na atividade exercida pela empresa.

x) Perfil dos indivíduos afetados:

- Sua posição na estrutura administrativa da empresa e, em consequência, seus privilégios de acesso a informações sensíveis ou confidenciais.

xi) O número ou o tipo dos sistemas afetados

xii) O impacto que o incidente pode ter para a organização

Do ponto de vista da proteção da informação, da prestação dos serviços, do cumprimento legal e/ou da imagem pública (reputacional). Ele estará relacionado à categoria ou criticidade dos serviços afetados e das pessoas afetadas. Nesse sentido, diferencia-se os seguintes impactos:

- Baixo: prejuízo limitado
- Médio: prejuízo grave
- Alto: prejuízo muito grave

xiii) Os requerimentos legais e regulatórios:

- Notificação do incidente à autoridade de controle e qualquer outra obrigação de notificação.

Conforme elencando acima verifica-se que a AEPD utilizou como base o Guia sobre Incidentes da WP29 (ver item 2.1) a partir do qual foram incluídos novos elementos de análise e maiores detalhes. Desse modo, a ANPD pode utilizar como base a metodologia estabelecida pela AEPD para análise da gravidade do incidente.

* * * *

14. Canadá

De acordo com a autoridade canadense de proteção de dados pessoais, as perguntas que devem ser feitas para se analisar um incidente são[44]:

- O que aconteceu e qual a probabilidade de alguém ser prejudicado pelo incidente?
- Quem realmente acessou ou pode ter acessado os dados pessoais?
- Há quanto tempo os dados pessoais foram expostos?
- Existe evidência de intenção maliciosa (por exemplo, roubo, invasão de hacker)?
- Dados pessoais foram violados, aumentando, portanto, o risco de uso indevido?
- Os dados pessoais violados foram expostos a indivíduos ou empresas/entidades que representam risco a reputação do titular (por exemplo, ex-cônjuge ou chefe)?
- Os dados pessoais foram expostos a empresas/entidades conhecidas que se comprometeram a destruir e não divulgar os dados pessoais?

[44] DLA PIPER. **DLA Piper GDPR data breach survey: January 2020**. p. 6. Acesso em: 12/03/2021. Disponível em: <https://bit.ly/3tr8OkG>.

	• Os dados pessoais foram expostos a indivíduos, empresas ou entidades com baixa probabilidade de compartilhá-los de uma forma que causaria danos (por exemplo, no caso de uma divulgação acidental para destinatários)? • Os dados pessoais foram expostos a indivíduos, empresas ou entidades que são desconhecidos, ou a um grande número de indivíduos, onde certos indivíduos podem usar ou compartilhar as informações de uma forma que causaria danos? • Os dados pessoais foram expostos a indivíduos, empresas ou entidades que provavelmente tentarão causar danos a partir de tais informações (por exemplo, ladrões de informações)? • O dano se materializou (demonstração de uso indevido)? • Os dados pessoais foram perdidos, acessada indevidamente ou furtada/roubada? • Os dados pessoais foram recuperados? • Os dados pessoais estão adequadamente criptografados, anônimos ou não são facilmente acessíveis?
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	**15. ENISA** Nas recomendações para uma metodologia de avaliação de gravidade de incidente de segurança da informação,[45] a ENISA define a gravidade de um incidente como a "*estimativa da magnitude de um impacto potencial em indivíduos derivado de um incidente*". Resumidamente, a metodologia é baseada em três variáveis: **i)** o contexto do tratamento dos dados (DPC); **ii)** a facilidade da identificação dos indivíduos envolvidos (EI); e **iii)** as circunstâncias específicas do incidente (CB). A gravidade do incidente é classificada entre baixa, média, alta e muito alta e calculada pelo produto entre o contexto do tratamento dos dados e a facilidade de identificação dos indivíduos somado com as circunstâncias específicas do incidente ($SE = DPC \times EI + CB.$). Os critérios para o cálculo da pontuação de cada variável e a determinação da gravidade do incidente podem ser encontrados em mais detalhes no relatório. **16. Breach Level Index (BLI)** O *Breach Level Index* (BLI) é a metodologia desenvolvida pela IT-Harvest que se propõe a criar um índice para mensurar a gravidade de um incidente de segurança.[46] Segundo a proposta, deve ser atribuído um índice aos incidentes de segurança da mesma forma que são atribuídos índices a fenômenos naturais como ventos, erupções vulcânicas e terremotos. O índice baseia-se em uma operação logarítmica – Log10(NxTxSxA) – exposta

[45] ENISA. **Recommendations for a methodology of the assessment of severity of personal data breaches**. Disponível em <https://bit.ly/3r7JoHn>. Acesso em 18/03/2021.
[46] STIENNON, Richard. **Categorizing Data Breach Severity with a Breach Level Index**. Disponível em: <https://bit.ly/3bZESpT>. Acesso em 18/03/2021.

	a quatro variáveis, cada qual com um valor próprio: número de incidentes registrados (N), origem do vazamento (S), tipos de dados afetados (T) e danos causados com os dados (A) – p. ex.: roubo de identidade, solicitações de empréstimos, transferências bancárias.
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	**17. Compartilhamento de Informações sobre Incidentes** Quando se considera a complexidade e a constante evolução das práticas de violação da segurança da informação, verifica-se que incentivos meramente negativos/punitivos são insuficientes para atingir um dos principais objetivos da LGPD: a garantia da confidencialidade, integridade e disponibilidade dos dados pessoais.[47] Assim, a ANPD deve considerar incentivos positivos para fomentar um ambiente de cooperação entre agentes de tratamento e reguladores, a fim de se desenvolver um ecossistema de segurança da informação mais robusto no Brasil. A preocupação com o desenvolvimento de ambientes de cooperação quanto à segurança da informação também tem ocorrido em outros países, principalmente devido à constatação de que a complexidade do tema impede que apenas uma das partes envolvidas seja capaz de, isoladamente, garantir o melhor nível de segurança possível. Com o objetivo de garantir um ecossistema mais integrado e colaborativo tem sido elemento chave à implementação de políticas de fomento ao compartilhamento de informações sobre segurança da informação. Esse tema já tem sido debatido a certo tempo nos Estados Unidos. O fomento ao compartilhamento de informações nos EUA tem sido feito tanto do viés legislativo e regulatório, como na elaboração de guias de boas práticas. A lei federal *Cybersecurity Information Sharing Act* (CISA)[48] estabelece mecanismos voluntários de troca de informações sobre incidentes e ameaças de segurança da informação entre o setor público e privado. Como uma das principais dificuldades de se fomentar o compartilhamento está na criação de um ambiente de confiança institucional e de segurança jurídica, a CISA buscou endereçar este ponto por meio de determinadas proteções contra processos judiciais para agentes que compartilham determinadas informações.[49] A qual pode ser complementada por meio de acordos de confidencialidade. No mesmo sentido, a Presidência dos EUA elaborou a "*Executive Order 13691: Promoting Private Sector Cybersecurity Information Sharing*"[50] que estabelece procedimentos para a criação de organizações de troca

[47] Art. 46, LGPD.
[48] ESTADOS UNIDOS. **S.2588 - Cybersecurity Information Sharing Act of 2014**. 113th Congress (2013-2014). Acesso em: 11/03/2021. Disponível em: < https://bit.ly/3roeU3D>
[49] "Protection from liability. (b) Sharing or receipt of cyber threat indicators. — No cause of action shall lie or be maintained in any court against any entity, and such action shall be promptly dismissed, for the sharing or receipt of cyber threat indicators or countermeasures under subsection (c) of section 4 if:
(1) such sharing or receipt is conducted in accordance with this Act; and (2) in a case in which a cyber threat indicator or countermeasure is shared with the Federal Government in an electronic format, the cyber threat indicator or countermeasure is shared in a manner that is consistent with section 5(c).". *Ibid.* Sec. 6.
[50] ESTADOS UNIDOS. Executive Order 13691. 12/02/2015

	voluntária de informações sobre segurança da informação entre governo e setor privado, os *Information Sharing Analysis Organizations* (ISAOs).[51] A criação de ISAOs é flexível, podendo ser formadas a partir de diversos critérios, como, por exemplo, por área de atuação no mercado, por região ou para incidentes específicos. Já o *National Institute of Standards and Technology* (NIST) dos EUA elaborou um guia para compartilhamento de informações sobre ameaças de cyber segurança.[52] O guia foi elaborado com base na premissa de que o compartilhamento de informações sobre incidentes contribui para um maior nivelamento no acesso à informação; maior capacidade de prevenção e resposta à incidentes; maior maturação do tema pelo incentivo ao cruzamento de informações; e mais agilidade nas respostas defensivas dos agentes.[53] De forma resumida, o incidente sofrido/detectado por uma organização transforma-se em prevenção para as demais.[54] Este caminho regulatório também pode ser complementado pela suspensão da aplicação de determinados regulamentos, sendo que esta prática já vem sendo adotada nos EUA. Por exemplo, a agência regulatória estadunidense *Food and Drug Administration* (FDA) elaborou guia em 2016 orientando que não iria aplicar determinadas exigências de notificação de vulnerabilidades de segurança da informação em equipamentos médicos se o fabricante fosse membro de uma ISAO e compartilhasse a informação com a organização.[55]

[51] Para uma avaliação governamental dos impactos na privacidade e na proteção das liberdades civis da Executive Order nº 13691 ver: DEPARTMENT OF HOMELAND SEDCURITY. Executive Order 13636 Privacy and Civil Liberties Assessment Report. Novembro de 2018. Acesso em: 11/03/2021. Disponível em: <https://bit.ly/3clda5S>

[52] ESTADOS UNIDOS. The National Institute of Standards and Technology (NIST). NIST Special Publication 800-150 - Guide to Cyber Threat Information Sharing. 2016. Acesso em: 11/03/2021. Disponível em:<https://bit.ly/2PONOpj>

[53] *Ibid*. pp 3-4.

[54] *Ibid*. p 3.

[55] "If the manufacturer actively participates as amember of an ISAO and shares information about the vulnerability within the ISAO, FDA does not intend to enforce compliance with the reporting requirements in21 CFR part806.For class III devices, the manufacturer does submit a summary of theremediation as part of itsperiodic (annual) report to FDA."ESTADOS UNIDOS. Food and Drug Administration. Postmarket Management of Cybersecurity in Medical Devices: Guidance for Industry and Food and Drug Administration Staff. 28/12/2016. p.23. Acesso em 11/03/2021. Disponível em: <https://bit.ly/3tdA2eC>

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: BARRAL PARENTE E PINHEIRO ADVOGADOS
CPF/CNPJ: 32.083.314/0001-91

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS **IMPORTANTE:** Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	**Quando os dados do titular forem expostos de forma ilícita, contrariando o previsto na legislação brasileira e, em especial, na LGPD. Deve-se verificar todos os itens que cercam a utilização dos dados sob aspectos da LGPD, finalidade, base legal, origem dos dados, compromisso com a proteção de dados (medidas de controle, governança, práticas de conscientização). Deve-se observar o interesse do controlador em tratar os dados, bem como o legítimo interesse das empresas na obtenção e processamento de dados.**
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	**Sim, os danos devem ser divididos em categorizações fracionadas de baixo, médio, alto e crítico. Tal metodologia de risco deve levar em consideração (i) a medição do volume de dados tratados, (ii) se os dados são considerados pessoais, pessoais sensíveis ou confidenciais, (iii) se há ou não medidas protetivas, (iv) se o controlador tem certificações (válidas) que certifiquem as boas práticas, e (v) se há ou não estrutura dedicada de armazenamento de dados para determinar a responsabilidade civil.**
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	**O risco ao titular seria algo ainda intangível, mas com potencial de atingir o titular. Já o dano é materialização de prejuízo ao titular. Portanto, o risco inerente de tratamento de dados pode ser um potencial causador de dano.**

O que deve ser considerado na avaliação dos riscos do incidente?	**Deve-se considerar os requisitos elencados na LGPD, como por exemplo se houve notificação à autoridade em prazo razoável, ponderar se os dados atingidos são pessoais, pessoais sensíveis ou confidenciais, se foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, se tratador de dados atende aos requisitos de segurança e governança estabelecidos, o quanto a exposição afeta a privacidade do titular de dados, as medidas adotadas, se houve vantagem financeira do controlador e como é feito o armazenamento de dados (banco de dados próprio ou terceirizado), entre outras requisitos estabelecidos.**
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	**Os itens obrigatórios de notificação listadas no §1º do art. 48 são suficientes, à luz do art. 33 da legislação europeia sobre proteção de dados, GDPR (General Data Protection Regulation).**
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	**O prazo para notificação deve ser de 72 horas. Isso se deve pela necessidade de avaliação do grau e o dano de um incidente, bem como de atividades analíticas até que tenha integral evidência do dano, facilitando inclusive a comunicação com o regulador. Deve-se levar em consideração, ainda, o elevado volume de dados tratados pelos controladores e o trâmite interno nas empresas e o tempo para ativar seu comitê de crises, por exemplo. Há que se mencionar, por fim, que o tratamento de dados feito por algumas empresas funciona sob modelo híbrido de armazenamento de dados, sendo os dados armazenados em data center próprio e em bancos de dados terceirizados, o que aumenta o tempo para verificação dos dados a serem investigados. Assim, prazo de 72 horas se faz justificável.**
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	**Após confirmado o incidente e devidamente identificado, os titulares de dados devem ser informados em até 24 horas, constando da notificação as informações já delineadas no §1 do art. 48.**
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em	**Via comunicação eletrônica (e-mail ou similar) aos titulares de dados ligados ao controlador. Os titulares devem ser comunicados direta e individualmente, principalmente quando houver incidente envolvendo dados pessoais sensíveis. Não se tratando de dados pessoais sensíveis, admite-se comunicação pública, como divulgação em mídias sociais, na imprensa e no URL da empresa.**

determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	**A comunicação de incidentes para ANPD deve acontecer apenas nos casos de incidentes elencados como médio e alto risco, quando identificado um cenário de exposição de dados pessoais, pessoais sensíveis ou confidencias.**
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	**Incidentes que não envolvam exposição de dados pessoais, dados pessoais sensíveis ou dados confidenciais, bem como aqueles elencados como baixo risco.**
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	**A ANPD poderia adotar critérios como avaliar as medidas protetivas adotadas, as certificações do controlador, a revisão de código aplicação, a adoção de pentest, entre outras práticas protetivas que demonstrem a preocupação do controlador com o tratamento dos dados pessoais, pessoais sensíveis ou confidenciais.**
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	**Normativas como NIST e ISO´s possuem metodologias para tratamento de incidentes, bem como o Technical Guideline for Incident Reporting da European Union Agency for Cybersecurity (ENISA).**
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	**Como premissa para o início das tratativas, a ANPD deve incialmente notificar o controlador para alertar acerca de uma possível exposição de dados em sua base de dados, estabelecendo prazos de respostas/manifestação sobre o incidente e delimitando os pontos a serem tratados na manifestação.** **Quando se trata de medidas a serem tomadas pela ANPD, é necessário que estas sejam elencadas de acordo com o nível de gravidade dos incidentes. No entanto, antes de se imputar punição à empresa, a agência deve verificar o nível de adequação das medidas de governança da gestão de privacidade de dados e segurança da informação pela empresa, assegurar que medidas protetivas dos dados sejam implementadas ou elevadas em casos de não suficiência do tratamento de dados, a fim de evitar novos incidentes.** **Em casos da gravidade de exposição seja considerada crítica, o Guia de gestão de incidentes de segurança das empresas deve ser posto em prática, bem como a ativação de um comitê de crise específico.**

SUGESTÃO DE NORMATIVO, SE HOUVER
ISO9001, ISO27001, ISO27002, ISO27771 e ISO29134 em todos seus itens.
NIST Cybersecurity Framework
Technical guideline for Incident Reporting da European Union Agency for Cybersecurity (ENISA)
General Data Protection Regulation

COMENTÁRIOS DA BRASSCOM À TOMADA DE SUBSÍDIOS PARA REGULAMENTAÇÃO DO DEVER DE COMUNICAÇÃO SOBRE INCIDENTES DE SEGURANÇA

Brasília (DF), 22 de março de 2021

A Brasscom, Associação Brasileira das Empresas de Tecnologia da Informação e Comunicação, entidade que congrega algumas das mais dinâmicas e inovadoras empresas de Tecnologia da Informação e Comunicação (TIC) alinhadas com a Era Digital, que prestam serviços de TIC, desenvolvem e licenciam software, fabricam e comercializam hardware, disponibilizam redes sociais ou plataformas variadas; ou ainda prestam serviços telecomunicações, tem como Propósito trabalhar em prol de um Brasil Digital, Conectado e Inovador por meio da propositura e defesa de políticas públicas, com especial enfoque no emprego, na diversidade e a educação, bem como, na inovação.

Neste mister, a Brasscom parabeniza a Autoridade Nacional de Proteção de Dados (ANPD) por lançar esta Tomada de Subsídios para discutir a regulamentação sobre o dever de comunicação de incidentes de segurança, nos termos do artigo 48, parágrafo 1º da LGPD.

Consideramos fundamental essa iniciativa de abrir espaço para que todas as partes interessadas possam apresentar considerações e permitir que a futura regulamentação atinja seus objetivos de forma equilibrada e eficiente. Neste sentido, a Brasscom, respeitosamente, vem apresentar suas considerações abaixo dispostos nos seguintes tópicos:

Sumário

1. A COMUNICAÇÃO DE INCIDENTES DE SEGURANÇA

A LGPD, em seu artigo 48, prevê a necessidade de comunicação pelo controlador à ANPD e ao titular dos dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Para evitar eventuais confusões de conceitos, sugerimos que a ANPD estabeleça de forma clara a diferença entre o termo "incidente de segurança" do termo "incidente de segurança com dados pessoais". Apresentamos abaixo nossas sugestões de definições para ambos os conceitos, usando como referência a ISO 27035-1:2016[1]:

> *"Um incidente de segurança é qualquer evento adverso identificado que pode prejudicar os ativos de uma organização ou comprometer suas operações.*
>
> *Um incidente de segurança com dados pessoais é qualquer evento adverso, identificado e confirmado ou ~~sob suspeita~~, relacionado à violação na segurança de dados pessoais, ~~tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita~~" (grifo nosso).*

Essa clara dissociação entre os conceitos auxiliará as organizações a efetivamente compreender a qualificação legal para a comunicação à autoridade, ou seja, realizá-la apenas quando for identificado e confirmado que o incidente de segurança com dados pessoais acarretará risco ou dano relevante aos titulares. E para que o controlador possa chegar a essa determinação, é fundamental que ele faça um exercício de gestão de risco quando da estruturação do seu processo de tratamento de dados pessoais.

O objetivo da LGPD é a proteção dos titulares dos dados pessoais e não a proteção dos dados em si. Desse modo, o exercício de gestão de risco e de aplicação dos princípios fixados na lei deve ser norteado pelo objetivo de proteção do titular do dado. Dito de outra forma, eventual incidente de segurança que não tenha qualquer potencial de gerar riscos ou prejuízos ao titular do dado não deveria para fins do arcabouço normativo da LGPD, ensejar uma movimentação de comunicação e/ou ações sob a óptica da lei (sem se falar, aqui, em possíveis adoções de medidas de mitigação de risco de segurança da informação propriamente dita).

[1] Organização Internacional de Normalização, ISO 27035-1:2016. Disponível em: https://www.iso.org/standard/60803.html.

Dessa forma, será explicado a seguir a lógica por trás da gestão de risco com o objetivo de promover a avaliação dos norteadores que devem ser adotados para determinar as regras de comunicação de incidentes de segurança para a ANPD.

2. A PREMISSA DE GESTÃO DE RISCO

A premissa de gestão de risco traz sua inspiração nas práticas já corriqueiras de segurança da informação e se concretiza no processo sistemático de identificação, avaliação, tratamento e monitoramento de riscos e eventuais danos, com o objetivo de minimizar ou até mesmo eliminar a possibilidade de impactos negativos sobre objetivo pretendidos, caso alguns dos riscos avaliados venham a se concretizar. Portanto, o gerenciamento de riscos visa reduzir ao mínimo possível os impactos dos riscos sobre a própria organização e terceiros, com a adoção de melhores práticas de infraestrutura, políticas e metodologias, tendo em mente a tecnologia disponível; o custo de implementação; a natureza, escopo, contexto e finalidade das atividades de processamento do controlador de dados; e a probabilidade e magnitude dos riscos envolvidos[2].

Não menos importante, o gerenciamento de riscos é (i) uma ferramenta eficaz a fim de garantir um alto nível de proteção dos direitos e liberdades individuais; (ii) permite que as organizações dediquem seus esforços onde os impactos são mais significativos e mitiguem esses riscos e (iii) promove a inovação, na medida em que permite que as organizações adotem as medidas de proteção de dados necessárias para minimizar o impacto aos indivíduos de suas operações de tratamento nos limites do necessário[3].

Conforme o entendimento do Grupo de Trabalho do Artigo 29[4], grupo europeu independente que lidava com questões relacionadas a proteção de dados[5] antes da entrada em vigor da GDPR, os riscos estão relacionados de acordo com o potencial impacto negativo sobre os direitos e liberdades individuais, e devem ser determinados levando em consideração critérios objetivos.

> Considerando a ampla variedade de tratamento de dados realizados por diferentes tipos de organizações, é importante manter uma flexibilidade em torno da metodologia de análise de risco de modo que as especificidades de cada organização e da natureza dos dados que ela trata possam ser ponderados como parte desse processo de avaliação. Nesse sentido, sugerimos que a ANPD procure adotar - ainda que em caráter orientativo e não normativo - os principais critérios a serem utilizados pelos agentes de tratamento nesse exercício, auxiliando dessa forma agentes menos familiarizados com a proteção de dados e trazendo mais segurança jurídica para o conjunto dos agentes. Tendo em vista a experiência internacional sobre o tema sugerimos que tais critérios incluam as seguintes temáticas:
>
> (i) O tipo de violação *(por exemplo, dependendo do cenário, uma violação da confidencialidade pode ter um impacto maior do que se os dados forem simplesmente perdidos ou apagados);*
>
> (ii) A natureza e sensibilidade dos dados pessoais *(quanto mais sensíveis os dados, maior será o risco de dano para os titulares afetados. De todo modo, aspectos como*

[2] Centre for Information Policy Leadership. The Role of Risk Management in Data Protection, 2014. Disponível em: https://bit.ly/2NZnvMB.
[3] Centre for Information Policy Leadership. Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR, 2016. Disponível em: https://bit.ly/3ulsNNf.
[4] Article 29 Data Protection Working Party. Statement on the role of a risk-based approach in data protection legal frameworks, 2014. Disponível em: https://bit.ly/2PtgWT3
[5] Função hoje desempenhada pelo European Data Protection Board.

se outros dados pessoais do titular já estavam disponíveis quando o incidente ocorreu também devem ser considerados);

(iii) Facilidade de identificação dos indivíduos;

(iv) Gravidade das consequências para os indivíduos *(por exemplo, as violações em que haja provas de agentes maliciosos que tenham acesso aos dados pessoais podem indicar um risco mais elevado do que as violações em que os dados sejam divulgados por acidente);* e

(v) Características especiais do indivíduo afetado *(por exemplo, dados relativos a crianças/outros indivíduos vulneráveis podem levar à classificação do incidente como de maior risco)*.

Um aspecto adicional importante quando se fala da questão de gestão de risco refere-se ao volume de titulares afetados por um determinado incidente. Nesse particular, entendemos importante destacar que não necessariamente um volume maior de titulares afetados implique em um maior risco aos titulares pois será fundamental se considerar os outros fatores envolvidos no caso concreto, tais como a natureza do dado objeto do incidente, o contexto, dentre outros. Em suas orientações, portanto, recomendamos que a ANPD esclareça que o volume de titulares impactados como um critério para avaliar o risco/dano do incidente não deve ser o aspecto primário a ser considerado, e sim um fator em conjunto com tantos outros para permitir uma avaliação precisa da maior ou menor gravidade da situação. Isso é importante pois o número de usuários afetados não necessariamente indicará um aumento na probabilidade de danos que um indivíduo possa sofrer em razão de um incidente de segurança.

É importante que a ANPD compreenda que o fato de ter havido uma violação não significa necessariamente que as medidas de segurança técnicas e organizacionais implementadas pelos agentes de tratamento tenham sido insuficientes. Em outras palavras, um incidente de segurança não deve ser considerado um indicador incontestável de proteção insuficiente dos dados pessoais ou de que uma empresa agiu de forma "irrazoável" ou inadequada. Cada incidente e as medidas de segurança implementadas têm de ser considerados com base em suas próprias peculiaridades.

Como se pode observar, essa premissa vai além do mero cumprimento das exigências legais. Vai ao cerne do que as organizações responsáveis procuram alcançar, como implementar as medidas de proteção de dados e como demonstrar que estão em conformidade com a lei[6]. Temos, portanto, uma premissa importante no arcabouço de proteção de dados pessoais: não se presume que incidentes não irão ocorrer; espera-se, sim, que as empresas tenham adotado todas as medidas razoáveis para evitar que tais incidentes de fato representem um risco ou levem a um dano aos titulares dos dados pessoais.

Cumpre ressaltar que a Autoridade não deverá, no exercício de sua competência legal, decidir no caso concreto se houve ou não risco ou dano ao titular no caso de um incidente de segurança. Para garantir uma maior segurança jurídica, parece-nos recomendável que normativo específico sobre o tema venha a deixar claro tal entendimento decorrente da própria LGPD.

3. CONCEITO DE RISCO E DANO

[6] Centre for Information Policy Leadership. A Risk-based Approach to Privacy: Improving Effectiveness in Practice, 2014. Disponível em: https://bit.ly/3e1Rnm6.

O conceito de risco e dano para o titular dos dados são conceitos próximos mas essencialmente distintos. Podemos interpretar o risco para o titular dos dados como uma definição mais ampla do que a definição de dano efetivo; o que sugere que o dano "potencial" também seria compreendido pela primeira definição, portanto, a definição de "risco" pode ser entendida como "risco de dano". Tanto o "risco" como o "dano" apontam para uma certa gravidade do impacto do incidente sobre os titulares dos dados, sendo identificados antes de serem levantados os requisitos de notificação.

Isto é semelhante a outras jurisdições onde vimos os termos "risco" e "dano" serem utilizados de forma bastante intercambiável. A ANPD poderia procurar tratar o termo "dano" de forma semelhante. Por exemplo:

- No GDPR[7], a notificação de violações aos titulares dos dados afetados deve ser realizada quando uma violação é "suscetível de resultar num elevado risco para os direitos e liberdades das pessoas naturais";

- Na Lei de Privacidade da Austrália[8], a notificação de violações aos titulares dos dados afetados deve ser realizada quando uma "uma pessoa razoável concluir que o [incidente] poderia resultar em sérios danos a qualquer um dos indivíduos aos quais as informações se referem";

- Na Lei de Privacidade da Nova Zelândia[9], a notificação de violações aos titulares dos dados afetados deve ser realizada para qualquer violação de privacidade que seja "razoável acreditar que tenha causado danos sérios a um indivíduo ou indivíduos afetados ou que seja provável que o faça"; e

- Na Lei de Privacidade do Canadá[10], a notificação de violações aos titulares dos dados afetados deve ser realizada quando a violação cria "um risco real de danos significativos para os indivíduos afetados".

Comparativamente a estes fatores desencadeadores de notificação, o Artigo 48 da LGPD estabelece que: "o responsável pelo tratamento deve informar a Autoridade Nacional de Proteção de Dados e o titular dos dados sobre a ocorrência de incidentes de segurança que possam implicar riscos ou danos relevantes para os titulares dos dados".

Tal como nas outras quatro jurisdições acima enumeradas, o Brasil parece ter uma abordagem comum na identificação de um requisito de "probabilidade" ("poderia") paralelamente a um requisito de "gravidade" ("risco ou dano relevante"). Diante disso, entendemos que a ANPD deveria, em um exercício de harmonia e interoperabilidade com os arcabouços existentes, adotar o conceito de “risco” que siga a experiência sedimentada no GDPR e, por outro lado, o conceito de “dano” e fixado nas legislações da Austrália, Nova Zelândia e Canadá quanto ao “risco relevante [de dano]” ou dano” da LGPD. Certamente, tal diferenciação clara dos conceitos facilitará o entendimento de que o “risco” está relacionado quanto a probabilidade de ocorrência de um dano, enquanto o “dano” está relacionado ao impacto negativo de um dano já materializado.

Tal construção interpretativa se assemelha aquela já consolidada na doutrina brasileira no que tange a conceituação de tais figuras no direito civil pátrio.

[7] GDPR. Disponível em: https://bit.ly/3lupdlq.
[8] Privacy Act 1988. Disponível em: https://bit.ly/3cNqgZN.
[9] New Zealand Privacy Act. Disponível em: https://bit.ly/3tFy6eL.
[10] Personal Information Protection and Electronic Documents Act. Disponível em: https://bit.ly/2QomwGL.

4. MODELOS DE FRAMEWORKS

Neste momento de amadurecimento da sociedade brasileira a uma nova cultura de proteção de dados pessoais é ideal para a ANPD exercer sua competência educacional sobre a temática, promovendo a disseminação da cultura de proteção de dados pessoais e trabalhando para a elaboração de guias para auxiliar no processo de adequação de organizações, apontando os agentes de tratamento para modelos de framework de risco existentes e respeitados, garantindo que as organizações estejam gerenciando o risco adequadamente, fazendo referência às melhores práticas e padrões internacionais de gestão de risco, como alguns modelos a seguir:

4.1. NORMAS ISO

O modelo padrão adotado pela norma ISO 31000:2018[11], publicada pela Organização Internacional de Normalização, apresenta um conjunto de diretrizes para a gestão de riscos enfrentados pelas organizações. A aplicação dessas diretrizes pode ser personalizada para qualquer organização e seu contexto, seja, por exemplo, sobre riscos regulatórios, trabalhista, ambientais, segurança da informação ou jurídicos. Tal norma oferece uma abordagem comum para gerenciar qualquer tipo de risco e não é específica para determinada indústria ou setor e, dessa forma, um modelo como a ISO 31000, na medida em que aborda o risco sob a ótica corporativa, poderá também ser ajustada para que as organizações apliquem a norma sob a gestão de risco ao titular de dados.

Nessa mesma linha, a ISO 27001:2013[12], integra um conjunto de políticas, procedimentos e processos que formam o Sistema de Gestão da Segurança e Informação, uma estrutura central que permite às organizações adotar uma consistência para os seus exercícios de gestão de risco e segurança da informação. Esse padrão indica em linhas gerais quais medidas e ferramentas uma organização deve adotar, alinhado com as melhores práticas internacionais, sem apresentar uma lista taxativa.

A ISO 27005:2018[13], por sua vez, dá sustentação aos conceitos aplicados da ISO 27001, formando a espinha dorsal do projeto de conformidade, delineando como as organizações podem identificar os perigos de segurança da informação que enfrentam, priorizar suas maiores ameaças e selecionar um curso de ação apropriado. Este processo revela quando é apropriado realizar a criptografia de dados, por exemplo, bem como onde as organizações devem reforçar seus processos organizacionais ou outras defesas técnicas e também contém passos que as organizações podem tomar para lidar com a resiliência cibernética, o que as ajudará a proteger processos comerciais críticos.

4.2. NIST PRIVACY FRAMEWORK

O NIST *Privacy Framework*, desenvolvido pelo *US National Institute of Standards and Technology's*, elaborado em colaboração com uma série de organizações, oferece um conjunto de ferramentas para viabilizar uma estratégia de privacidade para as organizações que desejam

[11] International Organization for Standardization.. ISO 31000:2018 Risk management — Guidelines, 2018. Disponível em: https://bit.ly/3bTKdPE.
[12] International Organization for Standardization. ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements, 2013. Disponível em: https://bit.ly/3rVkrzT.
[13] International Organization for Standardization. ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management, 2018. Disponível em: https://bit.ly/3qPlP5L.

aprimorar sua forma de utilizar a proteger os dados pessoais; também oferece detalhadamente explicações sobre conceitos de gerenciamento de risco[14].

O NIST não se trata necessariamente de uma lei ou regulação do setor, mas sim uma ferramenta de uso voluntário que pode ajudar as organizações a melhor gerenciarem seus produtos e serviços que afetem indivíduos, a melhor forma de como comunicar suas práticas relacionadas à privacidade, assim como demonstrar o cumprimento de leis que possam afetá-las, como por exemplo o Regulamento Geral sobre a Proteção de Dados (GDPR).

Tendo em vista a natureza global das cadeias de valores em inúmeros setores econômicos, recomendamos a ANPD que ofereça flexibilidade para que as organizações adotem as melhores práticas já internacionalmente disseminadas, escolhendo aquela que mais se aproximar do negócio da empresa, a volumetria e a natureza dos dados coletados.

4.3. METODOLOGIA DA ENISA (2013)[15]

No contexto de DANO e RISCO, acreditamos que a metodologia sugerida pela Agência da União Europeia para a Cibersegurança possa ser uma referência para a ANPD e um guia para os controladores, pois nela são levados em consideração alguns critérios ao avaliar a gravidade de uma violação de dados pessoais como:

- Contexto de processamento de dados: aborda o tipo de dados violados, juntamente com uma série de fatores vinculados ao contexto geral de processamento;

- Facilidade de identificação: determina a facilidade com que a identidade dos indivíduos pode ser deduzida dos dados envolvidos na violação; e

- Circunstâncias de violação: que avalia as circunstâncias específicas da violação, que estão relacionadas ao tipo de violação, incluindo principalmente a perda de segurança dos dados violados, bem como qualquer intenção maliciosa envolvida.

As recomendações incorporadas nesses diversos *framework* de segurança da informação devem ser consideradas não só na sistematização dos processos de gestão de risco mas também como balizadores para a avaliação de situações de incidente de segurança. Notamos que a metodologia ao fim da avaliação preliminar considera outros dois parâmetros que podem atenuar ou acentuar a gravidade de suposta violação, tais como a quantidade de pessoas atingidas e a ininteligibilidade.

As metodologias acima listadas são construídas com um caráter voluntário, não sendo obrigatórias para as organizações, mas sendo consideradas melhores práticas internacionais e comumente disseminadas como o estado da arte em segurança da informação. Entendemos que a ANPD deverá em seus guias orientativos estimular que frameworks dessa natureza sejam efetivamente utilizados pelas organizações como uma forma de atendimento das obrigações fixadas no artigo 46 da LGPD.

5. PRAZO DE COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA

[14] National Institute of Standards and Technology. NIST Privacy Framework: a tool for improving privacy through enterprise risk management, 2020. Disponível em: https://bit.ly/3kliRP8.
[15] ENISA, Recommendations for a methodology of the assessment of severity of personal data breaches, Working Document, v1.0, December 2013.

O artigo 48 da LGPD indica que a comunicação sobre o incidente de segurança deverá ser comunicada tanto para o titular dos dados pessoais quanto para a ANPD em prazo razoável a ser definido pela autoridade. Enquanto a regulamentação ainda se encontra pendente, o site da ANPD recomenda que a comunicação seja realizada no prazo de 2 dias úteis, contados a partir da data do conhecimento do incidente[16].

Entendemos que o formulário atualmente disponível no site da ANPD foi desenvolvido em caráter transitório para auxiliar a sociedade em um momento em que inúmeros incidentes de segurança vêm sendo revelados e a ANPD ainda não teve a oportunidade de desenvolver instrumento normativo próprio sobre o tema.

Nesse sentido, aproveitamos para apresentar alguns exemplos do cenário internacional no que diz respeito a esse tipo de comunicação para explorar alguns caminhos que deverão ser examinados pela ANPD como referência para a adoção do normativo pátrio.

5.1. EUROPA - Regulamento Geral sobre a Proteção de Dados (GDPR)

O Regulamento Geral sobre a Proteção de Dados (GDPR)[17], no seu artigo 33 indica que, no caso de um incidente de dados pessoais, os controladores de dados devem notificar a autoridade de supervisão competente sem demora indevida e, quando possível, em até 72 horas após terem tomado conhecimento do incidente, a menos que este não resulte em risco para os direitos e liberdades dos indivíduos. Quando a notificação à autoridade de supervisão não for feita dentro de 72 horas, ela deverá ser acompanhada dos motivos do atraso. De acordo com um estudo realizado pela DLA Piper[18], de 25 de maio de 2018 a 27 de janeiro de 2020, houve um total de 160.921 violações de dados pessoais notificadas por organizações às autoridades de supervisão de proteção de dados dentro da União Europeia.

5.2. ESTADOS UNIDOS

O modelo norte-americano de proteção de dados pessoais é bastante distinto daquele adotado no Brasil e nas demais jurisdições inspiradas na estrutura europeia. Ainda assim, vale observar o caminho adotado por alguns estados americanos no sentido de editar normativas específicas justamente para estabelecer critérios relativos à comunicação de incidentes de segurança.

Alguns estados americanos adotam um modelo pelo qual se fixa um patamar mínimo de titulares afetados para gerar a obrigação de comunicação do incidente de segurança ao órgão competente, como no caso do estado do Colorado[19], Delaware[20] e Illinois[21], onde, ocorrendo um incidente de segurança que afete 500 ou mais indivíduos residentes desses estados, a organização deverá notificar o escritório do respectivo procurador-geral. Vale lembrar que a sistemática da legislação americana é estruturada de uma maneira diferente do Brasil.

Para incidentes de segurança envolvendo dados pessoais sensíveis de saúde, um exemplo notável é o do *Health Insurance Portability and Accountability Act* (HIPAA)[22], lei federal que apresenta um conjunto de normas para a proteção de dados voltado a organizações de saúde norte-americanas, que adota dois caminhos: (i) se o incidente afetar 500 ou mais

[16] Incidentes de segurança com dados pessoais e sua avaliação para fins de comunicação à ANPD. GOV.BR, 2021. Disponível em: https://bit.ly/203VkMH.
[17] Regulamento Geral sobre a Proteção de Dados. Disponível em: https://bit.ly/3rPsu0Y.
[18] DLA Piper. GDPR data breach survey, 2020. Disponível em: https://bit.ly/3bC6yRt.
[19] Colo. Rev. Stat. § 6-1-716.
[20] Del. Code tit. 6, § 12B-101 et seq.
[21] 815 Ill. Comp. Stat. 530/5, 530/10, 530/12, 530/15, 530/20, 530/25.
[22] Health Insurance Portability and Accountability Act. Disponível em: https://bit.ly/3l7DMeH.

indivíduos, a organização deverá notificar a Secretaria do Departamento de Saúde e de Serviços Humanos dos Estados Unidos sem atraso injustificado e em nenhum caso depois de 60 dias corridos a partir da descoberta do incidente; ou (ii) se a incidente afetar menos de 500 indivíduos, a organização deverá notificar a Secretaria dentro de 60 dias a partir do final do ano-calendário em que foi descoberta.

Esse modelo setorial nos EUA traz uma referência bastante interessante no sentido de poder ajudar a gerenciar o fluxo de incidentes de segurança envolvendo dados pessoais sensíveis de saúde encaminhados à ANPD, estabelecendo um montante de referência de titulares afetados para se aplicar a obrigação de comunicação. Tal número, se adotado para dados pessoais sensíveis de saúde, precisará considerar o tamanho da população brasileira bem como a natureza transversal da obrigação, não sendo fixada para um único setor econômico.

Nessa estrutura, os incidentes de segurança de menor impacto não deverão ser desconsiderados mas sim compilados em uma única comunicação ao final do período de 12 meses, permitindo assim a autoridade ter um conhecimento da maturidade de segurança e proteção de dados pessoais sensíveis de saúde do país, acompanhar o amadurecimento individual das organizações e estabelecer um fluxo de informações e obrigações menos oneroso e mais eficiente tanto para as organizações que tratam dados pessoais sensíveis de saúde quanto para à ANPD.

5.3. AUSTRÁLIA - *Australian Privacy Act*

O *Australian Privacy Act*[23], lei de proteção de dados australiana, exige que as organizações realizem uma avaliação sobre o risco efetivo do incidente dentro de 30 dias após terem tomado conhecimento de que possa ter havido uma violação, devendo notificar a autoridade australiana e os titulares de dados pessoais afetados após a confirmação de que o incidente apresenta um risco de danos graves para os indivíduos afetados, a causa ou fonte, o tipo de dado pessoal que foi acessado ou divulgado, e o número de indivíduos que estavam em risco de danos graves como resultado do incidente.

5.4. CANADÁ - *Personal Information Protection and Electronic Documents Act* (PIPEDA)

O *Personal Information Protection and Electronic Documents Act* (PIPEDA)[24], lei de proteção de dados canadense, também exige que o controlador realize a comunicação assim que possível, logo após determinar que um incidente, que represente um risco real de dano significativo ao titular, ocorreu.

Os fatores relevantes elencados para auxiliar a determinar que um incidente apresenta um risco real de dano, de acordo com o PIPEDA são (i) o nível de sensibilidade dos dados pessoais envolvidos no incidente e (ii) a probabilidade de que tais dados tenham sido, estejam sendo ou venham a ser utilizados indevidamente. Já no que se refere ao dano significativo ao titular, os fatores considerados na lei incluem danos corporais, humilhação, danos à reputação, perda de emprego, oportunidades comerciais ou profissionais, perda financeira, roubo de identidade, efeitos negativos no registro de crédito e danos ou perda de propriedade.

[23] Australian Privacy Act. Disponível em: Disponível em: https://bit.ly/2ODkMIN.
[24] Personal Information Protection and Electronic Documents. Disponível em: https://bit.ly/3l9IlQm.

5.5. BRASIL - Considerações para a ANPD

Como pode ser observado, cada uma dessas leis, regulamentos e/ou normas setoriais apresentam prazos distintos para a comunicação do incidente de acordo com o grau de maturidade de proteção de dados desses países. O dever de ter que notificar açodadamente, ou seja, em curto espaço de tempo, à ANPD pode acarretar inúmeras notificações de meras ameaças ou de incidentes que, embora confirmados, não geram risco ou dano relevante aos titulares, além de sobrecarregar a autoridade prejudicando sua eficiência nas investigações que realmente merecem sua atenção.

Em meados de 2020, foi publicado um relatório pelo "Grupo de Especialistas Multissetoriais para a Avaliação do GDPR" que identificou que tem havido uma tendência entre as organizações de sobre-notificação de violações de dados, o que resultou em autoridades de proteção de dados locais sendo sobrecarregadas com notificações. Considerando a atual estrutura enxuta da ANPD, este é um ponto de séria preocupação e instamos a regulamentação futura a considerar critérios para que a ANPD se concentre nos casos mais relevantes, em vez de receber todas e quaisquer notificações de incidentes de segurança de dados pessoais.

Há que se considerar que muitas vezes pode haver apenas a mera suspeita de um incidente, que, porém, precisa de mais tempo para ser investigado de modo que haja sua confirmação ou não, dessa forma, a comunicação em duas etapas, a notificação prévia para a ANPD informando a suspeita de um incidente, seguido do prazo após sua confirmação, proporciona fôlego para que as organizações possam envidar seus melhores esforços para uma investigação aprofundada do incidente.

Nesse sentido, com relação aos incidentes que devem ser notificados, a ANPD, seguindo, por exemplo, os moldes da legislação canadense, poderia estabelecer os critérios ali apresentados como balizadores de incidentes de segurança que ensejam um risco ou dano relevante aos titulares, conforme exigido no *caput* artigo 48 da LGPD e, por consequência, indicar que seriam casos efetivos de notificação à ANPD e aos titulares.

Caso o controlador seja informado que é necessário realizar tal notificação, após preencher o questionário, a disponibilização de um formulário simplificado elaborado pela ANPD seria fundamental para permitir uma maior agilidade na submissão da comunicação pelos controladores, o qual deverá solicitar apenas informações objetivas e pertinentes ao incidente de segurança com dados pessoais a ser notificado.

Além disso, considerando que a análise e avaliação de riscos são processos que demandam bastante tempo para serem bem executados, é possível afirmar que o prazo sugerido de 2 dias úteis para notificar um incidente seria bastante oneroso e na prática pouco efetivo, pois muitas vezes o agente de tratamento ainda está procurando entender o que de fato ocorreu.

Nesse sentido, tendo em vista as dificuldades práticas que as empresas enfrentam nos primeiros dias após tomar conhecimento de um incidente de segurança, bem como o volume de incidentes ou suspeitas de incidentes que as organizações enfrentam diariamente, sugerimos uma alternativa faseada para que a comunicação de incidentes seja feita à Autoridade, conforme segue.

A organização que identifica um incidente de segurança deverá, no prazo de 3 dias úteis a contar da tomada de conhecimento concreto do incidente, enviar o que estamos chamando de uma notificação preliminar a ANPD, informando que foi detectado um incidente e que a empresas está trabalhando para identificar se de fato esse incidente afetou dados pessoais e tem o potencial de gerar riscos ou danos aos titulares de dados.

Tal notificação deverá ser feita em um formulário simplificado, permitindo assim a Autoridade monitorar os incidentes existentes e não onerando as organizações enquanto ainda estão buscando entender o ocorrido e adotar as medidas de mitigação necessárias. Uma referência interessante de citar refere-se à ferramenta criada pela Agência Espanhola de Proteção de Dados[25]. Disponibilizada no próprio site da Agência, em espanhol e em inglês, os controladores podem preencher, de forma anônima, um questionário com mais informações a respeito de incidentes de segurança com dados pessoais. A partir das respostas apresentadas, e com base em critérios pré-estabelecidos, a ferramenta indica para o controlador se o incidente deve ser notificado ou não. Sugerimos que a ANPD desenvolva algo no mesmo sentido, entendendo que tal ferramenta será muito útil em auxiliar as organizações a entenderem quais medidas devem ser adotadas.

Uma segunda etapa seria a efetiva comunicação do incidente à Autoridade, decorridos até 30 dias da notificação preliminar, e em um momento em que o controlador pode, de fato, afirmar se há potencial de risco ou dano ao titular do dado. É crucial garantir que as notificações submetidas à ANPD contenham informações precisas e sejam referentes apenas a incidentes relevantes, para evitar um sobrecarregamento do pessoal da autoridade.

Se o prazo for muito curto, conforme sugerido no formulário ora disponibilizado no site, a ANPD corre o risco de ser inundada com muitos incidentes pouco relevantes e não será capaz de se concentrar nos incidentes de maior relevância, causando atrasos desnecessários e prejudicando o bom desempenho da autoridade. O excesso de notificação também gerará um impacto negativo para os titulares, inicialmente alarmando-os indevidamente quanto aos impactos do incidente (e incitando suposições erradas em relação a algumas empresas), além de sujeitá-los a correr o risco de ignorar/perder aqueles incidentes que realmente representariam motivos de preocupação e gerariam a necessidade de tomar medidas.

Em adição ao prazo de 30 dias para a comunicação detalhada do incidente a ANPD, sugerimos que o mesmo prazo seja fixado para a comunicação do incidente aos titulares dos dados pessoais, caso necessária. Importante frisar que a comunicação ao titular dos dados sobre um incidente não deve ser exigida em toda e qualquer ocorrência sob pena de se gerar uma banalização de tais notificações, levando a sintoma similar àquele que se convencionou chamar de fadiga do consentimento. Algo que se faz o tempo muitas vezes deixa com que os titulares considerem com a atenção e seriedade que de fato demandam.

Por fim, gostaríamos de enfatizar que a privacidade, a segurança da informação e a confiança no ambiente digital são preocupações primordiais de nossos associados. A proteção de dados de nossos clientes e de sua privacidade em geral são essenciais para ganhar a confiança dos cidadãos em um mercado tecnológico global. Naturalmente, é de interesse das organizações parte do ecossistema de adotar medidas técnicas e organizacionais para gerenciar e analisar riscos, assim como para mitigá-los. Similarmente, a transparência com a ANPD e os titulares de dados é fundamental para nossos negócios e, portanto, prazos mais extensos para submissão de notificação permitirão com que os controladores tenham informações mais detalhadas sobre os incidentes de segurança que possam causar risco ou dano relevante e, consequentemente, farão com que as notificações sejam mais robustas e esclarecedoras possíveis, destacando todos os seus aspectos de interesse.

6. MECÂNICA DA REGRA DA COMUNICAÇÃO DE INCIDENTES

[25] AEPD. Comunica-Brecha RGPD. Disponível em: https://bit.ly/2P428Kt.

Sugerimos à ANPD que estabeleça algumas exceções à obrigatoriedade da notificação, especialmente em casos nos quais o controlador tenha comprovadamente implementado medidas de segurança apropriadas.

A Lei de Proteção de Dados da Irlanda[26] traz uma estrutura interessante para a implementação de proposta nesse sentido. De acordo com tal arcabouço, o controlador não é obrigado a notificar um incidente de segurança com dados pessoais quando ele tiver implementado medidas de proteção tecnológica e organizacional adequadas que foram aplicadas aos dados pessoais afetados pelo incidente, em particular quando as referidas medidas, incluindo a criptografia, tornam os dados pessoais ininteligíveis para qualquer pessoa que não esteja autorizada a acessá-lo, ou até mesmo quando tiver tomado medidas em resposta ao incidente de segurança com dados pessoais que garantem que o elevado risco para os direitos e liberdades do titular em causa decorrente da violação já não é provável de se concretizar.

Desse modo, incidentes que não forem comunicados à ANPD deverão ser devidamente documentados pelas instituições, incluindo relatório de impacto à proteção de dados pessoais, a fim de que seja comprovado o cumprimento dos preceitos da LGPD. Tal prática está de acordo com os padrões globais de privacidade, incluindo o GDPR (Artigo 33).

6.1. CANAIS DE COMUNICAÇÃO TITULAR

Tendo em vista o caráter transversal da LGPD, aplicável a todas as organizações que tratam dados pessoais, independente de seu tamanho ou setor de atuação, entendemos que a normatização da lei deverá ser cuidadosa no sentido de estabelecer critérios flexíveis que possam ser atendidos por entidades dos mais diversos portes e natureza.

No que tange a possível necessidade de comunicação de um incidente de segurança aos titulares de dados atingidos por um incidente de segurança, entendemos que será importante que a norma venha a esclarecer que a organização responsável deverá escolher, de maneira autônoma, a forma pela qual a comunicação deverá ser implementada ao titular do dado.

Uma norma que permita que o meio de comunicação seja escolhido pelo controlador permitirá uma melhor gestão das informações e um melhor atendimento das expectativas dos titulares. Preocupa-nos que uma obrigação muito rígida de comunicação a LGPD poderá levar a experiência similar àquela que se convencionou fadiga de consentimento. Dito de outra forma, tantas serão as comunicações recebidas por um titular que de nada valerão pois serão vistas de maneira banalizada pelo titular de dados pessoais.

Portanto, a comunicação de incidentes de segurança aos titulares deve ser definida pelas próprias empresas e organizações, de modo que seja possível uma avaliação caso a caso, considerando a natureza da atividade da empresa, o contexto da coleta e do próprio incidente de segurança, a natureza dos dados pessoais objeto do incidente, o volume dos dados, dentre outros aspectos. Por exemplo:

(i) Se o número de titulares afetados for inferior a um determinado número, o controlador poderá optar por notificar de forma individualizada.

(ii) Se for muito difícil encontrar as informações de contato de todos os titulares envolvidos, ou se o número de titulares afetados atingir um limite onde seja muito

[26] Irlanda, Data Protection Act 2018. Disponível em: https://bit.ly/3f3wVBM.

trabalhoso notificá-los individualmente, a organização pode optar por criar avisos em seus respectivos sites, ou até mesmo optar pela divulgação do fato em outros meios de comunicação.

6.2. CONTEÚDO DA COMUNICAÇÃO AOS TITULARES IMPACTADOS

Conforme mencionado anteriormente, o artigo 48 da LGPD traz o dever de comunicação de incidentes de seguranças tanto a ANPD como aos titulares dos dados pessoais possivelmente afetados pelo incidente.

Embora a lei não antecipe os contornos e diferenças nessas comunicações, entendemos que o arcabouço normativo a ser editado pela ANPD deverá fazê-lo. O nível de detalhes fornecidos aos titulares dos dados pessoais não deve ser o mesmo que o fornecido à ANPD, e deve ser flexível para atender às necessidades específicas de cada tipo de incidente. Essa mesma abordagem é preceituada no GDPR em seu artigo 34(2)[27] e outras leis de privacidade. Os controladores não devem ser obrigados a revelar todos os detalhes específicos do número de pessoas afetadas para todas as pessoas afetadas, mas, em vez disso, eles devem apenas revelar as categorias de pessoas afetadas (por exemplo, se clientes, funcionários foram afetados etc.); também seria inadequado (e arriscaria futuros incidentes) que os controladores tivessem que compartilhar os mesmos detalhes em torno de suas "medidas técnicas e de segurança" que compartilham com a ANPD.

As organizações estão frequentemente mais bem posicionadas para saber como se comunicar com usuários/titulares de dados e podem ter suas próprias formas de efetuar tais comunicações, respeitando até mesmo o linguajar e estilo de comunicação de cada agente de tratamento com seu público-alvo.

Portanto, sugerimos que a ANPD adote os princípios fixados na LGPD, em especial o de responsabilidade e prestação de contas e permita as organizações flexibilidade para a determinação da melhor forma de atender o dispositivo legal com transparência e responsabilidade.

6.3. FORMULÁRIO DE COMUNICAÇÃO INCIDENTE DE SEGURANÇA

Entendemos que o formulário atualmente disponível no site da ANPD foi desenvolvido em caráter transitório para auxiliar a sociedade em um momento em que inúmeros incidentes de segurança vêm sendo revelados e a ANPD ainda não teve a oportunidade de desenvolver instrumento normativo próprio sobre o tema. De toda forma, gostaríamos de listar alguns pontos problemáticos da versão atual do documento, como uma forma de sugerir que essas questões sejam endereçadas durante a elaboração de futuro formulário definitivo:

1) Exigência de CPF/CNPJ: o formulário atual exige que o notificante apresente um número de CPF ou de CNPJ. Exigir essas informações pode impedir que empresas estrangeiras não estabelecidas no país, mesmo que sujeitas à LGPD, submetam notificações de incidentes de segurança;

2) Operador como comunicante: de acordo com o artigo 48 da LGPD, o controlador é o único agente de tratamento responsável por comunicar quaisquer incidentes de segurança. Sendo assim, entendemos que o operador não pode se configurar como

[27] Art. 34(2) A comunicação ao titular dos dados a que se refere o n. o 1 do presente artigo descreve em linguagem clara e simples a natureza da violação dos dados pessoais e fornece, pelo menos, as informações e medidas previstas no artigo 33. o , n. o 3, alíneas b), c) e d).

notificante e, portanto, deve-se presumir que todas as notificações submetidas foram realizadas por controladores.

3) Lista extensa sobre a natureza de dados afetados: no momento da comunicação, o controlador dificilmente terá a visibilidade de todos os tipos de dados pessoais afetados, pois esse levantamento será realizado durante o processo de análise e avaliação de riscos. Portanto, sugerimos que ao perguntar qual a natureza dos dados afetados, tenham apenas duas opções: (i) dados pessoais; e (ii) dados pessoais sensíveis.

4) Medidas de segurança: no momento da notificação, entendemos que seja fundamental que o controlador indique apenas as medidas de segurança que foram ou serão adotadas para mitigar os riscos ou danos atrelados ao incidente de segurança em questão. Isso porque é de nosso entendimento que todas as medidas técnicas e organizacionais de segurança compõem a estrutura de gestão de risco e são, portanto, muito complexas para serem apresentadas exaustivamente em uma notificação.

5) Confidencialidade: a ANPD deve deixar claro que todas as informações fornecidas pelos controladores nos formulários de notificação não serão publicizadas, tendo em mente os possíveis prejuízos em termos de reputação das organizações envolvidas.

7. ELABORAÇÃO DE ORIENTAÇÕES SOBRE INCIDENTES DE SEGURANÇA

Tendo em vista o estágio inicial da adoção da proteção de dados pessoais como direito fundamental e a disseminação da cultura de proteção de dados no país entendemos ser um passo importante e necessário a ANPD divulgar orientações para os agentes de tratamento de dados pessoais e os titulares com relação a definição de critérios para a gestão de risco necessária para a decisão com relação a comunicação de incidente de segurança nos termos da lei.

Um exemplo do que tem sido adotado no cenário internacional é o que recentemente o Comitê Europeu de Proteção de Dados realizou em janeiro de 2021, em que divulgou uma orientação sobre incidentes de segurança[28]. Nele discute-se diversos casos hipotéticos em que são analisadas quais medidas o controlador deveria ter adotado preliminarmente para oferecer o produto e/ou serviço, as medidas de mitigação e a obrigatoriedade de comunicar ou não a autoridade de proteção de dados, baseado na análise de risco ou dano aos titulares de dados.

Seguindo esse mesmo caminho, a Agência da União Europeia para a Cibersegurança (ENISA), centro especializado que promove a cibersegurança na Europa, elaborou, em janeiro de 2018, um guia[29] com o objetivo de orientar as empresas para o tratamento de dados pessoais na implementação do GDPR, no qual o controlador deve avaliar o impacto sobre os direitos e liberdades fundamentais dos titulares, resultantes da possível perda de segurança dos dados pessoais. Quatro níveis de impacto são considerados (Baixo, Médio, Alto, Muito Alto):

- Baixo: Inconvenientes leves que serão superados sem nenhum problema (tempo gasto reinserindo informações, aborrecimentos etc.);

[28] European Data Protection Board. Guidelines 01/2021 on Examples regarding Data Breach Notification, 2021. Disponível em: https://bit.ly/3bSgbuo.
[29] European Union Agency for Cybersecurity. Handbook on Security of Personal Data Processing, 2018. Disponível em: https://bit.ly/3t4rzu4.

- Médio: Inconvenientes razoáveis, que serão superados, apesar de algumas dificuldades (acesso negado a serviços comerciais, falta de compreensão, estresse, custo extra etc.);

- Alto: Inconvenientes expressivos, que serão superados, apesar de sérias dificuldades (dano patrimonial, perda de emprego, perda reputacional, agravamentos da saúde física e mental, nome sujo nos serviços de crédito etc.); e

- Muito alto: Consequências graves e até mesmo irreversíveis (inabilidade para trabalhar, danos físicos ou mentais permanentes ou de longo-prazo, morte etc.).

Por fim, a Agência Espanhola de Proteção de Dados[30] elaborou um guia prático para a gestão e comunicação de incidentes de segurança com objetivo de simplificar a interpretação do GDPR e auxiliar as organizações sobre a importância da gestão, tratamento e solução desses tipos de incidentes, assim como as medidas para sua prevenção, contendo uma (i) lista de mecanismos para detecção e identificação de possíveis violações, (ii) os tipos de violações de acordo com sua gravidades e (iii) um plano de ação de acordo com o número de titulares afetados e os processos que precisam ser levados para a comunicação perante a Agência[31].

Neste sentido, importante que a ANPD adote um guia orientativo para os agentes de tratamento de dados e que possam ser utilizados de referência - no processo de disseminação da cultura de proteção de dados no Brasil - para que organizações fiquem atentas para as medidas técnicas e administrativas que poderão adotar para demonstrar que estão em conformidade com a lei, assim como eventuais exemplos e hipóteses que devem ser olhadas com cautela por potencialmente se configurarem como um incidente de segurança.

Esse guia orientativo de medidas técnicas e administrativas pode ser bastante simples, mas ajudarão as organizações que estão dando seus primeiros passos na mudança de cultura com relação a proteção de dados e segurança da informação, tais como documentação de fluxo de dados, controles de acesso físico e digital, capacitação, treinamento e conscientização de colaboradores; dentre outros.

CONSIDERAÇÕES FINAIS

Esperamos que a visão prática e consequência da experiência de nossos associados com a experiência da implantação da cultura de proteção de dados e a legislação específica sobre esse tema em outras jurisdições ajude a trazer elementos para ajudar o importante papel da ANPD na normatização do tema de incidentes de segurança no Brasil.

Como forma de facilitar a compressão deste documento, apresentamos abaixo, de forma resumida, as recomendações desenvolvidas ao longo do texto para a tomada de subsídios proposta pela ANPD:

(i) Estabelecer, de forma clara, a diferença entre o termo incidente de segurança (evento adverso identificado que pode prejudicar os ativos de uma organização) do termo incidente de segurança com dados pessoais (evento adverso identificado que possa ocasionar risco e/ou dano para os direitos e liberdades do titular dos dados pessoais);

[30] AEPD. Guía para la gestión y notificación de brechas de seguridad. Disponível em: https://bit.ly/3e01DPm.
[31] Como exemplos ilustrativos, o guia apresenta critérios e valores para a criação de um cálculo sobre a classificação separado por: tipo de violação, descrição, origem, gravidade e volume aproximado de afetados.

(ii) Estabelecer os critérios a serem considerados em torno da metodologia da análise de risco para fins de determinação dos incidentes de segurança que deverão efetivamente ser comunicados, que podem incluir: (i) o tipo de violação, (ii) a natureza e sensibilidade dos dados pessoais, (iii) facilidade de identificação dos indivíduos, (iv) gravidade das consequências para os indivíduos e (v) características especiais dos indivíduos afetados;

(iii) Adotar conceitos de risco e dano claros para o contexto específico de incidente de segurança, respeitando o ordenamento jurídico pátrio e se beneficiando das experiências internacionais na temática de proteção de dados pessoais de modo a garantir uma interoperabilidade e harmonia entre os vários arcabouços de proteção de dados existente;

(iv) Estimular a utilização pelos agentes de tratamento de dados de framework globalmente reconhecidos no gerenciamento de risco para servir como uma forma de atendimento das obrigações previstas no artigo 46 da LGPD;

(v) Estabelecer que o prazo de notificação para a ANPD em até 3 dias úteis para que seja feita, na primeira etapa, a notificação preliminar sobre a ocorrência do incidente e, na segunda etapa, a efetiva comunicação do incidente decorridos 30 dias da notificação preliminar, garantindo informações precisas sobre o incidente;

(vi) Estabelecer exceções para a obrigação de notificar a ANPD quando o controlador comprovadamente tenha implementado as medidas de segurança apropriadas e não tiver havido risco ou dano ao titular dos dados;

(vii) Permitir que as organizações tenham flexibilidade sobre quais canais utilizam para comunicar os titulares dos dados pessoais atingidos por um incidente de segurança;

(viii) Esclarecer procedimentos e granularidade distintos para a comunicação sobre incidente de segurança aos titulares dos dados pessoais e à ANPD;

(ix) Ajustar o formulário de comunicação de incidente de segurança disponível no site da ANPD para (i) permitir que empresas estrangeiras submetam notificações à ANPD, (ii) excluir o operador como notificante, em respeito ao artigo 48 da LGPD, (iii) simplificar a lista sobre a natureza de dados afetados, (iv) permitir que o controlador apresente tão somente as medidas adotadas para mitigar os riscos/danos atrelados ao incidente e (v) garantir a confidencialidade do formulário com relação a terceiros;

(x) Elaboração de guias práticos ilustrativos como forma de orientar organizações de todos os tamanhos para que elas possam ter um balizador para o gerenciamento de riscos;

(xi) Elaboração de manuais exemplificativos de incidentes de segurança e elaboração do roteiro do exercício que deverá ser feito pelas organizações para verificar o melhor caminho para o atendimento da legislação.

Tendo em vista o exposto, claro está que os desafios diante da ANPD não são pequenos. Para que a Autoridade tenha uma história de sucesso na implementação da LGPD é fundamental que se tenha em mente que a normatização da LGPD deverá estar sempre pautada pela premissa de gestão de risco estruturante da legislação de proteção de dados no Brasil e em tantas outras jurisdições.

A norma não deverá tirar das organizações a autonomia - e a responsabilidade - de fazer o exercício de risco em cima de sua realidade e daí fixar as maneiras mais apropriadas para, naquele contexto, honrar com os princípios e direitos que emanam da LGPD. É fundamental, portanto, não estabelecer uma lista exaustiva de condutas, eis que fundamental permitir que as organizações, independentemente de seus tamanhos, possam fazer esforços proporcionais aos seus orçamentos e aos riscos atrelados aos seus respectivos modelos de negócio, tendo em mente a natureza, escopo, contexto e finalidade de suas atividades de tratamento, o que, inclusive, incentiva o desenvolvimento tecnológico, a inovação e a proteção aos direitos do titular dos dados pessoais.

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: Brotto e Campelo Advogados

CPF/CNPJ: 22.772.212/0001-20

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS **IMPORTANTE:** Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	Em primeiro lugar, antes de adentrarmos em questões relacionadas ao que seria um incidente que traria um "risco" ou "dano" relevante ao Titular, devemos primeiro entender qual seria a definição de um "incidente". A Lei Geral de Proteção de Dados ("LGPD" ou "Lei n.13.709/2018") no tocante ao assunto não traz uma definição clara do que seria um incidente de segurança focando apenas em termos genéricos como "dano" ou "risco". Nesse sentido, de forma a termos um comparativo do que poderia ser um incidente de segurança por normas similares internacionalmente, o Regulamento Geral de Proteção de Dados Europeu (GDPR) descreveria um "incidente" como uma *"uma violação da segurança que provoque, de modo acidental ou ilícito,* ***a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados****, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento"* no Artigo 4(12). Deve-se ter claro que a violação de dados pessoais é apenas um tipo de incidente de segurança. Enquanto todas as violações de dados pessoais são incidentes de segurança, nem todos os incidentes de segurança são necessariamente violações de dados pessoais (neste sentido: ISO 27701 - 6.13.1.5; Article 29 Working Party WP250rev.01). É a partir desta diferenciação fundamental em que se poderá avaliar se há subsunção do incidente em concreto à norma legal em abstrato da LGPD (a exemplo da subsunção nos "tipos penais", no direito penal, e no "fato gerador", no direito tributário), que é o dever de comunicação à ANPD e/ou titulares. Internacionalmente, a diferenciação se dá sob as nomenclaturas "*security incident x data breach*", sendo que somente o segundo possui efeitos jurídicos no âmbito da regulamentação de proteção de

	dados pessoais no sentido de comunicação/notificação. O incidente de violação de dados pessoais, isto é, que possa acarretar risco ou dano relevante ao titular, será aquele que impacte ao menos um dos pilares da reconhecida tríade da Segurança da Informação – confidencialidade, integridade e disponibilidade -, mas afeta exclusivamente à categoria “dado pessoal”. Seguindo tal raciocínio, um incidente que causaria dado ou traria risco ao titular é qualquer um que ponha em xeque a confidencialidade, integridade e disponibilidade dos seus dados pessoais. Logo, a definição do Artigo 4(12) da GDPR abrange diversas hipóteses de situações que poderiam abarcar uma violação aos dados pessoais de um Titular. O que se entende por “destruição” de dados pessoais seria uma situação em que o dado deixa de existir, ou deixa de existir em uma forma que seja útil para o controlador. O “alteração ou dano”, não confundir com o dano jurídico que estamos discutindo aqui, previsto no dispositivo se refere a dados pessoais que foram alterados, corrompidos ou não estão mais completos. Já o termo “perda” de dados pessoais, deve ser interpretado como os dados ainda podem existir, mas o controlador perdeu o controle ou acesso a ele ou não o possui mais. Finalmente, não autorizado ou ilegal seria o processamento que pode incluir a divulgação de dados pessoais para (ou acesso por) destinatários que não estão autorizados ara receber (ou acessar) os dados, ou qualquer outra forma de processamento que viole a legislação europeia. Não obstante, em seu Parecer 03/2014 sobre notificação de violação, WP29 explicou que as violações podem ser categorizadas de acordo com os três principais princípios de segurança da informação, como já explicamos acima: confidencialidalidade, integridade e disponibilidade. • Violação de confidencialidade - onde houver uma divulgação não autorizada ou acidental ou de acesso a dados pessoais. • Violação de integridade - onde há uma alteração não autorizada ou acidental de dados pessoais. • • Violação de disponibilidade" - onde houver uma perda acidental ou não autorizada de acesso a, ou destruição de dados pessoais. Logo, um incidente de segurança em relação a dados pessoais coloca em risco quando há a **probabilidade de haver uma violação** a um dos princípios elencados acima, e causa danos quando as hipóteses elencadas a cima se concretizão (há perda, alteração, destruição ou/e divulgação dos dados pessoais do titular), **o que levaria ao dano físico, material ou imaterial ao Titular**.

	No que tange ao dano, a GDPR explica que isso pode incluir perda de controle sobre seus dados pessoais, limitação de seus direitos, discriminação, roubo de identidade ou fraude, perda financeira, reversão não autorizada de pseudonimização, danos à reputação e perda de confidencialidade de dados pessoais protegidos pelo sigilo profissional/empresarial, bem como também pode incluir qualquer outro fator econômico ou desvantagem social para esses indivíduos em ter seus dados violados. Não obstante, dependendo das circunstâncias, uma violação pode envolver a confidencialidade, integridade e disponibilidade de dados pessoais ao mesmo tempo, bem como qualquer combinação destes. Outro fator importante, é que enquanto a determinação de que se houve uma violação de confidencialidade ou integridade é relativamente fácil ante a suas naturezas, o mesmo não pode-se dizer acerca da violação de disponibilidade. O WP29 (WP250rev.01)) entende que uma violação sempre será considerada como uma violação de disponibilidade quando houver uma perda permanente ou destruição de dados pessoais. No tocante aos critérios que a ANPD deve adotar, uma vez verificado tratar-se de incidente de violação de dados pessoais, deve o controlador, além de conter os efeitos do incidente, perquirir se tal violação é suscetível de causar risco ou dano relevante ao titular. Da LGPD depreende-se, como mencionado, de acordo com o Artigo 48 que o risco ou o dano relevante são os estímulos à obrigatoriedade da comunicação do incidente de violação de dados pessoais. Convém que os critérios a serem considerados pela ANPD nesta definição quanto à obrigatoriedade da comunicação, baseado inclusive nas recomendações do WP29 (WP250rev.01), sejam: • A gravidade do **impacto potencial** aos titulares de dados afetados e a **probabilidade** da sua ocorrência; • O tipo de violação de dados pessoais: definição de qual/quais o(s) pilar(es) de segurança da informação afetado(s), se da confidencialidade, da integridade e/ou da disponibilidade; • A natureza dos dados pessoais afetados: se dados sensíveis, dados de crianças ou também dados relacionados à informações críticas do titular, a exemplo de dados bancários, financeiros ou relacionados à sanções administrativas e condenações penais, capazes de afetar negativamente a reputação e estigmatizar o indivíduo. Assim, a natureza dos dados pessoais afetados influencia sobremaneira no potencial do risco ao titular;

	• O volume de dados pessoais afetados; • O volume de titulares afetados: a violação pode afetar um titular ou mesmo milhares e milhões de titulares. Assim, quanto maior o número de pessoas afetadas, maior o potencial de impacto do incidente de violação; • A facilidade de identificação das pessoas naturais: a identificação das pessoas pelo terceiro pode ocorrer de forma facilitada e direta, pela própria base vazada, ou exigir pesquisas adicionais e especiais para revelar as identidades dos titulares afetados, levando-se em consideração também o contexto do tratamento envolvido. De outro lado, a existência de técnicas de segurança em torno dos dados afetados, que os tornem ininteligíveis, por exemplo, pode figurar como minimizador do risco da violação. Um exemplo de ausência de risco ou dano relevante é quando há a perda de dispositivo de armazenamento de dados pessoais, mas estes estejam encriptados de forma a não permitir o acesso por terceiro; • A gravidade das consequências aos titulares: a depender da natureza dos dados afetados pela violação, o dano potencial pode ser elevado, em especial se puder causar a usurpação de identidade ou a afetação da honra, da imagem e da reputação, risco de ocorrência de discriminação, privação do exercício de direitos pelos bem como danos de natureza física, patrimonial e extrapatrimonial; • Por fim, outros elementos relevantes verificados pelo agente de tratamento: para além dos critérios que possam ser utilizados pela ANPD, frisando-se não ser uma lista exaustiva de critérios, mas sim um guia ao controlador, este deverá avaliar quaisquer outras circunstâncias que reputar relevantes relacionadas ao incidente de violação, inclusive para motivar a não comunicação da violação. Um exemplo da ausência de risco ou dano relevante ao titular pode ser quando os dados pessoais afetados já estejam disponíveis publicamente e sua eventual divulgação não constitua risco provável ao titular, considerados os demais critérios acima.
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	A GDPR entende que nem toda violação deve ser notificada à Autoridade Nacional responsável pelo território ou comunicada ao Titular, não sendo necessário a notificação caso (i) a violação dificilmente promova ou resulte em risco ao Titular no que tange aos seus direitos e liberdades, com a (ii) comunicação sendo dispensável caso a violação não apresente **alto risco** ao Titular.

	Isso significa que, imediatamente após tomar conhecimento de uma violação, é de vital importância que o controlador não apenas procure conter o incidente, mas também avaliar o risco que poderia resultado disso. Existem duas razões importantes para isso: em primeiro lugar, saber a probabilidade e a gravidade potencial do impacto no indivíduo ajudará o controlador a tomar medidas eficazes para conter e resolver a violação; em segundo lugar, ajudará a determinar se a notificação é necessária à autoridade de supervisão e, se necessário, às pessoas envolvidas de acordo com o WP29. Logo, o risco é alto quando a violação pode levar a danos físicos, materiais ou imateriais para os indivíduos cujos dados foram violados. Exemplos de tais danos, como explicados no tópico anterior, são discriminação, roubo de identidade ou fraude, perdas financeiras e danos à reputação. Contudo, quando a violação envolver dados pessoais que revelam raça ou origem étnica, opinião política, religião, crenças filosóficas, filiação a sindicatos ou inclui dados genéticos, dados relativos à saúde ou dados relativos à vida sexual ou condenações criminais e ofensas ou medidas de segurança relacionadas (em sua dados sensíveis) tais danos devem ser considerados prováveis de ocorrer apenas pela simples violação de tais dados, elevando-se portanto o risco de acordo com as Considerandas 75 e 76 da GDPR. Talvez um problema nesse tópico seja justamente a questão do que seria um dado sensível de acordo com a LGPD, já que o Artigo 5,inciso II da lei brasileira expõe um rol taxativo para tal categoria, não incluíndo uma definição mais ampla, a exemplo da Consideranda 45 da GDPR que define dados sensíveis como todo e qualquer dado que seu tratamento possa promover um risco ou dano aos direitos e liberdades fundamentais de cada indivíduo, o que faz com que o Artigo 9(1) seja meramente exemplificativo. Logo, no que tange ao alto risco no tratamento de dados sensíveis a ANPD deve ampliar o seu rol ou o seu entendimento de forma a incluir mais hipóteses e dados que se violados podem causar um grande dano ao Titular, a exemplo de dados referentes à orientação sexual ou nome social de um indivíduo. A Consideranda 76 ainda dispõe que a probabilidade e gravidade do risco para os direitos e liberdades do titular dos dados deve ser determinada por referência à natureza, âmbito, contexto e objetivos do processamento, algo que pode e deve ser alcançado através da implementação prévia de um Relatório de Impacto de Proteção de Dados (“RIPD”) pelo controlador dos dados pessoais, para uma avaliação hipotética de risco. Contudo, em caso de impossibilidade ou não realização de um RIPD, entendemos que a resposta a cada critério da avaliação de risco, conforme tópico acima, influenciará na definição de um risco

	“baixo, médio, alto”. De forma a entendermos em como o risco irá se categorizar a ANPD deve analisar as possíveis violações no que tange a sua probabilidade x impacto (dano ao titular), em uma matriz que pontue de 1 a 3 (sendo 1 o nível mais baixo e 3 o nível mais alto). Assim, a cumulação de gravidade em cada critério, bem como sua pontuação, tenderá à subida da categoria do risco. Quanto mais critérios acumulados, maior o ranqueamento do risco, qualificando-o à obrigatoriedade da comunicação/notificação do incidente de violação. Do mesmo modo, uma determinada situação que eleve o risco em certo critério pode, por si só, determinar a obrigatoriedade da comunicação do incidente de violação. A somatória de critérios apenas traz o indicativo de que provavelmente trate-se de incidente de violação que exija a comunicação. Por fim, entendemos que riscos baixos, assim como na GDPR, não sejam passivos de comunicação/notificação já que não ofertam danos reais ao Titular. Tal notificação de riscos baixos além de sobrecarregar a Autoridade, irá também gerar rixas e desconfianças desnecessárias ao Titular, já que uma violação desse tipo já foi contornada e resolvida pelo controlador/operador de dados pessoais através de medias técnicas e organizacionais razoáveis e apropriadas para solucionamento da crise.
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	Para que possamos distinguir risco e dano, é necessário entendermos acerca da responsabilização civil objetiva, ou sem culpa, baseada na teoria do risco do dano que passou a ser admitida expressamente no ordenamento jurídico brasileiro em virtude da regra constante do art. 927[1], parágrafo único do Código Civil A teoria da responsabilização objetiva direcionou o direito a ser conduzido pelo primado do coletivo sobre o individual. Ao passo que essa teoria foi abarcada pela Constituição Federal de 1998 em seu artigo 37, §6º, a Carta Maior também tornou pacífica a tese pela reparabilidade dos danos imateriais, e o Código Civil de 2002, no mesmo sentido, dispôs no artigo 186 que a indenização por ato ilícito é devida ainda que o dano seja exclusivamente moral. A prova inequívoca da culpa expressava um sistema altamente individualista no qual não caberia a característica coletiva de futuros institutos referentes a reparação de danos injustos. Foi com o

[1] Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, é obrigado a repará-lo. Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem.

	desiderato de adequar a responsabilidade civil às necessidades sociais advindas do crescente desenvolvimento, paralelo a novas perspectivas constitucionais, a solidariedade social, a dignidade humana e a justiça distributiva, que fundamentos, como a teoria do risco, explicaram a necessária objetivação da responsabilidade. Nessa senda, a responsabilidade civil, enquanto um juízo de valor reprovativo, é entendida como o instituto que objetiva corrigir o desequilíbrio provocado pelo dano injusto por meio de reparação, que surge por deixar uma pessoa de observar um preceito normativo que regula a vida. Assim, o dever de indenizar desenvolve-se em uma obrigação legal derivada, em suma maioria, de atos ilícitos. A teoria de responsabilidade civil objetiva, conforme adotada pelo ordenamento jurídico brasileiro, desenvolve-se em uma responsabilização que independente de culpa. Isso se dá, tendo em vista que a parte final do parágrafo único do art. 927, enuncia que haverá a responsabilidade civil, independente de culpa, quando a atividade normalmente desempenhada pelo autor implicar, por sua natureza, dano aos direitos de outrem. Pela teoria do risco, tem-se que todo prejuízo será imputado ao seu autor, devendo por ele ser reparado, independentemente da caracterização de culpa ou não. De todo modo, é possível afirmar que o risco é um dos fatores mais importantes na responsabilização civil por danos, sendo a teoria do risco o embasamento jurídico da responsabilidade objetiva. Importa salientar que risco, nessa acepção, compreende o perigo, a potencialidade do dano, a previsibilidade de perda ou de possível responsabilização, compreendendo, assim, eventos incertos e futuros inesperados que possam resultar em perdas ou danos. Ainda assim, convém ressaltar as diversas concepções de riscos já desenvolvidas para enquadrar as modalidades potenciais de danos. A primeira delas é a do risco integral, sendo considerada a mais abrangente, tendo em vista que, uma vez afastada a culpa, qualquer fato ensejará a responsabilização desde que haja o dano, não se admitindo qualquer hipótese de excludente de responsabilidade civil. Outra modalidade é o risco-profissional, isto é, a possibilidade de responsabilização do dano oriundo da atividade laboral pelo lesado, que importe na diminuição ou privação da capacidade produtiva dele. Ato contínuo, tem-se o risco-proveito, fundado no princípio do *ubi emolumentum ibi onus*, ou seja, do lucro nasce o encargo, segundo o qual deverá responsabilizar aquele que tirar vantagem econômica do fato. Ademais, tem-se a espécie do risco-excepcional, segundo a qual, o dever de indenizar será derivado de uma situação excepcional, isto é, que foge da atividade habitual do agente.

	Por fim, há a modalidade do risco-criado, mais coerente com o disposto no Código Civil, uma vez que dispõe que a obrigação de reparar o dano, independente de culpa e dos casos especificados em lei, se dará quando a ação habitualmente exercida pela autor do fato danoso naturalmente implicar em risco aos direitos de outrem. Segundo essa acepção de risco, exceto se provado que o agente tomou todas as medidas prudentes para evitar a ocorrência do dano, todos os prejuízos decorrentes de uma atividade exercida em proveito próprio deverão ser reparados. Logo, o risco pode ser identificado como um evento capaz de causar dano em potencial, sendo qualificado conforme a probabilidade da sua ocorrência. O dano, por sua vez, qualifica-se pela situação já ocorrida, o dano já provocado. Nos moldes do previsto nos artigos 186 e 187 do Código Civil.
O que deve ser considerado na avaliação dos riscos do incidente?	Devem ser considerados os critérios indicados no tópico 1 “Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?”. Ainda, faz-se necessário notar e diferenciar a avaliação de risco em uma violação de dados pessoais do risco considerado em um DPIA. O DPIA considera tanto os riscos do tratamento de dados pesoais sendo realizado conforme planejado, como os riscos em caso de umaviolação. Ao considerar uma violação em potencial, analisá-se, em termos gerais, a probabilidade da ocorrência e os danos ao titular dos dados que possam surgir; em outras palavras, é uma avaliação de um evento hipotético. Com uma violação real, o evento já ocorreu e, portanto, o foco é totalmente sobre o risco resultante do impacto da violação nos indivíduos. Nesse sentido, deve-se ser considerado: • Tipo de incidente/violação; • Natureza, sensibilidade e volume dos dados pessoais; • Facilidade na identificação dos titulares; • Severidade das consequências aos titulares; • Características especiais dos titulares;

	• Características especiais do controlador; • Quantidade de titulares afetados; Portanto, ao avaliar o risco que provavelmente resultará de uma violação, o controlador deve consideraruma combinação da gravidade do impacto potencial sobre os direitos e liberdades dos indivíduos e aprobabilidade de ocorrerem como já mencionamos anteriormente. Claramente, onde as consequências de uma violação são mais graves, o risco é maior e da mesma forma, onde a probabilidade de ocorrerem é maior, o risco também é aumentado.
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	Como meio de orientar os controladores a fornecer informações mais completas sobre o incidente, convém que sejam também endereçadas as seguintes informações para além das já exigidas pelo §1º do art. 48 da LGPD: a) informações sobre o incidente de violação de dados pessoais: • Descrição dos fatos noticiados; • Natureza da violação de dados pessoais: se afeta à confidencialidade, à integridade e/ou à disponibilidade ou qualquer combinação destas, basicamente qual o tipo de incidente/violação; • Meio pelo qual o controlador tomou ciência do incidente de violação; • Data e hora da ocorrência do incidente de violação; • Data e hora da ciência da ocorrência do incidente de violação; • Medidas de segurança implementadas até então; • Se trata-se de incidente de natureza cibernética; • Se houve recuperação de sistemas quanto ao incidente; • Há quanto tempo o incidente está em curso ou por quanto tempo esteve em curso;

	• Se os titulares já estão cientes da ocorrência mediante comunicação do controlador ou outro meio; • Se foram comunicados outros agentes de tratamento (controladores e operadores) sobre os fatos; b) informações adicionais sobre a natureza dos dados pessoais afetados: se dados sensíveis, se dados de crianças e adolescentes, se dados de natureza remuneratória, bancária ou financeira, se dados relacionados à aplicação de sanções administrativas, cíveis e penais; c) informações adicionais sobre os titulares afetados: número ainda que aproximado de titulares afetados. Natureza dos titulares afetados, se consumidores, empregados, funcionários, usuários, crianças e/ou adolescentes etc; d) volume ainda que aproximado de dados pessoais afetados; e) Consequências prováveis da violação de dados pessoais; f) Indicação das medidas técnicas e organizacionais já implementadas ou planejadas para contenção da violação; g) Descrição das medidas já implementadas ou proposta de medidas a serem implementadas pelo controlador para reparar a violação e/ou atenuar seus efeitos aos titulares.
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	Baseado na matriz normativa do GDPR, não se afigura razoável exigir tempo inferior ao lá previsto (72 horas da ciência do incidente de violação). Isto porque a matéria de proteção de dados é uma verdadeira quebra de paradigma no contexto brasileiro, vez que não se contava, até então, com semelhante regulamentação e obrigações, diferentemente do cenário europeu que há décadas possui legislações sobre o tema. No que tange ao que seria “a partir da ciência do incidente/violação”, o WP29 considera que um controlador deve ser considerado como tendo se tornado "ciente" quando aquele controlador tem um grau razoável de certeza de que ocorreu um incidente de segurança que levou a dados pessoais comprometidos.

	Nesse sentido, quando, exatamente, um controlador pode ser considerado "ciente" de uma violação específica dependerá das circunstâncias da violação específica. Em alguns casos, será relativamente claro desde o início que houve uma violação, enquanto em outros, pode levar algum tempo para estabelecer se os dados pessoais foram comprometidos ou não. Logo, a ênfase deve ser na ação imediata para investigar um incidente para determinar se os dados pessoais foram realmente violados e, em caso afirmativo, tomar medidas corretivas e notifique se necessário. Por exemplo, se depois de ser informado sobre uma violação em potencial por um indivíduo, pela mídia, outra fonte, ou quando ele próprio detectou um incidente de segurança, o controlador pode realizar um curto período de investigação, a fim de estabelecer se uma violação ocorreu de fato ou não. Durante este período de investigação, é necessário que a legislação especifique que o controlador não pode ser considerado como estando “ciente”. No entanto, como a LGPD já estipula que o controlador já tenha toda uma boa prática relacionada a segurança, bem como em relação de avaliação de risco pelo DPIA, espera-se que a investigação inicial deve começar o mais rápido possível de forma a estabelecer com um grau razoável de certeza se uma violação ocorreu; uma investigação mais detalhada pode então seguir. Recomenda-se, assim, seja estipulado para comunicação do incidente de violação o prazo de 3 (três) dias úteis ou, ao menos, o prazo de 72 (setenta e duas) horas como mínimo razoável para a comunicação, por ser o necessário para averiguação não somente de uma investigação detalhada, bem como para avaliação do risco/dano do tal incidente.
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	Em sendo o caso de comunicação dos titulares sobre o incidente, convém que seja feito no prazo de 72 horas contadas da ciência do incidente de violação ou imediatamente em caso de determinação da comunicação pela ANPD. Convém que o controlador preste as seguintes informações aos titulares afetados: • Descrição do incidente e de sua natureza; • Nome e contato do encarregado de proteção de dados ou de outro ponto de contato; • Descrição dos riscos e consequências potenciais do incidente; • Descrição das medidas adotadas ou planejadas pelo controlador para reparar o incidente; • Sugestão de medidas para atenuar os efeitos decorrentes do incidente;

	• Oferecimento ao titular de serviços gratuitos de remediação dos efeitos decorrentes do incidente, a exemplo de serviço de monitoramento de crédito. Como exemplo das medidas tomadas para lidar com a violação e mitigar seus possíveis efeitos adversos, o controlador pode afirmar que, após ter notificado a violação à autoridade supervisora competente, o controlador recebeu aconselhamento sobre como gerenciar a violação e diminuir seu impacto. O controlador deve também, quando apropriado, fornecer conselhos específicos aos indivíduos para se protegerem de possíveis consequências adversas da violação, como redefinir senhas no caso de as credenciais de acesso foram comprometidas. Novamente, um controlador pode optar por fornecer informações em além do que é necessário aqui a depender mais uma vez do caso concreto.
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	Como regra geral, recomenda-se que a comunicação seja feita diretamente ao titular afetado. Nesse sentido, a comunicação direta deve e pode ser usada ao comunicar uma violação aos titulares dos dados, com tal comunicação não devendo ser enviada com outras informações, como atualizações regulares, boletins informativos ou newslatter. Desta forma a comunicação mantem-se clara e transparente. A WP29 ajuda a dar outros exemplos de métodos de comunicação transparentes como a comunicação direta mencionada acima (por exemplo, e-mail, SMS), a utilização de banners ou notificações em site do controlador, comunicações postais e notificação na mídia como mencionado acima caso haja um volume enorme de titulares envolvidos. Uma notificação feita exclusivamente a a mídia/imprensa, por exemplo, não seria um meio eficaz de comunicar uma violação a um indivíduo. Logo, recomenda-se que os controladores devem escolher um meio que maximize a chance de comunicar as informações de maneira adequada a todos os indivíduos afetados. Dependendo das circunstâncias, isso pode significar que o controlador empregue vários métodos de comunicação, em oposição ao uso de um único canal de contato. Os controladores também podem precisar garantir que a comunicação seja acessível em formatos e linguagens alternativos relevantes para garantir que os indivíduos sejam capazes de compreender as informações que estão sendo fornecido a eles. A chave é ajudar os titulares dos dados a compreender a natureza da violação e as etapas que podem seguir para se proteger.
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	A exemplo da exceção constante no modelo regulatório europeu, sugere-se a dispensa da comunicação do incidente à ANPD quando o incidente de violação não seja suscetível de resultado em risco ou dano ao titular.

	Um exemplo da ausência de risco ou dano relevante ao titular é quando os dados pessoais afetados já estejam disponíveis publicamente e sua eventual divulgação não constitua risco provável ao titular.
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	O Artigo 34 (3) da GDPR estabelece três condições que, se satisfeitas, não requerem notificação aos indivíduos no caso de uma violação. A exemplo quando: • O controlador aplicou medidas técnicas e organizacionais adequadas para proteger os dados pessoais antes da violação, em particular as medidas que processam dados pessoais ininteligível para qualquer pessoa que não esteja autorizada a acessá-lo. Isso poderia, por exemplo, incluir a proteção de dados pessoais com criptografia de última geração ou por tokenização. • Imediatamente após uma violação, o controlador tomou medidas para garantir que o alto risco colocado aos direitos e liberdades dos indivíduos não é mais provável que se materialize. Por exemplo, dependendo das circunstâncias do caso, o controlador pode ter identificado imediatamente e tomou medidas contra o indivíduo que acessou os dados pessoais antes que eles pudessem fazer qualquer coisa com ele. A devida consideração ainda precisa ser dada às possíveis consequências de qualquer violação da confidencialidade, mais uma vez, dependendo da natureza dos dados em causa. • Envolveria um esforço desproporcional para contatar indivíduos, como detalhes de contato do titular foram perdidos como resultado da violação ou não são conhecidos em primeiro lugar. Por exemplo, o arquivo de um escritório de estatística inundou e os documentos contendo os dados pessoais foram armazenados apenas em papel. Em vez disso, o controlador deve tornar um público comunicação ou tomar medida semelhante, em que os indivíduos sejam informados de forma igualmente maneira eficaz. Além disso, de acordo com o princípio de responsabilidade, os controladores devem ser capazes de demonstrar a ANPD que atendem a uma ou mais dessas condições apontadas acima. Deve-se ainda ter em mente que enquanto a notificação pode inicialmente não ser exigida se não houver risco para os direitos e liberdades naturais pessoas, isso pode mudar com o tempo e o risco teria que ser reavaliado. Entendemos que tais sugestões podem e devem ser adaptadas ao contexto brasileiro.
Quais são os possíveis critérios a serem adotados pela ANPD na análise	• gravidade do impacto potencial aos titulares de dados afetados e a probabilidade da sua ocorrência;

da gravidade do incidente de segurança? (art. 48, §2º)	• tipo de violação de dados pessoais: definição de qual/quais o(s) pilar(es) de segurança da informação afetado(s), se da confidencialidade, da integridade e/ou da disponibilidade; • natureza dos dados pessoais afetados: se dados sensíveis, dados de crianças ou também dados relacionados à informações críticas do titular, a exemplo de dados bancários, financeiros ou relacionados à sanções administrativas e condenações penais, capazes de afetar negativamente a reputação e estigmatizar o indivíduo. Assim, a natureza dos dados pessoais afetados influencia sobremaneira no potencial do risco ao titular; • volume de dados pessoais afetados; • volume de titulares afetados: a violação pode afetar um titular ou mesmo milhares e milhões de titulares. Assim, quanto maior o número de pessoas afetadas, maior o potencial de impacto do incidente de violação; • facilidade de identificação das pessoas naturais: a identificação das pessoas pelo terceiro pode ocorrer de forma facilitada e direta, pela própria base vazada, ou exigir pesquisas adicionais e especiais para revelar as identidades dos titulares afetados, levando-se em consideração também o contexto do tratamento envolvido. De outro lado, a existência de técnicas de segurança em torno dos dados afetados, que os tornem ininteligíveis, por exemplo, pode figurar como minimizador do risco da violação. Um exemplo de ausência de risco ou dano relevante é quando há a perda de dispositivo de armazenamento de dados pessoais, mas estes estejam encriptados de forma a não permitir o acesso por terceiro; • gravidade das consequências aos titulares: a depender da natureza dos dados afetados pela violação, o dano potencial pode ser elevado, em especial se puder causar a usurpação de identidade ou a afetação da honra, da imagem e da reputação, bem como danos de natureza física, patrimonial e extrapatrimonial; • quaisquer outras circunstâncias que reputar relevantes relacionadas ao incidente de violação.
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	Ao avaliar o risco, devem ser tidas em consideração a gravidade do impacto potencial aos titulares de dados afetados e a probabilidade da sua ocorrência. Recomenda-se ter por referência nesta análise da gravidade do incidente a natureza, âmbito, contexto e finalidades do tratamento de dados. Sugere-se a metodologia de processo de avaliação de riscos constante na ABNT NBR ISO 31000:2018.

Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	• Determinação do oferecimento ao titular de serviços gratuitos de remediação dos efeitos decorrentes do incidente, a exemplo de serviço de monitoramento de crédito; • Determinação de disponibilização de SAC específico por via telefônica e e-mail para disponibilização de informações aos titulares quanto ao incidente, ou ressarcimento de dados decorrentes de acordos com as autoridades públicas; • Determinação de disponibilização de portal contendo informações gerais sobre o incidente, podendo ser no formato FAQ (*Frequently Asked Questions* – perguntas frequentes) ou em site específico a ser feito exclusivamente para o incidente.
Sugestão: Categorização dos incidentes que configuram violação de dados pessoais conforme os pilares de Segurança da Informação	Em janeiro de 2021, o EPDB lançou a Guideline 01/2021[2] referente a exemplos de incidentes de segurança. Nesse sentido, foi elencado alguns exemplos de tais violações que podem ser úteis à ANPD: 1. Ramsomware • Ramsomware com backup e sem exfiltração • Ramsomware sem backup apropriado • Ramsomware com backup e com exfiltração 2. Ataques de exfiltração de dados • Exfiltração de dados referentes a processo seletivo por um website • Exfiltração de senhas hashed por um website • Aataque de credenciais bancárias em website 3. Incidentes internos • Exfiltração de dados corporativos por um ex-funcionário

[2] https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf

	• Transferência acidental de dados a um parceiro 4. Perda ou roubo de dispositivos e documentos físicos • Material roubado que armazenava dados criptografados • Material roubado que armazenava dados não criptografados • Documentos roubados que continham dados pessoais sensíveis 5. Engenharia social • Roubo de identidade • Extrafiltração de e-mails 6. Envio errado de comunicação • Erro de “snail” e-mail • Dados pessoais sensíveis enviados por e-mail por erro • Dados pessoais enviados por e-mail por erro
Sugestão: Comunicação do incidente à ANPD por fases	A depender da natureza e circunstâncias do incidente e em sendo necessária investigação adicional por parte do controlador para apurar todos os fatos relevantes relacionados ao incidente, recomenda-se a admissão de que a comunicação do incidente possa ser complementada após a comunicação inicial. Inclusive, este formato é admitido no GDPR no artigo 33, nº 4 “Caso, e na medida em que não seja possível fornecer todas as informações ao mesmo tempo, estas podem ser fornecidas por fases, sem demora injustificada”.

	Isso significa que o GDPR reconhece que os controladores nem sempre terão todos os informações sobre uma violação dentro de 72 horas após tomar conhecimento dela, de tão complexos e abrangentes os detalhes do incidente podem ser. Logo, nem sempre tais informações estarão disponíveis durante este período inicial. Nesse sentido, WP29 recomenda que quando o controlador notificar primeiro a Autoridade, o controlador também deve informar a Autoridade se o controlador ainda não tiver todas as informações necessárias no presente momento e só puder fornecer mais detalhes mais tarde. A autoridade supervisora deve concordar como e quando as informações adicionais devem ser fornecidas. Isso não impede que o controlador forneça mais informações em qualquer outra fase, se ele toma conhecimento de detalhes adicionais relevantes sobre a violação que precisam ser fornecidos ao autoridade de supervisão.

SUGESTÃO DE NORMATIVO, SE HOUVER

Art. 1º. Na ocorrência de incidente de segurança envolvendo dados pessoais que possa acarretar risco ou dano relevante aos titulares, o controlador comunicará o fato:
I – à Autoridade Nacional de Proteção de Dados;
II – aos titulares de dados pessoais afetados pelo incidente.

Anexo I - COMUNICAÇÃO INICIAL DO INCIDENTE DE VIOLAÇÃO DE DADOS PESSOAIS

I – Informações da entidade e contato;
- a) CPF/CNPJ;
- b) Pessoa de contato;
- c) Função;
- d) Telefone e e-mail de contato.

II – Informações sobre o incidente de violação de dados pessoais
- a) descrição dos fatos noticiados;
- b) natureza da violação de dados pessoais:
  - I. se afeta à confidencialidade;

II. à integridade; e/ou
III. à disponibilidade ou qualquer combinação destas.

c) Causa do incidente de violação;
d) meio pelo qual o controlador tomou ciência do incidente de violação;
e) data e hora da ocorrência do incidente de violação;
f) data e hora da ciência da ocorrência do incidente de violação;
g) motivos da demora da comunicação;
h) se trata-se de incidente de natureza cibernética;
i) se houve recuperação de sistemas quanto ao incidente;
j) há quanto tempo o incidente está em curso ou por quanto tempo esteve em curso;
k) se os titulares já estão cientes da ocorrência mediante comunicação do controlador ou outro meio;
l) se foram comunicados outros agentes de tratamento (controladores e operadores) sobre os fatos.

III – Dados pessoais envolvidos

a) Informações sobre a natureza dos dados pessoais afetados: se dados sensíveis, se dados de crianças e adolescentes, se dados de natureza remuneratória, bancária ou financeira, se dados relacionados à aplicação de sanções administrativas, cíveis e penais;
b) Volume ainda que aproximado de dados pessoais afetados.

IV – Titulares de dados pessoais envolvidos

a) Informações adicionais sobre os titulares afetados: número ainda que aproximado de titulares afetados. Natureza dos titulares afetados, se consumidores, empregados, funcionários, usuários, crianças e/ou adolescentes etc;

V – Consequências do incidente de violação

a) Consequências do incidente já verificadas;
b) Consequências prováveis do incidente.

VI – Medidas preventivas/corretivas

a) Indicação das medidas técnicas e organizacionais já implementadas ou planejadas para contenção da violação;
b) Descrição das medidas já implementadas ou proposta de medidas a serem implementadas pelo controlador para reparar a violação e/ou atenuar seus efeitos aos titulares.

VII – Transferências internacional de dados

a) Existe transferência internacional dos dados pessoais afetados pelo incidente?
b) O incidente foi ou será notificado à autoridade de país estrangeiro?

Art. Xxxx ....

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: BSA – THE SOFTWARE ALLIANCE

CPF/CNPJ: 02.469.832/0001-87

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS	
IMPORTANTE: Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	Convém que um incidente de segurança seja considerado relevante para fins de notificação quando o incidente cria um alto risco de roubo de identidade ou fraude financeira.
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	É importante que o regulamento deixe claro que apenas incidentes de segurança relevantes devam ser notificados, conforme exige a Lei Geral de Proteção de Dados Pessoais (LGPD). Para isso, o regulamento precisa adotar uma abordagem em duas vertentes: primeiro, é necessário definir um incidente de segurança e, em seguida, oferecer orientação sobre quando o incidente de segurança deve ser considerado relevante para notificação. **Definição de Incidente de Segurança**: Considerando que esta Consulta está relacionada à regulamentação da Lei Geral de Proteção de Dados Pessoais (LGPD), os incidentes no âmbito da próxima regulamentação devem estar relacionados a dados pessoais conforme definido pela LGPD. O regulamento deve deixar claro que os incidentes de segurança que requerem uma análise mais aprofundada para determinar se uma notificação de incidente de segurança será necessária são aqueles que **impactam negativamente a privacidade, disponibilidade ou integridade dos dados pessoais mantidos por uma organização.** **Incidente de segurança relevante**: De acordo com a LGPD, apenas incidentes de segurança relevantes devem ser notificados. A relevância de um incidente de segurança deve ser avaliada com base na probabilidade de apresentar altos riscos de roubo de identidade ou fraude financeira.

	Por exemplo, a violação de dados pessoais que são inutilizáveis, ilegíveis ou indecifráveis para um terceiro não autorizado devido ao uso de métodos como criptografia, redação, controles de acesso e outros mecanismos, não deve necessitar de notificação de segurança. Da mesma forma, os incidentes que afetam dados pessoais que já são de domínio público provavelmente não causarão alto risco de roubo de identidade ou fraude financeira. Por exemplo, se um banco de dados listando apenas os nomes e afiliações profissionais de indivíduos cujos perfis de mídia social publicamente disponíveis incluem essas informações fossem acessados por terceiros não autorizados, este é um incidente que provavelmente não criaria o risco de fraude financeira ou roubo de identidade, razão pela qual o incidente não deve ser considerado relevante para efeitos do presente regulamento.
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	Para fins de notificação de incidente de segurança, a relevância do incidente deve ser o fator determinante. Um incidente de segurança deve ser considerado relevante, indicando a exigência de notificação, se representar um alto risco de roubo de identidade ou fraude financeira devido ao acesso não autorizado, destruição, uso, modificação ou divulgação de dados pessoais. De acordo com o exemplo referido na resposta à pergunta 2, se um banco de dados listando apenas os nomes de indivíduos e suas afiliações profissionais que refletem informações publicamente disponíveis for acessado por um terceiro não autorizado, o risco de essas informações apresentarem um impacto negativo sobre esses indivíduos devido a fraude financeira ou roubo de identidade é muito baixo, então o incidente não seria considerado relevante. Por outro lado, se o mesmo banco de dados também contivesse números de previdência social dos titulares dos dados, haveria um risco de roubo de identidade e o incidente seria considerado relevante. É importante que o regulamento deixe claro que a notificação só será exigida se houver motivos razoáveis para supor que ocorreu um incidente de segurança relevante. Determinar a ocorrência de um incidente de segurança relevante requer uma investigação por parte do controlador de dados. Portanto, o simples fato de uma empresa ter conhecimento de um potencial incidente de segurança não deve incitar a necessidade de notificação. Por favor, veja detalhes adicionais sobre este problema na pergunta 6.
O que deve ser considerado na avaliação dos riscos do incidente?	Conforme descrito acima, o potencial de fraude financeira ou roubo de identidade deve ser avaliado ao considerar os riscos apresentados por um incidente de segurança. Essa avaliação pode ser feita por meio de uma avaliação do impacto da proteção de dados, por exemplo.

Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	As informações exigidas pelo artigo 48, §1 são suficientes. Se não for possível fornecer todas as informações necessárias ao mesmo tempo, as informações podem ser fornecidas em fases, sem atrasos indevidos.
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	Imediatamente após um incidente de segurança, as empresas devem ser encorajadas - e ter tempo adequado - a concentrar seus recursos na realização de uma investigação completa e na restauração da integridade dos sistemas potencialmente comprometidos. Oferecer às empresas um prazo razoável para tais esforços ajuda a prevenir danos adicionais. A exigência de notificação nas primeiras horas após a empresa ter conhecimento de um potencial incidente de segurança força a empresa a desviar seus recursos da investigação do incidente e da implementação de ações que poderiam mitigar ou eliminar o risco para os titulares dos dados. Para garantir que as empresas ajam rapidamente ao saber de um potencial incidente de segurança, o regulamento deve exigir que as empresas tomem medidas imediatas para estabelecer se há motivos razoáveis para supor que ocorreu um incidente de segurança relevante. Se, após realizar essa avaliação inicial, a empresa concluir que ocorreu um incidente de segurança relevante, ela deve tomar medidas corretivas para eliminar ou reduzir a probabilidade de danos relevantes aos titulares dos dados, bem como notificar a ANPD em até 72 horas. O prazo para notificar a ANPD deve começar a partir do momento em que a empresa estabeleça com um grau razoável de certeza que um incidente de segurança relevante ocorreu e que atende ao limite de notificação, e não quando souber inicialmente que um potencial incidente de segurança pode ter ocorrido. Essa abordagem ajudará a evitar sobrecarregar a ANPD com notificações imateriais e evitará o desvio de recursos da empresa de atividades que promovam a segurança de dados para a preparação de notificações que provavelmente não atingirão o limite de notificações.
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	As notificações de incidentes devem conter informações acionáveis suficientes para permitir que os titulares dos dados se protejam de possíveis efeitos negativos de um relevante interesse de segurança, sem conter muitos detalhes que possam tornar as notificações difíceis de entender e ineficazes. A notificação aos titulares dos dados deve incluir os elementos exigidos pela LGPD, art. 48, §1º I, IV e VI, bem como o nome e contatos do responsável pela proteção de dados ou outro ponto de contato onde possam ser obtidas informações adicionais. A empresa notificadora pode optar por acrescentar outras informações que considere relevantes para um determinado caso.

	Quanto ao prazo para notificação, os titulares dos dados devem ser notificados dentro de um prazo razoável, que pode variar dependendo das circunstâncias. No entanto, nos casos em que a notificação de incidente de segurança aos titulares dos dados pode interferir negativamente nas investigações conduzidas pela ANPD e / ou outras autoridades legais, e a notificação aos titulares dos dados pode exacerbar os riscos apresentados pelo incidente de segurança, a notificação aos titulares dos dados deve ser esperada quando a empresa notificadora é autorizada pelas autoridades competentes para fazê-lo.
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	Os métodos de notificação devem maximizar as chances de que a notificação chegue aos indivíduos afetados pelo incidente de segurança em tempo hábil. A notificação individual via correio, correio eletrônico ou telefone deve ser permitida, nos casos em que essas formas de comunicação sejam viáveis. As empresas também devem ter permissão para se comunicar com os titulares dos dados por meio de suas plataformas se considerarem que este é o melhor método para contatar os titulares dos dados afetados pelo incidente de segurança. Avisos públicos, referidos como "avisos substitutos" por algumas leis estaduais dos EUA, que são entregues por meio da mídia impressa ou anúncios postados de forma destacada no site da empresa notificadora também devem ser permitidos quando a empresa notificadora não tiver informações suficientes ou atualizadas para todos os indivíduos afetados pelo incidente de segurança. Os avisos públicos também devem ser autorizados se a notificação for urgente e a notificação individual causar atrasos que podem tornar a notificação ineficaz.
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	Conforme apontado na resposta à questão 2 acima, apenas incidentes de segurança relevantes devem gerar a obrigatoriedade de notificação à ANPD. Notificações sobre outros incidentes de segurança não devem ser exigidas.
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	Quando as empresas estabelecem que há motivos razoáveis para presumir que um incidente de segurança relevante possa ter ocorrido, elas devem tomar medidas corretivas imediatas para mitigar ou evitar o risco de danos ao titular dos dados. Se as ações corretivas tomadas eliminarem com sucesso o risco para o titular dos dados, não deverá ser necessária notificação aos titulares dos dados. Após análise das informações recebidas da empresa notificadora, caso a ANPD não considere que as medidas corretivas foram bem-sucedidas, poderá exigir que os titulares dos dados sejam notificados. Por exemplo, se as informações de crédito sobre vários titulares de dados forem removidas de um banco de dados por um terceiro não autorizado, apresentando riscos às pontuações de crédito dos

	titulares de dados, mas o controlador de dados for capaz de restaurar os dados, o risco representado pelo incidente de segurança teria sido eliminado e não deve ser necessária notificação aos titulares dos dados.
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	Quanto maior a sensibilidade e a confidencialidade dos dados envolvidos em um incidente de segurança, mais provável que eles possam causar danos mais graves devido ao roubo de identidade ou fraude financeira. Por exemplo, incidentes de segurança que causam o acesso não autorizado de nomes completos, endereços, registro geral (RG) e cadastro de pessoas físicas (CPF) podem desencadear a solicitação de notificação, já que esses dados normalmente não são amplamente compartilhados para evitar fraudes financeiras e roubo de identidade.
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	A ANPD poderia usar padrões internacionais de segurança da informação, como os padrões ISO.
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	Como a segurança perfeita não existe, os riscos de possíveis incidentes de segurança nunca podem ser totalmente eliminados, mas podem ser atenuados e seus efeitos podem ser interrompidos antes que ocorram danos aos titulares dos dados. A ANPD deve adotar uma abordagem baseada em risco e neutra em termos de tecnologia e exigir que as empresas mantenham práticas de segurança de dados que tenham um escopo razoável de acordo com o tamanho e a complexidade de uma organização, a confidencialidade e o volume de dados pessoais em seus sistemas e o custo das ferramentas disponíveis para melhorar a segurança e reduzir vulnerabilidades
SUGESTÃO DE NORMATIVO, SE HOUVER	
O papel dos controladores e operadores de dados As notificações de incidentes de segurança à ANPD e aos titulares dos dados, quando necessárias, devem ser feitas pela empresa com a qual os titulares de dados se relacionam diretamente (controladores de dados). Essa abordagem promove um bom gerenciamento de dados, garantindo que os controladores de dados adotem uma abordagem de ciclo de vida para gerenciar a segurança da informação.	

Os contratos entre controladores de dados e operadores de dados devem permanecer aplicáveis, permitindo uma alocação eficiente de risco. Na verdade, para aumentar a proteção da privacidade, os processadores de dados muitas vezes não têm visibilidade sobre o tipo de dados que processam, nem muitas vezes têm as informações de contato do titular dos dados. Isso evitaria que os processadores de dados determinassem com precisão se o incidente aciona os requisitos de notificação e que contatassem os titulares dos dados para notificá-los sobre o incidente, se necessário.

Se ocorrer um incidente de segurança envolvendo um processador de dados, o processador de dados deve notificar o controlador de dados. O controlador de dados, então, avalia o risco com base nas informações fornecidas pelo processador de dados e faz uma determinação sobre o risco apresentado aos titulares dos dados pelo incidente, emitindo as notificações necessárias se forem justificadas

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: **Grupo de Estudos CWC – LGPD do CWC Compliance Women Committee, por meio de sua coordenadora Renata Fonseca de Andrade e associadas: Morgana Ana Daler Casagrande, Raquel Pereira, Thais Rodrigues Collaço e Tatiana Strauch. Comissão de Anticorrupção e Compliance da 93ª Subsecção São Paulo – CAC OAB/SP Pinheiros por mei de sua Presidente Renata Fonseca de Andrade.**

CPF/CNPJ: [redacted]

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de

informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS

IMPORTANTE: Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.

TÓPICO/QUESTÃO	CONTRIBUIÇÃO/INSTITUIÇÃO
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	**1) Quando houver um volume de dados considerável; quando se tratar de vazamento de dado sensível, perda permanente dos dados que afetem o titular do dado; quando a combinação dos dados sob o incidente permitir o uso desses para cometer ato ilícito e/ou fraude que prejudique o titular dos dados; ou, quando os dados forem vazados em fóruns da Internet.** **2) Critérios ANPD: Apenas incidentes classificados como ALTO RISCO (matriz a ser definida pela ANPD com critérios gerais – ver recomendação questão 12). Critérios potencialmente lesivos - combinação dos dados (natureza dos dados), riscos de fraudes, falsidade documental e roubo de identidade, fraude contra o crédito, possibilidade do uso dos dados sensíveis para fins de discriminação ou crimes(sensibilidade) - volumetria, medidas adotadas para reverter ou mitigar sequestro, comprometimento da integridade física e moral, retaliação, constrangimento ou exposição pública, negativação X probabilidade de materialização.**
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como	**1) Entendemos que a classificação do incidente em risco ou dano "Baixo, Médio ou Alto" está adequado.** **2) Relevante = RISCO ALTO = estar exposto na internet e ter sido objeto de hackeamento,**

distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	**volume de dados, seja pequeno ou grande, o controlador não tem controle de mitigação do risco, na medida em que não pode/consegue estancar ou mitigar os efeitos, saindo do seu controle.** **Ideal que a ANPD promova um regulamento harmônico com as medidas mínimas para que os controladores e operadores implementem uma governança, considerando:** **- o regulamento de outras Agências Reguladoras Nacionais;** **- um *framework* de riscos, a exemplo do que acontece em outros países e regiões, como o COSO, NIST/ISO/ENISA, para classificar a severidade do risco e trazer objetividade para fins de reporte à ANPD.**
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	**O dano é um risco concretizado. O ponto aqui é avaliar se os controles aplicados aos riscos inerentes foram suficientes.** **Nesses casos fica evidente que houve uma falha dos mitigadores aos riscos avaliados.**
O que deve ser considerado na avaliação dos riscos do incidente?	**Para os controladores que deverão fazer essa avaliação de imediato, e muitas vezes sem subsídios, levar em consideração os itens abordados no 1° tópico.** **Para a ANPD, entendemos que essa avaliação será feita em momento oportuno, quando mais informações sobre o incidente já houverem sido levantadas, não de imediato. Se houve falha de processo, se a revisão dos controles estava adequada e atualizada (se de fato falharam), qual a causa raiz do vazamento. Havendo reincidência de um incidente, ainda que não tenha sido anteriormente reportado, e independentemente do grau de risco, deve ser reportado, sob pena de má fé.**
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	**Informações básicas que o controlador possuir naquele momento tais como, natureza da organização, data hora e local do evento, fatos já identificados (número de titulares afetados, dados envolvidos, etc), possíveis consequências do incidente de acordo com a matriz de riscos do controlador/operador, se o incidente foi com o controlador ou com o operador e ações adotadas até o momento da notificação.**
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	**Até 05 (cinco) dias úteis (Art. 33, GDPR), ressalvado o cumprimento das obrigações e dos prazos já estipulados aos setores regulados (Sistema Financeiro Nacional, ANS, etc). Os controladores devem complementar as informações em até 15 (quinze) dias corridos a contar da data do incidente ou da ciência deste, sem prejuízo de complementações periódicas subsequentes, até a conclusão da investigação.** **Considerar que no momento do incidente a prioridade é o gerenciando da crise e as informações necessárias aos titulares (princípio da transparência e prestação de contas) devem ser levados em consideração, bem como medidas protetivas à minimizar os danos**

	podem ser tomadas independente de prazos. Todo o esforço para a apuração frequentemente dependem de outros prestadores de serviços. **Não entendemos que o prazo do cadastro positivo seja adequado aqui, uma vez que ele se restringe aqueles players do mercado, aqui o escopo é outro, controladores de dados de diferentes portes, segmentos e indústrias.**
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	**Até 48 horas úteis, em formato simplificado, similar a um "alerta. Até 05 (cinco das) úteis informações complementares e sumarizadas e prestação de contas do depois de concluída a investigação, uma nova notificação deve ser enviada, se necessário, complementando e/ou prestando contas.**
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	**Pelos meios de comunicação regulares e já existentes com os titulares de dados, armazenando a respectiva evidência.** **Como regra geral, sugerimos comunicar individualmente e complementar facultativamente no website, quando afetar grande número de titulares.**
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	**Quando um incidente for avaliado com risco ou dano Médio (ambiente externo em exposição na internet) ou Baixo (ambiente interno), de acordo com os critérios que a ANPD definir.**
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	**Quando o controlador avaliar que o incidente não gere nenhum potencial risco/dano (sequestro, comprometimento da integridade física e moral, retaliação, constrangimento ou exposição pública, negativação, uso de falsa identidade) ao titular.**
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	**Volumetria, combinação de dados vazados, dados públicos, atrelados aos riscos que os titulares estariam expostos em decorrência do incidente e a ausência do atendimento dos controladores ao Art. 48, §1° da LGPD.**
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	**Metodologia: abordagem baseada em risco combinada com as métricas a serem definidas pela ANPD, por exemplo, utilizando-se como referência a seguinte formula para cálculo da severidade do risco, recomendada pela ENISA-*European Union Agency for Cibersecurity* https://www.enisa.europa.eu/publications/dbn-severity, que tem ampla abrangência:**

	SE = DPC x EI + CB, onde: SE = Severidade DPC = Data Processing Context (1 – dados não sensíveis; 2 – dados não sensíveis, mas que possibilitam *profiling*; 3 – dados sensíveis) EI = Ease of Identification (1 – se dados fortemente encriptados, como AES; 2 – dados em texto simples, permitindo conectá-los ao titular de dados) CB = Circumstances of breach (1 – dados vazados para recebedor conhecido e não autorizado; ou dados pessoais alterados e usados incorretamente ou ilegalmente, afetando o titular dos dados, porém os dados originais podem ser restaurados; ou os dados pessoais não podem ser acessados, mas podem ser restaurados; 2 - Dados vazados para recebedores desconhecidos; ou, dados são alterados e usados incorretamente ou ilegalmente, afetando o titular dos dados e os dados não podem ser restaurados; ou dados não podem ser acessados ou restaurados; ou incidente é causado por comportamento mal-intencionado afetando titular de dados (venda de dados por funcionários a terceiros; divulgação de dados em sites externos, por funcionários; roubo de dados por hackers, etc) **É necessário que haja objetividade nos critérios e que cada empesa defina sua Matriz de Riscos a partir dos critérios de classificação de riscos estabelecidos pela ANPD.**
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	**Verificar se houve o cumprimento do Art. 48, §1° da LGPD. Recomendar ações técnicas e educativas, tais como conscientização, melhorias de controles técnicos e organizacional. de**

SUGESTÃO DE NORMATIVO, SE HOUVER
Incluir no material educativo e preventivo da ANPD toolkit e modelos baseados em boas práticas e na regulação LGPD. A ANPD haverá de desenvolver materiais de estudos, ferramental ou toolkit, modelos de Relatório de Impacto de Proteção de Dados, modelos de Reporte de Incidentes e outros instrumentos e minimamente procedimentos necessários para a Governança e o Compliance.

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: CÂMARA BRASILEIRA DA ECONOMIA DIGITAL
CPF/CNPJ: 04.481.317/0001-48

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco e dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto à ANPD quanto aos titulares; e possíveis exceções quanto à obrigatoriedade de informar à ANPD e aos titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS **IMPORTANTE:** Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÕES DA CÂMARA BRASILEIRA DA ECONOMIA DIGITAL**
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	Preliminarmente, é importante frisar que o simples fato de ter ocorrido um incidente de segurança não significa necessariamente que as medidas técnicas e organizacionais de segurança implementadas tenham sido insuficientes, e que o dever de comunicação se refere apenas aos incidentes de segurança envolvendo dados pessoais que concretamente causem risco ou dano relevante, e não quaisquer suspeitas ou eventuais riscos e danos não relevantes. A fim de oferecer uma orientação precisa, consideramos importante que o conceito de incidente de segurança envolvendo dados pessoais esteja claramente definido. Em consonância com as orientações prévias da ANPD publicadas no dia 22 de janeiro de 2021, considera-se, em primeiro lugar, que incidente *"é qualquer evento adverso, confirmado, que, nos termos do art. 48 da LGPD possa acarretar risco ou dano relevante aos titulares, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito, que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita".* Com o objetivo de avançar no sentido de uma definição mais clara, recomenda-se a adoção de definições de forma semelhante ao modelo adotado pelo Grupo de Trabalho Artigo 29 da UE. Nesse sentido: (a) destruição indica casos nos quais os dados não mais existem, ou ao menos não existem em um formato que pode ser usado pelo controlador; (b) perda refere-se aos casos nos quais os dados ainda existem, mas o controlador perdeu o domínio ou acesso a eles, ou então não mais os tem

	em sua posse; alteração indica os casos nos quais os dados foram alterados ou corrompidos; por fim, (c) vazamento ou tratamento inadequado ou ilícito referem-se às situações de recebimento (ou acesso) aos dados por parte de pessoas ou entidades não autorizadas. Um incidente pode acarretar risco ou dano relevante ao titular, dependendo do volume e da natureza dos dados, bem como da quantidade de terceiros que indevidamente tenham tido acesso, da gravidade e da probabilidade de se concretizar. Dada a ampla gama de tratamento de dados pessoais realizado por diferentes tipos de organizações, nos parece adequado manter uma abrangência e flexibilidade em torno da metodologia de análise de risco. A ANPD deve procurar esclarecer os critérios a serem examinados e apresentar alguns exemplos de posições claras de sua própria análise de risco/gravidade. Os critérios a serem considerados, de maneira cumulativa, pela ANPD para determinar a probabilidade e gravidade do risco/dano podem incluir: ● O tipo de violação (por exemplo, dependendo do cenário, uma violação de confidencialidade pode ter um impacto maior do que se os dados fossem simplesmente perdidos ou excluídos); ● A natureza e a sensibilidade dos dados pessoais (quanto mais sensíveis os dados, maior o risco de dano às pessoas afetadas); ● Facilidade de identificação inequívoca de indivíduos; ● Gravidade das consequências para os indivíduos (por exemplo, violações onde há evidências de malfeitores acessando dados pessoais podem indicar maior risco do que violações onde os dados são divulgados acidentalmente); ● Características especiais do indivíduo afetado (por exemplo, dados relativos a crianças/outros indivíduos vulneráveis, vínculo empregatício, podem colocá-los em maior risco); Os critérios atenuantes a serem considerados são:

	● A boa-fé e as intenções dos terceiros que tiveram acesso aos dados após o incidente; ● O quantitativo de indivíduos afetados, desde que isso não seja um critério de caráter primário de avaliação. ● Emprego das medidas de segurança adequadas aos dados pessoais (técnicas de criptografia, pseudonimização e anonimização parcial de dados); Também é necessário evitar uma avaliação de risco ou dano baseada em eventos hipotéticos ou possibilidades remotas, ou com uma visão do que a violação poderia materializar-se no futuro. Conforme acima mencionado, reforçamos a recomendação de que a ANPD não considere o volume de usuários como um critério primário para avaliar a gravidade do incidente. O número de usuários afetados não é um bom indicador dos danos reais ou da probabilidade de danos que um indivíduo possa sofrer em razão de um incidente de segurança. A partir destes critérios listados acima, entendemos que cabe ao controlador, considerando o contexto e as especificidades de sua atividade empresarial, decidir sobre a possibilidade de um incidente acarretar risco ou dano relevante ao titular. Incentivamos as jurisdições a buscarem requisitos compatíveis entre si, para evitar sobrecarregar as empresas multinacionais no caso de um incidente de segurança e consequentemente criar vários tipos diferentes de relatórios de incidentes. A Agência Espanhola de Proteção de Dados, por exemplo, criou uma ferramenta em seu site[1], na qual os controladores, se assim desejarem, podem preencher, de forma anônima, um questionário com mais informações a respeito de incidentes de segurança com dados pessoais. A partir das respostas apresentadas, e com base em critérios pré-estabelecidos, a ferramenta indica para o controlador se o incidente deve

[1] https://servicios.aepd.es/AEPD/view/form/MDAwMDAwMDAwMDAwMDMyODAzOTgxNjE1OTg5NjE5MDM0?updated=true

	ser notificado ou não. Sugerimos que a ANPD desenvolva algo no mesmo sentido, entendendo que tal ferramenta será muito útil em auxiliar as organizações a entenderem quais medidas devem ser adotadas.
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	Em nossa experiência, definir limites vinculados a critérios objetivos e orientados por metodologia ajuda os controladores de dados a entenderem melhor a verdadeira natureza, impacto e necessidade de comunicação dos incidentes, especialmente em resposta à nova norma, consequentemente evitando um cenário de hipernotificação. Afinal, é razoável esperar que, na ausência de critérios objetivos e metodologicamente alicerçados, os controladores adotem excesso de cautela e tendam a hipernotificar, o que poderia definir expectativas erradas para a ANPD no longo prazo. A partir dos critérios que mencionamos na resposta anterior, acreditamos que seja importante o estabelecimento de uma métrica de referência para aferir os riscos, que reflita as variáveis decorrentes da **probabilidade de acontecer a violação, em contraste com o impacto se a violação acontecer**. Por fim, entendemos ser fundamental que seja oferecida autonomia para os controladores de dados poderem fazer exercício de análise de risco considerando as peculiaridades de seus próprios negócios. Considerando a natureza transversal da LGPD, entendemos perigosa a alternativa de se buscar estabelecer, por meio de norma, critérios prescritivos, pois as realidades das organizações que tratam dados pessoais são completamente distintas entre si.
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	Risco para o titular dos dados e danos ao titular dos dados têm sido, por vezes, equivocadamente usados como termos sinônimos. Entretanto, há diferenças fundamentais entre os conceitos: o risco para o titular dos dados geralmente é mais amplo do que o dano "real" e o precede; sugere que o dano "potencial" é passível de se concretizar - portanto, "risco" pode geralmente ser interpretado como "probabilidade razoável e/ou indício de

	materialização de dano". “Risco” e “dano” apontam para uma certa gravidade ou possibilidade de impacto sobre os titulares dos dados que estão sendo analisados e identificados pelo controlador antes que os requisitos de notificação sejam acionados. Os dois conceitos referem-se a diferentes estágios de um incidente relevante. Os riscos para os indivíduos devem ser interpretados como a possibilidade de que os danos à proteção de dados possam se materializar efetivamente, ao passo que o dano relevante é a materialização do risco e seus efeitos. Uma violação de dados pessoais pode revelar a existência de um risco significativo - caso em que o evento prejudicial permanece latente - ou de um dano relevante - caso em que há evidências suficientes de que o evento prejudicial já produziu seus resultados. Vejamos alguns exemplos de como os termos estão sendo utilizados em outras jurisdições: ● Na GDPR, a notificação de violação aos titulares de dados afetados deve ser emitida quando houver uma violação que *"provavelmente resultará em um alto risco para os direitos e liberdades das pessoas físicas"*[2]; ● Na Lei de Privacidade da Austrália, a notificação de incidente deve ocorrer quando uma *"pessoa razoável concluir que o [incidente] provavelmente resultaria em danos graves a qualquer um dos indivíduos a quem as informações se referem"*[3]; ● Na Lei de Privacidade da Nova Zelândia, a notificação deve ser realizada quando qualquer violação de privacidade que seja *“razoável acreditar que causou danos graves a um indivíduo ou indivíduos afetados ou é provável que o faça”*[4];

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679
[3] https://www.legislation.gov.au/Series/C2004A03712
[4] https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html

	● Na Lei de Proteção de Dados do Canadá, a notificação deve ser emitida quando a violação cria *"um risco real de danos significativos aos indivíduos afetados"*[5]. Similar às outras quatro jurisdições listadas acima, o Brasil parece ter uma abordagem comum na identificação de um requisito de "probabilidade" ("poderia") ao lado de um requisito de "gravidade" ("risco ou dano relevante"). Entretanto, entendemos que a ANPD deveria adotar o conceito de "risco" e seu contexto como apresentado na GDPR e, por outro lado, o conceito de "dano" e seu contexto, como apresentados nas legislações da Austrália, Nova Zelândia e Canadá, ao "risco relevante [de dano] ou dano" da LGPD. Essa clara dissociação facilitará o entendimento de que o "risco" está vinculado à probabilidade de um impacto ocorrer, enquanto o "dano" está vinculado a um impacto negativo já concretizado. Vejamos o que revelam juristas renomados acerca do tema: **Risco**, segundo Maria Helena Diniz: *"1. Possibilidade da ocorrência de um perigo ou sinistro causador de dano ou se prejuízo, suscetível a acarretar responsabilidade civil na sua reparação. 2. Medida de danos ou prejuízos potenciais, expressa em termos de probabilidade estatística de ocorrência e da intensidade ou grandeza das consequências previsíveis. 3. Relação existente entre a probabilidade de que uma ameaça de evento adverso ou acidente determinados, se concretize com o grau de vulnerabilidade do sistema receptor a seus efeitos."* (Dicionário Jurídico, Vol, 4, Ed. Saraiva. São Paulo, 1998); **Dano**, segundo Marcus Cláudio Acquaviva: *"Do latim damnu, prejuízo, perda. Prejuízo sofrido pelo patrimônio econômico ou moral de alguém. O dano pode ser material, também chamado real, quando atinge um bem economicamente apurável; ou moral,*

[5] https://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html

	quando macula bens de ordem moral, como a honra." (Dicionário Jurídico Brasileiro Acquaviva. 9ª edição revista, atualizada e ampliada. Ed. Jurídica Brasileira. São Paulo, 1998). Ou seja, o risco se caracteriza pela possibilidade de ocorrência de um dano e a probabilidade de real ocorrência do dano é um dos fatores a serem considerados para a medição de relevância do risco.
O que deve ser considerado na avaliação dos riscos do incidente?	Como mencionado anteriormente em nossa resposta à pergunta 1, entendemos que a avaliação dos riscos do incidente deve considerar: ● O contexto da operação de tratamento de dados e do próprio incidente de segurança; ● As boas práticas das empresas nas respostas a eventuais incidentes; ● O tipo de violação; ● A natureza dos dados pessoais objeto do incidente; ● O volume de dados; ● A probabilidade dos riscos se concretizarem; ● A previsibilidade; ● A gravidade; ● A boa-fé e as intenções dos terceiros que obtiveram acesso ou potencial acesso aos dados em função do incidente e a facilidade de identificação dos titulares por terceiros não autorizados; e ● O período de exposição ao risco/dano e a tempestividade de ações corretivas ou mitigatórias, considerando a data em que os dados pessoais ficaram expostos e o momento de correção ou reversibilidade da situação que gerou o risco/dano. Note-se que a lista elencada acima não implica necessariamente em uma consideração de pesos iguais dos vários fatores. Muitas vezes, os dados sujeitos ao incidente de segurança poderão não ser relevantes, como por exemplo a lista de todos os e-mails corporativos de uma determinada entidade.

	Na avaliação dos riscos do incidente, também é importante que seja considerado, além dos pontos listados na primeira pergunta: ● Se houve adulteração do dado pessoal do titular; ● Quem é o autor do fato que gerou o incidente; ● Possibilidade de verificação de origem e remediação e se possível, reversibilidade, do incidente; ● A concretização ou não do dano; e ● Avaliação da cadeia de custódia: conjunto de procedimentos documentados que registram origem, identificação, coleta, custódia, controle, transferência, análise e eventual descarte de evidências.
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	Entendemos que as informações listadas no §1º do art. 48 são suficientes para que a comunicação seja realizada com eficiência. Além dessas informações, da análise de caso a caso, a ANPD pode considerar fornecer aos controladores a oportunidade de esclarecer antecipadamente se o incidente está em andamento, se a investigação e a notificação são preliminares ou completas, e qual a classificação do risco e gravidade. Recomendamos também que a ANPD elabore um modelo de formulário simplificado e automatizado, que dê celeridade aos controladores na comunicação de riscos ou danos relevantes. Nesse particular, recomendamos como referência o formulário adotado pela Autoridade de Proteção de Dados Espanhola como um modelo interessante e educativo. Nesses moldes, o peticionamento eletrônico realizado à ANPD deveria ser eficiente e sistêmico. Em consonância com o princípio de minimização, conforme defendido pelo *Information Commissioner's Office do Reino Unido* (ICO), sugere-se que quaisquer outras informações a serem comunicadas, para além daquelas previstas no no §1º do art. 48, sigam os seguintes preceitos:

	● Adequação - as informações devem ser adequadas aos propósitos da comunicação. ● Relevância - deve haver um racional por detrás do compartilhamento daquela informação em específico. ● Mínimo Necessário - as informações compartilhadas devem corresponder ao mínimo necessário para que a comunicação seja eficiente. Caso neste primeiro momento as informações não sejam todas fornecidas, faz-se necessário também indicar se demais informações serão transmitidas posteriormente, bem como quais os meios estão sendo utilizados para obtê-las. Por fim, cumpre destacar que a ANPD deverá, obrigatoriamente manter os formulários de comunicação de incidentes como confidenciais, de modo a evitar possíveis prejuízos aos agentes de tratamento e até mesmo aos titulares dos dados antes que se tenha a oportunidade de aferir os riscos efetivos e adotar as medidas cabíveis de mitigação.
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	Considerando o prazo de 72 (setenta e duas) horas estabelecido pela GPDR (art. 33), aplicável a países que vivenciam a cultura de proteção de dados há aproximadamente três décadas, seria razoável estabelecer no Brasil um prazo maior, já que o país passou a experimentar condutas relacionadas há pouquíssimo tempo, e ainda está em fase de adaptação e aprendizagem. A camara-e.net entende que o prazo sugerido de 02 (dois) dias úteis para notificar um incidente seria bastante oneroso e impraticável, principalmente se os controladores de dados em questão tivessem muitos clientes e, especialmente considerando a quantidade de detalhes que uma notificação deve conter, conforme § 1º do art. 48 da LGPD. Apoiamos o padrão existente da LGPD, que não estabelece um prazo fixo para a notificação e coloca sobre a organização o ônus de garantir que a

	notificação foi emitida em tempo hábil. Cronogramas de notificação fixos têm a consequência não intencional de notificações apressadas por medo de sanções antes que uma avaliação completa dos eventos possa ser realizada. Isso cria um senso de urgência que pode, inadvertidamente, resultar em uma situação em que a notificação deve ser complementada ou retificada conforme a avaliação evolui, criando risco de responsabilidade para a organização mesmo quando ela está agindo com o maior padrão de diligência e cuidado. A ANPD deve considerar a manutenção do padrão existente e, ao mesmo tempo, fornecer orientações adicionais sobre notificações oportunas e como as organizações podem demonstrar que cumpriram o prazo razoável estabelecido pela LGPD. Caso a ANPD decida não incorporar esta sugestão, sugerimos a implementação de uma comunicação mais detalhada, com prazo maior, de 50 dias úteis contados da ciência inequívoca do incidente, sendo um incidente de segurança definido como qualquer evento adverso, confirmado relacionado à segurança de sistemas de informação levando a perda de um ou mais princípios básicos de Segurança da Informação: Confidencialidade, Integridade e Disponibilidade. Importante ressaltar também que, seguindo as recomendações do Grupo de Trabalho Artigo 29, sugere-se que o momento de início da contagem do prazo para comunicação é aquele no qual o controlador tem um nível de certeza razoável de que um incidente ocorreu e, portanto, já começou a tomar medidas de contenção de danos. Destaca-se que nos casos em que quais o controlador for notificado por um indivíduo, organizações da sociedade civil, autoridades, operadores e sub operadores ou qualquer outra fonte, de um possível incidente, o período no qual o controlador conduzirá investigações internas para confirmar a ocorrência do incidente não deve ser entendido como momento de confirmação - novamente, este só será computado quando da constatação definitiva de que o incidente envolvendo dados pessoais com risco ou dano relevante existe.

	Por fim, sugerimos que a ANPD consulte a Nota de Orientação da ANPD irlandesa[6] sobre notificação de violação de dados, que fornece um exemplo útil de orientação sobre o assunto, e que pode servir como um ponto de referência.
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	Considerando o prazo de 72 (setenta e duas) horas estabelecido pela GPDR, aplicável a países que vivenciam a cultura de proteção de dados há aproximadamente três décadas, seria razoável estabelecer no Brasil um prazo bem maior, já que o país passou a experimentar condutas relacionadas há pouquíssimo tempo, e ainda está em fase de adaptação e aprendizagem. A contagem deste prazo deveria ocorrer após a constatação inequívoca do incidente e a sua respectiva comunicação final à ANPD. Recomendamos que os controladores informem os titulares dos dados sem atrasos indevidos, após determinar que um incidente requer notificação (ao invés de definir um período específico). Caso seja necessária a definição de um período, sugerimos que, após notificar a ANPD, o controlador deverá ter até 30 (trinta) dias para analisar e avaliar os riscos e danos atrelados ao incidente de segurança confirmado, conforme os critérios que apresentamos acima. Caso identificado que o incidente em questão possa acarretar riscos ou danos relevantes aos titulares envolvidos, a notificação ao titular deve ser realizada em no mínimo 10 (dez) dias úteis, listando as informações listadas no §1º do art. 48. Isto porque nosso entendimento é de que permitir que as organizações tenham mais tempo para realmente entender o ocorrido e avaliar o verdadeiro risco do incidente significará que os titulares envolvidos receberão relatórios de melhor qualidade, com acesso apenas a informações relevantes, além de permitir que as organizações tenham tempo para realmente lidar com os incidentes de forma adequada antes de causar qualquer tipo de euforia pública.

[6] https://www.dataprotection.ie/sites/default/files/uploads/2019-10/Data%20Breach%20Notification_Practical%20Guidance_Oct19.pdf

	No que diz respeito ao conteúdo da comunicação, este deve limitar-se às informações úteis para o indivíduo, como os contatos do responsável pela proteção de dados em caso de dúvidas ou preocupações, e que podem ajudar o indivíduo a proteger os seus dados. Este último deve incluir as medidas específicas identificadas pelas organizações que podem ser adotadas pelos próprios indivíduos. Em consonância com o parágrafo anterior, entendemos que o conteúdo da comunicação às pessoas físicas não deve ser igual ao conteúdo da notificação dirigida à ANPD. Esses avisos têm finalidades diferentes e, portanto, requerem informações e estilos de comunicação diferentes. Fazer o aviso a pessoas alinhadas com o objetivo da referida comunicação, que é informar as pessoas sobre quaisquer riscos residuais e como se proteger, usando uma linguagem facilmente compreensível, tornaria a LGPD mais interoperável com outras leis de proteção de dados. Com base no defendido nas respostas anteriores, entende-se que a notificação de incidentes à ANPD, por parte do controlador, é obrigatória, a menos que o risco de o incidente causar danos relevantes aos direitos e liberdades individuais não esteja presente. Esse raciocínio implica que o patamar para notificação do titular é mais alto, de modo que o número de incidentes reportados aos titulares será menor. Tomando como referência o disposto na GPDR (art. 34), a comunicação para os titulares pode conter, a depender da avaliação do controlador, as seguintes informações: ● Descrição das possíveis consequências do incidente para o titular, bem como as medidas adotadas pelo controlador para controlar o incidente e mitigar os possíveis danos; ● Pontos de contato para obtenção de mais informações acerca do incidente; e ● Ações que o titular pode realizar para mitigar possíveis riscos/danos (como atualização de senha, por exemplo).

Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	Deve ser considerado o volume de dados envolvido e a quantidade de indivíduos afetados para avaliar a possibilidade e proporcionalidade da medida de comunicação direta e individual, ou por meio de newsletter, boletins informativos, divulgação em grandes meios de comunicação, etc. A forma de comunicação deve ficar à critério do controlador, possibilitando que adote seus próprios canais de comunicação, preservando a experiência do titular e a escalabilidade da comunicação. Na hipótese de a comunicação ao titular envolver esforço desproporcional, deveria ser admitida comunicação pública ou medida similar informando os titulares de dados de forma eficaz. Nesse sentido, pode-se utilizar como exemplo as disposições da GDPR. Considera-se que o esforço de comunicação individual ao titular é desproporcional nos casos em que os esforços para a comunicação excederem os limites técnicos razoáveis, tendo como referência o número de titulares afetados, bem como os custos da comunicação. Sugerimos que os seguintes métodos de comunicação também sejam considerados suficientes: (A) Notificação por e-mail; (B) Outro aviso eletrônico razoavelmente calculado para chegar ao indivíduo afetado; e (C) Quando nenhum outro método estiver disponível ou o custo do aviso for desproporcional, aviso público por meio de postagem no site do controlador com duração de ao menos 30 (trinta) dias. Caso o risco já tenha sido mitigado, sem qualquer impacto para o titular, a comunicação pelo controlador deveria ser facultativa. Nesse sentido, a GDPR já dispõe sobre essa possibilidade em seu artigo 34.3[7].

[7] https://gdpr-info.eu/art-34-gdpr/

Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	Entendemos que a norma deveria dispensar da obrigatoriedade da comunicação os casos em que medidas de segurança apropriadas forem implementadas imediatamente após o incidente ou as medidas implementadas anteriormente tenham sido suficientes para limitar os efeitos do incidente. Por exemplo, de acordo com a Lei de Privacidade da Irlanda[8], caso os dados envolvidos em uma violação tenham sido criptografados em um nível apropriado, a notificação não é necessária. O mesmo se aplicaria para os casos em que, apesar de não criptografados, os dados que foram acessados ou roubados foram anonimizados dentro da organização, de modo que, sem a chave para desbloquear os dados, eles se tornam não identificáveis (pelo menos não sem habilidade significativa e informações adicionais que as informações não foram roubadas), então tais incidentes não precisariam ser notificados à ANPD ou aos titulares. Além disso sugerimos que a ANPD considere adotar uma listar com categorias de incidentes que não requerem comunicação (o que é uma prática em alguns outros países da América Latina, como México e Colômbia, por exemplo): ● quando os dados pessoais se referem somente a informações de contato profissional (particularmente se já estiverem disponíveis publicamente - por exemplo, em um site da empresa); ● quando os dados pessoais se referem apenas a informações da "lista telefônica" que já são de domínio público; ● se imediatamente após o incidente a organização tiver tomado ações/medidas subsequentes que garantam que o nível de risco necessário para acionar a notificação às pessoas afetadas (o qual sugerimos que seja um "alto risco") não se concretize mais (por exemplo, se a organização tiver imediatamente identificado e tomado medidas contra a pessoa que acessou os dados pessoais antes que ela pudesse fazer algo com eles); e

[8] http://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html

	● quando é improvável que o risco/ dano resultante da violação de dados se materialize.
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	Neste momento, a LGPD estabelece o mesmo limite de risco para notificações à ANPD e aos afetados. Isso não está de acordo com as leis internacionais de proteção de dados e acarreta o risco de relatórios excessivos e custos administrativos para as partes interessadas, conforme observado anteriormente. Sugerimos limitar as comunicações aos indivíduos aos casos em que a organização estabelece que o incidente provavelmente resultará em alto risco ou dano relevante para os indivíduos afetados. Hipóteses nas quais os controladores não deveriam ter a obrigação de comunicar o incidente aos titulares: ● Se, antes da violação, o controlador tiver implementado medidas técnicas e organizacionais aptas a proteger os dados pessoais, tornando-os ininteligíveis para qualquer pessoa que não esteja autorizada a acessar aquele banco de dados; ● Se, imediatamente após uma violação, o controlador tomar medidas para garantir que o alto risco para os direitos e liberdades dos titulares não se materialize; e ● Se a comunicação com os titulares demandar esforços desproporcionais.
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	Os critérios a serem considerados, de maneira cumulativa, pela ANPD para determinar a gravidade do incidente podem incluir: ● O tipo de violação (por exemplo, dependendo do cenário, uma violação de confidencialidade pode ter um impacto maior do que se os dados fossem simplesmente perdidos ou excluídos); ● A natureza e a sensibilidade dos dados pessoais (quanto mais sensíveis os dados, maior o risco de dano às pessoas afetadas);

	● Facilidade de identificação inequívoca de indivíduos; ● Gravidade das consequências para os indivíduos (por exemplo, violações onde há evidências de malfeitores acessando dados pessoais podem indicar maior risco do que violações onde os dados são divulgados acidentalmente); e ● Características especiais do indivíduo afetado (por exemplo, dados relativos a crianças/outros indivíduos vulneráveis podem colocá-los em maior risco). Os critérios atenuantes a serem considerados são: ● A boa-fé e as intenções dos terceiros que tiveram acesso aos dados após o incidente; e ● O quantitativo de indivíduos afetados, desde que isso não seja um critério de caráter primário de avaliação. Também é necessário evitar uma avaliação de risco ou dano baseada em eventos hipotéticos ou possibilidades remotas, ou com uma visão do que a violação poderia materializar-se no futuro. A partir destes critérios listados acima, entendemos que cabe ao controlador, considerando o contexto e as especificidades de sua atividade empresarial, decidir sobre a gravidade do incidente.
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	Sim, sugere-se que a análise da gravidade do incidente siga a metodologia indicada na resposta à segunda questão. A metodologia mais recomendada para a análise de gravidade de incidentes de segurança é a gestão de risco. A gestão de risco é um elemento central do princípio de responsabilidade e prestação de contas, fazendo com que as organizações maximizem os benefícios potenciais do tratamento de dados, ao mesmo tempo em que reduz de forma mais eficaz quaisquer impactos negativos potenciais sobre os titulares de dados, na medida em que prioriza a identificação e a análise de riscos, bem como a

	tomada de decisões que sejam escalonáveis e proporcionais aos fatos e contextos nas quais o controlador está inserido. O objetivo do processo de gerenciamento de risco é, portanto, fornecer respostas proporcionais que reduzam o risco da forma mais prática possível e identifiquem os riscos remanescentes e como eles serão gerenciados. Citamos abaixo documentos nos quais essa metodologia é explorada de forma aprofundada, ressaltando que não devem ser entendidos como rol taxativo ou exaustivo. Tratam-se de referências voluntárias amplamente divulgadas e adotadas pelos setores econômicos: ● ISO 31000:2009 Risk management — Principles and guidelines; ● ISO/IEC 27035-2:2016 Information Technology — Security Techniques — Information Security Incident Management; e ● ENISA 2013 Principles[9].
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	É importante frisar que o simples fato de ter ocorrido um incidente de segurança não significa necessariamente que as medidas técnicas e organizacionais de segurança implementadas tenham sido insuficientes. De toda forma, eventuais sugestões de providências deverão depender do incidente de segurança da informação identificado e da estrutura do controlador, exigindo que a ANPD realize uma análise de caso a caso e até mesmo recorrência de um incidente de segurança de determinada natureza dentro da organização. Realização de análise “post mortem” do incidente, para verificação de suas causas, condições e consequências e listagem dos pontos de melhoria que podem ser adotados com o objetivo de evitar novas ocorrências semelhantes. Caso a pergunta seja reformulada para considerar as medidas que a ANPD pode esperar que as organizações implementem após tomarem conhecimento de um incidente que desencadeia uma notificação. Nesse contexto, a ANPD pode desejar considerar o item 8 do Guia da AEPD sobre

[9] https://www.enisa.europa.eu/publications/dbn-severity

	Gerenciamento e Notificação de Violação de Dados Pessoais[10], que inclui as seguintes categorias de medidas: ● Contenção de incidentes: tomar decisões rápidas, como desligar um sistema, isolando-o da rede e desativando certas funções; ● Solução / Erradicação: medidas destinadas a resolver certos efeitos do incidente de segurança, como por exemplo, eliminar malware ou desativar contas comprometidas; ● Recuperação: medidas que visam restabelecer totalmente os serviços aos seus níveis normais e evitar, na medida do possível, a ocorrência de novas ocorrências pela mesma causa; ● Coleta e custódia de provas: nesta etapa, serão realizadas as ações necessárias para conter e reverter o impacto que uma violação de dados pessoais poderia ter causado. Essas ações podem causar a modificação das evidências, o que pode inviabilizar a utilização das informações registradas pelos sistemas envolvidos para o envio a terceiros, pois poderia impactar a cadeia de custódia para utilização em processos judiciais; e ● Relatório de Comunicação/Resolução: todo o processo de resposta a incidentes deve ser devidamente documentado, incluindo as conclusões dos técnicos e chefes de equipe, de forma a extrair lições aprendidas e a serem incluídas em um relatório de resolução. De acordo com a relevância do incidente a ANPD poderá solicitar aos controladores um relatório detalhado do incidente, que contemple todas as ações e controles de segurança já implementados, de forma que a ANPD possa avaliar e solicitar medidas técnicas e administrativas, avaliar o quão diligente é o controlador no tema proteção de dados, bem como solicitar medidas técnicas e administrativas até o momento não executadas. A ANPD poderá utilizar um modelo pré-definido de relatório, com questões objetivas e expectativa de detalhamento que deverá ser utilizado pelas empresas para a documentação de todo o incidente de segurança. Isso

[10] https://www.aepd.es/sites/default/files/2019-09/guia-brechas-seguridad.pdf

	permitirá identificar as práticas e controles que potencialmente falharam e permitiram a materialização do incidente caso aplicável.
Outras Sugestões	Deve haver isenção de penalidades no caso de o controlador ter adotado as medidas técnicas, administrativas e físicas cabíveis (e dentro do seu controle) para prevenir o incidente e, quando da sua ocorrência, para mitigar os riscos atrelados a ele. É importante que sejam adotadas medidas para restringir a publicidade das investigações em curso, para garantir a integridade dos procedimentos investigatórios e não afetar desnecessariamente a reputação da empresa. Como a obrigação de reportar o incidente recai sobre o controlador e, em muitos casos, ele depende de uma prévia comunicação do operador, o controlador deve ser definido como único responsável pelo reporte do incidente. O operador, por sua vez, deveria ter um prazo mínimo de 72 (setenta e duas) horas para reportar ao controlador eventual incidente, independentemente de o contrato entre as partes prever essa obrigação, ficando facultado eventual negociação deste prazo de comum acordo entre as partes. Deve ser considerada a existência de governança, políticas e demais práticas internas do controlador para proteger os dados pessoais, bem como a ausência de reincidência, para a aplicação de penalidade ao controlador.
SUGESTÃO DE NORMATIVO, SE HOUVER	
Art. Xxxx	

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: CENTRO DE ESTUDOS EM POLÍTICA E ECONOMIA DO SETOR PÚBLICO | EESP e EASP | FUNDAÇÃO GETULIO VARGAS

CPF/CNPJ: 33.641.663/0001-44

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regularmente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos

titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS

IMPORTANTE: Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.

TÓPICO/QUESTÃO	CONTRIBUIÇÃO/INSTITUIÇÃO
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	**Um incidente de dados pode acarretar risco quando ocorrer as situações listadas, de forma acidental, ilegal e/ou não autorizada (i) acesso (inclusive divulgação, vazamento ou compartilhamento); (ii) modificação (comprometendo a qualidade dos dados) ou; (iii) eliminação e perda de dados pessoais. Em outras palavras, é preciso avaliar se o incidente afetou a confidencialidade, a integridade ou validade dos dados pessoais, Neste sentido, pode-se indicar o documento da autoridade do Reino Unido - https://ico.org.uk/for-organisations/report-a-breach/.** **Alguns dados podem gerar impactos maiores na vida dos cidadãos, de forma que incidentes envolvendo-os certamente devem ser considerados relevantes, como:** - **dados pessoais sensíveis (como dado sobre raça, grupos étnicos, vida sexual ou saúde);** - **dados de localização/deslocamento dos titulares;** - **dados de crianças e adolescentes;** - **dados pessoais relativos a processos penais ou condenações criminais;**

	- dados genéticos; **- dados de monitoramento direto (através de câmeras de reconhecimento facial, por exemplo) ou indireto (através da localização de celulares) de áreas públicas/publicamente acessíveis, especialmente considerando;** **- dados sobre desempenho de atividades laborais de funcionários/empregados/colaboradores/prestadores de serviço** **- dados biométricos capazes de identificar os indivíduos;** **- dados relativos a endividamento dos titulares.** **Envolvendo tais tipos de dados, entre outros, o vazamento já deve ser considerado relevante.**
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	**Estamos em um momento de maturação e consolidação da cultura de proteção de dados. O processo de classificação não deve impedir/limitar a obrigatoriedade do controlador reportar incidentes, inclusive porque a experiência dos casos reportados certamente ajudará a estruturar, no futuro, uma classificação adequada ao país e ao ordenamento jurídico nacional. Dessa forma, caso haja uma classificação de riscos relevantes, é importante que esta não impacte o processo de reporte à ANPD de qualquer incidente de dados. Por conta disso, acreditamos que riscos/danos baixos - especialmente caso contenham um dos tipos de dados apontados acima - devem ser considerados relevantes.** **Recomendamos que, ao invés de imputar adjetivos como "baixo, médio ou alto", a ANPD organize os incidentes por quatro indicadores para a finalidade de priorizar e distribuir os casos internamente:** **- número de titulares afetados;** **- a quantidade e tipos de dados diferentes envolvidos no incidente;** **- a distribuição temporal dos dados envolvidos no incidente (variando desde dados referentes a um momento específico até o acúmulo de informações produzidas ao longo do tempo);** **- a extensão geográfica dos dados envolvidos.**

Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	**O risco é a probabilidade da ocorrência de um evento prejudicial ao passo que o dano é o prejuízo ocorrido. Atividades de tratamentos possuem um risco inerente de gerar danos aos titulares de dados. Em outras palavras, é impossível que o tratamento tenha risco zero.** **Da perspectiva individual dos titulares, o risco se relaciona com a probabilidade de gerar dano a direitos e liberdades individuais. Da perspectiva coletiva, o não cumprimento da legislação de proteção de dados gera um dano difuso para a sociedade. Ou seja, a falta de gerenciamento adequado dos riscos, acarreta um dano - ainda que apenas se possa concebê-lo da perspectiva coletiva e difusa - induzindo responsabilização dos agentes de tratamento.** **Logo, a priori, a partir do momento que o incidente de dados já ocorreu, o dano já deve se pressupor materializado bem como o prejuízo para a sociedade. O controlador pode tentar demonstrar, no entanto, que o incidente ocorreu apesar da sua capacidade ou do alcance de seu gerenciamento de risco. Além disso, o dano gerado pode ser reduzido, a depender da gestão do incidente feita pelo agente de tratamento.**
O que deve ser considerado na avaliação dos riscos do incidente?	**O risco é a probabilidade da ocorrência de um evento prejudicial ao passo que o dano é o prejuízo ocorrido. Atividades de tratamentos possuem um risco inerente de gerar danos aos titulares de dados. Em outras palavras, é impossível que o tratamento tenha risco zero.** **Da perspectiva individual dos titulares, o risco se relaciona com a probabilidade de gerar dano a direitos e liberdades individuais. Da perspectiva coletiva, o não cumprimento da legislação de proteção de dados gera um dano difuso para a sociedade. Ou seja, a falta de gerenciamento adequado dos riscos, acarreta um dano - ainda que apenas se possa concebê-lo da perspectiva coletiva e difusa - induzindo responsabilização dos agentes de tratamento.** **Logo, a priori, a partir do momento que o incidente de dados já ocorreu, o dano já deve se pressupor materializado bem como o prejuízo para a sociedade. O controlador pode tentar demonstrar, no entanto, que o incidente ocorreu apesar da sua capacidade ou do alcance de**

	seu gerenciamento de risco. Além disso, o dano gerado pode ser reduzido, a depender da gestão do incidente feita pelo agente de tratamento.
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	**Os controladores deveriam notificar, além dos dados já descritos na legislação, dados sobre:** **- tipo do incidente (acesso, moficiação ou eliminação não autorizada/ilegal de dados pessoais).** **- categorias dos titulares de dados pessoais afetadas pelo incidente (se são dados pessoais de usuários, clientes, funcionários, estudantes, crianças, adolescentes, pacientes, pessoas vulneráveis – Cadúnico, etc).** **- a distribuição temporal dos dados envolvidos no incidente (variando desde dados referentes a um momento específico até o acúmulo de informações produzidas ao longo do tempo);** **- a extensão geográfica dos dados envolvidos.** **A ANPD também pode solicitar informações relativas ao cumprimento normativo, como:** **- Treinamentos relacionados à privacidade de dados fornecidos aos funcionários da entidade que teve os dados vazados,** **- Governança relacionado à privacidade e proteção de dados;** **1) política de privacidade,** **2) plano de resposta a incidentes,** **3) termo de uso,** **4) relatório de impacto,** **5) ciclo de vida dos dados** **6) Organograma da equipe responsável por proteção de dados, etc**
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	**O prazo deve ser o mais breve possível, considerando o tempo médio que uma pessoa jurídica pode levar para identificar a ocorrência de um incidente.**

	Nesse sentido, vale seguir o prazo de dois dias, considerando as consequências que incidentes de dados podem ter, e a existência de uma resolução nacional que determina tal prazo.
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	**Notificada a ANPD em dois dias, os agentes de tratamento devem possuir no máximo mais sete dias para notificar os titulares, tendo tempo suficiente para gerir o incidente e reduzir possíveis danos dele decorrente. Ou seja, desde que se saiba do incidente, o processo de notificação dos titulares não deve passar de 9 dias.**
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	**Cabe a comunicação individual e coletiva. A primeira é importante dada a rapidez da comunicação direta com o titular. A comunicação individual pode ser feita por SMS, notificação em aplicativo, whatsapp e/ou e-mail. Comunicações via correio devem ser utilizadas em último caso dado tempo da postagem e recebimento.** **A segunda possibilita maior exposição do reporte, trazendo, inclusive, maior transparência da situação. Por ser feita por notas de divulgação à imprensa e/ou publicação no site da entidade.**
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	**Em um primeiro momento, a existência de exceções de informação à ANPD pode não ser estratégica para a consolidação da cultura da proteção de dados e da transparência sobre os fluxos das informações pessoais.** **A ICO, por exemplo, traz um breve questionário online que auxilia pessoas físicas e jurídicas a avaliarem a necessidade do reporte .(https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach-assessment/). Tal metodologia possibilita que o indivíduo ou entidade realize uma avaliação do incidente, bem como a necessidade da comunicação. Simplificadamente, caso seja obrigatória a**

	realização de relatório de impacto para o tratamento sobre o qual houve o incidente, este deve ser reportado. **Assim, por exemplo, o reporte deve ser feito caso os dados dados pessoais refiram-se a pessoas vivas e identificáveis, caso haja mais de um tipo de dado pessoal, caso os dados refiram-se a um histórico e casa haja dados considerados especiais (dados pessoais sensíveis; localização/deslocamento dos titulares; dados de crianças e adolescentes; dados relativos a processos penais ou condenações criminais; dados genéticos; dados de monitoramento de áreas públicas/publicamente acessíveis; dados sobre desempenho de atividades laborais de funcionários/empregados/colaboradores/prestadores de serviço; dados biométricos capazes de identificar os indivíduos; dados relativos a endividamento dos titulares).**
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	**Mesma resposta da questão anterior.**
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	**Consideramos que um incidente já é, por si só, um risco materializado, ou seja, um dano.** **Para a finalidade de avaliar este dano e mensurar sanções, deve-se considerar:** - **o tipo dos dados afetados pelo incidente, sendo que o dano deve ser considerado maior havendo um dado de categoria especial (dados pessoais sensíveis; localização/deslocamento dos titulares; dados de crianças e adolescentes; dados relativos a processos penais ou condenações criminais; dados genéticos; dados de monitoramento de áreas públicas/publicamente acessíveis; dados sobre desempenho de atividades laborais de funcionários/empregados/colaboradores/prestadores de serviço; dados biométricos capazes de identificar os indivíduos; dados relativos a endividamento dos titulares);** - **o número de titulares afetados;** - **a diversidade de tipos dados diferentes envolvidos no incidente;**

	- **a distribuição temporal dos dados envolvidos no incidente (variando desde dados referentes a um momento específico até o acúmulo de informações produzidas ao longo do tempo);** - **a extensão geográfica dos dados envolvidos.**
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	**Seguem dois exemplos de metodologias:** **Reino Unido: https://ico.org.uk/for-organisations/gdpr-resources/pdb/** **Espanha: https://www.aepd.es/sites/default/files/2019-09/guia-brechas-seguridad.pdf**
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	**Após realizado registro, análise e classificação do incidente, a ANPD deve indicar ao agente de tratamento dois grupos de medidas - um deles voltado a própria gestão do incidente e outro para a fiscalização desta gestão:** **Para gestão do incidente, sugere-se de forma exemplar algumas medidas:** **a) contenção** - **Evitar o acesso ao meio que originou (fonte) a divulgação (vazamento), como, por exemplo, domínios, servidores, conexões (inclusive remotas), computadores, pastas.** - **Realizar a atualização software de detecção (antivírus, IDS, etc.) bloqueando o tráfego, desativar dispositivos, servidores, etc.** - **Suspender credenciais lógicas e físicas com acesso a informações privilegiadas, mudando todas as senhas de usuários ou orientando os próprios usuários a fazê-los com segurança.** - **Fazer uma cópia do sistema (clonado). Faça uma cópia bit a bit do disco rígido que contém o sistema e, em seguida, analise a cópia usando ferramentas forenses.** - **Isolar o sistema usado para revelar os dados para posterior análise forense.**

	- **Se os dados foram enviados para servidores públicos, peça ao proprietário (ou webmaster) para excluir os dados divulgados.** - **Caso não seja possível remover os dados divulgados, forneça uma análise completa ao departamento que tenha como função o contato com as autoridades competentes.** - **Acompanhar a divulgação dos documentos / dados vazados nos diversos sites e redes sociais (FB, Twitter, etc.), bem como os comentários e reações dos internautas.** **b) erradicação:** - **Definir o processo de desinfecção, com base em ferramentas, novas versões/revisões de softwares, etc, e certificar-se de que o processo de desinfecção funciona corretamente sem ocorrência de danos. Talvez haja a necessidade de eventuais aprovações para esse processo.** - **Verificar a integridade de todos os dados armazenados no sistema, por meio de um sistema de hashes, por exemplo.Para garantir que não foram modificados, deve ser dada atenção redobrada aos arquivos executáveis, isto é, aqueles que não foram comprometidos.** - **Revisar o planejamento e a atualização dos mecanismos e assinaturas de antivírus.** - **Verificar o antivírus de todo o sistema, discos rígidos e memórias.** - **Restaurar as conexões gradualmente, estabelecendo acesso restrito especial para máquinas remotas ou não gerenciadas.** - **Definir um prazo para a implementação das tarefas de erradicação.** - **Para casos complexos, as diferentes equipes devem ter sua atuação coordenada.** - **Após aplicar as medidas, deve-se verificar o seu correto funcionamento.**

	- **Verificar se as medidas adotadas possuem caráter temporário ou definitivo.** - **Verificar se o sistema afetado, e/ou as informações retornaram ao seu estado original.** - **Certificar-se que a vulnerabilidade não poderá ser explorada no futuro. Isso poderá alterar a avaliação de risco do sistema afetado, dessa forma, a depender da situação ocorrida, cabe a reavaliação dos Formulários de Avaliação de Risco.** **Para fiscalização da gestão do incidente, sugere-se:** **- Solicitar aos controladores, quais são os processos de resposta, contenção, solução/ erradicação e recuperação elaborados pelos controles para mitigar os danos consequentes do incidente. Isto é, solicitar o plano de resposta ao incidente identificado.** **- Identificar eventuais falhas no plano de resposta ao incidente apresentado.** **- Participar ativamente do processo de investigação do incidente, bem como identificar eventuais responsáveis.** **- Solicitar ao controlador a realização de treinamento sobre proteção e privacidade de danos obrigatório a todos os funcionários. A ANPD pode participar da elaboração do treinamento, bem como de plano de adequação para mitigar riscos relacionados à proteção de dados.** **- Instauração de processo de fiscalização regular para verificação da implementação do plano.** **- Aplicação de multa ao controlador, caso couber.**

SUGESTÃO DE NORMATIVO, SE HOUVER	
Art. Xxxx	
Art. Xxxx	

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: Núcleo de Informação e Coordenação do Ponto BR – NIC.br, Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil – CERT.br.

CPF/CNPJ: 05.506.560/0001-36

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

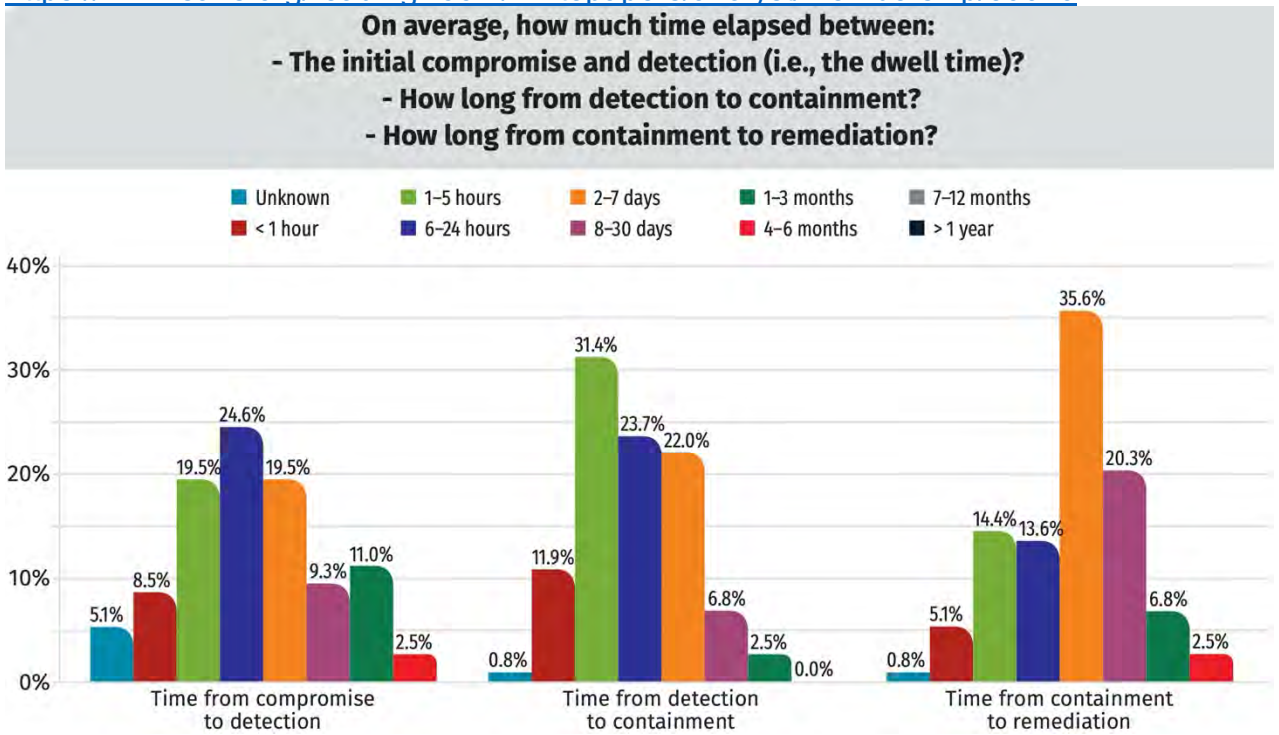
As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS **IMPORTANTE:** Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
1. Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	Um incidente pode acarretar risco ou dano a um titular quando as consequências da exposição de dados pessoais puderem levar o titular a sofrer: • risco de morte ou dano físico • preconceito • furto de identidade / prejuízos financeiros • dano à reputação / constrangimento • perda de acesso a sistemas relevantes para o titular
2. O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	Em nossa interpretação o texto da lei ao dizer “risco ou dano relevante” já reduz o escopo da comunicação apenas a incidentes de alto risco.
3. Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	O Risco é a <u>possibilidade</u> de sofrer dano ou perda: – há sempre a presença da incerteza – precisa ter uma condição de risco, ou seja, é necessário haver uma ameaça e uma vulnerabilidade no ativo – há um dano (consequência) somente se o risco for realizado (concretizado) Dano é a realização do risco, em que o dano <u>deixa de ser uma possibilidade e foi confirmado:</u>

	– não há mais incerteza – é possível comprovar o dano Estas definições são pacíficas em vários *frameworks* de segurança e gestão de risco, como OCTAVE, CERT RMM e normas do NIST. Referências: *CERT-RMM Glossary of Terms* https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=514932 https://resources.sei.cmu.edu/asset_files/BookChapter/2016_009_001_514934.pdf *NIST Glossary* https://csrc.nist.gov/glossary/term/risk https://csrc.nist.gov/glossary/term/harm https://csrc.nist.gov/glossary/term/impact https://csrc.nist.gov/glossary/term/damage *Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process* https://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf
4. O que deve ser considerado na avaliação dos riscos do incidente?	1. Gravidade das consequências para o titular, conforme resposta à questão 1. 2. Nível de exposição dos dados pessoais: • ex. 1: furto de dados em claro vs. dados cifrados • ex. 2: dados foram divulgados publicamente vs. estarem apenas em fóruns privados ou não divulgados 3. Complexidade técnica para fazer uso dos dados pessoais: • ex.: **furto do *hash* da senha** (exige conhecimento sobre uso de *software* de quebra de criptografia e, potencialmente, não seriam afetados sistemas bem implementados ou usuários com senhas fortes) **vs. furto da senha em texto claro** (qualquer atacante pode abusar dos dados e todos os usuários são afetados igualmente)
4. Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	As informações listadas no §1º do art. 48 nos parecem apropriadas e suficientes.
5. Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	Para que uma organização consiga reunir todas as informações requeridas pelo §1º do art. 48 é necessário que ela faça um processo completo de detecção, análise, contenção e remediação do incidente. Esse tempo é variável dependendo da complexidade do incidente, do número de sistemas envolvidos, e do tamanho e da experiência da equipe envolvida no processo. Há poucos dados públicos com métricas sobre tempo médio para resposta a um incidente, mas uma pesquisa realiza pelo *SANS Institute* em 2019 revelou alguns dados interessantes sobre o tempo dispendido em cada uma das duas fases desse processo:

	– tempo entre a detecção e a contenção de um incidente: 89% das organizações conseguem fazer este processo em até 7 dias; – tempo entre a contenção e a remediação de um incidente: 68.7% das empresas conseguem fazer este passo em até 7 dias, sendo que o número sobre para 89% se contarmos todos que conseguem fazer em até 30 dias. Nossa recomendação: seria ideal um prazo de 30 dias, mas nunca menor do que 2 semanas, dado que a comunicação à ANPD vai envolver além do processo técnico (que é o que a pesquisa citada considera), também um relatório jurídico interno, o que demandará mais tempo. Referências: SANS 2019 Incident Response (IR) Survey: It's Time for a Change https://www.sans.org/reading-room/whitepapers/analyst/membership/39070  Figura 2 do relatório, página 4: Tempos do comprometimento à remediação
6. Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que	O prazo deveria ser o mesmo da questão anterior. Para este público a informação deve ser em outra linguagem, simplificada e sem excesso de detalhes técnicos. Ao titular é importante priorizar informações sobre quais dados foram afetados, o que o titular deve fazer a respeito e como ele pode monitorar o uso abusivo de seus dados, incluindo possíveis riscos e danos.

informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	
7. Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	É desejável uma comunicação direta com o titular, principalmente em casos graves que podem levar a danos maiores, via o meio usual de comunicação do controlador com o titular. Obrigar um meio específico poderia criar uma coleta excessiva de dados, obrigando o controlador a coletar um dado cadastral específico (por exemplo, obrigar o uso de via postal, obrigaria o controlador a coletar o endereço, mesmo que isso não fosse necessário). Divulgação em meios de comunicação pública não garantem que o titular será informado, principalmente nos tempos atuais em que os veículos tradicionais estão perdendo audiência e não há plataformas na Internet que atinjam toda a população.
8. Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	Nossa interpretação do art. 48 é de que só devem ser comunicados à ANPD incidentes em que há confirmação de dano ou risco relevante ao titular, ou seja, incidentes de alto risco, desta forma não caberiam exceções.
9. Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	Idem à questão anterior.
10. Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	Os critérios elencados nas contribuições para as questões 1 e 4.
11. Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	Existem metodologias para Tratamento de Incidentes, mas estas metodologias não definem detalhes sobre como classificar um incidente. As metodologias preconizam que as graduações de gravidade do incidente precisam ser definidas por cada entidade, com base nos elementos do incidente, que além dos itens elencados nas contribuições para as questões 1 e 4, também incluem: – Natureza dos dados ou da informação afetada – Categoria ou tipo de ataque (*malware*, invasão, negação de serviço, etc) – Envolvidos (pessoas, organizações, etc) – Escopo (número de dispositivos, criticidade do ativo, etc) – Impacto na informação (como afeta confidencialidade, integridade, disponibilidade) Referências: – FIRST Computer Security Incident Response Team (CSIRT) Services Framework https://www.first.org/standards/frameworks/csirts/ – Defining Incident Management Processes for CSIRTs: A Work in Progress, SEI/CMU

	https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=7153 – Computer Security Incident Handling Guide, NIST Special Publication 800-61 Revision 2 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf – Reference Incident Classification Taxonomy https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy – CSIRT Case Classification (Example for Enterprise CSIRT) https://www.first.org/resources/guides/csirt_case_classification.html
12. Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	Seria importante sugerir à organização a realização de um *post mortem* do incidente e do seu tratamento, com uma avaliação das ações que tiveram sucesso, de processos que precisam ser melhorados e de mudanças nas medidas técnicas e administrativas que precisariam ser implatadas de modo a reduzir as chances de que um incidente similar volte a ocorrer. Especialmente, em casos de incidentes de segurança que tenham sido causados por vulnerabilidades em sistemas utilizados pela organização, seria imprescindível recomendar aos agentes de tratamento que todos os sistemas da organização sejam avaliados de forma a identificar, de maneira proativa, se a mesma vulnerabilidade não está também presente em outros sistemas, além daquele inicialmente afetado.
SUGESTÃO DE NORMATIVO, SE HOUVER	
Art. Xxxx	
Art. Xxxx	

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2/

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: Centre for Information Policy Leadership (CIPL)
CPF/CNPJ: N/A

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

SOBRE O CIPL

O Centre for Information Policy Leadership (CIPL) recebe com satisfação a oportunidade de responder à primeira consulta pública organizada pela Autoridade Nacional de Proteção de Dados (ANPD) e gostaria de elogiar a ANPD por buscar cooperação e contribuições de múltiplas partes interessadas.

O CIPL é um think tank global que atua na área de privacidade e proteção de dados e segurança da informação com sede em Washington DC, Londres e Bruxelas, fundado em 2001 no escritório de advocacia Hunton Andrews Kurth LLP. A missão do CIPL é se engajar em liderança de ideias e promover boas práticas que garantam tanto a proteção efetiva da privacidade quanto o uso responsável dos dados pessoais na era moderna da informação. O trabalho do CIPL facilita o engajamento construtivo entre líderes empresariais, profissionais de privacidade e segurança, reguladores e tomadores de decisão em todo o mundo. Trabalhamos com líderes seniores e especialistas em privacidade de mais de 80 organizações globais líderes que nos fornecem casos concretos sobre suas práticas de privacidade de dados e tomada de decisões. Veja mais sobre o CIPL em https://www.informationpolicycentre.com/.

Nada nesta apresentação deve ser interpretado como representando a opinião individual de qualquer empresa membro do CIPL ou do escritório de advocacia Hunton Andrews Kurth.

CONTRIBUIÇÕES RECEBIDAS **IMPORTANTE:** Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	As atividades de tratamento de dados sempre apresentarão algum grau de risco para os indivíduos, que podem resultar de incidentes de segurança. As avaliações de risco incluem a análise da probabilidade e gravidade dos riscos aos direitos e liberdades dos indivíduos, incluindo quaisquer danos potenciais a indivíduos. Os riscos e danos associados a um incidente de segurança específico nem sempre estão correlacionados com o tamanho ou escopo do próprio incidente (por exemplo, o vazamento de dados financeiros de um pequeno número de pessoas pode ser mais danoso do que o vazamento de um número maior de dados que sejam comparativamente menos sensíveis). Os danos podem ser classificados em: • Danos materiais e imateriais – também conhecidos como danos tangíveis e intangíveis. A materialidade deve ser expressa em termos mensuráveis e objetivos, como valor monetário associado ao dano causado. Os danos materiais podem exigir priorização sobre os danos imateriais, dependendo do contexto; e • Danos sociais – a consideração de danos sociais (por exemplo, o público se abster de usar um aplicativo de rastreamento do COVID-19 no caso de haver um incidente de segurança amplamente divulgado na mídia relacionado a esse aplicativo) não é um requisito da LGPD e a ANPD não deve esperar que as organizações considerem os danos sociais em todas as suas avaliações de risco. No entanto, as organizações podem optar por considerá-los em circunstâncias específicas (no exemplo mencionado anteriormente, ao processar dados pessoais para combater a pandemia de COVID-19). A avaliação dos riscos e da probabilidade de danos no contexto de incidentes de segurança, a notificação de incidentes e a remediação devem ser consideradas como parte, ou um exemplo, das avaliações de risco mais amplas derivadas

	dos requisitos da LGPD. As organizações brasileiras estão obrigadas, nos termos do artigo 6, VII e VIII, a adotar medidas técnicas e administrativas para garantir a segurança de dados pessoais e evitar danos – essas seriam medidas de mitigação consideradas integrantes de uma avaliação de risco. O artigo 46 da LGPD vai além, obrigando controladores e operadores a adotarem medidas específicas de prevenção e gestão de incidentes. Essas medidas incluem avaliações de risco, bem como mitigação e controles implementados com base em avaliações de risco. As organizações não podem ser obrigadas a garantir a segurança absoluta das atividades de tratamento de dados; elas devem, porém, implementar medidas de segurança apropriadas ao risco de quaisquer danos potenciais previstos, conforme determinado pelas avaliações de risco. O gerenciamento de segurança é uma tarefa complexa que envolve uma ampla gama de fatores, dependendo do contexto e exigindo monitoramento contínuo de ameaças internas e externas. As ameaças externas, em particular, tornam-se mais sofisticadas a cada dia e podem ser imprevisíveis até mesmo para organizações mais maduras. Além disso, o risco de erro humano jamais pode ser totalmente excluído; só pode ser reduzido por meio de treinamento. **Portanto, a regulamentação da ANPD sobre incidentes de segurança deve ser flexível para dar conta dos contextos e variedades específicas de quaisquer incidentes de segurança e <u>não</u> deve ser prescritiva ou esperar que as organizações adotem metodologias específica, especialmente porque os riscos podem variar com o tempo e as metodologias podem ter que evoluir com as mudanças do cenário de risco. A ANPD pode, em vez disso, fornecer às organizações exemplos** de (i) quais poderiam ser os possíveis riscos e danos resultantes de diversos tipos de incidente de segurança, (ii) critérios não exaustivos que os controladores podem usar ao avaliar o nível de risco envolvido no incidente de segurança, e (iii) metodologias comumente adotadas no mercado para gerenciar incidentes de segurança (ver resposta à pergunta abaixo em “Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?”. Com isto, a ANPD poderá criar e facilitar o máximo de consistência possível, tendo em mente o contexto e a sensibilidade das avaliações de risco individuais e a consequente necessidade de flexibilidade. Em relação ao ponto (ii) no parágrafo acima e na segunda parte desta pergunta da ANPD, segue abaixo uma lista não exaustiva de critérios que as organizações geralmente levam em consideração ao avaliar o nível de risco de um incidente de segurança: • Probabilidade de ocorrência/materialização de danos a indivíduos como resultado do incidente – isto é importante para diferenciar entre incidentes em que os riscos para os titulares podem estar presentes mas a probabilidade de tais riscos ou danos realmente se materializarem é baixa, e incidentes em que os riscos estão presentes e a probabilidade de tais riscos ou danos se materializarem é significativa; • A gravidade dos possíveis danos a indivíduos (por exemplo, possíveis danos resultantes de incidentes em que os dados são revelados por acidente a uma parte confiável são provavelmente menos graves que os possíveis danos resultantes de incidentes em que os dados são revelados ao público em geral); • O tipo de incidente de segurança (por exemplo, quebra de sigilo por uma pessoa com acesso a dados, invasão de um sistema e, portanto, violação de sua integridade, indisponibilização de dados a seus usuários legítimos);

	• A natureza e sensibilidade dos dados pessoais (ou seja, quanto mais sensíveis os dados, maior será o risco de dano às pessoas afetadas, mas também devem ser considerados os dados pessoais que talvez já tenham sido tornados públicos pelo titular); • A facilidade com que os indivíduos podem ser identificados (por exemplo, se os dados pessoais foram criptografados e a chave de criptografia não foi divulgada, os riscos provavelmente serão muito menores); • Quaisquer características especiais do indivíduo afetado (por exemplo, dados referentes a crianças/outros indivíduos vulneráveis podem resultar em um risco maior do que dados de adultos); • Se o mesmo tipo de incidente já aconteceu no passado; e • As medidas tomadas pelo controlador para mitigar o impacto do evento. O CIPL acredita que vincular a determinação de notificar um incidente de segurança ao número de indivíduos potencialmente afetados pode ter consequências indesejadas. Por exemplo, um incidente com baixa probabilidade de causar danos a indivíduos pode ser interpretado como tendo uma classificação de risco mais alta caso o número de indivíduos potencialmente afetados seja alto, podendo resultar em notificação regulatória inadequada. O número de indivíduos afetados não é um bom indicador do dano real ou da probabilidade de dano que um indivíduo pode sofrer como resultado de um incidente de segurança. **A ANPD deve, portanto, exigir que as organizações realizem uma avaliação de risco do incidente de segurança, levando em consideração os critérios listados acima e quaisquer outros critérios relevantes para definir se devem notificar o incidente à ANPD e aos titulares dos dados. O artigo 48 da LGPD determina que as organizações devem notificar incidentes que possam resultar em riscos ou danos "relevantes". Ao interpretar este requisito, a ANPD deve considerar como "relevantes" apenas os riscos e danos que sejam (i) materiais e/ou (ii) classificados como de alto risco na avaliação de risco dos controladores** (ver resposta à pergunta abaixo). É necessário que a ANPD interprete a LGPD de maneira a garantir que o limite dos riscos e danos "relevantes" seja definido no nível correto, para que as organizações tenham que notificar apenas aqueles incidentes em que haja probabilidade de danos materiais a indivíduos e que sejam classificados como de alto risco. O CIPL incluiu abaixo alguns exemplos práticos de incidentes que não são materiais nem de alto risco e que, portanto, não devem ser considerados como notificáveis: • Um funcionário tem acesso acidental a um documento relacionado a um processo de recrutamento. Embora o documento possa conter dados pessoais que, se expostos mais amplamente, poderiam criar o risco de consequências adversas para o titular (por exemplo, em termos de vínculo com o empregador atual), a probabilidade de tal risco se materializar é baixa porque o funcionário está sujeito a requisitos de confidencialidade e notificou internamente o acesso acidental com o compromisso de excluir o documento.

<table>
<tr>
<td></td>
<td>

Alguns dados pessoais (como fotografias, informações sobre promoções profissionais, etc.) foram disponibilizados involuntariamente por meio do acesso a um link de URL temporário, mas compartilhável, em ferramenta de comunicação interna. Embora não se possa excluir por completo a possibilidade de que tal link seja usado por pessoa não autorizada a acessar tal conteúdo, a probabilidade deste risco ocorrer é minimizada pela validade temporária do link, bem como por medidas de moderação que limitam a natureza do conteúdo compartilhado na ferramenta. Além disso, os possíveis danos aos indivíduos não se materializaram.
Faturas incluindo detalhes de transações individualizadas (por exemplo, data, hora e local da compra) são compartilhadas equivocadamente num contexto business-to-business. Embora as informações contidas na fatura possam potencialmente levar à identificação de clientes, tal processo exigiria esforço de correspondência e acesso a conjuntos de dados externos. Além disso, o estabelecimento comercial está sujeito a obrigações de confidencialidade e compromete-se a não fazer nenhum uso posterior de tais informações.

</td>
</tr>
<tr>
<td>O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto etc.)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?</td>
<td>
As organizações adotam diversas metodologias para realizar as avaliações de risco. Organizações maiores normalmente categorizam os níveis de risco ao realizarem tais avaliações, incluindo avaliações relacionadas a incidentes de segurança. Essas categorias geralmente são baixo risco/médio risco/alto risco, e algumas organizações também usam categorias extras, como sem risco/risco muito alto/risco muito baixo. São várias as metodologias usadas por organizações para medir o nível de risco associado a essas categorias. Organizações maiores também podem fazer uso de ferramentas que lhes permitam atribuir uma pontuação a cada uma dessas categorias e calcular objetivamente a pontuação final do evento usando critérios especificados (como os critérios descritos em nossa resposta à pergunta acima). Algumas organizações também utilizam uma matriz de risco, como a ilustrada abaixo. Conforme mencionado em nossa resposta à pergunta acima, o CIPL recomenda que apenas os riscos classificados como de alto risco sejam considerados notificáveis.

Abaixo segue um exemplo de matriz de probabilidade e gravidade que algumas organizações usam para avaliar os riscos envolvidos em incidentes de segurança:
<table>
<tr><th>PROBABILIDADE DE OCORRÊNCIA DE DANO</th><th>ALTA PROBABILIDADE</th><th>MÉDIA PROBABILIDADE</th><th>BAIXA PROBABILIDADE</th></tr>
<tr><th>GRAVIDADE DO DANO</th><td></td><td></td><td></td></tr>
<tr><td rowspan="2">ALTA GRAVIDADE</td><td>Alta probabilidade</td><td>Média probabilidade</td><td>Baixa probabilidade</td></tr>
<tr><td>Alta gravidade</td><td>Alta gravidade</td><td>Alta gravidade</td></tr>
<tr><td rowspan="2">MÉDIA GRAVIDADE</td><td>Alta probabilidade</td><td>Média probabilidade</td><td>Baixa probabilidade</td></tr>
<tr><td>Média gravidade</td><td>Média gravidade</td><td>Média gravidade</td></tr>
</table>
</td>
</tr>
</table>

	<table><tr><td rowspan="2">BAIXA GRAVIDADE</td><td>Alta probabilidade</td><td>Média probabilidade</td><td>Baixa probabilidade</td></tr><tr><td>Baixa gravidade</td><td>Baixa gravidade</td><td>Baixa gravidade</td></tr></table> **A ANPD <u>não</u> deve exigir que as organizações usem metodologias ou ferramentas específicas para avaliar os riscos relacionados a incidentes de segurança. A ANPD deve deixar que as organizações decidam quais metodologias e ferramentas de avaliação de risco são mais adequadas a seus respectivos contextos, desde que as organizações possam demonstrar que avaliaram os riscos de forma adequada** (por exemplo, organizações menores podem optar por avaliar os riscos informalmente com base em perguntas e experiência interna, enquanto organizações maiores podem implementar ferramentas mais complexas e até mesmo vincular essas avaliações à função geral de gerenciamento de risco corporativo). Os controladores devem ter a capacidade (mas não a obrigação) de construir matrizes de risco que funcionem para a sua organização. Pode ser útil, especialmente para organizações menores, que a ANPD forneça uma lista de verificação (checklist) ou uma lista de perguntas que indiquem se um incidente seria notificável (por exemplo, o incidente resultou em danos concretos e materiais a indivíduos? Envolveu dados pessoais sensíveis ou dados pessoais referentes a indivíduos vulneráveis?). A ANPD também poderia elaborar uma ferramenta que as organizações possam usar para avaliar os riscos (por exemplo, uma planilha com um sistema de pontuação), deixando claro que tal ferramenta é opcional e que as organizações podem desenvolver suas próprias ferramentas/metodologias ou usar ferramentas/metodologias terceirizadas. A ANPD também pode fornecer exemplos de quais são os riscos e danos que as organizações podem considerar, bem como estudos de caso envolvendo incidentes notificáveis e não notificáveis.
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	Riscos são a probabilidade ou possibilidade de ocorrência de danos. Quando houver risco de dano, existirá a possibilidade um dano real se materializar. Conforme explicado na pergunta acima, os danos podem ser materiais ou imateriais/tangíveis ou intangíveis. Um incidente de segurança pode revelar a existência de (i) um risco significativo, caso em que o evento danoso permanece latente, ou (ii) danos a indivíduos, caso em que há evidências suficientes de que o evento já produziu seus resultados danosos. Embora os conceitos de "risco" e "dano" sejam independentes, eles estão intrinsecamente relacionados para fins de avaliações de risco.
O que deve ser considerado na avaliação dos riscos do incidente?	Ver resposta à primeira pergunta acima em "Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?"
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	O artigo 48, parágrafo 1º, da LGPD estabelece uma lista suficientemente abrangente de informações que os controladores devem fornecer à ANPD e aos titulares ao notificarem incidentes de segurança. Não está previsto que a ANPD deva exigir o fornecimento de informações além do que consta nesta lista. **O CIPL recomenda que a ANPD <u>não</u> exija o fornecimento de informações adicionais específicas, mas que permita que os controladores decidam no caso a caso se o fornecimento de informações adicionais seria útil,** principalmente ao notificar o incidente à ANPD e cooperar com uma possível investigação da ANPD. Essas informações adicionais podem estar relacionadas, por exemplo, às complexidades de um incidente de alcance global envolvendo várias jurisdições e/ou outros terceiros.

Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	O artigo 48, parágrafo 1º, da LGPD determina que os controladores devem comunicar, "em prazo razoável", à ANPD e aos titulares a ocorrência de incidentes de segurança que possam acarretar riscos ou danos relevantes para os titulares, e que a ANPD pode definir esse prazo. O regulamento da ANPD deve estabelecer limites claros de notificação, especialmente para incidentes menores, e evitar definir um limite baixo para a notificação. A notificação de incidentes é uma atividade que pode consumir muitos recursos, dependendo do porte e da complexidade da organização. Isso pode resultar em significativo ônus financeiro e administrativo para as organizações, agravado pelo aumento de ameaças e ataques externos. Se o limite para notificação for muito baixo, os recursos que poderiam ser gastos para ampliar os processos de conformidade internos e proteger os indivíduos podem ser mal direcionados. A ANPD pode ficar tentada a seguir o padrão de 72 horas/três dias estabelecido pelo artigo 33 do Regulamento Geral de Proteção de Dados da UE (RGPD). É importante, no entanto, que a ANPD reconheça que nem todas as disposições do RGPD são realistas. A ANPD não precisa seguir os exemplos da UE em todas as instâncias, e sim seguir apenas aqueles exemplos que são eficazes e fornecem o mais alto nível de proteção aos indivíduos, considerando também as particularidades do contexto brasileiro – ver relatório da Hunton Andrews Kurth: Seeking Solutions: Aligning Data Breach Notification Rules Across Borders (Em busca de soluções: alinhando as regras de notificação de violação de dados entre fronteiras), que destaca as principais diferenças e oportunidades de convergência nos regimes de notificação de violação de dados existentes ao redor do mundo. 72 horas ou três dias (ou mesmo dois dias, conforme recomendação provisória da ANPD em seu site) não é tempo suficiente para uma organização compreender totalmente o escopo e a extensão de um incidente de segurança e, portanto, definir se deve ou não ser notificado. Por causa disso, as organizações da UE muitas vezes notificam preventivamente a autoridade de proteção de dados da ocorrência de violação de dados, apenas para parar o cronômetro, o que resulta em supernotificação e custos associados de tempo e recursos (ver a contribuição do CIPL no Multistakeholder Expert Group to the Commission 2020 Evaluation of the GDPR (Grupo de Especialistas Multissetoriais para a Avaliação da Comissão 2020 do RGPD), página 36. Na verdade, prazos fixos para notificação de incidentes de segurança podem ter uma série de consequências indesejadas: • Precipitar notificações por medo de sanções, antes que uma avaliação completa dos eventos possa ser realizada, resultando em supernotificação de incidentes à ANPD, incluindo a notificação de incidentes que são incidentais e que no fim acarretam apenas baixo ou médio risco. A notificação apressada e prematura também não promove boas práticas de responsabilidade de prestação de contas (accountability) para as organizações que notificarão mecanicamente a ANPD para se protegerem em vez de realizar avaliações de boa-fé levando em consideração a probabilidade e gravidade do risco para os indivíduos; • Criar um falso senso de urgência que possa inadvertidamente resultar em uma situação em que a notificação deve ser complementada ou retificada conforme a avaliação evolui;

	• Transferir recursos da contenção e mitigação do incidente para a notificação deste (o que é particularmente relevante em organizações de pequeno e médio porte com recursos limitados); e • Criar o risco de responsabilização legal (liability) para a organização, mesmo quando ela estiver agindo com o maior padrão de diligência e cuidado. Permitir que as organizações tenham mais tempo para realmente entender o que aconteceu, avaliar o verdadeiro risco do incidente e lidar com ele de forma adequada fará com que a ANPD receba relatórios de melhor qualidade e provavelmente menos notificações, pois os controladores saberão dizer com mais certeza se a notificação do incidente é cabida ou não. Frequentemente, há um atraso prático entre o momento em que o funcionário toma conhecimento de uma violação e o momento em que o funcionário responsável pelas questões de proteção de dados é devidamente informado. Além disso, uma avaliação confiável de risco incluirá uma análise forense detalhada para determinar a probabilidade e a gravidade dos danos aos indivíduos e avaliar a necessidade de notificação. Nos cenários mais complexos, e em particular aqueles que envolvem ataques externos sofisticados, as investigações podem ocorrer durante várias semanas antes que os fatos (mesmo os fatos básicos, como a existência de qualquer possibilidade de acesso não autorizado aos dados) possam ser determinados. Veja, por exemplo, o 2020 BakerHostetler Data Security Incident Response Report (Relatório de Resposta a Incidentes de Segurança de Dados de 2020 da BakerHostetler), que mostra que o tempo desde a descoberta do incidente até a notificação leva em média 38 dias. O 2020 Verizon Data Breach Investigations Report (Relatório de investigações de violação de dados de 2020 da Verizon) indica que as violações de dados levam meses ou mais para serem descobertas em grandes organizações, enquanto, em organizações de pequeno porte, esse tempo é menor. O CIPL, portanto, apoia o padrão da LGPD de não estabelecer prazo fixo para a notificação de incidentes de segurança e, em vez disso, colocar sobre o controlador o ônus de garantir que a notificação seja emitida em tempo hábil e adequado à natureza e ao nível de risco envolvido no incidente. **O CIPL recomenda que a ANPD (i) mantenha o padrão existente da LGPD de prazo aberto, mas "razoável", e que (ii) forneça orientações e exemplos adicionais (ou seja, casos de uso) para ilustrar quando uma organização "toma conhecimento" de um incidente, o que seria considerado como notificações em tempo hábil e como as organizações podem demonstrar o cumprimento do cronograma e a adoção das devidas medidas para conter e remediar o incidente com eficácia.** Caso a ANPD decida não incorporar esta sugestão, o CIPL sugere que o prazo mínimo para notificação seja de 3 dias úteis a partir do momento em que a organização tome conhecimento do incidente, levando em consideração os dias úteis de funcionamento da empresa. A ANPD também deve fornecer orientações sobre o que significa "tomar conhecimento" do incidente e, portanto, em que ponto começa a contagem do tempo para a notificação à ANPD. Em vez de exigir notificação dentro de um prazo razoável a partir do conhecimento do incidente, o CIPL recomenda iniciar o cronômetro a partir do momento em que o incidente foi (ou razoavelmente deveria ter sido) confirmado, com orientação clara sobre qual nível de certeza razoável os controladores devem ter em relação à real ocorrência do incidente.

	Além disso, a ANPD deve considerar que as mesmas pessoas responsáveis por mitigar os incidentes de segurança são também responsáveis por fornecer as informações necessárias para a notificação. Assim, a ANPD não deve priorizar a notificação sobre a remediação, pois isso poderia ser pior para os titulares. Isto é ainda mais relevante para entidades menores com menos recursos.
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	Ver a pergunta anterior para considerações sobre o prazo razoável de notificação. As mesmas considerações se aplicam à comunicação a indivíduos. Em particular, o CIPL recomenda que a ANPD exija que os controladores notifiquem os titulares "dentro de um prazo razoável" apenas quando houver confirmação de que os titulares estejam sujeitos a riscos de danos materiais à privacidade classificados como de alto risco, e o controlador está em posição de aconselhar sobre as medidas de proteção que os titulares podem tomar (ou seja, para reduzir o risco de danos ou os danos em si, case já tiverem materializados). Isso evitaria a "fadiga da notificação", que poderia resultar de constantes notificações sobre incidentes irrelevantes. Notificações constantes ou frequentes iriam, de fato, prejudicar a proteção dos indivíduos, pois prejudicaria a capacidade, ou até mesmo disposição, deles de diferenciar continuamente entre situações que requerem ação de sua parte para se protegerem e situações em que o risco de dano é trivial e nenhuma ação é necessária. A comunicação em fases também pode ser razoável, desde que não sobrecarregue ou cause ansiedade desnecessária aos titulares. Nos casos em que os titulares precisam ser informados para que eles próprios possam tomar medidas de mitigação, faz sentido notificá-los o quanto antes, desde que isso seja viável. Em relação ao conteúdo da comunicação, as informações enumeradas no artigo 48, parágrafo 1º, da LGPD são suficientes. O conteúdo e o estilo desta notificação não devem, no entanto, ser iguais ao conteúdo da notificação à ANPD, visto que elas têm finalidades diferentes. Quaisquer requisitos obrigatórios em termos do conteúdo da notificação devem ser interpretados de forma flexível e não entendidos como requisito para citar a LGPD. A ANPD deve, portanto, fornecer as seguintes orientações aos controladores: • A comunicação deve ser escrita em linguagem clara e simples, evitando termos técnicos e jurídicos, deve ser concisa e amigável (por exemplo, a ANPD pode recomendar uma abordagem em camadas para que os titulares obtenham mais informações, se desejarem); • A comunicação deve ser independente de outras comunicações emitidas pelo controlador (por exemplo, um e-mail específico em vez de parte de um e-mail com ofertas de produtos e serviços); • A comunicação deve evitar linguagem alarmante e concentrar-se nas medidas que os titulares podem tomar para se protegerem ainda mais; e • As informações fornecidas sobre as medidas de mitigação que foram ou serão adotadas devem ser limitadas a um nível que seja útil para os indivíduos (observe que fornecer muitos detalhes pode abrir portas para que atores mal-intencionados contornem os planos de remediação). Seja qual for o caso, o requisito de comunicação não deve ser utilizado como meio para penalizar o controlador que sofreu o incidente de segurança (por exemplo, prejudicar sua reputação pública). O foco da comunicação deve ser o

	indivíduo afetado e o conteúdo deve se limitar a informações úteis que o ajudem a se proteger, conforme previsto no artigo 48, parágrafo 1º.

Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	Não há um padrão ou uma abordagem única que sirva para todos para notificação de incidentes de segurança com titulares de dados. Os controladores são os mais bem posicionados para saber como se comunicar de forma mais eficaz com seus usuários/titulares de dados e podem ter suas próprias maneiras de efetivar tais comunicações. A eficácia da comunicação deve ser o critério principal para notificação, mais que um formato pré-determinado. Preferencialmente, a notificação deve seguir o método com o qual o controlador regularmente interage com o titular dos dados.
	
	O CIPL recomenda que a ANPD (i) não exija um tipo específico de notificação, mas em vez disso forneça exemplos aos controladores sobre como eles podem notificar titulares de dados, e (ii) reconheça que os esforços envolvidos na notificação devem ser apropriados para o nível de risco e as circunstâncias específicas do caso. A ANPD deve informar os controladores que eles devem escolher o tipo de notificação mais apropriado para atingir a meta de informar indivíduos sobre o incidente e permitir que eles tomem quaisquer medidas necessárias (p. ex., mudar suas senhas) para manter seus dados pessoais protegidos. Alguns exemplos incluem:
	
	• Quando titulares de dados são identificados/individualizados e o controlador tem relação direta com eles:
	  ○ Carta enviada por correio;
	  ○ E-mail;
	  ○ SMS;
	  ○ Notificação por aplicativo ou plataforma (p. ex., pop-ups ou banners).
	
	• Excepcionalmente, a ANPD deve permitir notificações públicas quando (i) os titulares de dados não são identificados/individualizados, (ii) o controlador não tem uma relação direta com eles, (iii) os meios habituais de comunicação se tornaram inacessíveis em razão de um incidente (p. ex., o titular dos dados perdeu acesso ao e-mail), (iv) identificar e notificar os indivíduos demandaria um esforço desproporcional (p. ex., envolvendo custos proibitivos) e (v) a notificação deve ser urgente devido ao caráter de alto risco do incidente específico. Os exemplos incluem:
	  ○ Postagem em website; e
	  ○ Comunicações através de canais de mídia (tais como sites relevantes de notícias e TVs).
	
	• Adicionalmente, a ANPD deve considerar que pode haver instâncias em que os titulares de dados são identificados, mas não é possível notificar todos eles (p. ex. quando contas de e-mail foram fechadas ou o indivíduo trocou de endereço e não atualizou o novo endereço no sistema do controlador). Uma notificação pública pode não ser adequada nestes casos, pois apenas serviria para causar mais ansiedade ao invés de

	oferecer informações aos indivíduos impactados. Nestes casos, a ANPD não deve exigir que o controlador comunique o incidente publicamente.
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	Não se deve exigir que os controladores notifiquem a ANPD sobre incidentes de segurança que/onde: • For improvável que resultem em alto risco de prejuízo real aos indivíduos de acordo com a metodologia de risco aplicada pelo controlador (veja a resposta à primeira questão); • Envolverem apenas dados não pessoais (incluindo dados anônimos), na medida em que a LGPD cobre apenas a proteção de dados pessoais; • Envolverem dados pessoais que tenham se tornado ininteligíveis ou inidentificáveis antes do incidente e não há risco que dados sejam reidentificados (p. ex., criptografia onde a chave não tenha sido revelada, dados anônimos); • Envolverem a revelação involuntária de dados pessoais apenas para uma terceira parte confiável; e • Imediatamente após o incidente o controlador tenha tomado ações/medidas mitigatórias que asseguram que o nível de risco exigido para desencadear uma notificação aos titulares de dados não esteja mais presente.
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	Adicionalmente às isenções listadas acima, não se deve exigir que os controladores notifiquem os titulares de dados sobre incidentes de segurança que/onde: • Tenham sido eficazmente mitigados pelo controlador depois que se tornou ciente do evento e, consequentemente, não mais apresente riscos de prejuízos aos titulares de dados; • A materialização de riscos e prejuízos a indivíduos for improvável; • Envolvam apenas dados pessoais que já estejam em domínio público; • Emitir tais notificações impediria uma investigação criminal; e • Um dos controladores associados em uma relação de processamento de dados não tem as informações identificadoras dos titulares de dados (p. ex. operadores de redes de cartão de crédito que são controladores associados com emissores de cartões de crédito e teriam apenas os números de cartões sem os dados de identificação). Nestes casos, a ANPD não deve requerer que este controlador associado notifique titulares de dados. Isto deve ser responsabilidade do outro controlador associado que detém a informação identificadora dos titulares de dados.
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	Veja a resposta na primeira questão acima, em “Quando um incidente pode resultar em riscos ou danos relevantes para titulares de dados? Que critérios a ANPD deveria levar em conta para considerar relevantes os riscos ou danos?”

Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	As três metodologias mais usadas para se avaliar incidentes de segurança e gerenciar riscos relacionados a processamentos de dados são: • Agência Europeia para a Segurança das Redes e da Informação (ENISA), Recommendations for a methodology of the assessment of severity of personal data breaches (Recomendações para uma metodologia de avaliação da gravidade das violações de dados pessoais), 20 de dezembro de 2013; • Organização Internacional para Padronização (ISO), ISO 31000 – risk management (ISO 31000 – gestão de risco); e • Instituto Nacional de Padrões e Tecnologia (NIST), NIST Privacy Framework: a Tool for Improving Privacy Through Enterprise Risk Management (Estrutura de Privacidade do NIST: uma ferramenta para melhorar a privacidade através da gestão de risco corporativo), versão 1.0, 16 de janeiro de 2020. Organizações brasileiras deveriam, entretanto, ter a capacidade de construir um processo de gerenciamento de incidentes adequado à sua estrutura, natureza de negócios e quadros de trabalho de gerenciamento geral de riscos. As metodologias para avaliar a severidade de incidentes de segurança podem ser usadas como materiais especializados de referência, mas não devem ser tratadas como um componente compulsório de um processo de gerenciamento de incidentes que seja visto como conforme com a LGPD.
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	O Artigo 48, parágrafo 2, II da LGPD estipula que a ANPD pode requerer dos controladores a adoção de medidas que revertam ou mitiguem os efeitos de um incidente de segurança. O CIPL recomenda, contudo, que, em vez de requer dos controladores que tomem medidas específicas, a ANPD faça recomendações de tais medidas ou exija que os controladores definam estas medidas e as apresente à ANPD (p. ex. em um documento). Isto acontece porque os controladores estarão mais bem equipados para saber quais seriam as medidas mais eficazes e teriam um entendimento melhor dos aspectos técnicos envolvendo o incidente de segurança. De modo semelhante, no caso de a ANPD recomendar (ou definitivamente requerer) que medidas específicas sejam tomadas, os controladores devem ser capazes de ponderar sobre tais medidas e propor outras mais adequadas. **Os controladores devem, assim, desempenhar um papel prioritário na determinação de medidas mitigatórias e o papel da ANPD deve ser o de oferecer uma validação geral sobre a suficiência de tais medidas remediadoras, levando em consideração requerimentos de segurança razoáveis.** Isto é particularmente relevante para controladores que sejam grandes organizações. Medidas que a ANPD pode recomendar incluem: • Tomar decisões rápidas para conter o incidente, tais como desativar o sistema, isolando-o da rede, e desativar certas funções; • Medidas destinadas a resolver certos efeitos do incidente de segurança, tais como eliminar malware ou desativar contas comprometidas; • Minimização de Dados;

	• Medidas para restaurar completamente serviços a seus níveis normais e evitar, tanto quanto possível, que ocorram quaisquer novos incidentes relacionados à mesma causa; • Medidas para evitar que incidentes semelhantes aconteçam no futuro, tais como melhorar a segurança de sistemas e criar políticas e procedimentos internos, aumento de privacidade e treinamento em segurança da informação, auditorias, tratamento de vulnerabilidades internas, implementação de um programa de governança de dados abrangente e de responsabilidade por prestação de contas (accountability). • Reunião e custódia de provas para conter e reverter o impacto do incidente; e • Documentação do incidente e de medidas tomadas.
Considerações adicionais relacionadas ao gerenciamento e à notificação de incidentes de segurança	• **A ANPD deve levar em conta a accountability como um fator mitigatório ao executar a LGPD em seguida a uma notificação de incidente de segurança** — particularmente nos casos em que o controlador tenha tomado atitudes abrangentes e eficazes para conter e mitigar os riscos e tenha sido capaz de demonstrar estas enquanto colabora com a ANPD. Ter uma arquitetura de accountability dentro de uma organização é essencial para se avaliar riscos relevantes, implementar um nível de segurança apropriado aos riscos, elaborar políticas e procedimentos de gerenciamento de crise, treinamento de empregados, desempenhar a devida diligência (due dilligence) do operador, auditar práticas e responder a um incidente de segurança. Veja, por exemplo, o Accountability Framework do CIPL no documento oficial "The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society" ("O caso a favor da responsabilidade por prestação de contas/accountability: como ela permite a efetiva proteção de dados e a confiança na sociedade digital"). • **Um incidente de segurança não é um indicador de proteção insuficiente de dados pessoais** — é importante que a ANPD entenda que o fato de apenas ter havido um vazamento não significa necessariamente que as medidas de segurança organizatórias e técnicas adotadas foram insuficientes. Cada incidente e as medidas de segurança implementadas precisam ser considerados em suas próprias circunstâncias. A ANPD deveria reconhecer que perfeição não é o padrão em segurança de informação. Padrões de segurança industrial são pensados como marcos que assegurem que as entidades estão gerenciando riscos adequadamente. Eles não devem ser entendidos normativamente, porque isso pode de fato diminuir a segurança ao consumir recursos e perder o foco em riscos críticos. • **Operadores não devem ser os que determinam se deve haver uma notificação de violação de dados** — quando a ANPD publicou a consulta pública em discussão, também publicou (i) um guia preliminar sobre violações de dados em que estabelecia que "[a]pesar de a responsabilidade e obrigação de relatar à ANPD ser do controlador, se a informação é excepcionalmente apresentada pelo operador, essa será devidamente examinada pela ANPD"; e (ii) um modelo da notificação com um campo a ser marcado pela entidade notificadora para informar se trata-se de controlador ou operador. O artigo 48, parágrafo 1 da LGPD é claro em dispor que o controlador deve notificar a ANPD sobre violações de dados. Controladores, com apoio de seus

	operadores na medida do necessário, estarão mais bem equipados para avaliar extensivamente a severidade da violação de dados e examinar os impactos potenciais que isso possa causar aos titulares de dados. Os controladores devem ser aqueles que determinam se a violação deve ser notificada à ANPD e aos titulares de dados. A respeito disso, o CIPL recomenda fortemente que a ANPD não sugira ou deixe implícito que os operadores deveriam ter de notificar a autoridade ou os titulares de dados. A ANPD poderia, em vez disso, recomendar que operadores notifiquem controladores sobre incidentes de segurança envolvendo seus dados pessoais e cooperar para fornecer aos controladores a informação relevante, assim como gerenciar o incidente. A ANPD poderia ainda recomendar que isso seja incluído no contrato entre controlador e operador. • **A ANPD deveria apenas proativamente contactar organizações depois de elas terem razoável certeza de que, sob sua seu mecanismo de avaliação de risco, um incidente é notificável.** A ANPD pode receber reclamações e questões de indivíduos a respeito de incidentes de segurança sobre os quais eles ficaram a par através de meios que não sejam a notificação formal de acordo com a LGPD. Nem todos estes incidentes ultrapassarão o limiar de notificação que a ANPD vai estabelecer. A ANPD não deveria estar tentada a seguir todos estes casos, mas em vez disso apenas aqueles a respeito dos quais há razoável certeza de que atingem os limiares de notificação.
Diretrizes regulatórias e materiais de referência recomendados	Diretrizes regulatórias recomendadas: • Data Protection Commissioner (DPC), da Irlanda, Guidance Note: A Practical Guide to Personal Data Breach Notifications under the GDPR (Nota de orientação: um guia prático para notificações de violação de dados pessoais sob o RGPD), outubro de 2019; • UK Information Commissioner's Office (Gabinete do Comissário de Informação) do Reino Unido, guidance on personal data breaches; (orientação) e • O Comitê Europeu de Proteção de Dados está atualmente atualizando suas Guidelines 01/2021 on Examples regarding Data Breach Notification (Diretrizes 01/2021 sobre exemplos relacionados à notificação de violação de dados) e a ANPD deveria seguir seus desenvolvimentos. Artigos do CIPL: • CIPL Response to the EDPB's Guidelines on Examples Regarding Data Breach Notification (Resposta do CIPL às diretrizes do EDPB sobre exemplos relacionados à notificação de violação de dados), 2 de março de 2021 • CIPL Comments on WP29's Breach Notification Guidelines (Comentários do CIPL sobre as diretrizes do WP29 sobre notificação de violação), 1 de dezembro de 2017

	• Documento oficial: Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR (Risco, alto risco, avaliações de risco e avaliações sobre o impacto da proteção de dados sob a LGPD), 21 de dezembro de 2016.

SUGESTÕES DE DISPOSIÇÕES
O CIPL não tem sugestões.

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO: CONFEDERAÇÃO NACIONAL DAS INSTITUIÇÕES FINANCEIRAS - CNF

CNPJ: 01.634.120/0001-3

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS

IMPORTANTE: Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.

TÓPICO/QUESTÃO	CONTRIBUIÇÃO/INSTITUIÇÃO
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	Quando há desvio da finalidade inicialmente acordada para o tratamento, ausência de transparência e de boa-fé, que possa corromper a confidencialidade, integridade ou a disponibilidade da informação, podendo acarretar danos que venha a comprometer a segurança do sistema. Os critérios de riscos devem ser avaliados de acordo com a identificação do incidente, após a avaliação e a elaboração do relatório. Os critérios que devem ser avaliados são: (i) a natureza e categoria do incidente; (ii) a natureza, a categoria, e a volumetria (considerando o porte da empresa) dos dados afetados (se dados sensíveis); (iii) a natureza, categoria e quantidade de titulares de dados afetado (se titulares vulneráveis); (iv) o tipo do dano causado; (v) as consequências concretas e prováveis; (vi) probabilidade; e (vii) impacto. No caso do mercado financeiro, por exemplo, a classificação dos riscos não poderá estar desvinculada do possível impacto sistêmico e das consequências do incidente para a higidez e pleno funcionamento do mercado financeiro e de capitais.
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como	Sim, o risco deveria ser subdivido de acordo com a matriz de risco de cada uma das instituições, por exemplo:

<table>
<tr>
<td>distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?</td>
<td>
- Impacto ao agente de tratamento e ao titular;
- Ruptura operacional significativa;
- Impacto em sistemas de alta criticidade;
- Quantidade de informações pessoais;
- Exposição na mídia;
- Ameaça aos negócios da empresa;
- Valor financeiro relevante.

Nossa sugestão é a divisão em 5 categorias de severidade: Muito alta, Alta, Média, Baixa, muito baixa. Riscos médio, baixo e muito baixo não seriam considerados como relevantes. Outra opção seria a seguinte classificação:

1ª classificação: Relevante ou Não (identificando a qualidade e quantidade de dados que levariam a um risco ou dano relevante).

2ª classificação: Categoria do risco (baixo / médio / alto) pois pode haver riscos relevantes porém com pequeno volume qualitativo de dados o que representaria um baixo risco, enquanto dados sensíveis ou financeiros, mesmo em poucos volumes representaria um risco alto por exemplo.

(em ambas as classificações utilizar a matriz abaixo:)

<table>
<tr><th>Risco</th><th>Relevante</th><th>Não Relevante</th></tr>
<tr><td>Baixo</td><td>Qualitativo Baixo e Quantitativo Moderado ou Alto</td><td>Qualitativo Moderado Alto e Quantitativo Baixo</td></tr>
<tr><td>Medio</td><td>Qualitativo Suficiente para possibilitar engenharia social e Quantitativo Moderado ou Alto</td><td>Qualitativo Suficiente para possibilitar engenharia social e Quantitativo Baixo</td></tr>
</table>
</td>
</tr>
</table>

	<table><tr><td>Alto</td><td>Qualitativo Relevante (dados Sensíveis, Sigilo Bancário, Dados suficientes para possibilitar fraudes no sistema financeiro) e Quantitativo Moderado e Alto</td><td>Qualitativo Relevante (dados Sensíveis, Sigilo Bancário, Dados suficientes para possibilitar fraudes no sistema financeiro) e Quantitativo Baixo</td></tr></table> A instituição deverá informar, com base nas cores da Matriz: Apenas ANPD Apenas Titulares Ambos
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	O dano se classificaria como qualidade de dados suficientes que possam ser/ou sejam utilizados contra o titular em fraudes (i.e. mesmo que a fraude não se materialize), uma vez que o titular de referido dados será compelido a tomar inúmeras medidas extras para proteger-se de eventuais impactos ou remediar o impacto. Há um risco quando os dados são fragmentados e não suficientes para que sejam utilizados sem que sejam adicionados outros dados (ou seja, dados que poderiam iniciar uma engenharia social para obter mais dados são um risco, mas não um dano). Nem sempre a violação implica em um risco ao titular. A afetação de integridade ou autenticidade pode afetar, por exemplo, outros direitos do titular, mas não necessariamente envolve a publicização de dados. A partir disso, verificando qual o atributo foi violado, é possível medir o risco (usando, também, o “Recommendations for a methodology of the assessment of severity of personal data breaches” do European Union Agency for Cibersecurity (ENISA). Disponível: https://www.enisa.europa.eu/publications/dbn-severity.). É possível ainda indicar o tipo de dano: - Danos ou riscos patrimoniais (realização de fraudes, por exemplo);

	- Danos ou riscos extrapatrimoniais (violação da privacidade, intimidade, honra, medo e insegurança do titular de sofrer incidentes futuros, etc).
O que deve ser considerado na avaliação dos riscos do incidente?	Sugerimos que sejam considerados os seguintes critérios: - Natureza da violação (perda de confidencialidade, desvio de finalidade, perda de integridade, indisponibilidade, por exemplo); - Natureza dos dados (pessoal, pessoal sensível, dados pessoais protegidos por outra legislação); - Facilidade na identificação do titular (se diretamente, a partir do incidente ou se é necessário a realização de algum processo para a identificação); - Natureza da base de dados, se pública ou privada; - Impactos ao titular; - Tempo histórico da base; - Volume de dados pessoais e/ou sensíveis envolvidos; - Se o destinatário que recebeu a informação é entidade e/ou pessoa natural que possui relação comercial, contratual e/ou de outra natureza vinculativa, com o controlador. - Tempo de exposição do dado ou duração do incidente; - Se o incidente possibilita ações fora do Brasil (cross border); - Potencial impacto à segurança pública e incolumidade física dos titulares; - Potencial impacto no funcionamento de atividades públicas essenciais; - Potencial de risco para funcionamento dos mercados em que o agente de tratamento está inserido, riscos sistêmicos e ou pleno funcionamento de atividade econômica relevante; - Potencial risco de continuidade da operação do agente de tratamento.
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	Além daquelas já listadas no §1º do art. 48 da LGPD, os controladores devem enviar à ANPD, as informações que estão disponíveis no formulário de comunicação de incidentes de segurança com dados pessoais da ANPD, conforme segue: Identificação e dados de contato de: - Entidade ou pessoa responsável pelo tratamento. - Encarregado de dados ou outra pessoa de contato.

	- Indicação se a notificação é completa ou parcial. Em caso de comunicação parcial, indicar que se trata de uma comunicação preliminar ou de uma comunicação complementar. Informações gerais sobre o incidente de segurança com dados pessoais: - Data e hora da apuração do incidente; - Data e hora do incidente e sua duração; - Circunstâncias em que ocorreu a violação de segurança de dados pessoais, por exemplo, perda, roubo, cópia, vazamento, dentre outros; - Se serão fornecidas mais informações posteriormente, bem como quais meios estão sendo utilizados para obtê-las; - Atributo de segurança que foi violado (confidencialidade, integridade e disponibilidade).
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	Entendemos que é preciso diferenciar incidentes de segurança de incidentes de segurança que envolvam dados pessoais, sendo que apenas o segundo deveria ser objeto de análise da ANPD. Com relação a incidentes de segurança que possam envolver dados pessoais, entendemos ser essencial distinguir as principais fases dos incidentes para que seja possível determinar em quais momentos a ANPD deverá ser comunicada e quais informações deverão constar das respectivas comunicações. 1) Fase 1 – Notícia/suspeita de incidente; 2) Fase 2 – Investigação do incidente; 3) Fase 3 – Conclusão da investigação do incidente; 4) Fase 4 – Contingenciamento, Erradicação e Recuperação de informações/processos; 5) Fase 5 – Lições aprendidas e implementação de novos processos. Note-se que as fases mencionadas acima foram baseadas tanto na experiencia já vivida com incidentes de segurança cibernética, quanto em publicações de organizações e órgãos técnicos tais como o National Institute of Standards and Technology (NIST) https://www.nist.gov/cyberframework

	Em razão da análise de um incidente contemplar diversas fases, a sua comunicação à ANPD também deveria refletir, ao menos em parte, as 5 fases supramencionadas. Assim sugerimos que sejam estabelecidos os seguintes prazos: 1) Após a notícia do incidente, o processo de investigação deverá ocorrer em até 30 dias corridos, contados do conhecimento do possível incidente; 2) Havendo a confirmação da ocorrência do incidente de segurança envolvendo dados pessoais, decorrente de evento interno ou externo, a comunicação deverá ser realizada no prazo de 5 dias úteis, com as seguintes informações mínimas: (i) identificação do incidente; (ii) apresentação de plano de ação e resposta ao incidente; (iii) medidas mitigatórias aos eventuais impactos ao titular; Caso a ANPD tome conhecimento de um incidente, eventuais trocas de informações/esclarecimentos entre a ANPD e o agente de tratamento acerca de eventual investigação deverão ser mantidas em sigilo para que não haja prejuízo das medidas de adotadas. Por fim, nos parece bastante importante reforçar que para agentes de tratamento inseridos em mercados regulados tais como o mercado financeiro, de capitais e securitário, entendemos que a adoção de medidas de publicização de incidentes por parte da ANPD deve ser coordenada com os respectivos reguladores. Isto porque o impacto de tais medidas, muitas vezes refletirão no próprio funcionamento de tais mercados e sistemas.
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	Considerando-se as observações acima, finda a investigação, e uma vez notificada a ANPD, entendemos que, a depender do volume de titulares envolvidos no incidente e a forma mais adequada de comunicação, e, levando-se em conta o mercado de atuação do agente de tratamento, o contexto do tratamento e as peculiaridades do incidente, a nossa sugestão é de que o controlador tenha até 30 dias corridos, contados da recepção da notificação pela ANPD, para comunicar os titulares acerca do incidente. Novamente, reiteramos que a depender do incidente, volume de titulares e das

	características do agente de tratamento, sugerimos que fique facultado a ANPD majorar o prazo de 30 dias, se assim requerido. As informações que devem ser acrescidas são: local, data e hora do evento (aproximados).
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	Entendemos que a forma mais adequada irá variar a depender (i) do volume de dados objeto do incidente, bem como (ii) do contexto do tratamento e dos eventuais impactos decorrentes da publicização do incidente. Idealmente, a realização da comunicação do incidente aos titulares deverá ser realizada individualmente, através de canal de contato que permita a transmissão adequada da comunicação, por qualquer meio (eletrônico, voz, ou mensagem instantânea), desde que assegurada a transparência.
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	Risco ou dano classificado como baixo - uso indevido e/ou vazamento de informações que não ofereçam vantagem competitiva aos agentes de tratamento, sem intencionalidade e/ou sem danos à imagem dos titulares, bem como na hipótese de vazamento interno de dados dentro da própria empresa, vide matriz acima.
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	Entendemos que a LGPD determina que somente serão objeto de notificação à ANPD os incidentes que envolverem dados pessoais e capazes de ensejar riscos e danos relevantes aos titulares. Assim, uma vez investigado o incidente, e, aplicada a metodologia acima exposta, os incidentes passíveis de serem informados aos titulares serão aqueles que apresentarem riscos ou danos relevantes (risco alto ou médio). As exceções de informar obrigatoriamente aos titulares são: 1 - os riscos classificados como baixo e médio; 2 – à depender da (i) a natureza e categoria do incidente; (ii) a natureza, a categoria, e a volumetria (considerando o porte da empresa) dos dados afetados (se dados sensíveis); (iii) a natureza, categoria e quantidade de titulares de dados afetado (se titulares vulneráveis); (iv) o tipo do

	dano causado; (v) as consequências concretas e prováveis; 3 - tipo do dano causado; 4 - as consequências concretas e prováveis; e 5- se o incidente consegue ser revertido rapidamente.
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	Os critérios para avaliação da gravidade do incidente de Segurança da Informação que inclua Dado Pessoal, devem considerar a possível ocorrência de riscos e danos relevantes aos titulares. Para isso deve se considerar os itens abaixo: - Envolvimento de dados sensíveis; - Indivíduos em situação de vulnerabilidade, incluindo crianças e adolescentes; - Potencial de ocasionar danos materiais ou morais, tais como discriminação, violação do direito à imagem e à reputação, fraudes financeiras e roubo de identidade; - Volume significativo de dados envolvidos; - Quantitativo significativo de indivíduos afetados; - Ausência de boa-fé e más intenções de quem teve acesso; - Facilidade de identificação dos titulares; - Extensão do vazamento; - Tempo de exposição do dado ou duração do incidente; - Se o incidente possibilita ações fora do Brasil (cross border); - Impactos à segurança pública e incolumidade física dos titulares; - Impactos no funcionamento de atividades públicas essenciais; - Risco para funcionamento dos mercados em que o agente de tratamento está inserido, riscos sistêmicos e ou pleno funcionamento de atividade econômica relevante.
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	Normas utilizadas como prática de mercado: ISO 31000 — Risk management; https://us-cert.cisa.gov/CISA-National-Cyber-Incident-Scoring-System; https://www.csusm.edu/iits/services/security/program/incident.html; https://www.nist.gov/. Acrescemos os controles, em especial a Família de Normas ISO's, os controles básicos, são apresentados no item 16, do Anexo A da ISO 27001:2013 e melhores detalhados item 16, da ISO 27002:2013, que preconiza ter como objetivo assegurar ter um enfoque consistente e efetivo para

	gerenciar os incidentes de segurança da informação, incluindo a comunicação sobre fragilidades e eventos de segurança da informação.
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	Seguir as medidas já previstas na lei considerando, (art. 52) observada a proporcionalidade e análise de risco e dano efetivamente materializado. Recomendamos estabelecer processo de lições aprendidas, incluindo as medidas tomadas para evitar que o incidente ocorra novamente, indicação da existência e revisão de política de segurança cibernética com determinada periodicidade, reuniões periódicas sobre o tema, criação de comitê de crise multidisciplinar que envolva diversas áreas da companhia do controlador, contratação de equipes de auditoria externa para revisão dos processos relacionados ao incidente, simulações de incidentes para treinamento de funcionários, workshops educativos e de conscientização sobre o tema para os colaboradores, plano de reestabelecimento do ambiente e sua integridade, plano de ação de acompanhamento aos titulares impactados, e fornecimento de diretrizes para identificação, cadeia de custódia, coleta, aquisição e preservação de evidencias digitais do incidente.
SUGESTÃO DE NORMATIVO, SE HOUVER	
Art. Xxxx	

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: Confederação Nacional do Transporte
CPF/CNPJ: 00.721.183/0001-34

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS **IMPORTANTE:** Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	A Confederação Nacional do Transporte, entidade representativa de grau superior das transportadoras brasileiras, em todos os modais (terrestre, aquaviário, ferroviário e aéreo), entende que a comunicação do incidente de segurança é essencial para assegurar ao titular de dados pessoais os direitos previstos na LGPD, além de ser uma etapa importante para que o agente de tratamento seja responsabilizado na medida de seus atos. Um incidente pode acarretar risco ou dano relevante ao titular quando apresentar negação ou impacto às liberdades civis e aos direitos fundamentais das pessoas naturais. Sugere-se que a ANPD considere, de maneira geral, para avaliação de risco ou dano relevante (i) critério quantitativo – a identificação da quantidade de pessoas afetadas; (ii) critério qualitativo – o tipo de dados pessoais que podem ser expostos (risco) ou foram expostos (dano). Especificamente, sugere-se que riscos inerentes as atividades de tratamento de dados não sejam consideradas relevantes, já que sobre eles pode ser exercido um juízo de normalidade e previsibilidade. Um risco ou dano que impacta uma dezena de pessoas deve possuir uma relevância menor do que um risco ou dano que impacta milhares de cidadãos. A respeito dos tipos de dados, o risco ou a exposição de dados comuns é menos grave do que um risco ou vazamento de dados pessoais sensíveis ou dados pessoais financeiros aptos a permitirem movimentações (por exemplo: número de cartão de crédito, senha do banco).

<table>
<tr>
<td>O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?</td>
<td>
Acredita-se que risco ou dano relevante deveria sim ser subdividido em categorias, conforme as consequências que poderiam ter para a esfera de direitos (de liberdade, privacidade e livre desenvolvimento da personalidade) do titular de dados pessoais. Salienta-se, inclusive, que risco e dano relevante deveriam ser subdivididos em categorias próprias, ou seja, ter-se risco baixo, risco médio, risco alto, os quais seriam distintos das categorias dano baixo, dano médio e dano alto.

Para distinguir os níveis de risco ou de dano relevante sugere-se que seja realizada análise por meio de uma matriz que permita o cruzamento de informações quantitativas (número de pessoa afetadas ou potencialmente afetadas) e de informações qualitativas (natureza dos dados) para se identificar o nível de risco ou dano relevante.

Ao lado das informações acima mencionadas, e considerando-se sobretudo o risco, as medidas técnicas de segurança e prevenção utilizadas no tratamento de dados são importantes elementos a serem considerados na distinção dos níveis, pois a depender da medida utilizada dentre as opções disponíveis e conhecidas (para evitar a exposição, por exemplo, criptografia dos dados, para evitar a perda permanente dos dados, backup e replicação), o risco de ocorrência de incidente de segurança pode ser maior ou menor.

A partir dos princípios sugeridos pela ABNT NBR ISO 31000 e pela LGPD, sugere-se a adoção da seguinte tabela para a análise de risco:

<table>
<tr><th rowspan="2">Fatores</th><th colspan="4">Risco</th></tr>
<tr><th colspan="2">Baixo</th><th>Médio</th><th>Alto</th></tr>
<tr><td>Quantidade de pessoas impactadas</td><td>1-10</td><td>11-100</td><td>101-1000</td><td>>1000</td></tr>
<tr><td>Dados pessoais</td><td></td><td></td><td>Financeiros (cartão de crédito, senha do banco)</td><td>Sensíveis (conforme Art 5º, inciso V da LGPD)</td></tr>
</table>

O risco deve possuir a maior categorização entre os fatores, desta maneira, um risco que impacte 50 pessoas, porém que envolva dados sensíveis deve ser considerado alto.
</td>
</tr>
</table>

	Por exemplo, um risco baixo impacta até 100 pessoas e não envolve dados pessoais financeiros ou dados pessoais sensíveis. Sugere-se que **riscos** baixos e médios, assim como **danos** baixos não sejam considerados relevantes para fins de comunicação de incidente de segurança, uma vez que a regulação estabelecida pela LGPD dá ênfase nas boas práticas dos agentes de tratamentos, que podem realizar internamente a gestão de riscos baixos e médios e de danos baixos.
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	Utilizando o conceito de que o **risco é o efeito da incerteza nos objetivos**, o conceito trata da possibilidade de algo ocorrer, positivo ou negativo, e que impacte o objetivo. Sendo o objetivo da lei a proteção dos direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (Artigo 1º), tudo que pode ocasionar um impacto a este objetivo, de forma negativa, deve ser considerado em uma análise de risco. Como exemplo: devido à ausência de atualização de um sistema, há um risco de que um malware infecte um banco de dados e todos os dados pessoais dos clientes sejam excluídos. Dano é o fato já ocorrido e que causou impacto negativo. Como exemplo: um malware infectou um banco de dados e excluiu todo o banco de dados de um cadastro de 100 pessoas, com os seguintes dados pessoais de cada pessoa: nome, endereço e CPF. O risco deve ser conhecido pelo controlador e é recomendado que seja realizado um Relatório de Impacto a Proteção de Dados Pessoais.
O que deve ser considerado na avaliação dos riscos do incidente?	Sugere-se que na avaliação de riscos sejam consideradas as salvaguardas que permitem que um dano seja minimizado, observando-se o contexto tecnológico e sociocultural. Considerando que o incidente de segurança é o tratamento inadequado ou ilícito de dados pessoais, sugere-se que a avaliação dos riscos do incidente aprecie o nível de compromisso principalmente com a transparência, o livre acesso, a segurança e a prevenção. As medidas de salvaguardas técnicas são, por exemplo:

	• Criptografia - arte de proteção da informação através de sua transformação em um texto cifrado (criptografado), com o uso de uma chave de cifragem e de procedimentos computacionais previamente estabelecidos, a fim de que somente o(s) possuidor(es) da chave de decifragem possa(m) reverter o texto criptografado de volta ao original (texto pleno). A chave de decifragem pode ser igual (criptografia simétrica) ou diferente (criptografia assimétrica) da chave de cifragem; • Backup - conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação. Tem a fidelidade ao original assegurada. Esse termo também é utilizado para identificar a mídia em que a cópia é realizada; Conforme glossário de segurança da informação Vide: *https://www.in.gov.br/web/dou/-/portaria-n-93-de-26-de-setembro-de-2019-219115663* Caso seja possível evidenciar que o conteúdo estava criptografado, é possível admitir, de acordo com a tecnologia utilizada e a evolução das técnicas para descriptografar, que ocorreu um incidente, porém não houve dano ao titular. Outro item é o controlador possuir backup dos dados pessoais dos titulares, neste caso o incidente trará impacto ao titular, mas não haverá perda definitiva dos dados pessoais.
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	A sugestão é que sejam adicionados os seguintes itens: • Comunicar o nome e os contatos do encarregado para que a ANPD possa obter mais informações, caso seja necessário e conforme consta no formulário de comunicação de incidente já disponibilizado pela ANPD; • Descrever as consequências prováveis da violação de dados pessoais. • Os dados constantes do incidente são compartilhados com terceiros e, em caso positivo, se houve a comunicação com este terceiro; • Que comprove a realização da comunicação prévia ao titular do dado sobre o incidente, desde que seja um incidente ou tratamento ilícito ou inadequado de dados pessoais que possam acarretar risco ou dano relevante às suas liberdades civis e aos seus direitos fundamentais.
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	A sugestão é que seja adotado o padrão da política de privacidade da União Europeia, a GDPR, com prazo de 72 horas, após a organização ter conhecimento. Vide: *https://gdpr-info.eu/art-33-gdpr/*

	Oportuno mencionar que alguns segmentos do setor de transporte dependem de tratamentos de dados menos automatizados, os quais contam com mecanismos de inteligência artificial ainda incipientes, motivo pelo qual o aumento do prazo é de suma importância. Ademais, pugnamos para que o incidente seja informado à ANPD por meios rápidos e menos burocráticos que permitam a rápida ciência, como um e-mail designado somente para esta função.
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	Sugere-se que o controlador comunique, igualmente, com prazo de 72 horas, aos titulares o tratamento ilícito ou inadequado de dados pessoais que possam acarretar risco ou dano relevante às suas liberdades civis e aos seus direitos fundamentais. Sugere-se que conste no comunicado ao titular, além das indicadas no §1º do art. 48: • Os dados pessoais que foram impactados; • A possível data do incidente; • As possíveis situações que podem ocorrer devido a divulgação dos dados violados. • Os dados constantes do incidente são compartilhados com terceiros e, em caso positivo, se houve a comunicação com este terceiro;
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	Sugere-se que seja avaliada a quantidade de pessoas impactadas e a recorrência. Caso ocorra um incidente de segurança que envolva dados pessoais de até 1000 pessoas, sem recorrência, a empresa poderá adotar os seguintes meios: e-mail e telefone. Caso ocorra uma recorrência em incidentes de segurança e com mais de 1000 pessoas envolvidas, deverá ser solicitado que a empresa realize comunicação pública (nota à imprensa ou publicação no site da empresa) dando publicidade ao incidente. Isso porque, caso o ocorrido se dê em larga escala, a notificação dos titulares dentro do prazo pode se tornar impossível, fato que poderia importar em futuros agravamentos da situação. O agente de tratamento também poderá adotar a comunicação pública quando a comunicação individual representar um grande esforço, da mesma forma que a GDPR, conforme artigo 34 (3c). Vide: *https://gdpr-info.eu/art-34-gdpr/*

	De toda fora, sugere-se que a ANPD adote meios rápidos e menos burocráticos, que permitam a ciência dos titulares no prazo mais adequado para que seja evitado o risco ou mitigado o dano.
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	Sugere-se que não haja obrigatoriedade de o controlador comunicar incidente de segurança à ANPD se os riscos aos direitos e liberdades dos indivíduos são improváveis e se o dano for baixo. Conforme mencionado acima, as categorias risco baixo, risco médio e dano baixo ficariam desobrigadas de comunicação à ANPD. Como exemplos: • Os dados pessoais estejam criptografados, com tecnologia adequada que permita uma razoável dificuldade para descriptografia. • Dados anonimizados sem a possibilidades de reversão, desta forma, sendo considerados pseudoanonimizados. • Dados pseudoanonimizados vazados não tenham sido expostos em conjunto com a informação adicional que permite a reversão.
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	Sugere-se que não haja obrigatoriedade de o controlador comunicar incidente de segurança ao titular se os riscos aos direitos e liberdades dos indivíduos são improváveis e se o dano for baixo. Conforme mencionado acima, as categorias risco baixo, risco médio e dano baixo também ficariam desobrigadas de comunicação ao titular. Como exemplos: • Os dados pessoais estejam criptografados, com tecnologia adequada que permita uma razoável dificuldade para descriptografia. • Dados anonimizados sem a possibilidades de reversão, desta forma, sendo considerados pseudoanonimizados. • Dados pseudoanonimizados vazados não tenham sido expostos em conjunto com a informação adicional que permite a reversão.

<table>
<tr><td></td><td>Caso tenha ocorrido um incidente em que as salvaguardas foram suficientes para não expor os dados pessoais do titular, como o uso de criptografia, o titular não precisa ser informado, embora a ANPD possa ser informada a depender do nível do risco.</td></tr>
<tr><td>Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)</td><td>A sugestão é que a ANPD adote os seguintes critérios:
Quantidade de pessoas impactadas;
Natureza dos dados pessoais;
<table>
<tr><th rowspan="2">Fatores</th><th colspan="3">Dano</th></tr>
<tr><th colspan="2">Baixo</th><th>Médio</th><th>Alto</th></tr>
<tr><td>Quantidade de pessoas impactadas</td><td>1-10</td><td>11-100</td><td>101-1000</td><td>>1000</td></tr>
<tr><td>Dados pessoais</td><td></td><td></td><td>Financeiros (cartão de crédito, senha do banco)</td><td>Sensíveis (conforme Art 5º, inciso V da LGPD)</td></tr>
</table>
O dano deve possuir a maior categorização entre os fatores, desta maneira, um incidente que impacte 50 pessoas, porém que envolva dados sensíveis deve ser considerado alto.

Um dano baixo seria um incidente que impacte até 100 pessoas e que não envolva dados pessoais financeiros ou dados pessoais sensíveis.

Adicionalmente, também podem ser considerados outros fatores que, caso existam, poderiam configurar um aumento da gravidade, como:
Análise se incidente representa risco ou dano para os titulares;
Quantidade de pessoas impactadas frente ao universo de dados pessoais tratados pelo controlador;
Caso seja dano, extensão do dano causado aos titulares;
Possibilidade de rastreabilidade sobre o incidente;</td></tr>
</table>

	• Se o incidente implicou transferência internacional de dados; • Caso tenha havido transferência internacional de dados, se o país para onde os dados foram transferidos tem tratamento semelhante ao dado pela LGPD (nível de segurança similar).
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	A sugestão é que sejam adotados os conceitos da norma brasileira e internacional, a ABNT NBR ISO 20000 - Sistema de Gestão de Serviço A gestão de incidentes da norma possui o seguinte fluxo: 1. Identificação – os incidentes devem ser identificados pelo próprio titular ou ferramentas de monitoramento. 2. Registro – o incidente deve ser registrado para que faça parte de uma base de conhecimento ou processo de auditoria. 3. Categorização – o incidente deve ser categorizado de acordo com o dano. 4. Priorização – os incidentes que causam os maiores danos devem ser priorizados. 5. Diagnóstico – análise do incidente com o objetivo de identificar a causa raiz. 6. Resolução – aplicação da resolução, questionamento e punição aos envolvidos. 7. Fechamento – documentar o incidente e registrar as lições aprendidas na base de conhecimento.
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	Inicialmente se deve verificar em termos objetivos a qualidade do dado que foi objeto do incidente. Ou seja, além dos dados sensíveis que possuem consequências discriminatórias, quais outros dados poderão ser utilizados em prejuízo do titular do dado, como dados relativos a crédito, a sigilo de correspondência e ao seio familiar, por exemplo. A partir daí, delimitar como seria a gradação do possível dano e a penalidade correspondente cabível, Assim, penalidades mais drásticas como perdimento/impedimento de banco de dados ao controlador, somente seriam aplicadas em casos de comprovada negligência e dados potencialmente nocivos vazados, ao passo que multas e advertências seriam aplicados apenas àqueles incidentes em que houve uma quantidade menor de dados vazados e uma qualidade limitada (somente o primeiro nome, número de identidade, entre outros) e com menor potencial de risco ao titular do dado.

	Ao serem analisados os limites que permitam distinguir (a) incidentes de segurança que possam trazer risco ou dano relevante e (b) que possam demandar providências adicionais daquela cuja ameaça, se houver, pode ser desconsiderada, deve ser considerado o volume de dados tratados (quantidade de Terabites), em consonância com o porte das empresas (pequena, média, grande). Um incidente em pequena empresa que trafega grandes volumes de dados é diferente e mais grave do que aquele que ocorre em uma empresa de grande porte que trata pequeno volume de dados. Recomendamos ainda que a Autoridade estabeleça a responsabilização das empresas que sofreram incidentes perante os prejudicados, a contar do momento da utilização indevida dos dados, considerando as medidas mitigatórias empenhadas. Isso porque hoje convivemos, por exemplo, com um incidente que inclui dados pessoais de mais de 230 milhões de brasileiros, sem que se saiba, até o momento, qual foi a empresa que sofreu o incidente. Trata-se de dados perenes (CPF, nome, telefone, etc., inclusive de pessoas já mortas) que poderão ser utilizados indevidamente por muitos anos. Considerando o vazamento de número de CPF e de documentos de identidade, é desejável que a Receita Federal e órgão de controle de identidades pessoais possibilitem a emissão de nova inscrição (com a devida vinculação ao número original), a fim de inibir novas fraudes contra a vítima dos vazamentos (a ser custeada pelo responsável pelo vazamento, acaso demonstrada a fragilidade das medidas de segurança). Solicitar as providências tomadas pelo agente de tratamento em relação ao incidente de segurança da informação e questionar se a falha que causou o incidente foi sanada ou profissional envolvido já teve seu acesso bloqueado.
SUGESTÃO DE NORMATIVO, SE HOUVER	
Art. Xxxx	
Art. Xxxx	

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: Comissão de Mediação e Métodos Consensuais da OAB/RJ

CPF/CNPJ: 33.648.981/0057-37

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS **IMPORTANTE:** Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	
O que deve ser considerado na avaliação dos riscos do incidente?	
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	

Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	

Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	Recomendação para que as reclamações entre os titulares de dados e as empresas / instituições sejam solucionadas através de soluções negociadas de conflitos como negociação, mediação e conciliação, inclusive no formato eletrônico. Justificativa: Os incidentes de segurança tendem a gerar um grande número de processos judiciais. O artigo 55-J, inciso XXIV da LGPD prevê dentre as atribuições da Autoridade Nacional de Proteção de Dados - ANPD a implementação de mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais. Além disso, o artigo 52, parágrafo 7º estabelece que os vazamentos individuais ou os acessos não autorizados de dados pessoais poderão ser objeto de conciliação direta entre controlador e titular e, caso não haja acordo, o controlador estará sujeito à aplicação de determinadas penalidades. A ANPD pode contribuir significativamente com o estímulo ao uso de soluções negociadas em formato eletrônico (também conhecidas como *online dispute resolution*) para solução dos conflitos decorrentes da LGPD. Diante de todas as novidades que permeiam a proteção de dados, os desfechos das reclamações submetidas à ANPD precisarão ser rápidos de modo a evitar a formação de um passivo de demandas administrativas e judiciais e a perpetuação de danos ao titular dos dados. Uma forma de garantir a praticidade e a otimização necessárias à gestão desses casos é através da criação de sistemas de gestão dessas demandas pelos próprios controladores dos dados. É de suma importância que os controladores disponham de colaboradores para monitorarem as reclamações submetidas por meio do sistema e que estejam treinados para o pronto atendimento do titular. Este canal de gestão de disputas não pode ser uma barreira ineficiente à solução do caso.
SUGESTÃO DE NORMATIVO, SE HOUVER	
Art. Xxxx .... Em casos de incidentes de segurança com grande número de titulares de dados afetados e grande potencial de judicialização, o Controlador apresentará à ANPD plano de gestão de reclamações, com previsão de métodos adequados de soluções de conflitos, inclusive em formato eletrônico.	

Parágrafo único - a apresentação do plano referido no *caput* será considerada pela ANPD como atenuante no momento de imposição de penalidades.
Art. Xxxx ....

ANPD Autoridade Nacional de Proteção de Dados

CONTRIBUIÇÕES À TOMADA DE SUBSÍDIOS Nº 02/2021

NOME DA INSTITUIÇÃO:
CONEXIS Brasil Digital – Sindicato Nacional das Empresas de Telefonia e de Serviços Móveis Celular e Pessoal
CNPJ: 06.102.961/0001-93

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

<table>
<tr><th colspan="2">CONTRIBUIÇÕES RECEBIDAS</th></tr>
<tr><th>TÓPICO/QUESTÃO</th><th>CONTRIBUIÇÃO/CONTIC</th></tr>
<tr><td>Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?</td><td>
Um incidente poderá acarretar risco ou dano relevante ao titular, quando houver:

Vulnerabilidade ou bug que ocasione acessos não autorizados ou situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão de dados pessoais;
Vazamento de:

dado sensível não público até a data da ocorrência do incidente para ambiente externo;
dado pessoal identificável não público até a data da ocorrência do incidente para ambiente externo, passível de perda financeira ao titular ou danos não materiais identificáveis

Exemplos de danos: perda de controle sobre seus dados pessoais ou limitação de seus direitos, discriminação, roubo de identidade ou fraude, perda financeira, reversão não autorizada de pseudonimização, danos à reputação, perda da confidencialidade (divulgação indevida) de dados pessoais protegidos pelo sigilo profissional ou qualquer outra desvantagem econômica ou social significativa para a pessoa singular em questão

Quanto aos critérios para avaliar o risco ou dano como relevante:
Sugere-se adotar métricas e parâmetros para a realidade brasileira, com o objetivo de verificar a criticidade de um incidente considerando os seguintes aspectos:

Veracidade do incidente
Natureza, sensibilidade e volume de dados pessoais

perda de integridade dos dados
indisponibilidade dos dados

Facilidade da identificação dos titulares

dados anonimizados, criptografados
relacionados às chaves de criptografia dos dados violados
relacionado a dados relacionados às credenciais de autenticação (matrícula, por exemplo) das partes interessadas

Nível de atualização e validade dos dados
Severidade das consequências aos titulares
Características especiais dos titulares

</td></tr>
</table>

	• Características do controlador • Número de titulares afetados • Grau de exposição de dados vulnerados (ambiente interno, externo e público) • Medidas técnicas, organizacionais e administrativas adotadas para mitigar o impacto sobre os titulares • Aspectos relacionados à violação de segurança para acesso aos dados (intencional, não intencional, ataque cibernético) • Se o responsável pelo dado objeto do incidente auferiu, direta ou indiretamente, vantagem com o ocorrido • Se o ambiente afetado pelos incidentes está relacionado ao país de operação de negócio do controlador/operador Referências para a criação de métricas adequadas e uniformes para questões gerais e comuns ao Setor: • *The European Union Agency for Cybersecurity - Agência Europeia para a Segurança das Redes e da Informação* (ENISA) • ***Guidelines 01/2021 - on Examples regarding Data Breach Notification - Adopted on 14 January 2021 do*** *European Data Protection Board,* além das Guidelines on Personal Data Breach notification under Regulation 2016/679 e da *Opinion 03/2014 on Data Breach Notification*[1]
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	O que importa verificar é se o risco ou dano é relevante para fins de acionamento dos mecanismos previstos no art. 48, mas o risco ou dano relevante não deve ser subdividido para estes fins. Deve ser algo tão simples quanto verificar se o dano é relevante ou se não é, sob pena de se adicionar muita subjetividade e pouca clareza na identificação dos incidentes que podem estar sujeitos aos mecanismos de notificação previstos na LGPD. Deve-se distinguir este mecanismo da metodologia que pode vir a ser utilizada dentro do *framework* de resposta a incidentes de cada agente de tratamento, sendo que essas avaliações podem ser internas, mas não devem se confundir com a classificação sobre ser um dano relevante. Importante ponderar, também, situações em que, por não ser relevante, não há a necessidade de notificação para a ANPD e não deve ser passível de punição. É o caso, por exemplo, de dados cadastrais que já estejam públicos de alguma forma ou, até mesmo, em casos que possam ser classificados como de baixa relevância para o usuário.

[1] https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2021/guidelines-012021-examples-regarding-data-breach_pt
https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052
https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	Juridicamente há distinção entre o conceito de risco e dano. O primeiro remete à ideia da **possibilidade** de ocorrer um perigo ou prejuízo. Já o segundo trata-se **efetivamente** do prejuízo suportado pelo sujeito propriamente impactado. Risco ao titular é a combinação da probabilidade de um evento vir a acontecer e de suas consequências de fato, portanto, potencial gravidade do impacto sobre o titular. O Dano relevante é efetivamente o prejuízo sofrido, seja econômico, material ou moral, como por exemplo, por meio da exposição pública de dados, usurpação de identidade, prejuízo econômico e até eventos de discriminação aos titulares impactados em um incidente em concreto. É importante que se entenda que o dano ao titular decorrente de um incidente envolvendo dados pessoais não é presumido. Nesse sentido, é possível que, mesmo com a exposição pública de dados pessoais, o titular não sofra danos diretos decorrente do "vazamento" das suas informações pessoais, contexto em que é necessária a demonstração do dano. Neste sentido é imperioso que seja diferenciado, no incidente que acarrete a violação de dados pessoais, se o acesso indevido somente expõe o titular a um risco, caso não haja comprovação de dano. Na hipótese de um vazamento de informações cadastrais de um consumidor, por exemplo, pode-se argumentar que há um maior risco, mas o dano concreto somente se configuraria após a sua comprovação. Ou seja, não existe o dano potencial.
O que deve ser considerado na avaliação dos riscos do incidente?	**Para avaliar risco ou dano como relevante, deve-se:** • Realizar investigação diretamente com a fonte denunciante, a fim de verificar a veracidade do incidente, obtendo informações comprobatórias da ocorrência deste; ○ O incidente realmente ocorreu? As informações já não eram públicas antes? • Avaliar se os dados são efetivamente passíveis de danos aos titulares, com base nos critérios apontados no primeiro item desta tomada de subsídios • Avaliar se o volume de informações relevantes comprovadamente comprometidas é expressivo em relação ao volume (%) de informações de posse da organização que sofreu o dano. • Considerar a classificação do risco, conforme níveis apontados nos itens anteriores. • Considerar os controles e medidas mitigatórias existem associadas aos riscos na organização; O Controlador deverá considerar uma combinação da gravidade do impacto potencial sobre os direitos e liberdades dos indivíduos e a probabilidade da sua ocorrência. Claramente, quando as consequências de uma violação são mais graves, o risco é mais elevado e, do mesmo modo, quando a probabilidade da sua ocorrência é maior, o risco é também aumentado[2].

[2] ARTICLE 29 DATA PROTECTION WORKING PARTY - Guidelines on Personal data breach notification under Regulation 2016/679, pág.26

Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	Poderia ser indicado o contato do Encarregado, considerando o seu papel de ser o porta-voz do Controlador nas interações com a ANPD e com os titulares de dados pessoais. Outras eventuais necessidades de informações dependerão do caso concreto, portanto, não se faz necessário adicionar outros itens ao previsto no §1º do art. 48. Quanto ao envio das informações, sugere-se incluir a possibilidade de envio parcial com a previsão de complementação futura, em termos e prazo a serem acordados diretamente com a ANPD.
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	Entende-se que a ANPD adotou - temporariamente e como recomendação até que se tenha resolução para o tema - o prazo de dois dias úteis para que se informe sobre incidentes é métrica analógica ao que determina o Decreto nº 9.936/2019, que regulamenta o cadastro positivo. Tal disposição, entretanto, aplica-se exclusivamente aos temas correlatos ao cadastro positivo, não devendo vincular os demais posicionamentos da ANPD nesta matéria. É importante buscar uniformidade para que não tenha uma confusa miríade de prazos entre setores e hipóteses, mas considerando a transversalidade da regulamentação da ANPD e a fim de evitar prejuízos ou prazos inviáveis a dados setores e hipóteses de aplicação, sugere-se que o prazo adotado seja maior. Dessa forma e considerando a complexidade técnica e a necessidade de uma investigação e análise da equipe de Segurança da Informação (interna ou terceirizada) para apurar os detalhes e vulnerabilidades do incidente, o Controlador poderá ter até 30 dias, a contar da ciência e comprovação do incidente, para avaliar, concluir e informar a ANPD se o evento em concreto poderá acarretar risco ou dano aos Titulares (nos termos do art. 48). No caso de não ser possível apurar se o incidente de segurança acarreta ou não risco ou dano relevante dentro do prazo de até 30 (trinta) dias, a notificação deverá ser feita com essa ressalva e pedido motivado da dilação do prazo para esta apuração[3]. Nestes casos as informações poderão ser enviadas de forma escalonada, conforme o desenvolvimento das apurações do incidente.

[3] ARTICLE 26WH (2) Assessment of suspected eligible data breach - Privacy Amendment (Notifiable Data Breaches) Act 2017.

Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	**Prazo Razoável** Sugerem-se as métricas da transparência e razoabilidade para a comunicação aos titulares, mas sem que se estabeleça prazo fixo. Deve-se sempre observar o nível de risco ou dano do evento para o Titular na calibragem do prazo. Esta sugestão toma como parâmetro a determinação da GDPR, no artigo 34, que fala em comunicação ao titular observando-se que seja demora injustificada. **Informações Constantes na Comunicação** **Deve-se priorizar o envio de informações claras e simples que esclareçam a ocorrência do incidente.** Sugere-se: • os dados envolvidos no incidente; • descrição da atividade e finalidade do tratamento dos dados envolvidos no incidente; • medidas para remediação do evento; • medidas que o titular possa tomar para evitar prejuízos – a depender da categoria dos dados afetados; • meios de contato com o DPO; • data da comunicação do incidente que envolva dados pessoais à ANPD.
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	Prezando pela boa-fé e transparência, observando o nível de risco ou dano do evento para o Titular, cabe ao Controlador, com base nas apurações do incidente, definir a melhor forma de comunicação, dispondo dos meios técnicos em posse da empresa para evitar onerosidade excessiva. Seriam possíveis, portanto, comunicações via e-mail; SMS; nota à imprensa; redes sociais; uso dos canais de atendimento, dentre outros. Deve-se priorizar o envio de informações claras e simples que esclareçam a ocorrência do incidente.

Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	Exceções da obrigatoriedade de informar a ANPD, seriam aquelas em que, após a avaliação, do potencial risco de dano relevante não seja considerado como alto, como por exemplo: • Após a avaliação imediata da violação de dados pessoais não for provável que resulte em risco de dano específico para direitos e liberdades fundamentais do titular (por exemplo, roubo de identidade, fraude, perdas financeiras); • Não houver evidência de que os dados tenham sido tratados indevidamente; e/ou os dados tenham sido modificados de maneira equivocada, podendo, no entanto estes serem recuperados e/ou corrigidos tempestivamente, sem dificuldade; • O evento envolver somente dados anonimizados, e, portanto, não pessoais; ou o evento envolve dados que tenham sido protegidos (antes de sua violação), através de medidas técnicas de proteção consideradas adequadas, tornando-os incompreensíveis para quem os violou, ou se os dados pessoais foram tornados essencialmente ininteligíveis para partes não autorizadas. • Adotadas medidas imediatas para mitigar e conter totalmente os riscos para os direitos e liberdades dos titulares de dados; • Os dados pessoais já se encontram disponíveis ao público e uma divulgação desses dados não constitui um risco provável para o titular.
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	A exceções da obrigatoriedade de informar os titulares, seriam aquelas em que, após a avaliação, do potencial risco de dano relevante sejam considerados de baixo risco ou dano **relevante**, como por exemplo: • Após a avaliação da eventual gravidade do incidente que envolva dados pessoais, pela ANPD (dano e risco), não for identificada a necessidade da comunicação. Este cenário poderia prover uma maior segurança aos controladores, podendo ser uma etapa/critério decisivo para comunicar ou não ao titular; • Após a avaliação/investigação da violação de dados pessoais for possível assegurar que não se trata de uma violação provável de resultar um risco elevado de dano específico para direitos e liberdades fundamentais do titular e, assim, evitar a desnecessária fadiga da notificação; • Quando o responsável pelo tratamento tiver adotado todas as medidas técnicas e organizacionais adequadas para a privacidade e proteção de dados pessoais antes da violação, ou mesmo após a violação de forma suficiente a sanar qualquer risco em tempo curto, especialmente aquelas que tornem os dados incompreensíveis para qualquer pessoa não autorizada a acessar.

Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	A ANPD deverá fazer um juízo de ponderação, de acordo com o caso concreto e com base nos seguintes critérios:
	
	• Aspectos relacionados com a violação de segurança (o incidente propriamente dito, se houve um ciberataque ou não, por exemplo, e suas características);
	• Perfil dos titulares afetados (por exemplo, dados de crianças e adolescentes etc.);
	• Tipo (dado pessoal e dado pessoal sensível);
	• Quantidade (registros) e volume de titulares afetados pela violação;
	• Grau de exposição de dados vulnerados (interno, externo e público);
	• Medidas adotadas para mitigar o impacto sobre os titulares afetados;
	• Consequências do incidente, isto é, avaliar até que ponto este causou maior ou menor dano aos direitos ou liberdades dos titulares afetados;
	• Se o incidente está relacionado ou não a:
	  ○ violação da confidencialidade e dos dados;
	  ○ perda de integridade dos dados;
	  ○ indisponibilidade dos dados;
	  ○ dados protegidos por senha, ou anonimizados, criptografados etc;
	  ○ chaves de criptografia dos dados violados;
	  ○ credenciais de autenticação (matrícula, por exemplo) das partes interessadas (no caso de um vazamento interno ou externo);
	• Se a violação foi ou não dolosa;
	• Se os dados pessoais objeto da violação já se encontravam publicamente disponíveis;
	• Se houve reincidência de conduta;
	• Se houve vantagem auferida (direta ou indiretamente);
	• Se o agente de tratamento já adotava ou não medidas técnicas de segurança e preventivas para não ocorrência de incidentes

Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	De início, é importante considerar o tamanho das empresas e os processos empregados nas operações de tratamento de dados para o desenho da metodologia e análise de gravidade do incidente de segurança. Empresas de grande porte podem ocorrer incidentes que, considerando o seu tamanho, não serão considerados relevantes ao se analisar a volumetria, tipologia e exposição. No entanto, em empresas de pequeno porte podem ocorrer incidentes que, considerando o seu tamanho, serão considerados relevantes ao se analisar a volumetria, tipologia e exposição. Entende-se que empresas classificadas como de porte grande, médio e pequeno devem possuir faixas distintas para cálculo da volumetria, com seus respectivos pesos, a serem definidos em conjunto com a ANPD. Uma metodologia possível é esta da ponderação entre: **Volumetria x Tipologia x Exposição** • Volumetria: indica a quantidade de registros vulnerados no incidente de segurança envolvendo dados pessoais. Quanto maior o número de registros e titulares impactados, mais crítico será o evento. • Tipologia: indica a categoria de dado pessoal vulnerado no evento, de acordo com a definição estabelecida pela própria LGPD (dados pessoais e pessoais sensíveis). Considerando o entendimento consolidado e a interpretação extraída diretamente da LGPD, o tratamento de dados pessoais sensíveis deve ser realizado com maiores cuidados e atenção pelos Agentes de Tratamento dada a sua sensibilidade natural. Nesse sentido, um incidente de segurança envolvendo dados pessoais sensíveis acaba sendo mais crítico que um incidente envolvendo dados pessoais comuns ou de identificação, por exemplo. • Exposição: identifica o ambiente no qual o evento em questão foi descoberto ou acabou sendo exposto. A Exposição poderá ser interna, externa e pública, sendo esta última a que indica maior criticidade para o evento, levando em consideração a eventual disseminação de dados pessoais, sobretudo na internet. ➢ Consideram-se os seguintes critérios para avaliar com notas e pesos diferentes, conferindo níveis de criticidade com base na **volumetria, tipologia e exposição**: o Quanto à volumetria, faixas diferenciadas de quantidade de titulares afetados. o Quanto à tipologia, pesos diferentes se são dados pessoais ou dados pessoais sensíveis.

<table>
<tr><td></td><td>

Quanto à criticidade, em função do grau de exposição de dados afetados, pesos diferentes se:

interno: quando a exposição dos dados afetados pela violação de segurança detectada é controlada internamente
externo: quando a exposição dos dados afetados pela violação de segurança detectada é controlada em um perímetro ao nível do fornecedor, operador
público: quando a exposição dos dados afetados pela violação de segurança detectada pode ser acessada por meio de uma rede pública ou da internet.

Outra sugestão de metodologia a ser utilizada seria a European Union Agency for Cybersecurity - Agência Europeia para a Segurança das Redes e da Informação (ENISA)
</td></tr>
<tr><td>Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?</td><td>
Sugestões de medidas administrativas no âmbito da governança, incluindo as de natureza jurídica:

Políticas e controles corporativos;
Treinamentos, capacitação de colaboradores, comunicação e aculturamento;
Contratos: inclusão de anexos de SI e LGPD; revisão; cláusulas; DPA;
Comitês de Crise e Executivo;
Políticas de privacidade, de cookies, termos de uso para sites e aplicativos;

Sugestões de medidas determinadas pela ANPD aos controladores:

Monitoramento da causa raiz para evitar novos incidentes que possam acarretar a violação de dados pessoais;
Correção de vulnerabilidades e planos de contingência e/ou melhoria;
Evolução da mitigação do impacto (aumento ou redução)
Controles a serem implementados ou aperfeiçoados

Importante levar em consideração que as medidas de comando e controle somente serão adotadas na hipótese do Controlador não colaborar com a Autoridade.
</td></tr>
<tr><td colspan="2">Referências bibliográficas:

• NÓBREGA MALDONADO, Viviane. OPICE BLUM, Renato. Comentários ao GDPR: Regulamento Geral de Proteção de Dados da União Europeia. São Paulo: Thomson Reuters Brasil, 2018.
• NÓBREGA MALDONADO, Viviane. OPICE BLUM, Renato. LGPD: Lei Geral de Proteção de Dados comentada. São Paulo: Thomson Reuters Brasil, 2019.
</td></tr>
</table>

• OPICE BLUM, Renato. VAINZOF, Rony. MORAES, Henrique Fabretti. Data Protection Officer (Encarregado): teoria e prática de acordo com a LGPD e GDPR. 1. ed. - São Paulo: Thomson Reuters Brasil, 2020. • TEPEDINO, Gustavo. FRAZÃO, Ana. DONATO OLIVA, Milena. Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito brasileiro. São Paulo: Thomson Reuters Brasil, 2019. • PALHARES, Felipe. Temas atuais de proteção de dados. São Paulo: Thomson Reuters Brasil, 2020. • SCHERTEK MENDES, Laura. DONEDA, Danilo. WOLFGANG SARLET, Ingo. RODRIGUES JR. Otavio Luiz. BIONI, Bruno. Tratado de Proteção de Dados Pessoais. Rio de Janeiro: Forense, 2021.

SUGESTÃO DE NORMATIVO, SE HOUVER
Sugerimos a **construção de padrão técnico-jurídico, autorregulado no setor, via Conexis**, sem a intenção de amarras e engessamento, mas de estruturação de métricas e metodologia no campo de telecomuniques - até com assessoramento externo de consultoria e atuação das áreas de Segurança de Informação e TI, das associadas, especifico para regras ao setor de telecomunicações para categorização de incidentes e tratamentos correlatos – a ser endossado pela ANPD, padronizando e simplificando o tratamento dos Incidentes – que se mostram constantes e o que ajudaria a todos com a uniformização geral do tema.

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA : CNseg
CPF/CNPJ:

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

TÓPICO/QUESTÃO	CONTRIBUIÇÃO CNSEG
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	Segundo dispõe o art. 48 da LGPD, o incidente de segurança que deverá ser comunicado à ANPD é aquele capaz de acarretar risco ou dano relevante ao titular. Deste modo, uma vez que o titular poderá estar sujeito a danos materiais e imateriais, a avaliação do incidente deverá considerar a quantidade e os tipos dos dados afetados e as possíveis consequências de seu uso irregular. Por exemplo: o vazamento de dados pessoais sensíveis de saúde pode expor a intimidade do titular, configurando um elevado risco de dano imaterial. O vazamento de dados bancários, por outro lado, pode trazer riscos ao patrimônio do titular. O vazamento de dados cadastrais (nome completo e data de nascimento), todavia, pode não trazer riscos relevantes. Nesse sentido, para avaliar se há risco ou dano relevante ao titular, necessário que seja feita uma análise dos dados envolvidos no incidente de segurança, para que ele possa ser classificado como de baixo, médio ou elevado risco. Quanto aos critérios que deverão ser considerados nessa classificação de risco, propomos sejam considerados: (i) os tipos e volume de dados pessoais envolvidos no evento adverso (com destaque para dados sensíveis), (ii) características especiais do controlador de dados (ex. atuação em mercado regulado, obrigação de sigilo profissional/financeiro/fiscal etc.), (iii) características especiais dos indivíduos afetados (ex. hipossuficiência, crianças e adolescentes, idosos etc.), (iv) impacto do evento adverso na confidencialidade dos dados pessoais (ex. dados não criptografados, não pseudonimizados ou não protegidos por senha), (iv) a relação dos titulares dos dados com o controlador (ex. empregado, prestador de serviço, cliente etc); (v) impacto do evento adverso na integridade dos dados pessoais (ex. alteração não autorizada), e (vi) impacto do efeito adverso na disponibilidade dos dados pessoais (ex. perda ou destruição não autorizada). Em resumo, seria interessante que a ANPD adotasse uma gradação de classificação do incidente de segurança, em que fossem consideradas, de acordo com os critérios acima mencionados, as hipóteses de baixo, médio e alto risco.

	Subsídios para a contribuição: • REGULAMENTO (UE) 2016/679 (Recital 75) - https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN • ENISA. Handbook on Security of Personal Data Processing (Methodological Steps Overview – páginas 10 e seguintes) - https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing • Grupo do Artigo 29. Orientações sobre a notificação de uma violação de dados pessoais ao abrigo do Regulamento (UE) 2016/679 - https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052 • Comitê Europeu para a Proteção de Dados. Guidelines 01/2021 on Examples regarding Data Breach Notification - https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	Para guardar coerência com a proposta contida no item anterior, seria interessante que fossem adotadas categorias diferentes de classificação dos riscos associados ao incidente de segurança. Assim, partindo dos critérios propostos no item anterior, poderia ser sugerida uma classificação em pelo menos três níveis de risco (baixo, médio e alto), sendo que o incidente classificado como de baixo risco não seria considerado relevante e, por consequência, não precisaria ser obrigatoriamente comunicado à ANPD e aos titulares. Sugere-se, contudo, seja avaliada pela ANPD a conveniência e eficiência de serem comunicados os incidentes qualificados como de médio risco, visto que pela experiência do setor de seguros com outras normas regulatórias que exigem a comunicação de eventos aos seus órgãos fiscalizadores, como, por exemplo, em relação às normas de combate à lavagem de dinheiro, tal exigência de informar incidentes ou situações que representem situação que não seja de alto risco pode levar a uma excessiva comunicação de incidentes, impossibilitando que a ANPD concentre-se naqueles incidentes que representam um risco alto para os titulares dos dados. No caso específico das normas que exigem a comunicação de situações que possam indicar prática de lavagem de dinheiro, no decorrer dos anos e com a experiência adquirida pelo órgão fiscalizador, seu escopo foi pouco a pouco sendo delimitado para apenas exigir que situações que possam representar uma indicação efetiva da prática de lavagem de dinheiro sejam comunicadas.

	Neste sentido, o segmento supervisionado pela Susep seguia o estabelecido na Circular Susep 445, de julho de 2012, que será revogada em 03.05.2021, quando passará seguir regras baseadas em gestão de risco, da Circular Susep 612 de 2020. O normativo anterior era a Circular Susep 380, de 2008. A Circular Susep 445 estabelece a obrigatoriedade de as supervisionadas desenvolverem controles internos com a finalidade de monitorar os riscos de a entidade estar envolvida em situações de lavagem de dinheiro ou financiamento ao terrorismo. O normativo divide as ocorrências a serem comunicadas em dois grupos. As ocorrências do Grupo I, que devem ser comunicadas independente de qualquer análise e as do Grupo II, após análise de que se tratam efetivamente de operações suspeitas. As alterações promovidas pela Circular Susep 445 em relação à Circular Susep 380 começam a explicar a queda no número de comunicações a partir do ano de 2013. Contudo, ainda com o cenário de muitas comunicações sem análise que acabam por aumentar a base reportada, mas prejudicam a análise e não contribuem para a melhoria da qualidade dos resultados. Não por outro motivo a Susep e outros órgão reguladores revisaram seus normativos recentemente, e todos (BACEN, CVM e SUSEP) publicaram novas normas baseadas em gestão do risco, em 2020, sobre o tema. A nova Circular 612 de 2020 trouxe uma alteração relevante em relação ao normativo vigente no qual eliminaram-se praticamente todas as situações em que se requeriam reporte automático de operações ao COAF, mantendo-se apenas a obrigação de se informar ao órgão aquelas em que houve pagamento de prêmio ou aporte em espécie em valor superior a R$ 10 mil durante um mês. As demais operações deverão passar por uma análise criteriosa de risco, que observará entre outros fatores, o perfil do cliente, a adequação do produto com a realidade financeira patrimonial do mesmo, seu enquadramento como pessoa politicamente exposta, o risco de o produto ser utilizado como veículo para a lavagem de dinheiro, entre outros. A abordagem baseada em risco, recomendada pelo GAFI, e agora incorporada na nova circular da Susep, oferece ao setor a possibilidade de adoção de medidas simplificadas, e sobretudo proporcionais aos riscos identificados, fator essencial para a alocação eficiente de recursos, redução do custo regulatório e maior eficiência no combate de práticas criminosas pelas autoridades competentes.

Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	Deve-se distinguir o risco, que é um dano em potencial (probabilidade), do dano, que é a concretização do risco. Nesse sentido, a sugestão é que o regulamento considere como risco a probabilidade da ocorrência de um dano ao titular, ou seja, uma situação hipotética. O dano, por sua vez, só pode ser considerado caracterizado quando, a partir de um caso concreto, puder ser aferido efetivo prejuízo (material ou moral) ao titular do dado.
O que deve ser considerado na avaliação dos riscos do incidente?	Para guardar coerência com as sugestões contidas nos itens anteriores, sugere-se que sejam considerados os seguintes critérios para a avaliação dos riscos do incidente: **(i)** os tipos e volume de dados pessoais envolvidos no evento adverso (com destaque para dados sensíveis), **(ii)** características especiais do controlador de dados (ex. atuação em mercado regulado, obrigação de sigilo profissional/financeiro/fiscal etc.), **(iii)** características especiais dos indivíduos afetados (ex. hipossuficiência, crianças e adolescentes, idosos etc.), **(iv)** a relação dos titulares dos dados com o controlador (ex. empregado, prestador de serviço, cliente etc); **(iv)** impacto do evento adverso na confidencialidade dos dados pessoais (ex. dados não criptografados, não pseudonimizados ou não protegidos por senha), **(iv)** impacto do evento adverso na integridade dos dados pessoais (ex. alteração não autorizada), e **(v)** impacto do efeito adverso na disponibilidade dos dados pessoais (ex. perda ou destruição não autorizada). Subsídios para a contribuição: • REGULAMENTO (UE) 2016/679 (Recital 75) - https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN • ENISA. Handbook on Security of Personal Data Processing (Methodological Steps Overview – páginas 10 e seguintes) - https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing • Grupo do Artigo 29. Orientações sobre a notificação de uma violação de dados pessoais ao abrigo do Regulamento (UE) 2016/679 - https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052 • Comitê Europeu para a Proteção de Dados. Guidelines 01/2021 on Examples regarding Data Breach Notification - https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf

Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	Sugere-se que além das informações listadas no art. 48, §1º, o controlador possa, a seu critério e de acordo com as particularidades de cada caso, prestar informações adicionais que julgar relevantes. Em contrapartida, para que possa haver um equilíbrio regulatório, a ANPD também poderia, desde que de forma justificada e que não ponha em risco os segredos comerciais e industriais do controlador, solicitar informações adicionais.
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	Na identificação de um incidente de segurança, e diante da possibilidade de a ANPD vir a adotar o mesmo prazo estabelecido na legislação europeia (72 horas), sugerimos que seja considerado o prazo de **5 (cinco) dias úteis**, que deverá ser contado a partir do momento em que o controlador tiver conhecimento inequívoco do incidente. Esse prazo maior se justifica pelo fato de que na LGPD existe a necessidade de se avaliar a relevância do risco, diferente do que ocorre na legislação europeia, onde incidente que representar risco, ainda que irrelevante, deverá ser comunicado à autoridade. Também seria útil que houvesse a possibilidade de o controlador, na hipótese de não ter todas as informações mencionadas no art. 48, §1º, da LGPD dentro do prazo de comunicação, poder fazer posterior complementação das informações, como aliás está previsto no art. 33, §4º do GDPR: *Artigo 33 – omissis* *4. Caso, e na medida em que não seja possível fornecer todas as informações ao mesmo tempo, estas podem ser fornecidas por fases, sem demora injustificada.* Essa previsão, aliás, já foi contemplada no formulário de comunicação de incidentes de segurança publicado pela ANPD em sua página de internet (https://www.gov.br/anpd/pt-br/assuntos/formulario-de-comunicacao-de-incidentes-de-seguranca-com-dados-pessoais_01-03-2021.docx), apesar de não estar respaldada em qualquer instrumento normativo no momento, por isso a importância dessa possibilidade ser reconhecida no ato normativo que regulamentará as disposições sobre incidentes de segurança contidas na LGPD.
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa	A proposta é no sentido de que o prazo para o controlador comunicar aos titulares dos dados sobre a ocorrência do incidente de segurança seja de **5 (cinco) dias úteis**, a contar da data da comunicação feita à ANPD.

comunicação? As mesmas do §1º do art. 48?	Como há a possibilidade de a ANPD determinar a adoção de medidas para salvaguardar os direitos dos titulares (art. 48, §2º), seria interessante que estes fossem comunicados sobre o incidente já sabedores de eventuais providências adotadas por determinação do órgão regulador. Sugerimos que seja possível, ainda, a dilação deste prazo dependendo das peculiaridades e complexidades de cada incidente, mediante autorização da ANPD. Quanto às informações que deverão constar nessa comunicação, parece-nos que o mais adequado seja limitar àquelas listadas no art. 48, §1º, facultando ao controlador, entretanto, prestar informações adicionais que julgar relevantes.
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	A sugestão é no sentido que devam existir possibilidades alternativas de comunicação, ou seja, caberia ao controlador, a seu critério, utilizar quaisquer dos seguintes meios que julgar mais eficazes: (i) direta e individualmente aos titulares, através de qualquer meio de comunicação (ex. e-mail, carta, portal do cliente); (ii) anúncio em seus canais oficiais (site, redes sociais etc); ou (iii) anúncio publicitário. A própria LGPD, ao prever no §2º de seu artigo 48 que a ANPD, dependendo da gravidade do incidente, poderá determinar ao controlador a *"ampla divulgação do fato em meios de comunicação"* sugere que exista uma maior liberdade por parte do controlador de escolher o meio de comunicação aos titulares dos dados. Vale citar, a fim de reforçar a ideia da possibilidade de livre escolha do meio de divulgação para os titulares dos dados a regra sobre notificação de vazamentos do HIPAA (*Health Insurance Portability and Accountability Act*). A importância dessa liberdade de escolha para utilizar o meio mais adequado se justifica pelo fato de que controladores podem estar com os dados para contato dos titulares dos dados defasados devido ao término do vínculo com o Titular e o decurso do tempo, bem como quando a volumetria de comunicações individuais a ser realizado envolver grande número de Titulares. <u>Subsídios para a contribuição:</u> HIPAA Breach Notification Rule - https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html

Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	Em consonância com as sugestões dos itens anteriores, não deveria ser obrigatória a comunicação à ANPD de incidentes de segurança considerados de baixo risco e sugeriu-se que a ANPD avaliasse a conveniência e eficiência de se exigir a comunicação de incidentes de médio risco.
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	Em consonância com as sugestões anteriores, não deveria ser obrigatória a comunicação aos titulares dos dados de incidentes de segurança considerados de baixo risco. Sugere-se, igualmente, que a ANPD avalie a conveniência e eficiência de se exigir a comunicação de incidentes de médio risco também as titulares dos dados, já que isso poderia levar a que passassem a receber um grande número de comunicações, pois a LGPD se aplica aos setores público e privado de uma maneira geral, o que eventualmente afastaria a atenção dos titulares dos dados daqueles incidentes que pudessem efetivamente apresentar um alto risco.
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	Propõe-se que a análise da gravidade do incidente de segurança pode ser definida como a estimativa da magnitude do impacto potencial, derivado da violação dos dados, sobre os indivíduos. Os elementos centrais que devem ser levados em consideração ao avaliar esta gravidade são: • **Contexto do tratamento de dados (CTD)**: aborda o tipo de dados violados, juntamente com uma série de fatores ligados ao contexto geral do tratamento. Está no centro da metodologia e avalia a criticidade de um determinado conjunto de dados em um contexto de tratamento específico. • **Facilidade de identificação (FI)**: determina quão facilmente a identidade dos indivíduos pode ser deduzida a partir dos dados envolvidos na violação. É um fator de correção em relação ao CTD. A criticidade geral de um tratamento de dados pode ser reduzida, dependendo do valor do FI. Em outras palavras, quanto menor for a facilidade de identificação, menor será a pontuação geral. Portanto, a combinação do FI e CTD (multiplicação) dá a pontuação inicial da gravidade da violação dos dados. • **Circunstâncias do incidente (CI)**: aborda as circunstâncias específicas da violação, que estão relacionadas ao tipo de violação, incluindo principalmente a perda de segurança dos dados violados, bem como qualquer intenção maliciosa envolvida. Quantifica as circunstâncias específicas da violação, podendo estar presente ou não em uma determinada situação. Deste modo, quando presente, o CI só pode aumentar a gravidade de uma infração específica. Por este motivo, a pontuação inicial pode ser ajustada ainda mais pelo CI. Assim, a pontuação final da avaliação da gravidade pode ser extraída usando a seguinte fórmula: **CTD x FI + CI.**

	Deste modo, caso venha a ser adotada essa sugestão, caberá à ANPD, a partir dos critérios propostos, classificar o incidente como de baixa, média ou alta gravidade. Subsídios para a contribuição: • ENISA. Recommendations for a methodology of the assessment of severity of personal data breaches - https://www.enisa.europa.eu/publications/dbn-severity
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	Sugere-se seja utilizada a metodologia proposta no quesito anterior.
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	Propõe-se o seguinte rol das providencias que poderiam ser determinadas pela ANPD: **(i)** a realização de auditorias, desde que não ponham em risco os segredos comerciais e industriais do controlador; **(ii)** a realização de auditorias pelo controlador junto a seus operadores envolvidos no incidente de segurança, respeitados os segredos comerciais e industriais dos operadores; **(iii)** a adoção de medidas de segurança de natureza técnica ou administrativa, desde que proporcionais e compatíveis com as atividades do controlador; **(iv)** a elaboração e implementação de plano de ação para mitigação de riscos; **(v)** a contratação de serviços de monitoramento de crédito em caso de incidente envolvendo dados financeiros ou que viabilizem fraudes financeiras.
COMENTÁRIOS SOBRE O FORMULÁRIO DE NOTIFICAÇÃO	De fato, a redação do art. 48 da LGPD atribui ao controlador (e não ao operador) a obrigação de comunicar a ocorrência de incidente de segurança. Portanto, parece-nos relevante destacar que o operador não deve poder notificar um incidente de segurança à ANPD, devendo tal opção ser excluída do formulário elaborado pela ANPD. Por outro lado, também concordamos que é mais compatível com a LGPD, que atribui ao encarregado o papel de atuar como canal de comunicação com a ANPD (art. 5º VIII), que seja dele a incumbência de fazer a comunicação do incidente de segurança, ressalvadas as hipóteses em que não houver encarregado (art. 41, §3º), quando a comunicação poderá ser feita por qualquer representante legal do controlador, desde que devidamente identificado.
PRAZO PARA TOMADA DE SUBISÍDIO	Propõe-se seja avaliada pela ANPD a possibilidade de alongamento dos prazos para apresentação de contribuições em futuras tomadas de subsídios, a fim de que se possa assegurar uma maior participação da sociedade, considerando-se a novidade e complexidade das matérias a serem

	regulamentadas pela ANPD. O prazo de 30 dias para a consulta pública é curto para tratar de temas tão complexos e variados.

ANPD Autoridade Nacional de Proteção de Dados

CONTRIBUIÇÕES REFERENTES À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: CONFEDERAÇÃO NACIONAL DE SAÚDE - CNSaúde

CPF/CNPJ: 97.496.574/0001-34

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS	
IMPORTANTE: Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	**A avaliação do potencial de riscos ou danos decorrentes de um incidente deve levar em conta critérios objetivos como: a natureza da violação (se decorreu de incidente de dentro da companhia para fora, ou se decorreu de fator extrínseco, por exemplo); a possibilidade de se identificar os titulares dos dados envolvidos no incidente; a natureza dos dados pessoais objeto do incidente (sensíveis ou não); e a probabilidade de que o uso dos dados objeto do incidente possa causar danos relevante aos titulares. Por outro lado, o volume de dados e/ou de usuários impactados não deve ser considerado como um critério inicial para aferição do potencial de risco ou dano, mas apenas como um elemento secundário que venha a contribuir para a aferição de uma maior ou menor gravidade do incidente.**
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	**Sim, poderia ser subdividido nos moldes utilizados pela Agência da União Europeia para a Cibersegurança (ENISA), em Baixo, Médio, Alto e Muito Alto. No entanto, o risco para ser considerado relevante deve ser aquele que extrapola a esfera da instituição em que o incidente ocorreu, e que possua potencial de causar prejuízos aos titulares dos dados. Ou seja: riscos ou danos baixos ou médios, assim considerados como aqueles que acarretem apenas inconvenientes de curta duração e pequeno impacto no dia a dia da empresa (baixo) ou que, apesar de envolver problemas e prejuízos razoáveis ao dia a dia da empresa (médio), conseguem permanecer dentro da alçada da empresa, não devem ser considerados relevantes para fins de comunicação à Autoridade.** **Já os riscos considerados altos possuem o condão de causar danos concretos aos titulares dos dados, mas são passíveis de correção ou reparos, e ao extrapolarem a esfera da instituição, podem acarretar danos de pequeno a médio impacto aos titulares. Por fim, os incidentes considerados de muito alto impacto são aqueles não são passíveis de correção ou reparos, e ao**

	extrapolarem a esfera da instituição, podem acarretar consequências graves e permanentes.Tratando-se de dados sensíveis ou de indivíduos vulneráveis, incluindo crianças e adolescentes, o risco ou dano deverá ser categorizado em um nível mais alto que os demais.
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	**Os riscos estão relacionados com o potencial impacto/probabilidade negativo sobre os direitos e liberdades individuais, e devem ser determinados levando em consideração critérios objetivos, como os destacados na resposta ao quesito anterior: potencial de baixo, médio, alto ou muito alto impacto. Por outro lado, o dano é a materialização do risco, que pode ser tangível/concreto ou intangível. Não deve ser considerada a tese do dano presumido ("in re ipsa").**
O que deve ser considerado na avaliação dos riscos do incidente?	**Na avaliação dos riscos de um incidente, deve-se ter em mente o potencial de efetivo prejuízo ao titular de dados, a fim de prevenir comunicações indevidas à ANPD e desgastes desnecessários ao agente de tratamento e aos próprios titulares. Neste sentido, para se avaliar os riscos do incidente devem ser considerados (i) o contexto em que o processamento de dados ocorreu e quais os tipos de dados violados, (ii) a possibilidade de identificação dos titulares de dados que tiveram suas informações violadas e, (iii) as circunstâncias da violação.**
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	**Além das informações listadas no §1º do art. 48, seria prudente que o controlador mencione na notificação, ainda, os dados de contato do Encarregado de Proteção de Dados da organização; as consequências prováveis ou já concretizadas em razão do incidente; e o número aproximado de registros/dados afetados, ressalvada a possibilidade de apresentação de informações adicionais a posteriori.**
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	**O regulamento europeu determina que o controlador deve comunicar a autoridade supervisora, sempre que possível, até 72 horas após ter tido conhecimento da violação, a menos que não seja suscetível de risco aos direitos e liberdades das pessoas singulares. A LGPD, por sua vez, recomenda que a comunicação seja feita no prazo de 2 dias úteis, contados da data do conhecimento do incidente. Entretanto, quando se trata do setor de saúde, estes prazos podem ser muito difíceis ou praticamente impossíveis de serem cumpridos, tendo em vista a enorme quantidade de dados pessoais, sobretudo sensíveis, envolvida no âmbito dos prestadores de saúde. Diante disso, uma importante referência a ser considerada pela ANPD é a legislação**

	americana, a Health Insurance Portability and Accountability Act (HIPAA), que determina que informações médicas de pacientes sejam protegidas, garantindo a privacidade e a segurança de dados pessoais, e traz a seguinte Regra de Notificação de Violação: no caso de incidente com mais de 500 pessoas afetadas, as organizações têm o prazo de 60 dias corridos, a partir da sua descoberta, para reportar o fato à autoridade competente; e sendo menos de 500 indivíduos afetados, a organização deverá notificar a autoridade dentro de 60 dias a partir do final do ano calendário em que foi descoberta. **Um prazo mais flexível, na linha do racional previsto no HIPAA, pode fazer jus à realidade brasileira e se justifica diante da sensibilidade e complexidade dos dados tratados no setor de saúde. Afinal, a comunicação de um incidente de segurança de dados pessoais sensíveis deve ser feita com a máxima cautela a fim de evitar manifestações açodadas/precipitadas, tanto por parte dos titulares/pacientes, quanto por parte da mídia e demais organizações.** **Nesta linha, entendemos razoável um prazo de 5 dias para incidentes envolvendo menos de 500 indivíduos afetados, e um mínimo de 10 dias para comunicação à ANPD, em caso de incidente envolvendo mais de 500 titulares.**
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	**Pelo referencial europeu, a comunicação de um incidente aos titulares de dados deve ser feita sem demora justificada, ou seja, o mais rápido possível. Acaso seja definido o prazo proposto no tópico anterior, todas as informações destinadas aos titulares já terão sido obtidas, sendo possível a comunicação em até 48 horas após a comunicação à ANPD. Além disso, ao informar o titular, deve ser utilizada uma linguagem clara e acessível, contendo, no mínimo, as informações do §1º do art. 48 e, ainda, sugestões de como os titulares podem se proteger de possíveis consequências advindas do incidente, como, por exemplo, a redefinição de senhas no caso de credenciais de acesso terem sido comprometidas.**
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias,	**A comunicação de um incidente de segurança ao titular de dados deve ser sempre direta e individual, exceto quando for impossível contatá-los individualmente ou quando necessário um esforço desproporcional ao agente de tratamento. No mesmo sentido, a Regra de Notificação de Violação do HIPAA exige que a organização notifique os indivíduos afetados por e-mail (se o titular concordou previamente com a comunicação eletrônica). Além disso, a norma dispõe sobre as seguintes situações: se forem menos de 10 titulares afetados, a comunicação poderá ser feita por telefone ou aviso por escrito; por outro lado, se o incidente envolver mais de 10 titulares afetados,**

pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	**e a organização não puder contatá-los, a comunicação deverá ser publicada na mídia. No Brasil, a comunicação aos titulares de forma direta e individual também se revela prioritária e deve ser a regra, sendo a comunicação pública a exceção.**
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	**A notificação à ANPD pode ser excepcionada nos casos de incidente em que os riscos para os direitos e liberdades dos indivíduos sejam improváveis. O referido entendimento advém das diretrizes do Grupo de Trabalho do artigo 29 do General Data Protection Regulation (GDPR). O HPIAA, por outro lado, determina que incidentes com menos de 500 indivíduos afetados devam ser comunicados à autoridade competente somente por meio de um registro anual. Esse racional pode se configurar como uma boa alternativa aos incidentes nacionais na hipótese dos dados em saúde.**
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	**Propomos a mesma linha prevista na GDPR, em que a comunicação de um incidente de segurança aos titulares de dados não será obrigatória: (i) quando o controlador tiver tomado medidas técnicas e organizacionais adequadas para proteger dados pessoais antes da violação (por exemplo, criptografia de ponta a ponta); (ii) quando, imediatamente após o incidente, o controlador tiver adotado medidas para garantir que o alto risco colocado aos direitos e liberdades dos indivíduos não é mais provável que se materialize; (iii) quando a comunicação com o titular for impossível ou onerosamente desproporcional para o agente de tratamento.**
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	**Os critérios de análise da gravidade de um incidente de segurança poderiam ser os mesmos daqueles apresentados para avaliação de risco/dano. Ou seja, a gravidade do incidente poderia ser igualmente subdividida em categorias: Baixa, Média, Alta e Muito Alta. Para tanto, seriam adotados critérios objetivos: tipo de violação; facilidade de identificação dos titulares; gravidade das consequências para os indivíduos e características especiais do titular, sendo que incidentes com 500 indivíduos afetados ou mais podem ser considerados muito graves.**

Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	**A Agência da União Europeia para a Cibersegurança (ENISA) elaborou, em janeiro de 2018, um guia para orientar as empresas para avaliar o impacto sobre os direitos e liberdades fundamentais dos titulares, resultantes da possível perda de segurança dos dados pessoais.** **ISO 31000 - Risk Management (https:www.nist.gov/).**
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	
O formulário traz a possibilidade de comunicação do incidente por meio do operador e, inclusive, anterior ao controlador. O operador pode/deve comunicar a ANPD sobre a ocorrência de incidentes de segurança?	**A regra geral é a notificação pelo controlador e não pelo operador, pois a notificação pelo operador pode gerar incentivos inadequados, além de ir de encontro a estipulações contratuais ou, ainda, atribuir ao operador o papel de avaliação da gravidade do incidente que, por lei, cabe ao controlador.**
SUGESTÃO DE NORMATIVO, SE HOUVER	
Orientações sobre a notificação de uma violação de dados pessoais nos termos do Regulamento 2016/679 - Grupo de Trabalho do artigo 29 do GDPR: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052	
Art. 34.º, nº 3, alínea C - GDPR: https://gdpr-info.eu/art-34-gdpr/	

Recital 75 GDPR: https://gdpr-info.eu/recitals/no-75/
Recital 76 GDPR: https://gdpr-info.eu/recitals/no-76/
Health Insurance Portability and Accountability Act (HIPAA): https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf
Agência da União Europeia para a Cibersegurança (European Network and Information Security Agency - ENISA)
ISO 31000 - Risk Management: https:www.nist.gov/

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: COTS Advogados (Cots Sociedade de Advogados)

CPF/CNPJ: 17.229.088/0001-10

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS **IMPORTANTE:** Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	**A Lei Geral de Proteção de Dados (Lei 13.709/2018), além de representar um importante marco regulatório para o país, tem um papel determinante no livre fluxo internacional de dados pessoais, sendo fundamental que suas disposições sejam, ao menos, compatíveis com as legislações sobre o tema a nível global, o que inclui a gestão de incidentes com dados pessoais.** **Isso porque, para que o fluxo de dados pessoais entre países e organizações seja facilitado, é necessário que as normas nacionais sobre o tema sejam minimamente equiparáveis, de modo a garantir a proteção de dados pessoais em um nível similar durante todo o fluxo das informações. Todavia, essa compatibilidade entre as normas não quer dizer, necessariamente, que o Brasil deva adotar exatamente as mesmas disposições encontradas em outras localidades, uma vez que nosso país tem diversas diferenças a nível cultural, social e econômico, o que demanda uma abordagem que seja aderente, também, à realidade brasileira.** **Desta feita, para a determinação sobre a gravidade de um incidente com dados pessoais, ou seja, para a avaliação dos possíveis riscos e danos advindos de um incidente, a ANPD deve estipular critérios similares àqueles já definidos em outras localidades, com a consideração das peculiaridades nacionais, aproximando, assim, a legislação brasileira daquelas que regulam o tratamento de dados pessoais ao redor do mundo.** **Dito isto, o primeiro ponto a ser abordado é o próprio tópico. Segundo consta, este tópico versa sobre "Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano**

	como relevante". Todavia, a nosso ver, antes de qualquer análise pela ANPD, a responsabilidade sobre a análise de risco ou dano ao titular cabe ao CONTROLADOR dos dados pessoais, conforme dispõe o caput do art. 48 da LGPD: "Art. 48. *O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.".* **Assim, a responsabilidade pela análise do risco/dano recai, a princípio, sobre o Controlador dos dados pessoais, não sobre a ANPD, razão pela qual a ANPD deve orientar os agentes de tratamento sobre como realizar tal análise. ANPD, por sua vez, deverá considerar os mesmos elementos que o Controlador, isto é, deverá verificar se o Controlador cumpriu sua orientação quanto à análise de risco/dano, observando os critérios indicados pela ANPD ao Controlador. Como exemplo, podemos citar a ferramenta disponibilizada pela ICO-UK (Information Comissioner's Officer) para que os controladores possam fazer uma auto-análise. (disponível em: https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach-assessment/)** **Com vistas a facilitar a análise sobre a severidade do incidente, sugerimos que a ANPD defina uma espécie de "checklist" para ser preenchida pelo Controlador dos dados, culminando em critérios objetivos para a análise. Como referência, podemos citar a metodologia da ENISA (European Union Agency for Network and Information Security), "Recommendations for a methodology of the assessment of severity of personal data breaches", publicada em dezembro de 2013.** **Neste sentido, o "checklist" deveria abranger:** **Contexto do Tratamento de Dados** **Análise das características dos dados afetados, bem como de seus titulares** • **Tipos de dados afetados: dados pessoais, dados pessoais sensíveis;** • **Categoria dos dados afetados: simples, comportamentais, financeiros, origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico;** • **Tipos de titular afetados: adultos, crianças, idosos, entre outros;**

	• **<u>Volume de titulares afetados:</u> indicação de faixas (1-100; 100-500; 500-1000; 1000-2000, etc)** • **<u>Volume de dados afetados:</u> indicação de faixas (1-100; 100-500; 500-1000; 1000-2000, etc)** • **<u>Características especiais do Controlador</u>: instituição financeira, instituição de saúde, instituição religiosa, sindicato ou organização equiparável, bureaus de informação/crédito, rede social, instituição de caráter filosófico, instituição de caráter político, entre outros tipos de organização que tem sua atividade voltada ao tratamento de dados sensíveis ou em larga escala;** **<u>Possibilidade de Identificação do Titular</u>** **Análise sobre o potencial do incidente em relação à identificação dos titulares. Deve ser analisada com base na probabilidade de identificação, direta ou indireta, considerando o contexto do incidente:** • **<u>Remota:</u> quando os registros envolvidos no incidente indiquem identificação impossível do titular ou extremamente difícil, ainda que possível em certas hipóteses (ex: dados anonimizados e pseudonimizados)** • **<u>Possível:</u> quando o contexto do incidente indicar a possibilidade de identificação do titular (ex: vazamento de registros atrelados nome e sobrenome de titular, quando ocorrido em cidade com poucos habitantes)** • **<u>Provável:</u> quando o incidente incluir elementos que, por si só, culminem na possibilidade de identificação, direta ou indireta do titular (ex: vazamento de registros com nome e sobrenome do titular, além de documentos de identificação, como CPF e RG).** **<u>Contexto do Incidente de Segurança da Informação</u>** **Análise sobre o incidente de segurança da informação propriamente dito, isto é, tipo de incidente e as circunstâncias do ocorrido.** • **<u>Tipo de incidente</u>: confidencialidade, integridade, disponibilidade;**

	• **Se confidencialidade: acesso por terceiro conhecido; acesso por terceiro desconhecido** • **Se integridade: alteração reversível; alteração irreversível;** • **Se disponibilidade: parcial; total;** • **<u>Motivação</u>: culposo; doloso; desconhecido;** • **Se culposo: falha humana, falha técnica;** • **Se doloso: autoria conhecida; autoria desconhecida** • **<u>Duração do incidente</u>: indicação da linha do tempo entre a ocorrência do incidente e sua identificação, em faixas (< 1 dia, 1 – 5 dias; 5-10 dias; 10-20 dias, desconhecido etc)** **A partir de tais critérios, a ANPD deve atribuir uma 'nota' para cada resposta, isto é, a ANPD deve apontar um valor objetivo para cada resposta, o qual serviria para mensurar a gravidade do incidente com dados pessoais.** **Como exemplo, nos referimos novamente à metodologia da ENISA, que utiliza o seguinte critério:** **"Gravidade = Contexto do Tratamento de Dados x Possibilidade de Identificação do Titular + Contexto do Incidente de Segurança da Informação."** **O resultado da análise, na metodologia da ENISA, é então mensurado da seguinte forma:** **<u>"Gravidade < 2</u>: (Baixa). Os indivíduos não serão afetados ou podem encontrar alguns inconvenientes, que eles vão superar sem nenhum problema (tempo gasto reinserindo informações, aborrecimentos, irritações, etc.)** **<u>2 ≤ Gravidade < 3:</u> (Média). Os indivíduos podem encontrar inconvenientes significativos, que irão ser capazes de superar apesar de algumas dificuldades (custos extras, recusa de acesso aos serviços comerciais, medo, falta de compreensão, estresse, pequenas doenças físicas, etc.).** **<u>3 ≤ Gravidade < 4</u>: (Alta). Os indivíduos podem enfrentar consequências significativas, que devem ser capazes de superar, embora com sérias dificuldades (apropriação indébita de**

	fundos, lista negra de bancos, danos materiais, perda de emprego, intimação, piora da saúde, etc.). **<u>4 ≤ Gravidade:</u> (Muito Alta). Os indivíduos podem enfrentar consequências significativas, ou mesmo irreversíveis, que não podem superar (dificuldades financeiras, como dívidas substanciais ou incapacidade de trabalhar, doenças físicas ou psicológicas de longo prazo, morte, etc."** **Assim, após a aplicação dos referidos critérios, os incidentes classificados como Média a Muito Alta gravidade devem ser comunicados à ANPD e aos titulares de dados pessoais, comunicação esta, especialmente aos titulares, condicionada à gravidade do incidente, isto é, quanto mais grave, mais específica a comunicação.**
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	**Conforme proposto no tópico anterior, após a análise, pelo Controlador, do incidente de segurança da informação, este deve ser classificado em faixas relacionadas à gravidade do ocorrido. A partir desta classificação, medidas diferentes devem ser tomadas pelo Controlador.** **A distinção entre os níveis de gravidade se daria conforme o critério objetivo a ser definido pela ANPD para cada resposta fornecida pelo Controlador dos dados pessoais.** **Assim, por exemplo, se o resultado da análise indica um incidente de gravidade baixa, o Controlador seria dispensado de comunicá-lo à ANPD e aos titulares, tendo como obrigação a manutenção dos registros sobre o incidente, em atenção ao princípio da responsabilização e prestação de contas. (art. 6° X, da LGPD). Todavia, no caso de um incidente considerado como de gravidade muito alta, o Controlador deveria notificar a ANPD, bem como adotar medidas para notificação pessoal dos titulares vitimados.**
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	**O risco é potencial, enquanto o dano é palpável.** **Em outras palavras, o risco ao titular decorre da possibilidade do incidente causar danos ao titular, podendo ser mensurado antes da efetiva ocorrência do dano e, com a adoção de medidas pelo Controlador, mitigado antes da ocorrência do dano. Já o dano, por sua vez, é objetivo, traduzindo-se em afetação material, moral ou física dos titulares. Mesmo o dano**

	moral, que é subjetivo, deve ser demonstrado objetivamente, devendo ser evitada a possibilidade de um dano moral *in re ipsa*, sob pena de insegurança jurídica para os agentes de tratamento de dados pessoais.
O que deve ser considerado na avaliação dos riscos do incidente?	**Tendo em vista que o risco é potencial e essencialmente relacionado à probabilidade de ocorrência de dano, este deve ser analisado em razão da relação entre a gravidade do incidente e as suas possíveis consequências.** **Assim, além da análise sobre a gravidade do incidente, o controlador deveria indicar, também, os possíveis riscos identificados.** **<u>Possíveis consequências</u>** • **roubo de identidade** • **perda financeira significativa pelo indivíduo** • **ameaças à segurança física de um indivíduo** • **perda de negócios ou oportunidades de emprego** • **humilhação, danos à reputação ou relacionamentos** • **intimidação ou marginalização no local de trabalho ou social** • **outro (a ser indicado pelo Controlador)**
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	**Além do que dispõe a LGPD, o Controlador deve enviar, também, a análise de gravidade do incidente, conforme proposto no primeiro tópico deste documento, de modo a comprovar a realização da análise e justificar as medidas que tomou ou pretende tomar em razão do incidente.**
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	**É fundamental que o prazo para notificação sobre incidentes com dados pessoais seja aderente à realidade brasileira, a qual diverge, e muito, daquela experimentada em outras localidades, como nos países do continente europeu.** **Considerando a realidade brasileira, bem como a inexistência de uma cultura de segurança da informação, a fragilidade dos sistemas governamentais sob a ótima da proteção de dados, as enormes diferenças socioeconômicas existentes e a baixa produção tecnológica do país, é fundamental que existam critérios objetivos para determinar o prazo de notificação de incidentes à ANPD. Dentre as medidas necessárias, destacamos algumas:**

	a) **<u>Regras relacionadas ao faturamento do Controlador:</u> Dependendo do faturamento anual do controlador, o prazo para notificação deveria ser endereçado. Assim, organização com faturamento anual de X milhões de reais deveria notificar incidentes no prazo de 10 dias, enquanto organizações com faturamento menor deveriam notificar os incidentes em prazo de 30 dias, por exemplo. Essa definição poderia ser feita por faixas de faturamento, e deve ser condicionada, também, ao tipo de organização (abordado abaixo);** b) **<u>Regras relacionadas ao tipo de organização</u>: algumas organizações, seja em razão das características de seu negócio, seja em razão do tipo ou volume de dados pessoais que tratam, devem ter regras mais rígidas sobre a notificação de incidentes à ANPD. Por exemplo, instituições de saúde, instituições financeiras, bureaus de crédito, bureaus de informação, redes sociais e empresas que tratam dados em larga escala (baseada no número de titulares), em razão do tipo de dados pessoais que lidam e/ou do volume de informações que tratam, devem possuir prazos mais curtos para a notificação, pois eventuais incidentes podem gerar mais riscos;** c) **<u>Possibilidade de notificação complementar</u>: é fundamental que a ANPD disponha sobre a possibilidade de notificação complementar, uma vez que, em muitos casos, todas as informações sobre o incidente e suas possíveis consequências podem demorar até total apuração. Assim, como a LGPD é silente sobre esta possibilidade, a ANPD deve dispor sobre isso expressamente;** d) **<u>Estipulação de período de transição:</u> tendo em vista que a LGPD inova em várias searas, é fundamental que exista um período de transição, com prazos maiores, para a realização da comunicação. Este período de transição, por sua vez, deveria prever fases para o endurecimento da norma, isto é, para diminuição do prazo. (Ex: inicialmente, prazo de 30 dias. Após dois anos, prazo de 15, etc).** **É importante notar que o prazo de "até 72 horas" previsto na legislação europeia (GDPR) não é compatível com a realidade da maior parte dos agentes de tratamento de dados pessoais do Brasil, sendo, portanto, temerária sua aplicação no país, ao menos nesta fase inicial da LGPD. Sugerimos como critério geral, portanto, a adoção do prazo previsto na legislação Australiana, que é de 30 (trinta) dias, a ser contado em dias corridos, sendo aplicada as demais considerações realizadas acima.**

Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	**O prazo para comunicação dos incidentes aos titulares deve seguir a mesma forma estabelecida para a comunicação da ANPD, conforme sugerido no tópico anterior. Em suma, as informações a serem comunicadas devem ser as mesmas fornecidas à ANPD, todavia, o meio para sua comunicação deve ser diferente, especialmente quanto à linguagem empregada, que deve considerar os titulares vitimados pelo incidente. Assim, a comunicação aos titulares deve ser feita em linguagem clara e acessível, em língua portuguesa, e considerando o tipo de titulares afetados. (Ex: se os dados envolvidos no incidentes são de acadêmicos, a linguagem pode ser mais rebuscada; se os dados envolvidos no incidente são de idosos, devem ser utilizadas fontes de tamanho maior e linguagem mais acessível.)**
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	**A comunicação do incidente aos titulares de dados pessoais deve ser realizada de acordo com a gravidade do incidente e os possíveis riscos advindos da ocorrência. Assim, para incidentes classificados como de média gravidade, a comunicação poderia ser geral e pública, enquanto os incidentes de gravidade maior (Alta e Muito Alta) devem demandar, também, a adoção de medidas específicas, como a comunicação direta com os titulares afetados, independentemente do meio. Sobre o meio, quando necessária comunicação direta, o controlador deve ter a prerrogativa de se utilizar dos meios viáveis, com preferência para o meio em que ele geralmente se comunica com o titular. (Ex: se a relação com o titular é travada fisicamente, a comunicação poderia ser realizada pessoalmente ou por meio de carta; quando a interação das partes se dá por meio digital, a comunicação deveria ser realizada também desta forma, como por e-mail.)**
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	**Os incidentes considerados de baixa gravidade, conforme exposto no primeiro tópico deste documento, deveriam dispensam o controlador de informar a ANPD. Porém, deveriam ser registrados internamente, com vistas ao atendimento do princípio da responsabilização e prestação de contas. (art. 6° X, da LGPD).**
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	**Os incidentes considerados de baixa gravidade, conforme exposto no primeiro tópico deste documento, deveriam dispensam o controlador de informar a ANPD. Porém, deveriam ser registrados internamente, com vistas ao atendimento do princípio da responsabilização e prestação de contas. (art. 6° X, da LGPD).**
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	**Os critérios devem ser os mesmos aplicados aos Controladores, uma vez que a obrigação inicial recai sobre eles. Assim, a ANPD deve orientar os agentes de tratamento sobre os critérios da análise,**
Existe alguma metodologia recomendada para a análise de	**Sim. ENISA, Recommendations for a methodology of the assessment of severity of personal data breaches, Dezembro de 2013. Disponível em: https://www.enisa.europa.eu/publications/dbn-severity**

gravidade do incidente de segurança? Se sim, qual(is)?	
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	----------
Referências	**Austrália – OAIC:** https://www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response/part-4-notifiable-data-breach-ndb-scheme/#is-serious-harm-likely **ENISA, Recommendations for a methodology of the assessment of severity of personal data breaches, Dezembro de 2013. Disponível em:** https://www.enisa.europa.eu/publications/dbn-severity **Reino Unido – ICO:** https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach-assessment/; https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/ **Japão - Amended APPI** https://www.dlapiperdataprotection.com/index.html?t=breach-notification&c=JP **Working Party 29, Guidelines on Personal Data Breach Notification under Regulation 2016/679. Agosto de 2018.:** https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

SUGESTÃO DE NORMATIVO, SE HOUVER
Art. Xxxx ....
Art. Xxxx ....

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: ASSOCIAÇÃO DATA PRIVACY BRASIL DE PESQUISA

CPF/CNPJ: 36.942.306/0001-04

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS **IMPORTANTE:** Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	A relevância de um incidente de segurança se dá na medida em que direitos fundamentais dos titulares são ameaçados, não se limitando apenas ao direito à privacidade em outros direitos dos titulares previstos pela LGPD, mas a todos os direitos constitucionalmente garantidos. Recomenda-se que a ANPD tenha uma abordagem baseada em direitos para a avaliação de relevância de incidentes de segurança. Ainda, com a constante evolução tecnológica, torna-se impossível prever todos os possíveis usos ilícitos de dados pessoais que podem colocar os titulares em risco. Sendo assim, é mais recomendável que não exista uma lista fixa de critérios de análise, mas sim diretrizes gerais para orientar a avaliação do risco de acordo com o contexto de cada caso. Possíveis critérios para essa avaliação serão melhor descritos na resposta da pergunta 4. <u>Justificativa:</u> Diferentes incidentes de segurança podem ocasionar diferentes riscos e/ou danos aos titulares de dados. Em razão da massificação das atividades de tratamento de dados, um titular pode ter seus direitos e liberdades fundamentais violados das mais variadas formas por um incidente de segurança. A ideia mais comum que se tem de incidente de segurança é associada ao “vazamento de dados”, ou seja, incidentes de confidencialidade que podem violar a privacidade, a intimidade e a autodeterminação do titular, por exemplo. Nesse caso, deve-se ter claro que, embora a exposição não autorizada de dados sensíveis possa ser ainda mais gravosa, mesmo dados a princípio considerados ‘’triviais’’, e até mesmo dados públicos, podem gerar riscos e danos para os titulares. Exemplo: A exposição de dados simples, como telefone e e-mail de clientes registrados em uma loja virtual pode dar ensejo a fraudes e golpes. Por outro lado, a exposição de dados de nome completo e CPF de pessoas que se identificaram para acessar uma clínica de reabilitação de usuários de drogas gera um risco à privacidade e à intimidade muito grande.

	Contudo, os riscos aos titulares não se limitam aos direitos tradicionalmente associados à privacidade. A indisponibilidade de dados de um paciente de um hospital pode gerar riscos à saúde e à integridade física do titular, por exemplo. Da mesma forma, a quebra de integridade de dados de um sistema de assistência social pode fazer com que pessoas que necessitam de algum benefício não o recebam. Por fim, com a constante evolução tecnológica torna-se impossível prever todos os possíveis usos ilícitos de dados pessoais que podem colocar o titular em risco. Sendo assim, é mais recomendável que não exista uma lista fixa de critérios de análise, mas sim diretrizes gerais para orientar a avaliação do risco de acordo com o contexto de cada caso. **Possíveis critérios para avaliação dos riscos serão melhor descritos na resposta da pergunta 4.** Sendo assim, a relevância de um incidente de segurança se dá na medida em que direitos fundamentais dos titulares são ameaçados, não se limitando apenas ao direito à privacidade, ou direitos dos titulares previstos pela LGPD, mas a todos os direitos constitucionalmente garantidos. Recomenda-se que a ANPD tenha uma abordagem baseada em direitos para avaliação de relevância de incidentes de segurança[1].
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	A categorização de risco e/ou dano em baixo, médio e alto é uma boa medida, tanto para avaliar as medidas que devem ser tomadas pelo agente de tratamento para mitigá-los, quanto para fixação de obrigações. Os níveis de risco devem ser distinguidos a partir dos critérios adotados para relevância do risco e/ou dano (conforme respostas das perguntas 1 e 4). Ainda, o risco e/ou dano baixo devem ser considerados como **não relevantes**, visto que não há que se falar em inexistência de risco. Ressalta-se, contudo, que mesmo com a adoção de critérios mais objetivos, a avaliação do risco é sempre casuística, independentemente da(s) categoria(s) em que a ocorrência esteja inserida, visto que as particularidades de cada caso podem se mostrar determinantes. <u>Justificativa:</u> Um risco e/ou dano baixo deve ser fixado de forma a **não** ser relevante. Isso porque toda atividade de tratamento de dados envolve algum grau de risco, bem como qualquer efeito adverso à confidencialidade, integridade e disponibilidade de uma base de dados. Sendo assim, não há de se falar em risco e/ou dano **nulo ou inexistente**.

[1] GELLERT, Raphaël. We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences Between the Rights-Based and the Risk-Based Approaches to Data Protection. In **European Data Protection Law Review (EDPL)**. 4/2016, Vol. 2, p. 481-492.

	Portanto, recomenda-se que riscos e/ou danos sejam considerados baixos à medida em que não causem grandes impactos adversos para direitos e liberdades do titular, representando mero incômodo. Nesse sentido, os critérios elencados na resposta da **pergunta 4** podem servir como um parâmetro para a definição do grau de risco e/ou dano. Ademais, o grau de risco pode variar também ao longo do tempo, tendo-se em vista as inovações tecnológicas e o estado da arte das medidas de segurança e mitigação de riscos disponíveis no mercado, bem como as tecnologias usadas por invasores para criar novos usos para dados extraídos ilegalmente. Um exemplo é o roubo ou perda de um computador de uma agência de publicidade com planilhas com dados detalhados de um grande número de titulares de dados, incluindo dados sensíveis. Caso esse computador não possua nenhum mecanismo de segurança, como senha, criptografia e/ou exigência de credenciais de acesso para a planilha, o risco aos titulares seria alto. Por outro lado, na hipótese de existência de mecanismos de segurança robustos, e sem nenhum indício de que houve um roubo arquitetado com o objetivo de extração de dados, os riscos aos titulares seriam baixos.
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	De forma geral, a principal diferença entre um risco e um dano, no campo da proteção de dados, é a **materialização de alguma violação aos direitos fundamentais**. Um risco representa um potencial de violações, enquanto um dano sugere uma violação em concreto. Contudo, deve-se também ter em mente que a tutela da proteção de dados opera na lógica da inviolabilidade, e em decorrência do princípio da autodeterminação informativa, a mera perda do controle das informações pessoais pode representar um dano na esfera moral. A distinção entre dano e risco, para o objeto em questão, possui um principal fator de relevância: a calibração das obrigações decorrentes de um incidente de segurança. Nota-se que o risco já é suficiente para deflagrar o dever de notificação. Ainda, quanto maior o grau desse risco, maiores os deveres, não só de notificação, mas também de adoção de medidas de mitigação. Justificativa: Um incidente de segurança pode causar uma série de danos extrapatrimoniais, diante da sensação, por exemplo, de insegurança e receio em face da potencial divulgação indevida dos dados em questão. Em especial no caso de um vazamento de dados sensíveis, o incidente pode constituir também uma violação direta da privacidade e intimidade dos titulares[2]. Já os danos patrimoniais podem acontecer quando terceiros mal-

[2] GOULART, Guilherme Damasio; MENKE, Fabiano. **Segurança da Informação e Vazamento de Dados.** In: BIONI, Bruno et al (org.). Tratado de proteção de dados pessoais. São Paulo: Forense, 2021. Cap. 17. p. 628-666.

	intencionados utilizam os dados para cometimento das mais variadas fraudes, no que se costuma chamar de *identity theft.* De forma geral, a principal diferença entre um risco e um dano, no campo da proteção de dados, é a materialização de alguma violação aos direitos fundamentais. Um risco representa um potencial de violações, enquanto um dano uma violação em concreto. Contudo, a proteção de dados apresenta duas particularidades: 1. Ela opera na lógica da inviolabilidade[3], de forma que uma vez ocorrido o dano, é impossível o retorno ao *status quo ante*. 2. A mera perda de controle de informações pessoais pode representar, por si só, um dano moral, à medida que a autodeterminação informativa do titular é afetada. O efetivo roubo de identidade, por exemplo, representa uma concretização material do dano. Contudo, a impossibilidade de exercer controle sobre as informações pessoais também gera, por si só, um dano, ainda que de outra natureza. A distinção entre dano e risco, para o objeto em questão, possui um principal fator de relevância: a calibração das obrigações decorrentes de um incidente de segurança. Nota-se, em primeiro lugar, que o risco já é suficiente para deflagrar o dever de notificação. Ainda, quanto maior o grau desse risco, maiores os deveres, não só de notificação, mas também de adoção de medidas de mitigação. Por outro lado, a configuração de um dano pode ensejar obrigações também na esfera de reparação, não só a título indenizatório dos titulares, mas também no sentido de mitigar a permanência ou agravamento do dano. A título de exemplo, cita-se o caso estadunidense Equifax, em que a Federal Trade Comission (FTC), ao constatar o dano a milhões de titulares, fixou obrigações ainda mais severas, não só de indenização, mas também determinando que a Equifax constituísse um fundo provisório a título cautelar, oferecesse gratuitamente aos titulares afetados um serviço de monitoramento de uso de seus dados [*free credit monitoring]* e serviços gratuitos de restauração de identidade [*Free Identity Restoration Services*] para casos de fraude e roubo de identidade[4]. Portanto, em uma lógica de regulação assimétrica, se o incidente de segurança chega a apresentar não só um risco, mas um risco e/ou dano, as obrigações de notificação e reparação se tornam ainda mais relevantes. Isso

[3] BRASIL. Supremo Tribunal Federal. *Medida Cautelar na Ação Direta 6.387/DF*. Medida cautelar contra o inteiro teor da Medida Provisória n. 954, de 17 de abril de 2020, que dispõe sobre "o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020". Requerente: Conselho Federal da Ordem dos Advogados do Brasil –CFOAB. Relatora: Min. Rosa Weber, 24 de abril de 2020. Disponível em: <http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI6387MC.pdf >.

[4] FEDERAL TRADE COMMISSION. Equifax Data Breach Settlement: What You Should Know. 2019. Disponível em: <https://www.consumer.ftc.gov/blog/2019/07/equifax-data-breach-settlement-what-you-should-know>

	não significa, contudo, que o risco não possa, por si só, ser relevante a ponto de desencadear tais obrigações, conforme aprofundado adiante.
O que deve ser considerado na avaliação dos riscos do incidente?	Apresenta-se aqui uma lista de critérios que podem ser considerados na avaliação dos riscos e/ou danos do incidente, para determinar a relevância desse incidente e, seguindo a lógica que vem sendo argumentada até aqui, determinar quais obrigações seriam deflagradas. Em uma lista não exaustiva, sugere-se os seguintes critérios de avaliação: Volume de dados pessoais; Número de titulares possivelmente afetados; Natureza dos dados pessoais; Perfil dos titulares dos dados; Existência de dados pessoais sensíveis; Natureza da atividade do controlador; O que levou ao incidente de segurança; Motivação do incidente de segurança; Possibilidade de identificação dos titulares; Consequências para os titulares da indisponibilidade ou quebra de integridade dos dados; Possibilidade de reversão do risco e/ou dano ocasionado; Possibilidade de agregação dos dados para extrair inferências ou traçar perfil comportamental do titular e, por fim, se a base de dados em questão foi psedounonimizada. <u>Justificativa:</u> Com a massificação do uso de dados para diversas finalidades, a própria atividade de tratamento já é capaz de impactar a vida e desenvolvimento da livre personalidade do indivíduo[5]. No entanto, cabe uma análise pormenorizada a partir de cada incidente de segurança, de modo que os diferentes efeitos adversos sobre os indivíduos sejam levados em consideração. Nesse sentido, os possíveis riscos e danos podem ser classificados em resultados físicos, materiais e imateriais[6]. Alguns exemplos podem ser roubo de identidade e fraudes diversas, envolvendo, inclusive, perdas financeiras, mas também danos à imagem, reputação pessoal e profissional, entre outros. Ressalta-se que violação à privacidade e à autodeterminação informativa não são meramente abstratas, mas possuem consequências reais nas vidas dos titulares, tanto de ordem emocional quanto material. Isso se torna especialmente mais grave no caso de grupos já vulnerabilizados, ou em situações em que havia uma relação de maior confiança entre o titular e o controlador de dados. Nesse sentido, os critérios para avaliação dos riscos do incidente devem partir do seguintes elementos: • Volume de dados pessoais,

[5] BIONI, Bruno Ricardo. Proteção de Dados Pessoais: a função e os limites do consentimento. Rio de Janeiro: Gen Forense, 2019

[6] ARTICLE 29 DATA PROTECTION WORKING PARTY. Guidelines on Personal data breach notification under Regulation 2016/679. 2017. Disponível em: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052>

	• Número de titulares possivelmente afetados.
	
	• Natureza dos dados pessoais
	  ○ Observação: Ressalta-se que a quebra de confidencialidade de dados públicos, publicamente acessíveis ou tornados manifestamente públicos pelo titular não representa, necessariamente, um menor risco e/ou dano, especialmente se houver cruzamento e/ou combinação desses dados com outros dados que não sejam publicamente acessíveis.
	
	• Perfil dos titulares dos dados
	  ○ Ex: Titulares em situações de maior vulnerabilidade, como crianças, idosos, pessoas com deficiência podem ser desproporcionalmente afetadas por um incidente de segurança.
	
	• Existência de dados pessoais sensíveis
	
	• Natureza da atividade do controlador
	  ○ Ex: Uma indisponibilidade dos dados de um hospital é muito mais grave do que uma indisponibilidade de dados em um site de comércio eletrônico.
	
	• O que levou ao incidente de segurança.
	  ○ Ex: Em um ataque *ransomware* em que há uma ameaça por parte dos invasores de violação dos direitos dos titulares pode apresentar um risco muito maior para os titulares de usos futuros desses dados do que uma deleção acidental dos arquivos.
	
	• Motivação do incidente de segurança
	  ○ Ex: Um incidente de segurança com motivações políticas, que quebra a confidencialidade de dados de ativistas, pode colocar esses titulares em posição ainda mais vulnerável, elevando o grau do risco.
	
	• Possibilidade de identificação dos titulares

<table>
<tr><td></td><td>

Consequências para os titulares da indisponibilidade ou quebra de integridade dos dados.
Possibilidade de reversão do risco e/ou dano ocasionado

Ex: A quebra de confidencialidade de dados como nome, CPF, impressão digital não pode ser reparada. Por outro lado, dados que podem ser alterados, como um login, ou dados pseudonimizados são passíveis de reparação.

Possibilidade de agregação dos dados para extrair inferências ou traçar perfil comportamental do titular.
Se a base de dados foi psedounimizada[7].

</td></tr>
<tr><td>Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?</td><td>
<table>
<tr><td>Critério: o tipo de incidente</td></tr>
<tr><td>Informações que devem ser prestadas:

• tipo do incidente de segurança, conforme divisão tripartite (confidencialidade, integridade, disponibilidade)
• descrição geral do incidente de segurança (ex: caso de hacking, malware, vazamento, etc)
• tipo de incidente de tratamento inadequado (tratamento em desconformidade com a LGPD, mas que não viole algum dos pilares da segurança da informação)</td></tr>
<tr><td>Critério: natureza, sensibilidade e volume dos dados pessoais</td></tr>
</table>
</td></tr>
</table>

[7] O artigo 32 (1) a da GDPR traz a pseudonimização e encriptação como medidas de segurança adequadas.

	• natureza dos dados (tipos de dados pessoais alvos do incidente, tais como dados cadastrais, identificadores únicos, dados financeiros, dados de geolocalização, etc) - art. 48, §1º, I da LGPD; • sensibilidade dos dados (no caso de haver dados sensíveis, conforme definição da lei, envolvidos no incidente, descrição em destaque) ○ caso não haja dados sensíveis, criticidade dos tipos de dados, como aqueles protegidos por algum tipo de sigilo regulatório (lei do sigilo bancário) ou que tenha alguma classificação de restrição de circulação (segredo, sigiloso, circulação interna, público) • volume estimado de dados afetados pelo incidente; • volume estimado de indivíduos afetados pelo incidente.	
	Critério: características dos titulares	

	• as informações sobre os titulares envolvidos (art. 48, §1º, I)
	  ○ tipos de titulares atingidos (clientes, pacientes, usuários, assinantes, estudantes, trabalhadores etc)
	  ○ relação dos titulares impactados com o agente, caso haja (clientes, pacientes, usuários, assinantes, estudantes, trabalhadores etc);
	  ○ presença de titulares impactados que são crianças ou adolescentes e estimativa de volume de indivíduos com essa característica afetados.	

	Critério: severidade das consequências para os indivíduos	

	• os riscos relacionados ao incidente (art. 48, §1º, IV)
	  ○ síntese da conclusão da avaliação de risco realizada previamente pelo agente, com destaque para principais pontos de atenção;
	  ○ tempo estimado em que os dados pessoais estiveram comprometidos;	

	Outras informações	
	• a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; (art. 48, §1º, III); • as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo (art. 48, §1º, VI); • dados do controlador (nome, informações de contato, identificação do encarregado ou ponto de contato designado); • indicação de caráter transfronteiriço do incidente.	

	• os motivos da demora, no caso de a comunicação não ter sido imediata (art. 48, §1º, V). • intenção de complementar posteriormente a notificação original, com indicação prévia de quais informações podem estar incompletas ou imprecisas. Justificativa: Ao adentrar no ‘’como’’ das notificações e comunicações relativas a incidentes de segurança que envolvam dados pessoais, é importante resgatar o próprio objetivo de se notificar a Autoridade competente e/ou comunicar os titulares acerca do ocorrido. O que se almeja com isso? A LGPD é, conhecidamente, uma norma que consagra, junto ao princípio da segurança (Art. 6º, VII), também o da prevenção (Art. 6º, VIII). Para além dos princípios, todo o desenho da norma aponta para a busca de um equilíbrio entre, de um lado, a razoabilidade na implantação de medidas (técnicas e administrativas) preventivas, isto é, que evitem a concretização de incidentes de segurança, e a mobilização para contenção de incidentes e mitigação de danos diante da sua ocorrência. Se é verdade que a lógica por trás de normas horizontais de proteção de dados é proteger os titulares contra quaisquer usos inadequados de seus dados pessoais, visando evitar os danos de diversas naturezas que eles podem causar, também é verdade que parte substancial dessas normas, e das obrigações que elas geram, dedica-se justamente a lidar com a quase inevitabilidade dos incidentes. Partindo desse ponto, destaca-se, mais uma vez, a lógica de corregulação e *accountability* (princípio denominado ‘’responsabilização e prestação de contas’’ na LGPD) que permeia a LGPD: no caso de incidentes de segurança e do dever de notificação, por exemplo, é responsabilidade dos agentes de tratamento adotar medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais. Isso se desdobra na previsão de que a dosimetria das sanções administrativas da lei levará em consideração “adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados” (Art. 52, § 1.º, VIII). Cabe ao agente, melhor posicionado nesse ecossistema, tanto a adoção de medidas preventivas, quanto a avaliação inicial do risco gerado por um eventual incidente e dos danos que podem recair sobre os titulares. Tal análise é que deflagra, ou não, o dever de notificação. Por outro lado e de forma complementar, cabe à Autoridade Nacional de Proteção de Dados (ANPD) a tarefa de conduzir a sua própria investigação, além de possivelmente determinar medidas específicas que o agente deve tomar para responder ao ocorrido. Um dos objetivos desta notificação (assim como o da própria comunicação ao titular) é o de limitar os danos decorrentes do incidente. Diante desse quadro, uma forma de sistematizar **quais** informações devem constar em uma notificação à Autoridade competente é partir do conjunto de informações reunido pelo próprio agente de tratamento de dados ao avaliar a gravidade/risco do incidente. Salvo poucas exceções, as informações que alimentaram a análise inicial do agente serão imprescindíveis ao trabalho da Autoridade, seja para identificar eventuais

	falhas no plano de resposta desenvolvido e determinar medidas adicionais, seja no curso geral da investigação por ela conduzida. Assim, os critérios gerais levados em consideração para a determinação do dever de notificar podem ser o ponto de partida, do qual são extraídas as categorias específicas de informações que devem ser fornecidas. Algumas dessas informações já são exigidas pela própria LGPD, no seu art. 48, mas há outras que não foram descritas pelo legislador, conforme tabela explicativa acima. Descritas as categorias de informação que devem ser fornecidas à Autoridade por meio de notificação, cabe ressaltar a possibilidade, consagrada no Regulamento europeu, de ‘’faseamento’’ da notificação, isto é, o fornecimento, em um primeiro momento (vide resposta seguinte) das informações disponíveis a partir da análise de risco que deflagrou o dever de notificação e, constatada a incompletude das informações, ou descobertas outras informações no curso da investigação interna, a possibilidade de complementação da notificação, sempre com o objetivo de munir a Autoridade do máximo de subsídios para atuar diante do incidente. Isso decorre da noção de que a indisponibilidade, em um determinado momento, de informações precisas ou completas sobre um incidente não deve ser um obstáculo para a pronta notificação. A intenção de complementar a notificação com informações adicionais também deve ser objeto da notificação original.
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	Os fatores que devem ser considerados na definição de um prazo razoável são, principalmente, os seguintes: por um lado, um dos objetivos primordiais da notificação é robustecer as medidas de contenção e mitigação dos danos gerados pelo incidente, de forma que a celeridade é um aspecto central; por outro, apenas incidentes que imponham ‘’risco ou dano relevante’’ geram o dever de notificar, o que pressupõe a existência de um período de avaliação interna do ocorrido e reunião de informações que darão suporte à própria notificação. A combinação entre os fatores - celeridade como regra e tempo razoável para identificação do nível de risco e dano - sugerem que a abordagem adotada pela GDPR **(72 horas a partir do conhecimento do incidente)** pode ser um ponto de partida interessante. Nesse ponto, importante ressaltar que a referência ao Decreto nº 9.936, de 2019, que regulamenta a Lei do Cadastro Positivo e prevê um prazo de dois dias úteis para notificação à ANPD, embora seja válida por se tratar da única previsão em lei atual sobre a matéria, não deve ser a base da regulamentação pretendida. <u>Justificativa:</u> Observando legislações de outros países que tratam do dever de notificar incidentes de segurança envolvendo dados pessoais, percebe-se que o prazo para a notificação inicial varia de 24 a 72 horas, a partir do conhecimento do agente responsável pela notificação acerca da existência de um incidente. Há também normas que optam por comandos abertos, como ‘’imediatamente’’, ou ‘’em tempo razoável’’, como é o caso da LGPD. Os fatores que devem ser considerados na definição de um prazo razoável são, principalmente, os seguintes: por um lado, um dos objetivos primordiais da notificação é robustecer as medidas de contenção e

	mitigação dos danos gerados pelo incidente, de forma que a celeridade é um aspecto central; por outro, apenas incidentes que imponham ‘’risco ou dano relevante’’ geram o dever de notificar, o que pressupõe a existência de um período de avaliação interna do ocorrido e reunião de informações que darão suporte à própria notificação. Por último, conforme mencionado anteriormente, a eventual incompletude ou imprecisão de certas informações não é óbice para a pronta notificação, na medida em que ela pode ser posteriormente complementada. Dessa forma, o controlador não pode se eximir de notificar o ocorrido sob a justificativa de aguardar a finalização de uma perícia ou outro processo técnico excessivamente prolongado. A combinação entre os fatores - celeridade como regra e tempo razoável para identificação do nível de risco e dano - sugerem que a abordagem adotada pela GDPR (72 horas a partir do conhecimento do incidente) pode ser um ponto de partida interessante. Nesse ponto, importante ressaltar que a referência ao Decreto nº 9.936, de 2019, que regulamenta a Lei do Cadastro Positivo e prevê um prazo de dois dias úteis para notificação à ANPD, embora seja válida por se tratar da única previsão em lei atual sobre a matéria, não deve ser a base da regulamentação pretendida. Não foi possível identificar outras legislações, ao redor do mundo, que considerem se tratar de dia útil ou não um fator na delimitação do prazo de notificação. Justamente em razão do potencial gravoso de incidentes de segurança que envolvam dados pessoais, é preferível que o prazo estabelecido se dê em dias corridos, ou até mesmo em horas, a fim de se evitar prolongamentos desnecessários. Por se tratar de situação excepcional, não há justificativa razoável para o condicionamento do prazo a esse fator específico. Por fim, discorre-se brevemente sobre o elemento ‘’a partir do conhecimento do incidente’’, ponto de partida para a contagem do prazo para notificação à Autoridade. Diante de previsão semelhante no Regulamento europeu, o antigo Working Party 29 debruçou-se sobre o tema e sugeriu a combinação de dois fatores sobre essa definição: a certeza razoável sobre a ocorrência de um incidente de segurança + a certeza razoável de que tal incidente envolveu o comprometimento, seja qual for o tipo, de dados pessoais. Veja-se, não se trata de ciência sobre os detalhes do incidente, nem mesmo sobre o volume estimado de indivíduos afetados, ou categorias específicas de dados comprometidos. Basta que o controlador tenha uma certeza, baseada em indícios razoáveis, de que um incidente de qualquer natureza ocorreu e que esse incidente envolveu dados pessoais em sua custódia, que é considerado o ‘’conhecimento do incidente’’. O fator existência de dados pessoais envolvidos é relevante, na medida em que pode ser que haja o alerta muito rápido sobre um incidente, sem que haja certeza razoável, em um momento inicial, de que dados pessoais (e não outros dados, por exemplo) foram comprometidos. Acerca disso, dois pontos conclusivos: a identificação da existência de um incidente, bem como a análise do risco envolvido e potenciais danos (ambos fatores essenciais tanto para a deflagração do dever de notificar quanto da possibilidade de fazê-lo no prazo adequado) estão diretamente relacionadas a obrigações

	estabelecidas na LGPD, como a instalação de medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais (art. 48) ou os próprios deveres relacionados à governança de dados. Isso evidencia a relação próxima entre os princípios da segurança e da prevenção. Ademais, seja quando se fala de prazo máximo para a primeira notificação, ou mesmo para a determinação do momento em que o agente tem conhecimento do incidente, o mote sempre deve ser de máxima prontidão na tomada de medidas necessárias para o controle do incidente e mitigação dos danos, desde a primeira investigação sobre uma suspeita. Em suma, entendemos que o prazo de 72 horas contados a partir do momento que o controlador toma conhecimento do incidente de segurança que envolve dados pessoais é razoável para atingir os objetivos de proteção da notificação.
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	Em um cenário de incidente tal qual descrito no caput do art. 48 da LGPD, ou seja, aquele que possa acarretar risco ou dano relevante aos titulares, entendemos que a comunicação ao titular deve ocorrer assim que do conhecimento do controlador acerca das circunstâncias de risco em questão e do não cabimento de nenhuma das hipóteses de exceção delineadas nas respostas anteriores, já que se parte do pressuposto de que nem todo incidente necessariamente será reportado aos titulares. Nesse sentido, o próprio processo de avaliação de riscos aos titulares, ao indicar que este é considerável, serve enquanto critério para se chegar à conclusão preliminar de que um incidente deve ser notificado ou, no caso, comunicado aos titulares. Ademais, o processo já pressupõe a reunião de informações mínimas que permitem ao titular tomar medidas protetivas e mitigatórias do risco ou dano. Diante disso, a comunicação deverá se dar imediatamente a partir da constatação do referido dever. Entendemos, entretanto, que a comunicação ao titular difere da notificação à Autoridade na medida em que há algumas circunstâncias em que as **próprias medidas tomadas pelo controlador, por exemplo, afastarão o dever de comunicação**. Dessa forma, o dever de comunicação ao titular deve se dar de forma independente do prazo máximo estipulado em relação à notificação da Autoridade, na medida em que há um elemento adicional de análise - a verificação de alguma hipótese de desobrigação da comunicação, inclusive pela adoção de medidas mitigatórias. **A regra, em todos os casos, deve ser que, constatado o dever geral de notificar e afastadas tais hipóteses, a comunicação seja imediata.** <u>Justificativa</u> Diferentemente da LGPD, a GDPR faz uma diferenciação expressa entre o que seria a obrigação de notificação à Autoridade e a obrigação de comunicação do titular dos dados nos casos de incidentes de segurança. Em relação à Autoridade, a GDPR estipula que a notificação deve ocorrer quando o incidente puder gerar riscos aos direitos e liberdades dos titulares, enquanto a comunicação aos titulares é mandatória apenas quando este risco for elevado.

	No caso da Autoridade, a normativa europeia estabelece o prazo de notificação de até 72h após o controlador ter realizado investigação sobre o incidente que o permita concluir que ele representa um risco aos direitos e liberdades individuais. Entretanto, não há previsões temporais específicas quanto ao prazo para a hipótese de comunicação do titular, a única determinação é de que esta deverá ser realizada assim que o controlador tiver conhecimento da situação de alto risco[8]. Considerando que a situação descrita no caput do art. 48º da LGPD descreve um "risco ou dano relevante", o cenário aproxima-se daquele inscrito na previsão do art. 34 da GDPR. É nesse mesmo sentido que entendemos que, via de regra, no caso de incidentes de segurança, deverá haver a notificação do titular, a não ser quando: (i) o risco e/ou dano ao titular for baixo; ou (ii) quando as medidas de segurança técnicas e organizacionais tornaram o incidente irrelevante para os titulares; ou (iii) quando, após o incidente, as medidas de mitigação garantam que o risco e/ou dano aos titulares não é mais provável de se concretizar; ou (iv) quando a comunicação aos titulares individualmente envolver um esforço desproporcional. Por isso, a notificação do titular, se não desproporcional, cabe sempre que houver uma circunstância de maior risco (não baixo) que não tenha sido dirimida por medidas do controlador. A caracterização da comunicação sem demora será entendida a partir da avaliação de oportunidade do controlador, em que serão consideradas a natureza e gravidade da violação em si, bem como do nível de risco para os titulares. O Considerando 86, por exemplo, aponta como a avaliação da oportunidade da comunicação deverá ser considerada diferentemente em determinados casos. Quando, por exemplo, o controlador tiver conhecimento da necessidade de mitigar um risco imediato, é necessária a comunicação de pronto. Por outro lado, a comunicação a respeito da necessidade do controlador implementar medidas contra a continuidade da violação ou prevenção de ocorrências semelhantes podem justificar mais tempo para envio. Ainda sobre circunstância que justifiquem a não imediata comunicação do titular, o Considerando 88, do mesmo modo que o art. 3, (5) do regulamento da Comissão Europeia n. 611/2013, indica que a comunicação ao titular dos dados pode ser atrasada por uma autoridade para preservar a integridade de uma investigação sobre as circunstâncias da violação. Algo importante a ser considerado na avaliação da razoabilidade do tempo de comunicação do titular é a diferença entre os objetivos desta e da notificação à Autoridade. No caso da comunicação do titular, a finalidade é de alerta e está relacionada ao fornecimento de informações específicas sobre as etapas que estes devem

[8] EUROPEAN DATA PROTECTION BOARD. **Guidelines 01/2021 on Exemples regarding Data Breach Notification**. Jan, 2021, p. 06. Ver também: CENTRE FOR INFORMATION POLICY LEADERSHIP. **Comments by the Centre for Information Policy Leadership On the Article 29 Working Party's"Guidelines on personal data breach notification under Regulation 2016/679"**. Dec. 2017, p. 11-15.

	seguir para se proteger e, caso necessário, buscar mais informações[9]. Como observado, dependendo da natureza da violação e do risco apresentado, a comunicação oportuna ajudará os indivíduos a tomar medidas para se proteger de consequências danosas da violação. Considerando que um dos objetivos da comunicação é fornecer informações para que o titular possa se proteger e, também, que os aspectos de um processo de investigação podem ser mais morosos que outros, a comunicação não necessariamente deve ser feita de uma só vez, podendo, se adequado, ser dividida em momentos distintos[10]. Se uma parte da investigação é concluída e o controlador percebe que há a necessidade de comunicação do titular, ele deverá fazê-la imediatamente, fornecendo ao indivíduo as orientações possíveis para mitigação do risco ou dano. Conforme novas partes da investigações forem sendo concluídas, novos comunicados, quando cabíveis, devem ser enviados. Partindo dessa perspectiva, entendemos que mais adequado que colacionar o prazo de comunicação do titular ao prazo de notificação da Autoridade, ou mesmo que afixar um prazo diferente para a comunicação, seria determinar de que ela ocorra logo que o controlador tenha conhecimento (ou informações suficientes para tanto) de que o incidente representa riscos relevantes aos titulares e que também tenha avaliado a inexistência de alguma hipótese de afastamento do dever de comunicação. Nesse sentido, caberá a Autoridade fazer uma avaliação de oportunidade sobre o período da comunicação e sobre a existência de eventuais justificativas para atrasos. *Que informações devem constar dessa comunicação?* Entendemos que as informações mínimas referentes à comunicação do titular devem ser: • A descrição da natureza dos dados pessoais afetados (§1º, I, art. 48 da LGPD) • A indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; (§1º, III, art. 48 da LGPD) • Os riscos relacionados ao incidente; (§1º, IV, art. 48 da LGPD) • Os motivos da demora, no caso de a comunicação não ter sido imediata; (§1º, V, art. 48 da LGPD) • As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo. (§1º, VI, art. 48 da LGPD) • Uma descrição da natureza da violação • Informações de contato do responsável pela proteção dos dados e também qual o melhor canal de comunicação para dirimir dúvidas (SAC).

[9] SOMBRA, Thiago Luís e CASTELLANO, Ana Carolina. **Plano de Resposta a Incidentes de Segurança: reagindo rápido e de forma efetiva**. Revista do Advogado. AASP, 2019 v. 39 n. 144 nov, p. 168-173.
[10] Commission Regulation (EU) N. 611/2013, (7).

	• Possíveis medidas a serem tomadas pelo titular para mitigar riscos, danos e efeitos adversos (como alterar a sua senha). • A data estimada do incidente. Entendemos, também, que a comunicação do titular deverá tratar exclusivamente do incidente, não podendo incorporar informes de assuntos distintos. Além disso, ressaltamos que a comunicação, nos termos da LGPD, não exime o controlador de cumprir com eventuais previsões de comunicação referentes a outras normativas setoriais eventualmente aplicáveis. <u>Justificativa</u> Por não diferenciar as hipóteses de notificação da Autoridade e de comunicação do titular, o conteúdo prescrito como mínimo dos informes em ambos os casos é a princípio o mesmo. Apesar de as indicações sobre informações mínimas necessárias aparecem de forma conjunta no texto da Lei, entendemos que, assim como em relação ao prazo de comunicação, deve-se considerar as particularidades acerca de seus objetivos, inclusive no tipo de linguagem utilizada. Com base em normativas europeias, e observando as particularidades da comunicação ao titular dos dados, entendemos que para além dos pontos já exigidos pelo §1º do art. 48, ainda é importante que a comunicação ao titular contenha: (i) Uma descrição da natureza da violação (eg. se foi um vazamento, uma encriptação, etc) (ii) Informações de contato do responsável pela proteção dos dados e um canal ativo de comunicação (iii) Possíveis medidas a serem tomadas pelo titular para mitigar riscos, danos e efeitos adversos. (iv) A data estimada do incidente Sobre o tópico (iii), é importante observar que as medidas de mitigação de riscos e danos irão variar de acordo com o caso concreto, de modo que não há como predeterminar uma lista de quais medidas a comunicação deve conter. Alguns exemplos nesse sentido, a depender do caso concreto, seriam: a redefinição de senha, aconselhamento de uso de senhas exclusivas, cuidado com e-mails de phishing ou atividades fraudulentas em suas contas, atualização de sistemas, criptografia de dados[11]. Do mesmo modo que alguns requisitos mínimos específicos poderiam ser acrescidos à hipótese de comunicação do titular, ao que parece, nem tudo o que está previsto nos incisos do art. 48º parecem enquadrar-se ao caso da comunicação. O inciso II, que prevê “as informações sobre os titulares envolvidos”, não parece

[11] INFORMATION COMMISSIONER'S OFFICE. **Personal data breaches**. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/personal-data-breaches/

	que deve ser lido da mesma forma para a Autoridade e para o titular dos dados. Este último não necessariamente precisa das informações de outros envolvidos. Assim, por mais que seja um requisito mínimo da notificação à ANPD, em relação à comunicação, a previsão do inciso II será adequada apenas em determinadas situações concretas. Além disso, cabe ressaltar que é importante que a notificação seja realizada de maneira transparente e não deve ser enviada com outras informações, tais como atualizações, boletins informativos ou mensagens-padrão. Esse ponto é descrito de maneira expressa no art. 3(4) do Regulamento da Comissão Europeia n. 611/2013, e é relevante para que de fato o titular dos dados tenha acesso claro ao ocorrido, podendo assim tomar medidas necessárias. Por fim, destacamos que a comunicação do usuário nos termos da LGPD não exime o controlador de cumprir com requisitos advindos de eventuais regulações setoriais a que estão submetidos, o que vale tanto para o caso de notificação da autoridade, como em relação à comunicação do titular dos dados.
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	Embora não faça parte dos direitos do titular dos dados em sentido estrito, o direito a ser informado sobre a ocorrência de incidentes de segurança e suas possíveis consequências também constitui um direito do titular dos dados em um sentido mais amplo, decorrendo do princípio da transparência e *accountability*, além das obrigações específicas de notificação previstas no artigo 48. A comunicação de incidentes aos titulares tem como objetivo orientar e proteger o titular dos eventuais riscos e danos decorrentes do incidente de segurança, devendo acontecer com celeridade e buscando trazer transparência e orientações objetivas para que o titular possa se defender de possíveis ameaças e usos inadequados dos seus dados. Com esse raciocínio podemos extrair algumas diretrizes sobre a forma mais adequada de comunicação aos titulares, como (i) a comunicação ao titular deve ser transparente, em linguagem acessível, objetiva e conter todas as informações exigidas por lei e sugeridas na presente contribuição; (ii) a comunicação direta é a regra (e-mail, telefonema, mensagem ou outro meio de contato direto efetivo); (iii) a comunicação pública por nota à imprensa, sites, banners, comunicados, boletins, não exclui a necessidade de realização de comunicação direta na ampla maioria dos casos; (iv) além da comunicação direta é recomendável a criação de outros meios de contato aos titulares, como sites, boletins informativos, comunicados à imprensa, páginas de perguntas e respostas etc. (v) em casos em que a comunicação individual demandar ‘’esforços desproporcionais’’, mencionados abaixo, ela poderá ser substituída pela comunicação pública. Justificativa Ao comunicar o titular busca-se possibilitar que ele tome as medidas que julgar necessárias e cabíveis para se proteger dos riscos e danos de um incidente. Assim, a comunicação ao titular deve conter informações claras e suficientes para que o titular dos dados tome medidas para resguardar seus direitos. Como tratado na

	pergunta (1) a proteção não se restringe a medidas preventivas, como a troca de credenciais e senhas, mas também medidas afirmativas de exercício de direitos, seja em sede judicial, administrativa ou extrajudicial. A comunicação tem como objetivo fornecer informações específicas aos titulares dos dados sobre as etapas que eles devem realizar para se proteger, desde ações mais simples como, por exemplo, alteração de senhas, ou ações mais complexas que requeiram, por exemplo, o fornecimento de um serviço de monitoramento de fraudes. A comunicação, assim, deve ser feita em uma mensagem específica, com linguagem clara e simples. A comunicação direta deve ser a regra, a partir da deflagração do dever de comunicar, na medida em que ela aumenta a possibilidade de que o titular efetivamente acesse e compreenda as informações sobre o incidente. Por outro lado, se essa comunicação ocorrer apenas por veículo público, ainda que de ampla circulação, torna-se difusa e reduz a chance de que os titulares impactados recebam e compreendam as informações sobre o incidente. Além do mais, em um contexto de aumento exponencial de incidentes de segurança, não é justo atribuir ao titular, parte vulnerável na relação, a responsabilidade de se atentar a todos os incidentes de segurança que acontecem e buscar saber se seus dados foram ou não comprometidos. Se a organização era responsável pelo tratamento seguro dos dados pessoais e não evitou a ocorrência de um incidente, nada mais justo comunicar ao titular, diretamente, acerca do ocorrido e suas potenciais consequências. Nesse contexto, a comunicação pública pode, em certos casos, complementar a comunicação individual, mas, em regra, não deve substituí-la. Para a organização, a comunicação direta também pode ser importante por diversos motivos, como (i) a comunicação direta possibilita que a organização dialogue e seja transparente com os principais interessados em ter informações sobre o incidente - os titulares dos dados (ii) a confirmação pode servir como forma da organização demonstrar, em uma eventual investigação, que o titular recebeu as informações de forma adequada (iv) quando o incidente for parcial, a comunicação direta possibilita que a organização dialogue apenas com os titulares afetados, não criando alarde desnecessário. Assim, a obrigação de comunicação aos titulares tem um efeito positivo para as organizações que tratam dados pessoais, moldando-se a políticas internas que incentivam a implementação de modelos de gestão e governança eficazes, transparentes e diligentes. Ser transparente em um contexto de incidente é fundamental para a reputação da organização, e assim, essa obrigação permite manter a relação de confiança que as partes interessadas nela depositaram. É importante mencionar, como já destacado nessa contribuição, que quando houver um esforço considerado desproporcional para comunicação individual aos titulares, pode haver uma exceção, desde que a comunicação pública seja realizada de forma ampla em meios de comunicação e que seja demonstrada a sua eficácia. Um exemplo de ‘’esforço desproporcional’’ seria quando o próprio meio de contato direto com o titular

	tenha sido objeto do incidente e torne o processo de comunicação individual excessivamente dificultoso, podendo impactar, inclusive, a celeridade do processo. Por fim, cabe ressaltar mais uma vez a importância de que a notificação seja entregue de maneira objetiva e não seja enviada junto a outras informações, tais como atualizações, boletins informativos ou mensagens-padrão[12]. Destaca-se, também, que o dever de notificação persiste mesmo em situações em que o titular não seja mais cliente ativo do responsável, mas seus dados estejam envolvidos em um vazamento[13].
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	A principal hipótese de exceção da obrigação de informar a ANDP a respeito da ocorrência de um incidente de segurança é quando este resultar em um **risco e/ou dano baixo aos titulares de dados**, representando mera inconveniência ou incômodo. Contudo, ainda que não exista a obrigação de notificar, argumenta-se que o dever de registro do incidente e da avaliação feita se mantém. Por fim, recomenda-se que, em observância ao princípio da prevenção e ao momento inicial de formação de uma cultura de proteção de dados no país, **que os agentes de tratamento, em caso de dúvida do grau de risco e/ou dano, notifiquem a Autoridade Nacional**, para que a ANPD possa oferecer maiores orientações e ajude o agente de tratamento na avaliação do risco e/ou dano, bem como indique possíveis medidas de mitigação. Justificativa: Com fulcro no artigo 48 da LGPD, a notificação à ANPD deve ser feita sempre que o incidente puder resultar em ‘’risco ou dano relevante’’ aos direitos e liberdades individuais, seja dos titulares de dados ou da coletividade. Nesse sentido, o grau de risco depende de fatores diversos, de modo que as boas práticas e governança do tratamento de dados (arts. 50 e 51, LGPD) têm um papel muito importante para determinar o que deve ou não ser notificado, inclusive sendo parte imprescindível para a justificativa de casos não notificados[14]. Sendo assim, os incidentes de segurança de dados pessoais que apresentarem riscos e/ou danos considerados “baixos” (conforme argumentado na resposta da pergunta 2), podem ser dispensados da obrigação de notificar a Autoridade Nacional de Proteção de Dados.

[12] SOMBRA, Thiago Luís e CASTELLANO, Ana Carolina. **Plano de Resposta a Incidentes de Segurança: reagindo rápido e de forma efetiva**. Revista do Advogado. AASP, 2019 v. 39 n. 144 nov, p. 168-173

[13] GOULART, Guilherme Damasio; MENKE, Fabiano. **Segurança da Informação e Vazamento de Dados.** In: BIONI, Bruno et al (org.). Tratado de proteção de dados pessoais. São Paulo: Forense, 2021. Cap. 17. p. 628-666.

[14] GOULART, Guilherme Damasio; MENKE, Fabiano. **Segurança da Informação e Vazamento de Dados.** In: BIONI, Bruno et al (org.). Tratado de proteção de dados pessoais. São Paulo: Forense, 2021. Cap. 17. p. 628-666.

	Por exemplo, uma hipótese de dispensa da notificação seria o caso da perda de um dispositivo móvel criptografado com segurança, utilizado pelo controlador ou equipe[15]. Isso porque, se a chave de criptografia permanece na posse segura do controlador e esta não é a única cópia dos dados pessoais, então tais dados ficarão inacessíveis para um invasor, o que certamente dificultaria qualquer tipo de violação resultante em riscos ou danos para os direitos e liberdades dos titulares de dados em questão. Por outro lado, a invasão do banco de dados de um hospital, por exemplo, é uma situação que implica maiores riscos e potencial de dano concretizado para a saúde dos titulares, haja vista que alterações ou exclusões de dados podem comprometer o tratamento adequado ao paciente. Desse modo, inevitavelmente, existe a necessidade de notificação à ANPD. No entanto, um incidente que tenha como consequência apenas a necessidade dos titulares alterarem uma senha de acesso, por exemplo, pode ser considerado de baixo risco e, portanto, excetuada a obrigação de notificar, uma vez que o risco seria considerado uma mera "inconveniência"[16]. Destacamos também alguns exemplos de boas práticas realizadas por outras autoridades de proteção de dados do mundo: a. A autoridade de proteção de dados do Reino Unido (Information Commissioner's Office – ICO), determina a notificação de incidentes que "coloquem em risco os direitos e liberdades das pessoas", excluindo dessa obrigação os casos nos quais **"não ofereceriam riscos para além da inconveniência";** b. c. A autoridade francesa de proteção de dados (Commission Nationale de L'informatique et des Libertés – CNIL), por sua vez, determina que deverão ser notificados à autoridade incidentes que coloquem em risco a "vida privada" dos titulares. A estes deverão ser comunicados os incidentes que representem "risco elevado". **Caso haja dúvida na avaliação da situação, deve-se notificar a autoridade para que ela determine a necessidade ou não de notificação.** Ressaltamos também a importância da documentação de todos os processos de tomada de decisão, inclusive quando o controlador julgar que não há a necessidade de notificar à Autoridade e nem aos titulares. Tal obrigação de registro se encontra alinhada com os princípios de prevenção e responsabilização e prestação de contas, e o dever geral de registro das atividades de tratamento (art. 37), facilitando, inclusive, a posterior justificativa dos casos que não forem notificados.

[15] ARTICLE 29 DATA PROTECTION WORKING PARTY. Guidelines on Personal data breach notification under Regulation 2016/679. 2017. Disponível em: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052>

[16] LUCIANO, Maria. Vazamentos de dados na LGPD: em busca do significado de "incidente de segurança". Revista do Advogado, São Paulo: AASP, ano 39, n. 144, p.163-225, nov. 2019

	Por fim, recomenda-se que, em observância ao princípio da prevenção e ao momento inicial de formação de uma cultura de proteção de dados no país, **que os agentes de tratamento, em caso de dúvida do grau de risco e/ou dano, notifiquem a Autoridade Nacional**, para que a ANPD possa oferecer maiores orientações e ajude o agente de tratamento na avaliação do risco, bem como indique possíveis medidas de mitigação.
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	Em harmonia com o que se argumentou até aqui, bem como os parâmetros internacionais sobre a questão, entende-se que o dever de informar os titulares sobre um incidente de segurança de dados pessoais pode ser excetuado nas seguintes hipóteses: 1) Quando o risco e/ou dano ao titular for baixo. 2) Quando o agente de tratamento tenha aplicado medidas de segurança técnicas e organizacionais que tornam eventual incidente irrelevante para os titulares. 3) Quando, após o incidente, o agente de tratamento tomar medidas de mitigação para garantir que um eventual risco e/ou dano aos titulares não seja mais provável de se concretizar. Por fim, 4) Quando a comunicação individual aos titulares envolver um esforço desproporcional, o controlador poderia fazer a comunicação de forma pública e difusa. Justificativa: O critério primordial para identificar a necessidade ou não de informar um incidente de segurança aos titulares de dados é a probabilidade de resultar em altos riscos para os seus direitos e liberdades individuais. Dessa forma, verificada a gravidade do incidente, a ANPD poderá determinar que o controlador adote algumas providências, como divulgar amplamente o fato em meios de comunicação, além de determinar a adoção de medidas para mitigar os possíveis efeitos (Art 48, §2º da LGPD). Nesse mesmo sentido, ao informar os titulares sobre o ocorrido, os controladores podem fornecer informações e orientações sobre as medidas a serem tomadas, para garantir a proteção em relação às possíveis consequências[17]. Ocorre que nem todos os incidentes precisam ser informados aos titulares, até para protegê-los de um excesso de notificações desnecessárias. Assim, tratando sobre hipóteses de desnecessidade de notificação, o artigo 34 (3) da GDPR elenca algumas condições e circunstâncias: a. **Quando o agente de tratamento aplicou medidas técnicas e organizacionais adequadas para proteger os dados pessoais antes da violação**, principalmente medidas que tornam os dados pessoais ininteligíveis, como a criptografia, para qualquer pessoa que não esteja autorizada a acessá-los. O que, dentro de uma perspectiva brasileira, coincide com o disposto no artigo 48 §3º da LGPD.

[17] ARTICLE 29 DATA PROTECTION WORKING PARTY. Guidelines on Personal data breach notification under Regulation 2016/679. 2017. Disponível em: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052>

	b. **Imediatamente após uma violação, o controlador tomou medidas para garantir que o alto risco inicialmente representado para os direitos e liberdades dos indivíduos não seja mais provável de se concretizar e resultar em dano**. Por exemplo, dependendo das circunstâncias do caso, o responsável pelo tratamento pode ter imediatamente identificado e tomado medidas contra o indivíduo ou grupo que acessou os dados pessoais antes que houvesse alguma consequência relevante decorrente do incidente. A devida consideração ainda precisa ser dada às possíveis consequências de qualquer quebra de confidencialidade, mais uma vez, dependendo da natureza dos dados em questão. c. **Quando a comunicação individual acerca do incidente envolveria um esforço desproporcional**. Nos casos em que, por exemplo, os dados de contato do indivíduo tenham sido perdidos como resultado da violação ou não sejam conhecidos em primeiro lugar. Um exemplo é a inundação de um depósito de um escritório de estatística, resultante na perda dos documentos contendo dados pessoais, que foram armazenados apenas em papel. Em situação semelhante, o controlador deve fazer uma comunicação pública ou tomar medida equivalente, a fim de garantir que as pessoas sejam informadas de forma igualmente eficaz. Nesse mesmo sentido, no parecer 03/2014[18], o qual aborda as notificações em caso de violação, o WP29 explicou que uma violação de confidencialidade de dados pessoais que foram, por exemplo, criptografados com um algoritmo de última geração, ainda assim configura uma violação de dados pessoais, devendo ser notificada à Autoridade. No entanto, se a confidencialidade da chave estiver intacta, ou seja, se a chave não foi comprometida com nenhuma violação de segurança e foi gerada de forma a não ser acessada por qualquer pessoa que não esteja autorizada, então os dados são, em princípio, ininteligíveis. Portanto, é improvável que a violação afete de maneira adversa os indivíduos e, como consequência, não exigiria comunicação aos mesmos.
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	Entende-se que critérios mínimos de análise da gravidade do incidente de segurança perpassam pela lógica da probabilidade e severidade do risco e de dano relevante para os titulares. Ou seja, **quanto maior for a probabilidade e/ou a severidade do dano, maior a gravidade do incidente de segurança** e, assim, maior atenção deve ser direcionada ao caso. Sugere-se que os critérios elaborados busquem se amoldar a acúmulos internacionais, cujos critérios são similares em diversas jurisdições, inclusive para que se facilite a cooperação em casos de incidentes de seguranças que ultrapassam as fronteiras brasileiras. Especificamente, sugere-se a discussão em tornos de

[18] ARTICLE 29 DATA PROTECTION WORKING PARTY. Opinion 03/2014 on Personal Data Breach Notification. 2014. Disponível em: <https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2014/03/WP-Opinion-032014.pdf>

	critérios que levem em consideração: O tipo de incidente; A natureza, sensibilidade e volume dos dados pessoais; Facilidade com que se consegue identificar os indivíduos; A severidade das consequências para os indivíduos e (v) As características especiais do indivíduo. A análise da gravidade do risco é fundamental nesse processo todo, visto que a rapidez e precisão dessa avaliação permite uma resposta da agência com uma rapidez proporcional à severidade do caso - i.e., maior probabilidade e gravidade dos danos decorrentes do incidente de segurança. De maneira geral, pode-se extrair da lei que a probabilidade de risco ou dano relevante para os titulares será maior sempre que o incidente envolver dados sensíveis ou de indivíduos em situação de vulnerabilidade, incluindo crianças e adolescentes, ou tiver o potencial de ocasionar danos materiais ou morais, tais como discriminação, violação do direito à imagem e à reputação, fraudes financeiras e roubo de identidade. Da mesma forma, deve-se considerar o volume de dados envolvido, o quantitativo de indivíduos afetados, a boa-fé e as intenções dos terceiros que tiveram acesso aos dados após o incidente e a facilidade de identificação dos titulares por terceiros não autorizados. Assim como na LGPD, a GDPR estabelece que somente somente incidentes que representem um risco provável aos direitos e liberdade dos titulares titulares, bem como a comunicação ao próprio titular só é necessária em caso de probabilidade de resultar em um alto risco aos seus direitos e liberdades - seguindo o mesmo racional de que a magnitude do risco está ligada aos fatores de severidade e probabilidade (conforme disposto nos considerandos 75 e 76 da GDPR). No Guia sobre Notificação de Vazamento de Dados conforme a Regulação 2016/679 ("Guidelines on Personal data breach notification under Regulation 2016/679"), publicado em 2017, o Working Party 29 (WP29) ressalta que há uma diferença nessa avaliação de riscos quando comparada à avaliação necessária para elaborar um DPIA. Nesta, a avaliação dos riscos existe tanto em dois cenários hipotéticos: (i) no caso do tratamento se dar conforme o planejado e (ii) no caso de acontecer um incidente. No caso de um incidente de segurança que já aconteceu, há avaliação somente do risco resultante desse acontecimento. Conforme o Guia, a concretização do risco se dá "[...] quando a violação pode levar a danos físicos, materiais ou imateriais para os indivíduos cujos dados foram violados. Exemplos de tais danos são discriminação, roubo de identidade ou fraude, perda financeira e danos à reputação." (WP29, 2017). Ainda quando a violação envolve dados pessoais que revelam origem racial ou étnica, opinião política, religião ou crenças filosóficas, ou filiação em sindicatos, ou inclui dados genéticos, dados relativos à saúde ou dados relativos à vida sexual, ou condenações criminais e ofensas ou medidas de segurança relacionadas, tal dano deve ser considerado provável de ocorrer. A Seção IV do Guia - parte dedicada à explicação de fatores a serem considerados ao se avaliar os riscos - elenca critérios para avaliação de risco de maneira bastante objetiva: **(i) O tipo de incidente; (ii) A natureza, sensibilidade e volume dos dados pessoais; (iii) Facilidade com que se consegue identificar**

	os indivíduos; (iv) A severidade das consequências para os indivíduos; (v) Características especiais do indivíduo; (vi) Características especiais do controlador e (vii) O número de indivíduos afetados. Consolidou-se a definição e exemplos de cada um desses critérios na Tabela anexada a esse documento, que, além de conceituar os sete critérios elaborados pela WP29, mapeia as diretrizes de outras sete Autoridades de Proteção de Dados, em busca de similaridades e diferenças desses critérios elaborados pelo WP29. Os países das autoridades escolhidas foram: Reino Unido (ICO), França (CNIL), Espanha (AEPD), Argentina (ADPA), Uruguai (URCDP) e Austrália (OAIC). A ICO, por exemplo, possui um breve guia sobre avaliação de risco e, para maiores esclarecimentos, indica especificamente a seção IV do WP29 no guia sobre notificação de incidentes. **Assim como recomenda a WP 29, o critério geral é severidade do risco e probabilidade.** A autoridade australiana, por sua vez, reuniu seis dos sete critérios elaborados pelo WP29, deixando de fora somente a "facilidade com que se consegue identificar os indivíduos". O Relatório da Argentina e do Uruguai também estabelece como critérios cinco dos sete acima mencionados. Sugere-se que a maioria dos critérios adotados pela ANPD estejam em consonância com aqueles aplicados pelas demais Agências de Proteção de Dados, para que eventual necessidade de cooperação internacional seja facilitada pelo uso de critérios similares. Por fim, sugere-se que não é desejável elaborar um critério específico para incidentes de segurança envolvendo políticos. No entanto, pode ser interessante considerar a motivação política do incidente por alguns *proxies,* como tem ocorrido em organizações da sociedade civil.
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	Sugere-se, especificamente para a elaboração de metodologias e critérios, que seja adotada a lógica de risco, na qual quanto maior for a probabilidade e/ou a severidade do dano, maior a gravidade do incidente de segurança e, assim, maior atenção deve ser direcionada ao caso. Através do estudo comparado da atuação e dos Guias disponibilizados por diversas Autoridades de Proteção de Dados ao redor do mundo, foi possível sistematizar algumas das melhores práticas metodológicas em termos de: i) organização da informação; ii) avaliação sistemática do risco e impacto e iii) exposição de critérios objetivos para análise de gravidade. São eles: • Proposta de análise quantitativa para avaliação de gravidade de incidente de segurança, disponível no documento “Data Breach Severity Methodology”, da European Union Agency for Network (Enisa) • Metodologia quantitativa e qualitativa para elaboração de análise de probabilidade e impacto, sistematizada pelo Guía de Evaluación de Impacto en La Protección de Datos, feito, de forma conjunta, pela Agencia de Acceso a la Información Pública (AAIP, Argentina) e pela Unidad Reguladora y de Control de Datos Personales (URCDP, Uruguai)

- Aplicação faseada de critérios de avaliação de riscos, expostos no Guia "Data breach preparation and response", preparado pelo Office of the Australian Information Commissioner (OAIC, Austrália)

- Tabelas e planejamento de avaliação de risco disponíveis nos Guias "Security of Personal Data" e Methodology for Privacy Risk Management, ambos da Commission Nationale de l'Informatique et des Libertés (CNIL, França).

Uma proposta metodológica para análise da gravidade de violações de dados pessoais foi proposta pela European Union Agency for Network and Information Security (Enisa), de 2011. O documento foi elaborado a partir de uma revisão das medidas e procedimentos existentes em Estados da União Europeia, no que diz respeito a violações relacionadas a incidentes de segurança de proteção de dados, como parte de um estudo sobre a implementação técnica da Diretiva ePrivacy do Parlamento Europeu sobre proteção da privacidade. O objetivo da metodologia proposta pela Enisa é servir de ferramenta quantitativa para avaliação da gravidade do incidente, auxiliar os controladores de dados a tomarem rápidas medidas de mitigação e dar ferramentas às Autoridades Nacionais de Proteção de Dados para realizar uma avaliação de gravidade do incidente.

Alguns aspectos principais da metodologia quantitativa elaborada pela Enisa serão apresentados abaixo.

1. **Metodologia geral**

De acordo com a metodologia proposta, a **gravidade** do incidente deve ser definida pela **estimação da magnitude do potencial de impacto aos titulares afetados pela violação de dados pessoais.** São três os critérios que devem ser considerados na avaliação, quais sejam:

- **O contexto do tratamento de dados (CTD):** o que envolve a avaliação da categoria dos dados pessoais envolvidos no incidente de forma aplicada ao contexto no qual são utilizados; nesse sentido, diz respeito à avaliação do critério de "criticidade" de uma base de dados em um determinado contexto de tratamento.

- **A facilidade de identificação dos indivíduos afetados (FI)**
  - Fator corretivo do critério CTD. A criticidade de uma atividade de tratamento pode ser reduzida dependendo do valor de FI, ou seja, quão mais difícil for identificar o titular de dados afetado, menor é o resultado final de análise da gravidade do incidente. Por esse

motivo, a multiplicação dos fatores CTD e FI gera o *score* inicial da de gravidade (SG) do incidente de segurança.

- **As circunstâncias do incidente, o que pode ter influência adicional na avaliação da gravidade do incidente (CI)**
  - Esse critério quantifica as circunstâncias específicas do incidente que podem se apresentar ou não em determinadas situações. Quando presente, o CI soma a potencial gravidade do incidente, servindo como critério de ajuste.

De tal forma, o *score* final de avaliação de gravidade é feito a partir da seguinte fórmula:

SG (score de gravidade) = **CTD** (contexto do tratamento) x **FI** (facilidade de identificação) + **CI** (circunstâncias do incidente)

O resultado é classificado em quatro níveis de gravidade: baixa, média, alta ou muito alta. Ao final da avaliação, outros critérios relevantes como o número de indivíduos afetados (para a Enisa, deve ser fator de aumento de gravidade caso exceda 100 indivíduos afetados) e o nível de inteligibilidade dos dados (utilização de criptografia forte pode ser fator de diminuição da gravidade) não considerados na valoração inicial, devem ser incluídos na análise.

1. Análise dos critérios

2.1. Contexto do Tratamento de Dados (CTD)

A fim de estabelecer o CTD, deve-se seguir 2 passos de avaliação:

1. Definir e classificar as categorias de dados pessoais envolvidos no incidente
   a. Definir os tipos de dados pessoais envolvidos no incidente
   b. Classificar os dados em quatro categorias de análise, quais sejam: simples, comportamental, financeiro ou dado sensível. Trata-se de lista não exaustiva que pode ser adaptada dependendo do caso concreto.

Dentro das quatro categorias propostas (simples, comportamental, financeiro ou sensível), caso um dado pessoal tenha correspondência com mais de uma, o cálculo deve ser repetido para tantas categorias forem. O

	critério CTD deverá ser aquele com maior *score* final. Na análise individual, as categorias possuem os seguintes *scores* básicos: 2. Dados simples: **3** 3. Comportamental: **2** 4. Financeiro: **3** 5. Sensível: **4** Em uma segunda etapa, deve-se ajustar a avaliação pela análise de outros fatores relacionados ao tratamento de dados, estabelecendo uma quantificação de 1-4, capaz de avaliar a ocorrência de fatores capazes de aumentar ou diminuir o *score* básico (volume de dados, características especiais do controlador ou dos indivíduos afetados, inexatidão ou falta de acurácia dos dados, disponibilidade pública dos dados antes do incidente e natureza dos dados). **2.2. Facilidade de Identificação (FI)** Há quatro níveis de Facilidade de Identificação estabelecidos pela metodologia, quais sejam: i) negligenciável; ii) limitado; iii) significante; iv) máximo, com uma progressão linear entre eles para avaliação do *score*. Para definição desse *score*, é importante considerar que a forma de identificação pode ser direta (*ex:* baseada no nome completo do indivíduo afetado) ou indireta (baseado em um número de CPF). Além disso, pode depender do contexto do incidente. Além disso, deve-se avaliar todos os meios razoáveis para identificação do titular de dados. Isso inclui outras informações públicas ou disponíveis na internet, bem como o cruzamento dos dados do incidente com outras bases de dados. Ao final, escolhe-se um nível de 1 a 4 a fim de atribuir o *score* **FI.** **2.3. Circunstâncias do incidente (CI)** Nessa etapa, considera-se a perda de segurança (confidencialidade, integridade e disponibilidade) e a intenção maliciosa do incidente, de acordo com os seguintes parâmetros: a. Perda de confidencialidade: Ocorre quando a informação é acessada por partes não autorizadas ou que não possuem finalidade legítima no acesso. A extensão da perda deve levar em conta o escopo da revelação, como o número potencial de indivíduos e tipos de indivíduos que podem ter tido acesso à informação.

b. Perda de integridade: Ocorre quando a informação original é alterada e o dado substituído pode ser prejudicial ao indivíduo. A situação mais severa ocorre quando o dado alterado pode ser utilizado para causar dano ao indivíduo.

c. Perda de disponibilidade: Ocorre quando o dado não pode ser mais acessado, mesmo sendo necessário. Pode ser *temporal* (limite de tempo no qual a falta de acesso é prejudicial ao indivíduo) ou permanente.

d. Dolo: Avaliação de se o incidente ocorreu por erro, negligência, por causa humana ou técnica, ou se foi causado de forma dolosa. Exemplos de incidentes não intencionais incluem perda acidental, erro humano. Exemplos de incidentes dolosos envolvem a venda de dados pessoais ou ações que visam expor dados pessoais do titular a terceiros com a finalidade de causar dano.

Para avaliação do critério **CI**, devem ser dados pontos para cada elemento. Os pontos devem ser somados para obter o *score* final.

SG = CTD x FI + CI

GRAVIDADE DO INCIDENTE DE SEGURANÇA		
SG <2	**Baixo**	Indivíduos não serão afetados ou sofrerão pequenos inconvenientes sem maiores problemas, como irritações.
2 ≤ SG < 3	**Médio**	Indivíduos podem encontrar inconveniências significativas, que poderão superar com alguma dificuldade (custos extras, perda de acesso, estresse, perda de interesse)
3 ≤ SG < 4	**Alto**	Indivíduos podem encontrar consequências significativas, as quais podem superar com sérias dificuldades como perda financeira, negativação, danos à propriedade e perda de emprego.
4 ≤ SG	**Muito Alto**	Indivíduos podem encontrar consequências de perdas significativas ou irreversíveis às quais podem não superar, como dívidas substanciais, incapacidade para trabalho, danos psicológicos de longo prazo, morte etc.

Além disso, para a elaboração de resposta a esse quesito, foi realizada análise comparada dos Guias de Notificação de Incidentes de Segurança, bem como dos guias de elaboração de Relatório de Impacto à Proteção de Dados Pessoais das Autoridades de Proteção de Dados da Argentina, Austrália, Espanha, França, Reino Unido e Uruguai.

No que diz respeito ao rigor metodológico, bem como à estruturação organizada de uma análise de impacto de um incidente de segurança, elegeu-se a apresentação do Guia "Security of Personal Data" do **Esquema de Notificação de Incidentes de Segurança - NBD-Scheme**, vigente na Austrália.

Em 2017, o Parlamento Australiano promulgou o "Privacy Amendment (Notifiable Data Breaches) Act". O Ato, além de oferecer provisões concretas para uma notificação de incidente de segurança, também oferece perspectivas positivas para uma boa realização de compreensão do impacto e da gravidade de um incidente de segurança.

Na Seção 26WG do documento, é estabelecida uma metodologia de análise de gravidade de incidentes. Os critérios, também presentes no Guia **Data Breach preparation and response,** foram transcritos abaixo para referência.

Os motivos de eleição de exposição dos critérios adotados pela OAIC são: i) o nível de detalhamento do Esquema para Incidentes de Segurança Notificáveis; ii) a utilização de critérios estabelecidos pela revisão de literatura realizada para apreciação da gravidade de um incidente de segurança e iii) a compreensão dialógica e propositiva adotada pelo conteúdo.

1. **Avalia se, da perspectiva de uma "pessoa razoável", o incidente de segurança será possivelmente capaz de gerar sério dano para o indivíduo que teve suas informações pessoais comprometidas.**

Por 'pessoa razoável', a OAIC compreende como uma pessoa que esteja na posição da entidade Notificante, e não do indivíduo que teve suas informações comprometidas no incidente de segurança e que esteja propriamente informada baseada em informações imediatamente disponíveis ou após a realização de inquéritos para compreensão do incidente.

A frase "possivelmente capaz de gerar" se refere aos riscos à danos severos à avaliação de se o risco de dano severo aos titulares é mais provável de ocorrer do que não (usa-se o termo provável, ao invés de possível, de forma proposital).

	Dano severo, para a OAIC, é caracterizado como: dano psicológico, físico, emocional, financeiro ou reputacional. As orientações da OAIC indicam que os agentes devem endereçar a avaliação do “risco severo” de forma holística, apreciando a probabilidade de dano e as consequências de dano. A apreciação inclui: • O tipo ou tipos de informações; • A sensibilidade da informação; • Se a informação está protegida por uma ou mais medidas de segurança e a possibilidade de que essas medidas de segurança possam ser superadas; • As pessoas ou os tipos de pessoas que obtiveram ou que podem vir a obter as informações • Se foi utilizada uma metodologia de segurança ou de tecnologia: o Em relação à informação o Feita de forma a tornar a informação inteligível ou sem significado para pessoas não autorizadas a obter a informação • A possibilidade que as pessoas ou tipos de pessoas que: o Obtiveram ou que podem obter informações possuem intenção de causar dano aos indivíduos titulares de dados ou capaz de superar as medidas de tecnologia da segurança aplicadas • A natureza do dano; • Quaisquer outros aspectos relevantes **2. Avaliação da categoria de titular de dados envolvida no incidente** Há algumas categorias de informação que são mais capazes de causar dano sério ao indivíduo se comprometidas. Alguns exemplos dos tipos de informação que podem causar dano severo no caso de incidente de segurança incluem: • Dados sensíveis, como informação sobre a saúde do indivíduo;

	• Documentos utilizados de forma comum para roubo de identidade, como detalhes de plano de saúde, carteira de motorista ou dados do passaporte; • Informação financeira • Uma combinação dos tipos de informação pessoal (ao invés de apenas um único tipo de informação) que permite maior conhecimento sobre o titular de dados afetado **3. Avaliação das circunstâncias do incidente de segurança** As circunstâncias específicas do vazamento são importantes para a consideração da existência de dano severo a um indivíduo. Isso pode incluir as seguintes considerações: • Quem são as pessoas que tiveram as informações pessoais afetadas pelo incidente? • Quantos indivíduos foram afetados? • As circunstâncias do incidente afetam a sensibilidade da informação? • Por quanto tempo a informação ficou acessível? • A informação estava adequadamente encriptada, anonimizada ou, de outra forma, inacessível? • Que pessoas ganharam acesso ou controle aos dados pessoais objeto do incidente de segurança? **4. Avaliação da natureza do dano** Ao avaliar a natureza do dano, as entidades devem pensar a diversa quantidade de danos que podem seguir um incidente de segurança. Para isso, seria importante considerar um número de cenários que podem resultar em dano severo e a possibilidade de que cada um ocorra. São eles: • Roubo de identidade; • Perda financeira significativa pelo indivíduo; • Ameaças para a integridade física do indivíduo; • Perda de emprego ou de oportunidades de emprego; • Humilhação, dano à reputação ou à relacionamentos; • Bullying social ou no ambiente de trabalho e marginalização. Além disso, é importante que seja avaliada a probabilidade de dano, bem como que sejam antecipadas as possíveis consequências aos titulares de dados.

Por fim, uma última abordagem metodológica de relevante interesse foi apresentada pela Agencia de Acceso a la Información Pública (AAIP) - Argentina e pela Unidad Reguladora y de Control de Datos Personales (URCDP) - Uruguai no Guia conjunto "Evalución de Impacto en la Protección de Datos".

Embora o Guia tenha sido proposto para realização de avaliação de risco de forma a prevenir riscos de incidente de segurança, a metodologia abordada pode ser considerada para nortear uma análise baseada em um risco material - que se concretizou com um incidente ou que pode estar em vias de se concretizar. Nesse sentido, é importante possuir critérios de avaliação do impacto efetivamente ocorrido ou provável de ocorrer diante da aplicação dos estándares aqui disponíveis, com base em um caso concreto.

A metodologia apresentada segue a seguinte matriz:

Risco = Probabilidade x Impacto

Probabilidade diz respeito às possibilidades existentes de que a ameaça se materialize. Impacto, por sua vez, é um critério determinado com base nos danos que se podem produzir caso a ameaça se materialize.

A realização de uma **avaliação de impacto** baseada em um caso concreto no qual foi constatada a existência de um incidente de segurança é uma metodologia possível para compreensão da análise de gravidade de um incidente e será explorada abaixo.

De acordo com o Guia, a **avaliação de impacto** deve ser considerada a partir de uma perspectiva valorativa material e moral. Ressalte-se que a fórmula para valoração dos critérios deve ser desenhada para cada organização, tendo em vista as atividades do Titular de Dados, a natureza dos dados pessoais tratados, o volume de dados vazados e demais informações sobre o incidente e critérios de avaliação, já explanados em resposta à Pergunta 11.

Da Avaliação de Impacto

Impacto baixo

Impacto baixo
Descrição: Os titulares de dados não serão afetados ou somente sofrerão alguns inconvenientes, que poderão ser solucionados sem muitas dificuldades.

Exemplos de Impactos Materiais	Exemplos de Impactos Morais
• Perda de tempo com a repetição e formalidades ou com a espera de sua realização • Recebimento de correio eletrônico não solicitado (*spam*) • (Re)utilização de suas informações, publicadas em sites ou plataformas *web,* para propaganda direcionada	• Mera perturbação causada pela solicitação ou recebimento de suas informações; • Medo de perder o controle de seus próprios dados; • Sensação de invasão de sua privacidade, mesmo que não tenha se materializado um dano objetivo ou real • Acesso negado à site ou plataforma *web* que deixa de prestar serviço importante ao titular por erro de acesso

Impacto médio	
Descrição: Os titulares de dados são afetados de maneira significativa, mas são capazes de superar a situação com alguma dificuldade	
Exemplos de Impactos Materiais	**Exemplos de Impactos Morais**
• Cobranças impostas de maneira errônea ou indevida • Recusa de acesso a serviços administrativos ou comerciais	• Medo ou negativa de utilizar um serviço relevante da sociedade da informação ou rede social

• Perda de oportunidade de conforto (cancelamento de compra ou transação vinculada ao período de férias) • Bloqueio de conta ou de serviços eletrônicos • Recebimento de *emails* direcionados com intenção de causar dano ou ameaçar a reputação do titular de dados • Desatualização de informações relevantes ao titular de dados	• Danos psicológicos objetivos, porém menores • Danos à reputação ou à honra • Problemas com relacionamentos pessoais ou no âmbito laboral • Sensação de invasão de privacidade sem um dano significativo • Intimidação em redes sociais

Impacto alto	
Descrição: Os titulares de dados são afetados de maneira significativa e apenas poderão superar a situação com grandes dificuldades	
Exemplos de Impactos Materiais	**Exemplos de Impactos Morais**
• Transferência errônea de ativos financeiros do titular à outras pessoas sem compensação	• Danos psicológicos sérios (depressão, paranoia, desenvolvimento de fobia)

• Dificuldades financeiras a médio e longo prazo • Perda de oportunidades únicas, não recorrentes • Perda de trabalho • Separação ou divórcio • Dano à propriedade • Perda financeira como resultado de uma fraude	• Sensação de invasão da privacidade com dano irreversível • Sensação de vulnerabilidade por ter que intervir em um procedimento judicial • Sensação de violação de direitos fundamentais (discriminação, liberdade de expressão) • Sofrimento de extorsões ou de manifestações públicas contrárias • Ciberbullying e assédio moral

Impacto crítico	
Descrição: Os titulares de dados enfrentam consequências gravíssimas ou irreversíveis que talvez não sejam capazes de superar	
Exemplos de Impactos Materiais	**Exemplos de Impactos Morais**
• Risco financeiro • Dívidas substanciais • Incapacidade laboral	• Dano psicológico permanente • Condenação penal • Sequestro

• Incapacidade de seguir vivendo em um mesmo lugar ou de mudar-se para outro • Perda de prova no contexto de um litígio • Perda de acesso à infraestrutura essencial (água, eletricidade)	• Perda de vínculos familiares e de amizade • Incapacidade de demandar em justiça • Mudança de *status* administrativo • Status de perda de capacidade

Outro material relevante foi proposto pela Commission Nationale de l'Informatique et des Libertés (CNIL), autoridade francesa de proteção de dados pessoais, no Guia "Security of Personal Data".

A Autoridade apresenta tabela de avaliação da gravidade do incidente, abaixo transcrita para referência:

Riscos	**Efeitos nos indivíduos**	**Principais fontes de riscos**	**Principais ameaças**	**Medidas existentes ou planejadas para mitigação**	**Gravidade**	**Probabilidade**

Dentro da avaliação, deve-se levar em consideração os critérios já levantados anteriormente, o que permitirá o estabelecimento de um *score* de gravidade que pode variar entre: negligenciável, moderado, significante ou máximo.

	Buscou-se, com a apresentação de materiais, metodologias e critérios utilizados por diferentes Autoridades de Proteção de Dados ao redor do mundo, disponibilizar ferramentas para que a ANPD possa elaborar uma metodologia própria, capaz de melhor atender a realidade brasileira.
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	Sugere-se que as providências a serem tomadas pela ANPD devam girar em torno de três nortes fundamentais: 1. Procurar alinhar as providências à lógica de regulação responsiva adotada pela LGPD; 2. Os deveres da própria agência, quais são: (i) guia/orientação aos regulados (ii) fiscalização e imposição de medidas sancionatórias (iii) Cooperação e (iv) Publicidade; e 3. Manter em mente que o papel da ANPD nesse contexto é, além de mitigar os danos já concretizados (art. 48, § 2º), proteger os dados de danos adicionais, buscando formas de conter o incidente. Nesse sentido, sugere-se os seguintes encaminhamentos: 1. A elaboração de um documento padrão sobre os passos gerais que serão tomados pela ANPD em resposta às notificações de incidentes; 2. Esclarecimento sobre quando e se os casos notificados acompanhados pela agência serão transformados em materiais de estudos e em quais termos; 3. Orientação aos controladores acerca da necessidade (ou não) da comunicação aos titulares; 4. Realização de uma análise inicial sobre quem deve gerir o incidente ao receber a notificação; 5. Elaboração de memorandos de entendimentos de cooperação procedimental com demais órgãos 6. Avaliação inicial de nível de periculosidade e impacto, a qual deve comunicada ao remetente, indicando as ações necessárias para a resolução do incidente (o que pode e deve ser feito consultando experiências de outras instituições que lidam com notificações de incidentes de segurança) 7. Delimitação sobre qual será o meio de comunicação oficial entre ANPD e controlador e quais as regras procedimentais desta comunicação. 8. Esclarecimentos de natureza jurídica (exemplos: O operador tem o dever de notificar um incidente de segurança à autoridade? Se sim, em quais casos? O pagamento de resgate nos casos de Ransomwares é legal? Se sim, como deve ser feito?) Conforme o art. 48, § 2º da LGPD, a ANDP, além do dever de verificar a gravidade do incidente, "[...] poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como: I - ampla divulgação do fato em meios de comunicação; e II - medidas para reverter ou mitigar os efeitos do incidente.". Importante manter em mente que, em uma lógica de regulação responsiva, as providências a serem tomadas pela ANPD também em casos de incidente devem seguir uma toada cooperativa com os controladores remetentes da notificação, visto que a meta principal de todo esse processo é, além da contenção do incidente, a proteção dos dados de danos adicionais. (ICO, 2019)

	As competências da ANPD estão elencadas no artigo 55-J da LGPD. A análise desse artigo com o enfoque no papel da Agência em termos de ações a serem tomadas frente à uma notificação de incidentes de segurança possibilita a classificação de quatro frentes de atuação da agência designadas pela lei: **(1) Dever guia/orientação aos regulados** (incisos III, VI, VIII, XIII e XX) **; (2) Dever de fiscalização e imposição de medidas sancionatórias** (IV, XVI, XVII)**; (3) Dever de cooperação** (IX e XXIII) (Incisos que se aplicam tanto à fiscalização e cooperação: XI, XXI e XXII) Todas essas categorias devem seguir, também por força normativa, o princípio da publicidade, que consiste na transparência ao público das ações e entendimentos da agência, culminando em uma quarta categoria de **(4) Dever de publicidade** (II, X, XII e XIV). As sugestões seguem nesse sentido de: regulação responsiva, proteção de dados como norte fundamental e categorias de competências da ANPD. → Entende-se que os planos de ação podem divergir conforme o incidente de segurança. No entanto, sugere-se a **elaboração de um documento padrão sobre os passos gerais que serão tomados pela ANPD em resposta às notificações de incidentes.** Importante que este seja publicizado, em respeito ao princípio da publicidade, assegurando aos controladores uma previsibilidade importante acerca do que esperar da agência após a notificação. Importante que seja publicizado, por exemplo, **quando e se os casos notificados acompanhados pela agência serão transformados em materiais de estudos e em quais termos** - o nome da empresa será publicado? Será necessário o consentimento da empresa? Por exemplo, além do já mencionado Padrões para Notificação de Incidentes de Segurança do Ctir Gov., a ICO, possui em seu website uma aba sobre políticas internas, dentre as quais se encontra um documento intitulado “Comunicando nosso regulatório e Política de Atividades de Execução” (“Communicating our Regulatory and Enforcement Activity Policy"). Além de outras informações, constam diretrizes de interação com os regulamentados e princípios de atuação regulatória - por exemplo: “Ação após incidentes serem relatados e preocupações levantadas: Podemos publicar ou divulgar informações que destacam a melhoria de práticas nos direitos de informação após reclamações e incidentes são relatados para nós. Isso incluirá nomes de organizações se o interesse público justificar isto”). → **Orientar os controladores acerca da necessidade (ou não) da comunicação aos titulares.** Essa é uma prática sugerida pelo WP29, por meio da qual "[...] ao notificar a autoridade supervisora, os controladores podem obter aconselhamento sobre se os indivíduos afetados precisam ser informados". A Agência francesa segue na mesma toada, ao determinar que, em caso de dúvidas sobre a necessidade de se notificar os titulares, é possível contatar a CNIL, que determinará se tal comunicação deve ou não ser feita. → **Ao receber a notificação, realizar uma análise inicial sobre quem deve gerir o incidente.** Essa é uma das providências indicadas pelo Guia Nacional de Notificação e Gestão de Incidentes Cibernéticos da Espanha ("Guía Nacional de Notificación y Gestión de Ciberincidentes da Espanha"), publicado em 2020. Sempre que a agência responsável recebe uma notificação sobre um possível incidente cibernético, a equipe técnica realiza uma análise inicial que determinará se o caso é passível de ser gerido por ela mesma ou por um terceiro.

	• Neste cenário complexo e fragmentado de enforcement, casos de competências concorrentes podem facilmente acontecer. Assim, é fundamental uma "[...] busca ativa por ferramentas hermenêuticas e por mecanismos de coordenação e articulação de competências, que podem ser construídos a partir da definição de procedimentos e parâmetros para a fixação de competências primárias e secundárias no endereçamento de casos concretos". Nesse sentido, sugere-se que a ANPD **elabore memorandos de entendimentos de cooperação procedimental com demais órgãos** que possam enquadrar-se como competentes para lidar com os incidentes de segurança. A ICO, por exemplo, adotou essa prática de procedimentalizar a cooperação com outros órgãos: possui memorandos de entendimento com quarenta e cinco instituições, desde a Advocacia Geral da União até o Centro de Informações de Saúde e Assistência Social. → Quando há indícios de que o caso pode ser gerido pela própria agência, faz-se uma **avaliação inicial de nível de periculosidade e impacto, a qual é comunicada ao remetente, indicando as ações necessárias para a resolução do incidente.** • Para além do uso dos critérios e metodologias sugeridos acima, a determinação das ações necessárias podem **contar com a experiência de outras instituições que lidam com notificações de incidentes de segurança.** Por exemplo, o Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal (CTIR), que já possui diretrizes para lidar com incidentes. Parte do processo de tratamento de incidentes perpassa pela análise de incidentes, suporte à recuperação de incidentes, coordenação na resposta a incidentes, distribuição de alertas e cooperação com outras equipes de tratamento de incidentes. (Delimitado em documento "Padrões Para Notificação De Incidentes De Segurança ao Ctir Gov.") → **Fundamental delimitar qual será o meio de comunicação oficial entre ANPD e controlador e quais as regras procedimentais desta comunicação.** Uma medida técnica estabelecida pelo Guia Espanhol consiste na **atribuição de um identificador único a cada caso**, o qual estará presente durante todas as comunicações relacionadas ao incidente. Se as comunicações são feitas por e-mail, este identificador aparece no campo "assunto" e não deve ser modificado ou eliminado, visto que isso retardaria o gerenciamento e a resolução final do incidente cibernético. → Sugere-se, por fim, que este guia contenha **esclarecimentos jurídicos**, como: O operador tem o dever de notificar um incidente de segurança à autoridade? Se sim, em quais casos? O pagamento de resgate nos casos de Ransomwares é legal? Se sim, como deve ser feito? Dentre outros.

	Um bom exemplo regulatório é o guia "Data breach preparation and response", publicado pelo Office of the Australian Information Commissioner (OAIC) em julho de 2019. Em seu Guia, a OAIC apresenta o design do Esquema para Incidentes de Segurança Notificáveis como uma espécie de estandarte metodológico para orientar o Controlador de suas ações diante de um incidente de segurança, que deve ser entregue à Comissão. Tratam-se de orientações para formatação de um completo Plano de Resposta a Incidentes de Segurança. A estrutura do Guia é a seguinte: Parte 1: Explicações sobre o conceito e a caracterização de incidente de segurança e exposição de obrigações dos agentes de tratamento na ocorrência de incidente e esquema visual Parte 2: Passo a passo para a preparação de um Plano de Resposta a Incidentes de Segurança, com *checklist* visual para fins de orientação. Especificamente nesse tópico, o guia se debruça em aspectos como a composição de uma equipe de resposta e ações a serem tomadas pelos agentes.

Information to be included	Yes/No	Comments
What a data breach is and how staff can identify one		
Clear escalation procedures and reporting lines for suspected data breaches		
Members of the data breach response team, including roles, reporting lines and responsibilities		
Details of any external expertise that should be engaged in particular circumstances		
How the plan will apply to various types of data breaches and varying risk profiles with consideration of possible remedial actions		
An approach for conducting assessments		
Processes that outline when and how individuals are notified		
Circumstances in which law enforcement, regulators (such as the OAIC), or other entities may need to be contacted		
Processes for responding to incidents that involve another entity		
A record-keeping policy to ensure that breaches are documented		
Requirements under agreements with third parties such as insurance policies or service agreements		
A strategy identifying and addressing any weaknesses in data handling that contributed to the breach		
Regular reviewing and testing of the plan		
A system for a post-breach review and assessment of the data breach response and the effectiveness of the data breach response plan		

Parte 3: O Guia apresenta 4 passos práticos para colocar em ação o Plano de Resposta a Incidentes de Segurança, quais sejam: (i) conter; (ii) avaliar; (iii) notificar e (iv) rever. As informações também são apresentadas no formato de infográfico visual.

Parte 4: Denominada “Esquemas para Incidentes de Segurança Notificáveis - *NDB Scheme*” (trad. nossa), o Guia aprofunda conceitos e procedimentos metodológicos de pontos de interesse trabalhados em suas outras seções, com orientações para: (i) incidentes que envolvem múltiplas entidades; (ii) exceções ao dever de notificação; (iii) notificação ao titular de dados; (iv) metodologia para avaliação de gravidade de incidente e (iv) o papel da *OAIC* diante de uma notificação de incidente de segurança.

Sobre este último ponto, a *OAIC* estabelece as seguintes medidas que podem ser tomadas pela Autoridade diante de uma notificação pelo controlador de dados:

	(i) **Da entrega voluntária de informações técnicas e organizacionais necessárias para apuração e diligências do incidente de segurança:** Apesar de não obrigadas pelo Privacy Act australiano, a Autoridade apresenta como uma prática de boa fé que os controladores repassem informações adicionais sobre o incidente ocorrido, bem como sobre as respostas tomadas pelo agente. Como exemplo, cita o fornecimento de informações técnicas que não necessitariam, necessariamente, de comunicação direta ao titular de dados pessoais. Esse tipo de informação auxilia a OAIC a estabelecer se deve realizar maiores diligências investigatórias ou tomar quaisquer outras ações. Esse tipo de informação também é utilizado pela OAIC para redigir relatórios estatísticos sobre as notificações recebidas. Além disso, a entidade que ofereceu a informação pode realizar uma requisição de sigilo à Comissão, que deverá respeitar a confiança das informações comerciais ou operacionais sensíveis fornecidas de forma voluntária em suporte à notificação realizada. A orientação da OAIC é de que a divulgação das informações só será realizada após consulta com a entidade notificadora, com seu consentimento ou quando assim for exigido por lei. (ii) **Da resposta da Autoridade às notificações:** A OAIC reconhece todas as notificações de incidentes de segurança recebidas. Ela poderá realizar inquéritos ou oferecer conselhos em resposta à notificação. Para isso, a Comissão se orienta pelo tipo e pela sensibilidade dos dados pessoais, pelo número de indivíduos potencialmente afetados ou em risco de sofrerem dano severo e pela extensão pelas quais a Notificação e quaisquer informações adicionais providas demonstrarem que: • O incidente de segurança foi contido ou está em processo de contenção, quando possível; • A entidade notificante tomou ou está tomando medidas razoáveis para mitigar os impactos do incidente nos indivíduos que possuem alto risco de dano potencial; • A entidade tomou ou está tomando medidas razoáveis para minimizar a possibilidade de que um incidente similar ocorra novamente. (iii) **Da ação regulatória e das prioridades da Comissão:** A prioridade de orientação da OAIC no processo é garantir e assistir indivíduos em risco de sofrer dano severo. Apesar disso, a Comissão estabelece a possibilidade de tomar medidas regulatórias, por sua própria iniciativa, em resposta à Notificação, nos termos do Privacy Act Australiano. (iv) **Dos poderes de *enforcement* e da aplicação de um Esquema para Incidentes de Segurança Notificáveis - NBD *scheme*** A Comissão avalia se a instituição notificante tomou medidas razoáveis para lidar com o incidente de segurança ocorrido. Uma falha da entidade de cumprir qualquer um dos seguintes requisitos representa, na

	interpretação da OAIC, uma interferência negativa à privacidade dos titulares de dados capaz de justificar uma ação de *enforcement*: • Realizar uma avaliação razoável e rápida do incidente de segurança, tomando todas as medidas razoáveis para garantir que a avaliação seja concluída dentro de **30 dias** da ciência do Notificante do incidente; • Preparar uma declaração sobre o incidente segurança e prover uma cópia à Comissão, no tempo mais rápido possível; • Notificar os titulares de dados em risco de sério dano sobre os conteúdos da declaração ou, dependendo da natureza do caso, realizar a publicação da declaração; • Cumprir com as diretrizes da OAIC no procedimento de elaboração de declaração e de notificação de forma tempestiva e ágil. Os poderes de *enforcement* da OAIC incluem: • Aceitar um Acordo e iniciar procedimentos para garantir o cumprimento do Acordo; • Realizar uma determinação e os procedimentos para obrigar o cumprimento da determinação; • Buscar uma liminar para evitar o incidente em curso ou sua recorrência; • Direcionar a demanda para uma Corte para que seja aplicada multa. Em muitos casos, a Comissão é provocada por indivíduos em situações nas quais o agente falhou em realizar seu dever de notificação. A ação preferencial da OAIC é estabelecer diálogo com o agente para que eles cumpram os passos delimitados pelo *NBD Scheme*, antes de aplicar medidas impositivas. (v) **Da obrigação de notificar - comunicação com o Controlador prévia à Notificação**

	A Comissão pode orientar o Notificante a realizar a comunicação do incidente para indivíduos em risco de sofrerem sério dano, bem como para a própria OAIC. Antes de solicitar a notificação, usualmente, a Comissão solicita que o agente concorde em realizar a notificação. Esse é o tipo de caso no qual a Comissão realiza orientações ao agente mesmo antes da Notificação, quando se tornou ciente da ocorrência de um incidente de segurança. Além disso, também é plausível que a OAIC informe o controlador sobre quando uma notificação não é necessária ou modifique, a depender da circunstância do caso, o prazo para que seja realizada a notificação. (vi) **Da busca de apoio técnico e legal pelo Controlador** A OAIC é responsável por informar e guiar a sociedade sobre as matérias relativas à proteção de dados pessoais na Austrália. Apesar disso, a OAIC não considera ser capaz de oferecer apoio legal e técnico próprio para cada incidente de segurança sobre o qual é notificada. Nesse sentido, embora haja orientações claras sobre a formulação do NBD Scheme, bem como acompanhamento do caso pela Comissão, os Controladores devem constituir suas próprias equipes para gerir o incidente de segurança. (vii) **Da publicação de informações sobre o incidente pela Comissão** A OAIC opta por publicar informações sobre as formas com que as entidades têm tratado incidentes de segurança de dados pessoais na forma de dados estatísticos não identificados. No caso específico do Sistema Nacional de Proteção de Dados no Brasil, percebe-se, entretanto, uma preocupação do legislador brasileiro de que a divulgação do fato em meios de comunicação esteja garantida nos casos em que isso for necessário para a salvaguarda dos direitos dos titulares (Art. 48, §2º, I). Nesse sentido, apesar de reconhecer a importância da publicação de dados estatísticos e relatórios que deem publicidade às informações sobre incidentes nacionais, também é relevante a ponderação sobre os casos em que se é apropriado determinar que os próprios controladores deem a devida publicidade ao ocorrido. Por fim, uma última referência de extrema relevância consiste no documento da União Europeia com exemplos de atuações das autoridades de proteção de dados nos casos de incidentes de segurança. A delimitação de como será a atuação da ANPD frente às notificações pode se basear nessas experiências internacionais documentadas.
SUGESTÃO DE NORMATIVO, SE HOUVER	

Art. Xxxx ....
Art. Xxxx ....

O que é um incidente de segurança e o que deflagra o dever de notificação?

Um incidente de segurança de proteção de dados é um evento que ocasiona a violação de algum dos três pilares da segurança da informação, ou de mais de um deles: confidencialidade, integridade e disponibilidade.

O dever de notificação, por sua vez, se apresenta a partir de duas perspectivas: um dever dialógico, tanto com o titular quanto com a Autoridade Nacional de Proteção de Dados, e uma obrigação que promove a adoção de medidas de mitigação para os riscos e/ou danos que podem ser ocasionados. Sendo assim, o dever de notificação é deflagrado pelo risco e/ou dano ocasionado aos titulares.

Por fim, entende-se que o incidente de segurança sempre deflagra um dever. Caso não exista um risco e/ou dano relevante, o agente de tratamento deve ao menos registrar o incidente e a avaliação que levou à considerá-lo irrelevante. Portanto, em uma lógica de regulação assimétrica propõe-se a seguinte escala de obrigações derivadas de um incidente de segurança:

> **i) sem risco relevante**: O incidente de segurança deve ser anotado nos registros das atividades de tratamento de dados, especialmente o juízo de valor do porquê foi considerado irrelevante;
> **ii) risco relevante**: Deve-se não só anotá-lo nos registros das atividades de tratamento de dados, mas, também, notificar os órgãos reguladores e titular e ser ativado um plano de resposta à incidente de segurança;
> **iii) dano relevante**: Deve-se não só anotá-lo nos registros das atividades de tratamento de dados, mas, também, notificar os órgãos reguladores e o titular e o plano de resposta deve ser mais robusto frente ao do item anterior;

Justificativa:

Inicialmente, é importante um recorte para delimitar o escopo da presente contribuição. Entende-se que o art. 46 da LGPD amplia o conceito de "incidente", não o restringindo apenas a violações de segurança da informação, mas a qualquer ilegalidade no tratamento de dados, na medida em que o referido artigo determinar que os agentes de tratamento adotem medidas de segurança, técnicas e administrativas a proteger dados pessoais de "acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito".

Nesse sentido, a contribuição terá sua análise restrita às consequências geradas por incidentes de segurança. Um outro ponto importante é que o incidente de segurança (*security incident*) é um termo guarda-chuva para qualquer evento que comprometa as normas de segurança da informação de uma organização. O CERT.br define incidente de

segurança como “qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores”.[1]

Para o contexto da proteção de dados pessoais, deve-se limitar a análise para incidentes de segurança que envolvam dados pessoais. Incidentes de segurança que comprometam o funcionamento de uma máquina agrícola, por exemplo, ou que resultem no compartilhamento não autorizado de material protegido por segredo industrial não devem, a princípio, ser considerados como incidentes de segurança de dados pessoais, fugindo portanto do escopo da contribuição.

Feita essa ressalva, incidentes de segurança de dados pessoais podem ser divididos em três categorias: 1) incidentes de confidencialidade; 2) incidentes de disponibilidade; e 3) incidentes de integridade.[2]

Sendo assim, eventos que ocasionem a violação de algum desses três elementos de segurança da informação, ou de mais de um deles, serão considerados incidentes de segurança de dados pessoais.

A violação de confidencialidade pode se caracterizar quando há tentativa ou uso não autorizado de um sistema, seja utilizando técnicas como varreduras, força bruta SSH, ou mesmo sistemas de engenharia social capazes de fraudar identidades e usuários autorizados a acessar uma base de dados.

A violação de disponibilidade pode se caracterizar quando um dado é deletado permanentemente de forma acidental ou de forma não autorizada. A encriptação não autorizada ou acidental dos dados de forma a torná-los inacessíveis também deve ser considerada uma violação de disponibilidade, como no caso de um *ransomware*, por exemplo.

A violação de integridade pode se caracterizar quando existe algum tipo de alteração não autorizada com relação aos dados, criando dados inexatos, incompletos ou desatualizados.

Um exemplo de incidente pode ser uma situação em que um sistema que possui uma falha técnica (vulnerabilidade) tem essa falha explorada por um agente malicioso; ou ainda, a referida falha técnica pode permitir que dados sejam inadvertidamente publicados em área pública do sistema que não deveria mostrar aqueles dados.

Ainda, é possível que a disponibilidade seja afetada temporariamente, como no caso de um apagão de energia ou sobrecarga do servidor de armazenamento, por exemplo. Nesse caso, caso esse evento resulte em uma impossibilidade de acessar os dados, será caracterizado um incidente de segurança. Contudo, deve-se avaliar o risco apresentado por

---

[1] CERT - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Perguntas frequentes ao CERT. 2017. Disponível em <https://www.cert.br/docs/certbr-faq.html#6>

[2] ARTICLE 29 DATA PROTECTION WORKING PARTY. Guidelines on Personal data breach notification under Regulation 2016/679. 2017. Disponível em: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052>

essa indisponibilidade. Uma indisponibilidade de acesso a uma aplicação de comércio eletrônico não oferece um risco significativo aos titulares. Por outro lado, a incapacidade de acessar dados de um paciente em um hospital oferece um risco muito maior.

Um último ponto a se considerar na definição de "incidente de segurança de dados pessoais" é se o incidente só é caracterizado quando uma ação comitiva viola algum desses elementos, ou se a mera inobservância de padrões de segurança que assegurem a confidencialidade, disponibilidade e integridade pode ser considerada, por si só, um incidente de segurança de dados pessoais.[3]

> Exemplo: Um hospital que possui um sistema de controle de acesso falho, permitindo que mais funcionários possuam a credencial e as permissões de "médico" do que o número de médicos empregados pelo hospital. Nesse caso, ainda que não se verifique um evento específico, em que um funcionário não autorizado acessou dados de saúde de pacientes, por exemplo, o risco aos titulares já está caracterizado por não haver um sistema que garanta a confidencialidade dos dados.[4]

Ressalta-se que não há necessariamente uma relação de causalidade entre a inobservância de padrões de segurança e o risco aos titulares. É possível que sistemas não seguros não gerem riscos relevantes para os titulares. Dito de outra forma, a relevância do risco é um elemento constitutivo do que se entende por incidente de segurança notificável. Essa interpretação sistemática entre dos caputs dos artigos 44, 49 e 48 da LGPD. Apesar de um evento poder ser considerado um incidente de segurança, este só ganha repercussão jurídica, a ponto de desengatilhar a obrigação de notificação, se causar um risco relevante.

Contudo, isso não significa que um efeito adverso à confidencialidade, integridade e disponibilidade de uma base de dados, ainda que não cause um risco relevante, seja desprovida de qualquer efeito jurídico. Isto porque a negligência em não corrigir uma sucessão de incidentes de segurança sem risco relevante é o que pode assim torná-lo. Por esse motivo, tão importante quanto endereçar as nuances conceituais de um incidente de segurança nortificável, é fixar que cabe ao agente de tratamento de dados guardar registros sobre tais incidentes e, principalmente, acerca do seu juízo de valor acerca da sua (ir)relevância. O objetivo é formar uma trilha auditável dos incidentes de segurança.

Trata-se de uma interpretação que decorre da lógica precaucionário da proteção de dados, a partir da exegese do art. 49 da Lei Geral de Proteção de Dados, que traz o dever de "atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares" e nos princípios

---

[3] ALUNGE, Rogers. Breach of security vs personal data breach: effect on EU data subject notification requirements.International Data Privacy Law. 2020. Disponível em: < https://doi.org/10.1093/idpl/ipaa021>

[4] O exemplo citado encontra similaridades com o caso "Hospital do Barreiro", primeira multa aplicada pelo CNPD, Autoridade de Proteção de Dados de Portugal por, dentre outras violações, violar a confidencialidade e integridade dos dados sob seu controle. Disponível em: <https://visao.sapo.pt/exameinformatica/noticias-ei/mercados/2018-10-19-CNPD-Hospital-do-Barreiro-multado-em-400-mil-euros-por-permitir-acessos-indevidos-a-processos-clinicos/>

da prevenção (art. 6º, VIII da LGPD) e da responsabilização e prestação de contas (art. 6º, X)

Por fim, em relação ao dever de notificar, para se estabelecer o que deflagra esse dever, é preciso primeiro entender as razões pelas quais existe o dever de notificação. O principal objetivo da proteção de dados pessoais é a garantia dos direitos fundamentais dos titulares (art. 1º, caput da LGPD). Sendo assim, a notificação de um incidente de segurança deve ser compreendida como uma medida que tem como objetivo último proteger, ou mitigar os danos e/ou riscos ocasionados ao titular.

Ao notificar o titular, permite-se que ele tome as medidas que achar necessárias para resguardar seus direitos. Sejam elas medidas preventivas como a troca de credenciais e senhas, uma maior atenção em relação a e-mails e mensagens possivelmente fraudulentas, sejam também medidas afirmativas de exercício de direitos, seja em sede judicial, administrativa ou extrajudicial.

A notificação à Autoridade Nacional de Proteção de Dados, por outro lado, possui um objetivo objetivo duplo. Primeiro, a Autoridade Nacional pode auxiliar o agente de tratamento na avaliação dos riscos e/ou danos do incidente, e se haveria necessidade de também notificar o titular, além de sugerir medidas de mitigação de danos. Em segundo lugar, essa notificação ao órgão regulador é também uma maneira de demonstrar que o agente de tratamento está tomando as medidas necessárias para mitigar os riscos e cessar a violação.

Portanto, risco e/ou dano aos titulares que surgem a partir de um incidente de segurança de dados pessoais deflagra o dever de notificação. Ressalta-se, contudo mais uma vez, que um mero incidente de segurança, especialmente o juízo acerca do porquê não acarretaria risco relevante, também deve ter repercussão jurídica que é compor os registros das atividades de tratamento de dados. Seguindo a ideia de uma regulação assimétrica e responsiva, quanto maiores os riscos, maiores os deveres. Há uma escalada na intensidade do conjunto de obrigações que derivam de um incidente de segurança:

> **i) sem risco relevante**: O incidente de segurança deve ser anotado nos registros das atividades de tratamento de dados, especialmente o juízo de valor do porquê foi considerado irrelevante;
> **ii) risco relevante**: Deve-se não só anotá-lo nos registros das atividades de tratamento de dados, mas, também, notificar os órgãos reguladores e titular e ser ativado um plano de resposta à incidente de segurança;
> **iii) dano relevante**: Deve-se não só anotá-lo nos registros das atividades de tratamento de dados, mas, também, notificar os órgãos reguladores e o titular e o plano de resposta deve ser mais robusto frente ao do item anterior;

Uma vez reportado qual deve ser o papel dos órgãos reguladores em

termos de fiscalização e colaboração em um plano de contenção?

Para análise do papel dos órgãos reguladores em termos de fiscalização e colaboração para produção de um plano de contenção, foram analisadas as competências normativas da ANPD estabelecidas pela LGPD em seu artigo 55-J, de forma a abordar: i) o dever de informação e publicidade; ii) a cooperação para a construção de um Sistema Nacional de Proteção de Dados e iii) os limites e parâmetros para cooperação internacional com outras Autoridades de Proteção de Dados.

O artigo 55-J da LGPD estabelece, logo em seu primeiro inciso, o zelo pela proteção dos dados pessoais como o norte da atuação da ANPD[5]. Pode parecer redundante positivar esse dever de proteção como meta dentro de uma legislação de proteção de dados pessoais. No entanto, essa regra serve como norte: todas as atuações da agência devem girar em torno desta máxima, inclusive nos casos de incidentes notificados. Assim, o papel da agência reguladora é, além de mitigar os danos já concretizados (art. 48, § 2º), proteger os dados de danos adicionais, buscando formas de conter o incidente. Somado a esse norte fundamental de atuação, a LGPD foi elaborada com base em uma lógica regulatória responsiva, que se afasta do racional de comando e controle, dando lugar a um método mais cooperativo[6]. Assim, é importante manter em mente que as providências a serem tomadas também em casos de incidentes de segurança devem seguir uma toada predominantemente cooperativa com os controladores remetentes da notificação.

O artigo 48 da lei, responsável pelo dever de notificação do controlador nos casos de incidentes de segurança, prevê que "a autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências [...]"[7]. Há duas providências que podem ser tomadas, quais sejam, I - ampla divulgação do fato em meios de comunicação; e II - medidas para reverter ou mitigar os efeitos do incidente, mas o artigo limita-se a esses dois exemplos. Nesse sentido, há uma preocupação sobre como a ANPD deve prosseguir nos casos de notificações de incidentes para além dessas breves providências. Para uma resposta coerente, é necessário compreender quais as competências gerais da ANPD, elencadas no artigo 55-J da LGPD elenca as competências da ANPD.

A análise desse artigo com o enfoque no papel da Agência em termos de ações a serem tomadas frente à uma notificação de incidentes de segurança possibilita a classificação de quatro frentes de atuação da agência designadas pela lei: **(1) Dever guia/orientação aos regulados; (2) Dever de fiscalização e imposição de medidas sancionatórias; (3)**

[5] Art. 55-J: Compete à ANPD: I - zelar pela proteção dos dados pessoais, nos termos da legislação; (Incluído pela Lei nº 13.853, de 2019)

[6] WIMMER, 2020, p. 4

[7] Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. [...] § 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como: I - ampla divulgação do fato em meios de comunicação; e II - medidas para reverter ou mitigar os efeitos do incidente.

Dever de cooperação. Todas essas categorias devem seguir, também por força normativa, o princípio da publicidade, que consiste na transparência ao público das ações e entendimentos da agência, culminando em uma quarta categoria de **(4) Dever de publicidade**. De modo sistematizado:

Competências normativas da ANPD a serem seguidas no caso de recebimento de notificação de incidente de segurança (Art. 55-J, LGPD)		
Dever de orientação aos regulados	**III** - elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade; (Incluído pela Lei nº 13.853, de 2019); **VI** - promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança; **VIII** - estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, os quais deverão levar em consideração as especificidades das atividades e o porte dos responsáveis; **XIII** - editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei; (Incluído pela Lei nº 13.853, de 2019) **XX** - deliberar, na esfera administrativa, em caráter terminativo, sobre a interpretação desta Lei, as suas competências e os casos omissos; (Incluído pela Lei nº 13.853, de 2019)	
Dever de fiscalização e imposição de medidas sancionatórias	**IV -** fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso; (Incluído pela Lei nº 13.853, de 2019) XVI - realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização de que trata o inciso IV e com a devida observância do disposto no inciso II do caput deste artigo, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público; (Incluído pela Lei nº 13.853, de 2019) XVII - celebrar, a qualquer momento, compromisso com agentes de tratamento para eliminar irregularidade, incerteza jurídica ou situação contenciosa no âmbito	**XI** - solicitar, a qualquer momento, às entidades do poder público que realizem operações de tratamento de dados pessoais informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado, com a possibilidade de emitir parecer técnico complementar para garantir o cumprimento desta Lei; (Incluído pela Lei nº 13.853, de 2019) **XXI** - comunicar às autoridades competentes as infrações penais das quais tiver conhecimento; (Incluído

	de processos administrativos, de acordo com o previsto no Decreto-Lei nº 4.657, de 4 de setembro de 1942; (Incluído pela Lei nº 13.853, de 2019)	pela Lei nº 13.853, de 2019) **XXII -** comunicar aos órgãos de controle interno o descumprimento do disposto nesta Lei por órgãos e entidades da administração pública federal; (Incluído pela Lei nº 13.853, de 2019)
Dever de cooperação	**IX** - promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional; (Incluído pela Lei nº 13.853, de 2019) **XXIII** - articular-se com as autoridades reguladoras públicas para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação; e (Incluído pela Lei nº 13.853, de 2019)	
Dever de publicidade	**II** - zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei; (Incluído pela Lei nº 13.853, de 2019) **X** - dispor sobre as formas de publicidade das operações de tratamento de dados pessoais, respeitados os segredos comercial e industrial; (Incluído pela Lei nº 13.853, de 2019) **XII** - elaborar relatórios de gestão anuais acerca de suas atividades; (Incluído pela Lei nº 13.853, de 2019) **XIV** - ouvir os agentes de tratamento e a sociedade em matérias de interesse relevante e prestar contas sobre suas atividades e planejamento; (Incluído pela Lei nº 13.853, de 2019)	

Assim, tendo em mente esses três nortes: (1) objetivo último de proteger os dados, (2) regulação responsiva e (3) quatro frentes de atuação da ANPD positivadas pela LGPD, é possível adentrar um campo mais concreto de qual o papel da agência regulatória frente a notificações de incidentes de segurança.

I. Dever de orientação aos regulados

Primeiramente, conforme o dever de orientar os regulados, entende-se que um papel central da ANPD consiste na **elaboração e publicação de materiais como guias e diretrizes de orientações em seu site oficial.** Especificamente, esse material deve versar

sobre: (a) Como evitar um incidente de segurança (medidas preventivas)[8]; (b) O que fazer se um incidente acontecer (incluindo instruções de notificação); e (c) Os passos que a Agência irá tomar após o recebimento da notificação.

É fundamental que a ANPD possua um guia de "Próximos Passos - O que fazer depois de um incidente de segurança" (b), contendo orientações como, por exemplo: **quando é necessário notificar a autoridade** (uma tabela com exemplos de casos concretos seria interessante). **Orientações sobre quando é necessário notificar os titulares** dos dados também parece ser uma medida importante. Essa é uma prática sugerida pelo WP29, por meio da qual "[...] ao notificar a autoridade supervisora, os controladores podem obter aconselhamento sobre se os indivíduos afetados precisam ser informados" (WP29, 2017, p.5). A Agência francesa segue na mesma toada, ao determinar que, em caso de dúvidas sobre a necessidade de se notificar os titulares, é possível contatar a CNIL, que determinará se tal comunicação deve ou não ser feita. (CNIL, 2018).

A agência australiana, por sua vez, possui sobre a matéria o guia "Data breach preparation and response", publicado pelo Office of the Australian Information Commissioner (OAIC) em julho de 2019, no qual apresenta o design do Esquema para Incidentes de Segurança Notificáveis como uma espécie de estandarte metodológico para orientar o Controlar de suas ações diante de um incidente de segurança, que deve ser entregue à Comissão. Tratam-se de orientações para formatação de um completo Plano de Resposta a Incidentes de Segurança[9]. Em um dos itens, a OAIC algumas medidas que podem ser tomadas pela Autoridade diante de uma notificação pelo controlador de dados, dentre as quais informar o controlador sobre quando uma notificação não é necessária ou modifique, a depender da circunstância do caso, o prazo para que seja realizada a notificação. (p. 58). O guia também estabelece que a OAIC orientará o notificante a realizar a comunicação do incidente para a própria agência e para indivíduos - no caso destes estiverem em situação que possa ensejar sérios danos[10].

Além disso, um **material sobre o que os regulados devem esperar da atuação da ANPD após o recebimento da notificação** também consiste em prática transparente e

[8] Este item não será abordado aqui, visto que a pergunta refere-se à atuação da agência *após* o recebimento de notificação de incidente de segurança.

[9] A estrutura do Guia é a seguinte: **Parte 1:** Explicações sobre o conceito e a caracterização de incidente de segurança e exposição de obrigações dos agentes de tratamento na ocorrência de incidente e esquema visual; **Parte 2:** Passo a passo para a preparação de um Plano de Resposta a Incidentes de Segurança, com *checklist* visual para fins de orientação. Especificamente nesse tópico, o guia se debruça em aspectos como a composição de uma equipe de resposta e ações a serem tomadas pelos agentes. **Parte 3:** O Guia apresenta 4 passos práticos para colocar em ação o Plano de Resposta a Incidentes de Segurança, quais sejam: (i) conter; (ii) avaliar; (iii) notificar e (iv) rever. As informações também são apresentadas no formato de infográfico visual; e Parte 4: Denominada "Esquemas para Incidentes de Segurança Notificáveis - *NDB Scheme*" (trad. nossa), o Guia aprofunda conceitos e procedimentos metodológicos de pontos de interesse trabalhados em suas outras seções, com orientações para: (i) incidentes que envolvem múltiplas entidades; (ii) exceções ao dever de notificação; (iii) notificação ao titular de dados; (iv) metodologia para avaliação de gravidade de incidente e (iv) o papel da *OAIC* diante de uma notificação de incidente de segurança.

[10] A autoridade, por sua vez, pode até mesmo solicitar uma notificação - apesar de sempre solicitar ao controlador que concorde em realizar a notificação. Esse é o tipo de caso no qual a Comissão realiza orientações ao agente mesmo antes da Notificação, quando se tornou ciente da ocorrência de um incidente de segurança.

responsiva (c). Especificamente, a elaboração de um documento padrão sobre os passos gerais que serão tomados pela ANPD em resposta às notificações de incidentes. Por exemplo, é importante que a ANPD tenha **canais de comunicação com o controlador bem definidos.** Uma medida técnica estabelecida pelo Guia Espanhol consiste na atribuição de um identificador único a cada caso, o qual estará presente durante todas as comunicações relacionadas ao incidente. Se as comunicações são feitas por e-mail, este identificador aparece no campo "assunto" e não deve ser modificado ou eliminado, visto que isso retardaria o gerenciamento e a resolução final do incidente cibernético. (ESPANHA, 2020, p. 25) Assim, para além de delimitar o canal de comunicação, é fundamental **estabelecer previamente as regras procedimentais dessa comunicação.**

Importante que seja publicizado, por exemplo, **quando e se os casos notificados acompanhados pela agência serão transformados em materiais de estudos e em quais termos** - o nome da empresa será publicado? Será necessário o consentimento da empresa? Por exemplo, a ICO, possui em seu website uma aba sobre políticas internas, dentre as quais se encontra um documento intitulado "Comunicando nosso regulatório e Política de Atividades de Execução" ("Communicating our Regulatory and Enforcement Activity Policy"). Além de outras informações, constam diretrizes de interação com os regulamentados e princípios de atuação regulatória - por exemplo: "Ação após incidentes serem relatados e preocupações levantadas: Podemos publicar ou divulgar informações que destacam a melhoria de práticas nos direitos de informação após reclamações e incidentes são relatados para nós. Isso incluirá nomes de organizações se o interesse público justificar isto").

Sugere-se, por fim, que este guia contenha **esclarecimentos jurídicos**, como: O operador tem o dever de notificar um incidente de segurança à autoridade? Se sim, em quais casos? O pagamento de resgate nos casos de Ransomwares é legal? Se sim, como deve ser feito? Dentre outros.

Por fim, se a autoridade tem de realizar uma avaliação sobre a gravidade do incidente (art. 48, § 2º) , cabe explicar nesse documento público o que, exatamente, significa essa análise: quais as metodologias e critérios adotados pela agência.

A. Análise de Gravidade

Sugere-se, especificamente para essa adoção de metodologias e critérios que seja adotada a lógica de **risco**, na qual quanto maior for a probabilidade e/ou a severidade do dano, maior a gravidade do incidente de segurança e, assim, maior atenção deve ser direcionada ao caso. A GDPR, por exemplo, estabelece que somente somente incidentes que representem um risco provável aos direitos e liberdade dos titulares titulares, bem como a comunicação ao próprio titular só é necessária em caso de probabilidade de resultar em um alto risco aos seus direitos e liberdades - seguindo o mesmo racional de que a magnitude do risco[11] está ligada aos fatores de severidade e probabilidade (conforme disposto nos

[11] No Guia sobre Notificação de Vazamento de Dados conforme a Regulação 2016/679, o Working Party 29 (WP29) ressalta que há uma diferença nessa avaliação de riscos quando comparada à avaliação necessária para elaborar um DPIA. Nesta, a avaliação dos riscos existe tanto em dois cenários hipotéticos: (i) no caso do

considerandos 75 e 76 da GDPR).

Conforme o Guia sobre Notificações de Vazamento de Dados conforme a Regulação 2016/679 ("Guidelines on Personal data breach notification under Regulation 2016/679"), publicado em 2017 pelo Working Party 29 (WP29), a concretização do risco se dá "[...] quando a violação pode levar a danos físicos, materiais ou imateriais para os indivíduos cujos dados foram violados. Exemplos de tais danos são discriminação, roubo de identidade ou fraude, perda financeira e danos à reputação."[12] . Ainda quando a violação envolve dados pessoais que revelam origem racial ou étnica, opinião política, religião ou crenças filosóficas, ou filiação em sindicatos, ou inclui dados genéticos, dados relativos à saúde ou dados relativos à vida sexual, ou condenações criminais e ofensas ou medidas de segurança relacionadas, tal dano deve ser considerado provável de ocorrer.

A Seção IV do Guia - parte dedicada à explicação de fatores a serem considerados ao se avaliar os riscos - elenca critérios para avaliação de risco de maneira bastante objetiva: (i) O tipo de incidente; (ii) A natureza, sensibilidade e volume dos dados pessoais; (iii) Facilidade com que se consegue identificar os indivíduos; (iv) A severidade das consequências para os indivíduos; (v) Características especiais do indivíduo; (vi) Características especiais do controlador e (vii) O número de indivíduos afetados. Consolidou-se a definição e exemplos de cada um desses critérios na Tabela Anexa, que, além de conceituar os sete critérios elaborados pela WP29, mapeia as diretrizes de outras sete Autoridades de Proteção de Dados, em busca de similaridades e diferenças desses critérios elaborados pelo WP29. Algo em comum, no entanto, é a existência de guias com critérios mais ou menos claros sobre qual o entendimento da autoridade sobre quais critérios devem ser usados para mensurar o risco dos incidentes de segurança.

As autoridades possuem, também, orientações em grau mais ou menos detalhado, qual a metodologia que será usada para essa avaliação de risco. Sugere-se que a escolha de uma metodologia padrão seja feita pela ANPD, para geral coerência e segurança jurídica aos regulados, e que essa escolha seja pública e de fácil acesso.

A análise da gravidade do risco é fundamental nesse processo todo, visto que a rapidez e precisão dessa avaliação permite uma resposta da agência com uma rapidez proporcional à severidade do caso - i.e., maior probabilidade e gravidade dos danos decorrentes do incidente de segurança.

Um interessante caso de estudo para análise é o Caso Equifax, birô de crédito, no qual ocorreu o vazamento de dados pessoais e financeiros de 145 milhões de estadunidenses, 8

tratamento se dar conforme o planejado e (ii) no caso de acontecer um incidente. No caso de um incidente de segurança que já aconteceu, há avaliação somente do risco resultante desse acontecimento.

[12] WP29, 2017

mil canadenses e 693 mil cidadãos do Reino Unido[13] no ano de 2017.[14] Dentre as informações divulgadas, estavam, além de documentos e informações pessoais, os números de cartão de crédito de 209 mil titulares. Uma das primeiras ações de mitigação de risco tomadas pela empresa foi a criação de um website com o objetivo de conscientização da população, de modo a evitar fraudes financeiras[15]. Apesar disso, diversos websites falsos foram criados na internet, na tentativa de propagar informações falsas e aplicar novos golpes na população afetada.[16] No próprio Twitter oficial da Equifax, foram divulgados, erroneamente, links que direcionam os consumidores a sites de *phishing*.[17] A falta de uma estratégia concreta de avaliação e mitigação dos riscos do vazamento, no primeiro momento, contribuiu para a confusão pública e perda de confiança no sistema quanto ao caso.

Devido à natureza e à dimensão do vazamento, a resposta ao caso foi feita de maneira multissetorial, com: (i) o envolvimento de todos os 50 Procuradores de Estado dos EUA para elaboração de acordo indenizatório no valor de 600 milhões de dólares[18]; (ii) a condução de investigações dos sistemas de segurança da Equifax pelas agências Internal Revenue Service (IRS), Social Security Administration (SSA) e U.S. Postal Service (USPS), que também adaptaram seus contratos para exigir notificações mais tempestivas em futuros casos de incidente e/ou encerraram contratos com a empresa; (iii) a condução de investigação administrativa pelo Bureau of Consumer Financial Protection e pela Federal Trade Comission (FTC)[19]; (iv) a participação ativa do Congresso Nacional que, além de realizar audiências para apuração e investigação do vazamento, propôs diversos Projetos de Lei de regulamentação do setor.[20]

Apesar do agravamento da gravidade do vazamento pela demora excessiva de notificação por parte da empresa, foi realizada uma cooperação efetiva entre diversas agências federais, junto ao legislativo, para tentar solucionar e mitigar os efeitos do vazamento com foco na proteção dos titulares de dados afetados.

No Brasil, a natureza e a complexidade de um incidente de segurança pode exigir uma

---

[13] Para compreender a utilização dos critérios de análise de gravidade de incidente de segurança em um caso concreto, é possível observar a decisão da ICO para aplicação de multa diante do Caso Equifax, no qual a Autoridade realizou uma apreciação gradual da gravidade do incidente. Nesse sentido, a ICO levou em conta: (i) volumetria de dados vazados; (ii) total de indivíduos atingidos; (iii) falta de medidas de segurança, como utilização de criptografia, segregação de network ou proteção de senhas dos usuários; (iv) tempo de disponibilidade indevida dos dados; (v) a falta de consciência dos sujeitos de dados de que seus dados eram objeto de tratamento pela Equifax; (vi) a natureza da atividade de tratamento; (vii) a natureza dos dados e a possibilidade de sua utilização para atividades fraudulentas; (viii) as consequências potenciais da utilização maliciosa dos dados; (vii) percepção pública do incidente, ou seja, capacidade do vazamento em ocasionar uma quebra de confiança no sistema financeiro como um todo. (ICO, 2018)

[14] THOMAS, 2019, p. 5.

[15] EQUIFAX, 2017

[16] ATLESON, 2019

[17] Técnica de engenharia social com o objetivo de enganar usuários e obter informações pessoais para fins fraudulentos (DEAHL, CARMAN, 2017).

[18] DEPARTAMENTO DE JUSTIÇA DE OREGON, 2019

[19] Agência governamental dos EUA que possui o objetivo de promover a defesa dos consumidores e promover a lei antitruste.

[20] GAO, 2018

rápida avaliação de riscos e danos a fim de criar medidas rápidas e efetivas de contingência, a depender da complexidade e natureza das informações comprometidas e a adoção de uma estratégia de cooperação entre demais órgãos regulatórios que tenham interesse na matéria, como Banco Central do Brasil, a Comissão de Valores Mobiliários, a Secretaria Nacional do Consumidor, o Ministério Público e, eventualmente, demais entes.

Isso nos leva a:

II. Dever de cooperação e dever de fiscalização e imposição de medidas sancionatórias

O caso do Equifax dá a dimensão da importância da cooperação com demais reguladores e da necessidade de articulação em diversos níveis da administração pública no caso de incidentes de segurança de alta complexidade.

Mesmo antes da LGPD entrar em vigor, o ordenamento jurídico brasileiro já estava permeado de normas (gerais e específicas) que estabeleciam mecanismos protetivos para os cidadãos quanto ao tratamento de seus dados,[21] por meio dos quais é possível "[...] vislumbrar a grande quantidade de órgãos e entidades públicos que potencialmente poderiam ser considerados competentes para atuar em casos concretos envolvendo o mau uso de dados pessoais" (WIMMER, 2020, p. 9). Wimmer destaca os órgãos de proteção e defesa do consumidor (em particular, os Procons e o Ministério Público), agências reguladoras e órgãos com competências normativas e sancionadoras em áreas como telecomunicações, saúde, mercado financeiro e educação.

Os casos de competência concorrente[22] acentuam-se ao se considerar a "[...] tendência de que também Estados e municípios adotem legislações referentes à proteção de dados pessoais, podem ainda existir órgãos competentes quanto ao tema em níveis estadual e municipal". (WIMMER, 2020, p. 9). Essa tensão, por fim, não se restringe aos sistemas

[21] "Os exemplos são inúmeros. O Código de Defesa do Consumidor (Lei 8.078, de 11 de setembro de 1990 – CDC) assegura o direito de acesso, pelos consumidores, a informações existentes em bases de dados e cadastros, estabelecendo, dentre outros direitos, o de retificação de informações inexatas. A Lei do Cadastro Positivo (Lei 12.414, de 9 de junho de 2011) dispõe de maneira detalhada sobre os direitos do cadastrado, incluindo os direitos de acesso a informações, de cancelamento do cadastro, de retificar informações errôneas, de ter seus dados pessoais utilizados somente para finalidade para a qual foram coletados, de revisão de decisão realizada exclusivamente por meios automatizadas e, ainda, de conhecer os principais elementos e critérios considerados para a análise de risco, resguardado o segredo empresarial. No campo da legislação setorial, a Lei Geral de Telecomunicações (Lei 9.472, de 16 de julho de 1997 – LGT) estabelece o direito do usuário de serviços de telecomunicações à inviolabilidade e ao segredo de sua comunicação, à não divulgação de seu código de acesso e ao respeito à sua privacidade nos documentos de cobrança e na utilização de seus dados pessoais pela prestadora do serviço. Na área da saúde, o Código de Ética Médica (Resolução 2.217/2018 do Conselho Federal de Medicina) regula o sigilo médico e assegura ao paciente o acesso ao seu prontuário e veda o seu fornecimento a terceiros, exceto mediante ordem judicial ou requisição pelos Conselhos Regionais de Medicina, autorização do paciente ou para a defesa do próprio médico. No que tange a dados custodiados pelo Poder Público, a Lei de Acesso à Informação (Lei 12.527, de 18 de novembro de 2011 – LAI) traz regras de proteção às informações pessoais, estabelecendo hipóteses de tratamento com e sem consentimento expresso do titular." (WIMMER, 2020, p. 21)

[22] "[...] casos concretos em que uma mesma conduta envolvendo o uso de dados pessoais seja considerada ilícita à luz de duas ou três normas simultaneamente" (WIMMER, 2020, p. 9)

normativos que cuidam de proteção de dados pessoais, mas pode ocorrer entre normas que objetivam proteger diferentes bens jurídicos, "[...] ensejando, eventualmente, decisões conflitantes entre órgãos públicos competentes para analisar um mesmo objeto a partir de distintos vetores interpretativos."[23] Isso demonstra como é fundamental o "[...] estabelecimento de relações permanentes entre tais órgãos, que se encontram submetidos a cadeias hierárquicas distintas, de modo a evitar que a ação de um deles obstaculize o desempenho das competências do outro".[24]

Concorda-se com a sugestão de Wimmer sobre como a ANPD deve proceder para evitar esses conflitos com outros órgãos reguladores:

> "Esse cenário complexo e fragmentado de *enforcement* requer a busca ativa por ferramentas hermenêuticas e por mecanismos de coordenação e articulação de competências, que podem ser construídos a partir da **definição de procedimentos e parâmetros para a fixação de competências primárias e secundárias no endereçamento de casos concretos**." (grifos nossos)[25]

A ICO, por exemplo, adotou essa prática de procedimentalizar a cooperação com outros órgãos: possui, em seu website, memorandos de entendimento com quarenta e cinco instituições, desde a Advocacia Geral da União até o Centro de Informações de Saúde e Assistência Social. Recomenda-se que **a ANPD constitua esses acordos com demais agências e órgãos reguladores que poderão, eventualmente, possuir competência concorrente ou complementar para lidar com um caso de incidente de segurança.**

Nesse mesmo sentido, **a ANPD deve, ao receber a notificação, realizar uma análise inicial sobre quem deve gerir o incidente**, avaliando e indicando se é o caso de competência própria ou competência concorrente ou complementar com quais outros reguladores. Como é feita essa avaliação inicial deve constar no guia de orientações aos regulados, mencionado no item anterior. Essa é uma das providências indicadas pelo Guia Nacional de Notificação e Gestão de Incidentes Cibernéticos da Espanha ("Guía Nacional de Notificación y Gestión de Ciberincidentes da Espanha"), publicado em 2020. Sempre que a agência responsável recebe uma notificação sobre um possível incidente cibernético, a equipe técnica realiza uma análise inicial que determinará se o caso é passível de ser gerido por ela mesma ou por um terceiro.[26] Esse ponto é fundamental para delimitar quem tem o dever de fiscalizar e, eventualmente, sancionar as práticas em questão. Em outras palavras, a cooperação entre reguladores produz uma fiscalização mais eficiente.

A cooperação vai além de uma solução ao problema de eventuais conflitos de competências: surge como uma medida para aprender com outros agentes reguladores que

---

[23] "Trata-se de situação de competências complementares, em que órgãos sem qualquer relação de hierarquia possuem competências coincidentes quanto ao objeto, mas distintas quanto às tarefas ou fins públicos perseguidos."(WIMMER, 2020, p. 10)
[24] WIMMER, 2020, p. 10
[25] WIMMER, 2020, p. 10
[26] ESPANHA, 2020, p. 24

têm maior experiência acumulada ao lidar com notificações de incidentes de segurança. Ou seja, **a determinação das ações necessárias a serem tomadas pela ANPD pode contar com a experiência de outras instituições que lidam há mais tempo com notificações de incidentes de segurança.** Por exemplo, o Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal (CTIR), que já possui diretrizes para lidar com incidentes. Parte do processo de tratamento de incidentes perpassa pela análise de incidentes, suporte à recuperação de incidentes, coordenação na resposta a incidentes, distribuição de alertas e cooperação com outras equipes de tratamento de incidentes. (Delimitado em documento "Padrões Para Notificação De Incidentes De Segurança ao Ctir Gov.")

Há, ainda, que se considerar e planejar como será a **cooperação com autoridades de proteção de dados internacionais** no caso do incidente de segurança envolver atores de fora do Brasil[27]. Como sintetiza Wimmer:

> "[...] uma vez que a LGPD pode produzir efeitos extraterritoriais semelhantes aos do Marco Civil da Internet, aplicando-se a pessoas naturais e jurídicas independentemente do país de sua sede ou do país onde estejam localizados os dados, uma condição crucial para que a legislação seja dotada de efetividade é que a ANPD se engaje ativamente em arranjos internacionais de cooperação para, ao mesmo tempo, simplificar os fluxos globais de dados e viabilizar o enforcement no caso de condutas ilícitas."[28]

Ou seja, em um caso de breach global, como a ANPD pode cooperar em nível internacional/entre agências?[29] É importante observar estruturas de cooperação internacional e diálogo entre Autoridades Nacionais de Proteção de Dados já existentes. Nesse sentido cita-se como exemplo a Red Iberoamericana de Protección de Datos (RIPD) e a Global Privacy Enforcement Network (GPEN).

Importa destacar que há estratégias de cooperação internacional entre Autoridades de Proteção de Dados organizadas por diferentes critérios, como a French-speaking

[27] "Dada a natureza global da chamada economia digital, um desafio importante a ser enfrentado pela ANPD diz respeito à cooperação internacional para enforcement quanto à proteção de dados pessoais e ao desenvolvimento de conceitos e standards comuns que permitam a interoperabilidade de marcos normativos em diferentes países. O estabelecimento de mecanismos de cooperação internacional quanto à proteção de dados pessoais é justificado não apenas em razão da necessidade de assegurar a proteção de direitos para além das fronteiras nacionais, mas também em vista da crescente importância econômica dos fluxos transnacionais de dados pessoais e da sua estreita relação com os fluxos globais de bens e serviços. (WIMMER, 2020, p. 7)

[28] WIMMER, 2020, p. 7

[29] "De fato, as dificuldades para a aplicação da lei em atividades envolvendo o fluxo transnacional de dados têm sido vivenciadas de maneira intensa no Brasil, especialmente em conexão com investigações criminais em que há necessidade de coleta de provas detidas por provedores de aplicações de Internet sediados em outros países. Os bloqueios de aplicativos de comunicação interpessoal por ordem judicial, ocorridos no Brasil em 2015 e 2016, tiveram como pano de fundo não apenas o debate acerca do uso de criptografia forte, mas também a discussão sobre o cumprimento de ordens judiciais brasileiras por empresas sediadas no exterior e, consequentemente, sobre a necessidade, ou não, de utilização de mecanismos de cooperação jurídica internacional para obtenção de elementos probatórios" (WIMMER, 2020, p. 7)

Association of Personal Data Protection Authorities (AFAPDP), conferência internacional que reúne membros de Autoridades de países que falam a língua francesa, ou como a Asia Pacific Privacy Forum (APPA), que reúne Autoridades territorialmente localizadas na região do pacífico asiático.

Observando especificamente a cooperação entre países localizados na América do Sul, é possível perceber que trocas têm sido realizadas pela Agencia de Acceso a la Información Pública (AAIP, Argentina) e pela Unidad Reguladora y de Control de Datos Personales (URCDP, Uruguai), com a elaboração de orientações conjuntas, como é o caso da publicação conjunta Guía de Evaluación de Impacto en la Protección de Datos.

Nesse sentido, é recomendável que a ANPD, em nível internacional, colabore com outras Autoridades não apenas para desenvolver respostas para incidentes de segurança em nível transnacional, mas também para estabelecer diretrizes, orientações e estratégias de cooperação que visem a garantia de um Sistema Internacional de Proteção de Dados. Sugere-se, ainda, que parcerias e colaborações nesse sentido busquem demais Autoridades de Proteção de Dados de países da América do Sul, fato que se justifica pela proximidade territorial, histórica e contextual a fim de estabelecer compreensões em comum da região quanto à formação de conhecimentos, políticas e estratégias de proteção de dados.

Bibliografia:

2017 Cybersecurity Incident & Important Consumer Information. *Equifax.* 2017. Disponível em: https://www.equifaxsecurity2017.com

ARTICLE 29 DATA PROTECTION WORKING PARTY - WP29. *Guidelines on Personal data breach notification under Regulation 2016/679.* 2017. Disponível em: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052>.

AAIP; URCDP. *Guía de Evaluación de Impacto en la Protección de Datos.* 2019. Disponível em: https://www.argentina.gob.ar/sites/default/files/guia_final.pdf.

ATLESON, Michael. *Equifax Data Breach:* Beware of Fake Settlement Websites. *Federal Trade Comission Consumer Information*. 2019. Disponível em: https://www.consumer.ftc.gov/blog/2019/07/equifax-data-breach-beware-fake-settlement-websites

DEAHL, Dani; CARMAN, Ashley. For weeks, Equifax customer service has been directing victims to a fake phishing site. *The Verge.* 2017. Disponível em: https://www.theverge.com/2017/9/20/16339612/equifax-tweet-wrong-website-phishing-identity-monitoring

ESPANHA, Guía Nacional de Notificación y Gestión de Ciberincidentes da Espanha. 2020. Disponível em:

https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf.

GAO - UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE. *Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach.* 2018. Disponível em: https://www.gao.gov/assets/gao-18-559.pdf

OAIC, D*ata breach preparation and response.* 2019. Disponível em: <https://www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response/>.

OREGON DEPARTMENT OF JUSTICE. *50 State Attorney Secure 600 Million from Equifax in the Largest Data Breach Settlement in History.* 2019. Disponível em: https://www.doj.state.or.us/media-home/news-media-releases/50-state-attorneys-general-secure-600-million-from-equifax-in-largest-data-breachsettlement-in-history/.

THOMAS, Jason. *A Case Study Analysis of the Equifax Data Breach.* 2019. Disponível em: https://www.researchgate.net/publication/337916068_A_Case_Study_Analysis_of_the_Equifax_Data_Breach_1_A_Case_Study_Analysis_of_the_Equifax_Data_Breach.

WIMMER, Miriam. *Os desafios de enforcement na LGPD:* fiscalização e aplicação de sanções administrativas e coordenação intergovernamental. In: MENDES, Laura Schertel et al (org.), *"Tratado de Proteção de Dados Pessoais"* (Forense, 2020).

WP29		ICO (UK)	CNIL (FR)		Agencia Española de Protección de Datos		Agencia de Acceso a la Información Pública (AAIP, Argentina) e pela Unidad Reguladora y de Control de Datos Personales (URCDP, Urugual)		Office of the Australian Information Commissioner	
O tipo de incidente		Menciona	Menciona como **identificação de possíveis ameaças.**		Não menciona		Não menciona		Menciona	
Descrição do critério	Exemplos dados:		Descrição	Exemplos	Descrição	Exemplos	Descrição	Exemplos	Descrição	Exemplos
Os incidentes de segurança são caracterizados em três categorias, quais sejam: Incidente de confidencialidade: quando ocorre uma divulgação não autorizada, divulgação acidental ou acesso indevido a dados pessoais. Incidente de integridade: quando ocorre uma alteração não autorizada ou acidental de dados pessoais. Incidente de disponibilidade: quando ocorre perda acidental ou não autorizada de acesso à dados pessoais ou destruição de dados pessoais.	Uma violação de confidencialidade pela qual as informações médicas foram divulgadas a partes não autorizadas pode ter um conjunto diferente de consequências para um indivíduo do que em uma violação na qual os dados médicos de um indivíduo foram perdidos e não estão mais disponíveis.	N/A	Em uma análise prévia ao incidente, a pergunta a ser feita para se avaliar o risco é: o que poderia permitir que cada evento temido ocorresse? Essas ameaças ocorrem por meio da mídia na qual os dados dependem (hardware, software, canais de comunicação, mídia de papel, etc.) que podem ser:	Uso de forma inadequada (ex .: abuso de direitos, erro de tratamento); Modificação (por exemplo: software ou hardware bloqueado - keylogger, instalação de software malicioso); Perda (por exemplo: roubo de laptop, perda de pen drive); Observação (ex .: visualização de uma tela em um trem, geolocalização de um equipamento); Danificação (por exemplo: vandalismo, degradação devido ao desgaste natural); Sobrecarregamento (por exemplo: meio de armazenamento completo, ataque de negação de serviço).	N/A	N/A	N/A	N/A	**Acesso não autorizado de dados pessoais:** ocorre quando as informações pessoais de uma entidade é acessado por alguém que não tem permissão para ter acesso. **Revelação não autorizada de dados pessoais:** ocorre quando a entidade, seja intencionalmente ou não, torna informações pessoais acessíveis ou visíveis a outros de fora da entidade e perde o controle dessa informação de maneira não permitida pela lei. **Perda:** perda acidental ou inadvertida de dados pessoais mantidos pela entidade, em circunstâncias em que seja provável que acarrete acessão não autorizado ou revelação de dados	**Acesso não autorizado:** - Acesso por pessoa não autorizada, funcionário da entidade ou autônomo *Ex: um emprego que acessa dados sensíveis de consumidores sem qualquer finalidade legítima* - Acesso não autorizado por terceiro externo (como por hacking) *Ex: uma rede de computadores que é comprometida por um ataque externo que resulta no acesso de informações sem autoridade para tal* **Revelação não autorizada:** - Quando o empregado de uma entidade acidentalmente publica um arquivo confidencial
A natureza, sensibilidade e volume dos dados pessoais		Menciona	Não menciona		Menciona como duas categorias distintas: **Natureza, Sensibilidade e Categorias dos dados pessoais afetados e Volume dos dados**		**Menciona**		Menciona	
Descrição do critério	Exemplos dados:		Descrição	Exemplos	Descrição	Exemplos	Descrição	Exemplos	Descrição	Exemplos
Geralmente, quanto mais sensíveis os dados, maior o risco de dano. No entanto é necessário atentar-se para outros tipos de dados pessoais que já estão disponíveis sobre o indivíduo. A divulgação de diversas categorias de dados pessoais geralmente é mais sensível do que uma única peça de dados pessoais. À primeira vista, alguns tipos de dados pessoais podem parecer relativamente inócuos, no entanto, o que esses dados podem revelar sobre o indivíduo afetado deve ser cuidadosamente considerado. Uma pequena quantidade de dados pessoais altamente confidenciais pode ter um grande impacto em um indivíduo, e uma grande variedade de detalhes pode revelar uma gama maior de informações sobre esse indivíduo. Uma violação que afeta grandes volumes de dados pessoais sobre muitos titulares de dados pode ter um efeito sobre um grande número correspondente de indivíduos.	Violações envolvendo dados de saúde, documentos de identidade ou dados financeiros, como detalhes de cartão de crédito, podem causar danos por si próprios, mas se usados juntos, podem ser usados para roubo de identidade. A divulgação do nome e endereço de um indivíduo em circunstâncias normais provavelmente não causará danos substanciais. No entanto, se o nome e o endereço de um pai adotivo forem revelados a um pai biológico, as consequências podem ser muito graves tanto para o pai adotivo quanto para o filho. Uma lista de clientes que aceitam entregas regulares pode não ser particularmente sensível, mas os mesmos dados sobre clientes que solicitaram que suas entregas fossem interrompidas durante as férias seriam informações úteis para os criminosos.	N/A	N/A	N/A	**Natureza, sensibilidade e categoria dos dados:** N/A **Volume:** Expressa por quantidade (registros, arquivos, documentos) e / ou períodos de tempo (uma semana, ano, etc.)	**Natureza, sensibilidade e categoria dos dados:** Sem nenhuma classificação do risco desses tipos de dados, a Agência apresenta uma lista exemplificativa de tipos de dados: Dados de baixo risco: detalhes de contato, educação, membros da família, profissional, biográfico Dados comportamentais: localização, trânsito, hábitos e preferências Dados financeiros: transações, ativos, receitas, contas, recibos Dados pessoais sensíveis: saúde, biométricos, dados relativos à vida sexual, etc. **Volume:** N/A.	N/A	N/A	**Natureza dos dados e sensibilidade:** Dados com maior potencial de causar dano severo ao titular na ocorrência de um incidente, dependendo do tipo ou tipos de dados que se tornaram vulneráveis. **Volume:** está localizada dentro do critério "quantos indivíduos estiveram envolvidos no incidente?"	**Natureza dos dados:** dados sensíveis como dados médicos, documentos utilizados para fraude de identidade como passaporte, carteira de motorista, informação financeira, etc. **Volume:** de uma perspectiva de análise de risco, seria prudente considerar que um incidente que envolva um número grande de pessoas pode causar dano efetivo a, pelo menos, um desses indivíduos, a não ser que o contexto ou circunstâncias não permitam essa conclusão. **Sensibilidade dos dados:**
Facilidade com que se consegue identificar os indivíduos		Menciona	Não menciona		Menciona como duas categorias distintas: **Facilidade de se Identificar os Indivíduos e Legibilidade do Dado**		Não menciona		Não menciona	
Descrição do critério	Exemplos dados:		Descrição	Exemplos	Definição	Exemplos	Definição	Exemplos	Descrição	Exemplos
Dependendo das circunstâncias, a identificação pode ser possível diretamente a partir dos dados pessoais violados, sem necessidade de pesquisa especial para descobrir a identidade do indivíduo, ou pode ser extremamente difícil combinar os dados pessoais com um determinado indivíduo, mas ainda pode ser possível sob certas condições. A identificação pode ser direta ou indiretamente possível a partir dos dados violados, mas também pode depender do contexto específico da violação e da disponibilidade pública de detalhes pessoais relacionados. Isso pode ser mais relevante para violações de confidencialidade e disponibilidade.	Os dados pessoais protegidos por um nível apropriado de criptografia serão inteligíveis para pessoas não autorizadas sem a chave de descriptografia. A pseudonimização devidamente implementada também pode reduzir a probabilidade de indivíduos serem identificados em caso de violação. No entanto, as técnicas de pseudonimização por si só não podem ser consideradas como tornando os dados ininteligíveis. A divulgação de dados pseudonimizados ou uma quebra de confidencialidade de dados protegidos por criptografia, apesar de não garantirem, de forma absoluta, a não identificação do indivíduo na situação concreta, podem reduzir a probabilidade de identificação do Titular no caso de um incidente.	Menciona	N/A	N/A	**Facilidade de se identificar os indivíduos**: Facilidade com que a identidade dos indivíduos pode ser deduzida dos dados envolvidos na violação. **Legibilidade do Dado:** dados protegidos por um sistema de pseudonimização	**Facilidade de se identificar os indivíduos:** : N/A **Legibilidade do Dado:** Criptografia ou hash	N/A	N/A	N/A	N/A
A severidade das consequências para os indivíduos		Menciona	Menciona como **identificação dos possíveis efeitos sobre os direitos e liberdades dos indivíduos em causa**		Menciona		Menciona		Menciona	
Descrição do critério	Exemplos dados:		Descrição	Exemplos	Definição	Exemplos	Definição	Exemplos	Descrição	Exemplos
Dependendo da natureza dos dados pessoais envolvidos em um incidente, o dano que potencial em relação aos indivíduos pode ser especialmente grave. Se a violação envolver dados pessoais sobre indivíduos vulneráveis, eles podem correr maior risco de danos. O fato de o controlador estar ciente de que os dados pessoais estão nas mãos de pessoas cujas intenções são desconhecidas ou possivelmente maliciosas pode ter influência no nível de risco potencial. Ou, ao contrário, o controlador pode ter um nível de garantia com o destinatário (relação de confiança) de modo que possa razoavelmente esperar que ele não leia ou acesse os dados enviados por engano e cumpra suas instruções para devolvê-los. Um destinatário confiável pode erradicar a gravidade das consequências da violação, podendo ser levado em consideração na avaliação de risco que o controlador realiza após a violação. Isso, porque, mesmo que os dados tenham sido acessados, o controlador ainda pode confiar no destinatário para não tomar nenhuma ação adicional com eles e para devolver os dados ao controlador prontamente e cooperar com sua recuperação. Ou seja, apesar da violação ter ocorrido (o controlador ainda deve manter as informações relativas à violação como parte do dever geral de manter registros de violações), um alto nível de confiança do destinatário pode remover a probabilidade de risco para os	Consequências especialmente graves: quando a violação puder resultar em roubo de identidade ou fraude, dano físico, sofrimento psicológico, humilhação ou danos à reputação. Além disso, quando o incidente de segurança envolver dados pessoais que revelem origem racial ou origem étnica, opinião política, religião ou crenças filosóficas, filiação em sindicatos, ou incluir dados genéticos, dados relativos à saúde ou dados relativos à vida sexual ou condenações criminais, é provável que acarrete dano severos às liberdades ou direitos dos indivíduos. Violação da confidencialidade, na qual os dados pessoais são divulgados a terceiros, conforme definido no artigo 4.º, n.º 10, ou a outro destinatário por engano. Isso pode ocorrer, por exemplo, quando dados pessoais são enviados acidentalmente para o departamento errado de uma organização ou para uma organização de fornecedor comumente usada. Nesses casos, o controlador pode solicitar ao destinatário que devolva ou destrua com segurança os dados que recebeu.	N/A	N/A	Identificar os efeitos potenciais sobre os direitos e liberdades dos indivíduos em causa, para os três seguintes eventos temidos: - acesso ilegítimo aos dados (ex .: roubo de identidade na sequência da divulgação de recibos de vencimento de todos os colaboradores de uma empresa); - modificação indesejada de dados (por exemplo: acusar indevidamente um indivíduo de um erro ou crime após a modificação de logs de acesso); - indisponibilidade temporária ou definitiva de dados (por exemplo: não detecção de interação medicamentosa devido à impossibilidade de acesso ao prontuário eletrônico do paciente).	Baixa: os indivíduos não serão afetados ou podem encontrar alguns inconvenientes que serão facilmente retificado Média: os indivíduos podem encontrar inconvenientes significativos, o que pode levar a outras dificuldades Alta: os indivíduos podem enfrentar consequências significativas, que só serão superadas com sérias dificuldades Muito alta: os indivíduos podem enfrentar consequências significativas, mesmo irreversíveis, que não podem superar	Baixa: Tempo necessário para inserir informações novamente, frustração, irritação etc. Média: Despesas adicionais, recusa de acesso a serviços comerciais, medo, falta de compreensão, estresse, pequenas queixas físicas, etc. Alta: Apropriação indébita de fundos, lista negra de bancos, danos à propriedade, perda de emprego, intimação judicial, agravamento da saúde, etc. Muito alta: exclusão social ou marginalização, dificuldades financeiras, como dívidas significativas ou incapacidade de trabalhar, doenças físicas ou psicológicas de longo prazo, morte, etc.	N/A	N/A	Análogo ao critério "natureza do dano"	Roubo de identidade Perda financeira significativa Ameaças à integridade física do indivíduo Perda de negócios ou oportunidades de emprego Humilhação, dano à reputação ou à relacionamentos Bullying social ou no local de trabalho Marginalização
Características especiais do indivíduo		Menciona	Não menciona		Menciona como duas categorias distintas: **Características especiais dos indivíduos** e **Perfi dos Usuários Afetados**		Menciona		Menciona	
Descrição do critério	Exemplos dados:		Descrição	Exemplos	Definição	Exemplos	Definição	Exemplos	Descrição	Exemplos
Uma violação pode afetar dados pessoais relativos a crianças ou outros indivíduos vulneráveis, que podem ser colocados em maior risco de perigo como resultado. Pode haver outros fatores sobre o indivíduo que podem afetar o nível de impacto da violação sobre ele.	N/A	N/A	N/A	N/A	**Características especiais dos indivíduos:** Se afeta pessoas com características especiais ou com necessidades especiais. **Perfil dos usuários afetados:** sua posição na estrutura organizacional da entidade e, portanto, seus privilégios de acesso a informações sensíveis ou confidenciais.	**Características especiais dos indivíduos:** N/A **Perfil dos usuários afetados:** N/A	Titular de dados em situação de especial vulnerabilidade.	Dados de pessoas que, em razão de sua idade, sexo, status físico ou mental, ou por circunstâncias sociais, econômica, étnica e / ou culturais estão mais vulneráveis a violações de direitos fundamentais.	Indivíduos que estão em situação de risco potencial ou de sério dano.	Mesmo que uma divulgação não autorizada de endereços possa não afetar algumas pessoas, na medida em que é bem possível que esses endereços já estejam até mesmo publicamente disponíveis, há pessoas especialmente vulneráveis para quem esse tipo de divulgação pode causar sério dano. Não há exemplificação no exemplo dado.
Características especiais do controlador		Menciona	Não menciona		Menciona,		Menciona		Menciona	
Descrição do critério	Exemplos dados:		Descrição	Exemplos	Definição	Exemplos	Definição	Exemplos	Descrição	Exemplos
A natureza e o papel do controlador, bem como suas atividades podem afetar o nível de risco para os indivíduos como um resultado de uma violação.	Uma organização médica processará categorias especiais de dados pessoais, o que significa que haverá uma ameaça maior aos indivíduos se seus dados pessoais forem violados, em comparação com uma lista de mala direta de um jornal.	N/A	N/A	N/A	Baseado nas atividades da entidade controladora.	N/A	Baseado nas atividades da entidade controladora.	Diferença por atividade. Dedica critério de avaliação de risco especial para as, por eles denominadas, tecnologias invasivas, quais sejam, o uso de "tecnologias que, em princípio, representariam riscos à privacidade ou aos direitos dos indivíduos devido à sua natureza ou extensão", como sistema de reconhecimento biométrico, videovigilância, uso de drones ou	Menciona de forma indireta, na medida em que realiza definições de análise de gravidade do incidente atreladas às atividades desempenhadas pelo controlador.	N/A
O número de indivíduos afetados		Menciona	Não menciona		Menciona		Menciona		Menciona	
Descrição do critério	Exemplos dados:		Descrição	Exemplos	Definição	Exemplos	Definição	Exemplos	Descrição	Exemplos
Uma violação pode afetar apenas um ou alguns indivíduos ou vários milhares, se não muitos mais. Geralmente, quanto maior o número de indivíduos afetados, maior o impacto de uma violação. No entanto, uma violação pode ter um impacto grave até mesmo em um indivíduo, dependendo da natureza dos dados pessoais e do contexto em que foram comprometidos. Novamente, a chave é considerar a probabilidade e a gravidade do impacto sobre as pessoas afetadas.	N/A	N/A	N/A	N/A	N/A	Em uma escala definida; por exemplo, mais de 100 indivíduos.	Há operações de tratamento que, quando avaliadas individualmente, não são relevantes mas que a análise do agregado de dados pessoais pode criar risco significativo para direitos fundamentais e liberdades dos titulares.	Em uma escala definida em comparação proporcional com a população do país. Apesar de não apresentar o critério de forma absoluta, exemplifica com número de indivíduos maior a 1% da população do país.	Mesmo se o agente considerar, inicialmente, que a gravidade do incidente de segurança ocorrido é baixa, uma análise de risco apropriada deve levar em conta que, caso haja um grande número de indivíduos afetados, é capaz que o incidente ocasione risco sério a, pelo menos, um dos indivíduos, a não ser que as circunstâncias materiais e o contexto do caso provem o contrário.	N/A
Comentários Gerais										
Ao avaliar o risco que provavelmente resultará de uma violação, o controlador deve considerar uma combinação da gravidade do impacto potencial sobre os direitos e liberdades dos indivíduos e a probabilidade de ocorrerem. Claramente, onde as consequências de uma violação são mais graves, o risco é maior e, da mesma forma, onde a probabilidade de isso ocorrer é maior, o risco também é elevado. Em caso de dúvida, o controlador deve errar por cautela e notificar.		A ICO segue precisamente todos os critérios delineados pela WP 29, visto que em seu guia, indica a seção IV Guia sobre Notificação de Incidentes de Segurança para maiores esclarecimentos. De maneira geral, assim como recomenda a WP 29, fica claro que o critério geral é severidade do risco e probabilidade: "[...] ao tomar conhecimento de uma violação, você deve contê-la e avaliar as possíveis consequências adversas para os indivíduos, com base em quão sérias ou substanciais são e na probabilidade de acontecerem". A severidade do dano é diferenciada de inconveniências, apontando para uma avaliação sempre casuística: "uma violação pode ter uma série de efeitos adversos sobre os indivíduos, que incluem sofrimento emocional e danos físicos e materiais. Algumas violações de dados pessoais não acarretarão riscos além da possível inconveniência para aqueles que precisam dos dados para realizar seu trabalho. Outras violações podem afetar significativamente os indivíduos cujos dados pessoais foram comprometidos. Você precisa avaliar isso caso a caso, observando todos os fatores relevantes."	O documento francês cuida das análises de avaliação de risco prévias à concretização de um incidente de segurança, ou seja, é um guia de prevenção. Por isso, muitas das categorias não estão expressamente presentes, priorizando fatores como identificação das fontes de riscos (quem ou o que poderia ser a causa de cada evento temido, levando em consideração fontes humanas internas e externas (por exemplo: o administrador de TI, o usuário, atacante externo, concorrente) e não humanas internas e externas fontes (por exemplo: água, materiais perigosos, computador não direcionado vírus)) e determinação das medidas existentes ou planejadas. No entanto, **ainda que nesse exercício de prevenção, a autoridade francesa deixa claro que é necessário avaliar a gravidade e probabilidade dos riscos, em relação aos critérios elencados.** O processo de avaliação prévia é sintetizado por uma tabela auto-explicativa de classificação dos riscos conforme os critérios elencados pela autoridade. (página 3 do documento)	A Agência de Proteção de dado Espanhola apresenta uma categorização genérica do risco em si antes de elencar os critérios da lista acima: > Crítico (afeta dados valiosos, grandes volumes e em pouco tempo) > Muito alto (quando existe o potencial de afetar uma quantidade significativa de informações valiosas) > Alta (quando há potencial para afetar informações valiosas) > Médio (quando existe o potencial de afetar uma quantidade significativa de informações) > Baixo (limitado ou nenhum potencial para afetar uma quantidade significativa de informações). Essa classificação genérica parece dar prioridade ao volume e à sensibilidade dos dados afetados no ncidente. **Critérios Específicos Adicionais:** > Número e classificação dos sistemas afetados (sem definição/ exemplos) > O impacto que a violação pode ter na organização, do ponto de vista da proteção da informação, prestação de serviços, conformidade legal e / ou imagem pública. Isso estará relacionado à categoria ou criticidade dos serviços e indivíduos afetados: (Baixo (dano limitado), Médio (dano grave), Alto (dano muito grave)).	As Autoridades de Control de la República Oriental del Uruguay y de la República Argentina divulgaram o referido guia para elaboração de Evaluación de Impacto en la Protección de Datos, mecanismo similar ao Relatório de Impacto à Proteção de Dados (RIPD - art. 5º, XVII) da LGPD. Apesar de não estabelecer critérios específicos para avaliação de **dano**, com preventivo na avaliação de risco, o Relatório é um importante instrumento de colaboração de Autoridades da América Latina sobre a interpretação de conceitos comuns a ambas análises, o que justifica a apresentação de seus critérios e referências na tabela. No guia, as Autoridades consideram que, para a elaboração de Relatório de Impacto à Proteção de Dados Pessoais, deve ser realizada um matriz que compreende Risco		A Comissão utiliza um critério interessante para avaliação da gravidade do incidente, não presente nas outras análises realizadas de forma tão explícita: Compreensão de por quanto tempo a informação esteve acessível, que contabilize o tempo entre a ocorrência do incidente e a ciência do incidente pelo agente de tratamento. Esse tipo de análise de critério possibilita a compreensão do **tempo de vulnerabilidade** causado pelo incidente.

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: DATABLOCK PROTEÇAO DE DADOS LTDA

CPF/CNPJ: 37.887.024/0001-14

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS

IMPORTANTE: Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.

TÓPICO/QUESTÃO	CONTRIBUIÇÃO/INSTITUIÇÃO
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	Em primeiro lugar, é necessário definir de forma separada o "dano" e o "risco". O "dano" é algo presente, palpável e estimável. É sofrido pelo titular e/ou pelo agente de tratamento. O dano pode ser de diversa consideração, dependendo das características intrínsecas do indivíduo/entidade que o sofre. Entretanto, a materialização do dano pode dar-se em diferentes situações cotidianas, que de forma geral, afeta a todos de uma maneira incontestável. Neste sentido, entre os tratamentos com potencial para gerar danos relevantes para os direitos e liberdades dos indivíduos (titulares) podemos mencionar aqueles que possam impedir o titular de exercer algum direito, utilizar um serviço ou de firmar um contrato, ou aqueles que se realizem de maneira continuada a larga escala. Com relação ao "risco", este é futuro, impalpável, porém estimável. É algo que se pode prever, mas cujos efeitos ainda não se materializaram. O risco é sofrido pelo agente de tratamento, não pelo titular. Para a estimação do risco devem ser considerados alguns fatores específicos e predeterminados, de forma que sua graduação seja feita com base nos mesmos critérios para todos os agentes de tratamento. A estimação do dano deve ser um dos critérios adotados para a classificação do risco. Nosso entendimento é que os critérios que devem ser considerados pela ANPD para avaliar o risco que implica um tratamento de dados deve estar baseado no impacto causado pelo incidente e na probabilidade de que ocorra. Similar é o entendimento da Agencia Espanhola de Proteção de Dados, "AEPD" (expressado em sua "*Guia para a gestión y notificación de brechas de seguridad*", disponível no seguinte link: https://www.aepd.es/sites/default/files/2019-09/guia-brechas-seguridad.pdf). Segundo a AEPD, este impacto pode ser avaliado de acordo com os seguintes fatores: A. Categoria ou nível de criticidade da segurança dos sistemas afetados. Podemos distingui-la entre:

	a. Crítico: afeta dados de alto valor, alto volume e em pouco tempo; b. Relevante: tem capacidade de afetar dados de alto valor, em alto volume; c. Alto: tem capacidade de afetar dados de alto valor; d. Médio: tem capacidade de afetar um volume considerável de dados; e. Baixo: escassa ou nula capacidade de afetar um volume considerável de dados. B. Natureza, sensibilidade e categoria de dados pessoais afetados: • Dados de escasso risco: dados de contato, acadêmicos, familiar, profissionais e biográficos. • Dados de comportamento: localização, tráfico, hábitos e preferencias. • Dados financeiros: transações, posições, ingressos, contas, notas fiscais. • Dados sensíveis: de saúde, biométricos, relativos à vida sexual etc. C. Dados legíveis / ilegíveis: dados protegidos mediante algum sistema de anonimização ou criptografia. D. Volume de dados pessoais: apontado em quantidades (registros, arquivos, documentos) e/ou em períodos de tempo (uma semana, um ano, etc.) E. Facilidade de identificação de titulares: facilidade de identificação dos titulares a partir dos dados envolvidos no incidente. F. Severidade das consequências para os titulares: a. Baixa: Dano moral escasso ou inexistente (perda de tempo na recuperação da informação, irritação). b. Média: Dano moral relativo (medo, estresse) e dano econômico relativo (custos adicionais). c. Relevante: Dano moral alto, porém superável (impedir o titular de exercer algum direito, utilizar um serviço ou de firmar um contrato, malversação de fundos, negativação do nome, danos à propriedade, perda de emprego, citação judicial, adoecimento). d. Extrema: Dano moral e/ou econômico alto e irreversível (exclusão ou marginalização social, dívidas altas, incapacidade para trabalhar, doenças psicológicas ou físicas a longo prazo, morte) G. Características relevantes dos titulares: afetação de titulares especialmente vulneráveis (pessoas idosas, menores de idade, analfabetos). H. Número de titulares afetados: I. Características relevantes do controlador dos dados: baseando-se em sua atividade (hospital, escola, empresa). J. Número e tipo de sistemas afetados:

K. Impacto que o incidente pode ocasionar na empresa, desde o ponto de vista da proteção da informação, a prestação dos serviços, o cumprimento legal e /ou a imagem pública. Está relacionado com a categoria ou criticidade dos serviços e pessoas afetados.

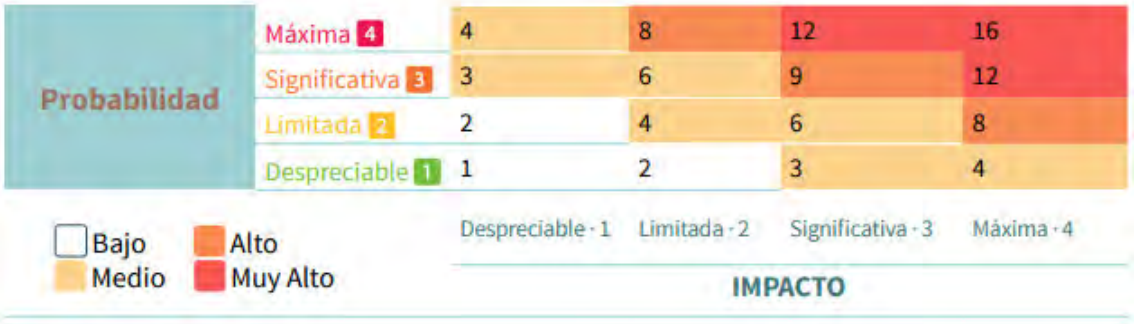
   a. Baixo: prejuízo limitado
   b. Médio: prejuízo grave
   c. Alto: prejuízo extremo

L. Requerimentos legais e regulatórios: notificação do incidente a ANPD e qualquer outra obrigação de notificação ou comunicação à Polícia ou Poder Judicial em caso de delito.

Todos estes requisitos devem ser avaliados conjuntamente para determinar o impacto causado por um incidente de segurança e, uma vez verificado o impacto, passaremos a calcular a probabilidade de sua ocorrência. Assim reza o Considerando 76 do Regulamento Europeu Geral de Proteção de Dados 679/2018 ("GDPR"):

"*A probabilidade e gravidade do risco aos direitos e liberdades do titular devem ser determinadas baseando-se na natureza, âmbito, contexto e objetivos do tratamento de dados. O risco deve ser ponderado com base em uma avaliação objetiva, na qual é determinado se as operações de tratamento de dados representam um risco ou se o risco é alto*."

A Agência Espanhola de Proteção de Dados (em sua "*Guia práctica de análisis de riesgos em los tratamientos de datos personales sujetos al RGPD*", disponível no seguinte link: https://www.aepd.es/sites/default/files/2019-09/guia-analisis-de-riesgos-rgpd.pdf) interpreta a questão a través da seguinte tabela de correlação entre impacto X probabilidade:



O Anexo 6.1. da mencionada Guia traz uma planilha modelo de análise da necessidade de realização de avaliação de impacto por parte dos agentes. Esta planilha avalia diferentes aspectos do tratamento de dados como: tipos de dados tratados, finalidades do tratamento, tecnologias utilizadas, compartilhamentos e transferências internacionais de dados, entre outros. Trata-se de um

	documento acessível e intuitivo, para que os agentes possam determinar se os tratamentos realizados por ele podem gerar riscos relevantes para os titulares, caso em que estariam, então, obrigados a realizar uma segunda avaliação mais extensiva: o relatório de impacto à proteção de dados.
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	Conforme identificado na pergunta anterior, as categorias do dano para o titular dos dados podem subdividir-se em: a. Baixa: Dano moral escasso ou inexistente (perda de tempo na recuperação da informação, irritação). b. Média: Dano moral relativo (medo, estresse) e dano econômico relativo (custos adicionais). c. Relevante: Dano moral alto, porém superável (impedir o titular de exercer algum direito, utilizar um serviço ou de firmar um contrato, malversação de fundos, negativação do nome, danos à propriedade, perda de emprego, citação judicial, adoecimento). d. Extrema: Dano moral e/ou econômico alto e irreversível (exclusão ou marginalização social, dívidas altas, incapacidade para trabalhar, doenças psicológicas ou físicas a longo prazo, morte). Por sua vez, o risco deverá ser avaliado baseando-se no impacto que o incidente de segurança pode gerar para os direitos e liberdades dos titulares dos dados (conforme os critérios explanados na pergunta anterior) e a probabilidade de que ocorra. Em outras palavras, para determinar o risco de materialização de um incidente, o fator "impacto" deverá ser avaliado juntamente ao fator "probabilidade", já que quando a probabilidade da materialização de um incidente é ínfima, por mais que seu impacto potencial seja extremo, sua ocorrência resultaria em um risco médio. Outrossim, outros fatores, como a existência de medidas de contenção e planos de gerenciamento de incidentes robustos, minimizariam o impacto e a probabilidade da materialização de um risco. Todos estes fatores devem ser avaliados pelo agente de tratamento no contexto de sua política de governança de dados, especificamente no momento de elaborar o relatório de impacto a proteção de dados.
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	Como expusemos anteriormente, o dano é do titular ou do agente, porém o risco é exclusivamente do agente de tratamento. Em outras palavras, o dano se relaciona aos prejuízos econômicos ou morais que o titular possa sofrer em decorrência de um incidente de segurança que envolvam seus dados pessoais. Já o risco é a correlação entre o impacto que um incidente de segurança pode gerar para o agente ou para o titular do dado e a probabilidade de sua ocorrência.
O que deve ser considerado na avaliação dos riscos do incidente?	A AEPD, na "*Guia práctica de análisis de riesgos em los tratamientos de datos personales sujetos al RGPD*" disponível no seguinte link: https://www.aepd.es/sites/default/files/2019-09/guia-analisis-de-riesgos-rgpd.pdf , pontuou o seguinte:

	"*Avaliar um risco envolve considerar todos os cenários possíveis em que o risco poderia se materializar. A avaliação do risco consiste em avaliar o impacto da exposição à ameaça, juntamente com a probabilidade de que se concretize. O impacto, por sua vez, é determinado com base nos possíveis danos que podem ocorrer caso a ameaça se materialize, por exemplo, um impacto seria insignificante se não tivesse consequências para o titular ou, por outro lado, um impacto seria significativo se os danos causados aos direitos e liberdades do titular fossem críticos. De acordo com a probabilidade e o impacto, associados às ameaças, é possível determinar o nível de risco inerente*".
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	Nossa sugestão é de que os controladores notifiquem também a natureza do incidente: roubo de informação física, ataques informáticos (vírus, scripts, DoS), desastres naturais (inundação, incêndio), incumprimento normativo, etc. e, ademais das informações sobre os titulares envolvidos, também, quando seja possível, o número aproximado de titulares afetados. Esta informação ajudará a ANPD a mapear, qualificar e quantificar os tipos de incidentes de segurança, favorecendo o direcionamento de suas atividades educativas e preventivas no âmbito da segurança da informação. Além disso, a coleta desta informação pode facilitar a colaboração da ANPD com outros entes públicos relacionados à segurança da informação para a concretização de ações conjuntas contra o cybercrime e a promoção de iniciativas de fomento da segurança da informação. Finalmente, entendemos ser importante que seja comunicado o nome e os dados de contato do Encarregado pelo tratamento para que este possa atuar conjuntamente ao controlador e a ANPD na adoção das medidas e providências que sejam necessárias para a resolução do incidente.
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	Acreditamos que um prazo de 72hs seja razoável. Entretanto, nossa sugestão é que a ANPD possibilite o controlador realizar retificações e complementações na informação previamente fornecida. Assim prevê o RGPD em seu art. 33.4: "*Se não for possível fornecer as informações simultaneamente, as informações serão fornecidas gradualmente, sem atrasos indevidos*.". Aproveitamos para fazer uma reflexão sobre o sujeito desta obrigatoriedade de informar a ANPD. A LGPD direciona esta obrigação exclusivamente ao controlador, isentando o operador de dita responsabilidade. Entretanto, entendemos que o operador, como agente de tratamento, e, sendo ele muitas vezes o responsável direto do incidente de segurança, é quem estaria mais preparado, em determinadas situações, para informar a ANPD sobre as características do ocorrido. Portanto, entendemos que seria justo e razoável que também o operador deva arcar com esta obrigatoriedade quando seja responsável direto pelo incidente. Neste caso, se verificado o cumprimento íntegro da normativa de proteção de dados por parte do controlador, com a implantação de medidas pertinentes e eficazes de segurança técnicas e organizativas, este poderia isentar-se ou minimizar sua responsabilidade com relação ao incidente. Para ilustrar esta hipótese, poderíamos dar o exemplo de uma empresa (controladora) que utiliza os serviços de um provedor de

	armazenamento de dados na nuvem (operador). Fazendo uma leitura atual da LGPD, mesmo que o incidente houvesse ocorrido nos sistemas do provedor, a obrigação de comunicar a ANPD seria da empresa. Em casos como estes, se o operador não for capaz de informar o controlador em tempo sobre o incidente, é possível que o controlador não possa cumprir o prazo estabelecido para realizar a comunicação à ANPD por falta de informação sobre o incidente, deixando-o de mãos atadas.
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	A comunicação aos titulares é uma obrigação legal que pode gerar prejuízos consideráveis para a reputação de uma entidade, e que, portanto, deve ser avaliada com cautela e exigida somente em determinadas situações (situações objetivas), em que o controlador não possa reverter os efeitos do incidente e em que o dano potencial seja relevante. O prazo para a realização desta notificação deve ser flexível para que o controlador possa dispor de toda informação necessária para informar devidamente os titulares. A informação deverá ser fornecida em linguagem acessível, sem terminologias técnicas, por meio de uma descrição geral do incidente e dos dados afetados. Acreditamos que as informações arroladas no §1º do art. 48 da LGPD sejam suficientes. Informações como a natureza do incidente e o número de afetados (que indicamos como informação a ser adicionada à notificação à ANPD) não devem ser comunicadas aos titulares sob pena de causar dano desnecessário à imagem da entidade.
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	A comunicação pública deve ser admitida quando o número de titulares afetados é elevado ou quando suponha um esforço econômico desproporcional ao controlador. Este é, também, o entendimento do legislador europeu: *Art. 34, RGPD: Comunicação de um incidente envolvendo dados pessoais ao titular dos dados.* *1. Quando incidente envolvendo dados pessoais for suscetível de implicar um elevado risco para os direitos e liberdades dos titulares, o controlador comunicará o incidente ao titular dos dados sem demora injustificada.* *2. A comunicação ao titular dos dados a que se refere o nº 1 do presente artigo descreve em linguagem clara e simples a natureza do incidente e fornecerá, pelo menos, as informações e medidas previstas no artigo 33.o, nº 3, alíneas b), c) e d).* *3. A comunicação ao titular dos dados a que se refere o nº 1 não é exigida se for preenchida uma das seguintes condições:* *a) O controlador tiver aplicado medidas de proteção adequadas, tanto técnicas como organizativas, e essas medidas tiverem sido aplicadas aos dados pessoais afetados pelo incidente, especialmente medidas que tornem os dados pessoais incompreensíveis para qualquer pessoa não autorizada a aceder a esses dados, tais como a cifragem;* *b) controlador tiver tomado medidas subsequentes que assegurem que o elevado risco para os direitos e liberdades dos titulares dos dados a que se refere o nº 1 já não é suscetível de se concretizar; ou* *c)* ***Implicar um esforço desproporcionado. Nesse caso, poderá ser feita uma comunicação pública ou tomada uma medida semelhante através da qual os titulares dos dados são informados de forma igualmente eficaz.***

	4. Se o responsável pelo tratamento não tiver já comunicado a violação de dados pessoais ao titular dos dados, a autoridade de controle, tendo considerado a probabilidade de o incidente resultar num elevado risco, pode exigir-lhe que proceda a essa notificação ou pode constatar que se encontram preenchidas as condições referidas no nº 3.
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	O controlador estaria isento da obrigatoriedade de informar a ANPD quando, cumulativamente: (i) o incidente afete somente um número limitado de titulares; (ii) os dados envolvidos no incidente não sejam considerados dados sensíveis; (iii) os dados envolvidos no incidente não sejam referentes a pessoas especialmente vulneráveis (consumidores, crianças e adolescentes, idosas) e; (iv) o risco de que o dano se materialize tenha sido mitigado pela adoção de medidas técnicas adequadas.
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	O controlador estaria isento da obrigatoriedade de informar os titulares quando: (i) o incidente não seja passível de causar dano relevante aos direitos e liberdades dos titulares dos dados; (ii) o controlador adote medidas de proteção técnica e organizacional adequadas para proteger aos dados pessoais afetados, em particular aqueles que tornam os dados pessoais ininteligíveis para quem não está autorizado a acessá-los, como criptografia e; (iii) o controlador tome medidas adicionais para garantir que não haja mais qualquer probabilidade de concretização de risco relevante para os direitos e liberdades dos titulares.
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	A gravidade do incidente deve estar intrinsecamente relacionada como o dano que pode causar aos titulares. Desta forma, entendemos que o primeiro critério a ser adotado é este: o dano potencial aos titulares. Entretanto, existem outros fatores que também deverão ser analisados, como: (i) o tipo de incidente; (ii) a duração do incidente (iii) a natureza dos dados pessoais afetados (dados sensíveis, dados relacionados a pessoas especialmente vulneráveis); (iv) o volume dos dados pessoais afetados; (v) as características específicas do controlador (se é uma escola, hospital, um ente público); (vi) a culpabilidade do controlador ou do operador;

	(vii) reincidência; (viii) as medidas adotadas pelo controlador/operador para paliar os efeitos do incidente; (ix) o grau de maturidade do plano de governança de dados do controlador/operador, com avaliação das medidas técnicas e organizativas que estavam implementadas no momento do incidente; (x) O correto cumprimento dos deveres de notificação à ANPD e aos titulares por parte do controlador/operador; (xi) O grau de cooperação do controlador/operador com a ANPD e com os titulares para solucionar o incidente e mitigar os danos; (xii) Qualquer outro fator agravante da responsabilidade do controlador/operador, como verificação, direta ou indireta de obtenção de lucros ou a minimização de perdas em decorrência do incidente. **Recomendamos a leitura do documento "*Guidelines on Personal data breach notification under Regulation 2016/679*", disponível no seguinte link:** https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	Ao nosso ver, a gravidade de um incidente de segurança depende de vários fatores (como os expostos na pergunta anterior) que deverão ser analisados caso por caso. O estabelecimento de uma metodologia excessivamente restrita e inflexível poderia dar lugar a incorreções e injustiças. Não é do nosso conhecimento neste momento nenhuma metodologia adequada para a análise de gravidade de um incidente de segurança.
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	Independentemente da obrigatoriedade do incidente ser ou não notificado à ANPD, o controlador deverá documentar o ocorrido, registrando detalhes como a causa, as consequências e o tipo de dados pessoais afetados, bem como as medidas corretivas adotadas. Além desses detalhes, é recomendável que o controlador documente o processo de tomada de decisões realizadas durante este período e suas justificativas, especialmente quando o controlador considere que um determinado incidente não é passível de causar dano ou risco relevante aos titulares. Esta informação poderá ser necessária para avaliar posteriormente uma eventual sanção por incumprimento do dever de notificar a ANPD ou os titulares.
SUGESTÃO DE NORMATIVO, SE HOUVER	

Art. 33 do GDPR sobre notificações de incidentes de segurança à autoridade de controle
Art. 34 do GDPR sobre notificações de incidentes de segurança aos titulares de dados

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DAS INSTITUIÇÕES: DaVita Brasil Participações e Serviços de Nefrologia Ltda. e Davita Healthcare Brasil Serviços Médicos LTDA.

CNPJs: 23.097.104/0001-61 e 27.072.564/0001-96

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS **IMPORTANTE:** Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
1. Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	Para melhor responder a essa pergunta, entendemos ser relevante que essa Autoridade (i) considere as definições já previstas pelo ordenamento jurídico brasileiro para "risco" e "dano", pois, como se sabe, é necessário que haja unicidade e coerência entre os conceitos estabelecidos nas diferentes áreas do direito interno, para que a interpretação legal não sofra variações e para que haja isonomia na aplicação das leis nacionais; e (ii) observe a experiência internacional, como a da União Europeia com a implementação do Regulamento (UE) 2016/679 (Regulamento Geral de Proteção de Dados Pessoais – "GDPR"). Na legislação brasileira, **dano** é qualquer lesão a bem legalmente protegido, que gere prejuízo patrimonial ou moral ao titular. O Art. 186 do Código Civil dispõe que "*Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito*.". **Para que o dano seja indenizável, ele deve ser concreto e deve haver nexo de causalidade, isto é, uma conexão entre a causa e os resultados, de forma que resulte diretamente da ação ou omissão, negligência ou imprudência do agente causador**. Alinhada a esse conceito de dano, a Lei Federal Nº 13,709/18 (Lei Geral de Proteção de Dados ou "LGPD") prevê em seu Art. 48 que "*O controlador deverá comunicar à autoridade nacional e ao **titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante** aos titulares*." Portanto, não é qualquer evento que cause (ou tenha o potencial de causar) danos que

	gerará a obrigação de notificação prevista pelo dispositivo em questão, mas sim o evento que realmente cause (ou tenha o potencial de causar) um dano concreto e relevante à pessoa em questão. Essa é a linha de raciocínio que vem sendo adotada por outras agências reguladoras no Brasil. Por exemplo, o Art. 35-C, §1º da Instrução CVM 612/2019 da Comissão de Valores Mobiliários ("CVM") dispõe que "*O intermediário deve, tempestivamente, comunicar à SMI e aos órgãos de administração a ocorrência de incidentes relevantes que afetem seus sistemas críticos e* ***tenham impacto significativo sobre os clientes***." Assim, no âmbito da CVM, para fins de notificação, o incidente não deve apenas afetar os sistemas críticos, mas também ter um impacto significativo aos clientes. Isso ocorre porque, nas atividades habituais dos agentes de tratamento de dados, uma série de eventos atípicos e inesperados podem ocorrer. No entanto, nem todos esses eventos geram (ou podem gerar) dano significativo a direitos de terceiros. Assim, para que haja a obrigação de notificar, nos termos do Art. 48.º da LGPD, o incidente deve apresentar o risco de causar, em termos concretos, danos relevantes e duradouros aos titulares dos dados. **Risco**, por sua vez, é um evento futuro e incerto que pode causar danos relevantes aos titulares dos dados. Nesse sentido, uma definição semelhante de risco é encontrada em âmbito nacional. A Portaria nº 42/2019, que estabelece a Política de Gestão de Riscos e Controles Internos (PGRCI) da Agência Nacional do Petróleo, Gás Natural e Biocombustíveis (ANP) define, em seu Art. 2, X, que "*risco: é um evento interno ou externo cuja ocorrência possa causar impacto no cumprimento dos objetivos organizacionais; um evento de risco pode decorrer de um ou mais elementos e ter origem advinda de fontes associadas a pessoas, eventos externos, tecnologia, processos, sistemas ou infraestrutura física/organizacional, ou então ser decorrente de outro evento de risco, caracterizando um encadeamento de riscos*". Tal disposição está em consonância com o disposto nos Considerandos 75 e 76 do GDPR, que estabelecem que, para analisar o risco de um incidente, devem ser avaliados dois fatores: (i) a probabilidade de o evento ocorrer e (ii) a gravidade do dano, caso se concretize. Essa análise deve observar critérios objetivos que levem em consideração a natureza, o escopo, o contexto e os objetivos do tratamento de dados pessoais, conforme pode ser observado abaixo: (75) "*O risco para os direitos e liberdades das pessoas naturais, cuja* ***probabilidade*** *e* ***gravidade*** *podem ser variáveis, poderá resultar de operações de tratamento de dados pessoais* ***suscetíveis de***

	***causar danos físicos, materiais ou imateriais**, em especial: quando o tratamento possa dar origem à discriminação, roubo da identidade ou fraude, a perdas financeiras, prejuízos para a reputação, perdas de confidencialidade de dados pessoais protegidos por sigilo profissional, à inversão não autorizada da pseudonimização, ou a quaisquer outros prejuízos importantes de natureza econômica ou social; quando os titulares dos dados possam ficar privados dos seus direitos e liberdades ou impedidos de exercerem o controle sobre os seus dados pessoais; quando forem tratados dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas e a filiação sindical, bem como dados genéticos ou dados relativos à saúde ou à vida sexual ou a condenações criminais e infrações ou medidas de segurança conexas; quando forem avaliados aspectos de natureza pessoal, em particular análises ou previsões de aspectos que digam respeito ao desempenho no trabalho, à situação econômica, à saúde, às preferências ou interesses pessoais, à confiabilidade ou comportamento e à localização ou às deslocações das pessoas, a fim de definir ou fazer uso de perfis; quando forem tratados dados pessoais relativos a pessoas naturais vulneráveis, em particular crianças; ou quando o tratamento incidir sobre uma grande quantidade de dados pessoais e afetar um grande número de titulares de dados*." (76) "*A probabilidade e a gravidade dos riscos para os direitos e liberdades do titular dos dados deverão ser determinadas com base na **natureza, âmbito, contexto e finalidades do tratamento de dados**. Os riscos deverão ser aferidos com base numa avaliação objetiva, que determine se as operações de tratamento de dados implicam risco ou risco elevado*." **Dessa forma, pode-se inferir que tanto o direito brasileiro como a lei europeia estipulam que risco é qualquer evento futuro e incerto que tenha potencial para causar danos físicos, materiais e imateriais aos titulares de dados. Já quanto ao dano, este é um resultado advindo diretamente da ação ou omissão do agente causador, e que efetivamente causa prejuízos relevantes aos titulares.** Assim, entende-se que seria importante que a ANPD adotasse definição semelhante, no sentido de que o incidente que causar (ou puder causar) dano relevante aos titulares dos dados deve gerar a obrigação de notificação. Para determinar se um risco ou dano é relevante, devem ser observando critérios objetivos que levem em consideração a natureza, âmbito, contexto e finalidades do tratamento de dados pessoais e do incidente, conforme descrito nas respostas às perguntas 4 e 11 abaixo**.**

2. O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	Entendemos que a subdivisão em categorias seria benéfica para que os controladores responsáveis pelo incidente de vazamento tenham maior facilidade para identificar em quais ocasiões o incidente ensejará a obrigação de notificar a ANPD e/ou o titular dos dados pessoais. Dessa forma, com critérios e fatores pré-estabelecidos, haveria maior precisão e eficiência, por parte dos controladores, para que medidas imediatas sejam tomadas para tentar conter os riscos advindos do incidente, bem como enviar as notificações necessárias. Portanto, a DaVita propõe os seguintes fatores para classificar os incidentes de segurança em níveis diferentes: **Categoria 1 – Riscos altos:** ○ Tentativa deliberada ou criminosa de desativar sistemas/obter/vazar informações; ○ Acesso não autorizado a dados pessoais; ○ Dados pessoais sensíveis afetados; ○ Divulgação de informações confidenciais para agentes não autorizados; ○ Perda irrecuperável de dados sensíveis ou outros dados pessoais; ○ Perda ou perda de acesso a grandes volumes de dados para agentes mal-intencionados desconhecidos ou conhecidos; ○ Na avaliação dos riscos do incidente, conforme fatores propostos na resposta à pergunta 4 abaixo, conclui-se que há chances prováveis de materialização de danos relevantes aos titulares de dados. **Categoria 2 – Riscos médios:** ○ Os dados pessoais envolvidos tenham sido obtidos ou vazados acidentalmente; ○ Provável perda irrecuperável de dados pessoais; ○ Dados pessoais sensíveis afetados; ○ Perda ou perda de acesso a volumes médios de dados para um agente externo ou interno conhecido. ○ Na avaliação dos riscos do incidente, conforme fatores propostos na resposta à pergunta 4 abaixo, conclui-se que há chances razoáveis de materialização de danos relevantes aos titulares de dados.

	<u>Categoria 3 – Riscos baixos</u>: o Perda ou acesso acidental aos dados; o Os dados estavam protegidos por criptografia ou outros métodos de segurança; o Perda de baixos volumes de dados pessoais e sem envolvimento de dados sensíveis; o Dados potencialmente recuperáveis; o Na avaliação dos riscos do incidente, conforme fatores propostos na resposta à pergunta 4 abaixo, conclui-se que há chances remotas ou inexistentes de materialização de danos aos titulares de dados. Os incidentes enquadrados na **Categoria 1** (riscos altos) devem ser considerados como capazes de acarretar riscos ou danos <u>relevantes</u> aos titulares dos dados à luz do Art. 48. Os riscos envolvidos em tal categoria poderiam ensejar danos relevantes, que são de difícil reparação aos titulares dos dados. Assim, a necessidade de notificação se fará necessária de forma automática, para que a ANPD possa investigar o ocorrido prontamente e os titulares estejam cientes das medidas que podem tomar para se resguardar. Os incidentes enquadrados na **Categoria 2** (riscos médios) devem se sujeitar à análise dos controladores que deverão, eles próprios, a partir de análises caso-a caso, determinar se o incidente acarreta riscos ou danos <u>relevantes</u> ou não de acordo com o Art. 48 e, portanto, se deve ser notificado. Isso porque, no momento da análise, a relevância dos riscos não é tão acentuada como na Categoria 3, mas também não é irrelevante o suficiente para descartar imediatamente a necessidade de notificação. Os incidentes enquadrados na **Categoria 3** (riscos baixos) não devem ser considerados como capazes de acarretar riscos ou danos <u>relevantes</u> ao titular, dispensando, portanto, a notificação à ANPD e aos titulares dos dados. **A adoção dessa categoria é de extrema importância para evitar o envio de notificações desnecessárias que poderão criar um *backlog* para essa Autoridade e impedi-la de concentrar seus esforços em apurar incidentes realmente graves, além de evitar que os titulares de dados sejam impactados por diversas notificações e tenham dificuldades de distinguir aquelas que realmente merecem sua atenção**.
3. Como distinguir o risco do dano ao titular? Como esses conceitos se relacionam?	Entendemos que há **risco**, quando existe, para os titulares, mais do que uma chance remota de que sejam afetados pelo incidente. **Os riscos relevantes têm o condão de gerar danos relevantes ao**

	titular, ainda que isso possa ser revertido com a tomada de medidas pelo controlador. Exemplos de riscos relevantes para os titulares podem incluir a possibilidade de limitação de seus direitos, discriminação, roubo de identidade ou fraude, perda financeira, reversão não autorizada de pseudonimização, danos à reputação do titular e perda de confidencialidade de dados pessoais protegidos por sigilo profissional, como dados de pacientes.. Por sua vez, **dano** corresponde aos danos materiais e morais efetivamente causados pelo incidente de segurança em si (ou seja, houve a materialização de um risco relevante). De acordo com o Enunciado n. 456 da V Jornada de Direito Civil "*A expressão "dano" no Art. 944 abrange não só os danos individuais, materiais ou imateriais, mas também os danos sociais, difusos, coletivos e individuais homogêneos a serem reclamados pelos legitimados para propor ações coletivas*.". O Superior Tribunal de Justiça já se manifestou no sentido de que "[*a] dor indenizável é exclusivamente aquela que afeta sobremaneira a vítima, que atinge sua esfera legítima de afeição, que agride seus valores, que a humilha, expõe, fere, causando danos, na maior parte das vezes, irreparável, devendo a indenização ser fixada apenas como forma de aplacar a dor*." (cf. STJ AgRg no RE 387.014-9-SP, Rel. Min. Carlos Veloso, em RT 829/129) A gravidade do risco e a probabilidade dos danos relevantes são dois fatores-chave a serem avaliados na determinação dos incidentes que devem ser notificados. Ao decidir a probabilidade dos efeitos adversos sobre o indivíduo, pode-se considerar fatores como (i) quem pode ter acesso aos dados pessoais como resultado do incidente e (ii) se isso envolve perda de dados, acesso ou divulgação dos mesmos. Se apenas funcionários internos provavelmente tiveram acesso, a probabilidade dos danos relevantes explorados acima seria reduzida. No entanto, se (i) os dados pessoais não foram usados ou alterados; (ii) o acesso a eles foi perdido; (iii) foram enviados a um agente externo ou (iv) tornados públicos como resultado do incidente, a probabilidade de que haja danos relevantes é maior. Como mencionado acima, o dano não pode ser presumido. Tem que haver uma conexão real entre o incidente de segurança e um dano material ou moral evidenciado. Além disso, o dano moral não deve ser considerado como mero desconforto, aborrecimento, tristeza, irritação ou sensibilidade exacerbada. Ao invés disso, para ser considerado dano moral, deve provocar efeitos intensos e duradouros sobre o titular de dados. **Importante mencionar que os riscos relevantes, embora possam atrair a obrigação de notificação tanto a essa Autoridade quanto aos titulares dos dados, via de regra e, ao contrário do que se aplica aos danos relevantes, não deverão gerar a obrigação de indenizar**.

4. O que deve ser considerado na avaliação dos riscos do incidente?	Entendemos ser importante levar em consideração a experiência europeia que, sob a égide do GDPR, já possui critérios para a avaliação dos riscos. Nesse sentido, conforme recomendado pelo WP29[1] em suas Diretrizes sobre a notificação de uma violação de dados pessoais ao abrigo do Regulamento (UE) 2016/679 (*Guidelines on Personal data breach notification under Regulation 2016/679*) e pelo EDPB[2] em suas Diretrizes sobre Exemplos de Notificação de Incidentes de Segurança (*Guidelines on Examples regarding Data Breach Notification*), os critérios a serem levados em consideração ao avaliar os riscos são: **1. tipo de incidente de segurança** (se o incidente está relacionado à divulgação, acesso, perda temporária ou perda irrecuperável de dados pessoais. Deve-se levar em consideração o destinatário da divulgação de dados, por exemplo, se é um funcionário interno ou um agente terceiro externo); **2. natureza, sensibilidade e volume dos dados pessoais** (por exemplo, quando os dados afetados revelam informações sobre a saúde do titular, considera-se que há probabilidade de ocorrência de danos mais relevantes); **3. facilidade de identificação dos titulares** (deve-se considerar se os dados envolvidos no incidente facilitariam a identificação dos titulares dos dados, causando maior risco de ocorrerem danos relevantes); **4. gravidade das consequências para os titulares** **5. características especiais dos titulares** (por exemplo, se crianças forem afetadas, presume-se risco relevante); **6. características especiais do controlador** **7. o número de titulares afetados.** **8. o grau de confiabilidade do controlador no fato de que os dados envolvidos no incidente não foram posteriormente acessados ou divulgados** (caso o uso posterior dos dados pessoais não puder ser descartado, o nível de risco será maior). Ademais, além dos critérios acima, o fato de um incidente de segurança representar uma violação de outra lei ou ato normativo, também deveria ser considerado pela ANPD, ao analisar a gravidade do incidente de segurança, pois isso pode ser um indicativo de que os riscos associados ao incidente de

[1] "O Grupo de Trabalho de Proteção das Pessoas com Relação ao Tratamento de Dados Pessoais" (WP29), era um órgão consultivo composto por um representante de cada autoridade de proteção de dados dos Estados-Membros da UE, a Autoridade Europeia de Proteção de Dados e a Comissão Europeia. Com o advento do GDPR, o WP29 foi substituído pelo EDPB (*European Data Protection Board*), cujas missões e objetivos são similares aos do 7P29.
[2] Vide referência acima.

	segurança são mais altos (por exemplo, nos casos em que há uma violação à Lei de Sigilo Bancário - Lei Complementar nº 105/2001 ou ao Código de Ética Médica – Resolução CFM Nº 2.117/18).
5. Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	O Art. 48, §1º da LGPD estabelece que a comunicação a ser enviada pelo controlador deve conter, no mínimo, os seguintes elementos: (i) a descrição da natureza dos dados pessoais afetados; (ii) as informações sobre os titulares envolvidos; (iii) a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; (iv) os riscos relacionados ao incidente; (v) os motivos da demora, no caso de a comunicação não ter sido imediata; e (vi) as medidas que foram ou que serão adotadas pelo controlador para reverter ou mitigar os efeitos do prejuízo. Além disso, a ANPD publicou um guia preliminar sobre incidentes de segurança, em conjunto com a presente tomada de contribuições, onde estabeleceu, dentre outros, as informações que devem ser incluídas nas comunicações de incidentes de segurança. Na ocasião, a ANPD detalhou e expandiu a lista de informações dispostas no Art. 48, §1º da LGPD, propondo que os seguintes elementos também devem constar nas comunicações: (i) data e hora da detecção; (ii) data e hora do incidente e sua duração; (iii) circunstâncias em que ocorreu a violação de segurança de dados pessoais, por exemplo, perda, roubo, cópia, vazamento, dentre outros; (iv) descrição dos dados pessoais e informações afetadas, como a natureza e conteúdo dos dados pessoais, categoria e quantidade de dados e de titulares afetados; (v) resumo do incidente de segurança com dados pessoais, com indicação da localização física e meio de armazenamento; (vi) possíveis consequências e efeitos negativos sobre os titulares dos dados afetados; (vii) medidas de segurança, técnicas e administrativas preventivas tomadas pelo controlador de acordo com a LGPD; (viii) resumo das medidas implementadas até o momento para controlar os possíveis danos; (ix) possíveis problemas de natureza transfronteiriça;

	(x) outras informações úteis às pessoas afetadas para proteger seus dados ou prevenir possíveis danos. A lista de informações previstas no Art. 48, §1º da LGPD, combinada com os complementos propostos no guia preliminar para incidentes de segurança, fornece subsídios mais do que suficientes para que a ANPD possa iniciar a investigação sobre o incidente e para que os titulares de dados possam tomar medidas iniciais para se protegerem, conforme aplicável. Ademais, importante ressaltar que é provável que mais informações sejam fornecidas pelo controlador à ANPD no curso da investigação de incidente de segurança, o que complementaria as informações disponibilizada na primeira notificação a essa Autoridade. A expansão da lista prevista no Art. 48§ 1º da LGPD pode, ainda, gerar demora na notificação à essa Autoridade, pois o controlador precisará de mais tempo para levantar as informações necessárias. **Diante desses motivos, recomendamos que, em eventual expansão da lista prevista no Art. 48 §1º da LGPD, o envio das novas informações propostas por essa Autoridade seja opcional e de acordo com os elementos que o controlador dispuser no momento da notificação.** De forma mais específica, é importante destacar que a informação de "data e hora do incidente" proposta no guia preliminar muitas vezes não estará disponível imediatamente, ou pode ser, até mesmo, de impossível determinação pelo controlado por razões técnicas. Por esse motivo, recomendamos que tal informação seja excluída de eventual lista adicional com elementos a serem apresentados a essa Autoridade. Para fins de referência, o Art. 33(3) do GDPR estabelece que a notificação à autoridade competente deverá conter, pelo menos: *a. Descrever a natureza da violação dos dados pessoais incluindo, se possível, as categorias e o número aproximado de titulares de dados afetados, bem como as categorias e o número aproximado de registos de dados pessoais em causa;* *b. Comunicar o nome e os contatos do encarregado da proteção de dados ou de outro ponto de contato onde possam ser obtidas mais informações;* *c. Descrever as consequências prováveis da violação de dados pessoais;*

	d. Descrever as medidas adotadas ou propostas pelo responsável pelo tratamento para reparar a violação de dados pessoais, inclusive, se for caso disso, medidas para atenuar os seus eventuais efeitos negativos; Note-se que em nenhum momento é estabelecida a obrigação de informar a data e a hora em que o incidente ocorreu. **Por fim, a DaVita gostaria de solicitar que a ANPD forneça mais detalhes acerca dos itens "*descrição dos dados pessoais e informações afetadas, como a natureza e conteúdo dos dados pessoais, categoria e quantidade de dados e de titulares afetados*;" e "*possíveis problemas de natureza transfronteiriça*" propostos no guia preliminar, caso eles venham a integrar uma lista adicional definitiva de itens a serem incluídos em notificações de incidentes. Consideramos importante que os controladores tenham mais detalhes sobre o que se espera em relação a esses itens, a fim de que possam assegurar que identificarão os elementos considerados relevantes para essa Autoridade na apuração do incidente.**
6. Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	**Prazo** Ao publicar a tomada de subsídios em pauta, a ANPD estabeleceu o prazo preliminar de dois (2) dias úteis, contados a partir do momento em que o controlador tenha conhecimento do incidente de segurança, para que as entidades notifiquem a ANPD em caso de incidente de segurança. Para fins de referência, o Art. 33 do GDPR estabelece que os controladores devem comunicar à autoridade competente sobre o incidente de segurança sem demora injustificada e, sempre que possível, até 72 horas após ter tido conhecimento do mesmo. O Art. 26-D da Lei de Proteção de Dados Pessoais de Cingapura, por sua vez, determina que os controladores devem comunicar ao DPA de Cingapura assim que possível, mas em no máximo 3 dias corridos, após o controlador determinar que o incidente enquadra-se nos critérios que requerem a notificação. Dessa forma, entendemos que, em linha com a experiência internacional e os primeiros pronunciamentos em âmbito nacional, o prazo proposto de 2 (dois) dias úteis é razoável, desde que considerados os fatores apresentados na sequência.

	<u>Marco inicial para contagem do prazo</u> **Acreditamos que o marco inicial para a contagem do prazo de 2 (dois) dias úteis deve se dar no momento em que o controlador toma conhecimento do incidente.** Para que seja considerado que o controlador tomou conhecimento do incidente, é necessário que ele tenha um nível razoável de certeza de que o incidente de segurança ocorreu **<u>e</u>** que comprometeu dados pessoais sob sua responsabilidade. Ou seja, se o controlador apenas tiver conhecimento de uma falha de segurança, mas ainda não tiver conseguido apurar se houve comprometimento da (i) confidencialidade; ou (ii) disponibilidade; ou (iii) integridade das informações **<u>e</u>** se, dentre as informações comprometidas, havia dados pessoais, o prazo de 2 (dois) dias úteis para notificação não se iniciará. Não recomendamos que sejam estipulados momentos de início da contagem do prazo que dependam de elementos menos objetivos – como o proposto pela Lei de Proteção de Dados Pessoais de Cingapura citado acima. Isso criaria margem para discussões sobre se o prazo foi cumprido ou não pelo controlador e criaria mecanismos para que os controladores demorem e tenham argumentos para justificar a demora na notificação. **<u>Notificação em fases</u>** **Independentemente do prazo de notificação a ser estabelecido por essa Autoridade, para que ele seja razoável, é fundamental que a ANPD autorize que a notificação ocorra em fases, de modo que a primeira notificação tenha, quando necessário, caráter preliminar**. Na prática, os controladores muitas vezes não serão capazes de reunir todas as informações solicitadas no §1º do Art. 48 da LGPD – e em eventual lista adicional proposta por essa Autoridade - imediatamente após o incidente. As informações disponíveis no momento da notificação dependerão das circunstâncias específicas de cada incidente de segurança. Além disso, não é razoável que o controlador concentre todos seus esforços em elaborar uma notificação completa dentro do prazo para notificação, já que no mesmo momento ele deverá estar trabalhando para conter o incidente e mitigar ou reverter os riscos e danos aos titulares dos dados. A depender do tamanho da organização do controlador e dos recursos disponíveis, elaborar uma notificação completa dentro de um prazo determinado poderá ser impossível.

	Assim, permitir que os controladores complementem a notificação após o prazo de notificação é fundamental para garantir que os interesses dos titulares dos dados sejam respeitados, sem criar uma obrigação excessivamente onerosa para os controladores. A ANPD parece concordar com esta abordagem, uma vez que, no guia preliminar de incidentes de segurança, está disposto que a comunicação deve conter uma série de informações, incluindo "*indicação se a notificação é completa ou parcial. Em caso de comunicação parcial, indicar que se trata de uma comunicação preliminar ou de uma comunicação complementar*.". Tal fato também está de acordo com o Considerando 85 do GDPR que determina que "*Se não for possível efetuar essa notificação no prazo de 72 horas, a notificação deverá ser acompanhada dos* motivos do atraso, podendo as informações ser fornecidas por fases sem demora injustificada." Por fim, vale mencionar que o sistema de notificações em fases já é previsto no ordenamento jurídico brasileiro. A Agência Nacional do Petróleo, Gás Natural e Biocombustíveis (ANP), estabelece em sua Resolução nº 44 de 22/12/2009 o procedimento para comunicação de incidentes, a ser adotado pelos concessionários e empresas autorizadas pela ANP a exercer as atividades da indústria do petróleo, do gás natural e dos biocombustíveis, bem como distribuição e revenda. Essa Resolução prevê, em seus artigos 2º e 3º, uma comunicação faseada da seguinte forma: (i) comunicação inicial do incidente, que deve ser imediata e (ii) relatório detalhado do incidente, apresentado em 30 dias, prorrogável mediante fundamentação técnica.
7. Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	O Art. 48, §1º da LGPD prevê que os controladores devem informar à ANPD e os titulares dos dados a respeito qualquer incidente de segurança que possa resultar em dano ou risco relevante para o titular dos dados. A LGPD estabelece que tal comunicação deverá ser apresentada em prazo razoável, sem estabelecer (i) um prazo exato que deva ser observado; e (ii) a partir de qual momento tal prazo passa a ser contado. Além disso, ao contrário de outras leis (como o GDPR na União Europeia e a Lei de Proteção de Dados Pessoais de Cingapura), a LGPD não (i) reconhece a possibilidade de notificar apenas a ANPD e não o titular dos dados, dependendo do caso concreto; e (ii) prevê prazos diferentes para essas comunicações. **No entanto, acreditamos que seria aconselhável abordar essas comunicações de diferentes perspectivas, pois seus objetivos e fundamentos são diferentes.**

	Entendemos que o objetivo da notificação ao titular dos dados é informar sobre um incidente de segurança e, também, fornecer algumas recomendações para viabilizar que o titular dos dados tome as precauções necessárias para evitar maiores riscos ou danos. Nesse sentido, a comunicação aos titulares dos dados deve contemplar informações claras sobre o incidente de segurança e as recomendações para mitigar potenciais danos relevantes. Diante do exposto, cabe mencionar que, na prática, muitas vezes o controlador não terá como reunir todas as informações obrigatórias, de modo a oferecer clareza suficiente para estabelecer recomendações de medidas a serem tomadas pelo titular, a fim de enviar as notificações dentro do prazo de 2 dias úteis, a partir do momento em que o controlador teve ciência do incidente. **A notificação ao titular com o mero objetivo de cumprir um prazo, sem prover subsídios suficientes e sugestões práticas de medidas a serem tomadas, pode gerar desinformação e pânico entre os titulares de dados, não representando nenhum benefício. Além disso, o envio de notificações nesse sentido poderá desgastar os titulares, que perderão a sensibilidade acerca das notificações, caso controladores notifiquem-nos regularmente independentemente de critérios específicos e disponibilidade de informações úteis.** Além disso, alinhamentos prévios com a ANPD podem ajudar a garantir uma comunicação adequada aos titulares dos dados. Para referência, a estreita cooperação entre o controlador e as autoridades nacionais em relação à comunicação ao titular dos dados é abordada no GDPR, uma vez que seu Considerando 86 afirma que essa comunicação aos titulares dos dados deverá ser efetuada logo que seja razoavelmente possível, *em estreita cooperação com a autoridade competente e em cumprimento das orientações fornecidas por esta ou por outras autoridades competentes, como as autoridades de aplicação da lei (law enforcemenet authorities).* A título de exemplo, o mesmo Considerando também prevê que "*a necessidade de atenuar um risco imediato de dano exigirá uma pronta comunicação aos titulares dos dados, mas a necessidade de aplicar medidas adequadas contra incidentes de segurança recorrentes ou similares poderá justificar um período mais alargado para a comunicação*". Nesse sentido, o Art. 33 do GDPR estabelece que o controlador deve, "*sem demora injustificada e, sempre que possível, até 72 horas após ter tomado conhecimento do incidente*, *comunicá-lo à autoridade relevante*". O Art. 34, por sua vez, determina que o controlador deve comunicar ao titular dos dados sobre o incidente de segurança sem demora injustificada, mas nenhum prazo ou parâmetro específico é mencionado. Dessa forma, pode-se observar que o legislador europeu prezou pela notificação que possua nível satisfatório de informações e que seja realizada de forma adequada, em

	detrimento do mero cumprimento de prazo estipulado em lei. Isto pois o prazo é determinado de forma abstrata na norma legal, mas, na prática, cada incidente de segurança possui características próprias, de forma que um modelo rígido de notificação não necessariamente será benéfico e permitirá fornecer aos titulares as informações que estes precisam para efetivamente resguardar suas liberdades e direitos fundamentais. Ainda, as Diretrizes sobre a notificação de uma violação de dados pessoais ao abrigo do Regulamento (UE) 2016/679 (*Guidelines on Personal data breach notification under Regulation 2016/679*) preveem que "(...) *O* Considerando 88 estabelece que a comunicação de um incidente deve *"levar em conta os legítimos interesses das autoridades de aplicação das leis nos casos em que a divulgação precoce de informações possa dificultar desnecessariamente a investigação das circunstâncias do incidente de segurança". Isso pode significar que, em determinadas circunstâncias, sempre que se justifique e mediante o aconselhamento das autoridades de aplicação das leis, o responsável pelo tratamento pode atrasar a comunicação do incidente aos titulares dos dados até que isso não prejudique essas investigações. No entanto, os titulares de dados ainda precisariam de ser informados imediatamente após esse período*." **Diante do cenário acima, entendemos que o envio de notificações para os titulares deve se dar após (i) a coleta de todas as informações necessárias para fornecer um cenário claro ao titular dos dados com as medidas correspondentes a serem tomadas para proteger os dados envolvidos no incidente de segurança; e (ii) após alinhamentos prévios com a ANPD, quando necessário, que possam fornecer orientações relevantes para garantir a devida comunicação ao titular dos dados; e (iii) após alinhamentos prévios com outras autoridades públicas relevantes que possam estar relacionados ao incidente, quando aplicável. Importante ressaltar que os itens (i), (ii) e (iii) devem ser realizados dentro de um prazo razoável, mas não específico.** Em relação ao conteúdo da comunicação ao titular dos dados, acreditamos que as informações mais relevantes são as seguintes: (i) descrição da natureza dos dados pessoais afetados, para que o titular dos dados tenha conhecimento dos dados pessoais expostos; (ii) riscos relacionados ao incidente de segurança, de forma que o titular dos dados esteja ciente dos riscos e danos a que pode estar sujeito em decorrência do incidente de segurança; (iii) recomendações para mitigar potenciais efeitos adversos, a fim de permitir que o titular dos dados tome as precauções necessárias; (iv) nome e detalhes de contato do DPO ou outro ponto de contato com quem mais informações podem ser obtidas.

8. Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	Inicialmente, **entendemos que a notificação individualizada não será sempre possível e eficiente na prática**. Dependendo do número de titulares de dados que foram afetados ou do tipo de relação entre o controlador e o titular (por exemplo, caso o incidente de segurança envolva dados pessoais dos titulares dos dados e o controlador não possua informações de contato dos referidos titulares atualizadas), a forma mais adequada de comunicar os titulares pode ser através de uma comunicação pública por meio de *press release*, publicações na internet, dentre outros. Para referência, esta possibilidade é admitida pelo GDPR, em seu Art. 34(3)c, que prevê a adoção de uma comunicação pública ou medida semelhante através da qual os titulares são informados de maneira igualmente eficaz sobre o incidente nos casos em que a comunicação individual aos titulares envolver um esforço desproporcional. **Por outro lado, quando o controlador (i) é capaz de identificar claramente a identidade de todos os titulares de dados envolvidos; e (ii) dispõe dos dados de contato de tais titulares de dados, entendemos que seria mais adequado notificar os titulares individualmente.** A validade de ambos os métodos de comunicação é evidenciada pelas Diretrizes sobre a notificação de uma violação de dados pessoais ao abrigo do Regulamento (UE) 2016/679 (*Guidelines on Personal data breach notification under Regulation 2016/679*), onde o WP29 estabelece que "*exemplos de métodos de comunicação transparente incluem o envio direto de mensagens (por exemplo, correio eletrônico, SMS, mensagem direta), banner de notificação em websites proeminentes, comunicações postais e anúncios em destaque nos meios de comunicação impressos*." **Em síntese, a forma de comunicar o titular dos dados sobre o incidente de segurança deve ser verificada em relação ao caso concreto e a ANPD pode estabelecer alguns critérios para orientar essa análise (como os critérios mencionados nas questões acima) e, também, auxiliar o controlador na prática a definir a melhor forma de comunicação.**
9. Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	Entendemos que somente deverão ser notificados os incidentes que efetivamente apresentem danos para os titulares dos dados – é o caso dos incidentes compreendidos na Categoria 3 e, quando aplicável, na Categoria 2, conforme critérios propostos pela DaVita nas respostas às questões 2, 4 e 11 desta contribuição. Assim, determinados incidentes enquadrados na Categoria 2 e todos os

	incidentes enquadrados na Categoria 1 estariam dispensando da obrigatoriedade de notificação a essa Autoridade.
10. Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	Primeiramente, vale destacar que pela experiência da União Europeia, à luz do GDPR, os eventos que desencadeiam a obrigação de informar os titulares e as autoridades relevantes, não são necessariamente os mesmos. Nesse sentido, o Art. 33 do GDPR estabelece que o controlador deve notificar o incidente de segurança à autoridade nacional, a menos que seja improvável que o incidente de segurança resulte em risco para os direitos e liberdades dos titulares de dados. **Ou seja, o parâmetro para notificação à autoridade competente é o fato de que o incidente de segurança pode gerar risco**, conceito cuja definição propusemos nas questões 1 (*Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?)* e 3 (*Como distinguir o risco do dano ao titular? Como esses conceitos se relacionam?*)**.** Por outro lado, o Art. 34 do GDPR determina que o titular dos dados deve ser notificado quando um incidente de segurança for suscetível a resultar em um alto risco para seus direitos e liberdades. **Ao adotar a definição "alto risco", o legislador europeu adotou um critério mais elevado para comunicar os titulares dos dados em relação ao critério para comunicar a autoridade competente.** Como o objetivo fundamental de uma comunicação ao titular dos dados é fornecer informações a fim de conscientizá-lo e permitir que ele tome as medidas necessárias para conter os riscos do incidente, na prática, quando os incidentes são rapidamente controlados, mitigando quaisquer riscos e danos em momento anterior à notificação, não haveria obrigatoriedade de informá-los. Isso porque, a notificação não ensejaria a tomada de atitudes por parte dos titulares, considerando que o controlador já teria se encarregado de mitigar a materialização de danos relevantes. Ademais, o excesso de notificações, ao invés de auxiliar os titulares a se protegerem, causaria desinformação e pânico, gerando uma "fadiga de comunicações desnecessárias". Isso faria com que os titulares perdessem a sensibilidade sobre a importância e urgência da notificação. Nesse caso, os titulares dos dados podem acabar ignorando ou não entendendo quando devem adotar algumas medidas de proteção para mitigar riscos relevantes.

	Nesse sentido, o Art. 34 (3) do GDPR isenta o controlador da obrigação de notificar o titular dos dados quando (i) *o controlador implementou medidas de proteção técnica e organizacional adequadas para proteger os dados pessoais antes do incidente de segurança, em particular aqueles que tornam os dados pessoais ininteligíveis para qualquer pessoa que não esteja autorizada a acessá-los, como criptografia ou tokenização*; e (ii) *o controlador tomou medidas subsequentes que garantem que o alto risco para os direitos e liberdades dos titulares dos dados não é mais provável de se materializar (por exemplo, o controlador identificou rapidamente o incidente de segurança e tomou medidas imediatas contra o indivíduo que acessou dados pessoais antes de ser capaz de fazer qualquer coisa com os dados em questão).* A Lei de Proteção de Dados Pessoais de Cingapura também reconhece a possibilidade de comunicar à autoridade competente e não ao titular dos dados sobre um incidente de segurança. Neste caso, o Art. 5 (3) da Lei de Proteção de Dados Pessoais de Cingapura estabelece que, quando o controlador não pretende comunicar nenhum indivíduo afetado sobre um incidente de segurança que deve ser comunicado à autoridade competente, o controlador deve especificar os motivos para não comunicar o titular dos dados. Assim, entendemos que seria importante que a ANPD implementasse dois critérios diferentes para determinar quando o controlador deverá notificar a autoridade nacional e os titulares dos dados. Afinal, como demonstrado, o objetivo que fundamenta as comunicações não é necessariamente o mesmo: a comunicação aos titulares visa a fornecer subsídios para que esses possam ser informados e tomarem medidas para se resguardarem, enquanto a comunicação a essa Autoridade tem como objetivo investigar e determinar medidas para que os efeitos do incidente sejam mitigados.
11. Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	Em linha com nossa resposta à questão 4 acima, entendemos ser importante levar em consideração a experiência europeia que, sob a égide do GDPR, já possui critérios para a avaliação dos riscos. Nesse sentido, conforme recomendado pelo WP29 em suas Diretrizes sobre a notificação de uma violação de dados pessoais ao abrigo do Regulamento (UE) 2016/679 (*Guidelines on Personal data breach notification under Regulation 2016/679*) e pelo EDPB em suas Diretrizes sobre Exemplos de Notificação de Incidentes de Segurança (*Guidelines on Examples regarding Data Breach Notification*), os critérios a serem levados em consideração ao avaliar os riscos são:

	1. tipo de incidente de segurança (se o incidente está relacionado à divulgação, acesso, perda temporária ou perda irrecuperável de dados pessoais. Deve-se levar em consideração o destinatário da divulgação de dados, por exemplo, se é um funcionário interno ou um agente terceiro externo); **2. natureza, sensibilidade e volume dos dados pessoais** (por exemplo, quando os dados afetados revelam informações sobre a saúde do titular, considera-se que há probabilidade de ocorrência de danos mais relevantes); **3. facilidade de identificação dos titulares** (deve-se considerar se os dados envolvidos no incidente facilitariam a identificação dos titulares dos dados, causando maior risco de ocorrerem danos relevantes); **4. gravidade das consequências para os titulares** **5. características especiais dos titulares** (por exemplo, se crianças forem afetadas, presume-se risco relevante); **6. características especiais do controlador** **7. o número de titulares afetados.** **8. o grau de confiabilidade do controlador no fato de que os dados envolvidos no incidente não foram posteriormente acessados ou divulgados** (caso o uso posterior dos dados pessoais não puder ser descartado, o nível de risco será maior). Ademais, além dos critérios acima, o fato de um incidente de segurança representar uma violação de outra lei ou ato normativo, também deveria ser considerado pela ANPD, ao analisar a gravidade do incidente de segurança, pois isso pode ser um indicativo de que os riscos associados ao incidente de segurança são mais altos (por exemplo, nos casos em que há uma violação à Lei de Sigilo Bancário - Lei Complementar nº 105/2001 ou ao Código de Ética Médica – Resolução CFM Nº 2.117/18).
12. Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	A metodologia mais conhecida desenvolvida para a avaliação dos riscos relacionados com incidentes de segurança é a publicada pela Agência Europeia para a Segurança das Redes e da Informação (ENISA), Recomendações para uma metodologia de avaliação da gravidade das violações de dados pessoais (*Recommendations for a methodology of the assessment of severity of personal data breaches*), que foi elaborada especialmente para incidentes de segurança envolvendo dados pessoais. De todo modo, elementos de diretrizes mais genéricas relacionadas à Segurança da Informação, como as fornecidas pelo Instituto Nacional de Padrões e Tecnologia (NIST - EUA), também podem ser úteis para o estabelecimento das metodologias a serem adotadas por essa Autoridade (por

	exemplo, *Computer Security Incident Handling Guide* and *Technical guide to information security testing and assessment*). Importante notar que, embora esses documentos possam fornecer critérios úteis às análises de incidentes de segurança, acreditamos que nenhuma metodologia fechada deva ser adotada como regra. Isso porque, como amplamente explorado na presente contribuição, entendemos que a gravidade dos incidentes e seus potenciais impactos devem ser considerados, também, a partir de análises caso a caso.
13. Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	O artigo 48, §2º, II, da LGPD estabelece que, após notificada, a ANPD poderá determinar que o controlador adote medidas para reverter ou mitigar o efeito da violação de dados. Nesse sentido, dada a abstração da norma, entendemos que as medidas a serem adotadas deverão ser estipuladas em relação a cada caso específico, a depender das circunstâncias do incidente de segurança. Ademais, acreditamos que não seria vantajoso que a ANPD publicasse ou elaborasse uma lista taxativa de medidas que poderiam ser tomadas, em razão da singularidade dos incidentes de segurança, que devem ser estabelecidas caso a caso. Para fins de referência, o Guia para Gerenciamento de Violações de Dados da DPA de Cingapura (*Guide on Managing and Notifying Data Breaches*) estabelece medidas que podem ser impostas pela autoridade competente, conforme exemplos listados abaixo. Reiteramos que a lista é meramente exemplificativa e pode não englobar todas as medidas providências que podem ser determinadas na prática. • Realizar auditorias no controlador (físicas, de sistemas e de documentos); • Solicitar ao controlador que implemente processos que podem limitar os danos se incidentes de segurança semelhantes ocorrerem no futuro; • Solicitar que o controlador atualize programas de computadores e medidas de segurança, como senhas e controles de acesso; • Solicitar ao controlador que envolva consultorias técnicas e jurídicas especializadas para implementar as medidas para mitigar os danos e conter o incidente de segurança; • Solicitar ao controlador que se atente às condições contratuais ao envolver terceiros no tratamento de dados pessoais; • Solicitar ao controlador para aumentar a conscientização sobre questões de proteção de dados entre funcionários, parceiros comerciais e prestadores de serviços;

	• Solicite ao controlador que tome medidas perante os titulares dos dados (como fornecer orientações mais práticas sobre as medidas que os titulares dos dados podem adotar para proteger seus dados pessoais que foram sujeitos ao incidente de segurança). • Fornecer serviços de monitoramento de crédito para titulares de dados afetados (quando aplicável). Ademais, também sugerimos os seguintes exemplos de medidas que podem ser adotadas: • Estabelecer um canal de comunicação seguro para monitorar e relatar o incidente; • Isolar determinada parte das redes ou sistemas da empresa que possam ter sido afetadas pelo; • Redefinir / restringir o acesso às instalações, redes ou sistemas da empresa por colaboradores e fornecedores do controlador; • Determinar o bloqueio / reinicialização remota de qualquer dispositivo de armazenamento eletrônico portátil perdido ou roubado (como smartphones, laptops etc.); • Identificar quando ocorreu o backup mais recente dos sistemas de TI da empresa e considerar se é necessário criar uma imagem forense do sistema para preservar a capacidade de identificar a causa do incidente.
	Questão adicional relevante: • **Possibilidade de notificação de incidente de segurança pelo operador:** Quando a ANPD publicou a tomada de subsídios em pauta, também publicou (i) um guia preliminar sobre incidentes de segurança onde estabelecia que "*embora a responsabilidade e a obrigação pela comunicação à ANPD sejam do controlador, caso excepcionalmente sejam apresentadas informações pelo operador, serão devidamente analisadas pela ANPD*"; e (ii) um formulário de comunicação de incidente de segurança com um campo a ser marcado pela entidade notificadora para informar se é o controlador ou operador. O Art. 48 estabelece precisamente que "*O **controlador** deverá comunicar à Autoridade Nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares*.". **Dessa forma, pode-se observar que a obrigação de notificar é do controlador, não podendo ser delegada ou transferida para o operador, pois isto estaria em total**

	desconformidade com a LGPD. Nesse sentido, acreditamos que esse Autoridade não deve estimular ou dar espaço para que os operadores apresentem notificações de incidentes. De acordo com outras legislações ao redor do mundo - como o GDPR -, acreditamos que o legislador não forneceu ao operador a opção de notificar a ANPD de forma intencional. uma vez que o controlador é a entidade responsável pela existência do processamento e, portanto, a entidade capaz de avaliar a gravidade de um incidente de segurança e de examinar os impactos potenciais que uma violação de dados pode causar aos indivíduos afetados. Por outro lado, os operadores devem ser intensamente estimulados por esse Autoridade a relatar ao controlador qualquer incidente de segurança do qual tenha conhecimento que envolva os dados pessoais processados em nome e sob as instruções do controlador em prazo razoável, para que o controlador possa avaliar se as especificidades do incidente desencadeiam a obrigação de notificação estabelecida pela LGPD. Essa lógica está de acordo com o GDPR, que estabelece no seu Artigo 33(2) que: "*O operador deve notificar o controlador sem demora indevida após tomar conhecimento de uma violação de dados pessoais*". Ao examinar a obrigação de notificação, o W29 em suas Diretrizes sobre a notificação de uma violação de dados pessoais ao abrigo do Regulamento (UE) 2016/679 (*Guidelines on Personal data breach notification under Regulation 2016/679*) concluiu que: "***O artigo 33(2) deixa claro que se um operador for contratado pelo controlador e tomar conhecimento de uma violação dos dados pessoais que está processando em nome do controlador, deverá notificar o controlador "sem atraso indevido"****”. Deve-se observar que o operador não precisa primeiro avaliar a probabilidade de risco decorrente de uma violação antes de notificar o controlador; é o controlador que deve fazer esta avaliação ao tomar conhecimento da violação. O operador só precisa estabelecer se ocorreu uma violação e, em seguida, notificar o controlador*". Além disso, o entendimento do W29 é que os operadores só devem notificar a autoridade competente, quando o controlador tiver expressamente instruído a proceder nesse sentido: "*Um operador poderia fazer uma comunicação em nome do controlador, se o controlador tiver dado a devida autorização ao operador e se isto fizer parte do arranjo contratual entre o controlador e o operador. Tal notificação deve ser feita em conformidade com os artigos 33 e 34.* ***Entretanto, é importante observar que a responsabilidade legal de notificar permanece com o controlador***".

MODELO PARA ENVIO DE CONTRIBUIÇÕES
REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA:

Universidade de São Paulo – USP / Faculdade de Direito / Departamento de Direito Civil / Grupo de Pesquisa "Direito Civil na Sociedade em Rede"

Elaboradores:

Amanda Thereza Lenci Paccola

Carolina Lopes Scodro

Eduardo Lopes Cominetti

Emanuele Pezati Franco de Moraes

Leonardo Perez Diefenthäler

Renata Chade Cattini Maluf

Victor Auilo Haikal

Responsável pelo Grupo de Pesquisa no CNPq: Prof. Dr. Eduardo Tomasevicius Filho

CPF/CNPJ: 63.025.530/0014-29

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS

IMPORTANTE: Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.

TÓPICO/QUESTÃO	CONTRIBUIÇÃO/INSTITUIÇÃO

Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	**O grupo, nesse tópico, desenvolveu duas possibilidades de análise de incidente que cause dano relevante aos titulares de dados pessoais.** **Em uma primeira abordagem do tema, mais objetiva,** destacamos que, conforme a Lei Geral de Proteção de Dados, existem os dados pessoais comuns e os dados pessoais sensíveis. Estes últimos demandam uma proteção maior, em razão de terem um potencial mais alto de causar danos relevantes aos titulares, bem como possível discriminação, violação do direito à imagem e à reputação, fraudes financeiras, roubo de identidade e de dados biométricos, acesso a conteúdos sensíveis, entre outros. Além dos dados pessoais sensíveis, também devemos considerar como maior risco ou dano relevante quando um incidente envolver dados de **crianças e adolescentes (art. 14 da LGPD) e vulneráveis**. Importante destacar que o volume de dados vazados também pode apresentar risco ou dano relevante, bem como o quantitativo de indivíduos afetados, sobretudo, a **boa-fé** e as intenções dos terceiros que tiveram acesso aos dados após o incidente e a facilidade de identificação dos titulares por terceiros não autorizados. Desta forma, um incidente pode acarretar risco ou dano relevante ao titular sempre que houver potencial de prejuízo ao titular em observância às informações existentes, como o vazamento de informações que não sejam públicas ou comuns. Em síntese, os critérios que podem ser considerados são: - dado pessoal sensível; - dados de crianças e adolescentes; - dados de vulneráveis; - grande volume de dados envolvidos, de indivíduos afetados, boa-fé e as intenções dos terceiros que tiveram acesso aos dados após o incidente e a facilidade de identificação dos titulares por terceiros não autorizados. **Agora, de forma mais analítica e detalhada, o grupo aponta o seguinte:** Antes de se iniciar a avaliação de risco,

	entendemos que algumas considerações sobre os tipos de dados pessoais e particularidades do contexto brasileiro são indispensáveis. Assim como já apontado anteriormente, a Lei Geral de Proteção de Dados prevê, a classificação básica dos dados pessoais compreende os dados pessoais comuns, indicados como "dados pessoais propriamente ditos", e os dados pessoais sensíveis. De pronto, há identificação imediata de prejuízo quando ocorre comprometimento dos 'dados pessoais propriamente ditos' em um incidente, pois pode acarretar na falta de confiabilidade das transações ou declarações assinadas por determinado titular, situação também conhecida pela falta de higidez esperada ao 'não repúdio' das transações. Adicionalmente, há os dados pessoais sensíveis, que são definidos no art. 5º inciso II da LGPD como: "dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural". Não é por acaso que são considerados sensíveis. Se comprometidos possuem potencial mais alto de causar danos relevantes aos titulares, bem como possível discriminação, perseguição, violação do direito à imagem e à reputação, fraudes financeiras e outras situações que dependam, ou sejam decorrentes da exploração, de dados biométricos ou de saúde, entre outros. Ainda em relação aos tipos de dados do titular, é prudente pontuar um tipo de informação pessoal que possui tanta sensibilidade quanto os dados sensíveis: são os dados identificados **por comportamentos históricos do titular, ou seja, das informações que consistam em suas declarações**, descrevam atos praticados e opiniões manifestadas em determinado contexto que podem ser associados a características já tipificadas na definição legal dos dados sensíveis ou que possam incitar o escrutínio público em prejuízo do titular, o que atualmente não é explicitamente diferenciado na LGPD.

	Elencados os tipos de dados pessoais que serão alvo da avaliação de riscos - dados pessoais propriamente ditos, dados sensíveis e dados de comportamentos históricos - é razoável realizar recorte histórico de tratamento de dados pessoais no Brasil para avaliar as possíveis situações que ensejam prejuízo ao titular de dados na forma de incidentes de segurança envolvendo suas informações pessoais pois se entende como crucial para a particularização do estudo do tema no contexto social e jurídico do Brasil. Ainda que a legislação própria à espécie tenha vindo de forma reconhecidamente tardia em relação aos demais países da América Latina, a Constituição Federal e o Código de Defesa do Consumidor já delinearam normas que, em alguma medida, possuem o escopo de proteger o tratamento de dados pessoais, ainda que de forma mais genérica e ampla. Entretanto, o cenário prático não acompanhava sequer a existência de quaisquer normas a esse respeito, sobretudo para fins de limitação ou combate efetivo ao compartilhamento de dados de forma ilícita. Inúmeros foram os incidentes cuja abrangência e alcance são indetermináveis a partir de vazamento de dados clandestinos e também com a origem difícil de ser determinada, a exemplo de repetidas e variadas ofertas de dados de brasileiros em centros comerciais populares apenas na cidade de São Paulo: http://g1.globo.com/Noticias/SaoPaulo/0,,MUL26277-5605,00-INFORMACOES+SIGILOSAS+SAO+VENDIDAS+EM+CDS+NA+SANTA+EFIGENIA+EM+SP.html http://g1.globo.com/sao-paulo/noticia/2010/05/cds-vendidos-no-centro-de-sp-tem-dados-sigilosos-de-consumidores.html https://sao-paulo.estadao.com.br/noticias/geral,santa-ifigenia-paraiso-de-cpfs-imp-,597705 https://atarde.uol.com.br/brasil/noticias/1178540-dados-de-policiais-sao-vendidos-em-cd-no-centro-de-sp Isso sem considerar alguns também conhecidos casos de sítios

	clandestinos de distribuição de dados pessoais, a exemplo do 'Tudo Sobre Todos' e admitindo-se a ocorrência de incidentes não reportados ou ainda não descobertos. Esse histórico revela que não é razoável considerar que no país havia cenário confiável de tratamento de dados pessoais em relação aos titulares de modo a se considerar como incidentes insignificantes ou de impacto não relevante os que ocorrerem *a posteriori* da vigência da LGPD, justamente em razão da possibilidade de combinação dos dados que forem comprometidos com aqueles historicamente já disponibilizados, a exemplo das mídias comercializadas de forma clandestina. Noutras palavras: a possibilidade de recombinação dos dados de titulares brasileiros em razão do histórico de falta de confiabilidade acumulada ao longo dos anos impõe a necessidade de consideração maior de risco e prejuízos ao titular ainda que eventual incidente fosse categorizado como de pequeno impacto ou risco em outro contexto social. Por isso, como regra geral, pode-se usar o critério da **existência de relevância** na gravidade de incidentes de dados pessoais até que exista circunstância comprovando a inexistência de tal premissa. Por outro lado, quando se comprovar que o incidente se enquadra nas hipóteses de inexistência de prejuízo, será o caso de situação de danos não relevantes conforme o enunciado, podendo também ser compreendido como **sem gravidade**. Então, quando não se é possível comprovar circunstâncias que levarão à classificação do incidente como **sem gravidade**, sugerimos a consideração do incidente **com gravidade**, conforme descrição pormenorizada na resposta seguinte.
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)?	**O grupo, nesse tópico, desenvolveu duas possibilidades de sugestões sobre divisão do risco ou dano relevante.** **Possibilidade 1 (baseada na experiência nacional):** Conforme o Guia de Avaliação de Riscos de Segurança e Privacidade, (https://www.gov.br/gover nodigital/pt-

Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	br/governanc a-de-dados/guia-de-avali acao-de-riscos-de-segur anca-e-privacidade.pdf) elaborado pelo Ministério da Economia, em conjunto com a Secretaria Especial de Desburocratização, Gestão e Governo Digital, a Secretaria de Governo Digital, o Departamento de Governança de Dados e Informações e a Coordenação-Geral de Segurança da Informação é possível a categorizar o risco em baixo, moderado e alto. Referido Guia tem como base o modelo de Relatório de Impacto à Proteção de Dados Pessoais (RIPD) referenciado na seção 2.5 do Guia de Boas Práticas da LGPD (CCGD, 2020). No item 1.4.1 Avaliação de Riscos do Guia, é disposto sobre os parâmetros que atribuem um valor gradual para cada uma das classificações (Baixo, Moderado e Alto), podendo ser utilizados esses padrões para distinguir os níveis. A Tabela 7 deste Guia exibe os parâmetros escalares, a Tabela 8, por sua vez, apresenta uma matriz que relaciona a probabilidade1 (chance de algo acontecer) com o impacto2 (resultado de um evento que afeta o objetivo). Ao multiplicar esses dois valores, obtém-se o nível de risco 3 (magnitude de um risco ou combinação de riscos). *Tabela 7. Parâmetros Escalares (CCGD, 2020).* **CLASSIFICAÇÃO** / **VALOR** Baixo / 5 Moderado / 10 Alto / 15

Tabela 8. Matriz de Probabilidade X Impacto (CCGD, 2020).

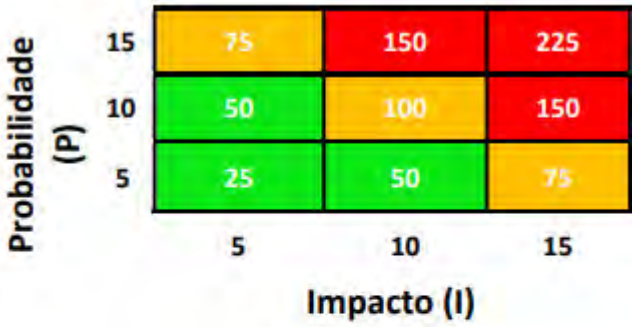


Tabela 9. Legenda de cores (CCGD, 2020).

Legenda (Cor)	Classificação do nível de risco
Verde	Baixo
Amarelo	Moderado
Vermelho	Alto

Em seguida, referido guia apresenta a Tabela 10, que refletirá uma análise do cenário atual (diagnóstico) do sistema que trata dados pessoais, visando identificar e avaliar os riscos.

Tabela 10. Riscos e níveis de riscos referente ao tratamento de dados pessoais (CCGD, 2020).

ID	RISCO REFERENTE AO TRATAMENTO DE DADOS PESSOAIS	P	I	NÍVEL DE RISCO (P X I)
R01	Acesso não autorizado.	10	15	150
R02	Modificação não autorizada.	10	15	150
R03	Perda	5	15	75
R04	Roubo	5	15	75
R05	Remoção não autorizada.	5	15	75
R06	Coleção excessiva.	10	10	100
R07	Informação insuficiente sobre a finalidade do tratamento.	10	15	150
R08	Tratamento sem consentimento do titular dos dados pessoais (Caso o tratamento não esteja previsto em legislação ou regulação pertinente).	10	15	150
R09	Falha em considerar os direitos do titular dos dados pessoais (Ex.: perda do direito de acesso).	5	15	75
R10	Compartilhar ou distribuir dados pessoais com terceiros fora da administração pública federal sem o consentimento do titular dos dados pessoais.	10	15	150
R11	Retenção prolongada de dados pessoais sem necessidade.	10	5	50
R12	Vinculação ou associação indevida, direta ou indireta, dos dados pessoais ao titular.	5	15	75
R13	Falha ou erro de processamento (Ex.: execução de script de banco de dados que atualiza dado pessoal com informação equivocada, ausência de validação dos dados de entrada etc.).	5	15	75
R14	Reidentificação de dados pseudonimizados.	5	15	75

Legenda: P – Probabilidade; I – Impacto.

Já o dano dependerá de comprovação e avaliação no caso concreto.

Podem haver situações que mesmo que sejam caracterizadas como risco baixo, o titular pode sofrer dano maior que o esperado, dependendo do caso concreto. Assim, deve ser considerado relevante o risco ou dano baixo.

Possibilidade 2 (baseada na experiência internacional):

1 - Introdução ao racional da classificação da criticidade dos incidentes proposta

Na tentativa de se aperfeiçoar a classificação desejada conforme a realidade nacional e levando-se em consideração as particularidades já postas na primeira resposta, com o fito de avaliarmos os riscos que estão diretamente correlacionados aos possíveis prejuízos e danos decorrentes do incidente ou das particularidades dos casos concretos, consideramos as seguintes perspectivas em relação ao incidente ocorrido ou dos riscos de tais eventos para atender ao exigido pelo enunciado:

- Do titular, em que prejuízos podem alcançar o comprometimento da própria subsistência ou danos permanentes à pessoa pela quebra da privacidade, sobretudo quando há dados sensíveis ou de histórico pessoal revelados, ou de características próprias que o diferencia dos demais;

- Da coletividade localizada, nas hipóteses de prejuízo local (Bairro, Cidade ou Estado) seja no tráfico comercial, oferta de serviços essenciais ou que também possam comprometer a segurança dos titulares afetados ou de quem estiver na localidade correspondente, ainda que de forma transitória.

Os esforços locais devem ser coordenados de acordo com as autoridades do espectro afetado para que os efeitos do incidente sejam mitigados;

- Da coletividade nacional, quando os dados afetados incluírem titulares de todos os Estados ou os sistemas comprometidos

	tenham informações de titulares de todos os Estados ou o alcance neles todos. Os esforços em âmbito nacional devem ser coordenados contando com as autoridades em todos os níveis e esferas de governo para que os efeitos do incidente sejam mitigados da melhor maneira possível; **- Da coletividade internacional,** quando os dados afetados incluírem titulares de todos os Continentes ou os sistemas comprometidos tenham informações de titulares de todos os Continentes ou alcance neles todos. Os esforços em escala internacional devem contar com apoio de entidades de fiscalização e supervisão do tratamento de dados pessoais daqueles países que tiveram titulares de sua nacionalidade afetados ou de blocos econômicos internacionais, ou ainda de órgãos supranacionais, a exemplo da Organização das Nações Unidas ou Organização Mundial do Comércio, por exemplo, para que os efeitos do incidente sejam mitigados. Com base nesses critérios consideramos: - Escala de **gravidade** de acordo com a extensão dos prejuízos acarretados ao titular e ao contexto social; - Possibilidade de haver circunstâncias laterais que podem ser associadas a quaisquer das **gravidades** e que exigirão cuidados específicos durante o contorno do incidente e mitigação de seus efeitos. Preferimos utilizar este critério para evitar excesso de níveis de gravidade e para otimizar a compreensão do cenário de prejuízos ocasionado pelo incidente e facilitando a aplicação de contramedidas conforme as mencionadas circunstâncias laterais, que serão identificadas pela expressão **agravantes**. A ideia de **agravante** aplicada no incidente carrega consigo a adição de ônus para o contorno do evento em razão da particularidade. De outro turno, pode haver situações específicas que admitem a existência diminuta de prejuízos eventualmente

	experimentados pelos titulares de dados, assim consideradas como **atenuantes**. Paralelamente, a ideia de **atenuante** no incidente implica na diminuição de ônus aplicáveis no contorno do evento em razão da particularidade que se identifica pela redução de prejuízos aos envolvidos. Considerando a particularidade brasileira, pode-se eventualmente pautar a gravidade (agravante/atenuante) em conformidade com o princípio da boa-fé. **1.1 - Classificação da gravidade dos incidentes envolvendo dados pessoais** A escala imaginada para classificação dos incidentes envolvendo dados pessoais, de forma decrescente descreve os incidentes com gravidade: **- Extrema:** Cenário de imprestabilidade dos sistemas (informatizados ou não) que dependiam das informações que foram comprometidas, revelando falta de confiança destes pela exposição elevada do titular e terceiros a ele vinculados a~~o~~ risco de suas liberdades, direitos e garantias jurídicas pelo comprometimento irreversível de sua privacidade ou de elevado número de titulares afetados. Situações que compreendam ameaça à segurança nacional, à independência dos poderes da República e às garantias constitucionais amplamente consideradas também devem merecer esse tipo de classificação. A título de exemplo, esta situação pode se configurar com a exposição de 'dados pessoais propriamente ditos' como o nome completo, a inscrição fiscal, data de nascimento e genitores do titular e cópias fiéis de documentos pessoais do titular. O incidente ocorrido no DETRAN-RN em 2019 e os mega vazamentos de dados em 2020 e 2021 seriam hipóteses dessas situações: https://olhardigital.com.br/2019/10/08/noticias/exclusivo-detran-vaza-dados-pessoais-de-quase-70-milhoes-de-brasileiros/

https://g1.globo.com/economia/tecnologia/noticia/2021/01/28/vazamento-de-dados-de-223-milhoes-de-brasileiros-o-que-se-sabe-e-o-que-falta-saber.ghtml

https://g1.globo.com/economia/tecnologia/noticia/2020/12/02/nova-falha-do-ministerio-da-saude-expoe-dados-de-243-milhoes-de-brasileiros-na-internet-diz-jornal.ghtml

A exposição dos dados da forma feita põe em xeque a confiabilidade da solicitação das informações vazadas como fatores de autenticação do titular, o que demandaria a implementação de mecanismo adicional seguro para que o sistema de autenticação volte a ser confiável.

Em outras palavras, o comprometimento desses dados permite sucessivas violações de privacidade do titular, pois a partir destes é possível burlar a autenticidade de outros serviços ou direitos que o titular utilizar ou fizer jus, pois perderá o controle de seu direito à identidade.

Ou ainda, quando se detecta a impossibilidade no processamento dos dados pessoais do titular pelo controlador afetado de forma generalizada, o privando de não atender ao esperado acesso a serviços críticos ou essenciais pela coletividade ou pela incapacidade de cumprir com o exercício de determinado direito líquido e certo pelos titulares correspondentes.

- Severa: Essa classificação compreende situações que são deletérias ao titular afetado pois será compelido a suportar situações irreversíveis em relação à sua privacidade e que poderão exigir esforços de toda a sociedade para reverter os prejuízos causados ou às suas liberdades, direitos e garantias jurídicas;

A exposição de dados bancários, financeiros, fiscais, de saúde e dados sensíveis de forma ampla são exemplos fiéis da gravidade severa de incidentes envolvendo dados pessoais, a exemplo do ocorrido em novembro de 2020 que expôs dados de infecções de COVID-19:

https://g1.globo.com/bemestar/coronavirus/noticia/2020/11/26/vazamento-de-senhas-do-ministerio-da-saude-expoe-informacoes-

	de-pessoas-que-fizeram-testes-de-covid-19-diz-jornal.ghtml Ou ainda, quando se detecta a impossibilidade no processamento dos dados pessoais do titular pelo controlador afetado de forma parcial, o privando de atender ao esperado acesso a serviços críticos ou essenciais a grupo limitado de titulares ou pela incapacidade de cumprir com o exercício de determinado direito líquido e certo destes. Os incidentes inicialmente enquadrados nesta categoria poderão ser reclassificados como de gravidade 'Extrema' se forem detectadas as características daquele tipo caso os impactos percebidos evoluam. **- Intensa:** Incidentes desta natureza compreendem prejuízos de ordem transitória ao titular e ao controlador no que tange o exercício de direitos ou atribuição de obrigações ou deveres, pois os dados comprometidos podem ser re-atribuídos ao titular para que a confiabilidade do sistema volte a ser estabelecida. A exposição indevida de números de cartões de crédito ou de nome de usuário e senha poderiam ser hipóteses destes casos. Esses incidentes podem ter a gravidade aumentada se os nomes de usuário e senha comprometidos permitirem situações elencadas nas características de 'Severa' ou 'Extrema'. **- Simples:** Sem características das gravidades anteriores. **1.2 - Situações laterais que exigem cuidados direcionados aos incidentes envolvendo dados pessoais - agravantes** Complementarmente à classificação anterior, existem situações laterais que demandam cuidados direcionados à melhor mitigação do incidente e seus efeitos, conforme já mencionado anteriormente, serão consideradas como **agravantes**. Particularidades aos tipos de dados e titulares afetados revelam a existência dessas circunstâncias. A título de exemplo, é possível identificar situação do incidente quando atinge dados de titulares com dificuldades de exercer autodefesa ou que exista situação de vulnerabilidade

ou hipervulnerabilidade, isto é, quando o incidente envolver dados de crianças, adolescentes (art. 14 da LGPD), superendividados, deficientes, idosos dentre outros.

A partir dessas linhas gerais, analisaremos a **gravidade** dos incidentes e possíveis **agravantes** ou **atenuantes**.

2 - Avaliação de riscos considerando o tipo de atributo da informação que foi comprometido

2.1 - Confidencialidade:

A regra geral a ser considerada é que este atributo sempre será afetado em incidentes de segurança, ainda que seja apenas em relação ao sujeito de direito que acessou os dados de forma não prevista ou não autorizada.

Todavia, tais incidentes podem ser considerados inócuos se as informações atingidas disserem respeito a dados pessoais com acesso público, uma vez que já são passíveis de conhecimento por amplo espectro de sujeitos de direito.

Afinal, não é plausível que exista comprometimento de sigilo de dados que são abertos.

Portanto, à exceção dos casos de informações com acesso público, que não apresentam qualquer tipo de prejuízo efetivo, aquelas que forem classificadas como internas, sigilosas, secretas, ultrassecretas, confidenciais ou indicações afins pressupõem a gravidade do incidente envolvendo dados pessoais.

Com isso, convêm atribuir duas classificações possíveis a esses cenários:

- Com gravidade

- Sem gravidade

2.1.1 - Grau de eficácia das medidas de ofuscação, criptografia ou técnica diversa para impedir o conhecimento dos dados que foram comprometidos.

Complementarmente às razões iniciais deste indicador, efeito

	similar a dados que estão ao alcance de todos, é a inteligibilidade das informações que foram comprometidas, pois, se aquilo que foi comprometido estiver submetido a grau intransponível de criptografia, cuja decifragem pode levar 100 (cem) anos ou mais com esforços computacionais acentuados, também não cabe considerá-los como capazes de gerar prejuízo. Dependendo do grau de ofuscação dos dados para impedir a organização dos dados atingidos pode se caracterizar como suficiente para se considerar como '**sem gravidade**' quando restarem apenas informações que são essencialmente de acesso público. Então, análise mais acurada sobre os dados inicialmente comprometidos em sua confidencialidade pode resultar em: - Considerados como **sem gravidade** sempre que inacessíveis, seja por criptografia hígida ou ofuscação exemplar; - Confirmados **com gravidade** quando avaliação concluir que são parcialmente acessíveis ou dedutíveis quando a criptografia não for suficientemente forte ou quando a ofuscação de dados for precária. **2.2 - Disponibilidade:** Os dados podem ter sido indevidamente excluídos da base atingida além do acesso não previsto ou não autorizado, o que poderá trazer prejuízos ao titular de dados ou seu controlador em situações de execução de obrigações, sobretudo. Nesse sentido, os bens da vida que podem ser afetados pela dificuldade no cumprimento de tais obrigações podem revelar graus 'Severos' ou 'Extremos' de incidentes envolvendo dados pessoais a partir da indisponibilidade desses, pois podem afetar direitos do titular de modo a comprometer sua sobrevivência ou de outras pessoas que dependam de seus recursos que eventualmente foram tornados inacessíveis. Existe possibilidade de incidentes que afetem a **disponibilidade** dos dados também serem considerados como '**sem gravidade**', desde que se comprove que as informações afetadas sejam inúteis ou possam ser identificadas como tal.

Partindo do pressuposto que a **disponibilidade** está essencialmente vinculada à capacidade de os dados estarem aptos para acesso e processamento, o comprometimento deste atributo inviabiliza o próprio tratamento, diferentemente da situação mencionada na **confidencialidade**, em que a hipótese de '**sem gravidade**' consiste na brecha de dados de acesso público, sem qualquer interferência na atividade de tratamento.

Assim, as hipóteses de incidentes de dados pessoais que se baseiam no comprometimento da **disponibilidade** e que possam ser classificados como '**sem gravidade**' gravitam situações de dados já inúteis para o tratamento ou quando se demonstrar que o período de inacessibilidade não produziu prejuízo a nenhum titular.

2.3 - Integridade:

Paralelamente ao atributo da disponibilidade, também pode ser comprometido o atributo da integridade, em que há a alteração indevida dos dados pessoais dos titulares na base do controlador, podendo gerar efeitos similares ao comprometimento da **disponibilidade** quando prejudicam as partes envolvidas pela dificuldade no cumprimento de execução obrigacional, exercício de direitos ou acesso a determinadas garantias e liberdades individuais.

Diferentemente do comprometimento da **disponibilidade**, os efeitos decorrentes do ataque à integridade dos dados pode demorar a ser percebida ou até mesmo impossível de se determinar sem o auxílio de terceiros para comparação de bases de dados na eventualidade de inexistência de cópias de segurança do próprio controlador aptas a tal confrontação.

Por isso, a incerteza da integridade dos dados dos titulares por parte do controlador deve ser considerada como uma **agravante**, demandando o auxílio por parte da ANPD ou entidade apta a auxiliar na investigação da dimensão dos prejuízos e grau de comprometimento dos dados dos titulares por parte do controlador para que a situação seja solucionada adequadamente.

As hipóteses que eventualmente se admitem como '**sem gravidade**' para o comprometimento da integridade dos dados

pessoais são similares a eventos que afetem a **disponibilidade** no que diz respeito à utilidade dos dados que foram atingidos.

Tal se deve, pois, a adulteração indevida de dados pessoais implica em esperados resultados indesejados do tratamento, ainda que o número de titulares afetados seja mínimo.

Ainda em caráter excepcional, poderá haver contorno de incidentes que afetem a **integridade** demonstrando-se que os dados afetados foram corrigidos a tempo de o titular respectivo não ter sofrido nenhum impacto, o que deverá ser levado em consideração na apuração das sanções eventualmente aplicáveis,

Contudo, classificar o incidente como '**sem gravidade**' nessas hipóteses pode ser temerário, sobretudo pelo tipo de exploração causada no banco de dados.

3 - Avaliação de riscos considerando os tipos de dados afetados

Conforme já indicado no ponto 1 desta resposta, o tipo de dado afetado é variável essencial para se dimensionar a gravidade do ocorrido de acordo com a criticidade em relação ao titular.

3.1 - Dados pessoais propriamente ditos ou cadastrais:

Dados do titular que disserem respeito a registros cadastrais ordinários, a exemplo do próprio nome, data de nascimento, identificação fiscal, registro civil, endereço, estado civil etc. e que normalmente são utilizados para formalizar operações negociais em seu nome.

A gravidade dos incidentes que comprometem esses dados pode variar desde 'Severa' a 'Extrema', conforme já indicado.

3.2 - Dados sensíveis:

Incidentes envolvendo esse tipo de informação pode revelar risco à integridade física, psíquica e eventualmente de subsistência por parte do titular, uma vez que certos dados podem quebrar a confiança de eventual empregador ou contratante e comprometer sua renda e sustento.

Isso porque terceiros podem utilizar de tais informações sensíveis para fins discriminatórios, se admitindo haver sujeição do titular a escrutínio público, a ações persecutórias ou de alguma forma exploradas como vulnerabilidades da pessoa, o que, '*per se*' deve merecer o '*status*' de Severo, conforme já indicado anteriormente.

Esta classificação deve também ser aplicada quando o incidente de segurança envolvendo dados pessoais admita associação das informações do titular com seus dados sensíveis e os efeitos descritos no parágrafo anterior sejam percebidos ou se depreende que tais resultados sejam esperados pelas particularidades do caso concreto.

3.3 - Dados de comportamentos históricos pessoais:

Dados do titular que revelam atos praticados ou registrados, podendo ser comunicações privadas, opiniões ou decisões a respeito de seus atos, o que, de forma similar ao comprometimento de dados sensíveis, pode também ocasionar comprometer a integridade física, psíquica e eventualmente de subsistência por parte do titular em virtude de atos discriminatórios, de escrutínio público, persecutórios ou que de alguma forma explorarem tais dados como vulnerabilidades da pessoa.

Seguindo o racional para os 'dados sensíveis', os incidentes contendo esse tipo de dados também merece o '*status*' de 'Severo'.

Esta classificação deve também ser aplicada quando o incidente de segurança envolvendo dados de comportamentos históricos pessoais permitam a associação das informações do titular e o sujeitem aos efeitos prejudiciais já mencionados, tanto quando percebidos ou razoavelmente se conclui que tais resultados sejam esperados pelas particularidades do caso concreto.

4 - Avaliação de riscos considerando a atualização dos dados tratados

Deve-se também levar em consideração a atualização dos dados que tratados, pois se as informações envolvidas no incidente estiverem desatualizadas os riscos se atenuam, sobretudo aqueles

que digam respeito à autenticidade de atos praticados pelo titular.

Por isso, sempre que houver a constatação de desatualização dos dados comprometidos, pode se considerar como **atenuante** do risco do tratamento de dados pessoais em atenção aos possíveis prejuízos que o titular pode estar sujeito.

Essa atenuante pode ser de aplicação:

- Remota quando os dados afetados tiveram a última modificação desejada ou confirmação no intervalo de 3-6 (três a seis) meses;

- Improvável quando os dados afetados tiveram a última modificação desejada ou confirmação no intervalo de 9-24 (nove e vinte e quatro) meses;

- Possível quando os dados afetados tiveram a última modificação desejada ou confirmação no intervalo de 25-60 (vinte e cinco a sessenta) meses;

- Esperada quando os dados afetados tiverem a última modificação desejada ou confirmação em período que supera 60 (sessenta) meses.

5 - Avaliação de riscos considerando as características particulares do titular

Além dos tipos de dados que eventualmente são afetados, deve-se levar em consideração eventual característica particular do titular afetado, podendo ser:

5.1 - De vulnerabilidade ou hipervulnerabilidade

Complementando a parte introdutória desta resposta, situações que envolvam o comprometimento de dados de titulares vulneráveis ou hipervulneráveis revelam condição que demanda cuidado especial na resposta e contorno do incidente havido, sendo uma **agravantes** nos termos sugeridos neste estudo.

Retomando os exemplos já indicados, estão nesta categoria as ‘crianças’ ou ‘adolescentes’, ‘idosos’, ‘deficientes’, ‘pessoa em superendividamento’ e outras que a legislação e a experiência

jurídica assim determinarem ou equipararem funcionalmente.

Tal cuidado especial se deve para que a exposição indevida de dados e informações das pessoas enquadradas em tais estados de vulnerabilidade seja não apenas respondida de forma a cessar o incidente com tenacidade, mas, de práticas proativas de modo a evitar maiores prejuízos aos direitos daqueles que foram atingidos, sempre que possível.

Isso porque a condição de vulnerabilidade já pressupõe dificuldades de autodefesa do titular em atenção a práticas abusivas, predatórias ou planejadas para se tirar vantagem desse, o que pode ser tão comprometedor quanto às situações elencadas nos dados pessoais sensíveis ou de histórico pessoal.

Demais das situações abusivas e predatórias que já são por muito conhecidas pelo Direito, as ameaças planejadas aos vulneráveis podem reunir elementos de convencimento que o titular esteja habituado, confortável e seguro, lhe transformando em alvo de uma fraude ou até mesmo práticas comerciais ilícitas, e.g., publicidade de jogos ou brinquedos favoritos direcionada a determinadas 'crianças e adolescentes', crédito consignado a 'idosos' que já possuam contratação com determinado banco ou ofertas de regularização de nome a 'superendividados' etc.

Exemplos de contramedidas a incidentes que prejudiquem vulneráveis envolvem adicionar camada de segurança para etapas de autenticação, podendo ser outra pessoa vinculada ao vulnerável, preferencialmente responsável legal ou de alguma forma pessoa de confiança por ele confirmada, podendo ser implementada como salvaguarda anterior ao incidente, inclusive, o que se recomenda.

Se mostra razoável, também, que entidades encarregadas ou com missão de proteção dos direitos dos vulneráveis ou hipervulneráveis sejam também incluídas nas rotinas de contato e providências por parte da ANPD em atenção ao controlador envolvido no incidente e aos titulares afetados, especialmente para proteção das liberdades e direitos que estiverem a seus alcances.

5.2 - De Funções ou Cargos Públicos exercidos

	Essas características já estão presentes em norma correlata ao assunto, qual seja a capitulação em incidente de segurança da informação em relação à invasão de dispositivos informáticos, assim capitulados no § 5º do artigo 154-A do Código Penal como circunstâncias de aumento de pena. Como decorrência lógica de interpretação sistemática, se os dispositivos comprometidos das pessoas que exercem tais cargos ou funções implicam em hipótese de crime mais intenso, os dados pessoais que lhes dizem respeito também devem merecer especial atenção quando envolvidos em incidentes de segurança da informação. As mencionadas funções e cargos públicos são: - Presidente da República, governadores e prefeitos; - Presidente do Supremo Tribunal Federal; - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou - Dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal. Esta **agravante** pode exigir o envolvimento de Procuradores das esferas correspondentes de jurisdição para acompanhar a tomada de providências por parte do controlador afetado, da ANPD e outras entidades que participarem da investigação ou tratamento do incidente, sobretudo para estarem aptos a exercer os deveres de ofício em atenção às violações havidas. É razoável que exista a extensão desta **agravante** aos pares dos cargos e funções descritas, pois o comprometimento dos dados pessoais das pessoas que ocupam tais posições pode impor situação prejudicial ao bem comum em relação ao titular afetado e funções análogas nos três poderes que não foram mencionadas, a exemplo: - Dos Ministros ou Secretários de Estado; - De juízes de direito;

- Parlamentares nas três esferas de governo;

- Presidente e membros da diretoria de empresas públicas, de economia mista ou autarquia, incluindo a ANPD.

5.3 - Da Internacionalidade de titulares

Outra circunstância lateral que deve ser considerada como **agravante** é a internacionalidade dos titulares afetados.

A situação descrita poderá envolver demais legislações de proteção de dados estrangeiras e demandar contato com entidades de proteção de dados internacionais para contorno adequado do incidente havido.

A existência dessa **agravante** pode requerer a comunicação do controlador que detinha as obrigações de custódia dos dados à autoridade do país cujos titulares foram afetados ou também pela ANPD, de forma subsidiária ou complementar.

Deve-se admitir a possibilidade de inclusão de órgãos supranacionais dependendo do número de nacionalidades dos titulares afetados a partir desta **agravante** para que auxiliem no contorno e mitigação dos prejuízos sofridos pelos titulares, sobretudo em hipóteses classificadas como 'Severas' ou 'Extremas'.

6 - Avaliação de risco pela existência de alerta ou comunicação prévia da ANPD (sanção de advertência ou mais graves) ou entidade diversa com especialidade técnica em proteção de dados pessoais, direitos do consumidor, difusos em geral.

Este indicador de **agravante** ao risco de haver incidente de segurança envolvendo dados pessoais e que, adicionalmente, possui impacto direto em eventual dosimetria na sanção ao Controlador ou Operador, pois já estariam cientes das vulnerabilidades ou medidas complementares que deveriam ser tomadas em razão do cenário identificado por eventual Relatório de Impacto ou Avaliação de Vulnerabilidades presentes nas operações de tratamento e dados pessoais que executa, influenciando tanto nos riscos quanto em um eventual incidente e nos danos que causaria.

	Já sabedores da condição de insegurança presente, a inércia, demora ou singela falta de atenção ao princípio da prevenção para solucionar a origem de risco conhecido pode ser considerada como **agravante** nesta medida.
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	Para se apresentar a distinção entre risco e dano, é necessário que, primeiramente, seja realizada a identificação dos conceitos, haja vista que risco no contexto de proteção de dados se refere às operações que possam causar "danos físicos, materiais ou imateriais" a uma determinada pessoa, segundo o Council of the European Union (2016) (tradução nossa). Ou seja, o conceito de risco se refere a uma probabilidade de ocorrência, que no caso de efetivação dará ensejo a um dano. Deste modo, o conceito de risco precede o de dano, na medida que este último é uma consequência do primeiro, pois sem o risco não há possibilidade de o dano ocorrer. Em consideração ao fato de que o dano se refere à prejuízos causados a determinados indivíduos, temos, como exemplos, segundo Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho: > a perda de controlo sobre os seus dados pessoais, a limitação dos seus direitos, a discriminação, o roubo ou usurpação da identidade, perdas financeiras, a inversão não autorizada da pseudonimização, danos para a reputação, a perda de confidencialidade de dados pessoais protegidos por sigilo profissional ou qualquer outra desvantagem económica ou social significativa das pessoas singulares. Entretanto, embora o dano dependa do risco para ocorrer, não é possível generalizar que todo o risco gerará um dano, na medida em que este pode acontecer ou não, a depender do nível de risco, conforme parâmetros já apresentados na questão anterior. Logo, a relação entre os conceitos decorre do fato de o dano evoluir a partir do risco, sendo assim, quanto maior a minimização de risco, menor também será a possibilidade de ocorrer o dano.

O que deve ser considerado na avaliação dos riscos do incidente?	Em consideração ao fato de que a avaliação tem como objetivo monitorar os riscos relativos à utilização de dados pessoais (Commission Natiole Informatique & Libertés, 2018, p. 53) (tradução nossa), inicialmente, deve ser realizada a identificação objetiva dos tratamentos que possam gerar riscos aos titulares de dados (Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho). Assim, devem ser considerados na avaliação dos riscos de incidente os atendimentos aos princípios legais quando do tratamento de dados, os riscos que os envolvem e as suas origens, os meios pelos quais os riscos podem dar origem a um dano, qual a classificação do risco e as medidas que podem ser tomadas para evitar o risco e para minimizar os danos no caso de ocorrência (Commission Natiole Informatique & Libertés, 2018, p. 53/54) (tradução nossa). Com a avaliação de risco do incidente e do conhecimento à respeito da possibilidade de ocorrência de risco e, portanto, de dano, caberão aos agentes responsáveis pelo tratamento de dados realizarem medidas que comprovem estar de acordo com o previsto nas normas de proteção de dados (Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho). Além disso, caberá aos agentes a realização de medidas que atenuem os riscos por meio de providências que possam diminuir a ocorrência do dano relativo a determinado tratamento, isso em razão do disposto no art. 46 da LGPD, que prevê como dever do agente a adoção de "medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais" (Lei Geral de Proteção de Dados Pessoais, 2018). Complementarmente aos critérios anteriores que amplamente são adotados pela experiência jurídica internacional baseada no paradigma europeu da proteção de dados pessoais durante seu tratamento, deve-se levar em consideração características particulares do contexto social e jurídico que se pretende balizar, conforme exposto na primeira resposta, o que permitirá particularização detida para melhores resultados.
Quais informações os controladores devem	● Tipo de notificação – completa, inicial ou complementar; ● Nome, contato e outras informações do controlador e do Encarregado para que possam ser obtidas outras informações.

notificar à ANPD, além daquelas já listadas no §1º do art. 48? I - a descrição da natureza dos dados pessoais afetados; II - as informações sobre os titulares envolvidos; III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; IV - os riscos relacionados ao incidente; V - os motivos da demora, no caso de a comunicação não ter sido imediata; e VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo. Bases utilizadas para a proposta: Artigo 33 do GDPR; Artículo 21 e 22 da Ley n° 25.326/2000 Argentina; Artículo 34 da Ley n° 18331/2008 e Artículo 4 do Decreto 64/020 Uruguai; Formulário da CNIL - França, disponível em: https://notifications.cnil.fr/notifications/index	• Nome, contato e outras informações do operador e seu eventual Encarregado para que possam ser obtidas outras informações. • Se os dados foram, antes do incidente, compartilhados ou transferidos a terceiros; se sim, quais, com quem e a finalidade. • Data e hora da detecção. Detalhamento e Comentários sobre forma da detecção. • Data e hora do incidente e sua duração. Comentários sobre as circunstâncias da violação. • Tipos de dados afetados, Número de titulares atingidos, quando não possível, número aproximado e justificativa sobre indicação por aproximação, além do inciso II. • Número de titulares, natureza e finalidade de dados *não* afetados. • Se sensíveis ou de comportamento histórico pessoal, se estavam anonimizados ou não, além do inciso I. • Indicação na natureza da violação e gravidade, de eventuais condições agravante ou atenuantes identificadas atendendo ao inciso IV. • Medidas implementadas para controlar os possíveis danos e riscos dos demais dados, conforme o inciso IV. • Meios que adotaram para realizar a comunicação aos titulares sobre as medidas implementadas para controlar os possíveis danos, mitigá-los ou resolvê-los. • Meios que adotaram para realizar a comunicação aos titulares sobre quais dados não foram afetados e o tempo de armazenamento. • Origem e formas da violação de segurança de dados pessoais. • Vulnerabilidades encontradas após o incidente e as medidas de correção adotadas. • Possíveis circunstâncias ou implicações de natureza transfronteiriça. • Outras informações úteis às pessoas afetadas para proteger seus dados ou prevenir possíveis danos.
Qual o prazo razoável para que controladores	Considerando que o Artículo 4 do Decreto 64/020 do Uruguai e o artigo 33(1) do Regulamento Geral sobre a Proteção de

informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	Dados da União Europeia, bem como diversas normas correlatas que estabelecem **o prazo de 72h** para a notificação da autoridade e que a comunicação ao titular dos dados seja efetuada "sem demora injustificada". Sendo que no Brasil há disposição no Decreto nº 9.936/19 (que regulamenta a Lei do Cadastro Positivo), determinando que a comunicação deve ser feita à própria ANPD e outras instituições em **dois dias úteis** da **data do conhecimento do incidente,** assegurando "a pronta comunicação aos cadastrados afetados pelo incidente de segurança" (art. 18, I e §§ 1º e 2º). Ainda, que os prazos de dois dias úteis anteriormente indicados compreendem incidentes de dados contidos nas bases de cadastro positivo e dizem respeito essencialmente a características de dados cadastrais ou de certos comportamentos históricos (pagamentos, sobretudo), situações envolvendo dados sensíveis ou que afetem essencialmente vulneráveis ou hipervulneráveis demandam maior rapidez para comunicação exatamente pela criticidade e prejuízos sucessivos que podem vir a ocorrer. Assim, com vistas a atender à conformidade de regramentos internacionais, a regra geral para comunicação à ANPD deve ser o máximo de 72h, devendo ser diminuído para: - Até 24h caso haja comprometimento de dados sensíveis, de comportamentos históricos ou se os dados afetados sejam essencialmente de pessoas vulneráveis ou hipervulneráveis; - Até 48h caso haja comprometimento de dados de titulares de outras nacionalidades além da brasileira ou se afetarem pessoas ocupando cargos públicos conforme balizado na seção de avaliação de risco. Conforme o cenário posto e avaliação conjunta com a ANPD haverá a comunicação ao titular afetado dentro do prazo que se entender como adequado e com o detalhamento compatível com a natureza do incidente e dos dados atingidos. Desta forma, há incentivo para que as empresas façam a comunicação imediata aos afetados pelo incidente e, ainda, há

	o atendimento às regras da União Europeia.
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	**1. Prazos e Regra Geral** O prazo para comunicação de um incidente deve levar em conta a classificação proposta. O tempo de comunicação de um incidente significa o equilíbrio entre a gravidade de dada circunstância e o tempo de conhecimento pelos titulares e autoridade responsável a fim de, diante de dada situação, os titulares evitarem danos futuros. Como exposto acima, por exemplo, o prazo para comunicação à ANPD de incidentes envolvendo dados cadastrais é de 72 horas. O artigo 48, *caput* da LGPD em relação ao dever de informar a ANPD **e** o titular é claro, contudo, entendemos que diante de determinados fatores do incidente, no que diz respeito ao tipo de dados e aos titulares envolvidos, deve-se comunicar, em primeiro lugar, a agência e, em seguida, a partir de sua decisão, comunicar os titulares; por outro lado, diante de outros fatores do incidente, deve-se comunicar, ao mesmo tempo, titulares e ANPD. Não se deixará de comunicar os titulares, mas há algumas questões as quais pedem atenção no diferente tratamento na comunicação à ANPD e aos titulares, por exemplo, ao se ter a resposta da agência, consegue-se informar melhor ao titular sobre a gravidade envolvida e o que tem sido feito, conjuntamente, entre controlador e agência no sentido de diminuir e evitar futuros riscos e danos à segurança dos dados pessoais. Essa lógica, para funcionar, depende, em primeiro lugar, da espécie de informação envolvida, ou seja, se se trata de a) dados pessoais propriamente ditos b) dados sensíveis c) dados de comportamentos históricos Em segundo lugar, depende das pessoas dos titulares envolvidos ou agravante: d) vulneráveis ou hipervulneráveis

e) integrante de cargo público ou função pública
f) titulares com internacionalidade

Se o incidente envolver “a”, levando em conta o Decreto nº 9.936/2019, art. 18, o prazo será de até 72 horas a partir da decisão da agência.

Se o incidente envolver “b” e “c”, o prazo será de até 24 horas da decisão da agência.

Se o incidente envolver “d”, o prazo segue a mesma lógica para “b”.

Se o incidente envolver “e” e “f”, o prazo será de 48 horas, concomitantemente, para a ANPD e titulares.

Deve-se notar que a diminuição dos prazos se deu para os casos nos quais os titulares e a natureza dos dados envolvidos demandam maior celeridade na resposta a eventuais riscos ou danos. É o caso de dados pessoais sensíveis ou de pessoas vulneráveis.

De forma resumida, a lógica dos prazos pode ser entendida como sendo de 24 horas para dados sensíveis e de 72 horas para dados pessoais propriamente ditos e dados de comportamentos históricos. Se, contudo, os titulares destes dois últimos tipos de dados forem de pessoas vulneráveis, o prazo é de 24 horas e se for de integrante de cargo público ou de titular com intencionalidade, o prazo é de 48 horas. Independentemente do titular, se o dado for sensível o prazo é de 24 horas.

2. Casos Especiais

Partindo e tomando como premissas os princípios da prevenção e da transparência, quanto ao prazo, excluem-se os casos os quais envolvem situações atenuantes, pois o juízo seria feito previamente pelo próprio controlador o que, em decisão e análise posterior pela agência, não se verifica situação atenuante, resultando isso em um prazo maior para comunicação e não equilibrando o possível risco ou dano envolvido com o tempo hábil para resposta e prevenção.

Na comunicação com a agência, o juízo do controlador deverá

	ser transmitido e fundamentado, levando em conta as atenuantes, as quais podem comprovar a baixa gravidade de um incidente, mas, em relação ao prazo, tal juízo não é cabível. Ademais, no decorrer de decisões, a criação de parâmetros e adoção de certificados de segurança podem ajudar o controlador a atuar de forma mais equilibrada, pois ao comprovar que se adotam determinados critérios de segurança requisitados pela agência na proteção de dados e que estão de acordo com os exames de finalidade, necessidade e adequação, o prazo poderá ser maior. Tais casos especiais podem ser colocados entre dois extremos e, com isso, independentemente, da espécie de dado envolvida e do titular. Um primeiro extremo é o da ampla publicidade e conhecimento geral de dados pessoais envolvidos em algum incidente de segurança. O outro extremo é o da intransponibilidade da criptografia de dados pessoais de algum incidente de segurança. Nesse meio, há casos que compreendem as agravantes e atenuantes. a) Então, para dados que são de acesso público, o prazo para comunicação aos titulares segue o período de 72 horas da decisão da ANPD. b) Para dados criptografados, o prazo para comunicação aos titulares segue o mesmo período de 72 horas da decisão da ANPD. **3. Conteúdo do comunicado de incidente de segurança:** Recomendação comum a todos os cenários, além do já previsto pelo §1º do art. 48, na comunicação aos titulares, é que devem ser eles informados sobre: a) os risco e danos envolvidos previstos pelo controlador e, caso já houver um juízo da ANPD, os previstos por esta; b) os meios utilizados como forma de contenção e mitigação e até regressão dos riscos e dados identificados; c) o setor ou local de onde os dados foram afetados ou vazados; d) a data, hora com fuso respectivo;

	e) se houve e quando houve comunicação à ANPD; f) atualização constante sobre tais informações; g) por fim, a linguagem, a qual pode ser muito técnica e de complexo entendimento, deve ser sempre clara e objetiva (Art. 34 (2));
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	A comunicação do incidente ao titular deverá, preferencialmente, ser feita pelo meio utilizado por ele para fazer o cadastro ou para solicitar o serviço como e-mail, telefone, whatsapp, entre outros. Ademais, a forma de comunicação deverá levar em conta a natureza dos dados pessoais envolvidos no incidente de segurança. Desse modo, a partir das classificações feitas no tópico anterior, se os dados envolvidos são sensíveis ou de crianças e adolescentes, deve-se proceder no sentido de manter o máximo possível a discrição na identificação do titular com seus dados e, ao mesmo tempo, de garantir que houve o recebimento da informação de incidente, ou seja, comunicar diretamente por e-mail pessoal e por telefone. Caso muito diverso, é a comunicação pública. Como se trata de dados pessoais, a publicidade pode, na verdade, prejudicar ainda mais a intimidade dos titulares, por outro lado, é do interesse público saber da reputação e das medidas tomadas pela empresa envolvida no caso. Dentro dessa dualidade, é mais acertado tomar tal postura a partir da decisão da ANPD (Art. 48, §2º, I.), podendo ser ela contestada pela empresa se, por exemplo, houve mitigação de riscos e danos, se há criptografia e se é possível informar individualmente a todos os titulares em tempo hábil. O prazo, então, será dado a partir da decisão da ANPD. A publicização, por outro lado, pode servir como forma de alertar e informar de modo mais eficaz o titular, sem haver uma identificação, de que houve algum risco ou danos a seus dados pessoais. Por fim, novamente, no caso de grandes vazamentos de dados pessoais, faz sentido a comunicação pelos meios registrados de contato e, também, como nota à imprensa. Nesse caso, a

	empresa deve tomar tal postura imediatamente da identificação de tal natureza de incidente de segurança.

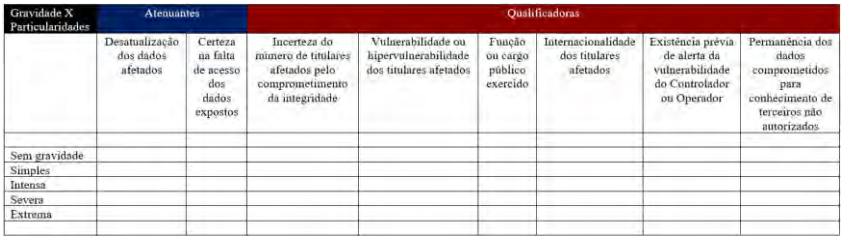
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	Nem todo incidente de segurança necessariamente envolve vazamento de dados pessoais. Quando não houver envolvimento com tais dados, a comunicação à ANPD não é obrigatória. Por sua vez, há incidentes que envolvem dados pessoais, mas não são hábeis a acarretar risco ou dano de caráter relevante. Os riscos ou danos são considerados relevantes quando impedem ou dificultam o tratamento de dados relacionados a direitos e garantias fundamentais (especialmente a intimidade e a privacidade); a dados de crianças, adolescentes e idosos; a dados sensíveis e aqueles relacionados a atividades profissionais, de consumo e de crédito. Contudo, independentemente da caracterização de risco ou dano relevante, adotamos o entendimento de que a ANPD deverá ser comunicada sobre todos os incidentes de vazamento de dados, invariavelmente. A notificação não se restringe aos vazamentos de dados tão corriqueiros, mas de todo e qualquer incidente de segurança, de origem interna ou externa. Tal comunicação obrigatória decorre do dever de prestar contas de forma transparente, guardando fundamentação no princípio da transparência e da responsabilização e prestação de contas, previstos, respectivamente, no art. 6º, VI e X da LGPD. Além disso, todas as violações de dados deverão ser obrigatoriamente documentadas e a empresa também pode precisar (ou posteriormente ser exigida pela ANPD) atualizar e/ou remediar medidas e procedimentos técnicos de segurança de dados pessoais e mitigação de riscos. Por fim, de acordo com o artigo 48 da LGPD, é obrigação do controlador a comunicação do incidente de segurança. Contudo, nas hipóteses em que um terceiro ou parceiro operador tenha assumido a responsabilidade pelo incidente e informado imediatamente a Autoridade Nacional, o controlador ficaria isento da obrigação de notificar o incidente, embora deva manter um relatório circunstanciado de todas as medidas adotadas para o caso de eventual fiscalização.

Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	Em caso de incidente de dados, o controlador deve, em curto período de tempo, verificar se ocorreu ou não uma violação de fato. A investigação inicial deve começar rapidamente, estabelecendo-se um grau razoável de certeza se ocorreu uma violação e as possíveis consequências para os indivíduos. Como resultado desta avaliação, os possíveis resultados com relação aos direitos dos titulares são: (i) o incidente não gerou risco ou não possui gravidade; (ii) o incidente gerou risco ou dano relevante; (iii) o incidente gerou risco ou dano intenso; (iv) o incidente gerou risco ou dano severo; e (v) o incidente gerou risco ou dano extremo. A avaliação do risco é imprescindível para a correta comunicação e esclarecimentos aos titulares. Ainda que se trate de incidente que não tenha gerado risco ou mesmo quando o dano possa não acarretar gravidade aos direitos e garantias individuais dos titulares, adotamos o entendimento de que não só a ANPD deve ser sempre comunicada como também todos os titulares dos dados, em qualquer situação ou incidente de dados. Por outras palavras, qualquer tipo de violação, independentemente de sua natureza, sensibilidade, volume de dados pessoais, número de titulares e caracterização de prejuízo é reputada importante e deve ser comunicada aos titulares de dados, em respeito ao princípio da transparência e ao direito potestativo de todos os titulares, pelo que sugerimos, inclusive, a inclusão de um inciso no artigo 18 da Lei 13.709/18 prevendo explicitamente tal direito. Isto porque o direito do cidadão à efetiva proteção de seus dados pessoais não pode ser menosprezado em qualquer hipótese, nem mesmo diante das dificuldades práticas da tutela. Em primeiro lugar, devem ser protegidos todos aqueles que foram afetados. Com efeito, a constituição de uma sociedade livre, justa e solidária pressupõe que os agentes envolvidos ou atingidos por episódios de vazamentos de dados pessoais assumam o protagonismo na busca por soluções céleres que permitam reverter ou mitigar os efeitos do incidente de vazamento de dados, agindo de forma clara e transparente, de maneira que qualquer comunicação ao titular de dados deve compreender, no

	mínimo: informações sobre o próprio incidente em si, quando foi identificado, qual a sua natureza; as medidas de correção técnicas e de governança adotadas; planos de ação adequados para assegurar a efetiva prevenção de novas ocorrências e o balanço geral do incidente e os danos porventura acarretados. Outras informações poderão ser necessárias como exposto nas demais respostas. Além disso, a comunicação aos titulares tem um fator mitigador para possíveis incidentes futuros do mesmo controlador que não pode ser desprezado, uma vez que eles também estão em posição de tomar as medidas necessárias para evitar futuros danos aos seus direitos e garantias individuais.
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	É possível enumerar incontáveis tipos de comprometimentos quando existe um incidente de segurança, sobretudo pelas perspectivas possíveis de análise, que vão desde o mais individual (do titular afetado) até a coletividade que pode alcançar extensão global. Os critérios já foram apresentados nas duas primeiras respostas, dada a correlação lógica da temática entre o risco, dano e incidente. De todo modo, ao se examinar a experiência internacional, de se perceber classificação sugerida pela CISA (Cybersecurity &

	Infrastructure Security Agency) dos Estados Unidos da América, os níveis de severidade são sete, classificados de acordo com os efeitos provocados pelo incidente: - Segurança e Saúde Públicas; - Segurança Nacional; - Segurança da Economia; - Relações Exteriores; - Liberdades e direitos civis; e - Confiança pública. A severidade é conferida pela intensidade crescente de 0 a 5 (zero a cinco) em que o primeiro estágio revela falta de consequências do evento e o último estágio significa ameaça a serviços críticos em escala nacional, à estabilidade do governo ou à vida dos cidadãos, passando por graus de probabilidade. As baixas gravidades indexadas no estudo da CISA apenas dizem respeito à probabilidade de ocorrência de eventos que pudessem afetar ao menos um dos sete elementos que serviram como parâmetro considerando o amplo espectro da coletividade, o que não dispensa esforços para a identificação correta da classificação do incidente sob perspectiva do próprio titular afetado. Em atenção ao já indicado nas primeiras respostas, consideramos que no contexto brasileiro a gravidade é presumida pela situação de falta de confiabilidade no sigilo de dados pelos repetidos incidentes já ocorridos e com alcance indeterminado, desde que não sejam apenas dados com acesso público afetados com o incidente de segurança da informação havido e mesmo com baixo número de titulares afetados. Complementando os critérios já expostos nas primeiras respostas, existe variável que somente será relevante depois de ocorrido o incidente, qual seja a avaliação de **<u>atenuante</u>** a partir da comprovação: - **<u>Do número de acessos aos dados atingidos</u>**. Isso porque o número de acessos aos dados comprometidos pode ser determinante para se identificar a confiança ainda restante no conhecimento das informações afetadas em relação à autenticidade de transações vinculadas ao titular afetado ou da própria privacidade deste. Isto é, na eventualidade de ser comprovada a ausência de nenhum acesso aos dados comprometidos, a certeza na inexistência de compartilhamento indevido dessas informações

	pode implicar na consideração de **sem gravidade** ao incidente. Não é adequado aplicar o racional desta **atenuante** quando se constatar que houve poucos acessos aos dados comprometidos, pois passa-se à incerteza de novos compartilhamentos a partir desses. Por isso, conforme se sugeriu a consideração de existência de gravidade como padrão a ser desconstituído, não será possível atenuar a extensão de prejuízos decorrentes do incidente aos titulares. Por outro lado, quando o número de acessos não puder ser objetivamente identificado, a estimativa deve contar com a avaliação dos pontos seguintes: **- Da Duração da exposição da vulnerabilidade que deu causa ao incidente:** O tempo de exposição da vulnerabilidade que possibilitou a ocorrência do incidente pode ser variável relevante para se estimar o alcance das informações que tiveram o sigilo comprometido quando não for possível determinar a quantidade de acessos ao conjunto de dados afetados. Assim, quanto maior for o tempo de exposição da vulnerabilidade, mais plausível será a hipótese que houve acesso não autorizado dos dados pessoais sujeitos à fraqueza do sistema identificada, ainda que impossível de se determinar com certeza tal cenário. Em relação a esta variável, não é possível se chegar a conclusões que **agravem** ou **atenuem** a ocorrência dos prejuízos a partir dos incidentes envolvendo dados pessoais, pois o fator determinante será a quantidade efetiva de acessos, sobretudo porque neste estudo se presume a ocorrência de gravidade do incidente, devendo sua ausência ser demonstrada pelo controlador atingido. **- Disponibilidade dos dados comprometidos para conhecimento indevido de terceiros:** Quando houver a disponibilização dos dados afetados em ambiente com intuito de compartilhamento com terceiros a situação pode ser considerada como **agravante** do incidente, pois exigirá a contramedida adequada para retirada sempre que se constatar tal fato, de modo a mitigar os efeitos do incidente ocorrido. O cuidado no tratamento do incidente poderá contar com

	colaboração da ANPD perante outras autoridades de proteção de dados pessoais caso o domínio que hospeda o compartilhamento indevido de tais informações não esteja sujeito à jurisdição brasileira. Consolidando-se a avaliação das primeiras respostas com situações que apenas são aplicáveis depois de ocorrido o incidente, pode-se visualizar a matriz de risco da seguinte forma (anexo I): 
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	Sim, existem algumas. Segue abaixo breve lista: **CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY.** ***National Cyber Incident Scoring System.*** **Disponível em < https://us-cert.cisa.gov/sites/default/files/publications/CISA_National_Cyber_Incident_Scoring_System_S508C.pdf > Acesso em 28 fev 2021.** **EUROPEAN COMMISSION.** ***Guidelines on Personal data breach notification under Regulation 2016/679*****. Disponível em < https://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=49827 > Acesso em 28 fev 2021.** **INFORMATION COMMISSIONER'S OFFICE.** ***Personal data breach examples.*** **Disponível em < https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-breach-examples/ > Acesso em 28 fev 2021.** **_____.** ***Self-assessment for data breaches.*** **Disponível em < https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach-assessment/ > Acesso em 28 fev 2021.** **_____.** ***Understanding and assessing risk in personal data***

Gravidade X Particularidades	Atenuantes		Qualificadoras					
	Desatualização dos dados afetados	Certeza na falta de acesso dos dados expostos	Incerteza do número de titulares afetados pelo comprometimento da integridade	Vulnerabilidade ou hipervulnerabilidade dos titulares afetados	Função ou cargo público exercido	Internacionalidade dos titulares afetados	Existência prévia de alerta da vulnerabilidade do Controlador ou Operador	Permanência dos dados comprometidos para conhecimento de terceiros não autorizados
Sem gravidade								
Simples								
Intensa								
Severa								
Extrema								

	breaches. **Disponível em < https://ico.org.uk/for-organisations/data-protection-advice-for-small-organisations/understanding-and-assessing-risk-in-personal-data-breaches/ > Acesso em 28 fev 2021.** **NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. Computer Incident Incident Handling Guide. Disponível em < https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf > Acesso em 28 fev 2021.** **_____. *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*. Disponível em < https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf > Acesso em 28 fev 2021.** **UNITED STATES FEDERAL CYBERSECURITY CENTER. *Cyber Incident Severity Schema*. Disponível em < https://obamawhitehouse.archives.gov/sites/whitehouse.gov/files/documents/Cyber%2BIncident%2BSeverity%2BSchema.pdf > Acesso em 28 fev 2021.**
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	- Implementação de plataforma específica da ANPD para relacionamento natural com o controlador e seu Encarregado, permitindo monitoramento do incidente e comunicações com o Encarregado e outros profissionais do controlador afetado em canal seguro, evitando-se falta de transparência ou canais paralelos de contato ou de comprometimento também dos contatos sigilosos entre eles. - Possibilidade de comunicação complementar a outros controladores para evitar danos subsequentes aos titulares afetados em determinados serviços que costumeiramente sofrem com fraudes envolvendo dados pessoais, a exemplo de instituições bancárias ou emissores de cartão de crédito. Tal comunicação poderia compreender aviso para o controlador adicionar fatores de autenticação que não os dados pessoais atingidos e poderia ocorrer via sistema como forma de contingência para proteção do titular afetado. - Exigir demonstrações que os sistemas operados pelo

	controlador sejam confiáveis para o controlador continuar tratando dados pessoais mesmo depois do incidente. Caso não seja possível fazê-lo, ponderar eventuais limitações para mitigar novos incidentes a partir dos sistemas afetados que podem ser indispensáveis;
SUGESTÃO DE NORMATIVO, SE HOUVER	
Art. Xxxx .... **Todos**	
Art. Xxxx .... **Todos**	

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: DR. OETKER BRASIL LTDA.

CPF/CNPJ: 61.193.496/0001-51

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS

IMPORTANTE: Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.

TÓPICO/QUESTÃO	CONTRIBUIÇÃO/INSTITUIÇÃO
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	**Ante a ausência de previsão expressa na Lei nº 13.709/18 a respeito da diferença entre risco e dano ao titular, nos valemos de conceitos civilistas e trabalhistas para, em conjunto, com os princípios e fundamentos presentes na Lei nº 13.709/18, elaborar conceito.** **O risco pode ser considerado como a probabilidade de se causar danos a outrem em decorrência da própria atividade desempenhada, conforme dispõe o artigo 927, parágrafo único, do Código Civil, adotando-se a Teoria do risco-proveito. O dano, por sua vez, é a manifestação dos riscos no prejuízo e lesão ao bem juridicamente tutelado do titular, incluindo bens patrimoniais e não patrimoniais, incluindo vida, honra, corpo, imagem etc.), como já apontavam Heinrich Lehmann e Ludwig Ennecerus.** **Com base nestes conceitos, podemos identificar que, na medida em que a Lei nº 13.709/18, em seu artigo 1º, visa dispor sobre o tratamento de dados pessoais com o objetivo de proteger os direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade da pessoa natural, sempre que o tratamento de dados puder desrespeitar a privacidade, liberdade de expressão ou informação, bem como a inviolabilidade da intimidade, honra e imagem do titular, dentre outros fundamentos dispostos no artigo 2º da Lei nº 13.709/18, pela própria natureza dos dados tratados, haverá probabilidade de danos serem causados ao seu titular.** **De acordo com o "Guia de Avaliação de Riscos de Segurança e Privacidade", com base na norma ISSO/IEC 29134:2017, há 14 riscos principais a serem utilizados na avaliação de seu escopo e potencial dano ao titular, incluindo: (1) Acesso não autorizado; (2) Coleção excessiva; (3) Compartilhamento ou distribuição de dados pessoais com terceiros fora da**

	Adm. Pública Federal e sem consentimento do titular dos dados; (IV) Falha em considerar os direitos do titular dos dados pessoais; (V) Falha ou erro de processamento; (VI) Informação insuficiente sobre a finalidade do tratamento; (VII) Modificação não autorizada; (VIII) Perda dos dados pessoais; (IX) Reidentificação de dados pseudonimizados; (X) Remoção não autorizada; (XI) Retenção prolongada de dados pessoais sem necessidade; (XII) Roubo; (XIII) Tratamento sem consentimento do titular dos dados pessoais; (XIV) Vinculação ou associação indevida, direta ou indireta, dos dados pessoais ao titular.
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	**Sim. De acordo com o Guida de Boas Práticas da LGPD (CCGD, 2020), para avaliação de riscos, primeiro é preciso que se faça uma classificação a fornecer parâmetros escalares que atribuem valor gradual para cada uma das classificações (Baixo, contendo valor 5; Moderado, de valor 10; e Alto, de valor 15). Na sequência, deve ser elaborada matriz que relacione a probabilidade com o impacto ou resultado do evento que afeta o objetivo. A multiplicação de ambos os valores com base no valor de classificação (Baixo, Moderado e Alto) fornece a classificação do nível de risco provocado por determinado incidente ou falha de segurança.** **Segundo o "Guia de Avaliação de Riscos de Segurança e Privacidade",** **Risco ou dano baixo podem ser considerados como qualquer combinação entre Baixa Probabilidade e Baixo Impacto; Baixa Probabilidade e Moderado Impacto; ou Moderada Probabilidade e Baixo Impacto. Isto significa que, por mais que não se visualize risco elevado ou dano considerável ao titular, é possível que se identifique a razão para tais incidentes e busque-se aprimorar o sistema, a fim de evitar o desdobramento de tais incidentes em hipóteses de risco de maior gravidade.**
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	**O risco ao titular representa a probabilidade de este vir a sofrer prejuízos ou violações de seu bem jurídico tutelado em razão da atividade exercida pelo agente de tratamento que utiliza seus dados para o exercício de atividade em proveito próprio. Na lição de Carlos Roberto Gonçalves (Responsabilidade civil. 9. ed., São Paulo: Saraiva, 2005, p. 22), o chamado "risco-proveito" se funda no princípio de reparar dano causado a outrem em razão de atividade realizada em benefício do responsável, que aufere lucros e deverá suportar o ônus de reparar outrem, sempre que sua atividade vier a lhe causar danos.** **Dessa forma, em havendo risco no tratamento de danos do titular, configurada a ilicitude a provocar danos e prejuízos ao bem jurídico tutelado do titular, nasce a responsabilidade objetiva. Segundo Luã Maia de Mello (Comentários à Lei Geral de Proteção de Dados. São Paulo: RT Brasil, 2019, p. 167 o caput do artigo 42 da Lei nº 13.709/18 não menciona a necessidade de comprovação de culpa pelo agente de tratamento, configurando a adoção de responsabilidade objetiva por parte da referida lei.**

O que deve ser considerado na avaliação dos riscos do incidente?	**Nos termos do "Guia de Avaliação de Riscos de Segurança e Privacidade", a identificação e avaliação de risco deve refletir os cenários apresentados pela norma ISSO/IEC 29134:2017 em conjunto com os valores de Probabilidade e Impactos referentes a cada cenário de risco, gerando-se o chamado "Nível de Risco (P x I)".** **O Nível de Risco (P X I) será, em seguida, utilizado em segunda avaliação para identificação do tratamento a ser aplicado na contenção e mitigação de cada risco.** **Este é o mesmo processo que vem sendo utilizado na análise e avaliação de riscos no contexto da General Data Protection Regulation (GDPR) europeia, conforme demonstra Pedro Alexandre Brandão Mendes em seu trabalho de Mestrado (Análise de Risco no GDPR. Mestrado em Segurança Informática. Universidade de Lisboa, Faculdade de Ciências. 2018, p. 55-56).**
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	**Em 22 de fevereiro de 2021, a Autoridade Nacional de Proteção de Dados (ANPD) publicou em seu website o texto "Incidentes de Segurança com Dados Pessoais e sua Avaliação para fins de Comunicação à ANPD". De acordo com referido texto, para além das informações listadas no artigo 48, § 1º, da Lei nº 13.709/18, a comunicação à ANPD deverá conter: (I) Identificação e dados de contato de entidade ou pessoa responsável pelo tratamento dos dados; (II) Identificação e dados de contato de encarregado de dados ou outra pessoa de contato; (III) Identificação se a notificação é completa ou parcial. Em caso de ser a comunicação parcial, deve-se indicar se se trata de comunicação preliminar ou complementar; (IV) Data e hora da detecção do incidente de segurança; (V) Data e hora do incidente de segurança e sua duração; (VI) Circunstâncias em que ocorreu a violação de segurança de dados pessoais; (VII) Descrição dos dados pessoais e informação afetadas (natureza, conteúdo, categoria e quantidade de dados afetados); (VIII) Resumo do incidente de segurança com dados pessoais, com indicação da localização física e meio de armazenamento; (IX) Possíveis consequências e efeitos negativos sobre os titulares dos dados afetados; (X) Medidas de segurança, técnicas e administrativas preventivas tomadas pelo controlador de acordo com a Lei nº 13.709/18; (XI) Resumo das medidas implementadas até o momento para controlar os danos; (XII) Possíveis problemas de natureza transfronteiriça; e (XIII) Outras informações úteis às pessoas afetadas para proteger seus dados ou prevenir possíveis danos.**
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	**A Lei Geral de Proteção de Dados brasileira, Lei nº13.709/18, não fornece prazo específico a respeito da notificação à autoridade nacional em caso de incidente de segurança, limitando-se a dispor que tal comunicação será feita em prazo razoável. A General Data Protection Regulation (GDPR) europeia dispõe que logo após tomar conhecimento de violação de dados pessoais, terá o responsável pelo tratamento prazo de até 72 para notificar violação à autoridade de controle, conforme artigo 33, item 1, da GDPR.**

	A título de parâmetro, o Decreto nº 9.936/19, que regulamenta a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou jurídicas, dispõe em seu artigo 18 que, na ocorrência de vazamento de cadastrados ou outro incidente de segurança que possa resultar em risco ou prejuízo aos cadastrados, o gestor de banco de dados terá prazo de 2 dias úteis, contado da data do conhecimento do incidente, para comunicar a ANPD, o Banco Central do Brasil e a Secretaria Nacional do Consumidor do Ministério da Justiça e Segurança Pública, a depender da hipótese de incidente (artigo 18, § 1º, do Dec. Lei nº 9.936/19).
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	**Assim como a Lei nº 13.709/18, a General Data Protection Regulation (GDPR) não dispõe a cerca do prazo razoável para que controladores informem os titulares de dados sobre o incidente de segurança, sendo razoável que se seja feita o mais rápido possível, no mesmo período máximo de 72 horas para notificação à autoridade de controle, conforme disposto no artigo 34, item 1, da GDPR.** **Segundo a GDPR, a comunicação não poderá ser feita com demora injustificada e deverá descrever em linguagem clara e simples a natureza da violação dos dados pessoais, bem como discorrer a cerca de, nos termos do artigo 34, item 2, da GDPR, no mínimo: (I) Comunicação do nome e contatos do encarregado para obtenção de novas informações (artigo 33, item 3, alínea b, da GDPR); (II) Descrever as consequências prováveis da violação dos dados pessoais (artigo 33, item 3, alínea c, da GDPR); e (III) Descrever as medidas adotadas ou propostas pelo responsável para reparação da violação de dados pessoais, incluindo medidas para atenuar eventuais efeitos negativos (artigo 33, item 3, alínea d, da GDPR).** **Nessa senda, considerando o disposto na GDPR, recomenda-se que a Lei nº 13.709/18 não se limite a apenas exigir as mesmas informações na comunicação entre controlador e titular dos dados violados, devendo ser feito análise tal como realizada pela GDPR para que a comunicação possa ser feita de forma rápida, concisa e disponibilizando informações práticas e acessíveis ao titular para o conhecimento e possível proteção futura.**
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	**Considerando a ausência de previsão legislativa a respeito da forma adequada de comunicação do incidente ao titular, bem como falta de previsão no texto da General Data Protection Regulation (GDPR), há que se considerar ser precipuamente relevante garantir a integridade e inviolabilidade dos bens jurídicos tutelados do titular, nos termos do artigo 2º, inciso I e IV, da LGPD. Por tal razão, a comunicação deverá ser feita direta e individualmente, através do modo mais eficiência a permitir a célere recepção e implementação, por parte do titular, das recomendações capazes de atenuar potenciais efeitos adversos. Cumpre destacar que a LGPD não autoriza a divulgação de dados pessoais do titular para fins de salvaguardar**

	direitos dos titulares, uma vez que o artigo 48, § 2º, inciso I, da LGPD, apenas autoriza que os fatos sejam divulgados, mantendo-se o sigilo e intimidade do titular violado resguardadas. **De acordo com o artigo 34, item 3, alínea c, da GDPR, a comunicação ao titular dos dados não será exigida se implicar esforço desproporcional. No entanto, nesta hipótese, será feita comunicação pública ou medida semelhante através da qual os titulares serão informados de forma igualmente eficaz.**
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	**A Lei nº 13.709/18 estipula, em seu artigo 48, caput, que a comunicação deverá ser feita quando a ocorrência de incidente de segurança puder acarretar risco ou dano relevante aos titulares. Dessa forma, não exige a LGPD que comunicação à ANDP seja feita quando a violação não representar perigo de risco ou danos relevantes. Nessa senda, a General Protection Data Regulation (GDPR), em seu "Considerando" nº 86, estabelece que o controlador dos dados pessoais poderá se eximir de notificar a autoridade de controle caso demonstre que a violação não é suscetível de implicar risco para os direitos e liberdades do titular de dados pessoais.**
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	**Segundo o texto "Incidentes de Segurança com Dados Pessoais e sua Avaliação para fins de Comunicação à ANPD", publicado no website da Autoridade Nacional de Proteção de Dados, em 22 de fevereiro de 2021, deverá ser feita comunicação ao titular de dados sempre que o incidente de segurança possa acarretar risco ou dano relevante ao titular dos dados violados. Nesse diapasão, o texto afirma que deve ser considerado: (I) probabilidade de risco ou dano relevante, sendo estes maior sempre que se tratar de dados sensíveis ou indivíduos em situação de vulnerabilidade; (II) haver potencial de ocasionar danos materiais ou morais, incluindo discriminação, violação ao direito de imagem e reputação, fraudes e roubo de identidade; (III) volume de dados envolvidos; (IV) quantitativo de indivíduos afetados; (V) boa-fé e intenções dos terceiros que tiveram acesso aos dados após o incidente; e (VI) facilidade de identificação dos titulares por terceiros não autorizados).**
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	**Com base na norma ISO/IEC 29134:2017 Seção 6.4.4, é possível ser produzida tabela contendo os 14 principais cenários de "Risco referente ao tratamento de dados pessoais", a fim de que seja feita análise sobre a probabilidade e impacto de tal violação, bem como identificar o "Nível de Risco (P X I).** **De acordo com a ISO/IEC 29134:2017:** **(I) "Acesso não autorizado" representa nível de risco igual a 150 (10 pontos de Probabilidade x 15 pontos de Impacto);** **(II) "Modificação não autorizada" representa nível de risco igual a 150 (10 pontos de Probabilidade x 15 pontos de Impacto);** **(III) "Informação insuficiente sobre a finalidade do tratamento" representa nível de risco de 150 (10 pontos de Probabilidade x 15 pontos de Impacto);**

	(IV) "Tratamento sem consentimento do titular" representa nível de risco de 150 (10 pontos de Probabilidade x 15 pontos de Impacto); **(V) "Compartilhamento e distribuição de dados pessoais com terceiros fora da Adm. Pública Federal e sem consentimento do titular" representa nível de risco de 150 (10 pontos de Probabilidade x 15 pontos de Impacto);** **(VI) "Coleção excessiva de dados" representa nível de risco de 100 (10 pontos de Probabilidade x 10 pontos de Impacto);** **(VII) "Perda de dados" representa nível de risco de 75 (5 pontos de Probabilidade x 15 pontos de Impacto);** **(VIII) "Roubo de dados" representa nível de risco de 75 (5 pontos de Probabilidade x 15 pontos de Impacto);** **(IX) "Remoção não autorizada de dados" representa nível de risco 75 (5 pontos de Probabilidade x 15 pontos de Impacto);** **(X) "Falha em considerar os direitos do titular dos dados" representa nível de risco de 75 (5 pontos de Probabilidade x 15 pontos de Impacto);** **(XI) "Vinculação ou associação indevida dos dados pessoais do titular" representa nível de risco de 75 (5 pontos de Probabilidade x 15 pontos de Impacto);** **(XII) "Falha ou erro de processamento" representa nível de risco de 75 (5 pontos de Probabilidade x 15 pontos de Impacto);** **(XIII) "Reidentificação de dados pseudonimizados" representa nível de risco de 75 (5 pontos de Probabilidade x 15 pontos de Impacto); e** **Retenção prolongada de dados pessoais sem necessidade" representa nível de risco de 50 (10 pontos de Probabilidade x 5 pontos de Impacto).**
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	**Com base nos riscos elencados e dispostos no Guia de Boas Práticas da LGPD (CCGD, 2020), em consonância com as diretrizes da norma ISSO/IEC 29134:2017, a metodologia que utiliza matriz de probabilidade e impacto, conforme destacado acima.** **Utiliza-se classificação de risco com base em três valores (Baixo – 5 pontos; Moderado – 10 pontos; e Alto – 15 pontos). A matriz é elaborada ao se atribuir uma das três classificações/pontuações ao quesito Probabilidade e Impacto. A multiplicação dos respetivos valores atribuídos comporá o "Nível de Risco (P x I), o qual poderá ser disposto em matriz.** **A análise combinatória dos eixos Probabilidade e Impacto indicam que os valores obtidos com nível de classificação de risco "Baixo" são valores de 25 ou 50 pontos; nível de classificação de risco "Moderado" são valores de 75 ou 100 pontos; e nível de classificação de risco "Alto" são valores de 150 ou 225 pontos.**

	A metodologia permite, também, que diferentes riscos sejam analisados (para além dos 14 mais relevantes dispostos na norma ISO/IEC 29134:2017), bem como, a depender da relevância e extensão do tratamento de dados, diferentes pontuações de probabilidade e/ou impacto sejam atribuídas. **Há também que se mencionar a metodologia apresentada pela General Data Protection Regulation (GDPR), uma vez que o artigo 35, item 3 e 7, indicam que avaliação de impacto sobre a proteção de dados deverá ser realizada e incluir, ao menos: (I) Descrição sistemática das operações de tratamento previstas e a finalidade do tratamento; (II) Avaliação da necessidade e proporcionalidade das operações de tratamento em relação aos objetivos; (III) Avaliação dos riscos para os direitos e liberdades dos titulares de dados; e (VI) Medidas previstas para mitigar e conter riscos, incluindo garantias, medidas de segurança e procedimentos a garantir conformidade com a GDPR.**
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	**Após conhecimento por parte da Autoridade Nacional de Proteção de Dados (ANPD) do incidente de segurança, é importante garantir que a ANPD se certifique que houve comunicação por parte do controlador ao titular de dados pessoais a respeito do vazamento, incluindo fornecimento de detalhes a respeito das medidas de segurança a serem adotadas pelo titular de dados para garantir que não ocorram novas violações ou o estado de vulnerabilidade se mantenha. Outra medida importante é garantir que o controlador informe em meios de comunicação de grande circulação a respeito de modo, garantindo-se a inviolabilidade da intimidade e privacidade do titular de dados pessoais ofendido.** **É importante, também, que a ANPD obrigue a implementação de Plano de Ação, caso já não o tenha desenvolvido, incluindo os seus responsáveis.** **Dentre os elementos que o Plano de Ação deverá conter, incluem-se, mas não se limitam: (I) Compilação de metadados, ou seja, informações sobre os próprios dados pessoais e seu tratamento pelo controlador, de modo a permitir o correto mapeamento e manutenção dos registros das operações de tratamento de dados pessoais; (II) Registro das operações de tratamento de dados, possibilitando identificar quais espécies de dados estão, de fato, envolvidos no incidente e são tratados pelo controlador; (III) Identificação prévia de funções e gestores responsáveis pela condução do de prevenção de incidentes; (IV) Definição do procedimento e gestores internos responsáveis por estabelecer a comunicação com os titulares de dados pessoais, sanando eventuais dúvidas e garantindo segurança às solicitações dos titulares de dados em momentos de incidente; (V) Adoção de soluções que permitam isolar dados pessoais particulares de outras secções do sistema de segurança e proteção de dados, de modo a garantir que seja possível identificar rapidamente, e sem**

	prejuízos, para o tratamento de outros dados pessoais não violados, por meio de instrumentos como "Firewall", "Single Sign-On", "Segurança criptográfica", "Backups", dentre outros.
SUGESTÃO DE NORMATIVO, SE HOUVER	
Art. 37-A. O controlador e o operador deverão, caso necessitem compartilhar dados pessoais junto a colaboradores, prestadores de serviços ou terceiros externos à sua estrutura interna, garantir a assinatura de Termo de Colaboração e Responsabilidade para o Tratamento de Dados Pessoais. ***§ 1º O Termo de Colaboração e Responsabilidade para o Tratamento de Dados Pessoais é documento a permitir que colaboradores, prestadores de serviços ou terceiros externos à estrutura interna do controlador ou do operador, conformem-se na observância e cumprimento de todas as políticas, procedimentos e sistemas de segurança e proteção apresentados pelo controlador e operador, adotando mecanismos e procedimentos para o tratamento de dados pessoais de idêntica ou superior proteção.***	
Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. § 1º A comunicação será feita em ***até 5 dias úteis, contados da data de conhecimento por parte do controlador do incidente de segurança que possa acarretar risco ou dano relevante aos titulares***, e deverá mencionar, no mínimo: (...) ***VII – As informações e dados de contato dos responsáveis pelo tratamento dos dados pessoais afetados;*** ***VIII – As informações e dados de contato do encarregado dos dados pessoais (DPO);*** ***IX – Data e hora da detecção do incidente de segurança;*** ***X – Data e hora do incidente de segurança e sua duração;*** ***XI – Circunstâncias em que ocorreu a violação de segurança de dados pessoais;*** ***XII – Descrição dos dados pessoais e informação afetada (categoria, quantidade de dados afetados, gravidade, extensão etc.);*** ***XIII – Resumo do incidente de segurança com dados pessoais, com indicação da localização física e meio de armazenamento;*** ***XIV – Descrição sobre as consequências e efeitos negativos aos titulares de dados afetados;*** ***XV – Resumo das medidas de contenção do incidente até o momento da comunicação para controlar os dados pessoais violados;***	
Sugestão de Esclarecimentos: Requer-se que a Autoridade Nacional de Proteção de Dados (ANPD) esclarece a natureza da responsabilidade civil do encarregado de dados, subsidiária ou solidária, junto ao controlador e operador de dados pessoais, bem como hipóteses em que sua responsabilidade poderá ser reconhecida, tendo em vista a falta de disposição na "Seção III – Da Responsabilidade e Do Ressarcimento de Danos" a respeito da figura do controlador, limitando-se a identificar o controlador e o operador, ou agentes de tratamento, na responsabilização pelo tratamento de dados	

(art. 42), excludentes de responsabilidade (art. 43), e não adoção de medidas de segurança previstas no art. 46 da LGPD (art. 44, parágrafo único).
Mesmo que o encarregado não seja responsável por realizar o tratamento, como sua função está intimamente ligada à conduzir e orientar colaboradores do controlador, bem como executar atribuições determinadas pelo controlador e servir como canal de comunicação entre controlador, titular e ANPD, é possível, sim, identificar situações em que atue de maneira inadequada, em desconformidade com a LGPD, ou até mesmo sendo o responsável por permitir que inadequações nos procedimentos ou mecanismos de controle de risco do controlador ou operador permaneçam em desconformidade com a LGPD, causando danos ao titular de dados por sua negligência.
Por tais razões, encontra-se na doutrina argumentos favoráveis para a adoção de responsabilização civil subsidiária ou solidária por parte do encarregado, em especial por tratar-se de reparação civil por perdas e danos sofridos ao titular de dados pessoais. No entanto, tendo em vista a ausência de disposição legal a respeito da responsabilidade do encarregado, bem como a impossibilidade de presunção de solidariedade (artigo 265, do Código Civil de 2002), seria importante que a ANPD esclarecesse a teoria a ser adotada no futuro.

CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

IDENTIFICAÇÃO DAS INSTITUIÇÕES COLABORADORAS (ordem alfabética):

ASSOCIAÇÃO NACIONAL DOS PERITOS EM COMPUTAÇÃO FORENSE, CNPJ 23.721.249/0001-91

ASSOCIAÇÃO PARQUE TECNOLÓGICO SÃO JOSÉ DOS CAMPOS, CNPJ 09.105.890/0001-70

COREIT-DATA CENTER, SERVIÇOS GERENCIADOS E INFRAESTRUTURA EM TI LTDA., CNPJ 12.012.908/0001-02

CORESEC SEGURANÇA DA INFORMAÇÃO LTDA., CNPJ 08.786.682/0001-11

ENERGY TELECOM COMÉRCIO E SERVIÇOS LTDA., CNPJ 04.635.565/0001-04

ENERGY TELECOM SUL SEGURANÇA DA INFORMAÇÃO LTDA., CNPJ 05.993.899/0001-04

INSTITUTO CTEM+, CNPJ 34.206.898/0001-70

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de

encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS

IMPORTANTE: Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.

Documento elaborado por:

Coordenação Técnica
Prof. Alexandre Pinheiro, MBA* – https://www.linkedin.com/in/pinheiroalexandre/ | http://lattes.cnpq.br/3223580276292335

* Indicado ao CNPD pelo Parque Tecnológico São José dos Campos

TÓPICO/QUESTÃO	CONTRIBUIÇÃO/INSTITUIÇÃO
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	**Quando um incidente pode acarretar risco ou dano relevante ao titular?** O risco para os direitos e liberdades dos titulares, cuja probabilidade e gravidade podem ser variáveis, poderá resultar de operações de tratamento de dados pessoais suscetíveis de causar danos físicos, materiais ou imateriais, em especial quando o tratamento possa dar origem à discriminação, à

	usurpação ou roubo da identidade, a perdas financeiras, prejuízos para a reputação, perdas de confidencialidade de dados pessoais protegidos por sigilo profissional, à inversão não autorizada da pseudonimização, ou a quaisquer outros prejuízos importantes de natureza econômica ou social; quando os titulares dos dados possam ficar privados dos seus direitos e liberdades ou impedidos do exercício do controle sobre os respetivos dados pessoais; quando forem tratados dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas e a filiação sindical, bem como dados genéticos ou dados relativos à saúde ou à vida sexual ou a condenações penais e infrações ou medidas de segurança conexas; quando forem avaliados aspectos de natureza pessoal, em particular análises ou previsões de aspectos que digam respeito ao desempenho no trabalho, à situação econômica, à saúde, às preferências ou interesses pessoais, à confiabilidade ou comportamento e à localização ou aos deslocamentos das pessoas, a fim de definir ou fazer uso de perfis (*profiling*); quando forem tratados dados relativos a pessoas vulneráveis, em particular crianças; ou quando o tratamento incidir sobre uma grande quantidade de dados pessoais e afetar um grande número de titulares de dados. **Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?** Na avaliação da relevância devem ser considerados critérios objetivos como natureza, contexto, finalidade do tratamento, volume de dados, categoria de dados, tipo do incidente e legitimidade do tratamento. Os riscos deverão, portanto, ser aferidos com base numa avaliação objetiva, que determine se as operações de tratamento de dados implicam risco ou risco elevado. **Referências**: 1. RGPD: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=FR#d1e4426-1-1
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano	**O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)?** Sim, certamente.

baixo deve ser considerado relevante ou não relevante?	**Como distinguir os níveis?** Entendemos ser extremamente importante a classificação do incidente quanto ao dano causado ao titular, e para isso usando critérios objetivos. Como exemplos de critérios sugerimos os seguintes: a) Volume: Quantidade de titulares envolvidos no incidente; b) Categoria de dados: Tipo do dado envolvido (Identificação pessoal, Dados financeiros, Características pessoais/psicológicas, Dados de familiares, Hábitos de consumo/lazer, Associações/Religião, Dados de crianças (ECA), Processos Adm/Judicial/Criminal, Dados profissionais, Dados residenciais, Dados de saúde/biométricos); c) Tipo do incidente: Acessos não autorizados, destruição, perda, alteração, comunicação, difusão; d) Legitimidade do tratamento: Se legítimo, qual a base legal associada ao tratamento de dados; e) Automação/IA: Se o tratamento de dados envolve decisão automatizada ou processos de Inteligência Artificial; f) Transferência Internacional: Se houve transferência internacional (voluntária ou não); g) Tempo para recuperação: Tempo necessário para o que agente de tratamento recupere a situação do incidente. Em algumas situações esta recuperação não será possível. **Risco ou dano baixo deve ser considerado relevante ou não relevante?** Entendemos que se após uma análise o risco é considerado baixo, então necessariamente ele se torna irrelevante. A relevância está diretamente relacionada ao nível do risco. **Referências**: 1. RGPD: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=FR#d1e4426-1-1 2. Guia de elaboração de inventário de dados pessoais do Governo Federal: https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaInventario.pdf 3. Modelo de registro das atividades de tratamento de dados pessoais da França: https://www.cnil.fr/sites/default/files/atoms/files/record-processing-activities.ods 4. Modelo de registro das atividades de tratamento de dados pessoais da Bélgica: https://www.autoriteprotectiondonnees.be/publications/modele-de-registe-des-activites-de-traitement.xls 5. Modelo de registro das atividades de tratamento de dados pessoais da Inglaterra: https://ico.org.uk/media/for-organisations/documents/2172937/gdpr-documentation-controller-template.xlsx

Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	**Como distinguir o risco ao titular do dano ao titular?** Risco na sua essência não é necessariamente algo negativo, mas sim um efeito incerto nos objetivos, podendo ser negativo, positivo ou ambos. Os riscos aos titulares quando elevados, devem ser monitorados continuamente em um processo de gestão de riscos dinâmico. O dano por sua vez é concretização do risco negativo. Se provoca dano é porque o evento se concretizou. **Como esses conceitos se relacionam?** O dano é a concretização do risco negativo. **Referências**: 1. Norma ABNT NBR ISO 31000 – Gestão de Riscos 2. Norma ABNT NBR IEC 31010 – Técnicas para o Processo de Avaliação de Riscos 3. Norma ABNT NBR ISO/IEC 27701 – Técnicas de Segurança – Extensão da Norma ABNT NBR ISO/IEC 27001 e Norma ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação – Requisitos e Diretrizes
O que deve ser considerado na avaliação dos riscos do incidente?	**O que deve ser considerado na avaliação dos riscos do incidente?** Para uma avaliação adequada dos riscos devemos considerar a fonte do risco, eventos potenciais e suas consequências e a probabilidade de ocorrência (concretização). Do ponto de vista da privacidade qual o impacto para o titular e para a organização, levando em consideração o nível de sensibilidade dos dados pessoais envolvidos, quais princípios da privacidade foram violados e número de titulares afetados. Objetivamente entendemos que estes são principais pontos que deve ser considerado na avaliação dos riscos de incidentes: a) Legitimidade do tratamento b) Qual(s) a(s) categoria(s) de dado(s) pessoal(is) envolvido(s)? c) Qual a sensibilidade dos dados envolvidos? d) Há risco elevado aos direitos e liberdade dos titulares envolvidos? e) Qual a quantidade de titulares envolvidos no incidente?

	f) Qual a base legal associada ao objetivo do tratamento de dados? g) Existência de salvaguardas para minimizar a probabilidade de incidente de segurança h) Existência de salvaguardas para minimizar o impacto de incidente de segurança i) Uso de tecnologia inovadora no tratamento de dados como Inteligência Artificial ou processo automatizado no tratamento de dados j) Histórico do controlador em incidentes de segurança k) Maturidade do controlador em processos e gestão de segurança e privacidade de dados l) Porte da empresa para dar lastro em possíveis sanções/multas **Referências**: 1. Norma ABNT NBR ISO/IEC 29134:2020 – Avaliação de Impacto de Privacidade – Diretrizes
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	**Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?** Além dos itens já listados no §1º do artigo 48 (LGPD), objetivamente como demonstra que atende os princípios norteadores da gestão de privacidade: • Consentimento e Escolha Se a base legal é o consentimento, como o titular de dados tem garantido o direito de permitir ou não o tratamento, sendo o consentimento obtido de forma válida (livre, claro, inequívoco e específico) • Legitimidade de Objetivo Como é demonstrado que o tratamento é legítimo através do apontamento da base legal associada eo objetivo do tratamento • Limitação da coleta Coleta limitada ao que ao que está dentro dos limites da lei e estritamente necessário ao atingimento do objetivo do tratamento • Minimização dos dados Minimizar dados tratados e número de partes interessadas envolvidas no tratamento, incluindo as necessárias e monitoradas permissões para acesso aos dados, levando em consideração ainda que o acesso será dado tão somente àqueles que de fato precisem. • Limitação de uso, retenção e divulgação

	Limitação de uso, retenção e divulgação ao tão somente que é necessário ao atingimento dos objetivos do tratamento. Se houver transferência internacional, como o titular de dados foi devidamente informado. • Precisão e Qualidade Como é assegurado que os dados são atualizados, precisos e completos, e ainda caso a fonte de coleta não seja o próprio titular, como é assegurada a confiabilidade e confidencialidade. • Abertura, Transparência e Notificação Que o titular de dados foi devidamente informado sobre os procedimentos, políticas e práticas do controlador e possíveis operadores. • Acesso e Participação Individual Como é garantido ao titular o direito de acesso e crítica de seus dados • Responsabilização Procedimentos, políticas e processos que tratam os dados pessoais possuem documentação atualizada. As pessoas envolvidas na organização estão inequivocamente informadas e capacitadas. • *Compliance* com a Privacidade Realização de auditorias periódicas com auditores internos ou externos para avaliação dos requisitos de privacidade e proteção de dados. Gestão de risco atualizada e monitorada para os escopos necessários. **Referências**: 1. Norma ABNT NBR ISO/IEC 29100 – Tecnologia da Informação – Técnicas de Segurança – Estrutura de Privacidade
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	**Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)** Consideramos que o prazo em uso pelo RGPD é adequado, portanto em até 72 horas após ter tido conhecimento do incidente. Se a notificação à ANPD não for transmitida no prazo de 72 horas, é necessário vir acompanhada dos motivos do atraso.

	Referências: 1. RGPD: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=FR#d1e4426-1-1
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	**Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º)** O mesmo prazo referente à comunicação para a ANPD, portanto em até 72 horas após ter tido conhecimento do incidente. Se a notificação ao titular não for transmitida no prazo de 72 horas, é necessário vir acompanhada dos motivos do atraso. **Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?** Entendemos que deve se acrescentada à notificação ao titular de dados, quais as ações que o mesmo deve realizar a fim de minimizar os impactos possíveis em função do incidente, sempre que possível. Seria então: "Descrever as ações que o titular de dados deve realizar para minimizar as consequências prováveis da violação de seus dados pessoais"
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	**Qual a forma mais adequada para a realização da comunicação do incidente aos titulares?** Entedemos que a comunicação aos titulares deve ser realizada através dos canais abaixo, em ordem de preferência: a) Por chamada de voz (telefone) b) Por mensagem (SMS ou aplicativo de mensageria como WhatsApp, Telegram, etc) c) Por e-mail d) Por telegrama e) Por carta (correio tradicional) Observação: Se faz necessário o registro da confirmação por parte do titular do recebimento da notificação. **A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?**

	Entendemos que se o volume de titulares envolvido no incidente for elevado ou algum outro motivo não for viável a comunicação de forma individual, será admitida a comunicação pública através de nota à imprensa (rádio e televisão) e sempre acompanhado de veiculação também em página específica do incidente no site próprio do agente de tratamento envolvido, além de divulgação em todas as redes sociais em que ele tenha conta. Observação: Neste caso é imprescindível que a ANPD delibere e publique com a maior brevidade possível, em quais casos será admitida a comunicação pública e não individual.
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	**Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?** Quando não implicar em risco elevado os direitos e liberdades dos titulares.
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	**Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?** Quando não implicar em risco elevado os direitos e liberdades dos titulares.
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	**Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)** Aqueles supracitados que reproduzimos abaixo: a) Volume: Quantidade de titulares envolvidos no incidente; b) Categoria de dados: Tipo do dado envolvido (Identificação pessoal, Dados financeiros, Características pessoais/psicológicas, Dados de familiares, Hábitos de consumo/lazer, Associações/Religião, Dados de crianças (ECA), Processos Adm/Judicial/Criminal, Dados profissionais, Dados residenciais, Dados de saúde/biométricos); c) Tipo do incidente: Acessos não autorizados, destruição, perda, alteração, comunicação, difusão; d) Legitimidade do tratamento: Se legítimo, qual a base legal associada ao tratamento de dados; e) Automação/IA: Se o tratamento de dados envolve decisão automatizada ou processos de Inteligência Artificial; f) Transferência Internacional: Se houve transferência internacional (voluntária ou não); g) Tempo para recuperação: Tempo necessário para o que agente de tratamento recupere a situação do incidente. Em algumas situações esta recuperação não será possível.

	Referências: 1. RGPD: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=FR#d1e4426-1-1 2. Guia de elaboração de inventário de dados pessoais do Governo Federal: https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaInventario.pdf 3. Modelo de registro das atividades de tratamento de dados pessoais da França: https://www.cnil.fr/sites/default/files/atoms/files/record-processing-activities.ods 4. Modelo de registro das atividades de tratamento de dados pessoais da Bélgica: https://www.autoriteprotectiondonnees.be/publications/modele-de-registe-des-activites-de-traitement.xls 5. Modelo de registro das atividades de tratamento de dados pessoais da Inglaterra: https://ico.org.uk/media/for-organisations/documents/2172937/gdpr-documentation-controller-template.xlsx
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	**Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança?** Sim. **Se sim, qual(is)?** Especificamente para incidentes de segurança da informação: • Norma ISO/IEC 27035:2011 - Information technology — Security techniques — Information security incident management • Capítulo 6.13 da Norma ABNT NBR ISO/IEC 27701 – Técnicas de Segurança – Extensão da Norma ABNT NBR ISO/IEC 27001 e Norma ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação – Requisitos e Diretrizes • NIST Special Publication (NIST SP) - 800-61 Rev 2 - Computer SecurityIncident Handling Guide (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf) De forma genérica para apoiar implementação de times de resposta a incidentes: • Norma ABNT NBR ISO 22320:2020 – Segurança e resiliência – Gestão de emergências – Diretrizes para gestão de incidentes
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	**Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?** Entendemos que existem alguns passos que precisam ser rigorosamente seguidos em um incidente de incidente segurança, incluindo a comunicação citada na pergunta, que não é o primeiro. Para

	sermos didáticos abaixo estão relacionadas as etapas de um processo de resposta a incidentes de segurança: 1. Detecção 2. Notificação 3. Triagem 4. Análise 5. Contenção 6. Erradicação 7. Recuperação Se considerarmos então apenas os passos após a comunicação à ANPD, há então 2 blocos de atividades o controlador deverá realizar. O primeiro será de investigação e análise, extremamente necessário para identificar a causa, entendimento do problema e aplicação de lições aprendidas. O segundo bloco será composto pelas atividades de contenção, erradicação e recuperação, necessários para mitigar o incidente e minimizar os impactos relacionados ao incidente. Para que estes 2 blocos de atividades ocorram em paralelo, é imprescindível a providência de preservação do estado, que deverá ser feito por profissionais de TI com conhecimento em perícia forense computacional. A preservação do estado é fundamental para que os artefatos envolvidos com o incidente tenham valor de prova em juízo. **Referências**: 1. Norma ISO/IEC 27035:2011 - Information technology — Security techniques — Information security incident management 2. AB RAHMAN, N. H.; CHOO. A survey of information security incident handling in the cloud. Computers & Security 3. CICHONSKI, P.; MILLAR, T.; GRANCE, T. ; SCARFONE, K. Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology 4. NIST Special Publication (NIST SP) - 800-61 Rev 2 - Computer SecurityIncident Handling Guide
SUGESTÃO DE NORMATIVO, SE HOUVER	
As referências foram mencionadas ao final das respostas para melhor entendimento.	

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: Fabio David Tomaspolski

CPF/CNPJ: [redacted]

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS

IMPORTANTE: Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.

Nota do contribuinte: sinto por alterar a estrutura do documento formatado, entendi necessário para enxugar o conteúdo

Por ser um profissional da área de segurança patrimonial e especializado em Compliance e LGPD nos últimos três anos, trago minha contribuição visando o lado da segurança e trazendo para dentro dela o LGPD.

Toda minha contribuição é voltada exclusivamente a para câmeras de vigilância e controle de acesso.

TÓPICO/QUESTÃO	CONTRIBUIÇÃO/INSTITUIÇÃO
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	As atividades de segurança devem ser proativas para que o delito não ocorra, então o entendimento da ANPD pode ser diferenciado e ter como base os índice de violência regional gerado pela SSP (Secretaria de Segurança Pública) referente ao delito cometido. Criar uma base histórica para avaliar o risco também é um caminho possível.
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	Em 4 categorias, baixo (verde), médio (amarelo), médio alto (laranja) e vermelho (alto). Nesta modalidade não existe o elemento “3” que em muitos casos é usado para não se tomar uma decisão mais assertiva.Os níveis devem ser distinguidos baseando se em históricos nacionais e/ou internacionais referentes ao setor (condomínios, indústrias, …).
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	Risco = nível do perigo antes do fato acontecer / Dano = risco realizado ou após o fato acontecer Se relacionam na linha de tempo - o evento / acontecimento ocorre, este é o divisor de águas, antes dele a pessoa está em risco após ele a pessoa sofreu o dano. O nível 1 de dano = nível 1 de risco

O que deve ser considerado na avaliação dos riscos do incidente?	5w2hs, histórico de ocorrências, RIPD, LIA, ações mitigatórias e accountability, implementação da família ISO27000, sendo a 27701 a primordial e considerar atenuante
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	N/A
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	15 dias
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	15 dias, 5W2H (bullet points enxuto)
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	Ambos, deve ser definido pela empresa caso a caso
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	Segredos / sigilos comerciais e/ou industriais, M&A e outros diferenciais de mercado como pesquisa de desenvolvimento de software ou hardware. Após a informação vir a público (segredo, sigilo, M&A, …) a empresa terá 5 dias para divulgação.
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	Segredos / sigilos comerciais e/ou industriais, M&A e outros diferenciais de mercado como pesquisa de desenvolvimento de software ou hardware. Após a informação vir a público (segredo, sigilo, M&A, …) a empresa terá 5 dias para divulgação.
Quais são os possíveis critérios a serem adotados pela ANPD na análise	Análise retroativa do poder do segredo, sigilo, .. para a empresa, ações mitigatórias e reações

da gravidade do incidente de segurança? (art. 48, §2º)	
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	Sempre haver um consultor / equipe de segurança técnica para auxiliar na dosimetria da gravidade x meios utilizados
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	Deverá haver uma classificação prévia e setorizada para o tema. Condomínios, Empresas, Escritórios, integradores (empresas que realizam a instalação de câmeras e controles de acesso), … Avaliar a segurança em separado dos demais incidentes de vazamento Adequação do sistema, treinamento de equipe terceirizada,, multa de X taxas condominiais, X% da receita líquida.
SUGESTÃO DE NORMATIVO, SE HOUVER	
https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201903_videosurveillance.pdf	
Art. Xxxx	

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: FEDERAÇÃO DAS ASSOCIAÇÕES COMERCIAIS E EMPRESARIAIS DO ESTADO DO PARANÁ

CPF/CNPJ: 40.312.993/001-51

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS **IMPORTANTE:** Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	Entende-se que um incidente pode causar risco ou dano relevante ao titular quando por exemplo, vários dados são "vazados" ao mesmo tempo, o que pode levar a um grande risco de fraudes com os dados dos titulares, tais como compras indevidas, firmamentos de contratos bancários, etc. Neste mesmo sentido, prevê a GDPR, em seu art. 85, que alguns danos que podem ser causados em caso de incidentes, tais como, a perda de controle do titular sobre os seus dados pessoais, a limitação dos seus direitos, a discriminação, o roubo ou usurpação da identidade, perdas financeiras, a inversão não autorizada da pseudonimização, danos para a reputação, a perda de confidencialidade de dados pessoais protegidos por sigilo profissional ou qualquer outra desvantagem econômica ou social significativa. Desta forma, sugere-se que estes critérios devem ser levados em consideração na hora da avaliação do risco ou danos.
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	Conforme citado no item acima, entende-se pela necessidade de classificar os riscos, tendo em vista que em eventuais incidentes com dados isolados, tais como somente nome, ou só data de nascimento, não traria o mesmo prejuízo ao titular que um incidente onde são revelados dados conjuntamente, como nome, CPF, endereço.
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	O Risco estabelece a expectativa da probabilidade de o titular ser lesado/prejudicado. Enquanto o dano é o efetivo prejuízo ao titular.
O que deve ser considerado na avaliação dos riscos do incidente?	Se no momento da ocorrência a controladora dos dados utilizou todas as medidas técnicas e de segurança que estava ao seu alcance, a sua boa-fé, bem como, se as formas de resolução consensual de controvérsias referentes eventuais incidentes por parte dos controladores com os titulares.
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	Poderão sugerir no comunicado as ações para reverter ou mitigar os efeitos do incidente, tais como sugestão de troca de senhas de bancos, senhas de acesso de sistema, etc.
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	Considerando que a Lei Geral de proteção de Dados foi inspirada na GDPR - General Data Protection Regulation (Regulamento Geral de Proteção de Dados) da União Europeia, que prevê que o prazo de 72 horas para a comunicação da incidência à Autoridade, após o conhecimento do incidente (art. 85 -GDPR). Entretanto, esta Entidade entende que o prazo para que as microempresas e empresas de pequeno porte, bem como iniciativa empresariais de caráter

	incremental ou disruptivo que se autodeclarem startups ou empresas de inovação e pessoas físicas que tratam dados pessoais com fins econômicos, que possuem tratamento diferenciado, façam a comunicação, deverá ser de 10 dias úteis.
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	Conforme previsto na GDPR, as comunicações aos titulares deverão ocorrer em até **72 horas do conhecimento dos fatos**. Entende-se que deverão constar na comunicação as mesmas informações previstas no art. 48, §1º, da LGDP, bem como, a inclusão de medidas que poderão ser adotadas pelos titulares para mitigar o dano e promover a para a defesa de seus direitos.
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	Sugere-se que a comunicação seja sempre de forma individual para garantir o recebimento desta pelo titular de dados. Entretanto, quando se tratar de um vazamento de grande de número de dados, ou por grandes empresas, sugere-se que a comunicação seja realizada de forma ampla, podendo ser realizada por comunicação pública. Em se tratando de microempresas e empresas de pequeno porte, bem como iniciativa empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação e pessoas físicas que tratam dados pessoais com fins econômicos, sugere-se que a comunicação seja realizada de forma individual, podendo fazê-lo diretamente mediante comunicação ao titular ou por meios alternativos, como correio eletrônico, conta em rede social, aplicativo de mensagens, ou qualquer outra forma que permita a comunicação direta entre estas e o titular de dados pessoais.
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	Considerando o que prevê a GDPR, poderá ser desconsiderado o dever de comunicação quando o controlador seja capaz de demonstrar que eventuais incidentes não são suscetíveis de implicar um risco para os direitos e liberdades dos titulares.
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	Considerando o que prevê a GDPR, poderá ser desconsiderado o dever de comunicação quando o controlador seja capaz de demonstrar que eventuais incidentes não são suscetíveis de implicar um risco para os direitos e liberdades dos titulares.
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	Deverão ser observados os possíveis danos ao titular, elencados no item 1 deste documento.
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	Entendendo que o objetivo da Lei é dar transparência e melhor a qualidade do tratamento de dados, sugerimos que a primeira sempre seja advertência por escrito, e no caso de reincidência, seja considerado se houve implementação de meios de segurança, verificando o grau de culpabilidade: negligência, imprudência ou imperícia.
SUGESTÃO DE NORMATIVO, SE HOUVER	

Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. § 1º A comunicação será feita em até 72 (setenta e duas) horas após o conhecimento do incidente. Se não for possível efetuar essa comunicação no prazo de 72 horas, a comunicação deverá ser acompanhada dos motivos do atraso.

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: FEDERAÇÃO BRASILEIRA DE BANCOS – FEBRABAN

CPF/CNPJ: 00.068.353/0001-23

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS **IMPORTANTE:** Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	Primeiramente, ponderamos que a ocorrência de um incidente de segurança não deve ser considerada uma falha na obrigação de zelo das empresas. O art. 48 da Lei 13.709/18 (“LGPD”) determina que o controlador deverá comunicar à ANPD e aos titulares de dados a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Assim, não é qualquer incidente de segurança que deve ser reportado à ANPD ou aos titulares, mas apenas aqueles que de fato possam causar risco ou dano relevante aos titulares. Adicionalmente, não é recomendável que a regulação dos incidentes aborde o tema de forma enumerativa e exaustiva. Afinal, as ameaças são mutáveis e estão constantemente em evolução, as tecnologias e serviços dispostos de forma legítima aos titulares avança, bem como há diversas possibilidades de incidentes. Recomendamos que a regulação aborde o tema de forma consisente, porém flexível, de forma a acompanhar a evolução das tecnologias e atividades empresariais. Quanto à questão, entendemos que um incidente de segurança pode ser considerado como um incidente passível de acarretar risco ou dano relevante na medida em que ele possa ocasionar risco elevado à integridade física ou moral do titular. Nesse sentido, podem ser considerados critérios para uma avaliação da relevância do risco ou dano ao titular do dado pessoal:

	• Volumetria dos dados pessoais e titulares afetados; • Tipos de dados pessoais afetados (sensibilidade e natureza dos dados pessoais); • Se os dados pessoais já estavam expostos ou publicamente acessíveis; • Probabilidade de os dados pessoais serem utilizados para propósitos irregulares e ilícitos ou ocasionarem danos morais e materiais relevantes e danos físicos aos titulares[1]; • Medidas tomadas para reverter ou mitigar as consequências do incidente. Por fim, importante ressaltar, porém, que a ANPD não deve estabelecer metodologia de avaliação de risco e dano a ser adotada por todas as instituições. Pode-se prever diretrizes mínimas, mas as instituições devem ter a flexibilidade de adotar a metodologia e critérios de avaliação de riscos e danos que entenderem factíveis e correspondentes ao seu porte, setor e tratamento de dados pessoais realizado. [1] Seguem exemplos não exaustivos de riscos e danos relevantes aos quais os titulares dos dados podem estar expostos em decorrência de incidentes de segurança com seus dados pessoais: • Sequestro; • Comprometimento da integridade física ou moral; • Retaliação; • Constrangimento ou exposição pública e reputação; • Discriminação; • Negativação por órgãos de crédito (Serasa/SPC); • Danos materiais significativos.
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	Consideramos que o risco ou o dano de um incidente de segurança pode ser subdividido em categorias, como: *(i)* baixo, *(ii)* médio, *(iii)* alto e *(iv)* muito alto, porém, apenas aqueles riscos ou danos categorizados como altos ou muito altos devem ser considerados como relevantes. Assim, o risco relevante não deve ser classificado em mais categorias, pois a nova divisão pode burocratizar a avaliação de riscos e torná-la mais complexa e, até mesmo, confusa. Existem diversas metodologias para classificação de riscos ou danos que podem ser usadas pelas instituições que tratam dados pessoais, como a da ENISA (European Union Agency for Cybersecurity), por exemplo, porém entendemos que a regulamentação da ANPD não deve especificar qual metodologia deve ser utilizada pelas instituições. A regulamentação da ANPD poderá prever diretrizes gerais sobre o tema para auxiliar as instituições na condução dos procedimentos de classificação dos incidentes. Por exemplo, pode-se considerar a gravidade/severidade do incidente como: 1. Baixo: os titulares dos dados não serão afetados, não é possível a identificação do titular ou o incidente possa causar pequenos inconvenientes; 2. Médio: quando o dado pessoal ou conjunto de dados pessoais relacionados ao incidente possibilitam, de forma direta ou indireta, a identificação do titular e quando tais dados podem gerar danos efetivos mais significativos ao titular.

	3. Alto e muito alto: situações nas quais há alto risco de dano real relevante a um indivíduo, ou seja, quando o dado pessoal ou conjunto de dados pessoais relacionados ao incidente possibilitam, de forma direta ou indireta, a identificação do titular **e** quando o incidente tiver probabilidade elevada de causar danos concretos à integridade física ou moral do titular, como dano físico, discriminação, danos materiais, roubo de identidade, fraude, significativos danos à reputação, por exemplo. Importante esclarecer que o risco e o dano são dissociados, ou seja, o risco classificado como alto não implica, necessariamente, a materialização de um dano de classificação como alto.
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	Entendemos que o risco ao titular sinaliza um evento que pode ou não ocorrer (calculado de acordo com uma matriz de risco), já o dano ao titular é o efeito concreto causado quando um risco comprovadamente se materializou. Esses conceitos estão inter-relacionados, sendo que o risco (cálculo de impacto e probabilidade) antecede o dano (quando o evento, de fato, acontece).
O que deve ser considerado na avaliação dos riscos do incidente?	Além dos critérios para avaliação do risco, mencionados na questão n.º 01 deste modelo, como: *(i)* volumetria dos dados pessoais e titulares afetados; *(ii)* tipos de dados pessoais afetados (sensibilidade e natureza dos dados pessoais); *(iii)* se os dados pessoais já estavam expostos ou publicamente acessíveis; e *(iv)* probabilidade de os dados pessoais serem utilizados para propósitos irregulares e ilícitos ou ocasionarem danos morais e materiais relevantes e danos físicos aos titulares, entendemos que a avaliação do risco também deve considerar aspectos técnicos. Alguns exemplos dos aspectos técnicos que podem ser considerados na avaliação do risco são: *(i)* medidas tomadas para reverter ou mitigar as consequências do incidente; *(ii)* medidas de segurança e boas práticas implementadas pelo controlador; *(iii)* origem e circunstâncias do incidente. Importante ressaltar, porém, que a ANPD não deve estabelecer metodologia de avaliação de risco a ser adotada por todas as instituições. Pode-se prever diretrizes mínimas, mas as instituições devem ter a flexibilidade de adotar a metodologia e critérios de avaliação de riscos que entenderem factíveis e correspondentes ao seu porte, setor e tratamento de dados pessoais realizado.
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	Ratificamos a orientação emitida pela ANPD que, além do disposto no artigo 48, §1º da LGPD, recomendou também que a comunicação a respeito do incidente deve conter: ▪ Identificação e dados de contato do controlador responsável pelo tratamento de dados pessoais e do encarregado, bem como indicação de se a comunicação é completa ou parcial; ▪ Informações gerais sobre o incidente. https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca Essas informações - trazidas pelo art. 48, §1º e pela orientação da ANPD - já são suficientes para a comunicação a ser elaborada pelo controlador à ANPD, não sendo necessárias mais informações além dessas.

	Aproveitamos para recomendar a exclusão da possibilidade de notificação do incidente à ANPD por operadores, como constou do formulário de comunicação de incidentes de segurança à ANPD. Entendemos que o operador de dados não deve notificar incidentes, pois esta é uma obrigação do controlador dos dados.
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	Primeiramente, é importante esclarecer que a investigação de um incidente de segurança é complexa e não trivial, de modo que um prazo muito exíguo para comunicação do incidente à ANPD pode não ser factível. Assim, entendemos que o prazo razoável para a primeira comunicação à ANPD sobre incidente de segurança relevante seria de, **no mínimo**, 5 (cinco) dias úteis, a contar da finalização da análise preliminar do incidente que possibilite ao controlador ter razoável grau de certeza que o incidente de segurança ocorreu envolvendo o controlador e que acarretou risco ou dano relevante aos titulares de dados pessoais. Ressaltamos que esse prazo pode ser, até mesmo, maior, a exemplo do que ocorre em alguns Estados dos Estados Unidos. Lembrando que a comunicação pode ser parcial, caso o controlador verifique que, após o prazo disposto em regulamentação, ainda não contém todas as informações sobre o incidente. Adicionalmente, não recomendamos a contagem do prazo em horas, mas sim em dias úteis, dada a dificuldade prática de se identificar, com clareza, o horário em que houve o incidente por parte do controlador. Ainda, não recomendamos usar o prazo de comunicação previsto na Lei do Cadastro Positivo (Lei n.º 12.414/2011), de 2 dias úteis a contar da ciência do incidente de segurança. Isso porque, o escopo da LGPD é bastante diverso e consideravelmente mais amplo do que o da Lei do Cadastro Positivo. Na Lei do Cadastro Positivo, a obrigação de comunicação aplica-se apenas aos poucos gestores de bancos de dados do cadastro positivo, enquanto a obrigação de comunicação de incidentes prevista na LGPD refere-se aos controladores de dados de todos os setores. Além disso, como já indicado acima a investigação de um incidente de segurança não é trivial. Ela requer a realização de procedimentos de investigação complexos e extensos e o prazo de 2 (dois) dias úteis é demasiado curto. Por fim, além dessas razões para não utilização do prazo previsto na Lei do Cadastro Positivo, também podemos mencionar que não há clareza a respeito do que seria considerada “ciência do incidente”. Ressaltamos que o início do prazo de comunicação não deve ser contado a partir do conhecimento do fato, mas após análises que permitam ao controlador ter razoável grau de certeza sobre o incidente e seus riscos. Dessa forma, entendemos que o prazo de 2 dias úteis não é factível.
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	Entendemos que, conforme disposto na LGPD, a comunicação ao titular de dados deve conter as informações mencionadas no art. 48, § 1º, porém, a comunicação ao titular deve seguir linguagem amigável e não deveria conter aprofundamentos técnicos que não serão necessários ou úteis ao titular. Quanto ao prazo, entendemos que a regulamentação não deveria estabelecer prazo específico, mas indicar que tal comunicação deve ser em prazo razoável tão logo se identifique uma ação necessária por parte do titular ou tão logo se conclua a aferição do incidente e se tenha informações úteis e relevantes ao titular. Ainda, no caso de o controlador entender ser necessária a comunicação ao titular a respeito de incidente de segurança que implique em risco ou dano relevante, a ANPD também deveria ser comunicada.

Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	É preferível que a comunicação seja direta ao titular, utilizando-se, preferencialmente, dos canais que o controlador faz contato com o titular (e-mail, bankline, por exemplo), mas é possível usar outros meios, como publicações nas redes sociais, comunicados por meio de centrais de atendimento/ouvidoria. A critério do controlador, pode-se utilizar nota à imprensa ou website, porém, tais meios de comunicação devem ser utilizados de forma excepcional (por exemplo, nos casos em que o controlador não conseguir encontrar o titular). Ainda, entendemos que a forma de comunicação ao titular dos dados deve depender da extensão e criticidade do incidente, bem como dos meios que o controlador considere mais efetivos para tal comunicação, a depender do seu relacionamento com o titular. Assim, o ideal é que a norma não regule ou limite as formas de comunicação, também não regule uma forma específica de comunicação, ficando a critério do controlador escolher os meios para tal comunicação.
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	A própria LGPD já determina que incidentes de segurança relevantes sob responsabilidade do controlador devem ser por ele comunicados à ANPD. Dessa forma, não deve haver comunicação de incidentes com riscos ou danos classificados como baixo ou médio. De toda forma, entendemos que a regulamentação da ANPD deve excluir da obrigatoriedade de comunicação os incidentes que: • tiveram seu risco ou dano remediado ou mitigado, por exemplo, aqueles incidentes com número limitado de titulares afetados em que foi possível fazer ação para mitigação dos danos ou riscos; • envolvem dados pessoais que estão protegidos (criptografados, anonimizados, por exemplo); • envolveram dados pessoais que já estavam acessíveis publicamente.
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	Primeiramente, entendemos que o titular não deve ser informado sobre todo e qualquer incidente. As comunicações devem ocorrer em casos de risco ou dano alto e se tal risco ou dano não tiver sido contido pelos agentes de tratamento. Quanto à comunicação dos incidentes com riscos ou danos relevantes, entendemos que não devem ser comunicadas aos titulares (ou a comunicação deve ser feita após a conclusão efetiva da investigação) situações em que a divulgação possa causar impacto adverso ou colocar em risco a investigação ou possibilidade de mitigação dos efeitos do incidente. Ainda, fazemos referência ao "*Guidelines on Personal data breach notification under Regulation 2016/679*" elaborado pelo Grupo de Trabalho instituído pelo artigo 29º, criado pela diretiva 95/46/CE da União Europeia[1] que estabelece possíveis exceções de notificação ao titular e que entendemos que pode ajudar a ANPD na definição das exceções à comunicação aos titulares que constará da regulamentação brasileira. Alguns exemplos dessas hipóteses são: • o responsável pelo tratamento tiver aplicado medidas técnicas e organizativas adequadas para proteger os dados pessoais antes da violação, especialmente medidas que tornem os dados pessoais incompreensíveis para

	qualquer pessoa não autorizada a acessá-los (dados pessoais com encriptação de ponta, ou através de codificação, por exemplo); • imediatamente a seguir a uma violação, quando o responsável pelo tratamento tiver tomado medidas para assegurar que o risco elevado colocado aos direitos e liberdades das pessoas singulares já não é suscetível de se concretizar. Por exemplo, dependendo das circunstâncias do caso, o responsável pelo tratamento pode ter identificado imediatamente e tomado medidas contra a pessoa que acessou os dados pessoais antes de esta ter conseguido fazer alguma coisa com eles; • quando o contato com os titulares implicar em esforço desproporcional, como quando os dados de contato tiverem se perdido em resultado da violação ou nunca tiverem sido conhecidos pelo agente de tratamento. [1] Disponível em: **https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052**
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	Os critérios que poderiam ser utilizados pela ANPD para avaliação da gravidade do incidente podem ser os mesmos que citamos acima como critérios válidos para a avaliação dos riscos (pergunta – "O que deve ser considerado na avaliação dos riscos do incidente?"). Ainda, entendemos que a ANPD pode considerar outros critérios para avaliação da gravidade do incidente como os recursos utilizados pela instituição para se mitigar a possibilidade do incidente (políticas, processos e procedimentos em vigor), a proatividade da instituição em identificar e comunicar à ANPD e aos titulares, bem como, a rapidez e presteza da instituição em estabelecer os planos de ação para evitar novos possíveis casos.
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	Entendemos que os controladores de dados devem ter a prerrogativa de definir sua própria metodologia para graduação da severidade do incidente de segurança. Essas metodologias devem ser escolhidas pela própria instituição, considerando o seu porte e ramo, bem como o volume e sensibilidade de dados pessoais tratados. De forma meramente exemplificativa, citamos abaixo algumas metodologias de análise de riscos disponíveis e que podem ser utilizadas, como: • ENISA (*European Union Agency for Cybersecurity*), com algumas adaptações considerando o cenário financeiro, pode ser usada para a análise de gravidade do incidente de segurança. • NIST (computer Security Incident Handling Guide – NIST. Disponível em https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf) • NCCIC Cyber Incident Scoring System.National Cybersecurity and Communications Integration Center. (Disponível em https://www.us-cert.gov/sites/default/files/publications/NCCIC_Cyber_Incident_Scoring_System.pdf) • ISSO 27001, ISSO 27002, ISO 27201, ISO 31.000.
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos	Entendemos que este ponto é de difícil predição, de modo que as providências irão variar de acordo com a situação concreta.

controladores após a comunicação do incidente de segurança?	Mais do que implementar uma reação imediatamente burocrática e onerosa aos controladores, a ANPD e as instituições envolvidas deveriam centralizar os esforços em resolver o incidente da maneira mais célere possível de forma a garantir a proteção dos dados pessoais dos titulares. De todo modo, além do entendimento, pela ANPD, a respeito das medidas já adotadas pelas instituições envolvidas, para proteção dos dados pessoais dos titulares, caso, a depender do caso concreto, a ANPD entenda necessário, pode-se sugerir: • Implementação ou melhoria na segurança da informação do controlador, para que se possa prevenir a repetição do incidente; • Adequação de políticas internas com processos relacionados ao incidente; • Elaboração e implementação de plano de ação de remediação do incidente. Adicionalmente, entendemos que a ANPD deveria trabalhar de forma educacional com o mercado, disponibilizando assistência técnica aos controladores, dividindo com o mercado suas expectativas e melhores práticas, publicando estudos de casos.
SUGESTÃO DE NORMATIVO, SE HOUVER	
Não temos sugestão de Normativo neste momento.	

ANEXO I

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2/2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: Federação do Comércio de Bens, Serviços e Turismo do Estado de São Paulo – FECOMERCIO/SP
CPF/CNPJ: 62.658.182/0001-40

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regularmente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS

IMPORTANTE: Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.

R. Dr. Plínio Barreto, 285 | Bela Vista | cep 01313-020 | São Paulo | SP | Brasil | tel 55 11 3254.1700

www.fecomercio.com.br

TÓPICO/QUESTÃO	CONTRIBUIÇÃO/INSTITUIÇÃO
1. Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	5 a 7
2. O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc.)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	8 a 10
3. Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	11
4. O que deve ser considerado na avaliação dos riscos do incidente?	12
5. Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1° do art. 48?	13
6. Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1°)	14 a 15
7. Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1°) Que informações devem constar dessa comunicação? As mesmas do §1° do art. 48?	16

8. Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	17 a 18
9. Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	19
10. Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	20 a 21
11. Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	22
12. Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	23
13. Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	24
14. O operador pode notificar diretamente a ANPD ou o titular? Se sim, em quais circunstâncias?	25

R. Dr. Plínio Barreto, 285 | Bela Vista | cep 01313-020 | São Paulo | SP | Brasil | tel 55 11 3254.1700

www.fecomercio.com.br

15. Outras sugestões:	**26**
SUGESTÃO DE NORMATIVO, SE HOUVER	
Art. Xxxx	
Art. Xxxx	

CONTRIBUIÇÕES

1. Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?

Sempre que detectado um incidente de segurança da informação, o agente de tratamento deverá fazer uma avaliação de risco ou dano face aos direitos dos titulares envolvidos, considerando a probabilidade de dano e o risco de impacto.

Conforme dispõe o *Recital* 75 do *General Data Protection Regulation* (*GDPR*)[1], um incidente de segurança tem potencial de causar risco quando possa expor os titulares a práticas discriminatórias, perdas financeiras, prejuízos efetivos a sua reputação, inversão não autorizada da pseudonimização ou quando titulares forem privados, por quaisquer outros meios, de seus direitos e garantias fundamentais.

Neste sentido, algumas situações denotam risco ou dano relevante ao titular, especialmente, quando envolvem: (i) dados pessoais sensíveis; (ii) dados pessoais classificados como confidenciais; (iii) titulares em situação de vulnerabilidade, como crianças; (iv) potencial concreto de ocasionar danos materiais ou morais, tais como discriminação, violação do direito à imagem e à reputação, fraudes financeiras e roubo de identidade; (v) volume significativo de dados envolvidos; (vi) número significativo de indivíduos afetados; (vii) características específicas do controlador de dados pessoais, observados a sua estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares; (viii) comprovação de dolo e/ou má-fé pelo agente causador do dano; e (ix) possibilidade de maior facilidade na identificação dos titulares a partir dos dados expostos. Outro critério relevante é a (viii) qualidade dos dados, isto é, se os dados são utilizados e atualizados frequentemente (“dados hot”), pois quanto mais atuais os dados, maior o risco de

[1] Disponível em: https://gdpr-info.eu/. Acesso em: 22.03.2021.

uma informação ser enriquecida para práticas ilícitas. Como exemplo, pode-se considerar que um número de telefone/celular desatualizado não terá o mesmo valor que um número atualizado. Em relação à definição do risco e do dano como "relevantes" é fundamental estabelecer parâmetros de forma objetiva e restritiva, de modo a garantir a segurança jurídica na aplicação da LGPD, uma vez que o próprio *Recital* 75 do *GDPR* possui uma ampla definição de "dano relevante", podendo levar a uma enormidade de interpretações distintas.

Alguns critérios podem ser adotados para caracterizar o risco, incluindo quaisquer situações que tragam a possibilidade concreta (i) do titular ser prejudicado com golpes financeiros; (ii) de insegurança pessoal do titular, ou seja, que permita ou exponha ele em situações de risco pessoal ou de seus familiares, não sendo considerados dados públicos para este fim; e (iii) de insegurança moral, expondo informações críticas sobre o titular de modo a lhe causar dano reputacional, à sua subjetividade e honra, bem como abalo psíquico.

No que diz respeito à configuração de dano moral, importante definir as situações em que será possível afirmar que um titular de fato sofreu tal dano em virtude de um incidente, vez que a adoção da teoria do dano moral presumido, ou *in re ipsa*, pelo ordenamento jurídico pátrio, poderá resultar no sancionamento e/ou na judicialização excessiva do tema e em prejuízos desproporcionais aos agentes de tratamento.

Também é possível que um incidente de segurança com dados pessoais ocasione danos materiais aos titulares afetados, resultando em roubos de identidade, fraudes bancárias, efeitos negativos ao histórico de crédito, e perdas financeiras em geral. Tais exemplos de danos materiais ao titular são apontados pelo *WP29* em suas diretrizes sobre a notificação de incidentes de dados ("*Guidelines on Personal data breach notification under Regulation 2016/679*")[2] e pela *Federal Trade Comission*, agência reguladora antifraude norte americana.[3] A perda de emprego, de negócios ou de oportunidades profissionais são apontadas na normativa canadense intitulada "*Personal Information Protection and Electronic Documents Act*"[4] como possíveis resultados

[2] Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052. Acesso em: 22.03.2021.
[3] Disponível em: https://www.consumer.ftc.gov/articles/0235-identity-theft-protection-services. Acesso em: 22.03.2021.
[4] Disponível em: https://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html. Acesso em: 22.03.2021.

negativos ao titular de um incidente envolvendo seus dados pessoais. Também é possível incluir aqui a perda de confidencialidade de dados pessoais protegidos por sigilo profissional.

Ademais, uma combinação envolvendo diferentes tipos de dados pessoais poderá ser parâmetro do nível de risco, tendo em vista que o cruzamento dessas informações com outras bases de dados poderá revelar aspectos relevantes sobre os titulares[5].

Ressalte-se que, ainda que o controlador deva aderir aos parâmetros definidos pela ANPD e cumprir com a LGPD, é essencial que seja preservada a autonomia do controlador na aplicação de suas respectivas políticas, nos termos de seus modelos de negócio.

[5] Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052. Acesso em: 22.03.2021.

2. O risco ou dano relevante deveria ser subdividido em mais categorias (ex. baixo, médio, alto, etc.)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?

Primeiramente, é importante diferenciar as definições de risco e dano. O dano é o risco que, de fato, se materializou, enquanto o risco é a probabilidade de uma ameaça se materializar.
Definir limites vinculados a critérios objetivos e orientados por metodologia fundamentada auxilia os controladores de dados a entenderem melhor a verdadeira natureza, impacto e "notificabilidade" dos incidentes, evitando o excesso de cautela e a uma tendência em prol da supernotificação de incidentes.

A inexistência de risco ou de baixo risco, assim como a inexistência de dano ou de dano relevante não devem ser considerados relevantes para a notificação de um incidente. De qualquer modo, sempre que o risco ou dano tiverem uma classificação "inexistente" ou "baixa", esta deve ser fundamentada, por meio de registros e documentações que contenham as medidas de mitigação aplicáveis, se necessário.

Para fins da análise de risco, pode-se dividir os riscos de acordo com a seguinte categoria (i) "baixo", (ii) "médio", (iii) "alto" e (iv) "muito alto", sendo que somente os riscos classificados como "altos" ou "muito altos" deveriam ser considerados como "relevantes" para eventuais notificações à ANPD ou ao titular.

Tal balizamento é de muita relevância para se evitar que os titulares sejam importunados com notificações desnecessárias ("*Unnecessary notification fatigue*", nos termos do *Working Party 29*[6]), mas ao mesmo tempo garantindo que tenham conhecimento dos incidentes mais relevantes. O impacto do dano ou risco gerado pelo incidente deveria ser avaliado após ponderados os seguintes aspectos com base nas diretrizes do *WP29*: (i) o tipo de incidente (se uma violação de confidencialidade, integridade ou disponibilidade de dados); (ii) a natureza dos dados pessoais (se simples, comportamentais, financeiros ou sensíveis); (iii) a facilidade de se identificar o titular;

[6] Disponível em: https://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358. Acesso em: 22.03.2021.

(iv) o volume de dados tratados e o número de indivíduos afetados; (v) as possíveis consequências adversas ao titular (severidade e duração/permanência dessas consequências); (vi) características especiais do titular (se criança); (vii) características especiais do controlador. Outro critério relevante é a (viii) qualidade dos dados, isto é, se os dados são utilizados e atualizados frequentemente ("dados hot"), pois quanto mais atuais os dados, maior o risco de uma informação ser enriquecida para práticas ilícitas. Como exemplo, pode-se considerar que um número de telefone/celular desatualizado não terá o mesmo valor que um número atualizado. O *Notifiable Data Breach scheme* (NDB)[7], norma australiana sobre a notificação de incidentes de segurança de dados, também adota critérios similares para o dever de notificação à Autoridade (e titulares), que deverá ser realizado somente quando houver a probabilidade de que o incidente resulte em dano grave ("*serious harm*") aos afetados. Tal qualificação leva em conta: o tipo de informação (ou natureza dos dados); a sensibilidade; as medidas de segurança existentes e a possibilidade de superá-las; as pessoas, ou tipo de pessoas, que obtiveram ou poderiam obter as informações, bem como suas possíveis intenções maliciosas; e a natureza do dano.

Para além da sensibilidade dos dados, a norma australiana também leva em consideração para a análise de "um risco real de dano significativo" ("*serious harm of significant damage*") ao titular a probabilidade de que os dados pessoais tenham sido, são ou possam ser utilizados indevidamente – levando em conta, portanto, a boa-fé e as intenções dos terceiros não autorizados que acessem os dados. Segundo a WP29, essa análise é importante para avaliar a severidade do incidente, vez que é possível que o controlador possua um relacionamento prévio com a pessoa ou instituição que teve acesso indevido aos dados pessoais (por exemplo, ao receber um e-mail encaminhado acidentalmente) e, estando ciente de seus procedimentos, histórico e outros detalhes importantes, possa considerá-lo como confiável.

O número de indivíduos afetados por um incidente é também utilizado como parâmetro, sobretudo, na legislação norte americana, para definir o dever ou não de comunicação às autoridades competentes. No Estado da Califórnia, empresas que forem vítimas de crimes cibernéticos ou violação de dados devem emitir notificações quando 500 ou mais residentes do

[7] Disponível em: https://www.oaic.gov.au/privacy/notifiable-data-breaches/ . Acesso em: 22.03.2021.

estado forem afetados. No Novo México, o prazo é de 45 dias para a notificação de incidentes que afetem mais de mil residentes.

Assim, é importante que a ANPD estabeleça parâmetros objetivos para definir o que constitui um "grande volume" de dados envolvido em um incidente e um "quantitativo elevado" de indivíduos afetados (parâmetros já estabelecidos pela Autoridade como importantes para a análise de risco ou dano relevante).

No que diz respeito ao cálculo de severidade do risco, sugerimos a adoção de um critério objetivo, baseando-se na metodologia criada pela *ENISA* (*European Union Agency for Network and Information Security*), segundo a fórmula a seguir:

Severidade do Risco = Contexto do Processamento x Facilidade de identificação do titular + Circunstâncias do Incidente.

A agência oferece parâmetros de ajuste para cada uma dessas variáveis, facilmente adaptáveis ao contexto brasileiro. Os resultados da fórmula proposta correspondem a quatro níveis de gravidade: "baixo" ou "médio" (por não haver possibilidade de risco ou dano relevante, ausência do dever de notificação); "alto" ou "muito alto" (dever de notificação à ANPD e/ou ao titular).

3. Como distinguir o risco ao titular do dano? Como esses conceitos se relacionam?

São considerados "riscos" ao titular aqueles casos classificados como eventos de segurança, ou seja, quando não há evidência de materialização de impacto ao usuário, mas, existe o risco enquanto o evento não for mitigado/resolvido pelo controlador. Por isso, o risco implica um modo particular de se referir a um evento futuro contingente, através da percepção da antecipação dos seus efeitos. Essa antecipação conduz à avaliação das possíveis consequências danosas para sopesar um coeficiente de probabilidade e discernir o seu valor. No risco, tem-se, portanto, um caráter ativo de avaliação e antecipação de consequências.

O dano, por sua vez, corresponde à efetiva materialização do risco, isto é, se considera um dano ao titular quando há evidências suficientes de que o risco foi concretizado afetando seus direitos. Em termos de proteção de dados pessoais, o risco de incidente corresponderá a todas as consequências danosas que poderão ser vislumbradas (por exemplo, a indisponibilidade de um serviço, a perda de informações, o acesso indevido por terceiros, etc.). Caso uma das consequências danosas venha a ser concretizada haverá um dano ao titular (por exemplo, a indisponibilidade de um prontuário médico pode resultar em um dano à saúde, ou o acesso não autorizado em um roubo de identidade).
Em síntese, deve ser considerado risco ao titular: (i) o vazamento ou exposição dos dados pessoais, desde que exista um potencial risco de serem utilizados de forma inescrupulosa, irresponsável e criminosa e, um dano ao titular: (ii) quando após a comprovação do vazamento ou exposição dos dados verificar-se, efetivamente, o prejuízo ao titular de dados.

Nesse contexto, a diferenciação entre risco e dano será essencial para fins de atribuição de responsabilidades e para o dever de reparação a um titular afetado. Por exemplo, para o ajuizamento de uma ação indenizatória, deverá, necessariamente, existir a materialização do dano (Art. 42, da LGPD). O risco, por sua vez, assim como o próprio dano, poderá ser utilizado como critério desencadeador da obrigação de notificar a ANPD e os titulares, conforme sugerido anteriormente.

4. O que deve ser considerado na avaliação dos riscos do incidente?

Deve-se considerar os critérios já mencionados neste documento para a avaliação dos riscos do incidente, a saber: (i) o tipo de incidente (se uma violação de confidencialidade, integridade ou disponibilidade de dados); (ii) a natureza dos dados pessoais afetados (se simples, comportamentais, financeiros ou sensíveis, por exemplo); (iii) a facilidade de se identificar o titular; (iv) o volume de dados tratados e o número de indivíduos afetados; (v) as possíveis consequências adversas ao titular (severidade e duração/permanência dessas consequências); (vi) características especiais do titular (se criança, por exemplo); (vii) características especiais do controlador; e (viii) qualidade dos dados, isto é, se os dados são utilizados e atualizados frequentemente ("dados hot"), pois quanto mais atuais os dados, maior o risco de uma informação ser enriquecida para práticas ilícitas. Como exemplo, pode-se considerar que um número de telefone/celular desatualizado não terá o mesmo valor que um número atualizado.

Ademais, a avaliação dos riscos de incidentes deve considerar se o risco foi originado por falha de segurança interna, imperícia, imprudência, negligência ou dolo. Assim, deve-se verificar se o controlador/operador, de alguma forma, deixou de tomar as medidas de segurança cabíveis no sentido de evitar ou mitigar os riscos de invasão, armazenamento ou eliminação dos dados pessoais, bem como se envidou os esforços necessários à sua mitigação e se adotou todas as providências pertinentes à comunicação dos titulares de dados envolvidos no incidente.

5. Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?

São necessárias, unicamente, as informações já constantes sugeridas do artigo 48, §1 da LGPD, as quais são suficientes para integrar a notificação encaminhada, avaliar eventual incidente e adotar as medidas necessárias. Essas informações correspondem àquelas já listadas em outras legislações de proteção de dados pessoais (*General Data Protection Regulation*[8], *Notifiable Data Breach Scheme*[9], *Personal Information Protection and Electronic Documents Act*[10], *Act on the Protection of Personal Information*[11], dentre outras).

Eventuais informações complementares ao §1º do art. 48 poderão ser requisitadas pela ANPD no caso concreto.

É importante, ainda, que o controlador possa complementar a notificação caso não tenha todas as informações pertinentes dentro do prazo estabelecido pela regulamentação.

[8] Disponível em: https://gdpr-info.eu/. Acesso em 22.03.2021.
[9] Disponível em: https://www.oaic.gov.au/privacy/notifiable-data-breaches/. Acesso em 22.03.2021.
[10] Disponível em: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/. Acesso em 22.03.2021.
[11] Disponível em: https://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf. Acesso em: 22.03.2021.

6. Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)

Sugere-se o prazo de 10 dias úteis para o controlador notificar a ANPD sobre um incidente, contados a partir do momento em que ele efetivamente verificar que, (i) o incidente envolve dados pessoais; (ii) a organização noticiante é a controladora da respectiva base de dados pessoais objeto do incidente e (iii) a análise do *score* do incidente leve a conclusão de que há risco ou dano aos titulares de dados. Ou seja, uma vez confirmado o incidente de forma inequívoca, o controlador deveria ter o prazo de 10 (dez) dias úteis contados desta confirmação para compilar as informações exigidas pela LGPD (e posterior regulamentação) a fim de comunicar o incidente à ANPD.

Seguindo esta linha, o *WP29* considera que um controlador deve ser considerado como tendo "tomado conhecimento" quando ele tem um grau razoável de certeza de que ocorreu um incidente de segurança que levou ao comprometimento de dados pessoais. A ciência do controlador acerca de uma violação específica dependerá das circunstâncias do incidente, podendo, em alguns casos, ser evidente desde o início da ocorrência ou, em outros, levar algum tempo para estabelecer se os dados pessoais foram comprometidos. A ênfase, no entanto, deve ser na ação imediata para investigar o incidente para determinar se os dados pessoais foram realmente violados e, em caso afirmativo, tomar medidas corretivas e notificar a ANPD, se necessário.

O prazo para a notificação da Autoridade competente, segundo o *GDPR*[12], é de 72 horas. Segundo o *Notifiable Data Breach Scheme*[13] australiano, o controlador deve tomar todas as medidas razoáveis para concluir a avaliação sobre o incidente dentro de 30 dias corridos. No Novo México, Estados Unidos, o prazo é de 45 dias para a notificação de incidentes que afetem mais de mil residentes. Segundo o *Health Insurance Portability and Accountability Act*[14] (*HIPPAA*, Estados Unidos) o número de indivíduos afetados é utilizado como critério para a definição do

[12] Disponível em: https://gdpr-info.eu/. Acesso em: 22.03.2021.
[13] Disponível em: https://www.oaic.gov.au/privacy/notifiable-data-breaches/. Acesso em: 22.03.2021.
[14] Disponível em: https://www.cdc.gov/phlp/publications/topic/hipaa.html. Acesso em 22.03.2021.

prazo de notificação: se superior a 500 indivíduos, deve-se notificar a Secretaria em no máximo 60 dias corridos; se inferior, dentro de 60 dias antes do término do ano em que o incidente ocorreu. Importa mencionar que tais prazos servem apenas como referência e que é de suma importância que a ANPD defina um prazo que se adapte à realidade do país, tendo em vista que a cultura de proteção de dados no Brasil ainda é incipiente e que o objetivo é consolidá-la de modo consistente.

Existem, ainda, requisitos setoriais específicos que determinam prazos próprios para a notificação. Por exemplo, os Requisitos de Segurança Cibernética do Departamento de Serviços Financeiros de Nova York[15], que entrou em vigor em 2017, estabelecem o prazo de 72 horas para que as organizações reportem um incidente.

[15] Disponível em: https://www.dfs.ny.gov/industry_guidance/cybersecurity. Acesso em 22.03.2021.

7. Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?

Sugere-se que seja realizado o quanto antes, sem demora injustificada, no prazo de até 15 dias úteis, a notificação do controlador aos titulares, contados a partir do momento em que ele efetivamente consegue chegar à conclusão de que:

1) O incidente envolve dados pessoais;
2) A organização noticiante é a controladora da respectiva base de dados pessoais objeto do incidente; e
3) A análise do score do incidente leve a conclusão de que há elevado risco ou dano aos titulares de dados.
4) O incidente foi reportado à ANPD, salvo nos casos em que a notificação à Autoridade não fosse requerida e que o controlador, a seu critério, decida notificar os titulares para que tomem eventuais medidas preventivas.

É importante que a comunicação seja realizada "o quanto antes" para que os titulares de dados, diante da relevância do evento, possam adotar as medidas que considerarem pertinente diante da ciência do ocorrido, porém, se houver justificativa do controlador, aqui o prazo seria maior diante da complexidade que há para se traçar a melhor estratégia para notificar os titulares, de acordo com o tipo de relação e de dados que há entre controlador e titulares.

Por fim, entende-se que a comunicação deve conter (i) descrição e natureza do incidente, (ii) riscos relacionados aos incidentes, (iii) medidas adotadas para reverter/ mitigar os riscos, e (iv) eventuais recomendações ao titular (se aplicável). Nesse sentido, seria possível replicar a lista de informações do artigo 48, parágrafo 1º, desde que fosse admitida a adaptação da informação para que de fato atenda às necessidades do titular, podendo ser mais objetiva e menos técnica.

R. Dr. Plínio Barreto, 285 | Bela Vista | cep 01313-020 | São Paulo | SP | Brasil | tel 55 11 3254.1700
www.fecomercio.com.br

8. Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?

A comunicação mais adequada é aquela que leva em consideração o tipo de relacionamento existente entre o controlador e o titular e as modalidades de comunicações prévias entre ambos. Outro critério que deve ser levado em consideração é o tipo de dado pessoal já existente no controlador quanto ao titular afetado para avaliar se seria possível uma comunicação individualizada ou não. Por vezes, o controlador pode não possuir uma base consistente de e-mails dos titulares, por exemplo.

Por isso, a forma de comunicação deve ficar à critério do controlador, possibilitando que adote seus próprios canais de comunicação, preservando a experiência do titular e a escalabilidade da comunicação, baseado nas interações já estabelecidas com o cliente.

Em regra, o incidente deve ser comunicado diretamente aos titulares dos dados pessoais afetados, a menos que isso implique um esforço desproporcional. Nesse caso, pode haver uma comunicação pública ou medida semelhante em que os titulares sejam informados de forma igualmente eficaz (artigo 34(3)c do GDPR).

Além disso, caso o risco já tenha sido mitigado, sem qualquer impacto para o titular, a comunicação pelo controlador deveria ser facultativa. Nesse sentido, o *GDPR* já dispõe sobre essa possibilidade em seu artigo 34.3, conforme abaixo:

A comunicação ao titular dos dados a que se refere o nº. 1 não é exigida se for preenchida uma das seguintes condições:

a) O responsável pelo tratamento tiver aplicado medidas de proteção adequadas, tanto técnicas como organizativas, e essas medidas tiverem sido aplicadas aos dados pessoais afetados pela

violação de dados pessoais, especialmente medidas que tornem os dados pessoais incompreensíveis para qualquer pessoa não autorizada a acessar a esses dados, tais como a criptografia;
b) O responsável pelo tratamento tiver tomado medidas subsequentes que assegurem que o elevado risco para os direitos e liberdades dos titulares dos dados a que se refere o nº 1 já não é suscetível de se concretizar; ou
c) Implicar um esforço desproporcional. Nesse caso, é feita uma comunicação pública ou tomada uma medida semelhante através da qual os titulares dos dados são informados de forma igualmente eficaz.[16]

Alguns exemplos de métodos de comunicação transparentes incluem mensagens diretas (como e-mail, SMS, mensagem direta), *banners* ou notificações em destaque no site, comunicações postais e anúncios importantes na mídia. Mas, novamente, o critério relevante será a relação entre controlador e titular e as modalidades de comunicações prévias já existentes, se assertivas.

Os controladores, principalmente quando interagem com frequência com seus clientes, estão na melhor posição para determinar o canal de contato mais apropriado para comunicar um incidente a eles. Justamente por isso, o critério de escolha do canal utilizado deve ficar a critério do controlador.

Em algumas hipóteses, porém, pode ser extremamente custoso ou até mesmo impossível realizar a notificação direta aos titulares afetados. Nesse sentido, o *Personal Information Protection and Electronic Documents Act*[17] estabelece as seguintes hipóteses em que a notificação indireta de titulares é permitida:

a) a notificação direta provavelmente resultaria em maiores danos ao titular afetado;
b) a notificação direta provavelmente seria excessivamente difícil para o controlador; e
c) o controlador não possui meios adequados para entrar em contato com o titular.

[16] Disponível em: https://gdpr-info.eu/. Acesso em: 22.03.2021.
[17] Disponível em: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/. Acesso em: 22.03.2021.

R. Dr. Plínio Barreto, 285 | Bela Vista | cep 01313-020 | São Paulo | SP | Brasil | tel 55 11 3254.1700
www.fecomercio.com.br

9. Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?

A obrigatoriedade de notificar um incidente à ANPD poderá ser excetuada sempre que o cálculo de risco adotado pelo controlador indicar a probabilidade de baixou ou médio risco ou dano.

Ainda, alguns outros elementos de análise podem ser extraídos do *Act on the Protection of Personal Information*[18] (APPI, Japão):

a) quando os dados pessoais afetados possuírem criptografia de alto nível (com o sistema de criptografia em conformidade com a *ISSO/IEC* 18033, por exemplo, ou a chave de descriptografia é controlada remotamente);
b) quando os dados pessoais forem recuperados pelo controlador antes de ser acessados por terceiros não autorizados;
c) quando não existir risco de um titular específico ser identificado;
d) quando o incidente seja flagrantemente insignificante (por exemplo, uma entrega incorreta de um pacote em que as informações pessoais estejam apenas na sua etiqueta de entrega).

Além disso, seguido a linha do GDPR, recomendam-se outras hipóteses nas quais os controladores não deveriam ter a obrigação de comunicar o incidente aos usuários, incluindo (i) se, antes da violação, o controlador tiver implementado medidas técnicas e organizacionais aptas a proteger os dados pessoais, tornando-os ininteligíveis para qualquer pessoa que não esteja autorizada a acessar aquele banco de dados; (ii) se, imediatamente após uma violação, o controlador tomar medidas para garantir que o alto risco para os direitos e liberdades dos indivíduos não se materialize e (iii) se a comunicação com os indivíduos demandar esforços desproporcionais em face do controlador.

[18] Disponível em: https://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf. Acesso em: 22.03.2021.

10. Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?

A obrigatoriedade de notificar um incidente ao titular poderá ser excetuada sempre que o cálculo de risco adotado pelo controlador indicar a probabilidade baixou ou médio risco ou dano.

Ou seja, resgatando a sugestão indicada na questão 2 acima, a comunicação aos titulares de dados somente deve ocorrer nos casos em que o incidente possa resultar em um alto risco ou dano, sendo a severidade do risco calculada com base em um critério objetivo. Recomenda-se a adoção da metodologia criada pela ENISA (*European Union Agency for Network and Information Security*), segundo a fórmula: Severidade do Risco = Contexto do Processamento x Facilidade de identificação do titular + Circunstâncias do Incidente.

Dessa forma, para além das exceções da obrigatoriedade de informar à ANPD (que, por conseguinte, aplicam-se também ao dever de informar aos titulares), sugere-se as seguintes exceções, consonantes com o artigo 34(3) do GDPR:[19]

a) quando existirem motivos razoáveis para o controlador crer que a notificação dos titulares poderá causar prejuízos a investigações em andamentos conduzidas pela força policial (em consonância também com a previsão da Consideranda 88 do GDPR e com o *Notification Data Breach Scheme* australiano);

b) se o controlador agir rapidamente de modo a remediar o incidente e, como resultado, reduzir a possibilidade de que ele resulte em elevados riscos ou danos para os titulares (previsão contida também na legislação japonesa[20]);

[19] Disponível em: https://gdpr-info.eu/
[20] Disponível em: https://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf

c) o controlador utilizou medidas técnicas e organizacionais adequadas para proteger os dados pessoais antes da violação (em especial, medidas aptas a tornar os dados pessoais ininteligíveis para qualquer pessoa que não esteja autorizada a acessá-los);

d) quando contatar os titulares requereria um esforço desproporcional, seja pela perda de informações de contato ocasionada pelo próprio incidente ou pela inexistência de tais informações; seja pela abrangência do incidente sobre um número extremamente elevado de titulares (aqui, deverá ser estabelecido critério objetivo pela ANPD para definição de uma exceção em virtude do número de indivíduos afetados.

11. Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)

Como ponto de partida para os critérios da análise de gravidade do incidente de segurança, indicamos os parâmetros mencionados nas respostas 1 e 2 acima.

Além disso, considerando que o artigo 48 §2º prevê o alinhamento da gravidade do incidente para definir as providências mirando a salvaguarda dos direitos dos titulares, complementarmente à mensuração do risco em si, é importante que a ANPD leve em consideração a postura do Controlador bem como as medidas tomadas para mitigar os riscos.

Neste sentido, nossas contribuições para este item seriam as seguintes:

a) Cálculo de risco do incidente apresentado pelo controlador (incluindo-se os requisitos sugeridos previamente);
b) Medidas de mitigação adotadas pelo controlador;
c) Tempo de descoberta e resposta ao incidente;
d) Nível de colaboração do controlador com a Autoridade e demais órgãos reguladores e/ou autoridades policiais;
e) Justificativas do controlador para eventuais atrasos em notificações;
f) Esforços adotados pelo controlador para informar e auxiliar os titulares afetados.

12. Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?

Sim, o Security - ENISA para uma metodologia de avaliação da gravidade das violações de dados pessoais.

Para questões de volumetria, o da Commission Nationale de L'Informatique et des Libertés (CNIL): Methodology for Privacy Risk Management, 2012[21].

[21] Disponível em: https://www.cnil.fr/sites/default/files/typo/document/CNIL-ManagingPrivacyRisks-Methodology.pdf

13. Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?

A ANPD deve determinar aos controladores após a comunicação do incidente as medidas segurança, boas práticas e de governança já existentes na LGPD, aplicáveis ao caso em concreto, observada a gravidade do incidente, tamanho do controlador, número de titulares de dados impactados e probabilidade de recorrência do incidente (entre outros).

De maneira complementar apontamos, ainda, as seguintes sugestões de providências:

1. Determinação de preservação dos dados afetados e sistemas utilizados;
2. Realização de auditoria para identificar a origem e os motivos pelos quais o incidente ocorreu;
3. Recomendação de técnicas de tratamento de dados pessoais (como forma de educação aos agentes de tratamento) bem como a recomendação de adoção de medidas baseadas na origem e motivos dos incidentes.
4. Viabilização de solução de conflitos entre Controlador de Dados Pessoais, ANPD e titulares de dados, com técnicas de mediação, conciliação ou dispute board para minimização da judicialização em caso de comprovação de responsabilidade dos agentes de tratamento de dados.

Ademais, as recomendações da ANPD devem levar em consideração as medidas de segurança já adotadas pelo controlador, bem como o impacto destas no modelo de negócio da empresa, incluindo a ponderação quanto à possibilidade técnica e financeira de suas respectivas implementações.

14. O operador pode notificar diretamente a ANPD ou o titular? Se sim, em quais circunstâncias?

De acordo com o artigo 5º, inciso VI da LGPD, o controlador é a "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais".

Neste sentido, entendemos que o operador não deve notificar diretamente a ANPD, mas o controlador, o quanto antes, sem demorada injustificada, bem como fornecer os insumos para que o controlador possa analisar o evento e realizar a comunicação.

Em nossa avaliação essa dinâmica é importante para que o controlador consiga reunir todas as informações necessárias (que constam expressamente no art. 48 da LGPD) e encaminhem de forma ordenada à ANPD, evitando, assim, informações divergentes e/ou comunicações que exponham os envolvidos no tratamento de dados em caso de incidentes.

Importante destacar que o GDPR estabelece o mesmo racional, qual seja, o de atribuir ao Controlador a obrigação de notificar a autoridade de proteção de dados, conforme considerado nos itens 85 a 88[22].

[22] (85) A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned. **Therefore, as soon as the controller becomes aware that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons.** Where such notification cannot be achieved within 72 hours, the reasons for the delay should accompany the notification and information may be provided in phases without undue further delay.

(86)
The controller should communicate to the data subject a personal data breach, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of the natural person in order to allow him or her to take the necessary precautions. The communication should describe the nature of

15. Outras sugestões

Independentemente da utilização de medidas técnicas e administrativas adotadas para proteger dados e prevenir incidentes, tanto pelo setor produtivo brasileiro, como também por órgãos da administração pública, acompanhamos no Brasil o triste avanço do comércio ilegal de dados sem a devida responsabilização criminal dos envolvidos.

Assim, as organizações poderão continuar investindo fortemente em políticas e procedimentos de segurança, adotando medidas, de acordo com melhores práticas, para identificar fraudes e proteger dados pessoais. Porém, possivelmente continuarão sendo vítimas de eventos ilícitos pela complexidade inerente a desproporcionalidade do binômio segurança e exploração de vulnerabilidades, de tal sorte que é fundamental também uma forte e competente estrutura investigativa contra aqueles que realmente buscam falhas, obtêm eventuais dados ilicitamente e ainda os expõem e os comercializam, para que sejam devidamente identificados e punidos.

Nesse sentido, as organizações que tiverem adotado as medidas técnicas e administrativas para garantir a segurança e a proteção de dados pessoais de seus clientes e colaboradores e que, diante de um incidente inevitável, tomam todas as medidas necessárias ao seu alcance para mitigar os riscos, não deveriam ser penalizadas pelas sanções da LGPD.

Além disso, é importante que sejam adotadas medidas para restringir a publicidade das investigações em curso, não afetando desnecessária e desproporcionalmente a imagem da empresa no mercado. Tais medidas também protegem os titulares de dados, uma vez que podem existir vulnerabilidades ainda em análise pelo controlador.

---

the personal data breach as well as recommendations for the natural person concerned to mitigate potential adverse effects. Such communications to data subjects should be made as soon as reasonably feasible and in close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities. For example, the need to mitigate an immediate risk of damage would call for prompt communication with data subjects whereas the need to implement appropriate measures against continuing or similar personal data breaches may justify more time for communication. (Grifos não constantes do original)

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: FEDERAÇÃO DAS INDÚSTRIAS DO ESTADO DE MINAS GERAIS (FIEMG)

CPF/CNPJ: 17.212.069/0001-81

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regularmente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS **IMPORTANTE:** Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	Sugere-se observar o incidente sob duas perspectivas, a saber: i) o tipo de enquadramento incidente: se este resulta em dano ao titular ou apresenta apenas algum tipo de risco de dano ao titular; ii) a responsabilização: a responsabilidade do controlador pelo incidente sempre vai existir, contudo, não pode ser confundida com eventual responsabilidade específica de reparação de dano causado ao titular (o dano deve ser sempre avaliado sob a perspectiva da legislação aplicável ao caso, exemplo: CDC, CLT...). A responsabilidade pode gerar uma penalidade administrativa e o dano efetivo ao titular é passível de reparação pessoal/coletiva.
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	Sugere-se o estabelecimento de metodologia de avaliação de riscos, que seja capaz de indicar o nível de sensibilidade do incidente em função da relação entre os critérios: i) tipos de dados vazados/expostos; ii) volumetria de titulares de dados; iii) natureza do incidente. A relação entre os critérios deverá categorizar o incidente na seguinte escala: i) muito alto; ii) alto; iii) moderado; iv) baixo; v) muito baixo.

	O risco ou dano categorizado como muito baixo deve ser considerado como "não relevante" e, portanto, não passível de comunicação à ANPD, mantidas as responsabilidades da controladora.
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	Sugere-se que o risco de dano ao titular seja caracterizado pela possibilidade/probabilidade de ocorrência de um prejuízo ao titular de dados. Já o dano materializado e relevante deve ser caracterizado como a ocorrência de um efetivo prejuízo ao titular de dados. (Em todos o casos, o dano e a consequente responsabilidade devem ser avaliados de acordo com a legislação específica). Eles se relacionam sob a perspectiva da responsabilidade, já que em ambos os casos poderá existir a responsabilidade do controlador.
O que deve ser considerado na avaliação dos riscos do incidente?	Sugere-se que sejam considerados: i) volumetria; ii) elemento (tipo de dado); iii) tipo de incidente; e iv) data provável da ocorrência.
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	Sugere-se apenas as informações do artigo 48. Informações adicionais devem ser solicitadas pontualmente pela ANPD, assegurando-se prazo razoável.
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	5 dias úteis. Após a ciência do fato pelo controlador, as prioridades devem ser em função de acionar frentes de proteção e segurança para mitigar os danos do incidente, comunicar ao titular dos dados e, por fim, colher detalhes para comunicação à ANPD.
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	2 ondas de comunicação: a primeira mais genérica, inicial, em até 72 horas após a ciência do incidente, comunicando que houve o vazamento de dados para todos os titulares potencialmente atingidos. A segunda onda, mais específica e com mais detalhes, aos titulares de fato atingidos. Todas as ondas dentro do prazo de comunicação à ANPD. Comunicar ao titular deve ser uma prioridade, de forma mais genérica para os potencialmente atingidos para que possam ser tomadas atitudes imediatas (como trocar senhas, por exemplo) e, assim que mais apurado o fato, orientar de forma mais específica aos titulares de fato atingidos.

Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	2 ondas de comunicação: i) a primeira mais genérica, inicial de forma ampla, pelo site, redes sociais ou nota à imprensa, contanto que seja efetiva. ii) A segunda onda, mais específica e com mais detalhes, pelo canal individual de comunicação com o titular (e-mail ou via postal), de acordo com a especificidade do incidente.
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	Não devem ser admitidas exceções para os casos de acesso não autorizado a dados pessoais. Entretanto, sem o potencial de risco não há razão para acionar todo o processo e a ANPD também não será acionada em situações dessa natureza evitando uma sobrecarga. Nesse sentido, nesses casos, deve haver um registro interno na organização que evidencie a ocorrência.
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	Quando não houver potencial de risco aos titulares. Sem o potencial de risco não há razão para acionar os titulares.
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	Volumetria, tipologia do incidente e dos dados impactados. Critérios que dão insumos para a ANPD avaliar o potencial de dano ou risco do incidente.
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	A ANPD deve estabelecer critérios independente de metodologia, tais como os acima mencionados (volumetria, tipologia do incidente e dos dados impactados), e propor uma *guideline* com diretrizes (exemplo: https://edps.europa.eu/sites/edp/files/publication/18-12-05_guidelines_data_breach_en_0.pdf, https://iapp.org/media/pdf/resource_center/ENISA-breach-severity-methodology.pdf). É mais importante estabelecer critérios do que a metodologia em si.
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	Reter o vazamento ou incidente, identificar sua origem e motivo, avaliar o grau de impacto aos titulares e elaborar um plano de recuperação do incidente, sendo acompanhado por um determinado tempo. Exigir conformidade com a LGPD e que o evento seja incluído em eventuais treinamentos. Reavaliar a política de segurança da informação e de privacidade.

SUGESTÃO DE NORMATIVO, SE HOUVER	
Art. Xxxx	
Art. Xxxx	

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: FEDERAÇÃO DAS INDÚSTRIAS DO ESTADO DE SÃO PAULO

CPF/CNPJ: 62.225.933/0001-34

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS	
IMPORTANTE: Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
QUESTÃO 1: Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	Incidentes envolvendo dados pessoais, conforme linha da União Europeia,[1] podem ser categorizados conforme três princípios básicos de segurança da informação: a) Violação de confidencialidade, quando ocorre a divulgação não autorizada ou acidental de dados pessoais, ou o acesso não autorizado a dados pessoais; b) Violação de integridade, onde há uma alteração não autorizada ou acidental de dados pessoais; e c) Violação de disponibilidade, quando ocorre uma perda acidental ou não autorizada de acesso a dados pessoais ou a destruição de dados pessoais. Desse modo, seguindo a linha da Consideranda 75 do GDPR[2], um incidente de segurança envolvendo dados pessoais poderá acarretar risco quando possa dar origem à discriminação, perdas financeiras, prejuízos efetivos para a reputação, inversão não autorizada da pseudonimização; quando os titulares dos dados possam ficar privados dos seus direitos; quando forem avaliados aspectos de natureza pessoal, em particular análises ou previsões que digam respeito ao desempenho no trabalho, à situação econômica, à saúde, às preferências ou interesses pessoais e comportamento, a fim de definir ou fazer uso de perfis; quando forem tratados dados relativos a vulneráveis, em particular crianças; ou quando o tratamento incidir sobre uma grande quantidade de dados pessoais e afetar um grande número de titulares de dados.

[1] O Article 29 Working Party (The Working Party on the Protection of Individuals with regard to the Processing of Personal Data ou WP29), antigo órgão consultivo composto por representantes da Autoridade de Proteção de Dados de cada Estado-membro da União Europeia, pela Autoridade Europeia para a Proteção de Dados e pela Comissão Europeia, posteriormente substituído, com a entrada em vigor do General Data Protection Regulation (doravante GDPR), pelo Conselho Europeu de Proteção de Dados, em sua Opinião 03/2014 sobre notificação de incidentes. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

[2] Disponível em: https://gdpr-info.eu/

	Neste sentido, algumas situações denotam risco ou dano relevante ao titular, especialmente, quando envolvem: (i) dados pessoais sensíveis; (ii) dados pessoais classificados como confidenciais; (iii) titulares em situação de vulnerabilidade, como crianças; (iv) potencial concreto de ocasionar danos materiais ou morais, tais como discriminação, violação do direito à imagem e à reputação, fraudes financeiras e roubo de identidade; (v) volume significativo de dados envolvidos; (vi) número significativo de indivíduos afetados; (vii) características específicas do controlador de dados pessoais, observados a sua estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares; (viii) comprovação de dolo e/ou má-fé pelo agente causador do dano; e (ix) possibilidade de maior facilidade na identificação dos titulares a partir dos dados expostos. Outro critério relevante é a (viii) qualidade dos dados, isto é, se os dados são atuais e passíveis de caracterizar risco efetivo. Acerca do dano, precisa haver uma possibilidade concreta de prejuízo financeiro, reputacional ou físico do titular. Quanto a possibilidade de dano moral, importante definir as situações em que será possível afirmar que um titular de fato sofreu tal dano em virtude de um incidente, vez que a adoção da teoria do dano moral presumido, ou *in re ipsa*, pelo ordenamento jurídico pátrio, poderá resultar no sancionamento e/ou na judicialização excessiva do tema e em prejuízos desproporcionais aos agentes de tratamento. Também é possível que um incidente de segurança com dados pessoais ocasione danos materiais aos titulares afetados, resultando em roubos de identidade, fraudes bancárias, efeitos negativos ao histórico de crédito, e perdas financeiras em geral. Tais exemplos de danos materiais ao titular são apontados pela WP29 em suas diretrizes sobre a notificação de incidentes de dados (*"Guidelines on Personal data breach notification under Regulation 2016/679")*[3] e pela *Federal Trade Comission*, agência reguladora antifraude norte americana.[4] A perda de emprego, de negócios ou de oportunidades profissionais são apontadas na normativa canadense[5] como possíveis resultados negativos ao titular de um incidente envolvendo seus dados pessoais. Também é possível incluir aqui a perda de confidencialidade de dados pessoais protegidos por sigilo profissional.

[3] Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052
[4] Disponível em: https://www.consumer.ftc.gov/articles/0235-identity-theft-protection-services
[5] Disponível em: https://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html

	Ademais, uma combinação envolvendo diferentes tipos de dados pessoais poderá ser parâmetro do nível de risco, tendo em vista que o cruzamento dessas informações com outras bases de dados poderá revelar aspectos relevantes sobre os titulares[6]. Critérios sugeridos para análise do risco ou dano relevante serão apresentados no tópico seguinte.
QUESTÃO 2: O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	Sim, sugere-se que o risco ou dano para os titulares como resultado de uma violação deve ser avaliado objetivamente de acordo com a probabilidade de "nenhum risco/dano", "risco/dano" ou "alto risco/dano". A classificação proposta está em conformidade com a nomenclatura adotada no GDPR, o entendimento consolidado na Consideranda 76[7] e nas diretrizes da WP29 sobre notificação de incidentes de dados.[8] Desse modo, a notificação à ANPD não deve ser necessária quando for improvável que o incidente resulte em risco ou dano para o titular (cabendo ao controlador, não obstante, documentá-lo e estar apto a comprovar a ausência do risco ou dano). Sempre que houver a probabilidade razoável de risco ou dano, por sua vez, o incidente deverá ser comunicado somente à ANPD. A comunicação aos titulares, porém, somente se aplicaria nos casos em que o incidente possa resultar em um alto risco ou dano. Tal balizamento é de muita relevância para se evitar que os titulares sejam importunados com notificações desnecessárias (*"Unnecessary notification fatigue"*, nos termos da WP29), mas ao mesmo tempo garantindo que tenham conhecimento dos incidentes mais relevantes. A fim de distinguir ambos os tipos de risco, deve-se levar em conta: a) o tipo de incidente (se uma violação de confidencialidade, integridade ou disponibilidade de dados); b) a natureza dos dados pessoais (se simples, comportamentais, financeiros ou sensíveis); c) a facilidade de se identificar o titular; d) o volume de dados tratados e o número de indivíduos afetados; e) as possíveis consequências adversas ao titular (severidade e duração/permanência dessas consequências); f) características especiais do titular (se criança, idoso, ou pertencente a outros grupos vulneráveis); g) características especiais do controlador. Novamente, tais critérios para calcular o risco ou dano do

[6] Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052
[7] Disponível em: https://gdpr-info.eu/
[8] Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

	incidente estão em consonância com as diretrizes da WP29. Outro critério relevante é a qualidade dos dados, isto é, se os dados são atuais e passíveis de caracterizar risco efetivo. O *Notifiable Data Breach scheme* (NDB)[9]*,* norma australiana sobre a notificação de incidentes de segurança de dados, também adota critérios similares para o dever de notificação à Autoridade (e titulares), que deverá ser realizado somente quando houver a probabilidade de que o incidente resulte em dano grave (*"serious harm"*) aos afetados. Tal qualificação leva em conta: o tipo de informação (ou natureza dos dados); a sensibilidade; as medidas de segurança existentes e a possibilidade de superá-las; as pessoas, ou tipo de pessoas, que obtiveram ou poderiam obter as informações – bem como suas possíveis intenções maliciosas; e a natureza do dano. Para além da sensibilidade dos dados, a norma canadense[10] também leva em consideração para a análise de "um risco real de dano significativo" (*"serious harm of significant damage"*) ao titular a probabilidade de que os dados pessoais tenham sido, são ou possam ser utilizados indevidamente – levando em conta, portanto, a boa-fé e as intenções dos terceiros não autorizados que acessem os dados. Segundo a WP29, essa análise é importante para avaliar a severidade do incidente, vez que é possível que o controlador possua um relacionamento prévio com a pessoa ou instituição que teve acesso indevido aos dados pessoais (por exemplo, ao receber um e-mail encaminhado acidentalmente) e, estando ciente de seus procedimentos, histórico e outros detalhes importantes, possa considerá-lo como confiável[11]. O número de indivíduos afetados por um incidente é também utilizado como parâmetro, sobretudo na legislação norte americana, para definir o dever ou não de comunicação às autoridades competentes. No Estado da California, empresas que forem vítimas de crimes cibernéticos ou violação de dados devem emitir notificações quando 500 ou mais residentes do estado forem afetados;[12] no Novo México, o prazo é de 45 dias para a notificação de incidentes que afetem mais de mil residentes.[13] Assim, é importante que a ANPD estabelece parâmetros objetivos para definir o que constitui um grande volume de dados envolvido em um incidente, e um quantitativo elevado de indivíduos afetados

[9] Disponível em: https://www.oaic.gov.au/privacy/notifiable-data-breaches/
[10] Disponível em: https://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html
[11] Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052
[12] Disponível em: https://oag.ca.gov/privacy/ccpa
[13] Disponível em: https://www.nmlegis.gov/Sessions/19%20Regular/bills/senate/SB0176.pdf

	(parâmetros já estabelecidos pela Autoridade como importantes para a análise de risco ou dano relevante[14]). No que diz respeito ao cálculo de severidade do risco, sugerimos a adoção de um critério objetivo, baseando-se na metodologia criada pela ENISA (*European Union Agency for Network and Information Security*), segundo a fórmula: Severidade do Risco = Contexto do Processamento x Facilidade de identificação do titular + Circunstâncias do Incidente. A agência oferece parâmetros de ajuste para cada uma dessas variáveis, facilmente adaptáveis ao contexto brasileiro. Os resultados da fórmula proposta correspondem a quatro níveis de gravidade: baixo e médio (ausência de risco ou dano e, consequentemente, do dever de notificação); alto e muito alto (risco ou dano, e dever de notificação à ANPD e/ou aos titulares afetados).
QUESTÃO 3: Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	O risco implica um modo particular de se referir a um evento futuro contingente, através da percepção da antecipação dos seus efeitos. Essa antecipação conduz à avaliação das possíveis consequências danosas para sopesar um coeficiente de probabilidade e discernir o seu valor. No risco, tem-se, portanto, um caráter ativo de avaliação e antecipação de consequências. O dano, por sua vez, corresponde à efetiva materialização do risco[15]. A identificação de riscos e das prováveis consequências da sua ocorrência são normalmente previstas/estimadas, com antecedência por uma avaliação contínua de risco. A verificação dos danos reais só acontecerá depois do risco ser materializado ou ocorrido. Em termos de proteção de dados pessoais, o risco de incidente corresponderá a todas as consequências danosas que poderão ser vislumbradas (por exemplo, a indisponibilidade de um serviço, a perda de informações, o acesso indevido por terceiros). Caso uma das consequências danosas venha a ser concretizada, haverá um dano ao titular (por exemplo, a indisponibilidade de um prontuário médico pode resultar em um dano à saúde, ou o acesso não autorizado em um roubo de identidade).

[14] Disponível em: https://www.enisa.europa.eu/publications/dbn-severity
[15] FERREIRA, Kelly. Responsabilidade Civil Preventiva: Função, pressupostos e aplicabilidade (tese). Faculdade de Direito da Universidade de São Paulo,2014.

	Nesse contexto, a diferenciação entre risco e dano será essencial para fins de alocação de responsabilidade e para o dever de reparação a um titular afetado. Por exemplo, para o ajuizamento de uma ação ressarcitória ou de danos morais, deverá, necessariamente, existir a materialização do dano (art. 42, da LGPD). O risco, por sua vez, assim como o próprio dano, poderá ser utilizado como critério desencadeador da obrigação de notificar a ANPD e os titulares, conforme sugerido anteriormente.
QUESTÃO 4: O que deve ser considerado na avaliação dos riscos do incidente?	Deve-se considerar os critérios acima mencionados e sugeridos pela WP29: a) o tipo de incidente (se uma violação de confidencialidade, integridade ou disponibilidade de dados); b) a natureza dos dados pessoais (se simples, comportamentais, financeiros ou sensíveis); c) a facilidade de se identificar o titular; d) o volume de dados tratados e o número de indivíduos afetados; e) as possíveis consequências adversas ao titular (severidade e duração/permanência dessas consequências); f) características especiais do titular (se criança); g) características especiais do controlador (se atua na área médica ou financeira, por exemplo). Outro critério relevante é a qualidade dos dados, isto é, se os dados são atuais e passíveis de caracterizar risco efetivo.
QUESTÃO 5: Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	As informações elencadas no §1º do art. 48 da LGPD são suficientes para integrar a notificação encaminhada pelos controladores à ANPD, em caso de incidente. Elas correspondem às informações listadas como necessárias em outras legislações de proteção de dados pessoais (*General Data Protection Regulation, Notifiable Data Breach scheme, Personal Information Protection and Electronic Documents Act, Act on the Protection of Personal Information,* dentre outras). Ademais, levando-se consideração a dificuldade com a qual o controlador se depara não apenas para detectar, mas também investigar e levantar as informações solicitadas, somadas a restrições temporais impostas pelo dever de comunicação[16], entendemos que apenas as informações já inseridas na Lei 13.709/2018 devem ser cobradas do controlador pela ANPD.

[16] IBM. *Relatório sobre o prejuízo de um vazamento de dados*, 2020. Disponível em: https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/pt. Acesso em: 24 fev. 2021.

	É importante, ainda, que exista a possibilidade de o controlador realizar uma comunicação parcial à ANPD, caso não seja possível apurar todas as informações listadas na lei antes dentro do prazo estabelecido pela Autoridade para a notificação. Essa comunicação parcial não deve resultar em prejuízos para o controlador desde que, respeitando o princípio da responsabilização e prestação de contas (art. 6º, X, Lei 13.709/2018), ele esteja apto a demonstrar que não era possível obter todas as informações solicitadas dentro do prazo. Na medida em que as investigações do controlador sobre o ocorrido avancem, poderão ser submetidas comunicações complementares à ANPD.
QUESTÃO 6: Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	Sugere-se o prazo de 10 dias úteis para o controlador notificar a ANPD sobre um incidente, contados a partir do momento em que ele efetivamente consegue chegar à conclusão de que: 1) O incidente envolve dados pessoais; 2) A organização noticiante é a controladora da respectiva base de dados pessoais objeto do incidente; e 3) A análise do score do incidente leve a conclusão de que há risco ou dano aos titulares de dados. Seguindo esta linha, o WP29 considera que um controlador deve ser considerado como tendo "tomado conhecimento" quando ele tem um grau razoável de certeza de que ocorreu um incidente de segurança que levou ao comprometimento de dados pessoais. A ciência do controlador acerca de uma violação específica dependerá das circunstâncias do incidente, podendo, em alguns casos, ser evidente desde o início da ocorrência ou, em outros, levar algum tempo para estabelecer se os dados pessoais foram comprometidos. A ênfase, no entanto, deve ser na ação imediata para investigar o incidente para determinar se os dados pessoais foram realmente violados e, em caso afirmativo, tomar medidas corretivas e notificar a ANPD, se necessário. O prazo para a notificação da Autoridade competente, segundo o GDPR, é de 72 horas. Segundo o *Notifiable Data Breach scheme* australiano, o controlador deve tomar todas as medidas razoáveis para concluir a avaliação sobre o incidente dentro de 30 dias corridos; no Novo México, Estados Unidos, o prazo é de 45 dias para a notificação de incidentes que afetem mais de mil residentes. Segundo o *Health Insurance Portability and Accountability Act*[17] (HIPPAA, Estados Unidos) o número de indivíduos afetados é utilizado como critério para a definição do prazo de notificação: se superior a 500 indivíduos, deve-se notificar a Secretaria em no máximo 60 dias corridos; se inferior, dentro de 60 dias antes do término do ano em que o incidente ocorreu. Existem, ainda, requisitos setoriais específicos que determinam prazos próprios para a notificação. Por exemplo, os Requisitos de Segurança Cibernética do Departamento de Serviços Financeiros de

[17] Disponível em: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/combined-regulation-text/index.html

	Nova York, que entrou em vigor em 2017, estabelecem o prazo de 72 horas para que as organizações reportem um incidente. A recomendação da ANPD requer 2 (dois) dias úteis, o GDPR 3(três) dias. Entendemos que no Brasil, empresas que disponham de um CSIRT (um grupo técnico responsável por resolver incidentes relacionados à segurança em sistemas computacionais, apoiados por ferramentas de softwares e hardwares adequados), podem conseguir atender esse prazo. As demais que representam a grande parte do mercado, possivelmente não terão condições de cumpri-lo.
QUESTÃO 7: Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	Sugere-se que seja realizado o quanto antes, sem demora injustificada, no prazo de até 15 dias úteis, a notificação do controlador aos titulares, contados a partir do momento em que ele efetivamente consegue chegar à conclusão de que: 1) O incidente envolve dados pessoais; 2) A organização noticiante é a controladora da respectiva base de dados pessoais objeto do incidente; e 3) A análise do score do incidente leve a conclusão de que há elevado risco ou dano aos titulares de dados. É importante que a comunicação seja realizada “o quanto antes” para que os titulares de dados, diante da relevância do evento, possam adotar as medidas que considerarem pertinente diante da ciência do ocorrido, porém, se houver justificativa do controlador, aqui o prazo seria maior diante da complexidade que há para se traçar a melhor estratégia para notificar os titulares, de acordo com o tipo de relação e de dados que há entre controlador e titulares.
QUESTÃO 8 - Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	A comunicação mais adequada é aquela que leva em consideração o tipo de relacionamento existente entre o controlador e o titular e as modalidades de comunicações prévias entre ambos. Outro critério que deve ser levado em consideração é o tipo de dado pessoal já existente no controlador quanto ao titular afetado para avaliar se seria possível uma comunicação individualizada ou não. Por vezes, o controlador pode não possuir uma base consistente de e-mails dos titulares, por exemplo. Portanto, em regra, o incidente deve ser comunicado diretamente aos titulares dos dados pessoais afetados, a menos que isso implique um esforço desproporcional. Nesse caso, pode haver uma

	comunicação pública ou medida semelhante em que os titulares sejam informados de forma igualmente eficaz (artigo 34(3)c do GDPR[18]). Exemplos de métodos de comunicação transparentes incluem mensagens diretas (como e-mail, SMS, mensagem direta), banners ou notificações em destaque no site, comunicações postais e anúncios importantes na mídia. Mas, novamente, o critério relevante será a relação entre controlador e titular e as modalidades de comunicações prévias já existentes, se assertivas. Os controladores, principalmente quando interagem com frequência com seus clientes, estão na melhor posição para determinar o canal de contato mais apropriado para comunicar um incidente a eles. Justamente por isso, o critério de escolha do canal utilizado deve ficar a critério do controlador. Em algumas hipóteses, porém, pode ser extremamente custoso ou até mesmo impossível realizar a notificação direta dos titulares afetados. Nesse sentido, o *Personal Information Protection and Electronic Documents Act*[19] estabelece as seguintes hipóteses em que a notificação indireta de titulares é permitida: a) a notificação direta provavelmente resultaria em maiores danos ao titular afetado; b) a notificação direta provavelmente seria excessivamente difícil para o controlador; e c) o controlador não possui meios adequados para entrar em contato com o titular.
QUESTÃO 9: Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	A obrigatoriedade de notificar um incidente à ANPD poderá ser excetuada sempre que o cálculo de risco adotado pelo controlador indicar a probabilidade de não haver risco ou dano aos titulares. Ainda, outros critérios podem ser extraídos do *Act on the Protection of Personal Information*[20] (APPI, Japão): a) quando os dados pessoais afetados possuírem criptografia de alto nível (com o sistema de criptografia em conformidade com a ISSO/IEC 18033, por exemplo, ou a chave de descriptografia é controlada remotamente);

[18] Disponível em: https://gdpr-info.eu/
[19] Disponível em: https://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html
[20] Disponível em: https://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf

	b) quando os dados pessoais forem recuperados pelo controlador antes de ser acessados por terceiros não autorizados; c) quando não existir risco de um titular específico ser identificado; d) quando o incidente seja flagrantemente insignificante (por exemplo, uma entrega incorreta de um pacote em que as informações pessoais estejam apenas na sua etiqueta de entrega).
QUESTÃO 10: Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	Para além das exceções da obrigatoriedade de informar à ANPD (que, por conseguinte, aplicam-se também ao dever de informar aos titulares), sugere-se as seguintes exceções, consonantes com o artigo 34(3) do GDPR:[21] a) quando existirem motivos razoáveis para o controlador crer que a notificação dos titulares poderá causar prejuízos a investigações em andamentos conduzidas pela força policial (em consonância também com a previsão da Consideranda 88 do GDPR e com o *Notification Data Breach Scheme* australiano); b) se o controlador agir rapidamente de modo a remediar o incidente e, como resultado, reduzir a possibilidade de que ele resulte em riscos ou danos para os titulares (previsão contida também na legislação japonesa[22]); c) o controlador utilizou medidas técnicas e organizacionais adequadas para proteger os dados pessoais antes da violação (em especial, medidas aptas a tornar os dados pessoais ininteligíveis para qualquer pessoa que não esteja autorizada a acessá-los); d) quando contatar os titulares requereria um esforço desproporcional, seja pela perda de informações de contato ocasionada pelo próprio incidente ou pela inexistência de tais informações; seja pela abrangência do incidente sobre um número extremamente elevado de titulares (aqui, deverá ser estabelecido critério objetivo pela ANPD para definição de uma exceção em virtude do número de indivíduos afetados).

[21] Disponível em: https://gdpr-info.eu/
[22] Disponível em: https://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf

QUESTÃO 11: Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	a) Cálculo de risco do incidente apresentado pelo controlador (incluindo-se os requisitos sugeridos previamente); b) Medidas de mitigação adotadas pelo controlador; c) Tempo de descoberta e resposta ao incidente; d) Nível de colaboração do controlador com a Autoridade e demais órgãos reguladores e/ou autoridades policiais; e) Justificativas do controlador para eventuais atrasos em notificações; f) Esforços adotados pelo controlador para informar e auxiliar os titulares afetados.
QUESTÃO 12: Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	*European Union Agency for Network and Information Security* (ENISA): Recommendations for a methodology of the assessment of severity of personal data breaches, 2013.[23] Para questões de volumetria, o Guia de Incidentes envolvendo Dados Pessoais da Autoridade Espanhola de Proteção de Dados[24]. **Critérios** - Os principais critérios levados em consideração ao avaliar a gravidade de uma violação de dados pessoais são: • Contexto de processamento de dados (DPC): aborda o tipo de dados violados, juntamente com um ou vários fatores ligados ao contexto geral de processamento. • Facilidade de Identificação (EI): Determina a facilidade com que a identidade dos indivíduos pode ser deduzida dos dados envolvidos na violação. • Circunstâncias de violação (CB): Aborda as circunstâncias específicas da violação, que são relacionadas ao tipo de violação, incluindo principalmente a perda de segurança dos dados violados, como bem como, qualquer intenção maliciosa envolvida. **Cálculo da gravidade** - Com base nos critérios acima, a abordagem desta metodologia é a seguinte:

[23] Disponível em: https://www.enisa.europa.eu/publications/dbn-severity
[24] Disponível em: https://www.aepd.es/sites/default/files/2019-09/Guide-on-personal-data-breach.pdf

	• DPC está no centro da metodologia e avalia a criticidade de um determinado conjunto de dados em um contexto de processamento específico. • EI é um fator de correção do DPC. A criticidade geral de um processamento de dados pode ser reduzida dependendo do valor de EI. Em outras palavras, quanto menor for a facilidade de identificação, menor se obtém na pontuação geral. Portanto, a combinação do EI e DPC (multiplicação) dá a pontuação inicial da gravidade (SE) da violação de dados. • CB quantifica as circunstâncias específicas da violação que podem estar presentes ou não em uma determinada situação. Portanto, quando presente, o CB só pode aumentar a gravidade de uma violação específica. Por esta razão a pontuação inicial pode ser ajustada posteriormente pelo CB. Assim, a pontuação final da avaliação da gravidade pode ser extraída usando a seguinte fórmula: pontuação inicial da gravidade (SE)> SE = DPC X EI + CB • Dessa forma, para que o controlador obtenha o resultado de gravidade, todos os três critérios devem ser pontuados. O resultado pertence a um determinado intervalo de valores que corresponde a um dos quatro níveis de gravidade: baixo, médio, alto e muito alto. No final da avaliação, outros critérios possivelmente relevantes (número de indivíduos e ininteligibilidade de dados) que não foram considerados na metodologia são avaliados e sinalizados para a autoridade competente, quando aplicável.
QUESTÃO 13: Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	As medidas segurança, boas práticas e de governança já existentes na LGPD, aplicáveis ao caso em concreto.
QUESTÃO 14: O operador pode notificar diretamente a ANPD ou o titular? Se sim, em quais circunstâncias?	Entendemos que não. O operador deve notificar o controlador, o quanto antes, sem demorar injustificada, bem como fornecer os insumos para que o controlador possa analisar o evento e eventualmente realizar a comunicação, se o caso. O GDPR estabelece o mesmo racional, qual seja, o de atribuir ao Controlador a obrigação de notificar a autoridade de proteção de dados, conforme Considerandas 85 ao 88.
Outras sugestões:	Independentemente da utilização de medidas técnicas e administrativas adotadas para proteger dados e prevenir incidentes, tanto pelo setor produtivo brasileiro, como também por órgãos da

	administração pública, acompanhamos no Brasil o triste avanço do comércio ilegal de dados sem a devida responsabilização criminal dos envolvidos. Assim, as organizações poderão continuar investindo fortemente em políticas e procedimentos de segurança, adotando medidas, de acordo com melhores práticas, para identificar fraudes e proteger dados pessoais. Porém, possivelmente continuarão sendo vítimas de eventos ilícitos pela complexidade inerente a desproporcionalidade do binômio segurança e exploração de vulnerabilidades, de tal sorte que é fundamental também uma forte e competente estrutura investigativa contra aqueles que realmente buscam falhas, obtêm eventuais dados ilicitamente e ainda os expõem e os comercializam, para que sejam devidamente identificados e punidos.
SUGESTÃO DE NORMATIVO, SE HOUVER	
Art. Xxxx	
Art. Xxxx	

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: Finep - Financiadora de Estudos e Projetos (Carla M. M. Urquidi)

CPF/CNPJ: 33.749.086/0001-09

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS **IMPORTANTE:** Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	
O que deve ser considerado na avaliação dos riscos do incidente?	
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	

Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	

Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	

SUGESTÃO DE NORMATIVO, SE HOUVER
ISO/IEC 27035-2:2016 - Information technology - Security techniques - Information security incident management - Part 2: Guidelines to plan and prepare for incident response (6.5. Incident classification scale, Annex C)
ISO/IEC 27035-3:2020 - Information technology - Security techniques - Information security incident management - Part 3: Guidelines for ICT incident response operations, (8. Incident notification operations, 12.3. How to stablish external reporting, if required)
ABNT NBR ISO/IEC 29134:2020 - Tecnologia da informação - Técnicas de segurança - Avaliação de impacto de privacidade – Diretrizes (Anexo A)
ABNT NBR ISO/IEC 29151:2020 - Tecnologia da informação - Técnicas de segurança - Código de prática para proteção de dados pessoais

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 02/2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: FEDERAÇÃO DAS INDÚSTRIAS DO RIO DE JANEIRO-FIRJAN

CPF/CNPJ: 42.422.212/0001-07

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS **IMPORTANTE:** Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	Observa-se o entendimento de que um incidente poderá acarretar "elevado risco ou dano relevante ao titular", quando englobar eventuais impactos, como perdas financeiras e/ou possibilidade de fraudes, advindas diretamente do incidente a ser reportado. Assim, para avaliar o risco ou dano relevante, sugere-se que sejam observados os critérios adotados pela *Opinion* 03/2014 do Grupo de Trabalho, do artigo 29, da União Europeia (Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf), no qual são considerados a natureza do dado pessoal, o tipo de incidente e se o controlador/operador responsável aplicou, preventivamente, medidas tecnológicas aptas à proteger a confidencialidade, integridade e disponibilidade dos dados pessoais afetados.
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	No moldes adotados pela *Opinion* 03/2014, do Grupo de Trabalho, do artigo 29 da União Europeia (Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf) e, prestigiando o princípio da equidade, verifica-se a necessidade de adotar diretrizes claras quanto as categorias de impacto, de forma a uniformizar os parâmetros dos relatórios de incidentes das empresas, os quais serão enviados à ANPD. Assim, conforme exemplificado na ISO 27005:2019 - Diretrizes da Gestão de Riscos de Segurança da Informação - a escala de medição deverá ser dividida com a finalidade de priorizar os riscos de maior impacto. Nesse primeiro momento, a divisão entre Baixo, Médio e Alto, apesar de simplificada, pode ser considerada mais assertiva na consolidação de informações basilares para o relatório de impacto de incidentes. Os níveis deverão ser medidos a partir da análise da natureza de dados envolvidos, reversibilidade de ações e volume de dados. Quanto aos riscos ou danos baixos poderão ser considerados não relevante, desde quando a reversibilidade de ações, quantidade e a natureza dos dados não forem significativos. Pois, o impacto nas violações de dados pessoais seria de baixa relevância para o titular de dados, e, portanto, não necessitariam ser reportados à ANPD ou aos titulares de dados pessoais. Contudo, a fim de permitir um controle por parte do controlador, sugere-se que os riscos baixos e não relevantes, sejam registrados internamente pelos controladores e/ou operadores responsáveis, pelo prazo de 5 anos, conforme sugestão de regulamentação ao final indicada.
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	Segundo o COSO ERM, Risco é o efeito da incerteza sobre os objetivos, e no caso específico do risco ao titular de dados, seria tudo que afasta o titular do seu direito à privacidade e à segurança de seus dados, no âmbito da Lei Geral de Proteção de Dados (LGPD). Já o dano ao titular seria a materialização do risco das naturezas citadas. Sendo assim, ambos estão

	diretamente relacionados, pois a ausência ou falha na identificação de vulnerabilidades e na realização de respostas adequadas ao risco, acarretarão prováveis danos ao titular. Assim, para distinguir o risco ao titular, do dano ao titular, devem ser observados os impactos decorrentes de tais danos, por meio de avaliação com a descrição de riscos e dos danos identificados, nos moldes da sugestão da legislação indicada abaixo.
O que deve ser considerado na avaliação dos riscos do incidente?	A avaliação dos riscos de incidente deve considerar a probabilidade de ocorrência, as medidas preventivas e mitigadoras aplicadas e o impacto do incidente aos direitos dos titulares de dados. Nesse sentido, conforme sugestão de regulamentação ao final indicada, sugere-se que sejam adotados 3 (três) níveis de critérios de impacto: Baixo – falha na gestão de dados pessoais (ie. coleta, armazenamento, tratamento, descarte) e/ou incidente, causando consequências pouco significativas ou reversíveis no curto prazo; Médio – incidentes ou utilização indevida de dados pessoais e/ou dados de crianças e adolescentes, causando impactos reversíveis no médio prazo, por conta dos controles utilizados e notoriedade dos dados vazados/utilizados; Alto – incidentes ou utilização indevida de dados pessoais sensíveis, dados pessoais e/ou dados de crianças e adolescentes, causando impactos irreversíveis ou de difícil reversão no longo prazo.
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	Para fins de uma melhor didática e objetividade, conforme sugestão de regulamentação ao final indicada, recomenda-se que além dos dados solicitados pelo §1º do art. 48, seja encaminhando à ANPD: (i) a descrição se a violação foi intencional ou não intencional, interna ou externa, de confidencialidade, disponibilidade ou integridade; (ii) a indicação do nome e dados de contato do encarregado (DPO) ou da pessoa indicada para prestação das informações complementares; (iii) a descrição das ações já tomadas ou propostas pelo controlador para abordar a violação de dados pessoais, incluindo, se for o caso, medidas para mitigar os possíveis efeitos adversos; (iv) e a descrição das recomendações e/ou acordos que os controladores efetuaram junto aos titulares de dados.
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	Conforme estudo realizado pela IBM Securiy (https://www.somaxi.com.br/post/brasil-%C3%A9-o-pa%C3%ADs-que-mais-tempo-leva-para-identificar-e-conter-incidentes-de-seguran%C3%A7a-diz-estudo), observa-se que o Brasil leva uma média de 380 dias para conseguir mitigar e conter uma violação de dados pessoais – 100 dias a mais que a média global. Cita-se também, as previsões expressas pela Autoridade de Controle da Irlanda, que prevê a possibilidade de complementação da notificação de incidente inicial, quando os dados solicitados se tornarem disponíveis, uma vez que algumas informações e questionamentos, só serão possíveis de serem respondidas após o término das investigações internas promovidas pelo controlador afetado (Vide: https://www.dataprotection.ie/en/organisations/know-your-obligations/breach-notification e https://www.dataprotection.ie/sites/default/files/uploads/2019-08/190812%20GDPR%20Breach%20Notification%20Quick%20Guide.pdf). Assim, (i) considerando a GDPR, bem como outros prazos legais nacionais que observam a partilha de prazos, com prazo inicial para informação e prazo maior para levantamento das informações; (ii) considerando que a LGPD já traz os itens mínimos que precisam ser encaminhados na notificação; e (iii) considerando que o ordenamento jurídico nacional se baseia em dias úteis, sugere-se, conforme já orientado pela ANPD de forma temporária, o prazo inicial mínimo de 2 (dois) dias úteis para a notificação de incidente à ANPD e, caso necessário, mais 10 (dez) dias úteis para complementação, contados a partir da data do conhecimento do incidente, ou prazo maior suplementar, mediante justificativa encaminhada no prazo dos 10 (dez) dias, conforme sugestão de regulamentação abaixo indicada.

Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	De forma a evitar uma divulgação infundada e imprecisa, recomenda-se que a notificação aos titulares de dados envolvidos seja realizada, tão somente, após a devida confirmação de que os dados pessoais do referido titular foram afetados no incidente. Assim, conforme sugestão de regulamentação abaixo indicada, verifica-se a pertinência da observância do prazo de até 2 (dois) dias úteis para tal notificação. Ademais, verifica ser oportuno, que nessa notificação também sejam incluídas as recomendações ao titular quanto à manutenção de seus dados na base (ex. troca de senha), com objetivo de mitigar prováveis efeitos adversos, ampliando as medidas de segurança por todos os envolvidos.
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	Recomenda-se que a notificação seja efetuada – em regra – diretamente aos titulares de dados envolvidos no incidente, por meio dos contatos diretos que o controlador possua, os quais possam ser registrados (como exemplo: e-mail, cartas ou comunicações gravadas). Contudo, observa-se que em alguns casos, mesmo tendo uma relação contratual direta com o usuário final, o controlador não possui detalhes suficientes dos dados de contato do titular afetado, não sendo capaz de garantir assim, a notificação adequada aos mesmos. Nesses casos, recomenda-se que seja possível efetuar notificação geral, por meio de anúncios em mídias, conforme sugestão de regulamentação abaixo indicada.
Quais seriam as eventuais **exceções** da obrigatoriedade de informar a ANPD?	Sugere-se que a ANPD, apenas receba notificações referente aos incidentes de segurança da informação, vinculados aos dados pessoais, que envolvam riscos médios e altos aos dados e que possam resultar em médio ou grave prejuízo aos titulares. Assim, entende-se pela desnecessidade de informar a ANPD nos casos: (i) em que a violação de segurança não for uma violação de dados pessoais; (ii) em que a violação de dados pessoais não afete negativamente a privacidade do titular de dados envolvido, de acordo com os resultados de uma avaliação de gravidade, a ser produzida pelo controlador na análise do risco; (iii) em que a violação ocorra internamente na empresa controladora, sem exposição externa dos dados pessoais envolvidos; ou (iv) quando o controlador tiver implementado medidas de proteção técnicas e organizacionais aptas a tornar os dados pessoais afetados ininteligíveis para qualquer pessoa que não esteja autorizada a acessá-los, como por exemplo por meio da adoção de criptografia, conforme recomendações da Autoridade Irlandesa e conforme, art. 48, §3º da LGPD. Tais pontos podem ser observados na sugestão de regulamentação abaixo indicada.
Quais seriam as possíveis **exceções** da obrigatoriedade de informar os titulares?	Sugere-se que o titular de dados seja notificado, apenas quando a violação possa acarretar elevado dano aos seus direitos ou grave prejuízo a sua esfera pessoal. Assim, entende-se pela não obrigatoriedade de informar ao titular de dados, nos seguintes casos: (i) quando a violação de segurança não for uma violação de dados pessoais; (ii) quando a violação de dados pessoais não afetar negativamente os direitos e liberdades do titular de dados envolvido (conforme https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca); e (iii) sempre que o controlador tiver implementado medidas de proteção técnicas e organizacionais aptas a tornar os dados pessoais afetados ininteligíveis para qualquer pessoa que não esteja autorizada a acessá-los, como por exemplo por meio da adoção de criptografia, conforme recomendações da Autoridade Irlandesa e conforme, art. 48, §3º da LGPD, ou quando se os dados envolvidos já sejam públicos por natureza.

	Nos moldes previstos na recomendação da Autoridade Irlandesa sobre violações de dados pessoais no âmbito do GDPR (Vide: https://www.dataprotection.ie/sites/default/files/uploads/2019-10/Data%20Breach%20Notification_Practical%20Guidance_Oct19.pdf e https://www.dataprotection.ie/sites/default/files/uploads/2019-08/190812%20GDPR%20Breach%20Notification%20Quick%20Guide.pdf), entende-se pela desnecessidade da comunicação quando for atendida uma das seguintes condições: (i) o controlador tiver implementado medidas de proteção técnicas e organizacionais aptas a tornar os dados pessoais afetados ininteligíveis para qualquer pessoa que não esteja autorizada a acessá-los, como por exemplo por meio da adoção de criptografia; (ii) ou o controlador tenha adotado medidas subsequentes que garantam que o alto risco para os direitos e liberdades dos titulares de dados não são mais propensos a se materializar; (iii) ou envolveria esforço desproporcional. Dessa forma, sugere-se que sejam abordadas as circunstâncias em que os controladores podem ser dispensados da comunicação obrigatória de incidente aos titulares de dados, mesmo quando a violação vier a resultar em alto risco para os direitos e liberdades do titular, tendo em vista os esforços desproporcionais ou a ineficácia da comunicação. Nesse último caso, no entanto, recomenda-se que seja determinado aos controladores de dados que efetuem uma comunicação pública aos titulares de dados, informando o incidente e as medidas que foram aplicadas, conforme sugestão de regulamentação abaixo indicada.
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	Na análise da gravidade do incidente de segurança envolvendo dados pessoais, conforme sugestão de regulamentação abaixo indicada, devem ser considerados pela ANPD: (i) a natureza dos dados pessoais; (ii) as circunstâncias da violação; (iii) se os dados pessoais foram ou não protegidos por técnicas e medidas apropriadas, como criptografia ou pseudoanonimizacão; (iv) a facilidade de identificação direta ou indireta dos titulares afetados; (v) a probabilidade de reversão da pseudoanonimização ou a perda de confidencialidade; (vi) a probabilidade de fraude de identidade, perda financeira ou outras formas de uso indevido dos dados afetados; (vii) a probabilidade da violação resultar em discriminação, danos à reputação ou a outros direitos fundamentais do titular de dados; (viii) se o controlador efetuou a avaliação de risco; e (ix) se o controlador efetuou acordo com os titulares de dados afetados.
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	Com relação a metodologia aplicável ao questionamento, poderá ser utilizada a ABNT NBR ISO 27035:2016, a qual menciona que a gestão de incidente de segurança da informação é o processo de detectar, reportar, avaliar, responder, tratar e aprender sobre os incidentes. Sendo as normas aplicáveis à análise de gravidade de incidentes, a norma supracitada e a ISO 27005:2019, que pondera sobre as Diretrizes da Gestão de Riscos de Segurança da Informação, como por exemplo, em seu anexo B-Item B.2 Valoração de Ativos- Subitem B.2.4 – Escala de Medição, que aborda sobre os níveis de escala que podem ser adotados com a finalidade de medir o nível de riscos (ex: Baixo, Médio e Alto). Assim, tendo por base a norma técnica referenciada acima, elaborou-se a metodologia para análise de riscos, conforme exposta na sugestão de regulamentação abaixo indicada.
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem	Tendo como base o Guia de Notificação de Incidentes elaborado pela autoridade de dados Irlandesa, (Vide: https://www.dataprotection.ie/sites/default/files/uploads/2019-10/Data%20Breach%20Notification_Practical%20Guidance_Oct19.pdf), para efeito do questionado, sugere-se que a ANPD possa recomendar diligências internas ao

determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	controlador, bem como o monitoramento de eventuais efeitos adversos oriundos do incidente relatado ou investigado, nos moldes da sugestão de regulamentação abaixo indicada.

SUGESTÃO DE NORMATIVO, SE HOUVER

Art. 1º Este regulamento, a fim de conferir tratamento isonômico aos agentes de tratamento de dados pessoais, dispõe sobre as condições de exercício da obrigação administrativa de efetuar Notificação de Incidente, prevista no art. 48 e seguintes da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD).

Art. 2º Entende-se por incidente de dados pessoais uma violação de segurança da informação, acidental ou intencional, interna ou externa, que resulte em destruição, perda, alteração, divulgação não autorizada ou acesso a qualquer informação relativa ou relacionada a um indivíduo identificado ou identificável.

Art. 3º Compete ao controlador efetuar a avaliação da relevância do risco ou dano do incidente ocorrido, a fim de determinar a necessidade de notificar a ANPD e/ou aos titulares de dados pessoais, classificando-os no mínimo em um dos 3 (três) níveis de impacto:

I - Baixo - falha na gestão de dados Pessoais (i.e. coleta, armazenamento, tratamento, descarte) e/ou incidente, causando consequências pouco significativas ou reversíveis no curto prazo;

II - Médio – incidentes ou utilização indevida de dados pessoais e/ou dados de crianças e adolescentes, causando impactos reversíveis no médio prazo por conta dos controles utilizados e notoriedade dos dados vazados/utilizados;

III - Alto - incidentes ou utilização indevida de dados pessoais sensíveis, dados pessoais e/ou dados de crianças e adolescentes, causando impactos irreversíveis ou de difícil reversão no longo prazo.

Parágrafo único. Os incidentes que englobam impactos com perdas financeiras e/ou possibilidade de fraudes aos titulares de dados pessoais, sempre serão considerados de alto risco ou dano relevante.

Art. 4º Na avaliação do incidente de dados pessoais, o controlador deverá considerar os critérios na determinação do risco e a verificação dos danos aos direitos e liberdades dos titulares dos dados, incluindo:

I - a natureza do dado pessoal;

II - o tipo de incidente;

III - o volume de dados pessoais envolvidos;

IV - os riscos potenciais decorrentes do incidente;

V - os danos potenciais ou efetivos decorrentes do incidente e o impacto aos titulares de dados;

VI - as ações já implementadas e as possibilidades de mitigar os danos causados.

§1º A avaliação da relevância do risco e/ou dano deverá considerar se, o controlador/operador responsável aplicou preventivamente medidas tecnológicas aptas a proteger a confidencialidade, integridade e disponibilidade dos dados pessoais afetados, e deverá considerar a natureza e a probabilidade de ocorrência de danos secundários.

§2º Os controladores devem dar ênfase especial, em considerar se os dados pessoais afetados são suscetíveis de serem usados de forma maliciosa por terceiros, em prejuízo aos titulares de dados.

§3º Se, após a avaliação de risco, com a devida aplicação de ações mitigadoras, o controlador de dados concluir que a violação seria improvável de resultar em um risco para os direitos e liberdades dos titulares de dados envolvidos, o controlador não será obrigado a notificar a ANPD.

§4º Em caso de dúvida, o controlador pode submeter a ANPD a avaliação de risco elaborada para chancela e/ou adequação.

Art. 5º Nos casos em que o incidente resultar em alto ou médio risco ou dano relevante aos direitos dos titulares, a ANPD deverá ser notificada no prazo de até 2 (dois) dias úteis, a contar da ciência do fato pelo controlador, com possibilidade de complementação das informações levantadas, em até 10 (dez) dias úteis.

§1º A notificação deverá informar, além do exigido no §1º do art. 48 da LGPD, os seguintes dados:

I- descrição se a violação foi intencional ou não intencional, interna ou externa, de confidencialidade, disponibilidade ou integridade;

II- indicação do nome e dados de contato do encarregado (DPO) ou da pessoa indicada para prestação das informações complementares;

III- descrição das ações realizadas e/ou das propostas de ação a serem tomadas pelo controlador para abortar a violação de dados pessoais, incluindo, se for o caso, medidas para mitigar os possíveis efeitos adversos;

IV- descrição das recomendações e/ou acordos que os controladores efetuaram junto aos titulares de dados, na forma do § 7º do art. 52 da LGPD.

§2º Caso necessário, e desde que justificado, o controlador poderá solicitar à ANPD prazo suplementar para o cumprimento das informações acima exigidas.

Art. 6º A notificação à ANPD não será obrigatória nos seguintes casos:

I- quando o incidente for de menor risco/ baixa relevância; e/ou
II- quando a violação não afetar negativamente a privacidade do titular de dados envolvido; e/ou
III- quando a violação ocorrer internamente no controlador ou grupo de controle, sem exposição externa dos dados pessoais envolvidos; e/ou
IV- quando o controlador tiver implementado medidas de proteção técnicas e organizacionais aptas a tornar os dados pessoais afetados ininteligíveis para qualquer pessoa que não esteja autorizada a acessá-los.

Art. 7º Nos casos em que o incidente resultar em alto ou médio risco ou dano relevante, o controlador deverá comunicar a violação diretamente aos titulares dos dados, fornecendo, em linguagem clara e simples, as ações mitigadoras já realizadas e as recomendações relevantes para que os titulares possam agir a fim de mitigar potenciais efeitos adversos da violação.

§1º A comunicação deverá ser efetuada em até 2 (dois) dias úteis, após a confirmação que o titular a ser notificado teve seus dados pessoas comprometidos no incidente previamente noticiado à ANPD.

§2º A comunicação deverá incluir ao menos as seguintes informações:

I - descrição das prováveis consequências da violação de dados pessoais;

II - descrição das medidas tomadas ou propostas a serem tomadas pelo controlador para abordar a violação de dados pessoais, incluindo, se for o caso, medidas para mitigar seus possíveis efeitos adversos;

III - o nome e os detalhes de contato do encarregado pela proteção de dados ou outro ponto de contato onde mais informações poderão ser obtidas pelos titulares.

§3º Os titulares que não tiverem seus dados envolvidos no incidente não necessitam ser comunicados.

§4º Caso não seja possível verificar uma relação contratual direta com o usuário final, e/ou o controlador ou operador afetado pelo incidente não possua detalhes suficientes para garantir a notificação adequada aos titulares de dados envolvidos, deverá ser realizada notificação geral, por meio de anúncios em mídias e/ou jornais de grande circulação.

Art. 8º Nos casos em que o incidente for de menor risco, cuja violação de segurança não for uma violação de dados pessoais; e/ou não afete negativamente os direitos e liberdades do titular de dados; e/ou que o controlador tiver demonstrado na Notificação de Incidente à ANPD, a satisfação desta, na implementação das medidas adequadas de proteção tecnológica aos dados envolvidos pela violação de segurança; e/ou quando os dados envolvidos sejam públicos por natureza, não será obrigatória a comunicação ao titular de dados.

§1º A comunicação ao titular de dados não será obrigatória, mesmo quando a violação resultar em alto risco aos direitos e liberdades do mesmo, quando estiverem presentes as seguintes condições:

I - o controlador tiver implementado adequadamente medidas técnicas e organizacionais de proteção aos dados pessoais afetados pela violação, que os tornam ininteligível para qualquer pessoa que não esteja autorizada a acessá-los, como por exemplo adoção de técnicas de criptografia; e/ou

II - o controlador tiver adotado medidas subsequentes que garantam que o alto risco para os direitos e liberdades dos titulares de dados não são mais propensos a se materializar; ou envolveria esforço desproporcional.

§2º Caso o nível de disponibilidade ou publicidade dos dados seja alterado pela violação, esta deverá ser considerada como uma violação de confidencialidade e, caso tenha alta probabilidade de afetar negativamente os direitos dos titulares de dados pessoais, deverá ser notificada.

Art. 9º Todas as violações e incidentes envolvendo dados pessoais – mesmo aquelas que não são obrigatórias a comunicação à ANPD e/ou ao titular de dados pessoais – devem ser registradas e monitoradas pelo controlador pelo prazo de 5 anos, para fins de fiscalização da ANPD.

Parágrafo único. O registro deverá conter ao menos a descrição detalhada da violação, avaliação dos impactos aos titulares de dados, e as respostas e medidas adotadas.

Art. 10. A ANPD, após o recebimento da notificação do controlador, deverá instaurar processo administrativo nos termos da Lei nº 9.784, de 29 de janeiro de 1999, que regula o processo administrativo no âmbito da Administração Pública Federal, para apuração da gravidade do incidente reportado e/ou investigado, bem como aplicação das sanções cabíveis, considerando os seguintes critérios:

I- natureza dos dados pessoais envolvidos no incidente;
II- circunstâncias que resultaram na violação de dados pessoais;
III- se os dados afetados foram ou não protegidos preventivamente por técnicas e medidas apropriadas de proteção, como criptografia e pseudoanonimização;
IV- facilidade de identificação direta ou indireta dos titulares de dados afetados;
V- probabilidade de reversão da pseudoanonimização ou perda da confidencialidade;
VI- probabilidade de fraude de identidade, perda financeira ou outras formas de uso indevido dos dados afetados;
VII- probabilidade de que a violação poderá resultar em discriminação, dano à reputação ou a outros direitos fundamentais do titular de dados;
VIII- se o controlador efetuou a avaliação de risco conforme os critérios do art. 4º deste regulamento;
IX- o fato do controlador ter efetuado acordo com os titulares de dados afetados.

Art. 11. A ANPD, no âmbito do processo administrativo instaurado, poderá recomendar que o controlador adote rotina de verificação dos incidentes de violação informados, especialmente onde for identificado potencial uso malicioso dos dados afetados.

Art. 12. A ANPD poderá emitir atos declaratórios para esclarecer eventuais dúvidas decorrentes da interpretação dos artigos que compõe este regulamento.

Art. 13. Este regulamento entra em vigor 45 dias após sua publicação.

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: FUNDAÇÃO SÃO FRANCISCO XAVIER

CPF/CNPJ: 19.878.404/0001-00

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS **IMPORTANTE:** Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	1) Quando provocar exposição/acesso indevido aos dados confidenciais/críticos ou sensíveis relacionadas ao titular. Exemplo: Dados de cartão de crédito/débito, senhas, dados de saúde, fotos/imagens que não haviam sido divulgadas publicamente ou dados discriminatórios 2) Levar em consideração: a volumetria de titulares afetados, se foram dados sensíveis, dados de vulneráveis, com transferência internacional, dados de geolocalização. Quando houver possibilidade de ocasionar danos materiais, morais, discriminatórios, violação do direito a imagem e à reputação, fraudes financeiras e roubo de identidade.
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	1) Sim, sugestão para a classificação de Risco: Muito Alto, Alto, Médio e Baixo para os processos envolvendo dados pessoais. 2) A classificação dos riscos poderia ser medida através de uma matriz, que utilize como cálculo: Impacto x Probabilidade. IMPACTO: natureza do dado (simples; crítico; sensível), formato do dado (físico; digital), tipo de dados (estruturado; não estruturado), titularidade (cliente; funcionário; terceiro; fornecedor), volumetria (1-200;201-1000;1001 acima). Multiplicar os valores. PROBABILIDADE: controles de armazenamento/transferência (Seguro sem riscos; Seguro com pouco risco; Critérios de segurança razoáveis; Boas práticas porém vulnerável; Vulnerável), frequência do tratamento (anual; semestral; mensal; semanal; diário; sob demanda). Multiplicar os valores. 3) Riscos a serem considerados Relevantes: Muito Alto e Alto.
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	1) RISCO: Probabilidade de um agente de ameaça tirar proveito de uma vulnerabilidade causando o dano/impacto. DANO/IMPACTO: Consequências que podem resultar para o titular se o risco se materializar.

	2) O Risco está associado á possibilidade de um evento comprometer por ex: a Segurança da Informação, o Dano é um evento que se concretizou e causou alguma perda financeira, de imagem, e de integridade ao titular de dados, violou sua privacidade. Um risco vincula a vulnerabilidade, ameaça e a probabilidade de impacto aos negócios e as pessoas envolvidas.
O que deve ser considerado na avaliação dos riscos do incidente?	1) Categoria de titulares envolvidos. Quantidade de titulares envolvidos. de titulares envolvidos. Ativos de informação envolvidos, as ameaças e vulnerabilidades que estes ativos estão expostos, assim como ferramentas e processos para tratativa dos mesmos. Nivel de classificação da Informação envolvida: Ex.: Restrita, Confidencial, Uso Interno, Pública. Nível de segurança do ativo envolvido - existência de: Firewall, Antivírus, DLP (Data Loss Protection), proteções físicas e tecnológicas, controles de acesso. Probabilidade de ocorrência de eventos e nível de impacto
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	1) Data/Hora da detecção do incidente Tipo de problema envolvido: < Envio / Compartilhamento/ Acesso indevido / Uso não autorizado / Ataque / Invasão / Vazamento > Grupo de ciência do incidente: <Presidencia / Diretoria / Gestores / Área envolvida / TI> Ação técnica em andamento: <Descreva alguma ação técnica emergencial que possa evitar maior dano ao titular> Ação administrativa em andamento:<Descreva alguma ação administrativa emergencial que possa evitar maior dano ao titular> Informação e dados de contato do encarregado/DPO.
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	1) 72 horas a partir da ciência do incidente, visando a investigação e tomada de decisão na mitigação dos riscos e para receber orientações/avaliação da ANPD.
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	1) Até 10 dias a partir da ciência do incidente, ou imediatamente após o ordenamento pela ANPD. Caso a divulgação precoce de informações não dificulte desnecessariamente a investigação das circunstâncias da violação (Ref.: GDPR – Considerando 88). 2) Sim. Deve se manter as informações de acordo com o Art. 48

Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	1) A comunicação poderia ocorrer através site da organização se for algo que envolva todo público que utiliza este meio. Através de um portal de atendimento ao titular dependendo da categoria de titulares envolvidos. Se for uma volumetria pequena e exista a informação de email dos titulares envolvidos, poderia ser através do envio de um email direcionado. 2) A comunicação pública poderia ocorrer de acordo com o tipo de dados envolvidos, o tipo de titular e a volumetria (ex: O incidente envolve mais de 70% dos titulares cadastrados), de forma que não provoque pânico e preocupação de titulares que não estão envolvidos no incidente.
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	1) Quando o incidente não provocar risco ou danos relevantes aos titulares (Risco Médio ou Baixo) ou a volumetria de titulares envolvidos for menor que 100.
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	1) Quando o incidente não provocar risco ou danos relevantes aos titulares (Risco Médio ou Baixo) ou a volumetria de titulares envolvidos for menor que 1.000.
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	1) Origem da ameaça (Hacker/Cracker, Criminoso Digital, Terrorista, Espionagem, Pessoa Interno). Ref.: NBRISO/IEC27005 FL55,FL56. 2) Envolvimento de dados identificados de doenças dos titulares (CID) no incidente. 3) Envolvimento de mais que 1.000 titulares. 4) Envolvimento de dados identificados de menores de 12 anos. 5) Evidência de prejuízo financeiro ou de imagem aos titulares. 6) Evidência de dano legal aos titulares. 7) Levar em consideração o conjunto de requisitos para atendimento às diretrizes, políticas e objetivos, o nível de maturidade em proteção de dados da organização (Existência de Política de Privacidade e de Segurança da Informação (SI), Programa de Governança e Privacidade de Dados implantado e divulgado. Existência e divulgação da figura do DPO. Evidência de treinamento e capacitação sobre Privacidade e SI aos funcionários da organização. Existência de procedimentos internos de Segurança da Informação: Classificação da Informação, Uso de dispositivos tecnológicos. Existência de acordos de confidencialidade de funcionários e parceiros de negócio. Existência de um Plano de Contingência D/R. Acordos contratuais com cláusulas de privacidade). 8) Existência do Mapeamento de Dados da organização. 9) Existência de Relatórios de Impacto dos processos críticos da organização (Risco Muito Alto e Alto) 10) Os processos de tratamento de dados pessoais adotados pela organização.

Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	1) Família NBRISO/IEC27000. 2) FMEA – Análise dos Modos de Falha e Efeito. **G x O x D = RPN.** **Gravidade** do problema (G): no qual 1 é "nunca" e 10 é "sempre". Probabilidade de **ocorrência** (O): no qual 1 é "nunca" e 10 é "sempre". Probabilidade de **detecção** da falha (D): começa no qual 10 é "nunca" e 1 é "sempre" 3) Plano de Continuidade de Negócio. Podem ser utilizado o PDCA, controles da ISO27001 (Gestão de Incidentes SI) / ISO 31000 (Gestão de Riscos).
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	1) Portal para registro dos incidentes. Com possibilidade de incluir atualizações até o encerramento do mesmo. 2) Canal de comunicação para solução de dúvidas. 3) Checklist das principais ações de governança de dados e privacidade que o controlador deveria cumprir. 4) Modelos de comunicação e guia de orientação para os controladores se comunicarem os titulares sobre os incidentes.
SUGESTÃO DE NORMATIVO, SE HOUVER	
Art. Xxxx	
Art. Xxxx	

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: FUNDAÇÃO DE ESTUDOS DAS DOENÇAS DO FÍGADO KOUTOULAS RIBEIRO - FUNEF

CPF/CNPJ:81.190.449/0001-61

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS **IMPORTANTE:** Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	**Sim. A distinção dos riscos poderia ser feita através do uso da ferramenta de Análise de Modo e efeito de falha (FMEA), que possui escalas de Severidade, Probabilidade e Detecção. Risco Alto (Prioridade 0), Risco Médio (Prioridade 1) e Risco Baixo (Prioridade 2).** **Risco ou dano baixo deve ser considerado RELEVANTE, pois se não tratado ele pode vir a se tornar um risco ou dano médio/alto. Os riscos, no entanto, devem ser tratados proativamente (Gestão proativa) enquanto os danos são tratados de forma reativa (Gestão Reativa).**
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	**Risco é a probabilidade de um evento ocorrer e devem ser tratados na Gestão de riscos Proativa (Ex. FMEA)** **Dano é quando o titular dos dados já foi lesado, ou seja, o incidente já ocorreu e a partir daí irá se buscar as causas e estabelecer plano de ação para que tal evento não ocorra novamente.** **Relação entre conceitos: Fazer o Gerenciamento dos riscos para que os mesmos sejam minimizados e consequentemente os danos sejam evitados.**

O que deve ser considerado na avaliação dos riscos do incidente?	**Severidade, Probabilidade e Detecção**
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de	

segurança? (art. 48, §2º)	
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	
SUGESTÃO DE NORMATIVO, SE HOUVER	
Art. Xxxx	
Art. Xxxx	

ANPD Autoridade Nacional de Proteção de Dados

CONTRIBUIÇÃO REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO: GARDEMANN & VIDOTTI ADVOGADOS ASSOSCIADOS

CNPJ: 32.531.243/0001-42

INTRODUÇÃO

O Gardemann & Vidotti Advogados Associados é um escritório de advocacia, fundado no ano de 2017, voltado para as necessidades do setor empresarial, especialmente o de telecomunicações, com visão inovadora, proativa, dinâmica, eficiente e, principalmente, focada em resultado.

Dedicamos nossos esforços em medidas preventivas e consultivas ao setor empresarial, principalmente o de telecomunicações, a fim de regularizar essas empresas nas mais variadas frentes.

Diante da entrada em vigor da Lei Geral de Proteção de Dados Pessoais – LGPD, nosso corpo técnico vem se empenhando em atender nossos clientes, cujas as dúvidas em relação a nova lei não são poucas.

Em regra, nosso público são empresas de pequeno a médio porte que, pela primeira vez, estão buscando implantar medidas de segurança da informação em seus processos, e mais especificamente, em relação ao tratamento de dados pessoais.

É indiscutível que no Brasil muitas são as empresas familiares e muitas são as empresas que nascem dentro de um cenário de informalidade, sendo esta a realidade da maioria das pequenas empresas em nosso país. O que nos faz refletir que a proteção de dados e, até mesmo, a segurança da informação, na maioria das vezes, não fazem parte dos valores da empresa brasileira.

Assim sendo, a conscientização dessas pequenas empresas vem sendo um grande desafio, cujos percalços vão desde o entendimento do conceito de tratamento de dados pessoais até a implantação de mecanismos mitigadores de riscos aos direitos dos titulares de dados.

Diante desse cenário, não poderia o Gardemann & Vidotti se manter omisso em um momento em que a ANPD busca construir argamasso regulatório compatível com os interesses dos setores empresariais, sociedade civil, setor acadêmico e Governo. Por estas razões, vem, respeitosamente,

à presença da ANPD apresentar contribuição a Tomada de Subsídios nº 2/2021 e se colocar à disposição desta Autoridade Nacional para eventuais contribuições no que for preciso.

CONTRIBUIÇÕES RECEBIDAS

IMPORTANTE: Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.

TÓPICO/QUESTÃO	CONTRIBUIÇÃO/INSTITUIÇÃO
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	Abre-se esta Contribuição informando que as sugestões aqui trazidas foram inspiradas nas Orientações Sobre A Notificação de Uma Violação de Dados Pessoais ao Abrigo do Regulamento (EU) 2016/679, documento elaborado pelo Grupo de Trabalho do Artigo 29 Para A Proteção de Dados. Como é de conhecimento, O Grupo de Trabalho do Artigo 29.º (GT Art. 29.º) é um órgão consultivo europeu independente que lidou com as questões relacionadas com a proteção de dados pessoais e da privacidade até 25 de maio de 2018 (data de aplicação do RGPD). Feitas essas considerações, passa-se a expor: Primeiramente, defende-se a adoção de documento específico de Avaliação de Risco ou Dano Relevante como mecanismo apto para verificar se um incidente pode acarretar risco ou dano relevante ao titular. A análise deve ter por princípio que risco relevante é aquele decorrente de violação suscetível de afetar direitos e liberdades do titular de dados, podendo resultar em danos materiais, físicos ou imateriais, tais como perda de controle sobre seus dados, limitação de direitos, discriminação, roubo ou usurpação da identidade, perdas financeiras, danos para reputação, entre outros. Dessa maneira mediante a Avaliação de Risco ou Dano Relevante, será possível calcular a probabilidade do incidente resultar em dano material, físico ou moral ao titular de dados. Sugere-se que os critérios a serem considerados pela ANPD sigam o padrão apontado pelo GT29, sendo indispensável ponderar: (i) o tipo da violação; (ii) Natureza, sensibilidade e volume dos dados pessoais; (iii) Facilidade de identificação de pessoas singulares; (iv) Gravidade das consequências para as pessoas; (v) Características especiais das pessoas singulares; (vi) Características especiais do responsável pelo tratamento de

	dados; (vii) Número de pessoas afetadas; (viii) combinação da gravidade do impacto potencial sobre os direitos e liberdades das pessoas e da probabilidade de este ocorrer.
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	Inspirando-se na União Europeia, acredita-se que é necessário que a classificação do risco tenha por base, principalmente, a probabilidade de um efeito negativo ocorrer diante de um incidente. Ou seja, deverá ser notificado a ocorrência de um incidente à ANPD quando houver chances consideráveis (risco relevante) de efeitos colaterais aos direitos e liberdades dos titulares de dados ocorrerem. Por sua vez, a gravidade do dano terá importante papel na avaliação, devendo ser adotada como um dos critérios dessa, haja vista que, dependendo da natureza dos dados pessoais afetados em uma violação (por exemplo dados sensíveis, bancários, etc), o dano poderá ser particularmente severo, é o caso de roubo, usurpação de identidade, entre outros. No que diz respeito a uma possível divisão em categorias de risco e dano como baixo, médio ou alto, entende-se que esta classificação é de difícil mensuração quando analisada sob o prisma de um único aspecto. Assim como, defende-se que tal classificação não deveria ser trazida de forma expressa pela regulamentação, haja vista que diversos fatores podem influenciar o nível de severidade de um dano, assim como, a probabilidade mais baixa ou mais alta de sua concretização (risco). Ademais, qualquer apontamento do que seria risco ou dano baixo, médio ou alto na regulação pode ser objeto de insegurança jurídica para os titulares de dados, visto que pode subestimar um dano concreto. Assim sendo, defende-se, mais uma vez, que seja feita uma Análise de Risco ou Dano Relevante e que esta seja fundamentada em diversos critérios, ao ponto que, se o responsável pelo tratamento, para facilitar o entendimento, fizer a classificação do risco ou dano pela subdivisão "baixo, médio, o alto" que este não seja o ponto central da validação da necessidade ou não de comunicação do incidente à ANPD e titulares, mas apenas metodologia de estudo. A conclusão pela necessidade ou não da comunicação à ANPD e titulares afetados de incidente, claramente necessita ser pautada nos critérios apontados nesta contribuição e sempre cruzando a probabilidade da ocorrência de um dano e a severidade desse dano aos direitos e liberdades dos titulares.
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	Risco ao titular diz respeito a probabilidade de um efeito colateral ocorrer diante de um incidente. Por sua vez, o dano constitui o efeito colateral em si, ou seja, a consequência negativa que poderá acontecer em virtude do incidente.
O que deve ser considerado na avaliação dos riscos do incidente?	Conforme anteriormente mencionado, sugere-se que os critérios a serem considerados pela ANPD sigam o padrão apontado pelo GT29, sendo indispensável ponderar: (i) o tipo da violação; (ii) Natureza, sensibilidade e volume dos dados pessoais; (iii) Facilidade de identificação de pessoas singulares; (iv) Gravidade das consequências para as pessoas; (v) Características especiais das pessoas singulares; (vi) Características

	especiais do responsável pelo tratamento de dados; (vii) Número de pessoas afetadas; (viii) combinação da gravidade do impacto potencial sobre os direitos e liberdades das pessoas e da probabilidade de este ocorrer.
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	A Notificação à ANPD deverá, no mínimo: a) Descrever a natureza da violação dos dados pessoais incluindo, se possível, as categorias e o número aproximado de titulares de dados afetados, bem como as categorias e o número aproximado de registos de dados pessoais em causa; b) Comunicar o nome e os contatos do encarregado da proteção de dados ou de outro ponto de contato onde possam ser obtidas mais informações; c) Descrever as consequências prováveis da violação de dados pessoais; d) Descrever as medidas adotadas ou propostas pelo responsável pelo tratamento para reparar a violação de dados pessoais, inclusive, se for caso disso, medidas para atenuar os seus eventuais efeitos negativos.
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	Embora a ANPD já tenha sugerido o prazo de 02 dias para comunicação, acredita-se que o mais razoável seria que se estabelecesse ao menos 05 (cinco) dias úteis para tanto. Caso não seja este o entendimento da ANPD, sugere-se que seja oportunizado ao responsável pelo tratamento o envio parcial de informações à ANPD, de modo que, caso o responsável precise de tempo superior para levantamento de maiores informações sobre o incidente, que possa submeter tais informações mediante comunicações complementares.
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	Na mesma linha da resposta anterior, acredita-se que seria interessante ao menos 05 (cinco) dias úteis para tanto. Com relação ao conteúdo da informação ao titular de dados, é importante que a comunicação conste ao menos: • uma descrição da natureza da violação; • o nome e os contatos do encarregado da proteção de dados ou de outro ponto de contato; • uma descrição das consequências prováveis da violação; e • uma descrição das medidas adotadas ou propostas pelo responsável pelo tratamento para reparar a violação, incluindo, se for caso disso, medidas para atenuar os seus eventuais efeitos negativos.
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em	Em princípio, a violação relevante deve ser comunicada diretamente aos titulares de dados afetados, a menos que isso implique um esforço desproporcional, ou seja, o caso de número significante de pessoas afetadas por exemplo. Nesse caso, deve ser feita uma comunicação pública ou tomada uma medida semelhante através da qual os titulares dos dados sejam informados de forma igualmente eficaz.

determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	Ainda, importante se faz pontuar que em qualquer das situações, seja por comunicação individualizada, seja por comunicação pública, devem ser utilizadas mensagens específicas ao comunicar uma violação aos titulares de dados e não devem ser enviadas com outras informações. Sendo que poderão ser considerados meios válidos de comunicação o e-mail, SMS, carta por correios, publicação do site, ou em impressos (jornais, folhetins, etc).
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	A notificação à ANPD deverá ser obrigatória para os controladores de dados pessoais, a menos que não seja suscetível a existência de um risco de dano para os direitos e liberdades das pessoas em resultado de uma violação. Um exemplo disto pode ser quando os dados pessoais já se encontram disponíveis ao público e uma divulgação desses dados não constitui um risco provável para a pessoa.
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	Igualmente ao caso da notificação à ANPD, a notificação aos titulares de dados afetados deverá ser obrigatória para os controladores de dados pessoais, a menos que não seja suscetível a existência de um risco de dano para os direitos e liberdades das pessoas em resultado de uma violação. Um exemplo disto pode ser quando os dados pessoais já se encontram disponíveis ao público e uma divulgação desses dados não constitui um risco provável para a pessoa. Ainda, assim como preconiza a GDPR, acredita-se que é interessante que a comunicação aos titulares de dados pessoais seja dispensada quando: • O responsável pelo tratamento tiver aplicado medidas técnicas e organizativas adequadas para proteger os dados pessoais antes da violação, especialmente medidas que tornem os dados pessoais incompreensíveis para qualquer pessoa não autorizada a aceder-lhes. Tal pode incluir, por exemplo, a proteção de dados pessoais com encriptação de ponta, ou através de codificação. • Imediatamente a seguir a uma violação, o responsável pelo tratamento tiver tomado medidas para assegurar que o risco elevado colocado aos direitos e liberdades das pessoas singulares já não é suscetível de se concretizar.
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	A gravidade do incidente deverá ser atribuída a probabilidade de dano aos direitos e liberdades dos titulares ocorrer e a severidade deste dado. Entende-se como dano severo aqueles de ordem material, físicos e imateriais (morais).
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	Acredita-se que a metodologia estabelecida pelo GT29 seja de grande relevância para o tema de proteção de dados pessoais e deve ser replicada pela ANPD.

Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	Acredita-se que o controlador deverá manter registro do incidente, assim como de todas as medidas tomadas para minimização dos riscos. Sendo que, caso solicitado, deverão os registros ser apresentados à ANPD.

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: Grupo de Estudos Estratégicos em Segurança da Informação e Proteção de Dados Pessoais
CPF/CNPJ:

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS

IMPORTANTE: Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.

TÓPICO/QUESTÃO	CONTRIBUIÇÃO/INSTITUIÇÃO
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	Um incidente de segurança pode acarretar risco ou dano relevante ao titular apenas e tão somente quando os dados que forem objeto de tal evento, forem dados pessoais, vez que nem todo incidente de segurança ocorre a partir de ataques a aplicações cujos dados sejam pessoais. Importante a classificação da tipologia de dados que podem estar sujeitos a incidentes. Observada a tipologia dos dados, importa também considerar a natureza do incidente e seus desdobramentos. A exemplo do que ocorre em ataques a grandes infraestruturas e seu potencial prejuízo coletivo, incidentes que envolvam dados

	sensíveis, tal como categorizados pela Lei 13.709/2018 em seu art. 5º, II, também sujeitam os titulares a maiores prejuízos. Isto posto, cabe considerar os seguintes critérios no balizamento dos prejuízos decorrentes de incidentes de segurança: *I- tipologia dos dados objeto do incidente;* *II- natureza do incidente;* *III- grau de sofisticação do ataque para fins de reparação de danos.* Finalmente, é necessário ter em mente a intertextualidade entre a legislação de proteção de dados e a garantia da neutralidade de rede trazida pelo Marco Civil da Internet, de tal sorte que -- exceto quando expressamente autorizado pela lei e constitucionalmente -- a obrigação de conferir maior segurança à rede para garantir maior proteção aos dados pessoais não confere a nenhum agente econômico, ou ao regulador com atuação na camada de aplicações a prerrogativa de interferir nas camadas interiores, como a camada de transporte e a camada internet/rede. A garantia oferecida pelo princípio da neutralidade de rede à liberdade constitucional de expressão deve dialogar com os direitos, também de índole constitucional, à privacidade e à proteção dos dados.
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc.)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	Fundamental a subdivisão, pois os ataques cibernéticos não são iguais e nem mesmo acarretam aos titulares os mesmos prejuízos. O tipo de operação de tratamento e a indicação de medidas mitigadoras para os diferentes contextos é considerada boa prática, já de longa data conhecida da comunidade de segurança. Infraestruturas críticas que tratam dados sensíveis devem, por certo, adotar medidas mais robustas que aquelas cujas operações em casos de incidentes não ofendam frontalmente direitos e garantias fundamentais. Outrossim, tal como adotado por Mendes[1], em seu trabalho Análise de Risco no GDPR, é possível criar

uma subdivisão, não especialmente pelo aspecto de segurança da informação, mas sim, centrando os riscos a partir dos dados pessoais tratados. Segundo o autor:

“Na identificação do processo é importante a definição da criticidade de ativos para posteriormente se poder estimar o nível de risco a que um processo pode estar sujeito levando em conta os seus ativos. ”

Ainda, o autor prossegue sua identificação de riscos a partir das classificações média, alta e elevada:

MÉDIA	Dados pessoais identificativos, muitas vezes publicados por livre vontade dos titulares, e que numa situação normal, sem a presença de dados sensíveis, o seu comprometimento por si só não deve causar um grande impacto.
ALTA	Dados pessoais que podem permitir chegar fisicamente perto do titular, identificar hábitos ou padrões dos mesmos, ou efetuar transações e/ou danos financeiros em nome dos/aos titulares.
ELEVADA	Dados pessoais classificados como sensíveis pelo próprio regulamento por poderem conter informação que pode colocar a integridade física e/ou moral do titular em causa.

	Não obstante, todo risco ou dano, sejam baixos ou elevados devem ser considerados relevantes, impedindo o resultado interpretativo de que "danos de natureza baixa não são relevantes", especialmente em razão do disposto no Art. 1º da própria LGPD: *Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.* Ao objetivar a proteção de direitos fundamentais de liberdade, privacidade e livre desenvolvimento da personalidade da pessoa natural, e havendo a possibilidade de concluir pela irrelevância de dados de natureza baixa aos titulares, o caráter de responsabilização aos agentes de tratamento poderá se fazer inócuo. [1]MENDES, Pedro Alexandre Brandão. Análise de Risco no GDPR. Universidade de Lisboa - Faculdade de Ciências. Mestrado em Segurança da Informática 2018, p. 34.
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	O risco deve ser mapeado previamente nos contextos em que se discute a privacidade das aplicações, no caso da tecnologia, dos fluxos de processos que envolvem o acesso direto de colaboradores e toda a cadeia de compartilhamento dos dados e a partir do estudo do risco da atividade de tratamento é que pode dimensionar a extensão do dano em casos de incidentes de segurança.
O que deve ser considerado na avaliação dos riscos do incidente?	Primeiramente, a tipologia dos dados objeto da operação de tratamento e, secundariamente, os fluxos pelos quais estes dados são acessados e compartilhados.

	Uma vez mais, é necessário identificar eventuais pontos de atrito entre a proteção dos dados pessoais e a garantia de neutralidade de rede. Ademais, a finalidade do tratamento de dados também é elemento que merece consideração na avaliação dos riscos, pois presente esse elemento, é possível considerar a característica particular de cada agente de tratamento que realizou a operação de tratamento.
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	Em coerência com o que se identificou nos itens anteriores, é necessário verificar se há risco de conflito entre a proteção dos dados pessoais e a abordagem agnóstica com relação aos dados exigida para a garantia da neutralidade de rede.
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	Todos os controladores devem, por obrigação legal manter o protocolo de *data breach* atualizado, de forma que a notificação acerca de um eventual incidente de segurança deverá ocorrer em 72 horas, que constitui um prazo minimamente razoável para que o controlador possa se inteirar do ocorrido e comunicar o fato à Autoridade Nacional de Proteção de Dados. Note-se, porém, que apontamos aqui apenas e tão somente o prazo para a notificação do evento e não suas características e demais providências, bem como o prazo ser exatamente o mesmo exigido pelo GDPR.
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (Art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	Deve constar do protocolo de *data breach* do controlador, previamente, todos os prazos relativos a cada uma das ações que deverá ser executada na ocorrência de um incidente de segurança e considerando as 72 horas propostas no item anterior, propomos que aos titulares esta notificação seja enviada em, no máximo, 5 dias úteis, ressaltando que embora, na maioria dos casos, o volume de titulares a ser comunicado seja muito grande, tal providência deve ser objeto de processo previamente delineado internamente pelo controlador e, portanto, não construída no momento da ocorrência do fato.

Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	A comunicação do incidente deve ser geral e pessoal. O controlador deve publicar uma nota em seu site institucional alertando sobre o incidente ocorrido, bem como notificar cada um dos titulares pelo meio cadastrado pelo próprio e utilizado para outras comunicações. Ressalta-se aqui que em situações de extrema relevância, tais como as que dizem respeito a ataques a grandes infraestruturas e exposição de dados sensíveis, dados de menores, adolescentes ou de cidadãos em condições vulneráveis, recomenda-se também uma nota à imprensa. A título de maior publicidade, tal como acontece com veículos (*Recall*), seria possível que o agente obrigado a comunicar realizasse este feito, ao menos na mesma mídia pela qual o titular o encontrou (ex: redes sociais, canais em plataformas de streaming), sabendo que, em diversos casos, a imprensa tradicional poderá não surtir efeito, especialmente ao pensar em crianças e adolescentes. .
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	Nos contextos de incidentes nos quais não haja dados pessoais envolvidos, tais como em ataques de negativa de serviço e ataques a infraestruturas críticas.
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	As mesmas acima descritas.
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	A ANPD deve verificar se a atuação do agente econômico responsável foi influenciada pela identificação de conflito entre a proteção dos dados pessoais e a garantia de neutralidade de rede. Objetivamente: I- A existência de uma política de segurança da informação, bem como certificações que chancelem as boas práticas de segurança adotadas pelo controlador;

	II- A existência de um programa de governança de dados efetivamente implementado e suas evidências de implementação; II- Quais as salvaguardas e medidas mitigadoras adotadas pelo controlador como providências para evitar a ocorrência de incidentes; IV- A existência de documentos que comprovem a gestão de vulnerabilidades das aplicações. V- Um protocolo de *data breach* devidamente detalhado.
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	Os Centros Federais de Segurança Cibernética dos EUA, em coordenação com Departamentos e Agências que possuem responsabilidades de segurança cibernética ou de operações cibernéticas, adotaram um esquema em comum para descrever a gravidade dos incidentes cibernéticos que afetam o país, as capacidades dos EUA ou os interesses dos EUA. O esquema denominado "*NCISS - National Cyber Incident Scoring System*"[1]- estabelece uma estrutura comum para calcular e avaliar incidentes cibernéticos. O NCISS é baseado na Publicação Especial 800-61 Rev. 2 0, denominado "Guia de manipulação de incidentes de segurança em computadores" (*Computer Security Incident Handling Guide*) - ver referência [2] - do Instituto Nacional de Padrões e Tecnologia (USA/NIST), e adaptado para incluir categorias de impacto potencial específicas da entidade que permitem avaliar a gravidade do risco e a prioridade do incidente de uma perspectiva nacional. Assim é possível garantir que todos os departamentos e agências tenham uma visão comum de: *- Gravidade de um determinado incidente;* *- Urgência necessária para responder a um determinado incidente;* *- Nível de maturidade necessário para coordenar os esforços de resposta; e*

	- Nível de investimento exigido dos esforços de resposta. Os elementos-chave do esquema de quantização são os seguintes: Nível 0 / Basal / Branco: Evento não comprovado ou **sem consequências** observáveis. Nível 1 / Baixo / Verde: É **improvável** que afete a saúde ou segurança pública, a segurança nacional, a segurança econômica, as relações exteriores, as liberdades civis ou a confiança pública. Nível 2 / Médio / Amarelo: **Pode vir impactar** a saúde pública ou segurança, segurança nacional, segurança econômica, relações exteriores, liberdades civis ou confiança pública. Nível 3 / Alto / Laranja: Provavelmente resultará em um **impacto demonstrável** na saúde ou segurança pública, segurança nacional, segurança econômica, relações exteriores, liberdades civis ou confiança pública. Nível 4 / Grave / Vermelho: Provavelmente resultará em um **impacto significativo** na saúde ou segurança pública, segurança nacional, segurança econômica, relações exteriores ou liberdades civis. Nível 5 / Emergência / Negro: Representa uma **ameaça iminente** ao fornecimento de serviços de infraestrutura crítica em larga escala, estabilidade do governo nacional ou às vidas de pessoas. Para um entendimento mais aprofundado a respeito de métricas para análise de incidentes de segurança cibernética, também recomendamos o artigo "*An Empirical Analysis of Cyber Security Incidents at a Large Organization*" [3]. **Metodologia 2:**

Em sentido semelhante o artigo ***“*** *Recommendations for a methodology of the assessment of severity of personal data breaches”* publicado pela ENISA (European Union Agency For CyberSecurity) – ver referência [4] - possui como teor, a explicação de uma metodologia de avaliação da gravidade do incidente de segurança, em um primeiro momento é necessário entender os principais critérios levados em consideração ao avaliar a gravidade de uma violação de dados pessoais, sendo eles:

- Contexto de processamento de dados (DPC): aborda o tipo de dados violados, juntamente com um número de fatores ligados ao contexto geral de processamento.

- Facilidade de identificação (EI): determina a facilidade com que a identidade dos indivíduos pode ser deduzida dos dados envolvidos na violação.

- Circunstâncias de violação (CB): aborda as circunstâncias específicas da violação, que são relacionadas ao tipo de violação, incluindo principalmente a perda de segurança dos dados violados, como bem como qualquer intenção maliciosa envolvida.

Prosseguindo ao cálculo da gravidade, com base nos critérios acima, a abordagem da metodologia é a seguinte:

- O contexto de processamento de dados (DPC) está no centro da metodologia e avalia a criticidade de um determinado conjunto de dados em um contexto de processamento específico.

- Facilidade de identificação (EI) é um fator de correção do DPC. A criticidade geral de um processamento de dados pode ser reduzida dependendo do valor do EI. Em outras palavras, quanto menor for a facilidade de identificação,

menor obtém a pontuação geral. Portanto, a combinação do EI e DPC (multiplicação) dá a pontuação inicial da gravidade (SE) da violação de dados.

- As circunstâncias da violação (CB) quantificam as circunstâncias específicas da violação que podem estar presentes ou não em uma determinada situação. Portanto, quando presente, o CB só pode aumentar a gravidade de uma violação específica. Por esta razão a pontuação inicial pode ser ajustada posteriormente pelo CB.

Assim, a pontuação final da avaliação da gravidade pode ser extraída usando a fórmula:

SE = DPC X EI + CB

Dessa forma, para que o controlador obtenha o resultado de gravidade, todos os três critérios devem ser pontuados. O resultado pertence a um determinado intervalo de valores que corresponde a um dos quatro níveis de gravidade:

Gravidade de um incidente de segurança		
SE < 2	Baixo	Os indivíduos não serão afetados ou podem encontrar alguns inconvenientes, que eles vão superar sem nenhum problema (tempo gasto reinserindo informações, aborrecimentos, irritações, etc.)
2 ≤ SE <3	Médio	Os indivíduos podem encontrar inconvenientes significativos, que irão ser capazes de superar apesar de algumas dificuldades (custos extras, negação de acesso a serviços de negócios, medo, falta de

		compreensão, estresse, menor doenças físicas, etc.)
3 ≤ SE < 4	Alto	Os indivíduos podem enfrentar consequências significativas, que devem ser capazes de superar, embora com sérias dificuldades (apropriação indébita de fundos, lista negra de bancos, danos materiais, perda de emprego, intimação, agravamento da saúde, etc.).
4 ≤ SE	Muito alto	Os indivíduos podem encontrar significantes, ou mesmo irreversíveis, consequências, que eles não podem superar (dificuldades financeiras, como dívida substancial ou incapacidade de trabalhar, psicológica ou de longo prazo doenças físicas, morte, etc.).

*SE = nível de gravidade.

Uma vez que o nível de gravidade tenha sido definido, ele pode ser acompanhado por sinalizadores indicando certos elementos da violação que, embora não afetem a priori a pontuação, são importantes para a avaliação final. Para efeitos da metodologia, duas bandeiras foram consideradas:

- **O número de indivíduos violados excede 100.** Dados de um indivíduo violados no contexto de um maior incidente, pode ser potencialmente mais facilmente divulgado, enquanto, ao mesmo tempo, um grande número dos indivíduos afetados influencia a escala geral da violação.

- **Dados ininteligíveis.** Ininteligibilidade (por exemplo, na forma de criptografia forte e sem chave compromisso) pode diminuir substancialmente o impacto para os indivíduos, uma vez que diminui bastante a possibilidade de acesso não autorizado aos dados.

Por fim, vale destacar que a metodologia apresentada neste estudo é baseada em uma abordagem o mais objetiva possível, embora ainda sendo flexível o suficiente para ser adotado por várias autoridades de proteção de dados, ajustando-o aos seus tamanhos, sistema jurídico nacional e outros fatores. De acordo com diferentes requisitos, a pontuação de algumas categorias pode ser ajustada para produzir os resultados mais adequados.

Para uma maior compreensão a respeito dos valores a serem adotados em cada etapa, recomendamos a leitura completa do artigo, onde constam tabelas informativas com os critérios especificados[4].

Referências:

[1] USA/CISA – Cybersecurity & Infrastructure Security Agency - National Cyber Incident Scoring System - https://us-cert.cisa.gov/CISA-National-Cyber-Incident-Scoring-System (acesso em 10/03/2021).

[2] USA/NIST Computer Security Incident Handling Guide - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf (acesso em 10/03/2021).

[3] M. Kuypers, T. Maillart & E. Paté-Cornell - An Empirical Analysis of Cyber Security Incidents at a Large Organization. Department of Management Science and Engineering, Stanford University, Stanford, CA & School of Information, UC Berkeley, Berkeley, California. https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/kuypersweis_v7.pdf (acesso em 10/03/2021).

*[4] Data Protection Authorities of Greece and Germany, Clara G. Manso, ENISA, Sławomir Górniak, ENISA - **Recommendations for a methodology of the assessment of severity of personal data breaches**. Enisa – European Union Agency For Cybersecurity. https://www.enisa.europa.eu/publications/dbn-severity (acesso em 11/03/2021).*

Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	Como medida prioritária**,** a notificação, tal como já descrita em itens anteriores aos titulares dos dados objeto do incidente pelas vias também já expostas neste documento. Do ponto de vista técnico, a comprovação da utilização de todas as salvaguardas e medidas mitigadoras para minimizar os efeitos do incidente. E, do ponto de vista administrativo, a instalação de auditorias para apuração de responsabilidades.
SUGESTÃO DE NORMATIVO, SE HOUVER	
Art. Xxxx	
Art. Xxxx	

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: Elo Participações Ltda

CPF/CNPJ: 09.227.099/0001-33

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS **IMPORTANTE:** Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	O incidente poderá acarretar risco ou dano relevante para os titulares sempre que tiver o potencial de ocasionar danos morais ou materiais, como, a título de exemplo, discriminação, fraude ou roubo de identidade. Além disso, deverá ser considerado, também, que os dados sensíveis demandam uma proteção maior e, por isso, o incidente que envolver dados sensíveis deverá ser considerado, automaticamente, como passível de ocasionar danos ao titular, visto que tratam de temas (dados de saúde, religião, política, etc.) que poderão culminar em atos discriminatórios ou gerar constrangimento ao titular. Por fim, entendo que também deve ser dado maior atenção aos dados de crianças e adolescentes considerando a situação de vulnerabilidade. Assim sugerimos que a ANPD considere no cálculo do impacto o volume de dados, a natureza do dado e a potencialidade de exposição.
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como	Sim, a subcategorização é importante para criar métricas padronizadas com relação à exposição de dados. Assim entendemos que deverá ser considerado o volume de dados vazados x tipo de dado x prejuízo para o titular do dado.

distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	Sendo assim, sugerimos os critérios abaixo: **Alto:** Financeiro + Imagem + Dados Sensíveis + Dados de Crianças e Adolescentes **Médio:** Imagem sem exposição financeira. **Baixo:** Exposição de Nome e/ou CPF – Dados Criptografados, tendo em vista que dificultará o acesso por terceiros. (Não relevante)
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	O risco é o potencial de causar um dano e, por sua vez, o dano é o prejuízo concretizado.
O que deve ser considerado na avaliação dos riscos do incidente?	Deverão ser considerados a extensão e potencialidade dos danos, a natureza dos dados envolvidos no incidente (Pessoal e/ou sensíveis e/ou dados bancários), a quantidade dos dados e quem teve ou poderá ter acesso aos mesmos em decorrência do incidente.
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	Durante as investigações, o report. à ANPD deverá ser realizado com as informações relevantes, como: Natureza dos dados, volumetria, identificação do titular, combinação dos dados e os possíveis impactos, risco de sequestro, comprometimento da integridade física/moral/financeira, retaliação, constrangimento ou exposição pública.
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	Para os casos de incidente do controlador, sugerimos o prazo de 7 (sete) dias úteis do conhecimento do incidente. Devido ao momento de crise e análises técnicas necessárias, entendemos que o prazo deve considerar a sensibilidade do momento. Especialmente quando o incidente ocorrer em um operador – prestador de serviços, o prazo deve ser de 10 (dez) dias úteis. Não concordamos em adotar o prazo do Cadastro Positivo, pois é aplicável a um universo menor de players no mercado. Na LGPD estamos falando de portes, seguimentos e estruturas diversos. Um prazo razoável seria de 15 dias úteis após o conhecimento do incidente, podendo a empresa enviá-las de forma gradual, quando não disponha de todas as informações necessárias, e de forma

	a garantir a maior celeridade possível, sendo que a comunicação/investigação completa deve ser enviada dentro do prazo inicial.
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	Como a comunicação à ANPD poderá ocorrer em um prazo muito exíguo considerando que a Agência quer tomar ciência o quanto antes, havendo, inclusive, a possibilidade de comunicação preliminar, que deverá ser complementada posteriormente. Um prazo maior para a comunicação aos clientes é necessário, pois essa notificação será sensível e as unidades de negócio terão que se preparar para absorver os impactos, como, por exemplo, a alta de chamados nas Centrais de Atendimento em razão do comunicado. Os atendentes terão que ser orientados para instruir corretamente os titulares dos dados. Assim, sugerimos a comunicação imediata para vazamentos com dados bancários e o prazo de 5 (cinco) dias úteis para os demais casos de baixo risco.
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	1) Formato: E-mail, notificação pelo App (validar com a área) e via postal quando o portador assim requisitar. 2) Direta e Individual. Comunicação Pública seria uma faculdade do controlador. Porém não exime a responsabilidade da comunicação individual dos titulares dado que eles devem adotar algumas ações para mitigar os riscos envolvidos.
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	Quando o risco, considerando probabilidade x impacto forem classificados como risco baixo ou médio.

Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	Quando foi algum procedimento interno, por exemplo, disponibilizou um arquivo criptografado para um email errado, ou seja, de baixo risco de exposição para o titular do dado.
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	1. Verificar se é um ataque de Hacker simultâneo em várias organizações e assim informar a situação para o mercado para que mitiguem o respectivo ataque; e 2. Para determinar a gravidade do incidente, a ANPD deverá avaliar a natureza dos dados envolvidos no incidente (dados sensíveis, dados financeiros, dados de crianças e adolescentes, por exemplo), a quantidade de dados (se foi um vazamento envolvendo 100 titulares ou 500.000 titulares), quem teve ou poderá ter acesso aos dados. Por fim, deve ser considerada a boa-fé do controlador, os controles técnicos e organizacionais comprovados e os mitigadores**.**
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	**COSO, NIST, ISO 27001, ENISA** - *European Union Agency for Network and Information Security* **(https://pesquisa.apps.tcu.gov.br/#/documento/acordao-completo/*/KEY%253AACORDAO-COMPLETO-1470754/DTRELEVANCIA%2520desc/0/sinonimos%253Dfalse)**
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	Recomendar a adoção de melhorias técnicas e administrativas – a depender do nível e maturidade da gestão da privacidade e proteção dos dados pessoais da organização, diferentes medidas podem ser sugeridas: gestão de acesso, criptografia, log de acesso, revisão de contrato, gestão de terceiros, governança de privacidade. Proporcionalidade entre o dano causado e o valor da pena pecuniária considerando a volumetria também.

SUGESTÃO DE NORMATIVO, SE HOUVER	
Art. Xxxx	
Art. Xxxx	

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: HUGHES TELECOMUNICAÇÕES DO BRASIL LTDA

CPF/CNPJ: **05.206.385/0001-61**

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS **IMPORTANTE:** Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	►Conceitualmente, um incidente decorre de algum risco (consciente ou não) ao qual os dados do titular estão expostos e/ou falha nos controles de segurança da informação. A extensão deste incidente depende necessariamente de uma investigação detalhada para então se determinar a gravidade. ►Entendemos também que "risco" e "dano" são conceitos distintos, onde o "dano" é geralmente visto como a materialização do risco, face à um incidente. ►Com relação aos critérios de avaliação, nota-se que o mercado tem usado métricas como: (i) volume de dados vazados (ex: 2%, 10% ou mais de 10% da base de titulares) e (ii) Sensibilidade (ex: Dados Pessoais imediatamente identificáveis (e.g. nome, e-mail, CPF), combinados ou não com informações comportamentais (e.g. histórico de atividades, preferências etc.). Porém, dada a grande diversidade dos setores da economia, a métrica a ser utilizada deve ser factível com o modelo de negócio das empresas. ►O fato de um vazamento de informações se tornar público já caracteriza um "dano" potencial à reputação do titular. A comprovação de que os dados do titular foram utilizados para realizar quaisquer ações em nome do mesmo, se caracteriza como um dano relevante. Como exemplo citamos, utilizar dados do titular para uma compra, sem o conhecimento do titular.
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como	►Sim, entendemos que esta seria uma boa abordagem inicial para a definição de definições tão complexas.

distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	►Para a distinção de níveis, acreditamos que um bom ponto de partida seria um levantamento sobre o que as Autoridades Europeias, sujeitas a GDPR, e mercado Norte Americano estão adotando neste sentido.
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	Dada a complexidade deste tema, uma visão passível de avaliação é a de que o "dano" é algo que pode ser comprovado após a materialização do "risco". Por exemplo o "risco" é que um dado pessoal seja vazado a quem não deve ter acesso. Já o "dano" seria a comprovação de que este vazamento causou algum prejuízo ao titular, seja este reputacional ou financeiro.
O que deve ser considerado na avaliação dos riscos do incidente?	Como uma das formas, sugerimos primeiramente uma análise dos controles de segurança aplicáveis ao modelo de negócio das empresas. A partir daí faz-se necessário a elaboração de uma Política de Segurança da Informação com o intuito de minimizar o risco e seus efeitos. Vide nosso comentário no primeiro tópico/questão.
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	Na prática o Artigo 48 já solicita informações que nem sempre podem estar disponíveis no momento de um incidente. Citamos por exemplo a informação de *"IV – os riscos relacionados ao incidente",* pois nem sempre é possível se determinar o que um ofensor poderá praticar com um dado acessado indevidamente. Entendemos que a ANPD deve solicitar esta gama de informações, porém sem o caráter obrigatório como uma comunicação imediatamente após o incidente. Somos da opinião que a ANPD não deve solicitar informações adicionais. Por outro lado, dependendo das características do incidente, nem todas as informações solicitadas neste artigo da Lei podem estar disponíveis.
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	Considerando a complexidade dos sistemas computacionais atuais e da economia digital, como o uso cada vez mais frequentes de sistemas terceirizados em nuvem, acreditamos que a ANPD deva considerar prazo não inferior à 72 horas, a exemplo do aplicado na GDPR.
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	Antes de se pensar em um prazo para a comunicação de incidentes aos titulares, entendemos que deve-se definir o que é "dano ou risco relevante", conforme previsto no art. 48, §1º, pois esta é a principal motivação para a necessidade ou não da comunicação ao titular. Em função do exposto no nosso comentário anterior, entendemos que o prazo para a comunicação ao titular deve ser superior ao prazo estabelecido para a comunicação à ANPD e dependente da sensibilidade e extensão do incidente (Ex: número de titulares impactados)

	Sem uma definição clara deste conceito, a comunicação poderá incorrer em um alarme falso ao titular e causar um prejuízo reputacional sério às empresas e ao mercado como um todo, dependendo da extensão do incidente.
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	►Entendemos que a forma da comunicação deve prioritariamente eletrônica (ex: e-mail, SMS) e endereçada somente ao titular nos casos, quando tal comunicação for factível. ►Nos casos de incidentes de grande extensão (ex: número de titulares impactados) e/ou cujo o risco envolva aspectos de saúde ou segurança, entendemos que um comunicado através de veículos de grande comunicação seja o mais apropriado.
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	Uma das exceções é quando não houver evidências de que o incidente causou algum risco ou dano ao titular, a depender da extensão do incidente.
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	Idem ao comentário acima
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	Vide nosso comentário no primeiro tópico/questão.
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	Acreditamos que um bom ponto de partida seria um levantamento sobre o que as Autoridades Europeias, sujeitas a GDPR, e mercado Norte Americano estão adotando neste sentido.
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	Acreditamos que um bom ponto de partida seria um levantamento sobre o que as Autoridades Europeias, sujeitas a GDPR, e mercado Norte Americano estão adotando neste sentido. Adicionalmente a ANPD poderia solicitar aos Controladores um plano de correção e melhorias para mitigar futuros incidentes.

SUGESTÃO DE NORMATIVO, SE HOUVER	
Art. Xxxx	
Art. Xxxx	

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: IAB BRASIL (AMI - ASSOCIAÇÃO DE MÍDIA INTERATIVA)

CPF/CNPJ: 02.861.708/0001-62

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regularmente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS **IMPORTANTE:** Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	Existem várias circunstâncias nas quais um incidente de segurança pode desencadear riscos ou danos relevantes aos titulares dos dados pessoais, sendo que os riscos e danos associados nem sempre estão relacionados ao tamanho ou ao escopo da própria violação. Por exemplo, a violação de informações financeiras específicas de um pequeno número de pessoas pode ser mais significativa do que uma violação maior de dados menos relevantes. Neste sentido, o IAB sugere que a ANPD leve em consideração os seguintes fatores para aferir se um incidente de segurança causa risco ou dano relevante aos titulares dos dados pessoais: ● Natureza dos dados pessoais objeto do incidente e o nível de sensibilidade associado aos mesmos; ● Intenção da violação (maliciosa ou não maliciosa, direcionada ou não direcionada); ● Tamanho, escopo ou volume da violação; e ● Facilidade na identificação de indivíduos com base nos dados pessoais violados.
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	O IAB sugere o uso de **critérios mensuráveis** para definir a materialidade ou relevância dos incidentes de segurança e limitar um regime de relatório obrigatório apenas aos incidentes que causaram danos materiais ou significativos (mais detalhes abaixo). Por exemplo, a materialidade pode ser expressa em termos do número de usuários impactados por um incidente, juntamente com a sensibilidade atrelada à natureza dos dados pessoais objeto da violação. As faixas para envio obrigatório de relatórios devem ser altas o suficiente para evitar o excesso de relatórios de incidentes insignificantes, o que aumentaria a carga administrativa das empresas e da ANPD sem um ganho proporcional para a segurança das operações de tratamento de dados pessoais.

	Gostaríamos de ressaltar também que um mero risco ou ameaça potencial de um incidente não deve ser considerado relevante. Por exemplo, os departamentos de segurança cibernética de provedores de serviços online estão constantemente lidando com ameaças. O alargamento do regime de notificação para abranger meras ameaças resultaria numa notificação excessiva significativa e em encargos administrativos desnecessários. Neste sentido, uma classificação de riscos em "Alto", "Médio" e "Baixo" pode permitir tal modulação, sendo que: - Risco ou dano baixo e médio: Não reportável, mas as medidas técnicas adequadas precisam ser adotadas e o incidente deve ser documentado pelo controlador; - Risco ou dano alto: Reportável à ANPD.
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	Risco para o titular dos dados e danos ao titular dos dados podem ser vistos como termos quase que sinônimos. A expressão 'risco' pode ser interpretada de maneira mais ampla do que 'dano', pois sugere que o dano 'potencial' também seria considerado. Porém a interpretação razoável, e alinhada com outras jurisdições, qualificaria o 'risco' como um 'risco de dano', assim sendo uma forma de definir o escopo (*potencialidade*) e severidade (*dano ou risco relevante*).
O que deve ser considerado na avaliação dos riscos do incidente?	Conforme sugerido na questão acima: ● Natureza dos dados pessoais objeto do incidente e o nível de sensibilidade associado aos mesmos; ● Intenção da violação (maliciosa ou não maliciosa, direcionada ou não direcionada); ● Tamanho, escopo ou volume da violação; ● Facilidade na identificação de indivíduos com base nos dados pessoais violados.
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	**- x -**
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	O prazo de 72 horas é visto globalmente como um padrão para relatar incidentes de segurança. Um período de tempo mais curto para envio do relatório preliminar pode criar uma carga administrativa muito onerosa. O foco dos controladores de dados pessoais seria desviado da investigação do incidente e do plano de remediação para o mero preenchimento do relatório de reporte em um prazo muito exíguo. Vale ressaltar à ANPD que as equipes internas responsáveis pela resposta aos incidentes de segurança também são aquelas que devem fornecer as informações necessárias para envio do relatório.

	Além disso, o prazo de 72 horas pode ser considerado insuficiente para reunir as informações necessárias para a notificação das autoridades relevantes. O GDPR (Artigo 33) explica isso observando "[quando] *... não for possível fornecer as informações ao mesmo tempo, as informações podem ser fornecidas em fases, sem atrasos indevidos*." É razoável que a ANPD adote também tal possibilidade, ou seja, que o relatório seja elaborado de maneira faseada. Por fim, um elemento importante é o início do prazo, isto é, a determinação de quando tal prazo se inicia. Investigações sobre os incidentes de segurança complexos costumam levar muito tempo (às vezes várias semanas) para estabelecer adequadamente os fatos. Assim, a ANPD deve considerar as dificuldades práticas de investigação forense, exames de sistemas, etc., e auxiliar os controladores a determinar exatamente os critérios de 'risco relevante' (como indicado nas questões acima) e qual o grau de certeza esperado para que se inicie tal prazo (ou seja, uma organização precisa ter um “grau razoável de certeza” de que o incidente ocorreu, ou o incidente precisa ser “mais provável do que não”). A ANPD pode permitir que as organizações tenham tempo para avaliar se algo realmente aciona a definição de um incidente de segurança que cause risco ou dano relevante ao titular dos dados pessoais, e apenas uma vez que foi determinado, passar ao início da contagem do prazo.
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	Se uma investigação resultar em uma determinação de que houve uma violação material que cause risco ou dano relevante ao titular dos dados pessoais, os controladores devem notificar os titulares dos dados no tempo mais expedito possível e sem atrasos excessivos, mas em qualquer caso dentro de 60 dias após a determinação da ANPD. Acreditamos que as informações que os controladores devem fornecer conforme listado no Artigo 48 do LGPD são suficientes para informar de maneira clara e transparente os titulares de dados pessoais. Porém, observamos que o grau de detalhamento de certas informações (como as medidas de segurança que foram ou estão sendo adotadas pela empresa) deve ser balanceado com o risco de uso de tais informações por atores mal-intencionados - por isso a informação pública sobre um incidente deve conter um detalhamento inferior ao comparada com o relatório enviado à ANPD. Seria importante a ANPD incentivar que as empresas adotem uma linguagem simples e clara para os titulares dos dados pessoais, respeitando as formas de comunicação que cada empresa tem com o seu público.

Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	Cada empresa, como regra geral, tem um bom mapeamento de como se comunicar com seus próprios usuários. Entendemos também que sempre que possível, a comunicação deve ser direta e individualizada. Considerando a ampla gama de opções para notificar os titulares dos dados pessoais afetados, é razoável que a ANPD adote os seguintes métodos como suficientes: - Notificação por escrito; - Aviso por e-mail; - Outro aviso eletrônico razoavelmente calculado para chegar ao indivíduo afetado (tais como notificações em aplicativos); ou - Quando nenhum outro método estiver disponível ou o custo do envio de aviso for proibitivo, aviso público por meio de postagem visível no site do controlador por pelo menos 30 dias e notificação para a grande mídia local e nacional.
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	Além das considerações acima quanto à obrigação de reportar apenas incidentes que causaram danos ou riscos materiais ou significativos (ou de 'alto risco' caso adotada tal classificação pela ANPD), em geral, se a entidade na qual a violação ocorreu já estiver sob a autoridade reguladora de uma entidade ou agência governamental setorial, pode não ser necessário notificar a ANPD. Da mesma forma, se a violação de dados pessoais se enquadrar em um regime de resposta a incidentes que inclui notificação aos indivíduos afetados e notificação a um regulador com poderes de supervisão específicos, a notificação ao ANDP não seria necessária.
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	Apenas incidentes que causaram danos/riscos materiais ou significativos, como indicado acima. Além disso, seria interessante que a ANPD considerasse o risco de "esforço desproporcional" em relação às notificações dos titulares dos dados pessoais.
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	**Nossa sugestão estaria em linha com o já apontado anteriormente:** ● Natureza dos dados pessoais objeto do incidente e o nível de sensibilidade associado aos mesmos; ● Intenção da violação (maliciosa ou não maliciosa, direcionada ou não direcionada); ● Tamanho, escopo ou volume da violação; e ● Facilidade na identificação de indivíduos com base nos dados pessoais violados.
Existe alguma metodologia recomendada para a análise de	Muitos dos critérios mencionados nas questões acima são descritos em mais detalhes nas "Recomendações para uma metodologia de avaliação da gravidade das violações de dados pessoais" [2013, disponível no link:

gravidade do incidente de segurança? Se sim, qual(is)?	https://iapp.org/media/pdf/resource_center/ENISA-breach-severity-methodology.pdf] da Agência da União Europeia para Segurança de Redes e Informações (ENISA).
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	**- x -**
SUGESTÃO DE NORMATIVO, SE HOUVER	
- x -	

Tomada de Subsídios 2/2021

Iagor Augusto <[redacted]>

ter 23/02/2021 09:13

Para: ANPD - Consulta Publica <consultapublica@anpd.gov.br>;

Caros,
Bom dia!

Tendo em vista a Nota Técnica nº 3/2021/CGN/ANPD, sobre a tomada de subsídios "Tomada de Subsídios para regulamentação do dever de comunicação de incidentes de segurança, nos termos do § 1º do art. 48 da Lei nº 13.709, de 14 de agosto de 2018.", assim dispõe a nota supracitada. Passo a contribuir nos pontos que seguem;

1 - Importante mecanismo que auxiliaria tanto na comunicação entre controlador dos dados, o titular e a ANPD, seria um banco nacional de cadastro de incidentes e comunicação de dados. Consiste numa espécie de "Registrato" dos dados, onde o titular, poderá efetuar ali seu cadastro prévio e saber todos que possuem e controlam seus dados, como sabemos as contas bancárias e em instituições financeiras que temos cadastro quando acessamos o "registrato" do BC. Desta forma, fica centralizado na ANPD esse controle, fazendo com que os dados dispostos na plataforma fiquem seguros.

2 - Para que os controladores comunicassem os dados que possuem ao titular e a ANPD seriam feitos em 3 passos:
Primeiro passo: ANPD disponibiliza a plataforma e solta nota técnica e regulamentação posterior a disponibilização da plataforma, informando prazo máximo para os grandes controladores de dados (qualificando os mesmos na nota técnica e regulamentação) passarem os mesmos, desde que sensíveis e outros que a ANPD julgar necessário, atribuindo penalidades caso não atendam ao prazo. (Haveria um enorme processo de conversação com as grandes controladoras de dados, pois as mesmas também teriam que verificar se de fato seria possível passar os dados no prazo estipulado)

Segundo Passo: ANPD recebe os dados, audita e guarda os mesmos, para posteriormente, disponibilizá-los aos seus titulares através da plataforma.

Terceiro Passo: Veicula nas mídias informações para a população efetuar o cadastro na plataforma (será um cadastro seguro pois estará aos cuidados da ANPD). E lá na plataforma serão informados os controladores dos dados dos titulares, os incidentes que já foram comunicados a ANPD que possuem dados daqueles titulares, e demais situações que a ANPD julgar necessário.

Acredito que dessa forma, ficaria, além de mais prático, no longo prazo resultaria em um melhor custo-benefício.

Agradeço a oportunidade de contribuir!

At.te
Iagor Marques

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: IBRAC – Instituto Brasileiro de Defesa da Concorrência, Consumo e Comércio Internacional

CPF/CNPJ:96.287.453/001-10

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS **IMPORTANTE:** Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
1. Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	Ao longo desta resposta à tomada de subsídios, buscou-se trazer normas e orientações aplicadas em outras jurisdições para explorar possíveis formas de regulamentação do tema da notificação de incidentes de segurança. Entende-se, entretanto, que é necessário realizar esforço para que a adoção destas orientações seja feita de forma seletiva, considerando especialmente que muitas das jurisdições citadas possuem já há alguns anos normas aplicáveis à proteção de dados pessoais e, mais especificamente, a incidentes de segurança. Neste sentido, entende-se que a leitura a ser feita das normas apresentadas a seguir deve ser sensível às peculiaridades do ordenamento jurídico brasileiro. Em especial, o fato de a Lei Geral de Proteção de Dados Pessoais (LGPD) ser a primeira legislação abrangente sobre proteção de dados pessoais no país, de forma que se observa um baixo nível de maturidade das entidades para lidar com demandas relacionadas à norma. Pesquisas que indicam a preponderância de empresas de pequeno e médio porte no país[1], bem como o atraso para a adequação de muitos agentes à legislação[2], apontam a necessidade de se criar regime coerente com a cultura institucional de proteção de dados pessoais brasileira. De certa forma, pode-se reconhecer que o próprio legislador, ao prever regime aberto sobre a notificação de incidentes de segurança, permitiu à ANPD estabelecer normas coerentes com o nível de maturidade dos agentes de tratamento de dados pessoais no país. Com normas aderentes à realidade brasileira, pode-se garantir ambiente apto ao desenvolvimento de cultura de proteção de dados

[1] https://www.sebrae.com.br/sites/PortalSebrae/ufs/sp/sebraeaz/pequenos-negocios-em-numeros,12e8794363447510VgnVCM1000004c00210aRCRD.
[2] https://valor.globo.com/empresas/noticia/2020/10/01/adaptacao-a-lgpd-ainda-e-meta-distante.ghtml.

	pessoais, de modo que o país possa inclusive evoluir posteriormente para regulamentações mais rígidas sobre o tema da notificação de incidentes de segurança. Para analisar o risco pode-se utilizar o quanto o incidente afetou um ou mais dos três princípios de segurança da informação (confidencialidade, integridade e disponibilidade) e se este vazamento teve ou não intenções maliciosas de prejudicar determinados indivíduos ou empresas. Como critérios para avaliar a relevância do risco ou dano pode-se considerar alguns dos aspectos listados abaixo que tornam um processamento como de alto risco pela CNIL: • Caso os dados vazados permitam avaliação sistêmica e extensiva sobre aspectos pessoais ou pontuação, incluindo definição de perfis e previsões de comportamento. Ex.: definição de perfis para colaboradores baseada em suas transações dentro de um sistema, que possui redefinição automática de tarefas; • Caso os dados vazados incluam dados sensíveis ou dados de natureza altamente pessoal. Ex.: exames médicos ou análise criminal para admissão; • Caso o vazamento inclua bases de dados distintas originadas de diferentes operações de tratamento executadas para diferentes objetivos ou por diferentes controladores. Ex.: análise de dados de controle de acesso em conjunto com autodeclaração de horas trabalhadas; • Processamento de dados em larga escala, considerando o número de pessoas, o volume de dados pessoais processados, extensão geográfica. Ex.: processamentos relativos à Inteligência artificial, Big Data, IoT, entre outras tecnologias que capturam elevado volume de dados, que cubram uma área geográfica extensa e processe dados pessoais; • Caso os dados vazados possam acarretar dificuldade de os titulares dos dados exercerem seus direitos ou utilizarem um serviço ou contrato. Ex.: exclusão de bases de dados. Na Austrália, uma violação de dados notificável ocorre quando o acesso ou divulgação provavelmente resultaria em danos graves a qualquer um dos indivíduos aos quais as informações divulgadas se referem. Embora dano "grave" não seja definido na legislação, a Office of the Australian Information Commissioner divulgou orientações sobre como o dano grave pode ser interpretado e avaliado. Há uma série de critérios-chave a serem examinados, em especial, (i) o tipo de dados pessoais envolvidos no incidente (i.e., se envolve informações sensíveis, documentos usualmente utilizados para fraudes de identidade ou um conjunto de informações pessoais, e não apenas um dado pessoal isolado); (ii) as circunstâncias relacionadas ao incidente (i.e., quem é o titular dos dados, quantos indivíduos foram envolvidos, a possibilidade de se associar um indivíduo à aquisição de um determinado produto ou

	serviço de caráter sigiloso, o período de tempo que as informações se mantiveram disponíveis); e (iii) a natureza do dano (i.e., perda financeira, ameaça à integridade física, perda de negócios ou oportunidade de emprego, danos reputacionais). Em Singapura, quando uma organização tem motivos para acreditar que ocorreu uma violação de dados, ela deve realizar uma avaliação para determinar se a violação de dados é uma violação notificável. Uma violação de dados deverá ser notificada se envolver os dados de, ao menos, 500 indivíduos, ou se resultar (ou provavelmente resultar) em danos significativos aos indivíduos afetados. De forma mais detalhada, estabeleceu-se que haverá dano significativo a um indivíduo se a violação de dados estiver relacionada a uma ampla gama de informações, que incluem, por exemplo, dados referentes ao nome completo ou pseudônimo, identidade, remuneração, informações bancárias, informações que possam associar o indivíduo a investigações ou determinados processos judiciais e dados de saúde. O Personal Information Protection Commission, no Japão, recentemente divulgou minuta de guia com orientações sobre a necessidade de notificação de incidente. A minuta estabelece que deverá ser reportado à autoridade o vazamento (i) de informações pessoais confidenciais; (ii) que suscitar risco de danos financeiros; e (iii) quando envolver mais de 1000 titulares de dados. Com relação à União Europeia, o Article 29 Working Party possui um guia sobre as notificações referentes a vazamentos de dados pessoais (Guidelines on Personal Data Breach Notification Under Regulation 2016/679). No documento, é oferecida uma lista de critérios para avaliação dos riscos aos indivíduos, tais como o tipo de vazamento, a natureza, a sensibilidade e o volume dos dados pessoais, a facilidade de identificação dos indivíduos, a severidade das consequências para os indivíduos em decorrência do incidente, as peculiaridades do indivíduo, as características do controlador dos dados, o número de indivíduos envolvidos e uma análise, sob uma perspectiva global, do vazamento. O Ibrac entende que, na análise de incidentes de segurança, a ANPD deve dar enfoque sob 2 perspectivas gerais, quais sejam, qualitativa e quantitativa. A análise qualitativa deve ser feita correlacionando os tipos de dados vazados, para além das categorias estritamente legais de dados pessoais sensíveis, levando em consideração a lógica da severidade do impacto envolvido ao titular. Nesse tipo de análise, deve-se ter um olhar mais contextual, concatenando

	os critérios aqui elencados com a perspectiva quantitativa de número de titulares afetados, podendo ser desenvolvida uma régua de risco/dano como forma de gradação do entendimento do impacto causado por um incidente de segurança. Já a análise quantitativa deve ocorrer apenas após a realização da análise qualitativa acima mencionada, uma vez que o volume de dados pessoais envolvidos não é, por si só, um critério que possa acarretar risco ou dano relevante ao titular. De todo modo, a análise quantitativa deve ser feita baseando-se no número de titulares afetados pelo incidente de segurança, de forma a priorizar incidentes com maior potencial de risco ou dano aos titulares; evitar fatiga de comunicações por parte de agentes de tratamento e titulares de dados; e resguardar a ANPD de um acúmulo de comunicações para análise e beneficiar uma melhor alocação dos limitados recursos do órgão. Vale destacar que para vazamentos de menor porte ou acessos não autorizados, a LGPD prevê no art. 52, §7º, que o controlador poderá realizar conciliação direta com os titulares afetados.
2. O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	Especialmente em face da existência de regimes consolidados de avaliação e reação a incidentes de segurança ao redor do mundo, entende-se que pode ser interessante desenvolver metodologia de avaliação que se coadune com normas internacionais e práticas de agentes de mercado. A EY utiliza uma metodologia com quatro categorias de severidade: baixa, média, alta ou muito alta, de acordo com um score quantitativo de 1 a 6 para verificar o impacto do incidente de privacidade. O cálculo para definir a severidade do incidente de privacidade é extraído usando a fórmula: SE = CPD* FI+CI, sendo: • Severidade (SE): Severidade do incidente de privacidade • Contexto do processamento de dados (CPD): Criticidade da informação tendo em conta o contexto específico do processamento de dados • Facilidade de identificação (FI): Facilidade de um terceiro que tenha acesso a um conjunto de informações e faça a correspondência unívoca a certo indivíduo • Circunstâncias do incidente (CI): Circunstâncias específicas do incidente

	Na Irlanda, ao reportar o incidente ao Data Protection Commission, as entidades devem classificar o risco envolvido como (i) baixo risco, quando é improvável que a violação tenha impacto sobre os indivíduos ou o impacto provavelmente será mínimo; (ii) risco médio, quando a violação pode ter um impacto sobre os indivíduos, mas é improvável que o impacto seja substancial; (iii) alto risco, quando a violação pode ter um impacto considerável sobre os indivíduos afetados; ou (iv) risco grave, quando a violação pode ter um impacto crítico, extenso ou perigoso sobre os indivíduos afetados. Na União Europeia, o *Article 29 Working Party* classifica os vazamentos entre (i) os que não são aptos a causar riscos para os direitos e liberdades dos indivíduos; (ii) os que são aptos a causar riscos; e (iii) os que são aptos a gerar riscos altos para os titulares de dados pessoais. O Ibrac se posiciona de forma favorável aos posicionamentos da Irlanda e do *Article 29 Working Party* elencados acima, por se mostrarem objetivos, mas flexíveis o suficiente para corretamente serem endereçados nas análises caso a caso que serão realizadas pela ANPD a partir dos incidentes de segurança que forem comunicados.
3. Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	O Ibrac entende, em síntese, que o risco não acarreta, necessariamente, em dano ao titular dos dados. A existência de eventual dano precisa ser analisada caso a caso, com base em evidências que possam demonstrar o prejuízo aos titulares de dados afetados pelo incidente de segurança. Porém, como forma de averiguar se há evidências suficientes de danos ocasionados no caso concreto, a ANPD deverá entender melhor o nexo de causalidade entre o incidente de segurança ocorrido e os danos acarretados aos titulares quando da análise do incidente de segurança.
4. O que deve ser considerado na avaliação dos riscos do incidente?	A avaliação de riscos associados ao incidente deve ter em conta os riscos colocados aos direitos e liberdades dos titulares de dados pessoais. Para mensurar os riscos aos incidentes, entende-se que devem ser considerados: 46. As recommended by the WP29 in its guidelines, the factors to be taken into account when assessing the risks are:

	1. type of breach 2. nature, sensitivity, and volume of personal data 3. ease of identification of individuals 4. severity of consequences for individuals 5. special characteristics of the individual 6. special characteristics of the data controller 7. the number of affected individuals. *(Guidelines on personal data breach notification For the European Union Institutions and Bodies)*

5. Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	**Os controladores deverão notificar:** (Obs: Caso os itens abaixo não possam ser apresentados na primeira notificação à ANDP, os controladores poderão requerer prazo para complementação das informações / documentos, desde que justifiquem a impossibilidade de apresentação imediata). - Descrever o tipo de notificação como *completa *inicial, *consequencial ou *conclusiva. Neste caso, é importante que as notificações gerem um número de referência - Dados do encarregado - Informações sobre o operador envolvido no incidente (se houver) e do encarregado do operador - Critérios de segurança afetados (i.e.: confidencialidade, integridade, disponibilidade) - Data do incidente / data da detecção / data da notificação - Número aproximado de pessoas afetadas - Se o incidente afetou dados pessoais de crianças e adolescentes

	- A definição do impacto aos titulares como: baixo / médio / alto e as razões - Potencial causa do incidente - Se houve notificação aos titulares e o motivo - Onde a base de dados pessoais afetada se encontra (e.g.: base de dados física, HD externo, dispositivo corporativo, VPN, etc.) - Quais medidas de segurança existiam à época do incidente e quais medidas de segurança foram implementadas após o incidente ou estão em processo de implementação (plano de ação, planos estratégicos e mitigatórias futuros). **Fontes:** ICO - https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/ WP29 - https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052 BFDI – Autoridade Alemã - https://www.bfdi.bund.de/DE/Service/Datenschutzverstoesse/datenschutzverstoesse_node.html Países Baixos DPA - https://datalekken.autoriteitpersoonsgegevens.nl/melding/aanmaken?1 Observação: A ANPD divulgou através do link https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca um formulário de *Comunicação de Incidente de Segurança com Dados Pessoais à Autoridade Nacional de Proteção de Dados (ANPD).* Com relação ao referido documento, recomendamos a supressão do item abaixo transcrito em razão da notificação à autoridade ser uma obrigação do controlador. *O notificante é:* *☐Controlador.* *☐Operador.*

	Se operador, informar se já houve comunicação ao controlador: [Resposta] Em sendo o caso, o operador deverá cooperar com o controlador, porém a obrigação de notificar a ANPD, nos termos do Art. 48 é do controlador.
6. Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	A (in)determinação de prazo específico para notificação à autoridade competente acerca de um incidente de segurança não é algo exclusivo do diploma brasileiro. Ainda que nos Estados Unidos não exista uma lei Federal sobre o tema, os estados têm leis que tratam sobre a matéria e, em diversas delas, não é estabelecido um prazo determinado, prevendo apenas que a notificação ocorra "sem atrasos indevidos". Outros estados, como o Novo México[3], determina o prazo de até 45 dias para emitir notificações quando uma violação de dados for descoberta. Da mesma forma, o *Digital Privacy Act* canadense estabelece que a notificação deva ocorrer "assim que possível" a partir do momento em que determinar que o vazamento ocorreu. O GDPR (art. 33) prevê que a violação deve ser reportada "sem atrasos indevidos" e, se possível, em até 72 horas após o conhecimento sobre o ocorrido. O prazo pode ser ampliado, desde que justificado, quando for improvável que o vazamento resulte em risco para os direitos e liberdades dos titulares. Da mesma forma, o ICO[4] reitera os termos do art. 33 do GDPR, no sentido de que a comunicação à autoridade deverá ocorrer em até 72h, quando viável. Se não for possível que o controlador reúna as informações necessárias para notificar a autoridade em até 72h, poderá realizá-la em fases, mediante justificativa (item 3, art. 33 do GDPR). Na Australia, a autoridade exige que, quando houver motivos razoáveis para suspeitar que pode ter havido um incidente, o responsável pelos dados deve tomar todas as medidas razoáveis para realizar uma avaliação aprofundada no prazo de 30 dias (após ela tomar conhecimento dos motivos razoáveis para suspeitar que tal incidente pode ter ocorrido) para determinar se ocorreu ou não uma violação de dados pessoais.[5]

[3] Disponível em: https://law.justia.com/codes/new-mexico/2017/chapter-57/article-12c/section-57-12c-6/. Acesso em 18/03/2021.
[4] Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-law-enforcement-processing/personal-data-breaches/. Acesso em 18/03/2021.
[5] Disponível em: https://www.dataguidance.com/notes/australia-data-protection-overview#:~:text=%27%20Unless%20a%20specific%20limited%20exemption,data%20breach%20has%20occurred%3B%20or. Acesso em 18/03/2021.

	Diante desse cenário, entende-se que a imposição de um prazo específico para todas as situações de incidentes não é algo praticável. Por outro lado, a sugestão de um prazo razoável (não mandatório) e a notificação seguida de uma justificativa caso o prazo tenha transcorrido, parecem soluções mais viáveis. A mera sugestão de um prazo que a ANPD entenda como razoável (como é o caso das autoridades europeias que sugerem o prazo de 72h) traz maior segurança aos controladores, pois saberão que após aquele prazo deverão apresentar a justificativa para tanto. Por fim, outro ponto que merece atenção é a definição de quanto se considera o conhecimento, pelo controlador, do incidente de segurança. O *Working Party 29* da *European Data Protection Board*[6] considera que o controlador deve ser considerado "ciente" quando tiver um grau razoável de certeza de que ocorreu um incidente de segurança que levou ao comprometimento de dados pessoais. Isso, por obvio, dependerá das circunstâncias da violação específica. Em alguns casos, será relativamente clara a identificação do início em que houve uma violação, ao passo que, em outros, pode levar algum tempo para determinar se os dados pessoais foram, de fato, comprometidos. De qualquer modo, é importante ressaltar a necessidade de ação imediata para investigar um incidente e determinar se os dados pessoais foram realmente violados. Finalizamos com o comentário de que entendemos ser importante um alinhamento a padrões internacionais no que se refere a regulamentação de proteção de dados pessoais. O mundo é hoje eminentemente global e as empresas estão cada vez mais se conectando com outras em outras regiões do globo para prestação ou fornecimentos de serviços. Assim que é impraticável que cada regulamento decida o seu "prazo mínimo" de notificação as autoridades competentes, uma vez que dificulta em muito a organização global de controladores e seus processadores. Da mesma forma que padrões mínimos globais foram necessários para regulamentar direitos de propriedade intelectual, por exemplo, seria altamente recomendável que o mesmo se busque no caso de regulamentação de proteção de dados. Portanto, se a LGPD buscou

[6] Disponível em: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2021/guidelines-012021-examples-regarding-data-breach_en. Acesso em 18/03/2021.

	inspiração na GDPR em tantos pontos, neste em particular, seria ideal a busca pela harmonização do prazo estabelecendo-se o critério das 72 horas úteis e não 48 horas úteis, como proposto.
7. Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	O artigo 48, §1º, da LGPD estabelece um dever de comunicar o titular do dado pessoal quando houver um incidente de segurança "que possa acarretar risco ou dano relevante aos titulares". A partir dessa determinação, surgem dois pontos para regulamentação: (i) qual a informação adequada ao titular de dados pessoais sobre o incidente; e (ii) qual o prazo adequado para os controladores prestarem informações aos titulares dos dados pessoais sobre o incidente. A respeito da informação aos titulares de dados pessoais, um princípio básico tanto da LGPD quando da GDPR diz respeito ao princípio da transparência. O princípio da transparência exige que qualquer informação destinada ao público ou ao titular dos dados seja concisa, de fácil acesso e compreensão, bem como formulada numa linguagem clara e simples, e que se recorra, adicionalmente, à visualização sempre que for adequado. É importante a menção de que o princípio da transparência não pode ser confundido ou tratado como um dever de revelação integral aos titulares de dados pessoais, uma vez que o excesso de informação acaba levando à desinformação do consumidor e/ou titular de dados pessoais. A esse respeito, cita-se o trabalho de Cass Sustein, "*Too much information: Understanding what you don't want to know*" (Cambridge: MIT Press, 2020). A rigor, o princípio da transparência e informação é melhor tratado a partir do dever de prestar informações compreensíveis e completas aos titulares de dados pessoais que podem ou não ser letrados em computação de dados. Justamente em razão disso, que atualmente recorre-se usualmente ao uso de "Nudges" e economia comportamental para interpretação do dever de informação e transparência.

	Pelle Hansen define "nudge" como: "qualquer tentativa de influenciar o julgamento, escolha ou comportamento das pessoas de uma forma previsível, que é (1) possibilitada em virtude de limites cognitivos, vieses, rotinas e hábitos na tomada de decisão individual ou social, que impõem barreiras para que as pessoas ajam racionalmente em seu próprio autointeresse; e que funcionam valendo-se desses limites, vieses, rotinas, e hábitos" (Hansen, Pelle Guldborg (março de 2016). «The Definition of Nudge and Libertarian Paternalism: Does the Hand Fit the Glove?». European Journal of Risk Regulation. 7 (1): 155–174. ISSN 1867-299X. doi:10.1017/S1867299X00005468). No direito brasileiro, a Portaria n. 618/2019 do Ministério da Justiça já utiliza esse comportamento/dever do fornecedor nas informações disponibilizadas aos consumidores quando da realização de recall de produtos nocivos ou defeituosos: "As diretrizes e outros documentos e estudos do Grupo de Trabalho sobre Segurança de Bens de Consumo da Organização para a Cooperação e Desenvolvimento Econômico, notadamente as relacionadas a aplicação de indutores (insights) comportamentais ao consumidor, deverão ser levadas em consideração pelos fornecedores quando da elaboração da documentação referente ao plano de atendimento". Ou seja, no comunicado aos titulares de dados pessoais sobre incidentes de vazamento, deve-se privilegiar a informação em uma linguagem clara e simples e que permita a fácil e rápida compreensão a respeito dos riscos e medidas mitigatórias que devem ser adotadas pelo titular dos dados pessoais (por exemplo, troca de senha, entre outros). Entre as informações constantes do Art. 48, §1, da LGPD, nos parece que apenas as seguintes informações deverão constar do comunicado ao titular dos dados: (i) a descrição da natureza dos dados pessoais afetados; (ii) os riscos relacionados ao incidente; e (iii) as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo. Adicionalmente, entendemos que deve haver (iv) medidas que devem ser adotadas pelo próprio titular dos dados para reverter ou mitigar os efeitos do prejuízo (por exemplo, alterar senha).

	Não parece haver relevância ou fundamento para que conste no comunicado ao titular de dados: (i) as informações sobre os titulares envolvidos; (ii) a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; e (iii) a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial Em relação ao prazo para comunicação de um evento de vazamento de dados pessoais, a GDPR estabelece um prazo de 72 horas para comunicação para as Autoridades Competentes após o controlador ter tido conhecimento do ocorrido, mas não há um prazo definido para comunicação aos titulares de dados pessoais. O prazo padrão de 72 horas para comunicação pelo controlador para as Autoridades Competentes após ter tido conhecimento do ocorrido parece alinhado com as melhores práticas internacionais e se coaduna com o princípio de transparência e responsabilidade ao fornecedor. De toda forma, nos parece que o prazo não deve ser absoluto e o controlador poderá apresentar justificativa fundamentada para apresentar a comunicação para as Autoridades Competentes em prazo superior.
8. Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	Entendemos que a forma mais adequada de comunicar os titulares de dados pessoais afetados sobre incidente de segurança constatado pode variar dependendo das características do caso concreto. A comunicação individualizada aos titulares de dados afetados é sempre preferível, na medida em que a mensagem efetivamente atingirá os titulares de dados afetados, sendo prestadas informações precisas sobre como foram afetados pelo incidente de segurança, bem como sobre as medidas mitigadoras de risco já adotadas pelo controlador, e sobre aquelas medidas mitigadoras adicionais que podem ser adotadas diretamente pelo titular, por exemplo a troca de senha ou a configuração de autenticação em dois fatores.

	Conforme demonstram evidências práticas, a informação individualizada terá mais atenção do titular se comparada a mensagem generalista divulgada em termos mais macros. Nesse sentido, veja-se como exemplo que o Serpro - Serviço Federal de Processamento de Dados desenvolveu, a pedido do Denatran - Departamento Nacional de Trânsito, uma solução tecnológica por meio da qual os proprietários de veículos são avisados diretamente sobre as campanhas de recall, por aplicativo, e-mail ou correspondência, de forma mais rápida, prática e efetiva, contribuindo, assim, para garantir maior segurança ao motorista, aumento nos índices de atendimento às campanhas e melhor gestão de serviços de recall pelas montadoras. Como a matéria objeto da presente consulta pública consiste, justamente, em incidentes de segurança envolvendo dados pessoais, na maioria dos casos o controlador dos dados objeto de incidente tem em mãos ao menos dados pessoais para contato com os titulares de dados afetados - o que lhe viabiliza enviar informe individual e qualificado aos titulares de dados afetados por determinado incidente. A título exemplificativo, as Orientações sobre a notificação de uma violação de dados pessoais ao abrigo do Regulamento (UE) 2016/679 estabelecem que “exemplos de métodos de comunicação transparente incluem o envio direto de mensagens (por exemplo, e-mail, SMS, mensagem direta), banner de notificação em websites proeminentes, comunicações postais e anúncios em destaque nos meios de comunicação impressos." Não obstante, reconhece-se que, em certas hipóteses atípicas e excepcionais, uma comunicação direta e individualizada ao titular afetado acerca de incidente de segurança poderá se mostrar inviável.). A forma mais adequada de comunicar poderá, nesses casos em que inviável comunicação individual qualificada, ser uma comunicação pública. Para referência, essa possibilidade residual (isto é, para os casos de inviabilidade de envio de comunicação individual qualificada) é aceita nesses termos no GDPR (art. 34 (3), c) e nas legislações de proteção de dados pessoais dos estados norte-americanos: nos casos em que a comunicação individual e direta aos titulares for impossível ante a ausência de informações para realização dessa comunicação, ou ainda envolver esforço desproporcional, tornando-se inviável, o GDPR e as legislações de proteção de dados pessoais dos estados norte-americanos permitem a adoção de comunicação pública através da qual os titulares de dados sejam informados acerca do incidente de maneira também eficaz.

	Constata-se, assim, que tanto o GDPR europeu como também as legislações de proteção de dados pessoais dos estados norte-americanos adotaram, a sistemática de informação aos titulares de dados afetados de forma individual prioritariamente, optando-se por comunicação de incidente via grande mídia apenas de forma subsidiária, em caso de impossibilidade ou de inviabilidade de informação individualizada aos titulares de dados afetados, nos termos acima expostos. Cumpre ressaltar que, no âmbito das legislações de proteção de dados pessoais dos estados norte-americanos, a despeito das diferenças existentes quanto a aspectos diversos, a opção prioritária por informação de incidente aos titulares de dados afetados de forma individualizada foi adotada por todas as leis estaduais, dos 50 estados norte-americanos. Assim, propõe-se que, em regulamento, a ANPD determine, como a regra geral, que a comunicação de incidente de segurança aos titulares de dados pessoais afetados seja realizada de maneira individual e direta a esses titulares. A comunicação pública deve ser considerada apenas em caráter secundário e excepcional, somente em caráter residual e quando a comunicação individual e direta aos titulares afetados mostrar-se impossível ante a ausência de informações para realização dessa comunicação por escrito, ou ainda envolver esforço desproporcional, tornando-se inviável. No que diz respeito à hipótese residual de comunicação de incidentes de segurança na mídia, propõe-se que seja adotada para sua instrumentalização (com as alterações pertinentes a fim de identificar que a matéria objeto de comunicação será incidente de segurança envolvendo dados pessoais), a norma objeto do artigo 4º da Portaria 618/2019 do Ministério da Justiça e Segurança Pública.
9. Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	O ICO estabelece que apenas vazamentos que possam gerar riscos prováveis aos titulares (independente do grau) devem ser reportados. Nesse sentido, esclarece que tais riscos são aqueles que podem resultar em discriminação, danos à reputação, perda financeira e desvantagens econômicas ou sociais significativas aos titulares. Para a autoridade canadense[7], nem todos os vazamentos devem ser reportados ao OPC. A lei exige notificação se for razoável acreditar que a violação cria um risco real de dano significativo a um

[7] Disponível em: https://www.priv.gc.ca/en/privacy-topics/business-privacy/safeguards-and-breaches/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/#_Part_1. Acesso em 18/03/2021.

	indivíduo (não importando a quantidade de titulares afetados quando há um risco real de dano significativo resultante da violação). Para a análise de risco, devem ser considerados: (i) a sensibilidade dos dados pessoais envolvidos na violação e (ii) a probabilidade de que os dados pessoais tenham sido ou serão utilizados indevidamente. Ou seja, há uma inclinação para que a obrigação dependa do risco para o titular (*risk-based approach*). Já na Califórnia, apenas os incidentes que atinjam mais de 500 pessoas devem ser notificados ao *Attorney General*, autoridade semelhante ao Ministério Público brasileiro. Além disso, a empresa responsável pelos danos causados aos titulares dos dados deve publicizar o incidente de maneira irrestrita, publicando o ocorrido em lista fornecida pelo *Attorney General*. Na maior parte dos casos, a exceção para que não seja notificado um incidente de segurança ocorre quando a violação não representa risco relevante para os direitos ou liberdades dos titulares. Entendemos que essa é a exceção adequada a ser adotada pela ANPD também. Não há critérios mais objetivos para referida exceção, que dependerá de julgamento do próprio controlador. No entanto, é importante que os responsáveis pelo tratamento registrem todos os incidentes, inclusive aqueles não reportados à autoridade pelo prazo de 05 (cinco) anos. Nesses casos, o relatório deve apresentar e provar que a violação não constitui risco relevante para os direitos e liberdades dos titulares.
10. Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	O art. 34 do GDPR estabelece que o titular de dados pessoais deve ser notificado pelo controlador, quando for afetado por incidente de segurança que importe alto risco para os direitos e liberdades do titular de dados pessoais em questão. Referido dispositivo também prevê exceções objetivas, em que fica expressamente dispensado o dever de notificação aos titulares de dados pessoais afetados por incidente, quais sejam, quando: (i) o controlador implementou medidas de proteção técnica e organizacional adequadas para proteger os dados pessoais antes do incidente de segurança, em particular aquelas que tornam os dados pessoais ininteligíveis para qualquer pessoa que não esteja autorizada a acessá-los (como criptografia); (ii) o controlador tomou medidas subsequentes que garantem que o alto risco para os direitos e liberdades dos titulares dos dados não é mais provável de

	se materializar (por exemplo, o controlador identificou rapidamente o incidente de segurança e tomou medidas imediatas contra o indivíduo que acessou os dados pessoais, antes de ser capaz de utilizar de qualquer forma os dados em questão). Assim, considerando que o envio de comunicações desnecessárias ao titular de dados pode causar desinformação e alarde desnecessário, além de fadiga (podendo o titular de dados perder a sensibilidade/atenção sobre quando tal comunicação é realmente importante), entendemos, respeitosamente, que a obrigatoriedade de comunicação ao titular de dados, à exemplo do previsto na GDPR e em consonância com a norma objeto do *caput* do art. 48 da LGPD, dever ocorrer quando um incidente de segurança for suscetível de resultar relevante risco ou dano os titulares de dados, incidindo, nesse sentido, também as exceções ao dever de informação aos titulares de dados pessoais afetados por incidente, conforme as excludentes nesse sentido previstas no artigo 34(3), *c* da GDPR, acima descritas e que se propõe sejam concretamente adotadas pelo regulamento da ANPD acerca do artigo 48 da LGPD.
11. Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	A análise aqui pretendida será restrita à indicação de critérios que podem, eventualmente, serem considerados para análise da gravidade de um incidente de segurança. Cabe salientar o fato de que, em que pese alguns destaques sejam dados a determinados critérios – em especial quando relacionados à letra expressa da LGPD –, todos os critérios e elementos aqui trazidos podem ser utilizados para análise nacional quanto à severidade do incidente de segurança previsto pelo art. 48. *European Union Agency for Cybersecurity – ENISA* Em suas recomendações, a ENISA considera, basicamente, três critérios para a análise da severidade de um incidente de segurança. São eles: *"**Data Processing Context (DPC)**: Addresses the type of the breached data, together with a number of factors linked to the overall context of processing.* ***Ease of Identification (EI)**: Determines how easily the identity of the individuals can be deduced from the data involved in the breach.*

	Circumstances of breach (CB)**: Addresses the specific circumstances of the breach, which are related to the type of the breach, including mainly the loss of security of the breached data, as well as any involved malicious intent."*[8] No que diz respeito ao contexto do tratamento de dados (Data Processing Context – DPC***), a ENISA sugere que sejam considerados dois fatores: **(i)** a natureza dos dados pessoais por categorias, as quais divide a ENISA em quatro hipóteses (simples; comportamental; financeira; e dados sensíveis); e **(ii)** consideração de fatores que possam influenciar na definição do contexto, como, por exemplo, volume de dados, características específicas do Controlador ou dos titulares de dados, se o dado já era público ou não e se o dado era ou não preciso[9]. Com relação à facilidade de identificação do titular (***Ease of Identification – EI***), traz o documento os graus de facilidade para identificação de um indivíduo proporcionados pelos dados pessoais envolvidos no incidente, ou seja, a ideia é analisar o quanto os dados pessoais relacionados ao incidente têm potencial de identificar um indivíduo de maneira inquestionável (*univocally*). Para tal, são quatro os graus considerados: **(i)** insignificante; **(ii)** limitado; **(iii)** considerável; e **(iv)** máximo. Para analisar o grau, sugere-se que sejam considerados tanto identificadores diretos quanto indiretos e que, a depender do contexto, mais ou menos informações poderão ser levadas em consideração para tal qualificação do grau. Além disso, sugere o documento que sejam considerados os meios razoavelmente disponíveis para tal identificação. Ainda, prezando pela abordagem contextual, o documento traz que deve se ter em mente que é possível que um mesmo identificador tenha pesos diferentes de acordo com cada contexto. Por último, no que se refere às circunstâncias do incidente (***Circumstances of Breach – CB***), indica-se que sejam considerados quatro cenários: **(i) Perda de Confidencialidade**: acesso indevido aos dados pessoais envolvidos; **(ii) Perda de Integridade**: quando há modificação ou substituição dos dados pessoais de maneira que possa prejudicar o titular de dados; **(iii) Perda de Disponibilidade**: quando o dado não pode mais ser acessado mesmo se necessário. Pode ser uma perda temporária ou perpétua; e

[8] ENISA. ***Recommendations for a methodology of the assessment of severity of personal data breaches***. *Working Document*. 2013. p. 9. Disponível em: https://www.enisa.europa.eu/publications/dbn-severity

[9] ENISA. ***Recommendations***. Op. Cit., p. 10.

	(iv) *Malicious Intent*: aqui se verifica se o incidente foi ocasionado por erro, por engano, ou se foi causado por má intenção. O art. 48, §3º, parece de grande relevância o critério referente à facilidade de identificação, pois estabelece que *No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.* Nesse sentido, se o fato de medidas terem ou não tornado os dados pessoais *ininteligíveis* é o elemento utilizado para o *juízo de gravidade do incidente*, a ***facilidade de identificação***, quando maior, mais deverá pesar para sua severidade. Parece, pois, ser esse um critério de grande importância à análise da gravidade de incidentes no âmbito da LGPD e que merece uma atenção diferenciada quando da consideração dos subsídios. É relevante também notar que os elementos trazidos para qualificar as circunstâncias do incidente estão diretamente relacionados aos elementos previstos pelo art. 46 da LGPD, que trata da obrigação dos agentes de tratamento em adotar medidas capazes de proteger os dados contra: *acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.* Assim, parece que considerar esse critério em análise nacional é também de grande importância. *Article 29 Data Protection Working Party – WP 29* No caso das *Guidelines*[10] adotadas pelo WP29, o grupo de trabalho decidiu reiterar a posição apresentada em sua Opinião 03/2014[11], quando categorizou os tipos de incidentes de segurança de acordo com a tríade amplamente conhecida da Segurança da Informação (*CIA – Confidentiality, Integrity and Availability*). O documento destaca que, a depender das circunstâncias do caso, as três espécies de incidente poderão estar envolvidas.

[10] Article 29 Data Protection Working Party. ***Guidelines on Personal data breach notification under Regulation 2016/679***. 2017. Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

[11] Article 29. ***Opinion 03/2014 on Personal Data Breach Notification***. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

	Destaca o grupo de trabalho que, nos moldes dos Considerandos 75 e 76 do Regulamento Geral de Proteção de Dados Europeu, a avaliação do risco à privacidade, normalmente, considera tanto a probabilidade de incidência do risco quanto a severidade de sua ocorrência, entretanto, destaca que, para o caso de análise de riscos à privacidade em situações de incidentes de segurança, já há a incidência de uma situação problemática, sendo, portanto, o foco voltado para a severidade da incidência, dos impactos causados aos titulares. São os critérios trazidos pelo WP29: **(i) O Tipo de Incidente**: o tipo de incidente considerando as espécies acima descritas, por exemplo, a perda de confidencialidade em casos em que a sensibilidade dos dados é alta pode ser um fato que aumente a severidade do incidente; **(ii) A Natureza, Volume e Sensibilidade dos Dados Pessoais**: deve-se considerar se os dados são sensíveis, financeiros, comportamentais e afins, qual a volumetria de dados pessoais envolvidos no incidente; **(iii) A Facilidade de Identificação**: assim como no tópico acima, o WP29 também estabeleceu a facilidade de identificação do titular por meio dos dados como um critério para análise da severidade do incidente; **(iv) A Severidade das Consequências para o Titular**: bastante relacionado com os outros critérios, aqui o WP29 decidiu considerar que as consequências possíveis aos titulares devem ser levadas em consideração para a análise quanto à severidade do incidente. Por exemplo, a depender da natureza dos dados pessoais envolvidos o incidente pode ser majorado e muito em sua severidade; **(v) Aspectos Específicos do Titular**: características do titular de dados, por exemplo, se é menor de idade, se, de alguma maneira, está em situação de vulnerabilidade e afins; **(vi) Aspectos Específicos do Controlador**: a depender da natureza do Controlador e dos tratamentos que realiza o incidente pode ser majorado em sua severidade; **(vii) O Número de Titulares Afetados**: relacionado, mas não igual, ao volume de dados pessoais tratados, o volume de titulares de dados afetados deve ser levado em consideração; e **(viii) Pontos Gerais**: por fim, sugere o WP29 que seja considerada a possibilidade de violação de direitos e liberdades individuais dos titulares em razão do incidente. Tal consideração deve levar em conta tanto o grau de impacto nesse sentido quanto a probabilidade de ocorrência de tal violação.

	Considerando os pontos acima dispostos, novamente, todos os critérios podem ser úteis à análise nacional quanto à gravidade de um incidente de segurança, entretanto, alguns chamam atenção pela relação com o que está expressamente previsto pela LGPD. De início, a categorização dos tipos de incidente por meio da tríade de Segurança da Informação, assim como no item anterior, também está diretamente relacionada ao que prevê o art. 46 da LGPD. Além disso, também como no item anterior, a facilidade de identificação, também trazida pelo WP29, serve como importante critério para análise relacionada ao incidente previsto pela LGPD. Como já mencionado, o §3º do art. 48 traz expressamente uma preocupação em tornar os dados ininteligíveis, o que tem relação tanto com a identificação do titular e, assim, quanto maior a facilidade de identificação causada pelo incidente, maior será sua gravidade. Também está relacionada a disposição trazida pelo §3º do art. 48 ao acesso aos dados, uma vez que a ideia de torná-los ininteligíveis é justamente para que não sejam acessados de maneira indevida, assim, o critério de perda de confidencialidade merece também sua parcela de atenção diferenciada. *Data Protection Commission – DPC* Em seu Guia Prático[12], a DPC, em 2019 sugeriu os seguintes critérios para análise da severidade de riscos envolvidos num incidente de segurança: **(i)** Natureza do Dado Pessoal; **(ii)** As circunstâncias do incidente (como ocorreu); **(iii)** Se o dado estava ou não protegido por medidas técnicas apropriadas como criptografia e pseudoanonimização; **(iv)** A facilidade proporcionada pelo incidente em identificar direta ou indiretamente os titulares de dados envolvidos; **(v)** A probabilidade de a pseudoanonimização ser revertida ou de ocorrer uma perda de confidencialidade; **(vi)** A probabilidade de fraude contra identidade, danos financeiros ou outras formas de uso indevido dos dados; **(vii)** Se o dado pessoal poderá ou provavelmente será utilizado com má intenção;

[12]Data Protection Commission ***A Practical Guide to Personal Data Breach Notifications under the GDPR***. 2019. Disponível em: https://www.dataprotection.ie/sites/default/files/uploads/2019-10/Data%20Breach%20Notification_Practical%20Guidance_Oct19.pdf

	(viii) A probabilidade de o incidente resultar em danos físicos, materiais e não materiais, bem como qual a severidade de tais possíveis danos; **(ix)** Se o incidente poderá resultar em discriminação, dano à reputação ou algum tipo de prejuízo a direitos e liberdades fundamentais dos titulares. Como se pode verificar, os critérios trazidos são, basicamente, iguais ou de grande correlação aos demais trazidos nos itens anteriores. Importante destacar que, quando se fala em analisar o fato de o dado pessoal estar ou não protegido por medidas apropriadas, bem como qual a probabilidade de reversão de medidas nesse sentido, não deve ser interpretado como uma análise de adequação do grau de segurança aplicado pelo agente de tratamento, ao menos não nesse momento de análise do grau de severidade do incidente. O critério ali indicado deve servir apenas para verificar a possibilidade de perda de confidencialidade e, portanto, possível acesso indevido aos dados, aumentando os impactos. Outrossim, há pontos relevantes trazidos por Daniel J. Solove em seu *A Taxonomy of Privacy*[13] que podem ser de grande utilidade para melhor entender os danos à privacidade que podem decorrer de um incidente de segurança, corroborando com elementos e critérios acima já trazidos e trazendo concepções que podem ser relevantes à análise da gravidade de um incidente em âmbito nacional, considerando a LGPD. Perda da Confidencialidade e a Natureza da Relação entre Agentes e Titulares de Dados Um primeiro ponto a ser trazido aqui, tratado por Solove, é o dano à privacidade decorrente de perda da confidencialidade. Tal dano tem bastante relação com a natureza dos titulares e natureza dos agentes, conforme acima explicado nos dois primeiro itens da Seção anterior. Além disso, esse conceito trazido por Solove possui grande relação com o incidente de segurança, uma vez que uma das espécies de incidente é justamente a perda da confidencialidade. Solove apresenta uma diferença entre *disclosure* e *breach of confidentiality*. A quebra de confidencialidade tem o dano pautado pela quebra de confiança e não pela divulgação dos dados em si. Atesta Solove que *"When people establish a relationship with banks, Internet service providers, phone companies, and other businesses, they are not disclosing their information to the world. They*

[13] SOLOVE, Daniel J. ***A Taxonomy of Privacy***. University of Pennsylvania Law Review. Vol. 154. No. 3. 2006. Disponível em: https://www.law.upenn.edu/journals/lawreview/articles/volume154/issue3/Solove154U.Pa.L.Rev.477(2006).pdf

	are giving it to a party with implicit (and often explicit) promises that the information will not be disseminated."[14] Assim, a depender da natureza da relação entre titulares e agentes, bem como a natureza de cada uma dessas partes, uma quebra de confidencialidade decorrente de um incidente de segurança pode ser mais ou menos severa, a depender das circunstâncias de cada caso. Assim, valendo-se dos conceitos trazidos por Solove e contando com os critérios acima explicados, ponto que merece atenção quando da análise da severidade de um incidente é a natureza da relação entre titulares e agentes, em especial, considerando a natureza dos agentes e dos titulares, a qual, a depender do caso, considerando uma perda de confidencialidade, pode majorar a gravidade do incidente ou não. <u>*Disclosure* e A Natureza dos Dados Pessoais</u> Ainda seguindo a ideia de diferenciar divulgação de perda de confidencialidade, Solove esclarece que a divulgação dos dados pessoais causa danos à privacidade em razão da disseminação de uma informação que, de certa maneira, pode trazer efeitos negativos ao titular. São suas palavras: *"Disclosure differs from breach of confidentiality because the harm in disclosure involves the damage to reputation caused by the dissemination; the harm with breach of confidentiality is the violation of trust in the relationship.289 Disclosure can harm even if the information is revealed by a stranger."*[15] Para Solove, a divulgação não está ligada à quebra de confiança, mas ao dano causado pela divulgação dos dados pessoais, independentemente de quem o faça. Sendo assim, o dano relacionado à divulgação tem muita relação com o incidente de segurança, no sentido de que, por meio de um incidente, há a divulgação dos dados indevidamente. Além disso, em consonância com o que foi trazido acima, o possível impacto causado pela divulgação está diretamente relacionado à natureza dos dados pessoais e características específicas dos titulares. A depender da informação divulgada, o dano pode ser muito maior ou menor. Em mesma linha, está o dano referente à exposição (*exposure*) explicada por Solove. É o que diz o autor:

[14] SOLOVE, Daniel J. ***A Taxonomy of Privacy***. University of Pennsylvania Law Review. Vol. 154. No. 3. 2006. p. 527. Consulta 19.03.2021. Disponível em: https://www.law.upenn.edu/journals/lawreview/articles/volume154/issue3/Solove154U.Pa.L.Rev.477(2006).pdf

[15] SOLOVE. Daniel J. Op. Cit., p. 529.

	"Exposure involves the exposing to others of certain physical and emotional attributes about a person. These are attributes that people view as deeply primordial, and their exposure often creates embarrassment and humiliation"[16]*.* Assim, considerando a relação do incidente com os danos extraídos do estudo de Solove, tanto para o dano referente à divulgação (*disclosure*) quanto para o dano relacionado à exposição dos dados (*exposure*), os critérios da natureza dos dados pessoais e das características específicas dos titulares e agentes devem ser levados em consideração para majoração ou não da gravidade do incidente. <u>Grau de Exposição</u> Daniel Solove explica, em seu *Taxonomy of Privacy*, por que o que chama de a*cessibilidade aumentada* deve ser considerada como um elemento danoso à privacidade: "*With increased accessibility, a difference in quantity becomes a difference in quality—it enhances the risk of the harms of disclosure"*[17]*.* Nesse sentido, um incidente de segurança pode causar um grande aumento do acesso a dados que, não necessariamente, precisaria ter toda a disponibilidade ocasionada pelo incidente. Portanto, tanto o volume dos dados, quanto o volume dos titulares e a natureza do incidente (por exemplo, se perda de confidencialidade), são critérios todos relacionados à possível majoração do dano referente ao grau de exposição explicado por Solove, o que por sua vez implica majoração da severidade do incidente.
12. Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	Além dos critérios acima indicados, que poderão ser utilizados para a análise dos possíveis riscos ou danos em si, traz-se, aqui, uma sugestão de método que pode ser adaptado à realidade brasileira de acordo com a definição dos critérios que serão, de fato, utilizados para análise da gravidade do incidente. <u>*European Union Agency for Cybersecurity – ENISA*</u>

[16] SOLOVE. Daniel J. Op. Cit. p. 533.
[17] SOLOVE. Daniel J. Op. Cit. p. 537.

	Conforme mencionado no item anterior, em suas recomendações, a ENISA considera três critérios para a análise da severidade de um incidente de segurança, quais sejam: **(i)** contexto do tratamento de dados (***Data Processing Context – DPC***); **(ii)** facilidade de identificação do titular (***Ease of Identification – EI***); e **(iii)** circunstâncias do incidente (***Circumstances of Breach – CB***)[18]. Com base nesses critérios, a ENISA propõe uma metodologia centrada no que chama de contexto do tratamento de dados, sendo esse o principal elemento da fórmula, contando com mais dois elementos complementares que devem ser somados e multiplicados ao contexto do tratamento. A fórmula, portanto, fica desta forma[19]: **SE = DPC x EI + CB** Onde ***SE*** representa a gravidade do incidente (*severity*), ***DPC*** representa o contexto do tratamento (*data processing context*), ***EI*** significa facilidade de identificação (*ease of identification*); e ***CB*** representa as circunstâncias do incidente (*circunstamces of the breach*). O resultado da análise poderá corresponder a quatro níveis de gravidade do incidente: **(i)** baixo; **(ii)** médio; **(iii)** alto; e **(iv)** muito alto. Diante dessa metodologia, um incidente de segurança pode ser considerado: **(i) de baixa gravidade se *SE < 2***: isso significa que os indivíduos não serão afetados ou poderão encontrar poucos inconvenientes, que superariam sem maiores problemas; **(ii) de média gravidade, se 2 =/< SE < 3**: ou seja, indivíduos encontram inconvenientes significativos que podem ser superados, apesar das dificuldades (custos extras, estresse, falta de entendimento, medo, negação de acesso a serviços etc.); **(iii) de alta gravidade, se 3 =/< SE < 4**: neste caso, são possíveis consequências significativas para os indivíduos que podem ser superadas com dificuldades consideráveis (dano material, perda de emprego, piora de saúde etc.); e **(iv) muito alta gravidade, se 4 =/< SE**: indivíduos podem se deparar com significativas ou até irreversíveis consequências, podendo não serem superadas (morte, doenças físicas ou psicológicas permanentes, dificuldades financeiras como dívidas ou incapacidade para trabalhar etc.).

[18] Para uma explicação dos critérios, por favor, verificar a resposta anterior.

[19] ENISA. ***Recommendations.*** Op. Cit., p. 9. Disponível em: https://www.enisa.europa.eu/publications/dbn-severity

	Para que se chegue aos resultados acima identificados, é necessário considerar quais serão os critérios utilizados dentro da metodologia e qual o peso de cada um. No referido documento, a ENISA sugere, em seus Anexos I, II e III, uma abordagem de acordo com a sua valoração dos critérios[20], entretanto, nacionalmente, para que se possa criar algo condizente à realidade da LGPD, tal valoração dos critérios só será possível uma vez tendo definidos, de fato, quais serão os critérios utilizados para análise da gravidade do incidente, conforme já explicado no item anterior. Assim, o que se buscou trazer aqui é um direcionamento para uma primeira versão de possível metodologia aplicável à análise da gravidade do incidente, devendo, claro, esta primeira versão ser detalhada uma vez definidos os critérios que serão utilizados para análise da gravidade e, ainda mais importante, seus pesos de acordo com o entendimento de critérios mais ou menos relevantes, ainda que tal carga seja fornecida de maneira subjetiva num primeiro momento e especificada de modo objetivo por meio do desenvolvimento da presente metodologia. https://www.enisa.europa.eu/publications/dbn-severity
13. Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	Após a comunicação pelos controladores de um incidente de segurança, a depender das informações enviadas à ANDP, poderia haver a determinação da realização de uma investigação adicional sobre as causas do incidente e sobre a existência de vulnerabilidades adicionais. É importante saber se o incidente foi causado por falha humana ou por um erro do sistema, de modo a prevenir problemas adicionais. Adicionalmente, a ANDP poderia solicitar relatório sobre incidentes, impactos e ações tomadas para mitigação dos danos e para proteção adicional dos dados. Esses são as medidas recomendadas pelo ICO do Reino Unido, para que as empresas tomem após incidentes. O procedimento adotado pela empresa é fundamental para garantir que não existem vulnerabilidades no sistema. Após a comunicação do incidente, a ANPD poderá exigir, de forma justificada e fundamentada, que o controlador: - apresente informações detalhadas sobre a origem e extensão do incidente; - apresente provas técnicas de que a vulnerabilidade que deu origem ao incidente foi sanada;

[20] ENISA. ***Recommendations.*** Op, Cit., p. 15-26. Disponível em: https://www.enisa.europa.eu/publications/dbn-severity

	- elabore relatório descritivo do incidentes, inclusive das providências tomadas e mantenha a documentação comprobatória até o encerramento do procedimento administrativo perante a ANPD.- apresente relatório periódico por um prazo determinado (3 meses, por exemplo), sobre as medidas de remediação adotadas, em especial no auxilio aos titulares; - apresente evidências de que estabeleceu e passou a adotar política de segurança e plano de resposta a incidentes, para evitar que novos incidentes ocorram. Poderão ser solicitados, por exemplo, documentos que evidenciem que a empresa adotou programa de treinamento dos funcionários, aplicou recursos para atualização de sua infraestrutura de segurança etc; - nos casos extremos e reincidentes, exigir auditoria e certificação dos sistemas de gestão de segurança da informação como por exemplo, normas ISO. - Sob o ponto de vista procedimental, o Ibrac entende que, em linha com as práticas adotadas pela Senacon em processos de chamamento (*recall*), a ANPD, na qualidade de órgão central para implementação da LGPD, coordenará e concentrará o procedimento de comunicação de incidente, envolvendo demais autoridades competentes, caso necessário e aplicável. Adicionalmente, o Ibrac também entende que a comunicação do incidente "per se" não configura ilícito administrativo. Em relação às medidas mitigadoras (ex: treinamento de funcionários), o Ibrac sugere que sejam caracterizadas como circunstâncias atenuantes em eventual procedimento administrativo sancionatório. De toda forma e, considerando que o objeto da presente tomada de subsídios não é o processo administrativo sancionatório, o Ibrac se coloca à disposição dessa DD. Agência para discussão e contribuição, oportunamente. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/ https://www.ftc.gov/system/files/documents/plain-language/pdf-0154_data-breach-response-guide-for-business-042519-508.pdf

SUGESTÃO DE NORMATIVO, SE HOUVER
Art. Xxxx ....
Art. Xxxx ....

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: Instituto Brasileiro de Defesa do Consumidor

CPF/CNPJ: 58.120.387/0001-08

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS **IMPORTANTE:** Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Comentários iniciais / introdução	O Idec (Instituto Brasileiro de Defesa do Consumidor) é uma organização não governamental, sem fins lucrativos, totalmente independente de governos, partidos políticos e empresas privadas, criada em 1987. A missão do Idec é promover a educação, a conscientização, a defesa dos direitos do consumidor e a ética nas relações de consumo. A meta do Instituto é contribuir para que todos tenham acesso aos serviços essenciais para o desenvolvimento social, consumo sustentável, saúde do planeta e a consolidação da democracia na sociedade brasileira. Entre as atividades desenvolvidas pelo Idec destacam-se a realização de pesquisas relacionadas à qualidade e segurança de produtos e serviços. Acompanhamos as legislações referentes às relações de consumo e a participação no seu processo de formulação, bem como a proposição de ações judiciais de caráter coletivo, quando necessário, sempre visando garantia e preservação de direitos a partir de duas pontas, se o direito já existe, defendemos, se não existe, pautamos a elaboração. Para gerar conhecimento e informar os consumidores, utilizamos, entre outros instrumentos, a Revista do Idec e portal do Idec (www.idec.org.br), além de campanhas de mobilização. A presente contribuição trata da Tomada de Subsídios da ANPD sobre regulamentação aplicável à comunicação a ser feita à Autoridade e ao titular de dados sobre a ocorrência de incidentes de segurança. É importante destacar que autoridades de proteção de dados das mais variadas jurisdições já se debruçaram sobre o tema, a título de exemplo:

	Colômbia[1], México[2], Costa Rica[3], Egito[4], Uruguai[5], Moldávia[6], Guernsey[7] e Vietnã[8]. Na presente contribuição, o Idec responde às questões trazidas pela ANPD à luz dos exemplos citados, assim como questões suplementares importantes para a consecução da autodeterminação informativa e do direito à informação, princípios garantidos tanto pela LGPD quanto pelo Código de Defesa do Consumidor.
Quando um incidente pode acarretar **risco ou dano relevante** ao titular? Que **critérios** devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	**Toda alteração no risco de uso indevido de dados deve ser considerada relevante. O que diferencia os riscos é o seu grau de severidade, não a sua relevância.** **Risco** (ou risco relevante), nesse sentido, deve ser considerado como todo e qualquer risco no plano financeiro, à personalidade, à privacidade, à saúde, à segurança, à liberdade política e de orientação sexual, a pessoas vulneráveis (idoso, criança e adolescente), que podem constranger, cercear ou impedir a fruição de direitos e liberdades. **Dano relevante**, de forma semelhante, é todo e qualquer dano no plano financeiro, à personalidade, à privacidade, à saúde, à liberdade política e de orientação sexual, a pessoas vulneráveis (idoso, criança e adolescente), que podem constranger, cercear ou impedir a fruição de direitos e liberdades. Critérios podem ser utilizados, contudo, para a diferenciação de graus de risco e dano: Critérios possíveis para diferenciar os **graus dos riscos**: ● **Tipo de incidente** (falha de segurança / exposição de dados / indício de extração / extração);

[1] Guía para la gestión de incidentes de seguridad en el Tratamiento de Datos Personales. Superintendencia de Industria y Comercio. Disponível em: <https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia_gestion_incidentes_dic21_2020.pdf>
[2] Recomendaciones para el Manejo de Incidentes de Seguridad de Datos Personales. INAI - Instituto Nacional de Transparencia Acceso a la Información y Protección de Datos Personales. Disponível em: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/Recomendaciones_Manejo_IS_DP.pdf
[3] Reglamento a la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales. N° 37554-JP. Disponível em: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=74352
[4] Personal Data Protection Law No.151 of 2020. Disponível em: <https://www.dataguidance.com/notes/egypt-data-protection-overview>
[5] Decreto N° 64/020. Reglamentación de los artículos 37 a 40 de la Ley 19.670 y artículo 12 de la Ley 18.331, referente a Protección de Datos Personales. <https://www.impo.com.uy/bases/decretos/64-2020>
[6] Governmental Decision No. 1123 of 14 December 2010 on the approval of the requirements for the assurance of personal data security and their processing within the information systems of personal data. Disponível em : <http://old.datepersonale.md/file/hotariri/cerinte_securitate%20eng_101228.pdf>
[7]Guidance: personal data breach reporting. The Office of the Data Protection Authority (ODPA). Disponível em: <https://www.odpa.gg/information-hub/organisations/handling-data-breaches/list-page-guidance-on-personal-data-breach-reporting/>
[8] Decree 15/2020/ND-CP. Disponível em: <https://www.dataguidance.com/notes/vietnam-data-protection-overview>

	● **Perfil e quantidade de dados** (natureza, sensibilidade e volume de dados pessoais); ● **Tipo de serviço e características especiais do controlador** de dados (p.e. serviço público, aplicação de internet com milhões de usuários); ● **Uso posterior** à extração dos dados; ● Número de **indivíduos afetados**; ● Facilidade para **identificação do titular;** ● **Severidade das potenciais consequências para os titulares**: dano no plano financeiro, à personalidade, à privacidade, à saúde, à liberdade política e de orientação sexual, a pessoas vulneráveis (idoso, criança e adolescente), que podem constranger, cercear ou impedir a fruição de direitos. Em relação a critérios específicos para avaliação de grau de **dano para titulares**, podem ser considerados os seguintes critérios adicionais, sem prejuízo de outros: ● Dano para sua saúde, segurança física ou psicológica ● Extorsão econômica ou sexual ● Roubo de identidade ● Perda financeira ● Negação de crédito ou seguro ● Criação de perfis para fins ilícitos ● Perda de negócios ou oportunidades de emprego ● Discriminação ● Humilhação, perda de dignidade e danos à reputação
O risco ou dano relevante deveria ser **subdividido** em mais categorias (ex. Baixo, médio, alto, etc)? Como **distinguir** os níveis? Risco ou dano baixo deve ser considerado **relevante** ou não relevante?	É salutar e razoável que sejam criados graus diferentes para risco e dano. Contudo, é importante salientar que **TODO RISCO AO TITULAR É RELEVANTE**, o que os diferencia é o **GRAU DO RISCO**, e as **MEDIDAS ESPECIAIS/ADICIONAIS** que devem ser tomadas em casos de riscos médio e alto. Dessa forma, a **diferenciação em graus de risco NÃO PODE SER UTILIZADA PARA CERCEAR O DIREITO À INFORMAÇÃO DO TITULAR** sobre riscos de incidentes de segurança, em cumprimento ao disposto no Art. 6º, incisos I e III, do Código de Defesa do Consumidor.

	Além dos critérios utilizados para a valoração dos graus de risco (acima detalhado), sugerimos abordagem a partir de alguns critérios gerais para mensuração do grau de risco: ● **Risco alto** deve ser considerado, ao menos, aquele incidente que envolve dados sensíveis (seja o dado sensível coletado ou inferido a partir de dados não sensíveis), dados financeiros, dados utilizados para realização de perfilizações, dados em grandes dimensões que revelem características de coletividades, dados de idosos ou dados de crianças e adolescentes, ou grande base de dados sobre o titular. ● **Risco médio**: incidente que não envolva grande base de dados sobre o titular e não envolva dados pessoais sensíveis. ● **Risco baixo**: incidente que não envolva grande base de dados, dados sensíveis e se circunscreva a dados que são anonimizados no início do tratamento - exceto quando envolver dados sensíveis, financeiros, perfilizações ou revelarem conhecimento sobre grandes coletividades (atributos que envolvem alto risco, mesmo se posteriormente anonimizados).
Como **distinguir o risco ao titular do dano ao titular**? Como esses conceitos se relacionam?	**Risco** é o dano potencial, com qualquer grau de severidade. **Dano** é o prejuízo ou dano material ou moral objetivo, individual e coletivo, com qualquer grau de severidade.
O que deve ser considerado na **avaliação dos riscos** do incidente?	Os elementos básicos para avaliação do grau de risco, sem prejuízo de outros, devem ser os seguintes: ● **Tipo de incidente** (falha de segurança / exposição de dados / indício de extração / extração); ● **Perfil e quantidade de dados** (natureza, sensibilidade e volume de dados pessoais); ● **Tipo de serviço e características especiais do controlador** de dados (p.e. serviço público, aplicação de internet com milhões de usuários); ● **Uso posterior** à extração dos dados; ● Número de **indivíduos afetados**; ● Facilidade para **identificação do titular;** ● **Severidade das potenciais consequências para os titulares**: dano no plano financeiro, à personalidade, à privacidade, à saúde, à liberdade política e de orientação sexual, a pessoas vulneráveis (idoso, criança e adolescente), que podem constranger, cercear ou impedir a fruição de direitos.

Quais **informações** os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	Além das informações descritas no §1º do art. 48 da LGPD devem ser comunicadas à ANPD: (1) A **hora** e a **data** em que a investigação do incidente começou; (2) A descrição detalhada de **como o incidente ocorreu**; (3) Os **sistemas** de tratamento de dados **comprometidos**; (4) A **pessoa ou as pessoas designadas** para prestar mais informações à ANPD. Além disso, devem ser enviadas as seguintes informações complementares, especificamente em relação à garantia do direito à informação dos titulares: (5) os meios e formas utilizados para a **comunicação do incidente diretamente aos titulares**; (6) os meios e formas utilizados para a **comunicação pública** do incidente; (7) os **canais de comunicação a serem disponibilizados** para que os titulares possam obter **mais informações** sobre o incidente, os **riscos** envolvidos, os **cuidados** específicos de segurança a serem tomados pelos titulares para evitar golpes e fraudes, entre outros danos; (8) os meios e instrumentos para que os titulares **solicitem reparação de danos**, caso ocorram. Em alguns casos, pode ser apropriado notificar instituições como seguradoras, instituições financeiras, autoridades policiais ou centros de resposta a incidentes, entre outros, para que a informação sobre o incidente seja compartilhada e para que essas instituições também possam agir, zelar pelos direitos e apoiar titulares afetados.
Qual o **prazo razoável** para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	O prazo máximo para que os controladores **informem a ANPD** sobre incidentes de segurança deve ser de **no máximo 48h**, em sintonia com os prazos estabelecidos no no § 1º do art 18 do Decreto 9.936/2019, que regulamenta a Lei 12.414/2011 (Lei do Cadastro Positivo). Em caso de **risco alto para o titular**, a comunicação à ANPD deve ser feita **em até 24h**.
Qual seria um **prazo razoável** para que os controladores informem os titulares de dados sobre o incidente de segurança?	A comunicação aos titulares deve ser feita **de forma imediata**, em sintonia com os prazos estabelecidos no § 3º do Art. 18 do Decreto 9.936/2019, que regulamenta a Lei 12.414/2011 (Lei do Cadastro Positivo) e com o disposto no Art. 6º, incisos I e III, do Código de Defesa do Consumidor.

(art. 48, §1º) Que **informações** devem constar dessa comunicação? As mesmas do §1º do art. 48?	Ressaltamos que, em cumprimento ao princípio de prestação de contas, além dessa primeira comunicação aos titulares, devem ser realizadas outras comunicações quando o controlador já tiver informações mais concretas sobre o incidente, acerca das investigações em andamento e sobre a exposição dos dados envolvidos na violação, disponibilizando ao titular um relatório final acerca do ocorrido. Portanto, além das informações descritas no §1º do art. 48, deve ser comunicado aos titulares: (1) **os canais diretos de comunicação** da empresa ou do poder público a serem disponibilizados para que os titulares possam obter mais informações sobre o incidente, com a disponibilização de canais específicos para o atendimento da demanda online (numa aba específica do site ou endereço próprio) e por telefone (telefone específico ou ramal exclusivo); (2) os **riscos ao titular** e os **cuidados específicos a serem tomados** para evitar golpes e fraudes; (3) os meios e instrumentos para que os titulares **solicitem reparação de danos**, caso os mesmos ocorram.
Qual a **forma mais adequada** para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	A comunicação deve sempre **conjugar ações diretas e individuais com ações de comunicação pública**. Esta é a forma mais eficaz de garantir o direito à informação dos consumidores, pilar do CDC (art. 6º, III)e da LGPD (arts. 6º, IV, e 18). Reafirma-se que, **se for diagnosticada qualquer alteração no nível de risco, é direito dos titulares dos dados serem informados**, especialmente se envolver relações de consumo. Para comunicação direta, a depender dos dados pessoais disponíveis, devem ser enviados **email**, **SMS e aplicativo de mensageria privada**. Em caso de aplicações de internet, ou do uso destas para a oferta de serviços, devem ser utilizados **avisos e notificações obrigatoriamente visualizáveis pelo titular**. Em caso de serviços continuados, deve-se utilizar as **contas de consumo** como instrumento auxiliar. Em caso de graves riscos, deve ser utilizado mecanismo complementar por meio de **via postal registrada**. Para comunicação pública, devem ser utilizados, em todo os casos, **comunicado amplo e visível em website** e **nota distribuída à imprensa**, além de disponibilização do **contato do encarregado de forma visível**. Em casos de maior gravidade, além desses instrumentos, devem ser utilizados **anúncios em jornal** e, especialmente, no **rádio e televisão abertas**. Em todos os casos, os **canais de atendimento ao consumidor**, como o SAC, devem ter capacidade de esclarecer dúvidas sobre os incidentes e registrar as demandas dos consumidores em relação ao tratamento de seus dados pessoais. É importante que se tenha um canal de comunicação não-digital (como telefone ou ramal específico) para viabilizar o

	acesso à informação para todos os afetados.
Quais seriam as **eventuais exceções da obrigatoriedade** de informar a ANPD?	As exceções devem ser exclusivamente os incidentes que não geram riscos para os usuários, como as tentativas mal sucedidas de invasão de sistemas, os falhas de segurança com a garantia de não extração dos dados. Se há risco efetivo, em qualquer grau, é direito dos titulares obterem informações plenas sobre os incidentes. Contudo, reitera-se que, embora seja impossível e tampouco salutar que a ANPD seja notificada de todos os incidentes de segurança, e que nem todos os registros de casos enviados à ANPD também sejam notificados aos titulares, que a ANPD deve se munir de dados para avaliar o cenário geral em relação aos incidentes, para aprimorar as políticas públicas de proteção de dados. Nesse sentido, além de incidentes que gerem riscos aos titulares, devem ser notificados incidentes relevantes que de alguma maneira sejam úteis para o cumprimento da missão institucional da ANPD. Sugere-se que a ANPD crie um modelo de formulário para ajudar a registrar as informações que forem consideradas necessárias, inclusive para que a ANPD e os membros do Conselho Nacional de Proteção de Dados possam inspecionar esses registros posteriormente.
Quais seriam as **possíveis exceções** da obrigatoriedade de informar os titulares?	**Os titulares devem ser informados em todos os incidentes que gerem risco ao titular, em qualquer grau, em cumprimento ao** disposto no Art. 6º, incisos I e III, do Código de Defesa do Consumidor, a saber: Art. 6º São direitos básicos do consumidor: I - a proteção da vida, saúde e segurança contra os **riscos provocados por práticas no fornecimento de produtos e serviços considerados perigosos ou nocivos**; II - a educação e divulgação sobre o consumo adequado dos produtos e serviços, asseguradas a liberdade de escolha e a igualdade nas contratações; III - **a informação adequada e clara sobre** os diferentes produtos e serviços, com especificação correta de quantidade, características, composição, qualidade, tributos incidentes e preço, bem como s**obre os riscos que apresentem**;

Quais são os possíveis **critérios** a serem adotados pela ANPD na análise da **gravidade** do incidente de segurança? (art. 48, §2º)	Os critérios a serem adotados pela ANPD na análise do incidente de segurança podem ser os seguintes, em linha com as recomendações do Working Party 29 (GDPR/UE - WP250[9]): 1. Tipo de vazamento, 2. Natureza, sensibilidade e volume de dados pessoais; 3. Nível de facilidade de indicação dos indivíduos; 4. Severidade das consequências do incidente para os indivíduos; 5. Características especiais do indivíduo; 6. Características especiais do controlador e/ou controlador (poder público, birô de crédito, etc); 7. Número de indivíduos afetados; 8. Questões gerais Os critérios a serem adotados pela ANPD na análise do incidente de segurança podem ser os seguintes, em linha com as recomendações da *Superintendencia de Industria y Comercio (SIC)*[10] da Colômbia: Quanto aos titulares: 1. Quantas pessoas foram afetadas? 2. Que categoria de pessoas foi afetada? 3. Quais são as características especiais das pessoas afetadas? Por exemplo: crianças e/ou adolescentes; pessoas em estado de vulnerabilidade; idosos; funcionários sindicalizados, etc. Quanto aos dados pessoais: 1. Qual foi o volume de dados afetado? 2. Qual foi o período durante o qual os dados foram afetados ou comprometidos? 3. Que tipo de informação pessoal foi afetada? Por exemplo, identificação pessoal, dados biométricos, histórico médico, dados genéticos, testes acadêmicos, registros de localização, endereços IP, mensagens de texto, informações financeiras e de crédito, dados genéticos, perfis comportamentais, pontuação de crédito, etc. 4. Quão sensível é a informação comprometida? Por exemplo: dados sobre crianças e / ou adolescentes; dados biométricos, genéticos ou de saúde; perfis de comportamento; resultados de decisão automatizados; orientação sexual; dados políticos; etc. 5. Qual é o contexto das informações pessoais comprometidas? 6. As informações pessoais foram devidamente criptografadas e anonimizadas? Estavam inacessíveis? 7. Como as informações pessoais afetadas podem ser usadas? 8. Existe um risco de maior exposição de informações pessoais?

[9] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052
[10] https://www.sic.gov.co/sites/default/files/files/Publicaciones/Guia_gestion_incidentes_dic21_2020.pdf

	9. As informações pessoais estão publicamente disponíveis na Internet? 10. As informações pessoais podem ser utilizadas para fins fraudulentos ou podem causar qualquer tipo de dano material e/ou imaterial ao titular? 11. As informações pessoais foram recuperadas? Quanto à organização 1. O que causou o incidente de segurança? 2. Quando e com que frequência ocorreu o incidente de segurança? 3. Este é um problema sistêmico ou isolado? 4. Qual foi o escopo do incidente de segurança? 5. Que medidas foram tomadas para mitigar os danos? 6. Quais são as atividades e operações realizadas pela organização? Por exemplo: entidades financeiras, entidades públicas, provedores de aplicativos móveis, escolas, farmácias, hospitais, lojas de roupas, operadores de informações, provedores de mídia social, etc. 7. Os dados comprometidos afetarão as transações que a organização deve realizar com terceiros externos?

Quais seriam **sugestões de providências**, incluindo medidas técnicas e administrativas, a serem determinadas pela **ANPD** aos controladores após a comunicação do incidente de segurança?	De uma forma geral, é necessário que a Autoridade determine medidas que tanto apliquem as sanções ao caso concreto, como permitam a mitigação dos riscos e danos e a realização dos vários princípios elencados na LGPD, inclusive permitindo ao consumidor se defender dos eventuais riscos e mitigar seus danos, além de pedir o ressarcimento dos danos sofridos. Por isso, recomenda-se à ANPD a possibilidade de adoção das seguintes providências, sem prejuízo de outras: ● Determinar elaboração de relatório final detalhado, contendo a violação de segurança e as medidas tomadas, e que não ultrapasse duas semanas para ser elaborado, a fim de não perder detalhes importantes sobre o que foi aprendido, podendo inclusive ser compartilhado com entidades de defesa de direitos do consumidor, conforme elencado na Lei da Ação Civil Pública. O relatório deverá conter, no mínimo, (i) descrição detalhada do incidente de segurança com comunicação ao titular e demais comunicações pós-incidente; (ii) lista de quem foi afetado e providências tomadas; (ii) se teve algum pedido de ressarcimento de dano; (iii) expectativa dos danos sofridos pelos titulares e pela sociedade. ● Criar um Fundo específico na empresa, reservando montantes para pagamento de ressarcimento e danos individuais e coletivos, materiais e morais, dos consumidores e titulares afetados. ● Determinar ao controlador/operador que simule o incidente que levou à implementação das medidas de segurança, para confirmar que novos controles podem evitar que um incidente semelhante volte a acontecer. Em caso de nova falha, a implementação deve ser corrigida. ● Criar um histórico que permita que os responsáveis por respostas a incidentes tenham uma base de conhecimento, que pode ser usada para treinar usuários ou novos membros da equipe de resposta a incidentes. ● Determinar o cumprimento de obrigações de fazer e não fazer, prevendo multas em caso de descumprimento. ● Determinação de contratação de apólice de seguro. ● Determinação para arcar com os custos referentes a monitoramento de crédito e do uso indevido de informações e dados pessoais dos consumidores/titulares.

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec)

CPF/CNPJ: 30.858.409/0001-04

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS **IMPORTANTE:** Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	Algumas balizas podem ser traçadas na avaliação de risco ou dano pela ANPD diante de um incidente de segurança. Ainda que seja recomendável que sejam traçados critérios objetivos, do ponto de vista organizacional, para que o controlador faça a avaliação de risco de um incidente de segurança que diga respeito à proteção de dados, bem como que a ANPD também estabeleça um fluxo procedimental objetivo, a observação das notificações de incidente por parte da Autoridade deve ser realizada caso a caso, restando espaço para avaliação descritiva. Uma dupla função reforça a recomendação: a notificação do controlador pode incorrer em erro de avaliação, mensurando como baixo um risco ou dano efetivamente maior. Logo, a avaliação deverá ser validada pela Autoridade para um fiel dimensionamento. Ademais, o repertório de

	incidentes de segurança tende a ser variável e depende das superfícies de ataque disponíveis em um dado momento, bem como das técnicas de invasão e segurança empregadas ao tempo do incidente (uma tecnologia de proteção ao sigilo, por exemplo, por deixar de ser segura em um dado intervalo de tempo, gerando um risco superveniente). É necessário pontuar que o incidente é relevante ao titular, para fins de avaliação pela ANPD, se envolver, necessariamente, dados pessoais. É importante que o controlador saiba diferenciar entre incidentes de segurança que devem ser comunicados à ANPD e os incidentes de segurança da informação que devem ser comunicados a Centros de Tratamento e Respostas a Incidentes de Segurança (e.g. CERT.br ou CTIR Gov). A diferenciação, se bem delimitada pelo controlador, tem o poder de desafogar órgão de notificações cuja resposta não esteja em sua competência, bem como delimitar as expectativas do titular em relação à Autoridade. Além disso, a avaliação de risco e dano deve levar em conta unicamente as chances de danos/danos efetivamente identificados aos direitos dos titulares. A título de risco ou dano, aqui, deve ser considerada a amplitude de direitos fundamentais conexos à proteção de dados pessoais. Deverá cobrir a possibilidade de danos imateriais, como morais ou psicológicos/emocionais

	(discriminação, difamação, prejuízos à reputação); materiais (perda ou dano à propriedade), ou à integridade física (como danos à saúde, agressão física ao risco de morte). Uma leitura expansionista no que diz respeito aos direitos dos titulares também avaliaria a possibilidade do incidentes de segurança poderem provocar situações de calamidade pública (e.g. prejuízos ao suprimento de energia de uma região) ou riscos à segurança nacional (e.g. nome e endereços de agentes da inteligência infiltrados). Quaisquer camadas de danos aos direitos dos titulares são igualmente relevantes para o pronto envolvimento da ANPD. Um incidente pode acarretar um risco ou dano quando é acompanhado de razoável probabilidade de ameaçar direitos dos titulares dos dados. A probabilidade será analisada caso a caso e terá como pontos de partida a descrição do ocorrido, as medidas assecuratórias e de mitigação de riscos tomadas antes e depois do incidente (à luz do Relatório de Impacto à Proteção de Dados Pessoais e dos termos da notificação do incidente de segurança), considerando a natureza dos dados, escopo e termos do tratamento. Dado o período inaugural das atividades da ANPD, é importante pontuar que a métrica da relevância do incidente pode ser mais garantista/extensiva. Isso porque a mensuração dos impactos à

	proteção de dados ainda estão em fase de amadurecimento, em termos administrativos, bem como a cultura organizacional e empresarial sobre a proteção de dados no País, a qual, certamente, tenderá a subnotificação. Essa abordagem busca provocar uma atuação mais garantis ta à ANPD, tendo em vista a centralidade do titular dos dados na dinâmica da notificação de incidentes.
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	Consideradas as diferentes gradações de bens jurídicos lesados por incidentes de segurança de naturezas distintas, considerado contexto social, econômico, tecnológico e político, sugere-se que a subdivisão de categorias de risco ou dano seja feita em termos de baixo, médio, alto e altís simo. Para isso, a título de mensuração da categoria do dano, critérios quantitativos e qualitativos deverão ser aplicados uma vez que a gradação não se dá exclusivamente pela quantidade de titulares ou dados vazados, tampouco apenas pela natureza dos dados ou do vazamento. Portanto, cri térios quali tativ os podem envolver os direitos e liberdades dos titulares dos dados potencialmente lesados: como patrimônio, liberdade de expressão, incolumidade física, não-

	discriminação, entre outros. Para isso será necessário identificar a natureza dos dados vazados: como nome e sobrenome, endereço de email, número de telefone, endereço residencial, dia de nascimento, origem étnica ou racial, opiniões políticas, identidade cultural ou social, crenças religiosas, dados genéticos e/ou biométricos, entre outros. Ainda no campo dos critérios qualitativos, será importante identificar a natureza do vazamento de dados: (i) se foi acidental ou malicioso; (ii) se visa obter vantagem econômica ou política (caso possível a identificação); (iii) ou se compromete a confidencialidade, a integridade ou a disponibilidade dos dados. Como critérios quantitativos, será fundamental equacionar o alcance do vazamento, envolvendo, em primeiro plano, a quantidade de dados vazados, bem como a quantidade de titulares em situação de risco ou dano. Feitas as considerações preliminares, a subdivisão pode se dar observados ao seguintes critérios: • Baixo: mediante teste de hipóteses de risco ou dano - realizado de forma objetiva e que sejam demonstráveis pelo

	controlador, considerados sobretudo as medidas tomadas para mitigação - que resultem em baixa probabilidade de violação aos direitos dos titulares. • Médio: considerados critérios qualitativos e quantitativos de mensuração do risco ou dano, o nível médio poderia abarcar danos de natureza imaterial, como psicológica/emocional (e.g. difamação ou prejuízos à reputação) e material/patrimonial (e.g. danos à propriedade). Frise-se que, a depender da equação aplicada, considerando, por exemplo, a extensão dos titulares dos dados ou a natureza dos dados vazados, a extensão do risco ou dano imaterial ou material pode ser considerada de nível alto. • Alto: chances de risco ou dano de gradação alta são consideradas aquelas que geram prejuízos de natureza imaterial ou material em proporções mais elevadas em comparação. Além disso, risco ou dano à integridade física dos titulares dos dados, resultando em riscos de agressão, danos à saúde ou ao bem-estar físico do titular dos dados. Também seriam considerados os vazamentos de dados sensíveis, envolvendo riscos de discriminação, perseguição e

	outras formas de preconceito de natureza socioeconômica, religiosa, política, de gênero, orientação sexual, entre outras. Importante frisar que, mais uma vez, a mensuração é feita caso a caso e os critérios qualitativos e quantitativos serão de maior ou menor importância. Isso quer dizer que, por exemplo, para os casos de risco à integridade física ou vazamento de dados sensíveis, a extensão da quantidade de titulares afetados teria como “piso” a categoria de risco ou dano alto, podendo se elevar a altíssimo. • Altíssima: incidentes de segurança que envolvam dados pessoais e que incorram em riscos ao Estado e à ordem pública, incluindo casos de calamidade pública de distintas naturezas (e.g. suprimento de energia, segurança e saúde pública), bem como riscos à segurança nacional, como percebidos em dinâmicas de ciberguerra e exploração de vulnerabilidades em sistemas governamentais e privados de interesse público por agentes internacionais ou a serviço desses. Uma vez mais, o rol não é taxativo e deve ser observado caso a caso. Logo, a depender da equacionalização do incidente ad hoc, em conjunto com os critérios quantitativos e qualitativos, risco ou dano envolvendo uma quantidade baixa de titulares também poderá ser

	percebida como de altíssimo grau (e.g. violação de banco de dados sobre indivíduos protegidos em programas de proteção à testemunha ou outras hipóteses de riscos à integridade física que possam levar à morte do titular). Por fim, no que se refere à relevância de risco ou dano baixo, recomenda-se que os incidentes que se encaixem nessa categoria sejam, ainda, considerados relevantes em função de duas razões: historicamente, há uma notável tendência à subnotificação por parte dos controladores, seja por imperícia, negligência, imprudência ou receio de danos à reputação empresarial. Em segundo lugar, mostra-se necessário a notificação de casos de gravidade baixa para fins estatísticos, considerando que as atividades da Autoridade Nacional de Proteção de Dados se encontram em fase de amadurecimento, sendo necessária a extração e produção de inteligência sobre a cultura de proteção de dados no Brasil.
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	A regulação baseada no risco é proveitosa para realizar a medição do horizonte da possibilidade de danos aos titulares, uma vez que, em primeira análise, por em risco já deve ser considerado fato suficientemente relevante para fins de

	notificação, tomada de medidas de precaução, mitigação das possibilidades de outros danos e responsabilização. Trabalha-se, portanto, com vistas a medir o potencial de impacto ao mesmo tempo em que é visada a proteção do titular. Ou seja, o risco gera um dano virtual que, ainda que esteja no campo da potencialidade, já frustra a expectativa do titular quanto à coleta, tratamento, armazenamento e descarte de seus dados. Entende-se a opção do legislador em diferenciar categorias distintas ao apresentar a lesão como “risco ou dano”, como forma de distinguir um dano materializado consequência do incidente de segurança e distinto daqueles conexos ao próprio risco (e.g., vazados os históricos de pesquisa de uma aplicação de buscador e utilizados para chantagear o titular, ensejando em mais extensas esferas de dano moral e de dano patrimonial). Mas, para fins de observância e aplicação da lei, o dano baseado no risco é o gatilho gerador de responsabilidade, dever de notificar e medidas de mitigação, uma vez que, diante de incidente de segurança, um dano de caráter moral já pode ser identificado dada a violação da privacidade e, especificamente, da erosão da autodeterminação informativa e da livre formação da personalidade, bem como dos direitos a ela conexos. Ademais, a abordagem do dever de responsabilização baseada no risco encontra respaldo na jurisprudência consumerista e trabalhista,

	por exemplo (e.g. ver o entendimento do Superior Tribunal de Justiça, Tribunal Superior do Trabalho). Para a avaliação dos riscos é fato que deve haver a obrigação da notificação por parte dos controladores. Não é obrigatória a notificação quando é improvável que a violação resultará em risco para os direitos e liberdades pessoais. Contudo, é necessário ter em mente que, a partir do momento em que recebe a informação de que houve incidente de segurança envolvendo dados pessoais, é vital que o controlador não apenas procure conter o incidente, bem como avalie os riscos que podem resultar dele. Ele precisa saber a probabilidade e a gravidade potencial do impacto sobre o indivíduo, para que tome medidas mais eficazes, além de avaliar a necessidade de envio da notificação tanto para a ANPD, quanto para os titulares de dados envolvidos. Ressalte-se que a obrigatoriedade de notificação de incidente só é relativizada em casos claros de que não houve violação dos direitos e liberdades dos indivíduos envolvidos. Ademais, o risco pode levar tanto a danos físicos, materiais, quanto imateriais para os titulares dos dados envolvidos no incidente de segurança. Por isso, a avaliação deve ser feita de modo a considerar todos os eventos hipotéticos, além dos eventos que

	já ocorreram e os que, com maior probabilidade, irão ocorrer. É recomendável, portanto, que o grupo de gestão de riscos coordenado pelo controlador, tenha à disposição profissionais destacados que possam sugerir, a partir de repertórios técnicos e de engenharia social, quais eventos resultantes do incidente de segurança estariam no horizonte do vazamento. Por fim, vale trazer à baila as diretrizes da GDPR, 8 pontos que servem de parâmetro para o procedimento brasileiro, quais sejam: (1) o tipo de violação; (2) a natureza, sensibilidade e volume dos dados pessoais; (3) a facilidade de identificação das vítimas; (4) a severidade das consequências para as vítimas; (5) as características individuais; (6) características especiais dos dados; (7) o número de vítimas envolvidas e (8) a possibilidade de impacto aos direitos e liberdades individuais.
O que deve ser considerado na avaliação dos riscos do incidente?	Para a avaliação dos riscos é fato que deve haver a obrigação da notificação por parte dos controladores. Não é obrigatória a notificação quando é improvável que a violação resultará em risco para os direitos e liberdades pessoais. Contudo, é necessário ter em mente que, a partir do momento em que recebe a informação de que houve incidente de segurança envolvendo dados pessoais, é vital que o controlador não apenas procure conter o incidente, bem como

	avalie os riscos que podem resultar dele. Ele precisa saber a probabilidade e a gravidade potencial do impacto sobre o indivíduo, para que tome medidas mais eficazes, além de avaliar a necessidade de envio da notificação tanto para a ANPD, quanto para os titulares de dados envolvidos. Ressalte-se que a obrigatoriedade de notificação de incidente só é relativizada em casos claros de que não houve violação dos direitos e liberdades dos indivíduos envolvidos. Ademais, o risco pode levar tanto a danos físicos, materiais, quanto imateriais para os titulares dos dados envolvidos no incidente de segurança. Por isso, a avaliação deve ser feita de modo a considerar todos os eventos hipotéticos, além dos eventos que já ocorreram e os que, com maior probabilidade, irão ocorrer. É recomendável, portanto, que o grupo de gestão de riscos coordenado pelo controlador, tenha à disposição profissionais destacados que possam sugerir, a partir de repertórios técnicos e de engenharia social, quais eventos resultantes do incidente de segurança estariam no horizonte do vazamento. Por fim, vale trazer à baila as diretrizes da GDPR, 8 pontos que servem de parâmetro para o procedimento brasileiro, quais sejam: (1) o tipo de violação; (2) a natureza, sensibilidade e volume dos dados pessoais; (3) a facilidade de identificação das vítimas; (4) a

	severidade das consequências para as vítimas; (5) as características individuais; (6) características especiais dos dados; (7) o número de vítimas envolvidas e (8) a possibilidade de impacto aos direitos e liberdades individuais.
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	As informações dadas pelo art. 48 da LGPD afirmam que o controlador deve informar acerca da descrição da natureza dos dados pessoais afetados, as informações sobre os titulares envolvidos, a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, os riscos relacionados ao incidente, os motivos da demora e as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo. Recomenda-se que o controlador informe a natureza do vazamento. Ou seja, se são violações de confidencialidade: quando a divulgação de dados sigilosos não for autorizada ou foi violada acidentalmente; violações de integridade: quando há alteração não autorizada ou acidental de dados pessoais; ou se são violações de disponibilidade: quando há uma perda acidental ou maliciosa de acesso ou destruição de dados pessoais. Da mesma forma, caso possível, informar a razão do vazamento, se foi feito por culpa ou por dolo, má-fé de funcionário interno ou terceiro não autorizado. Ato contínuo, a finalidade do vazamento, caso possível de ser

	mensurada, também deve ser comunicada à ANPD, ou seja, se a finalidade é política (e.g. desestabilização de órgãos e entidades representativas de grupos políticos) ou econômica (comercialização clandestina). Esses dados, ainda que de alto detalhamento, podem auxiliar a ANPD na tomada de medidas de mitigação e acompanhamento técnico ao controlador. Além disso, deve-se considerar os dados que, por um período de tempo, ficaram indisponíveis de serem acessados como uma forma de violação dos dados, pois deve-se avaliar que é uma clara violação ao direito de liberdade da pessoa natural. Entretanto, ressalta-se que, em caso de indisponibilidade por atualização ou manutenção do sistema, não se deve considerar como uma violação. Novamente, nesses casos, o controlador deve avaliar se isso impacta diretamente os titulares e se pode vir a causar riscos. Caso a resposta seja positiva, deve ser encaminhado também as informações para a ANPD.
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	Nos casos em que o risco ou dano for baixo ou médio, considera-se um prazo de 72 horas. Já para os incidentes que forem de alto risco ou dano, sugere-se um prazo de 24 horas. Por fim, no caso de risco ou dano altíssimo, recomenda-se notificação imediata.

	Ademais, em até 24 horas do conhecimento do incidente, cabe ao controlador fazer a avaliação da gravidade do incidente a partir da ferramenta da ANPD para esse fim, que, automaticamente, decide se o incidente tem que ser notificado e o faz, caso seja. Além disso, a notificação precisará de informações adicionais além daquelas feitas para avaliação do incidente, tendo o controlador mais 24 a 28 horas para complementar as informações referentes à notificação.
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	Em casos de risco ou dano de nível altíssimo, recomenda-se que haja a comunicação imediata ao titular dos dados. Nos casos de risco ou dano alto que não envolvam a incolumidade física, a recomendação é de que seja feita em até 24 horas após avaliação de risco e dano do incidente. Já nos demais casos, a recomendação é que seja em até 72 horas após a mesma avaliação. O parágrafo 1º do art. 48 define as seguintes informações a serem comunicadas aos titulares: I - a descrição da natureza dos dados pessoais afetados; II - as informações sobre os titulares envolvidos; III - a indicação das

	medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; IV - os riscos relacionados ao incidente; V - os motivos da demora, no caso de a comunicação não ter sido imediata; e VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo. Além dessas informações, recomendamos a comunicação de medidas essenciais de prevenção e redução de riscos e danos a serem realizadas pelos titulares, quando necessário e possível. Recomendamos também a indicação, aos titulares, pelo controlador, de um canal oficial de atualizações sobre incidente para reduzir a fricção e agilizar o processo de reparação e redução de danos e riscos.
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	A notificação aos titulares deve ser feita de forma direta e individual sempre que possível, como regra geral. A comunicação em veículos de mídia deve ser tratada como exceção ou como complemento à comunicação individual, para os casos em que não é possível contatar os titulares de dados ou quando eles forem de grande número.

	Para elaboração da comunicação aos titulares, é importante a noção de que eles não são especialistas no tema e podem não compreender mensagens demasiadamente técnicas. Por isso, esta comunicação deve ser feita em linguagem clara e acessível, de forma a ser compreensível por todos sem grandes questionamentos, atentando também para não causar pânico entre os titulares de dados. Deve ser pautada pela transparência, informando como aconteceu o incidente, o que foi ou vai ser feito para mitigar o problema e quais são as possíveis consequências para os titulares dos dados. Além disso, deve conter algum canal de comunicação com o controlador dos dados para o caso de dúvidas. Boas práticas adicionais envolveriam, também, a disponibilização de um sítio-web específico para perguntas e respostas frequentes dos titulares. Importa frisar que a comunicação pode se dar, também, em casos especiais, de forma contínua através da divulgação constante de sítio-web desenvolvido à cobertura de perguntas e respostas frequentes sobre o incidente de segurança. A medida facilitaria a acessibilidade dos titulares a informações críticas.
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	O comando legal do art. 48 da LGPD expressa que “o controlador deverá comuni car à autoridade nacional e ao titular a ocorrência de

	incidente de segurança que possa acarretar risco ou dano relevante aos titulares.” Nesse sentido, numa primeira análise, não é possível haver exceções, já que a lei afirma que o controlador deverá comunicar à ANPD a ocorrência de incidente de segurança. Entretanto, a ANPD é a entidade competente para fazer a análise sobre essa possibilidade de ocorrência de risco ou dano relevante, daí a necessidade de todos os incidentes de segurança serem reportados à Autoridade. Deixar a cargo do próprio agente de tratamento de dados uma avaliação que pode resultar em prejuízo para a sua empresa ou organização não seria uma prática recomendada, gerando o risco de colocá-lo como infrator ou negligente, o que poderia incorrer em sanção. Há um enorme potencial de subnotificação caso a linha adotada seja a da definição do potencial de risco ou dano relevante pelo próprio controlador. A ANPD, por sua vez, é o órgão que tem, entre suas atribuições previstas no art. 55-J, zelar pela proteção de dados pessoais e fiscalizar e aplicar sanções em caso de tratamento de dados realizados em descumprimento à legislação. Ou seja, a ANPD é a instância competente para determinar o potencial de risco ou dano relevante do incidente de segurança, conforme o comando legal.

	Ademais, conforme expresso no art. 12 da LGPD, a Autoridade deve ouvir o Conselho Nacional de Proteção de Dados para definir os parâmetros aceitáveis de anonimização, segundo o estado da arte das técnicas desta natureza. Por fim, é importante ressaltar que a ANPD, enquanto órgão da administração pública direta, está submetida aos princípios constitucionais previstos no art. 37 da Constituição Federal, entre eles o da legalidade. Tem, portanto, como obrigação a de atender ao comando legal de recebimento das comunicações sobre incidentes de segurança ocorridos em território nacional.
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	Para fins de desenvolvimento desta resposta, consideramos que a ANPD receberá toda comunicação de incidentes de segurança, avaliando o grau de risco ou dano aos titulares, por meio de processo administrativo próprio. Após a verificação do potencial de risco ou dano aos titulares, a única hipótese em que o controlador não precisa informar ao titular sobre a ocorrência do incidente de segurança é se não houver possibilidade de risco ou dano relevante ao titular dos dados, já que uma comunicação nesta hipótese pode ter um potencial de dano maior do

	que o próprio incidente, que nada provocou ao titular. Para exemplificar, tomamos como fundamento a metodologia publicada pela Agência da União Europeia para a Segurança da Informação e da Rede, a ENISA, para avaliação de gravidade de vazamentos de dados pessoais. A ENISA desenvolveu metodologia que, ao final, classifica a gravidade do vazamento de dados em baixa, média, alta e muito alta. Segundo a explicação sobre cada uma dessas categorias, mesmo a considerada baixa afirma que os titulares dos dados podem suportar algum inconveniente, que eles poderão superar sem problemas, mas, ainda assim, há potencial para irritação, por exemplo, o que já seria suficiente, em nossa avaliação, para provocar a informação sobre o incidente ao titular dos dados.
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	Os critérios para avaliação de incidentes de segurança devem se basear naqueles apontados pela legislação vigente no Brasil e pelas melhores práticas internacionais. Os princípios da União Europeia para Proteção de Dados, por exemplo, defendem que a avaliação de risco e dano deve ser o mais objetiva possível, requisitando a definição de critérios e sugerem os seguintes fatores a serem

	considerados: “1. type of incident; 2. nature, sensitivity, and volume of personal data; 3. ease of identification of individuals; 4. severity of consequences for individuals; 5. special characteristics of the individual; 6. special characteristics of the data controller; 7. the number of affected individuals.” A Agência para Segurança da Rede e da Informação da União Europeia (Enisa) defende três tipos de critérios para classificação de risco: • Contexto de processamento de dados, incluindo - tipo de dado vazado (simples, comportamental, financeiro e sensível); volume, características do controlador; (in)validade e (im)precisão do dado; disponibilidade pública prévia ao vazamento; natureza do dado; • Potencial de identificação

	• Circunstâncias de vazamento, incluindo perda de confiabilidade, de integridade, de disponibilidade e intenção maliciosa. • Além daqueles elencados no tópico 2 desse formulário. Os critérios devem ser considerados a partir da interação com o incidente de segurança, seja de mitigação ou aumento do risco ou dano do incidente, assim como sua interação com outros atributos do incidente e do contexto no qual se insere.
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	É necessário desenvolver ferramentas para se adequar ao cenário brasileiro, tanto em matéria administrativa quanto tecnológica. Recomendamos o desenvolvimento pela ANPD de uma ferramenta de avaliação que lance mão de critérios qualitativos e quantitativos (como aqueles sugeridos no tópico 2), partindo de uma análise e investigação de outras metodologias por um grupo de trabalho multissetorial. A recomendação de metodologia de avaliação da Agência da União Europeia para Segurança da Rede e da Informação (Enisa) é um ponto de partida.

Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	A ANPD realizará recomendações ao controlador autor da comunicação de incidente de segurança que envolvem, mas não se limita a, atos de comunicação aos titulares, reforço e mudança nas técnicas e procedimentos de segurança e de armazenamento, processamento e uso de dados. Recomendações essas que possuem caráter mandatório ou recomendatório e podem ser tomadas como fatores favoráveis ao controlador dos dados em caso de sanções. As recomendações devem estar à altura dos danos e riscos produzidos pelo incidente, mas devem incluir pelo menos medidas de pseudonimização e encriptação; medidas para garantia de confidencialidade, integridade, disponibilidade e resiliência de sistemas e serviços de processamento; capacidade de restaurar a disponibilidade e acesso a dados pessoais em tempo hábil em casos de incidentes; e a testagem e avaliação regulares das medidas técnicas aplicadas para garantir segurança da informação dos sistemas.

SUGESTÃO DE PROCEDIMENTOS EM CASO DE INCIDENTES DE SEGURANÇA

É sugerida, aqui, uma lógica de procedimentos e operação para a Autoridade em se tratando de incidentes de segurança. Esses procedimentos abarcariam as questões sobre relevância do incidente (1), seus níveis (2), distinção entre risco e dano (3), avaliação de riscos (4), forma, prazo e conteúdo de notificação (5-9), análise de gravidade (11) e recomendações ao controlador (13). Essa recomendação considera que as questões colocadas se entrelaçam intimamente e requerem uma resposta articulada.

Consideramos ainda uma alteração na lógica de avaliação pressuposta pela consulta. Ao invés da avaliação de incidentes de segurança ser realizada pelos controladores, defendemos um maior protagonismo da ANPD nessa avaliação que facilita para os controladores afetados pelos incidentes de segurança, especialmente aqueles com menores recursos humanos e tecnológicos. Através de uma ferramenta automatizada e publicamente disponível, desenvolvida pela ANPD com assistência de grupo de trabalho multissetorial a ser estabelecido, controladores afetados por incidentes de segurança terão agilidade para verificar as características dos incidentes e a necessidade ou não de notificação oficial à ANPD. Esta notificação, por sua vez, seria mais fácil, na medida em que poderia se aproveitar do próprio relatório feito pela ferramenta de avaliação de incidente de segurança, agilizando ainda as orientações e recomendações para mitigação de risco e dano. Além disso, os procedimentos e etapa operacionais sugeridos abaixo oferecem segurança jurídica e administrativa para os controladores e para a ANPD.

Destarte, a sugestão operacional abaixo se baseia nas seguintes assertivas:

- Nem todo incidente de segurança é um vazamento de dados, mas todo vazamento de dados é um incidente de segurança;
- Todo vazamento de dados em si gera danos aos titulares;

- Todo vazamento contém risco de dano futuro (potencialidade lesiva);
-

1. Desenvolvimento e disponibilização, pela ANPD, de ferramenta de avaliação de incidentes de segurança por meio de coleta padronizada e análise automatizada de um conjunto de dados informados pelo controlador-vítima do incidente. Tal ferramenta realizará a avaliação da relevância do incidente, assim como de tipo (vazamento, invasão etc), de danos e riscos produzidos pelo incidente, a gravidade, alcance, entre outros atributos do incidente. Ao fim da análise, será disponibilizado um relatório para o controlador dos dados e para a ANPD.

   Em até 24 horas de conhecimento do incidente, cabe ao controlador fazer a avaliação da gravidade do incidente a partir da ferramenta da ANPD para esse fim, que, automaticamente, decide se o incidente tem que ser notificado e o faz, caso seja.

   Caso o relatório aponte a necessidade de notificação:

2. Desenvolvimento e disponibilização, pela ANPD, de ferramenta de notificação oficial, que se baseará no relatório de incidente de segurança da informação produzido pela ferramenta 1, necessitando ainda de informações adicionais a serem comunicadas pelo controlador envolvido do incidente.

   A notificação precisará de informações adicionais além daquelas feitas para avaliação do incidente, tendo o controlador mais até 24 horas para completar as informações necessárias à notificação.

   A partir da análise e da notificação oficial do incidente de segurança:

3. ANPD realizará recomendações ao controlador autor da comunicação de incidente de segurança que envolvem, mas não se limita a, atos de comunicação aos titulares, reforço e mudança nas técnicas e procedimentos de segurança e de armazenamento, processamento e uso de dados. Recomendações essas que possuem caráter mandatório e podem ser tomadas como fatores favoráveis ao controlador dos dados em caso de sanções. As recomendações devem estar à altura dos danos e riscos produzidos pelo incidente, mas devem incluir pelo menos medidas de pseudonimização e encriptação; medidas para garantia de confidencialidade, integridade, disponibilidade e resiliência de sistemas e serviços de processamento; capacidade de restaurar a disponibilidade e acesso a dados pessoais em tempo hábil em casos de incidentes; e a testagem e avaliação regulares das medidas técnicas aplicadas para garantir segurança do processamento de dados.

4. Em determinadas situações, como em casos de suspeitas de má-fé, subnotificação ou ocultação de informações por parte do controlador, de gravidade acentuada de incidente de segurança, de demanda legal ou institucional (ações penais, CPIs etc) cabe à ANPD realizar auditoria da notificação do incidente de segurança, com revisão dos dados informados pelo controlado por máquina e por seres humanos, inclusive com demanda e coleta de informações adicionais para averiguar a situação concreta do incidente.

SUGESTÃO DE NORMATIVO, SE HOUVER	
Art. Xxxx	
Art. Xxxx	

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: INSTITUTO PARANAENSE DE COMPLIANCE - GRUPO DE TRABALHO DA LEI GERAL DE PROTEÇÃO DE DADOS (GT-LGPD)

ESTE FOI UM TRABALHO DESENVOLVIDO COLETIVAMENTE PELO GRUPO:

ADRIELE OLIVEIRA
CAMILLA RIBAS DA SILVA
GERMANO DE SORDI
JÚLIA ROCHA
LAÉRCIO ALMEIDA JUNIOR
LETÍCIA SUGAI
LUCILIANE RIBEIRO
LUIZ CARLOS ROSSI FILHO
MARIZETE FIGUEIREDO
MURILO ROBERTI

CPF/CNPJ: 29.864.819/0001-89

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS **IMPORTANTE:** Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	**Dano relevante = prejuízo comprovado (material, moral) e integridade física. Critérios para avaliar o risco como relevante = quantidade de dados das pessoas e de pessoas, classificação do dado, tempo de duração do vazamento até tomada de ação por parte da organização.**
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	**Sim, deveria ser dividido em baixo, médio, alto ou crítico, distinguíveis a partir do prejuízo comprovado. Entendemos que o risco baixo deve ser considerado relevante ao menos para base de dados (quantidade de riscos baixos podem gerar um risco médio, alto ou crítico).**
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	**Risco significa toda a incerteza sobre um evento, devendo ser levado em consideração (i) probabilidade e (ii) consequência. Dano é um prejuízo de ordem patrimonial ou extrapatrimonial sofrido ou causado por alguém. Assim, risco ao titular seria um evento hipotético provável ou possível de ocorrer. Dano é o evento efetivamente ocorrido, a lesão ao bem material ou imaterial (moral). A relação entre eles está no fato de ser o risco uma chance de ocorrência de um evento que cause dano. Assim, a consequência do risco (da possibilidade de ocorrência de um evento) é o dano, que é a efetiva lesão a um bem tutelado pelo direito (material ou moral).**

O que deve ser considerado na avaliação dos riscos do incidente?	**Deverão ser consideradas a relação do tratamento aos dados envolvidos no incidente, a natureza, o escopo, a finalidade das informações, a probabilidade, a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular, a estrutura, a escala e o volume nas operações relacionadas ao incidente, bem como a sensibilidade dos dados tratados, a probabilidade de ocorrência e a gravidade dos danos para os titulares dos dados e a criticidade de impacto nos processos da organização.**
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	**Facilitar a comprovação/preencher as informações sobre as medidas de segurança através um formato check list, a exemplo da HIPAA (Lei de Portabilidade e Responsabilidade de Seguros de Saúde), que tornou a proteção de informações de saúde uma responsabilidade legal nos Estados Unidos desde 1996. Ela utiliza em alguns de seus formulários de Compliance https://www.hippa.com)**

Medidas de Segurança

Técnicas:

- ☐ Controle de Acesso;
- ☐ Controle de auditorias;
- ☐ Segurança na transmissão de Dados;
- ☐ criptografia,
- ☐ controle de usuário

Administrativas:

- ☐ Políticas/processos de segurança;
- ☐ Política de acesso a informação;
- ☐ Treinamentos relacionados à segurança;

Físicas:

- ☐ Controle de Acesso
- ☐ Segurança no Local de trabalho

Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	**Para a <u>simples comunicação inicial</u> do incidente, 2 dias úteis como prazo máximo. No entanto, incidentes de segurança complexos demandam da equipe de Resposta a Incidentes uma análise minuciosa sobre:** **1. Categoria de dados vazados** **2. Perfis de titulares afetados** **3. Origem do vazamento** **4. Medidas de segurança que a organização detinha** **5. Medidas tomadas após o incidente para reverter ou mitigar** **6. Existência de RIPD** **7. Mapeamento de consequências aos titulares** **Considerando esses e outros elementos de informação, 15 dias úteis para a <u>complementação da comunicação inicial.</u>**
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	**A comunicação deverá ser feita de imediato ou no prazo máximo de 72 horas da constatação do incidente que apresentar qualquer risco que seja relevante e que possa acarretar risco ou dano aos titulares.** **Na comunicação aos titulares deverá mencionar, no mínimo:** **1- descrição da natureza dos dados pessoais afetados;** **2- informações sobre os titulares envolvidos;** **3- indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;** **4- os riscos relacionados ao incidente;** **5- os motivos da demora, no caso de não ter sido comunicado o incidente de imediato.Tal justificativa deverá ser devidamente fundamentada para reverter ou mitigar os efeitos de eventual prejuízo;** **6- as medidas que já foram adotadas e/ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo;** **7- possíveis medidas a serem adotadas pelos titulares para segurança de seus dados e sua integridade física.**
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas	**A comunicação deve ser feita mediante análise do caso concreto e do grau de impacto que este causará na sociedade como um todo ou no grupo afetado pelo vazamento de dados. Quando os titulares puderem ser identificados, a melhor forma é a direta. Quando não há mensuração do impacto, quantificação ou identificação de todos os titulares, o ideal é que seja de forma pública para não correr o risco de alguém que precisava ser avisado deixe de**

circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	**ser comunicado, vide o princípio da transparência e exemplos de boas práticas da norma ISO 27002.** **O art. 34 da GDPR traz alguns parâmetros a serem seguidos pelo responsável pelo tratamento do dado vazado, que podem ser usados como embasamento aqui no Brasil.**
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	**Dados pessoais "soltos" e "não estruturados" em documentos diversos devem ser exceções e eventuais vazamentos não necessitariam ser comunicados à ANPD.** **Dados "soltos" / "não estruturados" são dados pessoais contidos em comunicação diversa, contratos, e-mails e eventualmente chegam a quem não necessita saber de tais dados; também são dados pertinentes a documentos específicos (ex.: nome dos signatários de um contrato; e-mails de destinatários de mensagens eletrônicas, etc.).**
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	**As possíveis exceções quanto à obrigatoriedade de informar aos titulares a ocorrência de incidente seriam:** **- quando não houver ocorrência de dano ou eventual possibilidade de sua ocorrência para o titular;** **- quando o Controlador demonstrar que, embora tenha havido um incidente, tomou as providências necessárias capaz de voltar ao *status quo ante* (situação anterior antes do incidente);** **- quando se tratar de vazamentos de dados anonimizados ou pseudonimizados, sendo que para este último, não haja possibilidade de identificação do titular de dados;** **- quando o incidente for relativo a vazamento de dados manifestamente públicos e de conhecimento de todos.**
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	**1 - Volume de titulares de dados afetados: para ter percepção do total de pessoas físicas que poderão ser afetadas pelo vazamento.** **2 - Tipos de dados vazados: nessa tipificação, além de considerar se são dados sensíveis ou não, também é necessário considerar se os dados são substituíveis ou não. Por exemplo: número de CPF é informação única que, se vazada, pode trazer muito transtorno ao titular e não pode ser trocada, diferente de um número de telefone ou cartão de crédito.** **3 - Medidas de proteção implementadas: verificar se as medidas de segurança de informação implementadas permitem que os dados vazados sejam acessados integralmente ou se foram implementadas criptografias que impossibilitam esse acesso.**

	4 - Prejuízo financeiro: se os dados vazados poderão incorrer em prejuízo financeiro ao titular. **5 - Prejuízo de imagem: se os dados vazados irão incorrer em prejuízo de imagem ou reputação do titular.**
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	**Sugestão de quebrar em 3 níveis:** **1) Dados pessoais "substituíveis": dados pessoais que se vazados não causarão danos à integridade física do titular, mas proporcionarão certo grau de incômodo aos titulares visando regularização, mas que são substituíveis. Ex.: número de telefone, número de cartão de crédito, número de conta bancária, login / usuário de determinado site de e-commerce etc.** **2) Dados pessoais "não-substituíveis": dados pessoais que, se vazados, podem trazer sérios danos ao titular pois são inerentes à identidade do titular. Ex.: número de CPF, número RG, CNH.** **3) Dados pessoais sensíveis: respeitando a letra da lei.** **Sugere-se verificar normas ISO 27001 e 27701 para coletar boas práticas de gestão de incidentes de segurança da informação e privacidade.**
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	**As providências ao controlador são:** **1) Aviso aos titulares informando sobre o vazamento (conforme regra a lei)** **2) Contenção do vazamento através de medidas técnicas de informática** **3) Ações de tentativa de recuperação dos dados (caso tecnicamente possível)** **4) Ações internas para prevenção de novos vazamentos (soluções técnicas de TI)** **5) Ações internas de revisão de procedimentos (manuais e políticas)** **6) Treinamentos a funcionários, contratados, terceiros sobre segurança da informação** **No entanto, essas medidas serão efetivas, mesmo que bem executadas, para eventuais futuros casos de tentativa de invasão ou vazamento. Os dados que já vazaram dificilmente serão recuperados - o que vazou não tem volta.**

	Sugere-se verificar normas ISO 27001 e 27701 para coletar boas práticas de gestão de incidentes de segurança da informação e privacidade, e contenção e prevenção de vazamento de dados.
SUGESTÃO DE NORMATIVO, SE HOUVER	
Art. Xxxx	
Art. Xxxx	

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: Instituto de Referência em Internet e Sociedade - IRIS
CPF/CNPJ: 23.333.533/0001-90

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS

IMPORTANTE: Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.

TÓPICO/QUESTÃO	CONTRIBUIÇÃO/INSTITUIÇÃO
1. Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	Há diversos fatores que corroboram para a relevância de um incidente de segurança que afete dados pessoais. A seguir, procura-se apresentar razões pelas quais **a relevância do risco ou dano deve ser presumida** para fins de responsabilidade dos agentes de tratamento de dados pessoais. Conforme será exposto em mais detalhes a seguir, um incidente de proteção de dados pessoais repercute em responsabilidade objetiva por parte do agente de tratamento, por se tratar de um risco inerente à própria atividade de tratamento de dados pessoais. Dessa forma, a própria ocorrência de um incidente implica na quebra do dever de zelo pela informação em questão, o que atrai uma responsabilidade que se apoia tanto no parágrafo único do art. 927 do Código Civil quanto no art. 46 da própria LGPD; e, no caso de consumidores, no art. 6º, VI do CDC. Além disso, observa-se, diversas vezes, a dificuldade – ou impossibilidade – de se estabelecer um nexo causal entre o incidente ocorrido e as repercussões danosas do evento. Esse fenômeno também é conhecido como “prova diabólica” no direito civil. Essa barreira informacional torna potencialmente nebulosa a avaliação do incidente pelos agentes de tratamento, decorrente tanto de uma dificuldade de análise de precedentes quanto da baixa previsibilidade – e constatação – das consequências diretas desse incidente. Acrescente-se a isso o fato de que, uma vez substanciado, o dano decorrente de um incidente de proteção de dados é irreversível: quando as medidas de contingenciamento não são suficientes para

	impedir a consumação do dano, o que se sucede é inevitável. Isso, por sua vez, se intensifica no meio digital, no qual a constante evolução do estado da arte das tecnologias repercute em uma variedade crescente de modalidades de riscos e danos em um incidente que envolve dados pessoais. **Responsabilidade Objetiva e Direito do Consumidor** Como parte importante dos incidentes de segurança envolve dados pessoais de consumidores, a ANPD deve considerar os debates sobre o conceito de responsabilidade e dano desenvolvidos no direito do consumidor. O regime consumerista de responsabilidade é considerado pela LGPD, no parágrafo único do art. 46 e reforçado pelo comando expresso de diálogo de fontes normativas do art. 64. O Código de Defesa do Consumidor (arts. 6, VI, e 12 ao 20, Lei nº 8.078) adota como regra a responsabilidade objetiva. Assim, o dever de indenizar fundamenta-se na existência de um nexo causal entre a conduta do responsável (neste caso os agentes de tratamento) e o dano causado ao titular pelo incidente de segurança. O desenvolvimento da teoria da responsabilidade objetiva (independente de culpa) foi motivado pela necessidade de garantir a proteção de quem sofreu o dano causado; principalmente nos casos em que é a atividade econômica desenvolvida que gera e/ou potencializa as condições para que o risco se concretize em dano.[1] O desenvolvimento de atividades econômicas baseadas em dados pessoais (data capitalism[2]) gera incentivos para que os agentes de tratamento busquem ter maior acesso aos dados dos titulares, a fim de extrair informações úteis em termos econômicos. Desse modo, esses agentes de tratamento, ao criarem as condições para o uso dos dados, também geram

[1] BESSA, Leonardo Roscoe.Responsabilidade objetiva no Código de Defesa do Consumidor. **Revista Jurídica da Presidência** Brasília v. 20, nº 120. Fev./Maio 2018 p. 27.Disponível em: <https://bit.ly/3tHrYCR>. Acesso em 21/03/2021.

[2] "Data capitalism is, at its core, a system in which the commoditization of our data enables a redistribution of power in the information age. If communica-tion and information are historically a key source of power (Castells, 2007), data capitalism results in a distribution of power that is asymmetrical and weighted toward the actors who have access and the capability to make sense of data." WEST, Sarah Myers. Data Capitalism: Redefining the Logics of Surveillance and Privacy. **Business & Society**, Vol. 58(I). 2019. p. 23. Disponível em: <https://bit.ly/3cSsWW5>. Acesso em: 21/03/2021.

	maiores riscos em relação ao seu eventual uso indevido. Por isso é aplicável a **teoria do risco do direito do consumidor**[3]. Nesse sentido, a responsabilização objetiva, além do seu papel de censurar o causador do dano por meio de incentivo negativo (p. ex. punir agentes que adotam práticas insuficientes de segurança da informação), tem como principal meta garantir uma efetiva reparação à vítima. Um tratamento de dados pessoais que gere as condições para um incidente de segurança, como práticas de segurança insuficientes por parte do agente, pode ser abarcado pelo "fato do produto ou serviço" (arts. 12 e 14 do CDC). O "fato do produto ou serviço" refere-se aos casos em que o consumidor sofre um dano em decorrência de "defeito" do produto/serviço.[4] Nesse caso, a adoção de medidas inadequadas ou insuficientes de segurança da informação seria considerada um "defeito" do produto/serviço, pela ótica da regulação consumerista, por gerar dano ao consumidor. Alternativamente, em uma visão mais expansiva da responsabilidade objetiva consumerista, o art. 6º, VI do CDC pode ser entendido como cláusula geral de responsabilidade objetiva.[5] Assim, mesmo que se admitisse que um incidente de segurança da informação não configura "fato do produto ou serviço", a interpretação de que há cláusula geral de responsabilidade objetiva abarca os incidentes de segurança. Desse modo, recomenda-se que ANPD parta do princípio de que determinadas atividades de tratamento de dados pessoais, por sua própria natureza, acabam por gerar um maior risco e potencial de tratamento indevido, principalmente em relação a incidentes de

[3] "Na verdade, o CDC adotou expressamente a ideia da teoria do risco-proveito, aquele que gera a responsabilidade sem culpa justamente por trazer benefícios ou vantagens. Em outras palavras, aquele que expõe aos riscos outras pessoas, determinadas ou não, por dele tirar um benefício, direto ou não, deve arcar com as consequências da situação de agravamento. Uma dessas decorrências é justamente a responsabilidade objetiva e solidária dos agentes envolvidos com a prestação ou fornecimento." TARTUCE, Flávio; e NEVES, Daniel Amorim Assumpção. **Manual de direito do consumidor**. São Paulo: Editora Forense. 5ª edição. 2016.p. 119.

[4] "Por outra via, no fato ou defeito – seja também do produto ou serviço –, há outras decorrências [para além do defeito/vício do produto e/ou serviço em si], como é o caso de outros danos materiais, de danos morais e dos danos estéticos (prejuízos extrínsecos) [gerados ao consumidor]." *Ibid.* pp 125 e 126.

[5] "O regime da responsabilidade objetiva do CDC deve aplicar-se, de conseguinte, a todas as hipóteses de relação de consumo quando surgir a questão do dever de indenizar o consumidor pelos danos por ele experimentados. Isto porque o fundamento da indenização integral do consumidor, constante do art. 6°, VI, do CDC, é o risco da atividade, que encerra em si o princípio da responsabilidade objetiva praticamente integra".De acordo com Nelson Nery Júnior (1992, p. 58), conforme citado por Bessa (2018, p. 29-30).

	segurança da informação. A LGPD, ao ser uma regulação fortemente principiológica que impõe aos agentes a obrigação de analisar e mitigar adequadamente os riscos do tratamento, deve ser interpretada em conjunto com CDC, a fim de garantir a reparação e mitigação de danos (ver resposta 13 desta Tomada de Subsídios). **Método da Ponderação na Responsabilidade Civil e Grau do Dano** Conforme já explorado acima, a discussão sobre a conceituação e verificação do dano é uma tema fundamental no campo jurídico da responsabilidade civil. Com a expansão dos danos considerados ressarcíveis na esfera da responsabilidade civil, busca-se criar novos métodos de verificação do dano, principalmente para demandas relacionadas à responsabilidade objetiva, aos danos extrapatrimoniais e coletivos. Desse modo, Anderson Schreiber sugere que seja aplicado o método da ponderação constitucional, de forma adaptada, para verificação do dano. Para o autor, este método seria importante pois o novo cenário da responsabilidade civil envolve, em grande parte dos casos, interesses igualmente tutelados pelo ordenamento jurídico (p. ex. privacidade *vs* desenvolvimento tecnológico): > "Tal análise comparativa entre interesse lesado e interesse lesivo exige recurso ao método da ponderação, cujas potencialidades ainda permanecem pouco exploradas fora do âmbito constitucional. A identificação de condições de prevalência em cada caso particular, a partir do exame do ordenamento jurídico, permite, a um só tempo, um reconhecimento de ressarcibilidade limitada ao caso concreto e controle normativo da fundamentação das decisões que acolhem ou rejeitam as demandas de indenização"[6] A partir das considerações sobre dano no direito civil, parece-nos útil que a ANPD utilize um método de ponderação semelhante para verificar o **grau do dano** sofrido a partir de um incidente de segurança da informação. A premissa é que determinados incidentes, por suas próprias características, intrinsecamente causam danos aos titulares afetados (p. ex. cópia e

[6] SCHREIBER, Anderson. **Novos Paradigmas da Responsabilidade Civil** - Da Erosão dos Filtros da Reparação à Diluição dos Danos. São Paulo: Editora Atlas. 3ª Edição. 2011. p. 252.

	disponibilização ilícita de dados pessoais/vazamento), conforme exposto na definição de danos extrapatrimoniais. Desse modo, o método da ponderação constitucional pode ser utilizado pela ANPD como base para elaboração do seu próprio método de análise de danos aos titulares afetados por um incidente de segurança. **Presunção de Relevância e critérios para determinação de exceções** Por todos os motivos elencados, a ocorrência de um incidente repercute em dano *in re ipsa* ao titular de dados. Dessa forma, **deve-se presumir relevante qualquer risco ou dano decorrente de um incidente de segurança relativo a dados pessoais**, exceto quando os agentes de tratamento puderem demonstrar a existência de medidas para assegurar que do incidente não resulte prejuízo aos direitos e liberdades dos titulares afetados. Ademais, importa mencionar que a presunção de relevância do risco ou dano constitui uma recomendação de boas práticas por parte dos agentes de tratamento. Nesse sentido, o potencial para uma avaliação demasiadamente branda do ocorrido é reduzido, impactando diretamente na probabilidade de subnotificação de incidentes perante a ANPD e os próprios titulares de dados pessoais. Uma postura preventiva dos agentes de tratamento pode, dessa forma, evitar subsequentes responsabilizações por descumprimento dos enunciados da LGPD. Uma vez que a constatação de "risco ou dano relevante" resulta em obrigação de notificação à ANPD, o conceito opera como equivalente funcional ao que o legislador europeu nomeou como "risco" no Regulamento Geral sobre a Proteção de Dados (RGPD) da União Europeia.[7] Na referida norma, o responsável pelo tratamento é compelido a notificar todos os incidentes, a menos

[7] "[...] por risquificação da proteção de dados pessoais entende-se esse processo de reformatação jurídica a partir da ampliação da tutela coletiva e sua imbricação com a autoridade independente de proteção de dados pessoais, a disseminação de instrumentos regulatórios *ex ante* e o uso intensivo de metodologias de gestão de risco e calibragem entre riscos, inovações e imunidades – um processo de "negociação coletiva" (TUBARO e CASILLI, 2018) que supera a tradicional concepção bilateral entre sujeito de direito e aquele que processa dados pessoais pessoais." ZANATA, Rafael A. F. Artigos Selecionados REDE 2017 **I Encontro da Rede de Pesquisa em Governança da Internet Rio de Janeiro.** 14/11/ 2017.p. 184. Acesso em: 24/03/2021. Disponível em: <https://bit.ly/2Ps3ApT>

	que o ocorrido "não seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares" (art. 33, 1). **A presunção de relevância do risco e a obrigação de notificar que dela sucede são regra, portanto.** Dadas as similaridades entre o desenho da lei brasileira e do regulamento europeu, entendemos que a adoção de um entendimento análogo favorece maior interoperabilidade entre os sistemas regulatórios, o que beneficia sua observância pelo agente de tratamento. A análise não se esgota na presunção de relevância, contudo. Além de meio de salvaguarda ao titular de dados e incentivo à adoção de medidas de segurança efetivas, também devem ser consideradas eventuais exceções à regra de relevância presumida do incidente. **Como regra geral, só é razoável entender que o incidente referente a dados pessoais não acarretará prejuízo aos direitos e liberdades dos titulares quando da existência de medidas técnicas e organizacionais capazes de impedir a concretização do referido prejuízo.** Assim sendo, e em conformidade com os princípios de responsabilização e de prestação de contas afirmados no art. 6, inciso X da LGPD, o afastamento da presunção de relevância deve estar condicionado à demonstração da existência e da eficácia de tais medidas pelo agente. Ainda, o enquadramento de um caso concreto nessa exceção deve estar condicionado a uma avaliação de risco informada por uma miríade de fatores. Com base nas orientações sobre a notificação de uma violação de dados pessoais ao abrigo do Regulamento (UE) 2016/679 (p. 25-28) elaboradas pelo Grupo de Trabalho do Artigo 29º para a Proteção de Dados da União Europeia, destacamos os seguintes critérios: ● *Atributos da segurança comprometidos*: o incidente afetou a confidencialidade, a integridade, a disponibilidade ou a não-repudiabilidade dos dados? Incidentes podem comprometer apenas um ou múltiplos atributos e os prejuízos suscetíveis de resultar podem variar amplamente em função deles. Por exemplo, a depender do caso concreto, o comprometimento exclusivo da confidencialidade dos dados médicos de alguém pode ser mais suscetível de resultar em prejuízo reputacional e psicológico, enquanto uma violação que atinja exclusivamente sua disponibilidade

	ou integridade pode ser mais suscetível de afetar negativamente a possibilidade de recepção de tratamento adequado em uma emergência. ● *Natureza, volumetria e vulnerabilidade dos dados*: Dados de saúde, dados financeiros e dados referentes a documentos de identificação merecem especial atenção pois sua natureza implica que seu comprometimento pode resultar em prejuízo por si mesmos. Outras categorias de dados podem ser associadas a níveis mais elevados de risco por sua própria natureza, como dados de educação, endereços e registros de localização. Além disso, quanto mais categorias de dados forem comprometidas, maior sua probabilidade de resultar em prejuízo, pois a vulnerabilidade do titular vitimizado pelo incidente aumenta proporcionalmente às possibilidades de combinação e análise agregada dos dados. Em adição às categorias, portanto, deve-se considerar a quantidade de registros afetados e suas possibilidades de combinação. ● *Facilidade de identificação dos titulares*: Deve-se considerar o quão facilmente o titular afetado pelo incidente poderá ser identificado por um terceiro que obtenha acesso aos dados. Essa avaliação deve considerar tanto os dados afetados em si quanto as circunstâncias do incidente, por exemplo, se os dados podem ser combinados a outros que estejam publicamente disponíveis. ● *Severidade e probabilidade de concretização do prejuízo*: Incidentes podem tornar os titulares suscetíveis a consequências de ordens extraordinariamente severas, incluindo roubo ou fraude de identidade, perdas financeiras, prejuízos reputacionais, sofrimentos psíquicos e danos à incolumidade física. A avaliação de risco ou dano decorrente de um incidente deve considerar tanto a severidade do prejuízo potencial quanto sua probabilidade de concretização. No contexto de uma violação de confidencialidade, um fator a ser considerado na análise de severidade é o nível de confiança do agente de tratamento na parte que obteve acesso indevido aos dados. Se foram enviados por engano ao departamento errado de uma organização, por exemplo, o agente pode ter um grau maior de confiança na possibilidade de eliminação dos dados por parte do destinatário. Se, por outro lado, o agente entender provável que um ator malicioso, a exemplo de um criminoso cibernético, obteve acesso às informações, ele deve

	presumir uma maior probabilidade de concretização de prejuízo ao titular. Ademais, todo risco ou dano cujo prejuízo potencial apresentar elevada severidade ou elevada probabilidade de concretização deve receber a qualificação imediata de “risco ou dano relevante grave”, que detalharemos na resposta seguinte e que implica na obrigação de notificação ao titular. ● *Características especiais dos titulares*: É preciso considerar se o incidente afeta categorias que já se encontram em vulnerabilidade social, como crianças, idosos, mulheres, pessoas LGBT+, pessoas negras e indígenas, refugiados, pessoas de religiões de matriz africana, pessoas com deficiência, entre outros. Um incidente que resulte na exposição não-consentida de imagens íntimas provavelmente terá repercussões mais severas sobre as mulheres e pessoas trans afetadas do que sobre homens cisgêneros em virtude das dinâmicas de violência física, social e simbólica que incidem sobre tais sujeitos. Uma violação da integridade dos dados do histórico profissional de pessoas negras pode ser mais provável de prejudicá-las num processo seletivo em virtude da discriminação racial que permeia o mercado de trabalho. Similarmente, a divulgação da lista de nomes dos usuários de um aplicativo de encontros poderá ter impactos mais severos se o aplicativo for voltado a sujeitos do segmento LGBT, podendo resultar na publicização forçosa de sua identidade sexual e/ou de gênero. ● *Características especiais dos agentes*: a natureza das atividades de tratamento conduzidas pelo agente afetam desde os dados afetados, até a probabilidade do incidente decorrer de um ataque malicioso, bem como as consequências específicas. Um órgão público que trata informações de elevada delicadeza, como um tribunal alvejado por um ataque de *ransomware* ou um Ministério que teve seu banco de dados vazado, tenderão a provocar consequências mais severas para os titulares na ocasião de um incidente. Em síntese, **recomendamos que a relevância do “risco ou dano” decorrente de incidente de segurança que afete dados pessoais seja presumida, exceto quando os agentes de tratamento puderem demonstrar a existência de medidas**

	capazes de assegurar que do incidente não sucederá prejuízo aos direitos ou liberdades dos titulares. Por fim, a eventual demonstração de que as medidas tomadas pelo agente efetivamente justificam a **desconsideração da relevância do risco ou dano é de responsabilidade do agente de tratamento, em conformidade com o princípio da responsabilização e prestação de contas da LGPD.** Recomendamos, nesse sentido, que a identificação de negligência, imprudência ou imperícia na avaliação inicial importem na determinação e/ou agravamento de eventuais sanções administrativas, posto que prejudicam as diligências referentes ao incidente e podem agravar os riscos aos direitos e liberdades do titular.
2. O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	Como indicado na resposta anterior, recomenda-se a adição do qualificador grave para certas categorias de risco ou dano relevante. Tal conceito é análogo ao de “elevado risco” positivado no Art. 34, parágrafo 1, do RGPD e que culmina na obrigação de notificação aos titulares afetados. O risco ou dano relevante deve ser considerado grave nas seguintes hipóteses: 1. O incidente afetou dados sensíveis, nos termos do art. 5º, inciso II da LGPD; 2. O prejuízo potencial é altamente provável de concretização; 3. O prejuízo potencial é altamente severo, caso se concretize. Prejuízos altamente severos podem incluir roubo ou fraude de identidade, perdas financeiras, prejuízos reputacionais, sofrimento psíquico e danos à incolumidade física. A primeira hipótese se fundamenta na distinção estabelecida pelo próprio legislador entre os níveis de proteção aplicáveis a dados pessoais em geral e aqueles reservados a certas categorias de informações pessoais - os dados sensíveis. Em razão da própria natureza, seu comprometimento é tanto mais suscetível de resultar em prejuízo aos direitos e liberdades quanto tais prejuízos podem ser mais severos, razão pela qual se encontram sujeitas a um regime protetivo substancialmente mais rígido. O universo de bases legais para seu tratamento é mais restrito, por exemplo. A seu tempo, as hipóteses 2 e 3 se alicerçam na necessidade de assegurar a tomada de medidas de mitigação pelo titular, a

	exemplo de pedidos de bloqueio de cartão de crédito ou mudanças de senha. Desse modo, operam como remédios funcionais a incidentes dos quais resulta grave risco, seja por sua probabilidade ou severidade, aos direitos e liberdades dos titulares. Quanto à instituição de uma categoria de "risco ou dano baixo", a desaconselhamos veementemente. Dado que a avaliação de risco é realizada inicialmente pelos agentes no momento em que tomam ciência do incidente e importa sobretudo na obrigação de notificar, tal categoria poderia ser instrumentalizada para evadir tal obrigação, para evitar danos reputacionais, custos operacionais de uma investigação forense completa e/ou eventuais sanções. Pelas mesmas razões, **a desconsideração da relevância do risco ou dano deve ser excepcional**. Ainda, essa preocupação é reforçada pela consideração das especificidades do ambiente regulatório e cultural brasileiro: enquanto o RGPD entrou em vigor nem um contexto já regulado pela Diretiva 96/45/CE, nossa política nacional de proteção de dados ainda se encontra em estágio embrionário, com a entrada em vigor da LGPD bastante recente e sua observância amplamente encarada pelo setor regulado como um fardo regulatório adicional. Nesse contexto de desconhecimento e subvalorização dos princípios e normas de proteção de dados, uma obrigação ampla de notificar incidentes pode favorecer a construção de uma cultura de proteção de dados ao incentivar os agentes de tratamento à tomada de medidas técnicas e organizacionais para garantir a segurança dos dados tratados, de modo a evitar os custos reputacionais da notificação pela redução efetiva dos riscos. Isso pode incentivar, inclusive, a valorização do investimento na segurança dos dados pessoais como um diferencial competitivo no setor privado.
3. Como distinguir o risco ao titular do dano ao titular? Como esses	Ainda que já seja estabelecida a diferença conceitual entre "risco"e "dano", consideramos que para fins de regulação da matéria específica de que trata o art. 48 a ANPD tem o condão de equipará-los, em razão das particularidades representadas por

conceitos se relacionam?	incidentes de segurança para a efetivação de um sistema de proteção aos dados pessoais. Para fins do art. 48, risco ou dano relevante devem ser entendidos como sinônimos na medida em que neles deve se enquadrar qualquer situação decorrente de incidente que afete os dados dos titulares em que os agentes de tratamento não são capazes de demonstrar que medidas capazes de assegurar que do incidente não resulte prejuízo aos direitos e liberdades dos titulares afetados foram tomadas. Desse modo, os conceitos de “risco ou dano relevante” e “risco ou dano relevante grave” passam a operar como equivalentes funcionais aos conceitos de “risco” e “risco elevado” do RGPD. Essa equiparação facilita a preparação dos diversos agentes a partir do conhecimento já produzido em anos de debate e consolidado em uma série de documentos de referência, além de sinalizar internacionalmente pela busca de interoperabilidade entre os sistemas legais e de harmonização dos diferentes cenários a partir de pontos comuns. Ademais, a equiparação dos termos risco e dano para os fins do art. 48 encontra justificação teórica se examinamos os métodos de avaliação desenvolvidos no campo jurídico da responsabilidade civil. Quanto a este ponto, atenção especial deve ser dada aos casos que envolvam consumidores. É de simples constatação que um incidente de segurança pode causar aos titulares danos patrimoniais, extrapatrimoniais/morais e coletivos. A partir disso, a questão do dano extrapatrimonial deve ser melhor analisada quanto a sua definição e comprovação. Para Schreiber, a definição de dano extrapatrimonial pode ser traduzida como a lesão a um interesse merecedor de tutela, tendo o réu[8] agido de forma a trazer risco aos interesses do afetado que são tutelados juridicamente (p. ex. direitos da personalidade, privacidade, proteção dos dados pessoais, etc).[9] Assim, verifica-se que o dano extrapatrimonial pode ser intrínseco a determinadas atividades de um agente. Nesse sentido, o Superior Tribunal de Justiça (STJ) se manifesta:

[8] Utilizaremos o termo “réu” para nos referir aos agentes de tratamento responsáveis por garantir a segurança da informação.
[9] SCHREIBER, Anderson. **Novos Paradigmas da Responsabilidade Civil** - Da Erosão dos Filtros da Reparação à Diluição dos Danos. São Paulo: Editora Atlas. 3ª Edição. 2011. p. 204.

> "Como se trata de algo imaterial ou ideal, a prova do dano moral não pode ser feita através dos mesmos meios utilizados para a comprovação do dano material. Por outras palavras, o dano moral está ínsito na ilicitude do ato praticado, decorre da gravidade do ilícito em si, sendo desnecessária sua efetiva demonstração, ou seja, como já sublinhado: o dano moral existe *in re ipsa*".[10]

Com base na definição de dano extrapatrimonial elencada acima, podemos analisar brevemente como ela se aplicaria a um caso hipotético de incidente de segurança. Suponhamos que uma base de dados pessoais (nome, filiação, endereço, RG, CPF, conta bancária, dependentes, empréstimos feitos, profissão) de uma empresa de empréstimo foi acessada sem autorização por terceiros. Verificou-se que uma cópia dos dados foi extraída e que a empresa não adotava práticas de segurança adequadas e proporcionais. Contudo, não foi possível confirmar se esses dados foram postos à venda ou mesmo se foram utilizados ilicitamente (p. ex. fraudes), entre o período de tempo da notificação do incidente e a conclusão das investigações.

Pela definição de dano extrapatrimonial elencada acima, o próprio ato de violação da segurança das informações configura um dano, porque viola interesses dos titulares tutelados juridicamente como, por exemplo, o direito à privacidade e à autodeterminação informativa. Ademais, as circunstâncias do caso (invasão e cópia deliberadas das informações) levam ao entendimento de que é alto o suficiente o risco de que os dados possam ser usados ilicitamente. Isso impõe uma situação de incerteza aos titulares e gera a necessidade de adotarem precauções adicionais (p. ex. verificar regularmente sua nota de crédito, modificação de senhas, contratação não autorizada de serviços, retificação de dados) por período longo ou até mesmo indeterminado. Acerca desse último ponto, destaca-se ainda, que os riscos tendem a crescer conforme novas técnicas e formas de análise e exploração dos dados são desenvolvidas e se tornam disponíveis a atores maliciosos.

Em síntese**, ao serem expostos a uma situação de maior risco, há constatação de dano aos titulares pelas novas necessidades impostas de precaução e verificação constantes para detectar e mitigar eventual uso indevido de seus dados**. Esse raciocínio aplica-se especialmente aos casos

[10] BRASIL. Superior Tribunal de Justiça (1ª Turma). **Recurso Especial 608.918/RS**. 25/05/2004. Disponível em: <https://bit.ly/3tqe3kC>. Acesso em: 18/03/2021.

	em que não seja fácil: i) verificar tecnicamente como os dados foram afetados (se houve ou não cópia); e ii) se estes foram utilizados ilicitamente após o incidente. Por essas razões, conclui-se que o incidente de segurança do qual sucede risco de prejuízo particular, como fraudes de identidade ou danos reputacionais, já configura uma espécie de prejuízo geral aos direitos e liberdades do titular afetado. Tal prejuízo geral se concretiza em três elementos: 1. A violação direta à privacidade e à autodeterminação informativa, manifesta na ausência de medidas de segurança eficazes para impedir a concretização dos prejuízos concretos e particulares; 2. A incerteza e aflição impostas aos cidadãos vitimizados pelo incidente, que não podem gozar da segurança mental de saber que seus dados não estão sendo utilizados de forma indevida; 3. A necessidade, decorrente dessa insegurança, de tomar medidas de precaução, mitigação e verificação desses usos indevidos, o que implica em custos de tempo e esforço. A título comparativo, a definição de risco e dano também tem sido intensamente debatida nos tribunais federais dos Estados Unidos. Apesar das diferenças entre os sistemas jurídicos do *common* e *civil law*, e das especificidades do direito estadunidense, vale mencionar como os conceitos de risco e dano estão sendo analisados naquele contexto, a fim de considerar reflexões produzidas naquele contexto e que podem beneficiar o debate nacional. Atualmente não há um consenso doutrinário ou jurisprudencial sobre o tema nos EUA. Contudo, alguns tribunais e certos juristas de renome na área de proteção de dados (p. ex. Daniel Solove e Danielle Citron[11]) têm entendido que o risco gerado por um incidente de segurança da informação que afete dados pessoais (*data breach*) também se traduz em dano aos titulares afetados.

[11] "In our view, anxiety, and risk, together and alone, deserve recognition as compensable harms. […] The number of people affected by data breaches continues to rise as companies collect more and more personal data in inadequately secured data reservoirs [38]. Risk and anxiety are injuries in the here and now. Victims of data breaches have an increased risk of identity theft, fraud, and reputational damage. Once victims learn about breaches, they may be chilled from engaging in activities that depend on good credit, like house […]". SOLOVE, Daniel J.; e CITRON, Danielle Keats. **Risk and Anxiety**: A Theory of Data Breach Harms. GWU Legal Studies Research Paper No. 2017-2. 2017. pp 744-745. Acesso em:24/03/2021. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2885638. pp 744-745

	Este argumento é construído em parte ao se analisar como um número expressivo de incidentes têm afetado as vítimas, principalmente os de violação de confidencialidade. Como os dados violados são geralmente usados para fraudes e roubo de identidade, há um aumento de risco expressivo após o incidente que coloca os titulares em situação pior daquela em que se encontravam anteriormente, o que configura um dano. As cortes nos EUA identificam em casos de incidente que, normalmente, os titulares afetados acabam sendo forçados a tomar providências para evitar fraudes em seu nome; sofrem de ansiedade gerada pelos riscos de uso indevido; sofrem maior risco de terem impactos negativos em suas notas de crédito, o que afeta sua capacidade de realizar empréstimos (p. ex. comprar um imóvel, abrir um negócio etc.); entre outras consequências. A título ilustrativo, o Departamento de Justiça dos EUA estimou que 26 milhões de residentes nos EUA sofreram roubo de identidade em 2016.[12] O entendimento que o risco gerado por um incidente de segurança também gera dano aos afetados têm sido adotados pelos tribunais recursais do Sexto, Sétimo e Oitavo Circuitos Federais dos EUA.[13] A lógica do risco como um dano pode ser exemplificada por um julgado do 7º Circuito, relacionado a um caso de invasão de sistema de um restaurante onde dados cadastrais e de cartão de crédito de clientes foram obtidos ilicitamente: "O aumento do risco de haver cobranças fraudulentas e de haver roubo de identidade decorre do fato de seus dados terem sido roubados. As lesões alegadas são concretas o suficiente para garantir sua legitimidade processual. [...] É plausível inferir um risco substancial de dano originado do incidente de segurança [data breach], porque um dos principais incentivos

[12] ESTADOS UNIDOS. HARRELL, Erika. U.S. Department of Justice. Victims of Identity Theft, 2016. Acesso em 24/03/2020. Disponível em: https://bit.ly/31fcv0F

[13] Nos EUA, existem três instâncias de Justiça Federal: **(i)** a primeira instância é a "United States District Court"; **(ii)** a segunda instância "United States Court of Appeals", também chamados de "Circuit Courts"; e **(iii)** a última instância referente a "Supreme Court of the United States"

	dos hackers é '*mais cedo ou mais tarde [] fazer cobranças fraudulentas ou roubar as identidades dos consumidores afetados*'"[14] (tradução nossa) Adicionalmente, os tribunais que compõem esses circuitos têm entendido como dano: (**i**) os gastos com serviço de monitoramento contra fraudes; e (**ii**) os demais custos incorridos na tentativa de remediar o incidente (p. ex. tempo gasto com cancelamento de cartões de crédito, com a verificação de compras suspeitas, fechamento e abertura de novas contas bancárias)[15]. Desse modo, percebe-se como a interpretação jurídica de incidentes de segurança da informação tem sido um desafio para diversos ordenamentos, trazendo questões semelhantes - como em relação a definição de dano e risco - e produzindo, até mesmo, entendimentos similares sobre o tema. Assim sendo, entende-se razoável equiparar risco e dano para os fins da matéria tratada pelo art. 48. da LGPD.
4. O que deve ser considerado na avaliação dos riscos do incidente?	A avaliação de risco deve considerar os critérios indicados na resposta à pergunta 1. Adicionalmente, recomenda-se a consideração de critérios utilizados por outras autoridades nacionais de proteção de dados, a exemplo da Comissão de Privacidade do Canadá[16]. Também deve ser levado em conta o histórico de violações já analisadas pela ANPD – considerada a evolução do estado da arte em metodologias de gestão de incidentes de segurança –, a fim de preservar a consistência de suas decisões e criar previsibilidade para o cenário regulatório de proteção de dados no país.

[14] "the increased risk of fraudulent charges and identity theft they face because their data has already been stolen. These alleged injuries are concrete enough to support a lawsuit. P.F. Chang's acknowledges that it experienced a data breach in June of 2014. It is plausible to infer a substantial risk of harm from the data breach, because a primary incentive for hackers is "sooner or later [] to make fraudulent charges or assume those consumers' identities[.]". ESTADOS UNIDOS. United States Court of Appeals for the 7th Circuit. Lewert v. P.F. Chang's China Bistro, Inc, No. 14-3700. 2016. p.6. Acesso em: 24/03/2021. Disponível em: https://bit.ly/31giPVO.

[15] DOWTY, Megal. Life is Short, Go to Court: Establishing Article III Standing in Data Breach Cases. Southern California Law Review, Vol. 90, nº 3. março de 2017. p.687. Disponível em: https://bit.ly/3rkEt5G. Acesso em: 19/02/2019.

[16] CANADÁ. Escritório da Comissão de Privacidade do Canadá**. What you need to know about mandatory reporting of breaches of security safeguards**. Outubro, 2018. Disponível em: <https://bit.ly/2P2qLYd>. Acesso em: 23/03/20201.

5. Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	Quanto às informações listadas na lei, indicamos que a ANPD detalhe as informações contempladas pelos incisos do §1º do art. 48, de forma que: a descrição e natureza dos dados (inciso I) contemple a indicação de categorias de registros tratados, se são relativos à saúde, registros escolares, financeiros, etc., por exemplo; as informações sobre os titulares (inciso II) incluam categorias de titulares afetados e indiquem se há segmentos sociais vulneráveis afetados, conforme recomenda o Grupo de Trabalho sobre o Artigo 29[17]; as informações sobre riscos relacionados ao incidente (inciso IV) indiquem se algum tipo de prejuízo específico é suscetível de ocorrer, como fraude no cartão de crédito, a partir dos registros e titulares afetados. Além disso, consideramos que os controladores **devem notificar à ANPD o nome e o contato do encarregado (caso a organização o tenha) ou outro ponto de contato por meio do qual informações possam ser obtidas**. Essa recomendação é análoga à previsão contida no art. 33, parágrafo 3 do RGPD da UE. Adicionalmente, **devem informar data e hora aproximadas do incidente, bem como do momento em que o agente de tratamento tomou ciência dele**. A inclusão dessas informações visa facilitar as diligências relativas ao incidente e a avaliação das medidas de contingência tomadas pelo agente em resposta.
6. Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	A regra geral para notificação de um incidente de segurança deve ser em prazo mais rápido possível, ou seja, não pode haver demora injustificada. Importante apontar que isso deve se aplicar tanto à comunicação do incidente quanto à ação por parte da própria ANPD. Nesse sentido, recomenda-se a formulação de um regime de comunicação emergencial para incidentes de alta gravidade, que deve operar inclusive durante feriados e finais de semana. Além disso, recomenda-se que a ANPD estabeleça prazos conforme a gravidade do incidente de segurança. Assim, **quanto maior o risco aos titulares de dados, mais rápida deve ser a notificação**. O parâmetro de 72h como limite para notificação, a

[17] WP29 - **Guidelines on Personal data breach notification under Regulation 2016/679.** 2018. Disponível em: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052>. Acesso em 23/03/2021, p. 15.

	exemplo do que considera o RGPD também parece se aplicar de forma adequada ao cenário brasileiro. O termo inicial do prazo deve ser quando o responsável pelo tratamento tem um grau razoável de certeza de que ocorreu um incidente de segurança que afetou dados pessoais. Da mesma forma, a notificação não deve ser realizada apenas ao final da investigação sobre o incidente ou depois de tomadas as medidas de segurança. Isso porque a avaliação completa pelo agente poderá ser realizada em paralelo às medidas estabelecidas pela ANPD, que deverá acompanhar a progressão da investigação.
7. Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	**A regra geral para notificação de um incidente de segurança deve ser em prazo mais rápido possível, ou seja, não pode haver demora injustificada**. A ANPD deve estabelecer prazos conforme a gravidade do incidente de segurança. Assim, quanto maior o risco aos titulares de dados, mais rápida deve ser a notificação, observado o limite de 72h, como se sugere aplicar à ANPD. Além das informações definidas pelo §1º do art. 48 da LGPD, a notificação aos titulares deve incluir **os dados pessoais tratados pelo agente que não foram afetados pelo incidente e incluir canal de comunicação[18] para atendimento aos titulares.** Isso considera a necessidade de que a população em geral faça parte da construção de uma cultura de proteção de dados pessoais que o Brasil procura alcançar. A inclusão dessa informação pode contribuir ainda para evitar repercussões desproporcionais ou equivocadas ao incidente. Entre as informações listadas, vale destacar a orientação de auxiliar os titulares em relação a quais medidas eles podem tomar para se proteger do incidente.

[18] ESTADOS UNIDOS. Federal Trade Commission. **Data Breach Response:** A Guide for Business. 2019. Disponível em: https://bit.ly/3rdPhCV. Acesso em: 20/03/2021.

8. Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	A comunicação pode se dar por múltiplas formas, que incluem o envio individual de mensagens diretas ou a exibição de faixas ou notificações em sites ou plataformas de elevada visibilidade[19]. Deve ser dada preferência aos meios mais ágeis de comunicação aos titulares. Nesse sentido, meios de comunicação impressos e comunicação postal podem ser utilizados na impossibilidade do titular ser alcançado por outras vias. A depender do caso, múltiplos meios podem se fazer necessários. O conteúdo das notificações deve estar escrito de forma acessível e compreensível aos titulares, o que exige linguagem nítida e uso da língua portuguesa. No caso de mensagens diretas, estas podem ser feitas por e-mail, SMS ou plataformas de mensageria e devem ser realizadas de forma específica, ou seja, não podem ser enviadas junto de outras informações (ex: atualizações comuns, boletins informativos, etc). Não seriam consideradas notificações adequadas, por exemplo, emissões de comunicados de imprensa ou publicações em blogs empresariais de baixa visibilidade.
9. Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	**Cabe salientar que a comunicação, ainda que por etapas, é a regra geral para que a ANPD possa validar o juízo de relevância do incidente e tomar as providências que garantam a efetiva proteção dos dados pessoais.** Essa obrigação dos agentes deve ser afastada apenas quando o agente puder demonstrar que foram adotadas, preventiva ou reativamente, medidas técnicas e/ou organizacionais capazes de assegurar que o prejuízo potencial resultante do incidente não se concretizará. Isso pode ser aplicável, a depender do caso, quando os dados afetados pelo incidente já eram considerados públicos ou quando, com base em padrões técnicos, seja possível assegurar que a disponibilidade e integridade dos dados não foram afetadas, ainda que o outro atributo de segurança da informação, a confidencialidade, tenha sido comprometido. Este é o caso, por exemplo, de violações de confidencialidade de dados tornados ininteligíveis de forma segura (com criptografia forte, por exemplo, cuja chave criptográfica não foi comprometida) e existem cópias

[19] WP29 - **Guidelines on Personal data breach notification under Regulation 2016/679.** 2018. Disponível em: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052>. Acesso em 23/03/2021. p.22.

	seguras dos dados. Mesmo assim, se houver comprometimento posterior de tais padrões de segurança, fica o agente obrigado a notificar a ANPD. A exceção baseada na robustez das práticas de segurança da informação pode representar, igualmente, incentivos para a utilização de sistemas cada vez mais protetivos e reforçar a importância da adoção de medidas técnicas adequadas ao tratamento dos dados pessoais.
10. Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	Com base no exposto previamente, identificamos três cenários em que é razoável desobrigar o agente de tratamento do dever de notificação ao titular. O primeiro deles corresponde à inexistência de risco ou dano grave ao titular. Essa inexistência é constatada pela demonstração, por parte dos agentes de tratamento, de que o incidente não atingiu dados sensíveis e de que o prejuízo potencial que dele sucede é improvável de se concretizar e pouco severo, caso se concretize. O insucesso em demonstrar a ocorrência de qualquer um desses três requisitos deve ser suficiente para o enquadramento do risco ou dano resultante do incidente como grave e acionamento da obrigação de notificação aos titulares. O segundo cenário corresponde mais a um afastamento temporário ou parcial da obrigação de notificação. Ele diz respeito à recepção, pelos agentes, de orientações expressas para não notificar os titulares por parte da ANPD. Isto pode ocorrer no contexto de violações que atinjam dados relevantes para investigações criminais ainda em curso, por exemplo, em que pese a necessidade de verificação da aplicabilidade da LGPD no caso concreto. Nesses casos, a ANPD deve justificar suas orientações à luz dos riscos que a realização da notificação pode gerar para a condução das investigações e com base em padrões técnicos bem definidos. Alternativamente, a ANPD pode orientar o agente a realizar uma notificação parcial que exclua as informações que não possam ser compartilhadas naquele momento, porém comunique o titular das demais. Em todos os casos, tão logo cesse o risco decorrente da realização de notificação completa, a obrigação de notificar se torna aplicável novamente e os agentes deverão observá-la. Recomenda-se que

	a ANPD delimite rigorosamente as hipóteses em que tais orientações poderão ser emitidas. Por fim, o terceiro cenário se refere à incapacidade operacional do agente para o cumprimento do dever de notificação ao titular. Esse seria o caso, por exemplo, de violações à disponibilidade e/ou à integridade dos dados que comprometam o conhecimento do agente sobre a identidade dos titulares afetados. Um incêndio que provocou a destruição de documentos físicos contendo dados pessoais dos quais não havia cópias pode ter precisamente tais repercussões, que tornam efetivamente impossível a operacionalização da notificação individualizada. Assim como no segundo caso, o afastamento da obrigação de notificação deve ser apenas parcial, de modo que o agente reste compelido a notificar os titulares presumidos por outros meios cabíveis, como publicações em sites e/ou plataformas de elevada visibilidade. A notificação, nesses casos, deve informar quais categorias de titulares o agente presume terem sido afetadas – por exemplo, pessoas nascidas em uma cidade particular entre as datas x e y.
11. Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	Recomenda-se a realização da análise da gravidade de incidentes com base em metodologias já consolidadas para gestão de riscos em organizações. Algumas dessas metodologias cuja observância é recomendável serão enumeradas na resposta ao tópico 12. Critérios específicos para essa análise podem incluir, por exemplo: ● O contexto da atividade de tratamento de dados, observada a natureza dos dados envolvidos no incidente, sua vulnerabilidade e potencialidade para repercutir em eventos danosos para titulares de dados; ● A sensibilidade dos dados envolvidos no incidente; ● A facilidade de identificação dos titulares de dados a partir das informações envolvidas no incidente em questão; ● As circunstâncias do incidente, por exemplo, se os dados foram comprometidos de forma dolosa; ● A probabilidade de que o incidente repercutirá em uso não autorizado dos dados comprometidos; ● A adoção ou não de medidas de contingenciamento reativas, pelos agentes de tratamento, de forma que as consequências do incidente sejam anuladas, cessadas ou, ao menos, minimizadas;

	● O número de titulares cujos dados foram envolvidos no incidente em questão; ● Características específicas ligadas ao titular de dados, por exemplo, quando dados de crianças ou de grupos de indivíduos vulneráveis estão envolvidos no incidente; ● Entre outros.
12. Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	Existem diversas metodologias para análise de incidentes de segurança, de modo que sugerimos que a ANPD se apoie no estado da arte relativo à segurança da informação e incidentes de segurança. A título de exemplo do que já foi introduzido para o cenário brasileiro, a ABNT NBR ISO/IEC 27001 – relativa a técnicas de segurança em sistemas de gestão de segurança da informação – remete à ISO/IEC TR 13335-3 sobre metodologias para análise e avaliação de risco. Na mesma linha encontra-se a ISO/IEC 27005:2011, que foi criada para substituir a ISO/IEC TR 13335-3. Ambas foram validadas e possuem relevância internacional para gestão de riscos em atividades de tratamento de dados pessoais. Adicionalmente, como a família de padrões ISO 27000 refere-se especificamente ao ambiente de tecnologia da informação em uma organização, pode-se citar também a ISO/IEC 31000:2018, para gestão de riscos de natureza mais geral. Além disso, as recomendações da ENISA[20], embora publicadas no ano de 2013, ainda representam um bom referencial para a constituição de uma metodologia de análise da gravidade de incidentes de segurança. Essa metodologia considera como fatores principais o contexto do tratamento de dados (tipo de dado afetado, por exemplo), a facilidade de identificação dos titulares e as circunstâncias do incidente (atributos de segurança afetados e existência de dolo na violação). Essas são possíveis fontes de metodologia que, integradas e aplicadas no que é pertinente ao sistema brasileiro de proteção de dados pessoais, podem auxiliar a definição da metodologia

[20] ENISA. **Recommendations for a methodology of the assessment of severity of personal data breaches**: working document, v1.0, december 2013. Heráclito: Enisa, 2013. Disponível em: <https://www.enisa.europa.eu/publications/dbn-severity>. Acesso em: 23/03/2021.

	própria da ANPD, a partir dos parâmetros oferecidos nesta Tomada de Subsídios.
13. Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	**Sugestões de Providências** Considerando a finalidade de prevenção e mitigação de danos, seguem algumas sugestões de providências. ● Definição de uma política/plano de resposta a incidentes de segurança da informação. ● Estabelecimento de políticas de segurança com previsão de realização de treinamentos regulares com os colaboradores. ● Notificar os demais agentes de tratamento que possam ter sido afetados, a fim de que eles possam tomar providências adequadas de mitigação do incidente. ● Estabelecimento de canal de contato específico para os titulares afetados por um incidente. ● Aconselhar os titulares afetados sobre quais medidas adicionais eles podem adotar para mitigar/impedir os riscos e danos (p. ex. troca de senha; verificar se houve transações suspeitas, etc). ● Fornecer seguro contra fraudes para os titulares afetados. Em relação às providências exigidas pela ANPD, é recomendável que ela estabeleça um prazo de adoção de medidas para o agente. Nesse sentido, deve-se exigir que o agente comprove à ANPD que adotou as medidas necessárias após transcorrido o prazo (p. ex. através de envio de documentos comprobatórios, como no caso de políticas internas, contratação de serviços de consultoria, etc). **Manutenção dos Registros de Incidentes** Uma prática que deve ser exigida dos agentes de tratamento - e que deve ser verificada pela ANPD após a ocorrência de um incidente - é a manutenção de registros dos incidentes de segurança que afetam dados pessoais. Esses registros também devem conter, necessariamente, casos nos quais os agentes concluíram que não seria necessário uma notificação à ANPD e/ou titulares.

	Essa exigência é inferida da própria LGPD, pelo princípio da responsabilização e prestação de contas (art. 6, X), e pela própria lógica do mecanismo de notificação de incidentes relevantes. Considerando que a LGPD estabelece que somente incidentes relevantes devem ser notificados, a primeira análise de risco será realizada pelo próprio agente de tratamento. Assim, ocorrerão casos em que um incidente, a princípio, foi considerado como não relevante para fins de notificação, mas que desenvolvimentos futuros levem a constatação de que, na verdade, o incidente causou riscos ou danos consideráveis aos titulares envolvidos (p. ex. resultados mais precisos de uma investigação). Ainda, pode haver casos em que a materialização de parte do risco/dano ocorre somente após o incidente. Citamos como exemplo, um caso hipotético em que uma empresa X constatou invasão ao seu banco de dados por agente externo, contudo, não foi possível confirmar se houve ou não exfiltração dos dados pessoais. Após o incidente, houve reportagem midiática sobre a venda ilegal de banco de dados que teria como possível origem a empresa X. Em situações semelhantes a essa, a ANPD deve verificar se as análises de risco realizadas pela empresa X foram feitas de forma adequada, a fim de confirmar se a decisão do agente de não informar estava baseada em uma análise de risco/dano consistente com a LGPD e com as informações disponíveis no momento. Ou seja, considerando a natureza complexa que caracteriza parte dos incidentes de segurança da informação e as dificuldades forenses de uma investigação, um *assessment* inicial pode não constatar os riscos e danos relevantes que justificariam uma notificação, mas que podem ser descobertos ou vir a se materializar posteriormente. Assim, a exigência de manutenção de registros de incidentes de segurança da informação que afetam dados pessoais, **independentemente da gravidade**, é um incentivo para que os agentes não realizem análises inadequadas e negligentes para não terem de realizar uma notificação. Sob viés comparativo, a manutenção de registros de incidentes de segurança da informação é exigida no RGDP (art. 33, (5)), o qual estabelece que qualquer incidente de segurança que afete dados pessoais deve ser registrado pelo agente de tratamento; principalmente em relação aos fatos, os efeitos gerados e as

	ações de resposta/mitigação tomadas. A legislação de proteção de dados do Canadá também exige que os responsáveis pelo tratamento mantenham registros de todos os incidentes de segurança da informação que afetam dados pessoais; os quais podem ser requisitados pela agência reguladora.[21]
SUGESTÃO DE NORMATIVO, SE HOUVER	
Art. Xxxx	
Art. Xxxx	

Referências:

BESSA, Leonardo Roscoe.Responsabilidade objetiva no Código de Defesa do Consumidor. **Revista Jurídica da Presidência** Brasília v. 20, nº 120. Fev./Maio 2018 p. 27.Disponível em: <https://bit.ly/3tHrYCR>. Acesso em 21/03/2021.

BRASIL. **Lei nº 12.414**, de 9 de junho de 2011 (Lei do Cadastro Positivo). Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12414.htm>. Acesso em: 24/03/2021.

BRASIL. Superior Tribunal de Justiça (1ª Turma). **Recurso Especial 608.918/RS. 25/05/2004.** Acesso em: 18/03/2021. Disponível em: <https://bit.ly/3tqe3kC>

CANADÁ. **Personal Information Protection and Electronic Documents Act**. 2000. Disponível em: <https://bit.ly/2QgeZto>. Acesso em: 20/03/2021.

CANADÁ. Escritório da Comissão de Privacidade do Canadá**. What you need to know about mandatory reporting of breaches of security safeguards**. Outubro, 2018. Disponível em: <https://bit.ly/2P2qLYd>. Acesso em: 23/03/20201.

[21] Artigos 10.3(1) e (2), Division 1.1. CANADÁ. **Personal Information Protection and Electronic Documents Act**. 2000. Disponível em: <https://bit.ly/2QgeZto>. Acesso em: 20/03/2021.

DOWTY, Megal. Life is Short, Go to Court: Establishing Article III Standing in Data Breach Cases. **Southern California Law Review**, Vol. 90, nº 3. março de 2017. p.687. Disponível em: https://bit.ly/3rkEt5G. Acesso em: 19/02/2019.

EDPD. **European Data Protection Board's Guidelines 01/2021 on Examples Regarding Data Breach Notification.** Disponível em: <https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf>. Acesso em: 24/03/2021.

ENISA. **Recommendations for a methodology of the assessment of severity of personal data breaches**: working document, v1.0, december 2013. Heráclitón: Enisa, 2013. Disponível em: <https://www.enisa.europa.eu/publications/dbn-severity>. Acesso em: 23/03/2021.

ESTADOS UNIDOS. HARRELL, Erika. U.S. **Department of Justice**. Victims of Identity Theft, 2016. Acesso em 24/03/2020. Disponível em: https://bit.ly/31fcv0F

ESTADOS UNIDOS. Federal Trade Commission. **Data Breach Response:** A Guide for Business. 2019. Disponível em: <https://bit.ly/3rdPhCV>. Acesso em: 20/03/2021.

ESTADOS UNIDOS. **United States Court of Appeals for the 7th Circuit**. Lewert v. P.F. Chang's China Bistro, Inc, No. 14-3700. 2016. p.6. Acesso em: 24/03/2021. Disponível em: https://bit.ly/31giPVO.

ICO. **ICO Guide to the General Data Protection Regulation - Personal Data breaches**. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/#whendowe>. Acesso em: 24/03/2021.

ISO. **ISO IEC 27005:2008** - Information Technology - Information Security Risk Management.

SCHREIBER, Anderson. **Novos Paradigmas da Responsabilidade Civil** - Da Erosão dos Filtros da Reparação à Diluição dos Danos. São Paulo: Editora Atlas. 3ª Edição. 2011. p. 204.

SOLOVE, Daniel J.; e CITRON, Danielle Keats. **Risk and Anxiety**: A Theory of Data Breach Harms. GWU Legal Studies Research Paper No. 2017-2. 2017. pp 744-745. Acesso em:24/03/2021. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2885638.

TARTUCE, Flávio; e NEVES, Daniel Amorim Assumpção. **Manual de direito do consumidor**. São Paulo: Editora Forense. 5ª edição. 2016.

WEST, Sarah Myers. Data Capitalism: Redefining the Logics of Surveillance and Privacy. **Business & Society**, Vol. 58(I). 2019. p. 23. Disponível em: <https://bit.ly/3cSsWW5>. Acesso em: 21/03/2021.

WP29 - Guidelines on Personal data breach notification under Regulation 2016/679. 2018. DIsponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052>. Acesso em: 24/03/2021.

ZANATTA, Rafael A. F. Artigos Selecionados REDE 2017 **I Encontro da Rede de Pesquisa em Governança da Internet**. Rio de Janeiro. 14/11/ 2017.p. 184. Disponível em: <https://bit.ly/2Ps3ApT> . Acesso em: 24/03/2021.

ITI Promoting Innovation Worldwide

Comentários do Information Technology Industry Council sobre Comunicação de Incidentes de Segurança com Dados Pessoais

Março, 2021

O Information Technology Industry Council (ITI) é o principal defensor global da tecnologia, representando as empresas mais inovadoras do mundo. Fundado em 1916, o ITI é uma associação comercial internacional com uma equipe de profissionais em quatro continentes. Promovemos políticas públicas e padrões da indústria que incentivam a concorrência e a inovação em todo o mundo. Nossa associação diversificada e equipe de especialistas fornecem aos formuladores de políticas públicas a mais ampla perspectiva e liderança de pensamento em tecnologia, hardware, software, serviços e setores relacionados.

Um dos elementos de nossa missão, em todas as economias do mundo, é posicionar nossas empresas como verdadeiras parceiras do governo. O ITI navega pelos relacionamentos entre formuladores de políticas públicas, empresas e organizações não governamentais, fornecendo soluções criativas que promovem o desenvolvimento e o uso da tecnologia em todo o mundo. Fazemos isso porque acreditamos firmemente que os interesses de nossas empresas e do setor estão fundamentalmente alinhados aos das economias e sociedades em que operamos.

Como nosso mundo está cada vez mais digitalizado e orientado por dados, a segurança da informação é justamente uma prioridade para cidadãos, empresas e governos. A expansão fenomenal do ecossistema interconectado e sem fronteiras da Internet possibilitou um crescimento econômico, inovação e oportunidades sem precedentes. No entanto, essa conectividade traz riscos elevados e ameaças em constante evolução às nossas redes, sistemas e dados. Como a transformação digital permeia todos os aspectos da sociedade, desde dispositivos de consumo até infraestrutura crítica, os interesses da indústria e do governo em proteger as atividades habilitadas digitalmente estão fundamentalmente alinhados. Os sistemas de rede hoje sustentam muitos dos sistemas mais críticos em nossas economias. Esses sistemas devem ser adequadamente protegidos contra ameaças cibernéticas e as organizações devem adotar cada vez mais mecanismos e práticas baseadas em gestão de riscos para identificar, avaliar e mitigar danos potenciais, se quisermos garantir que os benefícios criados pela digitalização de nossas economias não sejam superados pelos riscos.

De forma mais geral, o ITI sublinha que ter uma estrutura de responsabilidade robusta dentro de uma organização é essencial para avaliar os riscos relevantes, implementar um nível de segurança adequado aos riscos identificados, conceber políticas e procedimentos de gestão de crises adequados, treinar funcionários, realizar diligência de agente de tratamento, além de práticas de auditoria para responder a um incidente de segurança.

Nesse sentido, parabenizamos a iniciativa da ANPD de abrir essa tomada de subsídios para discutir a comunicação de incidentes de segurança com dados pessoais. Acreditamos que é importante promover uma discussão entre todas as partes interessadas, a fim de compreender os fatores de risco a considerar na avaliação de incidentes de segurança e decidir se é necessária uma comunicação à ANPD e aos titulares.

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
www.itic.org
@iti_techtweets

Notamos que, na União Europeia, por exemplo, tem havido uma tendência entre as organizações de sobre-notificação de incidentes de segurança, o que resultou em autoridades locais sendo sobrecarregadas com comunicações[1]. Considerando o tamanho bastante enxuto da ANPD atualmente, este é um ponto de séria preocupação para a ANPD e instamos a regulamentação a considerar critérios para que a ANPD se concentre nos casos mais relevantes, em vez de receber todas e quaisquer comunicações de incidentes de segurança de dados pessoais.

O ITI espera que suas considerações ajudem a ANPD a identificar em quais situações as organizações devem notificar a autoridade de proteção de dados e os titulares de dados. Nossos comentários oferecem recomendações pragmáticas que consideram a complexidade dessas situações de incidentes de segurança para organizações que são vítimas de ataques perpetrados por malfeitores, como normalmente é o caso.

Uma abordagem de privacidade baseada em risco

Em um momento em que a nova era da informação desafia os conceitos e práticas de privacidade aceitos e pressiona nossos recursos limitados de conformidade e fiscalização, as organizações e os reguladores precisam priorizar suas atividades e encontrar novas maneiras de transformar requisitos abstratos em proteções de dados pessoais reais e eficazes. Como o ritmo da mudança tecnológica ultrapassa o pensamento convencional de legisladores, reguladores e empresas, sugere-se que uma abordagem calibrada e baseada em gestão de risco pode melhorar a capacidade das organizações em adotar uma abordagem mais bem informada e estruturada para lidar com problemas volumes colossais de informações pessoais que eles coletam, recebem, armazenam, usam e compartilham diariamente, bem como o potencial consequente para incidentes de segurança.

Leis de proteção de dados baseadas em princípios, como a LGPD, muitas vezes deixam o espaço necessário para contextualização, deixando para as organizações a tomada de decisões adequadas sobre como implementar esses princípios e os reguladores sobre como interpretar e fazer cumprir a lei, permitindo diferentes negócios de diferentes tamanhos e naturezas incorporar os princípios com o devido respeito e consideração pelas suas especificidades. O conceito de uma estrutura de responsabilidade baseada em risco visa preencher a lacuna entre os princípios de proteção de dados genéricos, por um lado, e a conformidade, por outro, desenvolvendo uma metodologia para que as organizações apliquem, calibrem e implementem obrigações abstratas de proteção de dados com base em gestão de riscos e benefícios reais do tratamento de dados proposto. Na verdade, a proteção de dados sempre se baseou na gestão de riscos como uma ferramenta crítica para cumprir as leis de proteção de dados e garantir que os dados sejam tratados de forma adequada e os direitos e interesses fundamentais dos titulares sejam protegidos de forma eficaz.

Isso ocorre porque uma abordagem de proteção de dados pessoais baseada em risco pode ajudar a fornecer maior clareza e proteção de dados mais eficaz. Vai além da mera conformidade com os requisitos regulamentares, pois pretende abordar o que as organizações responsáveis procuram alcançar, como implementam os requisitos de proteção de dados e como demonstram conformidade. Todas as organizações devem ser responsáveis por suas atividades de tratamento de dados e, portanto, ter programas de gerenciamento de proteção de dados que incluem todos os

[1] https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=21356

elementos de responsabilidade acordados (por exemplo, um encarregado, supervisão eficaz, políticas e procedimentos, treinamento, avaliação e verificação, aplicação, reparação e gestão de risco).

A maneira como esses programas de gerenciamento de proteção de dados baseados em risco são criados e como são implementados muito provavelmente dependerá dos riscos apresentados pelo tratamento de dados. Como um elemento central de responsabilidade, a abordagem baseada em risco permite que as organizações maximizem os benefícios potenciais do tratamento e usos mais amplos de dados, enquanto reduz de forma mais eficaz quaisquer potenciais impactos negativos sobre as pessoas, pois prioriza a ação, aumenta e informa a consciência sobre os riscos, identifica medidas de mitigação apropriadas e, nas palavras do antecessor do European Data Protection Board, o *Article 29 Working Party*, fornece uma "abordagem escalonável e proporcional para conformidade"[2].

Portanto, podemos afirmar que a gestão de riscos envolve três elementos principais - (1) o processo sistemático de identificação e avaliação de danos e outros impactos negativos, (2) evitar ou mitigar riscos relevantes, e então (3) aceitar e gerenciar quaisquer riscos restantes. Afinal, raramente o risco pode ser totalmente eliminado. O objetivo do processo de gerenciamento de risco é fornecer respostas proporcionais que reduzam riscos relevantes e identifiquem os riscos remanescentes e como eles serão gerenciados.

Tal processo de gestão de risco traz um desafio ao regulador quanto ao equilíbrio ideal entre a regulação para trazer certeza jurídica sobre como cumprir os princípios da lei e a transposição deles para a realidade de modo que as organizações considerarem o contexto de seus negócios, o volume e a natureza dos dados coletados para definir os riscos envolvidos nas suas operações de tratamento de dados pessoais.

Identificando os elementos de risco (atividades arriscadas de tratamento, ameaças e possíveis danos)

De acordo com a OCDE, em sua "Recomendação sobre Diretrizes para a Proteção da Privacidade e Fluxos Transfronteiriços de Dados Pessoais", o "risco pretende ser um conceito amplo, levando em consideração uma ampla gama de possíveis danos aos indivíduos"[3]. Uma definição de risco que tem sido usada na comunidade de privacidade e proteção de dados e proposta pelo *Center for Information Policy Leadership* (CIPL) é a seguinte: o "risco de privacidade é igual à probabilidade de que uma atividade de tratamento de dados resulte em um impacto, ameaça ou perda de (em vários graus de severidade) um resultado valorizado (por exemplo, direitos e liberdades)"[4]. Em outras palavras, o gerenciamento de risco é sempre um exercício contextual e que definir o padrão de forma prescritiva pode levar a consequências indesejadas.

---

[2] https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf

[3] http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf

[4] https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf

É universalmente reconhecido que o equilíbrio inerente à gestão de riscos deve levar em consideração a magnitude dos riscos potenciais e sua probabilidade de ocorrência. O padrão global de gerenciamento de risco ISO 31000, mantido pela Organização Internacional de Padronização, define “nível de risco” como a “magnitude de um risco ou combinação de riscos” e “sua probabilidade”[5]. Da mesma forma, o Regulamento Geral de Proteção de Dados da União Europeia (GDPR) se concentra significativamente na gestão de risco, enfatizando a necessidade de "o controlador ou operador" "avaliar os riscos inerentes ao tratamento e implementar medidas para mitigar esses riscos" e determinar "a probabilidade e a gravidade do risco para os direitos e liberdades das pessoas”[6].

A questão é que um risco não é uma mera possibilidade de ocorrência de uma consequência, mas deve ser entendido em termos de sua probabilidade de ocorrer e seu impacto se ocorrer. De acordo com a definição da ISO de "análise de risco": "A análise de risco envolve a consideração das causas e fontes de risco, suas consequências positivas e negativas e a probabilidade de que essas consequências possam ocorrer"[7].

A Metodologia de Gestão de Risco de Privacidade da Comissão Nacional para Informação e Liberdade (CNIL) francesa adota linguagem semelhante para o contexto de proteção de dados:

> *O **nível de risco** é estimado em termos de gravidade e probabilidade.*
>
> *A **gravidade** representa a magnitude de um risco. Depende essencialmente do nível de identificação dos dados pessoais e do nível de consequências dos potenciais impactos.*
>
> *A **probabilidade** representa a viabilidade de ocorrer um risco. Depende essencialmente do nível de vulnerabilidades dos ativos de suporte que enfrentam o nível de recursos das fontes de risco para explorá-los[8].*

Ao avaliar os riscos, é importante considerar todo um ciclo de vida de informações e tratamento de dados. Algumas ameaças serão visíveis no momento da coleta, mas algumas surgirão posteriormente, durante o uso ou compartilhamento de dados. É importante observar que as ameaças também podem mudar durante o ciclo de vida das informações - ameaças antigas podem desaparecer e novas podem se tornar proeminentes. Portanto, a avaliação de risco deve ser adotada como um processo recorrente dentro de uma organização.

As ameaças geralmente surgem do tratamento de dados pessoais, que dizem respeito ou podem estar relacionados a um titular identificável. Uma abordagem ampla das ameaças que surgem ao longo do ciclo de vida dos dados deve, portanto, incluir atividades e características determinadas. Sugere-se que, apesar das condições seguintes normalmente se enquadrarem como tratamento

---

[5] https://www.iso.org/standard/43170.html

[6] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

[7] Idem.

[8] https://www.cnil.fr/sites/default/files/typo/document/CNIL-ManagingPrivacyRisks-Methodology.pdf

ilegal sob a LGPD ou algumas vezes como tratamento legal mas com potenciais ameaças, adicionar o contexto ao tratamento é fundamental para ajudar a determinar e mitigar ameaças:

- coleta de dados injustificável ou excessiva;
- uso ou armazenamento de dados imprecisos ou desatualizados;
- uso inadequado de dados, incluindo:
  a) uso de dados além das expectativas razoáveis dos titulares;
  b) uso incomum de dados além das normas sociais, onde qualquer titular razoável neste contexto faria objeções; ou
  c) interferência ou tomada de decisão injustificáveis, que a organização não possa defender objetivamente;
- dados perdidos ou roubados; e
- acesso, transferência, compartilhamento ou publicação de dados injustificáveis ou não autorizados[9].

Em cada caso das ameaças acima, julgamentos objetivos serão necessários sobre: a) a **probabilidade** de uma ameaça causar danos a titulares de dados; e b) a **gravidade** desse impacto, caso se concretize. Isso significa que a avaliação de uma ameaça decorrente do tratamento de dados deve ser sempre **contextual**. Em outras palavras, é necessária uma flexibilidade que reconheça o contexto como um fator importante na determinação do nível de ameaça e seu potencial para causar danos.

Um dos principais desafios das avaliações de risco de proteção de dados é decidir quais riscos e danos aos titulares devem ser considerados, como avaliá-los e como avaliar a probabilidade e gravidade dos danos. E por dano, entendemos qualquer dano, lesão ou impacto negativo - seja tangível ou intangível, econômico, não econômico ou de reputação - para um titular que possa resultar do tratamento de dados pessoais. Estende-se a qualquer negação dos direitos e liberdades fundamentais. O documento da CIPL de 2014 fornece um catálogo de possíveis "danos" sob três títulos: "danos tangíveis a indivíduos e sofrimento intangível a indivíduos"[10]. O documento fornece os seguintes exemplos ilustrativos de cada um:

1) **Danos tangíveis,** normalmente físicos ou econômicos, incluem:

- lesões corporais;
- perda de liberdade ou liberdade de ir e vir;
- dano ao poder aquisitivo; e
- outros danos significativos aos interesses econômicos, por exemplo, decorrentes de roubo de identidade.

2) **Sofrimento intangível,** avaliado objetivamente, inclui:

- detrimento decorrente do monitoramento ou exposição de identidade, características, atividade, associações ou opiniões;

---

[9] https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/white_paper_1-a_risk_based_approach_to_privacy_improving_effectiveness_in_practice.pdf

[10] Idem.

- efeito inibidor sobre a liberdade de expressão, de associação, etc .;
- dano à reputação;
- medo, constrangimento, apreensão ou ansiedade pessoal, familiar, social ou no local de trabalho;
- intrusão inaceitável na vida privada; e
- discriminação ou estigmatização.

Definição de Incidente de Segurança e Incidente de Segurança com Dados Pessoais

Para evitar mais confusões, importante que a ANPD crie um conceito específico para incidentes de segurança diferente daqueles que envolvem dados pessoais, tendo como referência a definição trazida pela ISO 27035-1: 2016, conforme abaixo:

> *"Um incidente de segurança é qualquer evento adverso identificado que pode prejudicar os ativos de uma organização ou comprometer suas operações"*

E, a partir dessa definição, o ITI recomenda revisar a definição de "incidente de segurança com dados pessoais" conforme previsto nas orientações[11] sobre o assunto apresentadas pela ANPD junto com a tomada de subsídios, esclarecendo a diferença concreta entre os dois conceitos, conforme abaixo:

> *"Um incidente de segurança com dados pessoais é qualquer evento adverso, identificado e confirmado, relacionado à violação na segurança de dados pessoais, os quais possam ocasionar risco relevante para os direitos e liberdades do titular dos dados pessoais, como nos casos de acesso não autorizado, acidental ou ilegal que resulte em destruição, perda, alteração ou vazamento."*

Para evitar que a ANPD fique sobrecarregada de comunicações, bem como para garantir que apenas os incidentes relevantes e confirmados tenham a visibilidade necessária, entendemos que a definição de incidente de segurança com dados pessoais deve ser claro. Isso irá garantir que todos os esforços necessários, em termos de gestão de risco, sejam alocados de forma mais eficiente.

Avaliando a gravidade do incidente de segurança com dados pessoais

Considerando o Artigo 48 da LGDP, que estabelece que *"o controlador de dados deve notificar imediatamente a autoridade nacional e o titular dos dados sobre a ocorrência de qualquer incidente de segurança que possa causar risco ou dano relevante aos titulares dos dados*", bem como a complexidade intrínseca de situações de incidentes de segurança em geral e suas variáveis, o ITI sugere que a ANPD trabalhe na exploração do conceito de "risco ou dano relevante", de acordo com os diferentes conceitos do Código Civil Brasileiro, incluindo alguns exemplos claros, e estabeleça alguns critérios para ajudar as organizações a determinar o nível de gravidade dos incidentes de segurança com dados pessoais identificados durante suas atividades de avaliação de risco.

[11] https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca

É possível e útil identificar e enumerar categorias de risco gerais e amplamente relevantes. Essa identificação e enumeração permitem que as organizações e a ANPD identifiquem e avaliem os riscos específicos associados a uma atividade de tratamento específica ao longo de todo o ciclo de dados (desde a coleta, armazenamento, uso e compartilhamento, até o descarte) de maneira repetível e consistente. Também ajuda as organizações a definir o escopo de suas operações de gerenciamento de risco. Levando em consideração as considerações que trouxemos no item anterior deste documento, e utilizando como referência o "Manual de Segurança do Tratamento de Dados Pessoais" publicado pela Agência da União Europeia para a Segurança de Redes e Informações (ENISA) em 2017[12], gostaríamos de propor uma tabela para ajudar nesta distinção entre diferentes incidentes de segurança de dados pessoais, seus níveis de gravidade e classificação:

CLASSIFICAÇÃO	NÍVEL DE GRAVIDADE	CRITÉRIOS	DESCRIÇÃO
Risco ou dano não relevante	Baixo	Muito pouco impacto para os titulares dos dados; sofrimento intangível	• Um incidente que causa interrupção ou degradação mínima da entrega do serviço aos titulares afetados, ao ambiente de seus titulares ou à operação comercial. • Os titulares podem encontrar alguns pequenos inconvenientes, que serão superados sem nenhum problema (tempo gasto para inserir informações novamente, etc.)
	Médio	Impacto moderado para os titulares dos dados; sofrimento intangível	• Um incidente que causa uma interrupção ou degradação da entrega de serviço aos titulares afetados, seu ambiente de titulares ou operação de negócios. • Os titulares podem encontrar inconvenientes significativos, que serão capazes de superar apesar de algumas dificuldades (custos extras, recusa de acesso a serviços comerciais, falta de compreensão, etc.)
Risco ou dano relevante	Alto	Alto impacto para os titulares dos dados; dano tangível	• Um incidente que causa uma interrupção significativa, real ou potencial, ou degradação da entrega de serviço aos titulares/ambiente de produção principal ou operação de negócios. • Os titulares podem enfrentar consequências significativas, que devem ser capazes de superar, embora com sérias

[12] https://www.enisa.europa.eu/publications/handbook-on-security-of-personal-data-processing

			dificuldades (apropriação indébita de fundos, lista negra por parte de instituições financeiras, danos materiais)
	Muito Alto	Alto impacto para os titulares dos dados; dano tangível **E** Muitas pessoas afetadas	● Um incidente que causa uma interrupção completa da entrega do serviço aos titulares/ambiente de produção principal ou operação de negócios. Não há solução alternativa imediata. ● Os titulares podem encontrar consequências significativas, ou mesmo irreversíveis, que podem não superar.

Acreditamos ser oportuno identificar e enumerar categorias gerais e abrangentes de risco/dano. Essa identificação e dissociação permitem que as organizações e a ANPD identifiquem e avaliem os riscos específicos associados a uma atividade de tratamento específica ao longo de todo o ciclo de dados (desde a coleta, armazenamento, uso e compartilhamento, até o descarte) de maneira repetível e consistente. Também ajuda as organizações a definir o escopo de suas operações de gerenciamento de risco. Consequentemente, isto contribuirá cada vez mais para o cumprimento regulamentar, visto que as organizações têm a devida visibilidade dos riscos potencialmente associados às respectivas atividades de tratamento. Também deve ser utilizado como referência para estabelecer quais incidentes devem ser relatados, a quem, e os respectivos prazos.

Em princípio, entendemos que os critérios para definir a relevância do incidente devem usar como inspiração as mesmas diretrizes para comunicações de incidente de segurança da GDPR. Nesse sentido, a relevância dos riscos e danos deve considerar o tipo de incidente natureza, sensibilidade e volume dos dados pessoais; facilidade de identificação de titulares; gravidade das consequências para os titulares; características especiais do titular (crianças ou outros indivíduos vulneráveis, por exemplo); número de titulares afetados (geralmente, quanto maior o número de titulares afetados, maior o impacto de um incidente); e características especiais do controlador de dados (uma organização médica trata categorias especiais de dados pessoais, o que significa que há uma ameaça maior para os titulares se seus dados pessoais forem violados, em comparação com uma lista de mala direta de um jornal). Incentivamos as jurisdições a buscar requisitos compatíveis entre si, para evitar sobrecarregar as organizações no caso de um incidente de segurança, para criar vários tipos diferentes de relatórios de incidentes.

Por exemplo, a divulgação apenas de nomes não deve ser considerada tão severa quanto a divulgação de nomes juntamente com datas de nascimento.

Em nossa experiência, definir limites vinculados a critérios objetivos e orientados por metodologia ajuda os controladores de dados a entender melhor a verdadeira natureza, o impacto e em quais casos deve-se notificar um incidente, especialmente em resposta à regulamentação nascente, onde a maioria dos controladores erraria por excesso de cautela e teria uma tendência de notificar em excesso, o que também poderia definir expectativas erradas para a ANPD no longo prazo. O baixo risco ou dano não deve ser considerado relevante para a comunicação de incidente, e as razões

para uma classificação 'baixa' devem ser documentadas, juntamente com as medidas de mitigação aplicadas e (quando necessário), uma revisão periódica dos riscos contínuos.

Limiar Mínimo

Como complemento, e corroborando a classificação que criamos na tabela acima, citamos também o esquema de "Violações de Dados Notificáveis" da Austrália, que traz alguns exemplos de "danos graves" (conceito que eles usaram para definir quais incidentes devem ser relatados - semelhante ao termo LGPD de riscos/danos relevante)[13]:

> *"Exemplos de danos graves incluem:*
>
> - *roubo de identidade, que pode afetar finanças e relatório de crédito de uma pessoa*
> - *perda financeira por meio de fraude*
> - *um risco provável de dano físico, como por um ex-parceiro abusivo*
> - *dano psicológico sério*
> - *dano grave à reputação de um indivíduo."*

Da mesma forma, também poderíamos citar a lei canadense de proteção de dados, a Lei de Proteção de Informações Pessoais e Documentos Eletrônicos (PIPEDA)[14], que traz a definição de "dano significativo", que seria o resultado de um "risco real":

> *"A subseção 10.1 (7) do PIPEDA define 'dano significativo' como incluindo 'dano corporal, humilhação, dano à reputação ou relacionamentos, perda de emprego, [perda de] negócios ou oportunidades profissionais, perda financeira, roubo de identidade, efeitos negativos sobre o crédito registro e danos ou perda de propriedade."*

Esses exemplos se encaixam nos níveis de gravidade que definimos como "alto" e "muito alto" na tabela acima. No entanto, acreditamos que existem outras características contextuais que devem ser levadas em consideração e utilizadas para dissociar um nível de gravidade do outro. Por exemplo, o *Information Commissioner's Office* (ICO) publicou um guia listando parâmetros que devem ser levados em consideração por uma organização ao avaliar o impacto de um incidente[15]:

> *"Você [organização] precisa avaliar se o incidente causou um 'impacto substancial no fornecimento' de seu(s) serviço(s) digital(is), a fim de decidir se precisa notificar.*
>
> *[...]. Em suma, ao determinar o impacto de um incidente, você [organização] deve levar em consideração:*

---

[13] https://www.oaic.gov.au/privacy/data-breaches/what-is-a-notifiable-data-breach/

[14] https://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html

[15] https://ico.org.uk/for-organisations/the-guide-to-nis/incident-reporting/#:~:text=You%20must%20notify%20the%20ICO,Centre%20at%20the%20same%20time

- *o número de titulares afetados pelo incidente, em particular aqueles que dependem do serviço para a prestação dos seus próprios serviços;*
- *a duração do incidente;*
- *a distribuição geográfica em relação à área afetada;*
- *a extensão da interrupção do funcionamento do serviço;*
- *a extensão do impacto nas atividades econômicas e sociais; [...]".*

A dissociação dos níveis de gravidade, resultante da combinação da natureza do dano com os contextos e cenários em que estão inseridos, é um exercício interessante em que as organizações e a ANPD podem trabalhar para entender melhor a magnitude dos impactos decorrentes dos incidentes, e também definir quais procedimentos de comunicação são os mais adequados e proporcionais a serem realizados considerando o risco/dano relevante identificado.

Por fim, vale ressaltar que, de acordo com a LGPD, somente riscos ou danos relevantes aos titulares dos dados devem ser comunicados à ANPD. Portanto, esta obrigação deve ser excluída quando não houver risco de dano relevante aos titulares dos dados, com base na determinação razoável do responsável pelo tratamento. Por exemplo, a divulgação de dados criptografados ou anônimos que não identificam os titulares dos dados não deve dar origem a um incidente de segurança passível de ser reportado.

Prazos para comunicação

Para evitar possíveis reações públicas ou desinformação sobre eventuais incidentes de segurança com dados pessoais, a ANPD deveria estabelecer diferentes prazos para a comunicação à autoridade e aos titulares dos dados envolvidos. O conceito de abordagem baseada em risco que mencionamos anteriormente pressupõe que as organizações devem realizar processos sistemáticos para identificar e avaliar os danos e outros impactos negativos que podem surgir do tratamento de dados pessoais.

Uma avaliação de risco confiável inclui uma análise forense detalhada para determinar o risco de probabilidade e gravidade de danos aos titulares e avaliar se o incidente de segurança com dados pessoais deve ser comunicado. Nos cenários mais complexos, e em particular aqueles que envolvem ataques externos sofisticados, as investigações podem ocorrer durante várias semanas antes que os fatos (mesmo os fatos básicos, como se havia qualquer possibilidade de acesso não autorizado aos dados) possam ser estabelecidos.

De acordo com o *Office of the Information Commissioner* australiano, uma organização ou agência tem 30 dias para avaliar se um incidente de segurança pode resultar em danos graves. Entendemos que esse prazo de 30 dias é uma boa e importante referência para que as organizações avaliem com eficácia todos os impactos, riscos, danos - se houver ocorrido - e quantas pessoas foram afetadas. Tendo conhecimento de todos os fatos, as organizações já serão capazes de definir quais atividades relevantes de mitigação de risco - e reparo de danos relevantes - devem ser adotadas. Em seguida, essas informações consolidadas poderiam ser repassadas aos titulares dos dados envolvidos, para que tenham uma ideia melhor do que realmente aconteceu e evitem que sejam "inundados" com comunicações amplas e imprecisas que fornecem mais perguntas do que respostas.

O ITI entende que o prazo sugerido de 2 dias úteis para notificar um incidente seria bastante oneroso e impraticável, especialmente considerando a quantidade de detalhes que uma comunicação deve conter, de acordo com o § 1º do art. 48 da LGPD. Em outras palavras, regulamentação nesse sentido é dissonante dos princípios, pois as organizações estão sendo solicitadas a fazer uma avaliação objetiva e jurídica em um momento em que podem não ter informações suficientes sobre os eventos. Durante esse período, o foco principal nas empresas deve ser a identificação e resposta a atores/atividades mal-intencionados, em vez de cumprir um cronograma de relatórios. Expor informações sobre um incidente antes que um *patch*/correção seja aplicada ou as operações sejam restauradas torna as empresas e seus clientes vulneráveis a ataques de hackers. Esse requisito estrito também aumenta muito a probabilidade de a entidade relatar informações imprecisas ou contextualizadas de forma inadequada.

Nossa sugestão é, portanto, que quando uma organização identifica e confirma um incidente de segurança com dados pessoais, deve emitir uma pré-notificação à ANPD mencionando que há um incidente em avaliação no prazo de 5 dias úteis após a sua confirmação. Após a emissão dessa pré-notificação, a organização tem mais 30 dias para avaliar minuciosamente o evento adverso e confirmar com a ANPD a magnitude dos fatos. Com orientação adicional da ANPD, e identificado que o incidente de segurança com dados pessoais em questão se enquadra em nível de gravidade "alto" ou "muito alto" e, portanto, considerado como risco/dano relevante, a organização deve notificar os titulares dos dados, considerando a avaliação da ANPD conforme prevista no § 2º do art. 48 da LGPD. Recomendamos que os controladores informem os titulares dos dados imediatamente (ou seja, "sem atrasos indevidos") após determinar que um incidente requer comunicação aos titulares dos dados (em vez de um período de tempo definido). Se um determinado período de tempo deve ser aplicado, recomendamos a aplicação de 20 dias úteis após a data em que o controlador comunicou a ANPD e concluiu que o incidente é notificável. Esta comunicação também deve ser limitada a situações em que haja risco real de danos ou danos aos titulares dos dados considerados relevantes. Naturalmente, se o incidente de segurança de dados pessoais for considerado de nível de gravidade "baixo" ou "médio", a organização deve poder optar por se vai notificar os titulares dos dados ou não.

Essa lógica é vista no Canadá, e reforça o conceito de responsabilidade e prestação de contas. De acordo com a Lei de Proteção de Informações Pessoais e Documentos Eletrônicos (PIPEDA)[16], "a organização deve realizar uma 'avaliação de risco' para determinar se o incidente representa um 'risco real de dano significativo' com base nas circunstâncias circundantes. Mesmo se a organização determinar que não há risco significativo de dano que justifique a comunicação, uma avaliação de risco bem documentada pode proteger a organização se houver qualquer investigação subsequente sobre a violação."

Uma organização ou agência poderia comunicar os titulares dos dados por e-mail, mensagem de texto ou chamada telefônica. Porém, caso não seja possível entrar em contato com todas as pessoas de que precisam, a ANPD deve permitir que coloquem a comunicação de incidente de segurança de dados pessoais em seus sites. Esta é uma prática flexível que se mostrou eficaz e foi adotada na Austrália[17] e é recomendada pela Comissão Federal de Comércio dos EUA (FTC)[18].

---

[16] https://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html

[17] https://www.oaic.gov.au/privacy/data-breaches/what-is-a-notifiable-data-breach/

[18] https://www.ftc.gov/tips-advice/business-center/guidance/data-breach-response-guide-business

Quais informações os controladores devem fornecer à ANPD além das informações listadas no artigo 48, parágrafo 8º da LGPD?

O formulário atual de reporte de ocorrências à ANPD inclui:

(i) em relação ao agente de tratamento: o tipo e os dados do agente de tratamento e da entidade que notifica a ANPD (seja ela um controlador ou um processador); se for um processador, informações sobre comunicação ao controlador; e dados do encarregado;
(ii) quanto ao incidente: resumo de como ocorreu o incidente; data e hora em que ocorreu o incidente; quando e como a entidade teve conhecimento do incidente; caso a comunicação à ANPD tenha ocorrido após 2 dias, os motivos do atraso deverão ser justificados; natureza dos dados afetados; quantidade de titulares de dados afetados; categoria dos titulares dos dados;
(iii) no que diz respeito às medidas de segurança: que medidas de segurança, técnicas e administrativas foram tomadas para evitar a recorrência do incidente de segurança?; que medidas de segurança, técnicas e administrativas foram tomadas após o conhecimento do incidente de segurança?; que medidas de segurança, técnicas e administrativas foram ou serão tomadas para reverter ou mitigar os efeitos dos danos do incidente de segurança aos titulares dos dados?; informações sobre os relatórios de impacto do agente de tratamento;
(iv) quanto aos riscos relacionados ao incidente de segurança: quais as consequências prováveis para os afetados e, considerando os titulares afetados, possibilidade de consequências no exterior;
(v) no que diz respeito à comunicação aos titulares dos dados: informação sobre a comunicação das pessoas e, caso não seja notificada, explicação sobre a mesma.

Na visão preliminar do setor produtivo, informação complementar ao §1º do art. 48 deverão ser definidas caso a caso e não no regulamento como uma obrigação geral. A regulamentação deverá dar espaço para a ANPD solicitar informações adicionais conforme a necessidade do caso, mas não deverá incluir itens adicionais ao disposto no §1º do art. 48

Além do acima exposto, a ANPD deve considerar fornecer às entidades notificadoras a oportunidade de esclarecer antecipadamente se o incidente está em andamento, se a investigação e a comunicação são preliminares ou completas e a classificação de risco e gravidade. Além disso, um formulário de relatório abreviado separado também deve permitir que as entidades notifiquem a ANPD por meio de comunicações de 'cortesia', em relação a incidentes de que tenham conhecimento, mas não sejam obrigados a notificar. Quaisquer investigações ou consultas decorrentes de tais comunicações de cortesia devem então ser dirigidas às entidades relevantes que poderiam ter sido responsáveis por notificar a ANPD.

Medidas que a ANPD pode exigir, incluindo medidas técnicas e administrativas, dos controladores a adotar após notificarem os incidentes de segurança

Embora houvesse uma série de medidas que o regulador poderia exigir, incluindo comunicações para titulares de dados, solicitações de informações, restrições de tratamento, cooperação com várias outras agências e mudanças nas políticas, processos e conjuntos de tecnologia do

controlador, não há uma fórmula única de abordagem adequada para isso, e a ANPD precisará considerar caso a caso, dependendo da gravidade do incidente, tamanho do controlador, número de titulares de dados impactados e probabilidade de recorrência do incidente (entre outros).

Obrigada pela oportunidade de fornecer comentários e compartilhar nossas perspectivas sobre essas questões importantes. Esperamos continuar essa conversa com a ANPD e apoiar seus esforços para promover a proteção de dados no Brasil.

Atenciosamente,

Ashley E. Friedman
Vice-presidente de Políticas Públicas

Consulta Pública: Incidentes de Segurança

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO: Instituto de Tecnologia e Sociedade (ITS Rio)

O **Instituto de Tecnologia e Sociedade do Rio de Janeiro** vem, pela presente, apresentar a seguinte contribuição para a Tomada de Subsídios da Autoridade Nacional de Proteção de Dados (ANPD) acerca de regulamentação da Lei nº 13.709/2018, a Lei Geral de Proteção de Dados Pessoais, a respeito do dever de comunicação de incidentes de segurança.

Ementa: Proposta de realização de Tomada de Subsídios para regulamentação do dever de comunicação de incidentes de segurança, nos termos do § 1º do art. 48 da Lei nº 13.709, de 14 de agosto de 2018.

Autoria: Autoridade Nacional de Proteção de Dados (ANPD)

TÓPICO/QUESTÃO	CONTRIBUIÇÃO/INSTITUIÇÃO
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	Em razão do convite realizado ao Instituto de Tecnologia e Sociedade (ITS Rio) para contribuir com sugestões de providências à Autoridade Nacional de Proteção de Dados (ANPD) em sua atuação perante os incidentes de segurança, pretende-se desenvolver as medidas pontuadas durante a reunião. **A Estruturação de um Processo interno** O histórico dos últimos meses com um número significativo de incidentes de segurança (no Superior Tribunal de Justiça, mais 223 milhões de CPFs, mais de 100 milhões de dados de celulares, entre outros) somados ao exemplo europeu, em que houve aumento

	considerável no número de notificações na União Europeia após a entrada em vigor do Regulamento Europeu de Proteção de Dados (“GDPR”) indicam números elevados tanto de incidentes como de notificações à ANPD. Dessa forma, potencialmente um dos principais desafios para a autoridade recém formada será receber, responder e resolver notificações de incidentes de segurança que virão em grandes volumes e possivelmente em crescente complexidade. Nesse sentido, as soluções passam em visualizar a atuação da ANPD de duas maneiras: 1) como plataforma (dentro de um conceito de “governo como plataforma”) ou 2) como prestadora de um serviço essencial (dentro de um conceito de “governo como serviço”). Para tratar dos grandes volumes de notificações, a lógica de plataforma permite que a organização, ainda que diminuta, possa ter um papel central na lida com incidentes de segurança da informação. Pode se apoiar em outras entidades e servir de facilitadora do processo. Nos casos de maior complexidade, por outro lado, a autoridade pode ter que desenvolver as suas capacidades internas para desenvolver os serviços que lhe são requeridos. **I) Como lidar com grandes volumes**: O conceito de governo como plataforma, cunhado pelo americano Chris O’Reilly, é a primeira saída para o desafio do volume de notificações. O governo serve de infraestrutura informacional a permitir a reutilização de informações para construir novas aplicações úteis para a sociedade. Nesse sentido, a ANPD pode servir como ponto focal da comunicação de incidentes, mas não necessariamente concentrar todas as etapas do atendimento às comunicações de incidentes de segurança. De um modo geral, deve estruturar um processo simples, acessível e claro para que os

	diferentes atores do sistema possam se coordenar facilmente. Tenha-se claro que o objetivo nesses casos é diminuir tanto os riscos como os danos propriamente ditos derivados de incidentes de segurança. As formas de sanção servem mais que tudo por seu efeito educacional de evitar a reincidência. **O processo ideal seria que a autoridade desenvolvesse uma verdadeira plataforma que permitisse a ANPD meramente intermediar e supervisionar a interação entre os atores.** A título exemplificativo, a plataforma Consumidor.gov.br, serviço que permite a interlocução direta entre consumidores e empresas para solução de conflitos de consumo pela internet, é um ponto de referência. O monitoramento é realizado pelos órgãos de defesa do consumidor e pela Senacon. São mais de 2 milhões de reclamações registradas e 580 empresas participantes. Atualmente, 80% das reclamações registradas na plataforma são solucionadas pelas empresas, que respondem às demandas dos consumidores em um prazo médio de 7 dias. Da mesma forma que a relação entre empresas e consumidores é intermediada pela plataforma mencionada acima; a relação entre controladores e titulares poderia seguir o mesmo caminho. Assim, a ANPD estaria no centro da resolução de incidentes de segurança, auxiliando tanto aos controladores, como permitindo um espaço seguro de contato com os titulares de dados. Cabe reconhecer que implementar o governo como plataforma, nos termos mencionados, pode exigir certo aporte técnico e ser mais adequado como solução a longo prazo. Nesse sentido, medidas mais rápidas também devem ser consideradas: **Utilizar ferramentas de formulários**, como *typeforms* ou *surveys*, para estruturar o envio de notificação de incidentes, assim os dados obtidos são sistematizados automaticamente, o que facilita a todas as partes. Por

	um lado, os controladores têm claro o tipo de informação que necessitam enviar e, por outro, permite que a ANPD tenha uma visão padronizada das ocorrências; o que facilita na elaboração de relatórios e em avaliações de impacto. A proposta atual de formulário é um passo na direção correta, no entanto, a utilização de ferramentas automatizadas diminui a burocracia além de aumentar a eficiência da ação da autoridade. **Estabelecer opções de resposta mais institucionalizadas**. Na busca de manter a interação contínua com os titulares e controladores no processo de comunicação dos incidentes, é importante instituir opções de *feedbacks* na própria plataforma. Essas respostas e/ou informações podem servir tanto para notificação de incidentes de segurança como denúncias de titulares. Vale inspiração em experiências internacionais como a plataforma da autoridade do Reino Unido que oferece uma **auto avaliação para incidentes de segurança**, **checklists sobre como se preparar ou responder um incidente e exemplos didáticos de mitigação de danos**. **Cooperar com outras entidades para guiar as investigações de incidentes.** Não é necessário que a autoridade seja o braço de investigação em todos os sentidos e para todos os casos. Neste caso, a aplicação de governo como plataforma significa encontrar meios de guiar investigações com o auxílio de parceiros. É notável salientar que a Lei Geral de Proteção de Dados (LGPD), em seu art. 55-J, §4º, incentiva a prática aqui sugerida, isto é, ações de cooperação com órgãos e entidades da administração pública, a fim de facilitar as diferentes competências da ANPD (regulatória, fiscalizatória e punitiva). Cumpre enfatizar que a autoridade de certa forma já atuou de maneira colaborativa - ainda que *ad hoc* - quando abriu procedimento com a colaboração de

	órgãos como a Política Federal para investigar o vazamento de 223 milhões de CPFs. Similarmente, o acordo de cooperação com a Senacon para proteção de dados de consumidores é um movimento no sentido de atuar como plataforma, em que colabora com outros órgãos e autoridades no sentido de satisfazer o seu mandato, qual seja, o de assegurar a proteção de dados pessoais. A sugestão é que tal medida seja replicada com outras entidades para auxiliar na lida com incidentes de segurança. Vale uma nota que ao tratar de segurança da informação, poderia ter um impacto positivo se fosse levada em consideração a participação e a colaboração com os diferentes setores, incluindo, em situações cabíveis o setor privado, a sociedade civil ou mesmo a academia e o corpo técnico. **II) Como lidar com a complexidade**: O uso da lógica de plataforma faz com que seja possível a autoridade concentrar-se nos pontos que efetivamente sejam de sua responsabilidade final e que tenha maior especialidade. Nesse sentido, pode lidar com diferentes níveis de complexidade e lançar investigações próprias, por exemplo, somente nos casos que sejam efetivamente necessárias. Nesse contexto, há um elemento significativo que não deve ser ignorado. Há uma necessidade de transparência e de dar respostas. Isso começa com um espaço em que a autoridade deixa claro tanto o cenário atual como a sua atuação. O adágio clássico de “não basta ser fiel, mas deve aparentar também o ser” é um imperativo nessas situações. Para tanto as seguintes iniciativas são relevantes: **Reportar de forma constante e permanente a situação de incidentes de segurança.** Por meio das

	ferramentas automatizadas sugeridas previamente, a autoridade deve oferecer respostas e informações sobre a situação atual de incidentes de segurança no país. A partir desses dados, a comunidade científica, terceiro setor e outras entidades podem estudar estratégias, avaliações e colaborações com a autoridade. Com isso, avaliações e aprimoramentos serão favorecidos. **Publicar as investigações realizadas**. Um elemento que facilita a exponencialização do impacto é a clareza sobre o fato de haver investigações e os seus resultados. Auxilia no processo de legitimação da organização, pois explicita que há uma ação estatal além de deixar claro os critérios utilizados. Adicionalmente, fica evidente quando há reincidência, o que impacta tanto no processo interno da organização, quanto na no nível de confiança dos titulares. **Conclusões e caminhos para a ANPD**: Ante as razões expostas, sugere-se como norte **procedimentos explicativos, básicos e intuitivos para o público.** São pilares fundamentais para um sistema eficiente e, consequentemente, mais êxito para o papel da autoridade perante os titulares e controladores. Igualmente, a resposta ante os controladores não deve ser uma lista fixa e exaustiva de medidas a serem adotadas, mas deve-se trabalhar dentre as diferentes possibilidades com recomendações pontuais, vez que diferentes tipos de incidentes vão exigir diferentes medidas. As diretrizes do EDPB, (Guidelines 01/2021) apontam para isso. O decorrer do tempo permitirá a criação de procedimentos e indicações de medidas com certo grau de padronização, baseados em uma espécie de jurisprudência ou casos padrão. Nesse momento,

	pode-se ter mais claramente indicações de providências específicas. Antes de alcançar tal estado, corre-se o risco de ser insuficiente ou excessivo nas abordagens tomadas. Não sendo eficiente, ou desperdiçando energia que poderia ser melhor empregada em questões mais emergenciais. Portanto, **cabe dimensionar os procedimentos e compreender a função da autoridade em seus aspectos de atuação como plataforma e como serviço em que possa servir como coordenadora, intermediária e facilitadora da resolução de incidentes de segurança.**

Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	O conceito de de “risco ou dano relevante ao titular” aparece na Lei Geral de Proteção de Dados (LGPD) no art. 48, ao disciplinar a necessidade de comunicação pelo controlador tanto ao titular dos dados quanto à Autoridade Nacional de Proteção de Dados (ANPD) sobre a ocorrência de incidente de segurança. Estabelece um critério de relevância (do risco *ou* do dano) e um pessoal (ao titular) para haver uma comunicação. Nesse contexto, cabe construir limites claros que permitam distinguir incidentes de segurança que possam trazer risco ou dano relevante e, por tal razão, demandem providências específicas. A lógica da lei foi no sentido de discriminar situações que merecem maior cuidado e atenção das que não merecem para evitar tanto sobrecarregar a autoridade como não gerar “fadiga de notificações”. No intuito de alcançar tal discrimnação, é importante ter em vista as experiências internacionais para poder identificar (i) como são classificados incidentes de segurança em outras localidades; e (ii) quais são os parâmetros balizadores utilizados. **1) União Européia** **<u>Quando um incidente pode acarretar risco ou dano relevante ao titular.</u>** O *General Data Protection Law* (GDPR) define seu ‘*personal data breach’* no Artigo 4(12) como “*violação de segurança levando à destruição acidental ou ilegal, perda, alteração, não autorizada divulgação ou acesso a dados pessoais transmitidos, armazenados ou processados de outra forma”*. Nos termos do Artigo 33(1), considera que um incidente de segurança *que envolve dados pessoais* deve ser notificado à autoridade competente, salvo quando é

	improvável resultar em um risco a direitos e liberdades das pessoas naturais. Em sequência, a regra para a notificação aos titulares, preconizada no Artigo 34(1), estabelece que o incidente será comunicado quando acarretar um alto risco para os direitos e liberdades de pessoas naturais. O Considerando 75 oferece contornos ao que constituiria um risco a direitos e liberdades de pessoas naturais. Nesse sentido, o risco para os direitos e liberdades pode resultar do processamento de dados pessoais que levem a danos físicos, materiais ou imateriais aos indivíduos cujos dados foram violados. A título exemplificativo, tais danos são discriminação, roubo de identifdade ou fraude, perdas financeiras e danos à reputação, perda de controle sobre os dados pessoais, limitação de direitos, entre outros. Quando o incidente envolver dados pessoais que revelam racismo origem étnica, opinião política, religião, crenças filosóficas, filiação a sindicatos, dados genéticos, dados relativos à saúde ou à vida sexual, condenações criminais ou medidas de seguranças relacionais, tais danos devem ser considerados prováveis de ocorrer. (Ver Considerando 75 e 85 para mais informações). **Critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante.** O Considerando 76 aponta que a probabilidade e gravidade do risco para os direitos e liberdades do titular dos dados devem ser determinadas por referência à **natureza**, **escopo**, **contexto e objetivos do tratamento**. O risco deve ser mensurado com base em uma avaliação objetiva, pela qual é estabelecido se as operações de processamento de dados envolvem um risco ou um alto risco. A General Data Protection Law (GDPR) em seu Artigo 35(3) exemplifica quando o processamento de dados pode acarretar risco alto aos titulares, quais sejam: “*a) uma avaliação sistemática e extensa dos aspectos pessoais relativos às pessoas físicas que se baseia em*

	processamento automatizado, incluindo criação de perfil, e nas quais as decisões são que produzam efeitos jurídicos em relação à pessoa singular ou afetem de forma significativa a pessoa natural; b) tratamento em grande escala de categorias especiais de dados referidos no Artigo 9(1), ou de dados pessoais relativos a condenações criminais e infrações referidas no Artigo 10; c) um acompanhamento sistemático de uma área acessível ao público em grande escala. Ante um incidente que resulte em alto risco aos titulares, o Considerando 84 exige que seja realizada uma avaliação de risco e impacto (DPIA). Os critérios a serem considerados nesta são: 1) **Avaliação ou pontuação**, incluindo criação de perfil e previsão, especialmente de "aspectos relativos ao desempenho do titular dos dados no trabalho, situação econômica, saúde, preferências pessoais ou interesses, fiabilidade ou comportamento, localização ou movimentos". (Considerandos 71 e 91). 2) **Tomada de decisão automatizada com efeito legal ou similar significativo**: processamento que visa tomar decisões sobre os titulares dos dados que produzam "efeitos jurídicos relativos à pessoa singular" ou que "afeta de forma significativa de forma semelhante a pessoa singular" (Artigo 35 (3) (a)). 3) **Monitoramento sistemático**: processamento usado para observar, monitorar ou controlar os titulares dos dados, incluindo dados coletados por meio de "um monitoramento sistemático de uma área acessível ao público" (Artigo 35 (3) (c)). 4) **Dados sensíveis**: incluem categorias especiais de dados (por exemplo informações sobre opiniões políticas de indivíduos), bem como dados pessoais relacionados a crimes, condenações ou ofensas.

	5) **Dados processados em grande escala**: o GDPR não define o que constitui grande escala, embora o Considerando 91 forneça algumas orientações. O WP29 recomenda que sejam considerados (i) o número de titulares de dados envolvidos; (ii) o volume de dados e/ou a gama de diferentes itens de dados sendo processados; (iii) a duração, ou permanência, da atividade de processamento de dados; (iv) a extensão geográfica da atividade de processamento 6) **Conjuntos de dados que foram combinados**, por exemplo, originado de dois ou mais dados operações de processamento realizadas para diferentes fins e/ou por diferentes controladores de dados de forma a exceder as expectativas razoáveis do titular dos dados. 7) **Dados relativos a titulares de dados vulneráveis** (Considerando 75): o tratamento deste tipo de dados pode exigir um DPIA devido ao aumento do desequilíbrio entre o titular dos dados e o controlador de dados, isso significa que o indivíduo pode ser incapaz de consentir ou se opor ao processamento de seus dados 8) **Uso inovador ou aplicação de soluções tecnológicas ou organizacionais**, como combinar o uso de impressão digital e reconhecimento facial para melhor controle de acesso físico, dentre outras. 9) **Transferência de dados através das fronteiras fora da União Europeia** (Considerando 116). 10) Quando o processamento em si "**impede que os titulares dos dados exerçam um direito ou usem um serviço ou contrato**"(Artigo 22 e Considerando 91). A *Working Party* ("WP29") considera que quanto mais critérios forem atendidos pelo processamento, maior será a probabilidade de apresentar um alto risco para os direitos e liberdades dos titulares dos dados.

	2) Reino Unido O Reino Unido utiliza critérios semelhantes à União Europeia para a definição de incidentes de segurança relacionados a dados pessoais. Encontra-se, no entanto, diferentes ferramentas para auxiliar as organizações a conduzirem a avaliação dos incidentes. Nesse sentido, a ICO (*Information Commissioner's Office*) apresenta um "quiz" de aproximadamente cinco minutos para verificar a probabilidade e gravidade do risco aos direitos e liberdades das pessoas, após a violação, bem como a necessidade de notificar a ICO. Caso ainda restem dúvidas, pode-se recorrer ao *Data Security and Protection Incident Reporting tool*, que reúne diversos documentos e relatórios sobre incidentes de segurança. Destes se depreende dois pontos de análise: a seriedade do impacto eventual (ou atual) e a probabilidade de o impacto ocorrer. Tanto maior é o risco - que merece notificação - se houver maior severidade de um impacto e da probabilidade de que este ocorra. Dois exemplos utilizados pela ICO podem explicitar a situação: ■ Histórico de pacientes de um hospital vazaram. Aqui há potencial impacto alto pela natureza de saúde dos dados. O que deve levar a um risco elevado. ■ Dados de um paciente foram enviados de um médico a outro sem autorização de maneira acidental. Providências foram tomadas e houve a exclusão dos dados pelo segundo médico. Ainda que houvesse o mesmo potencial de impacto, devido a mesma natureza de saúde dos dados, o fato de que há uma probabilidade baixa de o impacto efetivamente ocorrer, faz com que se entenda que o risco seria mais baixo.

	Nesse contexto parece existir uma matriz em que severidade e probabilidade podem se cruzar. E o resultado dessa intersecção é que determina o risco. **3) <u>Canadá</u>** **<u>Quando um incidente pode acarretar risco ou dano relevante ao titular</u>**. De forma semelhante à LGPD, a legislação de proteção de dados do Canadá *Personal Information Protection and Electronic Documents Act* (PIPEDA) exige que organizações reportem à autoridade de supervisão canadense quando incidentes de segurança envolverem dados pessoais que acarretem risco real de dano relevante aos indivíduos. Nos termos da legislação, dano relevante significaria danos corporais, humilhação, danos à reputação ou relacionamentos, perda de emprego, oportunidades de negócios ou profissionais, perda financeira, roubo de identidade, efeitos negativos no registro de crédito e danos ou perda de propriedade. De acordo com a autoridade nacional de proteção de dados canadense, a avaliação para verificar risco de dano relevante deve considerar a **sensibilidade das informações envolvidas e a probabilidade de que as informações sejam mal utilizadas**. **<u>Critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante</u>**. No que tange aos critérios, a lei Canadense foca na **sensibilidade** dos dados e na **probabilidade que sejam mal utilizados.** Entende que estes dois pontos norteadores para avaliação se o risco de dano deve ser considerado como relevante. Nesse sentido, deve-se considerar os critérios a serem analisados nesses dois pontos norteadores.

	No contexto da legislação canadense, o Princípio 4.3.4 da PIPEDA auxilia na explicitação deste ponto quando expõe que "(...) *apesar de algumas informações (por exemplo, registros médicos e registros de receita) serem quase sempre consideradas sensíveis, qualquer informação pode ser sensível, dependendo do contexto. Por exemplo, os nomes e endereços dos assinantes de uma revista de notícias geralmente não são considerados informações sensíveis. No entanto, os nomes e endereços dos assinantes de algumas revistas de interesse especial podem ser considerados sensíveis*." Dessa forma, na análise de um incidente, não só a natureza dos dados pessoais presentes deve ser avaliada, como também deve ser cotejada com o contexto em que se encontram os dados. As circunstâncias do incidente podem tornar as informações sensíveis além de poder impactar os danos em potencial. No que tange a possibilidade de **mal uso dos dados**, a autoridade canadensa elenca diversas questões a serem consideradas, dentre elas: qual a probabilidade de alguém ser prejudicado pelo incidente? Quem realmente acessou ou poderia ter acessado os dados pessoais? Há quanto tempo os dados pessoais foram expostos? Há evidências de intenção maliciosa (por exemplo, roubo, hacking)? A informação foi perdida, acessada indevidamente ou roubada? Os dados pessoais foram recuperados? Os dados pessoais estão adequadamente criptografados, anonimizados ou não são facilmente acessíveis? **Conclusões e caminhos para a ANPD**: A partir da análise do contexto europeu em conjunto ao canadense, nota-se determinada divergência entre as definições para incidentes de segurança e, por conseguinte, as interpretações acerca de quando um

	incidente pode acarretar risco ou dano também detém particularidades. De forma geral, a União Européia e o Reino Unido consideram que o incidente que viola dados pessoais deve ser reportado à autoridade via de regra, salvo quando é improvável resultar em risco à direitos e liberdades. Por sua vez, na legislação do canadense, deve-se reportar o incidente de segurança quando existem circunstâncias razoáveis para deduzir que houve risco real de dano relevante. A lógica do texto da lei brasileira, ainda que muito inspirada na europeia, parece estar mais próxima do sistema canadense no sentido de entender que risco e dano são elementos diferentes e que a notificação deve ocorrer em casos em que exista risco ou mesmo em que exista dando. O que leva a crer que a análise de risco deve ser separada da análise do potencial de dano. **O risco deve ser, então, entendido de maneira mais ampla contemplando restrições a liberdades que ainda que não causem danos quantificáveis também devem ser reportadas.** Não seria nem qualquer risco e nem qualquer dano que deve ter como consequência a notificação. Nesse contexto, entende-se que em paralelo deva existir uma análise de se o risco é relevante e se o dano é relevante. Os critérios em si que permitem compreender a relevância parecem ser similares e se referem a sensibilidade do dado, extensão do incidente. O que muda é a potencialidade de materialização do risco a direitos e liberdades ou de danos. Nesse sentido, a sugestão é a realização de análises paralelas da relevância do risco e após do dano.

O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	No intuito de traçar mais contornos aos incidentes de segurança, cabe comentar sobre a possibilidade de subdividi-los em categorias. Com base nas experiências internacionais, **a subdivisão parece permitir às autoridades a direcionarem esforços e medidas cabíveis a cada tipo de incidente.** 1) **<u>União Européia</u>** **O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis?** A conceituação de risco na União Europeia advém de um quadro já presente nos considerandos (“recitals”) do GDPR. Nesse sentido, o Considerando 76 indica que a probabilidade e a gravidade do risco para os direitos e liberdades do titular dos dados devem ser determinadas por referência à natureza, âmbito, contexto e objetivos do tratamento. O risco deve ser avaliado com base em uma avaliação objetiva, pela qual é estabelecido se as operações de processamento acarretam nenhum risco, risco ou alto risco. Cumpre ressaltar que o Considerando 75 do GPDR, ao trazer especificações sobre os riscos à direitos e liberdades das pessoas naturais, destaca a variação de a possibilidade e gravidade entre eles. Isto posto, denota a importância de classificar em diferentes níveis os riscos também para atender com mais eficácia violações mais severas aos direitos e liberdades. Ao tratar de **riscos elevados**, o artigo 35(3) fornece exemplos e o Guia para Avaliação de Impacto de Proteção de Dados da WP29 indica 10 diretrizes a serem consideradas, bem como exemplos concretos para sua avaliação. De acordo com o documento, como regra geral, operações de tratamento que satisfaçam menos de **dois** critérios são consideradas de menor nível de risco, enquanto ao satisfazer pelo menos dois desses critérios são consideradas de alto risco.

	Nesse diapasão, as *Guidelines on Personal Data Breach Notification under Regulation 2016/679* recomendam que circunstâncias específicas de incidente devam ser consideradas para avaliar o risco aos indivíduos após uma violação, incluindo a gravidade do dano potencial e probabilidade do dano ocorrer. Quando as consequências de uma violação forem mais graves, o risco é maior e da mesma forma, onde a probabilidade de ocorrerem é maior, o risco também é aumentado. Assim, poder-se-ia utilizar tais critérios para distinguir os níveis de risco. Sejam eles: **(i) Tipo de violação**: O tipo de violação ocorrida aos dados pessoais pode afetar o nível de risco apresentado aos indivíduos. Por exemplo, uma violação de sigilo em que informações médicas foram divulgadas a pessoas não autorizadas pode resultar em diferentes consequências ao indivíduo, se comparada a uma violação em que detalhes médicos foram perdidos e não estão mais disponíveis. **(ii) Natureza, sensibilidade e volume dos dados pessoais**: No processo de avaliação do risco ou dano como relevante, a natureza, sensibilidade e volume de dados pessoais comprometidos pelo incidente de segurança é fundamental. Quanto mais sensíveis os dados, maior será o risco de danos às pessoas afetadas, mas deve-se levar em consideração outros dados pessoais que já podem estar disponíveis sobre o titular dos dados. Incidentes envolvendo dados de saúde, documentos de identidade ou dados financeiros, como detalhes de cartão de crédito, causam danos por si próprios, mas se juntos, podem ser usados para roubo de identidade. **Uma combinação de dados pessoais é normalmente mais sensível do que um único pedaço de dados pessoais**. **(iii) Facilidade de identificação de indivíduos**: A depender das circunstâncias, a identificação pode ser possível diretamente a partir dos dados comprometidos, sem buscas adicionais, enquanto em

	outros casos, pode ser mais difícil de combinar o dado pessoal a um indivíduo em particular. **(iv) Gravidade das consequências para os indivíduos**: Dependendo da natureza dos dados pessoais envolvidos em um incidente de segurança, por exemplo, categorias especiais de dados, o dano potencial aos indivíduos que poderia resultar pode ser especialmente grave, em particular onde a violação resultar em roubo de identidade ou fraude, dano físico, sofrimento psicológico, humilhação ou danos à reputação. Se a violação envolver dados pessoais sobre indivíduos vulneráveis, o risco de dano é ainda maior. Por outro lado, quando dados são divulgados a terceiros não autorizados acidentalmente e o controlador possuir um nível de confiança com o destinatário de modo a possibilitar certa expectativa de cooperação, a gravidade do incidente pode ser erradicada. Deve-se considerar também a permanência das consequências para os indivíduos, onde o impacto é visto como maior se os efeitos forem de longo prazo. **(v) Características especiais do indivíduo**: Quando um incidente afeta dados pessoais relativos a crianças ou outros indivíduos vulneráveis pode ser considerado de maior risco de dano. **(vi) Características especiais do controlador de dados**: A natureza e o papel do controlador e suas atividades podem impactar o nível de risco para os indivíduos envolvidos no incidente. Uma organização médica irá processar categorias especiais de pessoal dados, portanto, há uma ameaça maior para os indivíduos se seus dados pessoais forem violados. **(vii) Número de indivíduos afetados**: Geralmente, quanto maior o número de indivíduos afetados, maior o impacto de uma violação. Na União Europeia, portanto, a graduação dos riscos é dependente de fatores intrínsecos e extrínsecos aos dados, impactando quanto mais os fatores no nível de

	risco específico. Quanto maior os riscos, maior o mérito em realizar a notificação e tomar providências o mais rápido possível. Sendo necessário por vezes envolver diferentes atores (controladores e indivíduos são o ponto de partida). **2) Reino Unido** No Reino Unido, o *Guide to the Notification of Data Security and Protection Incidents* apresenta formas de subdivisão dos incidentes de segurança. Nesse sentido, o incidente deve ser classificado de acordo com o impacto no indivíduo ou grupos de indivíduos e não na organização. O grau da relevância e a probabilidade de ocorrência das consequências podem ser medidos em escala de 1 a 5. Nesse sentido, como comentamos acima na resposta anterior, segue uma lógica matricial de severidade e probabilidade. Por exemplo, quando o incidente está relacionado a um grupo vulnerável a pontuação mínima será 2 em relevância ou probabilidade, a menos que o incidente tenha sido contido. Nos exemplos mencionados na pergunta anterior, o caso em que foram tomadas medidas rápidas fez com que diminuísse a probabilidade da consequência adversa - ainda que a seriedade do impacto pudesse ainda ser a mesma. Para estabelecer a probabilidade de que o efeito adverso mediante o incidente, deve-se analisar: ■ **Nível 1**: Há uma certeza absoluta de que pode haver nenhum efeito adverso. ■ **Nível 2:** Nos casos em que não há evidências que possam provar que nenhum efeito adverso ocorreu. ■ **Nível 3**: É provável que haja um efeito adverso decorrentes da violação. ■ **Nível 4**: Há quase certeza de que em determinado momento um efeito adverso acontecerá.

	■ **Nível 5**: Há uma ocorrência relatada de um efeito adverso decorrente do incidente de segurança. **Conclusões e caminhos para a ANPD**: Dentro da mesma lógica da experiência internacional, parece ser útil a modulação em níveis para distinguir os tipos de ações tanto da própria ANPD como dos controladores. Dentro de conceitos de governo como plataforma e como serviço, é relevante poder classificar de maneira diferentes os incidentes *vis-à-vis* o seu impacto e complexidade. Uma chave para realizar essa classificação e as consequentes ações que daí decorrerão é partir da própria concepção legislativa e subdividir em diferentes níveis tanto de risco como de dano. Os critérios utilizados pela União Europeia a partir do GDPR são um bom indicativo de referência: (i) tipo de violação; (ii) natureza, sensibilidade e volume dos dados pessoais; (iii) facilidade de identificação de indivíduos; (iv) gravidade das consequências para os indivíduos; (v) características especiais do indivíduo; (vi) características especiais do controlador de dados; (vii) número de indivíduos afetados. Já a lógica matricial utilizada pela ICO no Reino Unido prevê um mecanismo procedimental para realizar a análise. **O que em um futuro próximo, se for esse o caminho seguido pela ANPD, poderia valer a criação de uma ferramenta tecnológica que facilitasse essa análise de risco e dano.** Essas diferentes subdivisões de risco e dano facilitaram a compreensão de como agir de acordo com os preceitos legais, o que vai além das obrigações de notificação. Incluem também mecanismos de segurança, de lida com danos e resiliência.

Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	Tendo em vista a inspiração da Lei Geral de Proteção de Dados (LGPD) nos diferentes modelos internacionais, nota-se que já há uma base significativa quanto aos elementos já listados no §1º do art. 48. O que se buscará mais adiante é apresentar o que pode ser incluído com inspiração nas demais legislações e em como as autoridades regulamentaram suas regras. Ao final, serão aduzidas recomendações objetivas a respeito do que seria relevante replicar das demais práticas. **1) <u>União Européia</u>** A maioria das informações que os controladores devem notificar à ANPD, listadas no §1º do art. 48 da LGPD estão refletidas na GPDR. Cabe, contudo, detalhar as diferenças e considerações do WP29 referente ao tema. Nos termos do art. 48, §1º, I e II da LGPD, é necessário descrever a natureza dos dados pessoais afetados e as informações sobre os titulares envolvidos. O comando equivalente na legislação europeia exige também que **tal informação esteja acompanhada, sempre que possível, das categorias e número aproximado de titulares** (Artigo 33 (A)). Como GDPR é silente sobre quais seriam as categorias de titulares de dados ou registros de dados pessoais, WP29 sugere categorias de titulares de dados para se referir aos vários tipos de indivíduos cujos dados pessoais foi afetado por uma violação, por exemplo, crianças e outros grupos vulneráveis, pessoas com deficiência, funcionários ou clientes. Similarmente, **categorias de registros de dados pessoais** podem se referir aos diferentes tipos de registros que o controlador pode processar, como dados de saúde, registros educacionais, informações de assistência social, detalhes financeiros ou bancários, números de passaporte e assim por diante.

	No mesmo sentido, o Considerando 85 deixa claro que um dos objetivos da notificação é a limitação dos danos às pessoas. Consequentemente, se os tipos de titulares de dados ou os tipos de dados pessoais indicarem um risco de dano ocorrido como resultado do incidente (por exemplo, roubo de identidade, fraude, perda financeira, ameaça ao sigilo profissional), é importante que a notificação indique essas categorias. Além disso, exige-se também o nome e os detalhes de contato do responsável pela proteção de dados ou outro ponto de contato onde mais informações podem ser obtidas. **A legislação europeia ressalta ainda a necessidade das organizações manterem um registro dos incidentes de segurança relacionados a dados pessoais.** Essa documentação permitirá à autoridade de supervisão verificar a conformidade com a legislação de proteção de dados, compreender eventuais incidentes futuros e, ainda, auxiliar em caso de reincidência. **2) <u>Reino Unido</u>** A autoridade de proteção de dados do Reino Unido indica a necessidade de fornecer: nome e detalhes de contato; data e hora da violação (ou uma estimativa); data e hora em que o incidente foi detectado; informações básicas sobre o tipo de violação; e informações básicas sobre os dados pessoais em questão. Ainda, requer, se possível, a inclusão de detalhes completos do incidente, o número de indivíduos afetados e os possíveis efeitos sobre eles, as medidas tomadas para mitigar esses efeitos e informações sobre a notificação aos titulares. Caso tais detalhes não estejam disponíveis, deve-se enviar um segundo formulário de notificação em três dias com tais detalhes ou informando quanto tempo levará para enviá-los.

	3) <u>Canadá</u> Em regulação específica, o Canadá estabelece os processos relativos às salvaguardas de incidentes de segurança (*Breach of Security Safeguards Regulations: SOR/2018-64*). De acordo com a normativa, a notificação do incidente à autoridade competente deve conter, dentre outros elementos: i. descrição das circunstâncias do incidente, caso a causa seja conhecida; ii. data ou o período durante o qual, a violação ocorreu ou, se nenhum for conhecido, o período aproximado; iii. o número de indivíduos afetados, caso desconhecido, o número aproximado; iv. descrição das etapas que a organização tomou ou pretende realizar para notificar os indivíduos afetados; v. o nome e contato de quem possa responder, em nome da organização, às perguntas da autoridade. Ainda, abre-se a possibilidade para que a organização submeta informações novas relacionadas ao incidente, caso fique ciente após notificação à autoridade. **Conclusão e caminhos para ANPD:** Com base nas melhores práticas internacionais e no intuito de complementar as informações exigidas no §1º do art. 48 da LGPD, recomenda-se que controladores também forneçam: **1)** Nome e contato do **Encarregado** ou outro ponto de contato na instituição. **2)** **Data ou o período** durante o qual, o **incidente** ocorreu ou, se nenhum for conhecido, o período aproximado; **3)** Detalhes complementares sobre a **natureza dos dados pessoais afetados** e as informações sobre os titulares envolvidos, quais sejam: as categorias e número aproximado de titulares;

	4) Etapas que a organização tomou ou pretende realizar para **notificar os indivíduos** afetados, quando necessário por lei ou por prudência; 5) **Registro de incidentes** de segurança, incluindo os fatos relacionados à violação, efeitos e as medidas corretivas tomadas. **Há que se ter em mente que apesar de ser necessário o procedimento seguir uma lógica de formulário e ser estruturado, deve existir certa flexibilidade.** Não só as mudanças tecnológicas podem afetar os incidentes, como podem existir fatores inesperados e deve haver campos e espaços abertos para poder lidar com essa aleatoriedade.
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	Como já demonstrado, um incidente de segurança pode acarretar uma série de efeitos adversos significativos sobre os indivíduos, que podem representar danos físicos, materiais ou imateriais. A prontidão na notificação do incidente à ANPD detém relação direta com a gravidade do dano acarretado ao titular, por isso é importante tratar do tema com a devida cautela. Sabe-se que atualmente o Decreto 9.936/2019, que regulamenta a Lei do Cadastro Positivo, exige que a comunicação à ANPD seja efetuado no prazo de dois dias úteis (art. 18, I e §§ 1º e 2º). Ainda, a orientação atual também é no sentido de que caso não seja possível fornecer todas as informações no momento da comunicação preliminar, informações adicionais poderão ser fornecidas posteriormente. De todo modo, busca-se expor os parâmetros internacionais tanto a respeito do prazo para comunicação dos incidentes como recomendar que seja estabelecido prazo para as informações adicionais essenciais, com base nas práticas internacionais. Como se observará adiante, o prazo comum é de no máximo 72 horas após ciência e, na hipótese de

	informações, deve-se explicar o atraso e quando pode ser esperado o envio dos detalhes adicionais. **<u>Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)</u>** **1) União Européia** A legislação europeia estabelece o **prazo de 72 horas** para a notificação do incidente de segurança. Conforme o Artigo 33(1) do GDPR, na hipótese de violação de dados pessoais, o controlador deve, sem demora indevida e, quando viável, sob o prazo máximo de 72 horas após ciência, notificar o incidente de segurança à autoridade supervisora de proteção de dados. Salvo casos em que seja improvável que o incidente resulte em risco para os direitos e liberdades das pessoas singulares. Quando a notificação para a autoridade é feita após o prazo de 72 horas, deve ser acompanhada dos motivos do atraso. De acordo com o WP29, a **ciência do controlador** a respeito do incidente de segurança se dá mediante um grau razoável de certeza de que ocorreu um incidente a comprometer dados pessoais. Isso pode variar a depender das circunstâncias específicas do incidente. Em alguns casos, será relativamente claro desde o início que houve uma violação, enquanto em outros, pode levar algum tempo para estabelecer se os dados pessoais foram comprometidos. No entanto, a ênfase deve ser na ação imediata para investigar um incidente para determinar se os dados pessoais foram realmente violados e, em caso afirmativo, tomar medidas corretivas e notificar se necessário Na hipótese de controladores conjuntos, o Artigo 26 do GDPR preconiza a necessidade dos controladores determinarem suas respectivas responsabilidades pelo cumprimento do GDPR. O WP29 recomenda que os acordos contratuais entre controladores conjuntos incluam disposições que determinam quais o

	controlador assumirá a liderança ou será responsável pela conformidade com a notificação de incidentes de segurança, nos termos do GDPR. 2) **Reino Unido** Na mesma linha da União Européia, a GDPR do Reino Unido (UK GDRP) impõe a todas as organizações o dever de relatar certas violações de dados pessoais à autoridade supervisora relevante. A notificação deve ser feita dentro de **72 horas** após tomar conhecimento dos fatos essenciais da violação, quando viável. É esperado que os controladores priorizem a investigação, empregando os recursos adequados com a devida urgência. No caso de ultrapassar o prazo de 72 horas, é recomendado explicar o porquê e indicar uma expectativa de envio futuro. **Conclusões e caminhos para a ANPD:** De um ponto de vista da experiência europeia, tem-se que 72 horas da ciência é o prazo prudencial. Nada parece levar a que no sistema estabelecido na LGPD o prazo razoável deva ser menor do que este prudencial encontrado no sistema europeu. Frise-se que não é o prazo mínimo, mas o máximo. A prontidão na notificação deve ser exaltada. Nesse diapasão, a ANPD deve incentivar a notificação oportuna. O que não quer necessariamente dizer antecipada. É importante para a atuação adequada da autoridade que sejam fornecidas informações suficientes para permitir a procedimentalização correta das ações, seja da autoridade enquanto plataforma, seja enquanto serviços. **Este prazo deve ser entendido no sentido de incentivar uma atuação de boa-fé por parte dos controladores.** Há um espaço de tomada de decisão e de atuação imediata do controlador. **O que se espera é**

	a existência das mais prontas medidas de mitigação e de resiliência.
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	Assim como o prazo para comunicação à ANPD, o prazo para que os controladores informem aos titulares sobre o incidente de segurança também possui impactos no indivíduo e pode acarretar em efeitos adversos. É o momento de explicar o ocorrido e, caso possível, sugerir providências ou mesmo formas de mitigação de danos que demandem ação da própria pessoa afetada. Há situações em que a urgência pode ser maior justamente tendo em vista a gravidade, seriedade ou probabilidade de risco ou dano seja mais iminente ou alto. A estrutura de riscos e danos em face da matriz sugerida acima auxilia nessa compreensão e pode recomendar em quais casos é mais premente essa comunicação. Para sugerir um modelo de resposta preciso, recorreu-se à União Européia, Reino Unido e Canadá, cada um com suas particularidades e focos ao tratar do tema. 1) **<u>União Européia</u>** **Qual prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança?** Em seu Parecer 03/2014 sobre notificação de violação de dados pessoais, o WP29 forneceu orientação aos controladores para ajudá-los a decidir se notificam os titulares dos dados em caso de violação. A manifestação considerou a obrigação dos fornecedores de comunicações eletrónicas no que diz respeito à Diretiva 2002/58/CE, concedeu exemplos de vários setores, no contexto do então rascunho do GDPR, e apresentou boas práticas para todos os controladores.

	O GDPR declara que a comunicação de uma violação aos indivíduos deve ser feita "sem indevido atraso", o que significa o mais rápido possível. O principal objetivo da notificação aos indivíduos é fornecer informações específicas sobre as etapas que devem seguir para sua proteção (Ver Considerando 86). **Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?** A legislação européia em seu Artigo 34(2) especifica a necessidade de a comunicação para os titulares descrever em linguagem clara e simples a natureza da violação de dados pessoais e conter ao menos as informações e medidas referidas nos pontos (b), (c), e (d) do Artigo 33(3), que impõe as informações necessárias durante a notificação da autoridade de supervisão, sejam elas: a) descrever a natureza da violação; b) fornecer o nome e os dados de contato do responsável pela proteção de dados ou outro ponto de contato; c) descrever as consequências (riscos) prováveis da violação; e d) uma descrição das medidas tomadas ou propostas a serem tomadas pelo controlador para resolver a violação, incluindo, quando apropriado, medidas para mitigar seus possíveis efeitos adversos. É recomendado ainda que o controlador, quando apropriado, forneça conselhos e auxílio aos titulares sobre como se proteger dos riscos e danos do incidente de segurança, por exemplo, alterar senha no caso de suas credenciais terem sido comprometidas. **2) <u>Reino Unido</u>** **Qual prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança?**

	Ante a possibilidade do incidente resultar em um alto risco para os direitos e liberdades dos indivíduos, o UK GDPR determina que os indivíduos devem ser informados diretamente e sem atrasos indevidos. **Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?** A autoridade de supervisão do Reino Unido *Information Commissioner Office* (ICO) entende que a notificação aos titulares deve conter: a) Nome e detalhes de contato; b) Data estimada da violação; c) Resumo do incidente; d) Natureza e o conteúdo dos dados pessoais; e) Efeito provável no indivíduo; f) Medidas tomadas para resolver a violação; g) Medidas de mitigação para possíveis impactos adversos. **3) Canadá** Em regulação específica, o Canadá regula os processos relativos às salvaguardas de incidentes de segurança (*Breach of Security Safeguards Regulations: SOR/2018-64*). Nesse sentido, a autoridade estabelece que a notificação aos titulares de dados deve conter: a) Descrição das circunstâncias da violação; b) Data ou período durante o qual a violação ocorreu ou, se nenhum for conhecido, o período aproximado; c) Descrição das informações pessoais que são objeto da violação, na medida em que as informações sejam conhecidas; d) Descrição das medidas que a organização tomou para reduzir o risco de dano que poderia resultar da violação;

	e) Medidas que os indivíduos afetados podem tomar para reduzir o risco de dano que pode resultar da violação ou para mitigar esse dano; f) Informações de contato que o indivíduo afetado pode usar para obter mais informações sobre a violação. **Conclusões e caminhos para a ANPD**: Percebe-se que diferentemente do prazo para notificação da autoridade, de um modo geral nos sistemas de proteção de dados da Europa e outros países a lógica prudencial predomina. Prazos estritos não necessariamente dão conta da urgência da situação. Há que se ter em mente que a comunicação prematura pode ser também danosa. Uma comunicação sem as informações suficientes pode gerar maior ansiedade. É importante então que a comunicação seja feita sem demora, mas de uma maneira estruturada e com as informações mínimas necessárias. A lógica da comunicação não é meramente de transparência é de possibilitar uma ação informada pelo titular. Nesse contexto, **a notificação deve vir em um prazo mínimo, de acordo com a urgência e com a informação de maneira completa, acessível e que permita a ação consciente e informada**.
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas	A forma de comunicação dos incidentes é mais uma faceta para garantir a mitigação dos danos ocorridos. Com base em experiências de diversos países, nota-se que *inexiste um padrão específico* de comunicação, todavia, a comunicação direta assume posição preferencial nos demais ordenamentos. Nota-se que como visto acima, o objetivo desse tipo de comunicação é mais do que dar transparência ao ocorrido, é também permitir a ação informada e consciente do titular. Para tanto, o formato deve ser

circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	subordinado à compreensão fácil do titular, de preferência seguindo cânones de linguagem simples, cidadã ("*plain text*"). No geral, as recomendações são de considerar as particularidades do caso e focar em aumentar a proteção para com relação aos dados violados. Esse aspecto também pesa na relação de confiança entre o titular e o controlador. Passa-se a detalhar as diretrizes internacionais quanto ao tema: 1) **<u>União Européia</u>** **Qual a forma mais adequada para a realização da comunicação do incidente aos titulares?** Comunicar um incidente aos indivíduos permite que o controlador forneça informações sobre os riscos apresentados como resultado da violação e as medidas que esses indivíduos podem tomar para se protegerem de suas possíveis consequências. O foco de qualquer plano de resposta a violações deve ser a proteção dos indivíduos e de seus dados pessoais. Consequentemente, a notificação deve ser vista como uma ferramenta para aumentar a conformidade em relação à proteção de pessoas dados. O WP29 estabelece melhores práticas a serem replicadas ante os diferentes tipos de incidentes: 1) **As mensagens de comunicação devem ser movidas exclusivamente para esse fim**. Não se deve enviar outras informações, como atualizações regulares, boletins informativos ou mensagens padrão. O objetivo dessa recomendação é tornar a comunicação do incidente clara e transparente. 2) Os controladores também podem precisar garantir que a comunicação seja **acessível em alternativa adequada a formatos e linguagens** relevantes para garantir que os indivíduos sejam

	capazes de compreender as informações que estão sendo fornecidas. **A comunicação deve ser sempre direta e individual ou, em determinadas circunstâncias, pode ser admitida a comunicação pública?** Conforme as Guidelines on Personal data breach notification under Regulation do WP29, uma notificação exclusivamente pública, como um comunicado à imprensa ou blog corporativo não seria um meio eficaz de comunicar o incidente de segurança a um indivíduo. Em síntese, encontra-se as seguintes recomendações sobre como realizar a comunicação com os indivíduos: a) Escolher de um meio que **maximize a chance de comunicar as informações de maneira adequada** a todos os indivíduos afetados. b) Empregar, dependendo das circunstâncias, **vários métodos de comunicação,** em oposição ao uso de um único canal de contato. c) Os controladores estão melhor posicionados para determinar o canal de contato mais apropriado para comunicar uma violação a indivíduos, especialmente se eles interagirem com seus clientes com frequência. **2) <u>Canadá</u>** **A comunicação deve ser sempre direta e individual ou, em determinadas circunstâncias, pode ser admitida a comunicação pública?** No Canadá, admite-se a possibilidade de notificação direta e indireta sob circunstâncias específicas. A notificação direta deve ser dada ao indivíduo afetado pessoalmente, por telefone, correio, e-mail ou qualquer outra forma de comunicação que uma pessoa razoável consideraria apropriada nas circunstâncias.

	A comunicação indireta será admitida quando: **(i)** a notificação direta provavelmente causar mais danos ao indivíduo afetado; **(ii)** a notificação direta provavelmente causar dificuldades indevidas para a organização; **(iii)** a organização não possui as informações de contato do indivíduo afetado. Essa comunicação deve ser dada por comunicação pública ou medida semelhante que poderia ser razoavelmente esperada para atingir os indivíduos afetados. **Conclusões e caminhos para a ANPD**: Tendo em vista a lógica da ANPD atuar como serviço e como plataforma, a existência de formulários claros e de uma plataforma de intermediação pode facilitar em diversos casos esses mecanismos de notificação. Podem inclusive estar automatizados no sistema. No entanto, eles não abarcam todas as circunstâncias possíveis. Há situações em que pode ser difícil o contato com o titular. Nesse sentido, o objetivo da notificação é permitir que o titular tome decisões informadas sobre como tentar mitigar os riscos e danos que incidentes de segurança podem vir a ter. Para tal, **os meios a serem utilizados devem ser pensados no sentido de alcançar este objetivo, podendo ter múltiplos meios.**
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	Após um incidente, é importante examinar quais dados pessoais foram violados e as circunstâncias de sua ocorrência. As circunstâncias do incidente podem tornar as informações mais ou menos confidenciais. Os danos potenciais que podem advir para um indivíduo também são um fator importante. 1) **União Europeia**: Os critérios apontados no documento *Guidelines on Personal Data Breach Notification under Regulation 2016/679* e elencados anteriormente podem servir de inspiração para os critérios a serem adotados pela

	ANPD para análise da gravidade do incidente de segurança. Além disso, com base em um estudo da Agência Europeia para a Segurança das Redes e da Informação (ENISA) de 2011 sobre a implementação do Artigo 4 da Diretiva de Privacidade Eletrônica, as Autoridades de Proteção de Dados da Grécia e da Alemanha, em colaboração com a ENISA, desenvolveram uma metodologia para avaliação da gravidade da violação de dados que poderia ser usada tanto pelas autoridades de proteção de dados quanto pelos controladores de dados. De acordo com a metodologia, os principais critérios levados em consideração ao avaliar a gravidade de uma violação de dados pessoais são: a) **Contexto de processamento de dados** (CPD): aborda o tipo de dados violados, juntamente com um vários fatores ligados ao contexto geral de processamento. b) **Facilidade de Identificação** (FI): Determina a facilidade com que a identidade dos indivíduos pode ser deduzida dos dados envolvidos na violação. c) **Circunstâncias de violação** (CV): Aborda as circunstâncias específicas da violação, que são relacionadas ao tipo de violação, incluindo principalmente a perda de segurança dos dados violados, bem como qualquer intenção maliciosa envolvida. **Conclusões e caminhos da ANPD**: A visão internacional sobre como lidar com incidentes de segurança entende que a gravidade depende dos seguintes critérios: (i) contexto de processamento de dados; (ii) facilidade de Identificação; (iii) circunstâncias de violação. Quanto à metodologia, detalha-se abaixo.

Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	A metodologia para análise de gravidade do incidente de segurança é importante na busca de padronizar sua implementação e auxiliar organizações a se auto-avaliarem. 1) **União Europeia**: A Agência da União Europeia para a Segurança das Redes e da Informação (ENISA), em colaboração com as Autoridades de Proteção de Dados da Grécia e Alemanha, produziram recomendações para uma metodologia de avaliação da gravidade do incidente de segurança. O relatório pode ser utilizado por controladores e processadores ao projetarem seu plano de resposta de gerenciamento ao incidente de segurança. A metodologia proposta é baseada em uma abordagem objetiva, matricial, sendo flexível o suficiente para ser adotada por várias autoridades de proteção de dados, ajustando-se ao tamanho, e ao sistema jurídico nacional. No contexto da metodologia indicada, a gravidade do incidente de segurança envolvendo dados pessoais é definida como "*estimativa da magnitude do impacto potencial sobre os indivíduos derivada dos dados violados*". São indicados três critérios principais para avaliar a gravidade do incidente (já descritos acima, mas por facilitação repetidos aqui), quais sejam eles: a) **Contexto de processamento de dados (*Data Processing Context* DPC)**: endereça o tipo de dados violados, juntamente com um vários fatores ligados ao contexto geral de processamento. Para definir a pontuação deste critério, deve-se (i) definir e classificar os tipos de dados pessoais, de forma a definir os dados envolvidos no incidente e categorizá-los em quatro (simples, comportamentais, financeiros e sensíveis); (ii) estabelecer quais fatos

	contextuais podem aumentar ou reduzir a pontuação, como volume de dados e natureza. b) **Facilidade de identificação (*Ease of Identification* EI)**: determina a facilidade com que a identidade dos indivíduos pode ser deduzida dos dados envolvidos na violação. Para essa metodologia, esse critério pode ser definido em quatro níveis: insignificante, limitado, significativo e máximo. A pontuação mais baixa é dada quando a possibilidade de identificar o indivíduo é insignificante e a mais alta quando é possível identificar diretamente a partir dos dados violados. c) **Circunstâncias do incidente (*Circumstances of breach* CB)**: endereça as circunstâncias específicas da violação, que são relacionadas ao tipo de violação, incluindo principalmente a perda de segurança dos dados violados, bem como qualquer intenção maliciosa envolvida. São quatro os elementos a serem considerados: confidencialidade, integridade, disponibilidade e intenção maliciosa. Com base nesses critérios, tem-se: a) o contexto de processamento de dados está no centro da metodologia e serve como avaliador da criticalidade de determinado conjunto de dados para um processamento específico; b) a facilidade de identificação pode reduzir a criticidade geral de um processamento de dados. Dessa forma, com a combinação desses dois elementos iniciais se obtém a 'pontuação' inicial do incidente de segurança ("SE"); c) as circunstâncias do incidente podem estar presente ou não em uma situação específica, esse fator pode aumentar a severidade do incidente. Como resultado, metodologia específica para o cálculo do risco seria: "*DPC x EI + CB*", ou seja, combinar o contexto de processamento de dados com a facilidade de identificação, incluindo então as circunstâncias do incidente. Ao final, a gravidade do incidente é

	categorizada em baixo, médio, alto e muito alto a partir do cálculo realizado. A lógica pensada segue em parte a compreensão matricial do risco para o titular somente com elementos de agregação específicos para representar a coletividade do incidente de segurança. **Conclusões e caminhos da ANPD**: Como visto, o uso de metodologia específica auxilia as autoridades a avaliarem a gravidade e complexidade de um incidente. É indicado que a definição dos critérios apresentados seja pensada no contexto brasileiro, considerando as legislações internas pertinentes e apresentada de forma clara aos controladores. A proposta seria enviar também a avaliação e metodologia adotadas pela autoridade aos controladores no formulário de notificação ou mesmo incluída por meio de quiz com perguntas e exemplos.

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: Jairo Willian Pereira

CPF/CNPJ: [redacted]

[redacted]

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

[redacted]

CONTRIBUIÇÕES RECEBIDAS **IMPORTANTE:** Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	1. Recomendo tratar incidente de forma diferente de risco (como preconiza os normativos internacionais e todas as ISOs de Segurança, especificamente a ISO27005 (Risco para Segurança) ou a ISO31000 (Risco de forma mais generalista/corporativa). Se observamos as literaturas de ITIL/ITSM ou mesmo COBIT/COSO (entre outros modelos utilizados de acordo com a linha de negócio) fica claro e evidente que cada uma delas possuem um ritual, fases e variáveis diferentes. Incidente é incidente (tem classificação e tipificações próprias) e risco é risco (e precisa obrigatoriamente atender as fases/caixas presentes na ISO31000). 2. Adicionalmente, consultar a observação feita em comentários a área de "Introdução". 3. Importante mencionar (como fonte de consulta extra) que o próprio BaCen questiona e cobra pela definição de "incidente relevante", mas mais importante ainda lembrar que nem ele sabe o que é isso (e transfere a responsabilidade para cada empresa ter sua interpretação – que pode ser ótimo ou péssimo de acordo com a qualidade do "redator" do outro lado).
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	4. Baixo, médio, alto e crítico (como a maioria dos regramentos/ferramentas internacionais utilizam). Observe que cada um deles pode ou não ser "relevante". 5. Novamente, ler as definições e termos da própria ISO27000. Não existe a palavra "dano relevante" e isso mais confunde que ajuda. Seria uma quarta dimensão que os times teriam que se "adaptar" para responder um modelo de relatório/atributo que somente a ANPD utiliza. **6.** Sim, todos devem ser considerados. Muito importante mencionar que, nem todo incidente crítico ou alto é relevante, e claramente, nem todo incidente médio ou baixo não pode ser relevante. Se a ideia é apenas incidentes materializados OK, mas se for algum "quase

	incidente" que DEVERIA ser compartilhado por questões de estudo (ineditismo, ocorrência parcial que ainda carece de esclarecimentos, malware ou artefato digno de pesquisa etc.). 7. Observe que a palavra compartilhamento acima foi propositalmente utilizada porque as observações aqui pontuadas consideram que este profissional/empresa não reporta/atende apenas a ANPD mas sim diversos outros reguladores em escala nacional e internacional e quanto menos forem as "versões dos relatórios" mais rápido todo mundo será atendido e melhor/com menos erros. Padronizar é preciso (modelos, atributos desejados, tipificações, classificações, granularidade etc.). Apenas como exemplo de "consumidores atuais" de relatórios/reporte de incidentes, podemos citar: MP-DFT, BaCen (vide 3909 e 4658), SEC (Security Exchange Comission via Sox 302 e 404 e todos os formulários recorrentes 8-K, 10-K, 12-K...), B3, CVM, Bandeiras (todos os cartões pedem a mesma coisa, seja por questões de atendimento ao PCI-DSS ou Master SDP e VISA CISP), ANBIMA, DPF (pede mas não tem padrão e ainda coloca a culpa no "armazenador"),
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	8. Talvez por volume (1:n, leia impacto), custo do dado (neste caso, o custo para a empresa versus o custo da pessoa física que se tornou exposta esse ativo). Fiquei com um pouco de dúvida na pergunta.
O que deve ser considerado na avaliação dos riscos do incidente?	9. Agente da Ameaça (desconhecido, controlado...), Impacto (abrangência geográfica ou volume de dados), Probabilidade, Vulnerabilidade (que levou ao incidente) e uma mensuração financeiro da massa de dados envolvidas. 10. Observe que, para custo por unidade, pode ser computado: campos/atributos divulgados, facilidade de agrupamento/cluster/correlação dos dados, quantidade de informações sensíveis do proprietário, extensão territorial (e se tiver estrangeiro na base, aciona GDPR? – se for necessário, sugiro padronizarem para 48h (SOX) ou máximo (72h) para pior caso).
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	11. Definir o que é razoável (sugestão de alinhar pelo menor prazo global – 48h). 12. Expressar a informação usando carimbo de tempo + timezone (neutro, global ou LOCAL). 13. Gerar um **hash** do arquivo final/relatório submetido a ANPD (para sanar possíveis conflitos de versão/interesse). 14. Art. 48 - IV - os riscos relacionados ao incidente; (observe que a lei diferencia Riscos de Incidentes!) 15. II - Medidas para reverter ou mitigar os efeitos do incidente. ← Precisa pensar um pouquinho sobre esse ponto porque TODO procedimento de gestão de incidentes já prevê essa fase. Se não existe essa fase, o Processo de Gestão de Incidentes está incorreto. Adicionalmente, a maioria dos reguladores já solicita que um resumo das ações que foram executadas em CADA um das fases seja apresentado.

	16. Sobre fases, vale mencionar que os CERTs internacionais, costumar adotar o mesmo padrão (utilizado inclusive pelo FIRST) que divide corretamente uma gestão de incidentes decente em 6 fases, a saber: Preparação, Identificação, Contenção, Remediação, Restauração e Comunicação (aftermath/post-morten). 17. Possuir uma assinatura e/ou contato de responsável pelo tema com data no final do relatório/comunicado.
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	**18.** Eterno defensor global de padrões "de-facto". Padronizar é sempre uma ótima opção (o email que sai para 1 destinatário sai para 10 com mesmo conteúdo). Sugeriria o pior caso internacional (SEC, 48h) ou GPRD para irmos de copy/paste em 72h. **No item7** há mais detalhes que ajudam nesse racional. **19.** Importante mencionar em algum local do regramento que, esse prazo, não necessariamente é o prazo final para esclarecer ou encerrar o vazamento, mas para a comunicação com os reguladores envolvidos.
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	**20.** Quanto mais variáveis e detalhes pior e maior a probabilidade de erro. Quem comunica o regulador pode muito bem informar (de forma resumida) o proprietário do dado. Importante mencionar que empresas que já possuem PCN (Plano de Continuidade de Negócios – BCP) esse é um padrão desejado e praticado, com recomendações de integração via ISO22301.
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	21. A individual usando algum mecanismo indicado pelo titular e comumente utilizado por ele (tipo email, APP ou SMS dependendo dos sistemas) deve ser obrigatória, sempre em redundância (pelo menos dois sistemas para diminuir a possibilidade de não-repudio). As demais, mesmo sendo em veículos de alta publicidade, penso que varie muito de público para público e deve ser avaliado de acordo com regiões (o que funciona em SP não funciona em RO). Todos os demais meios podem ser avaliados. Penso que pelo menos 3 locais devem ser utilizados, sendo obrigatoriamente um deles, via/na plataforma onde o cliente consome o serviço/produto.
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	22. Visando a melhoria, conhecimento da série histórico e indicadores estatísticos anuais, não sei se parece uma boa ideia ter exceções. Se houve incidente e tem relevância/importância, deveria ser notificado (até para motivos de estudos e melhoria do sistema/ecossistema como um todo ou mesmo avaliar os grandes ofensores da lei). 23. Único caso que creio seja "estudável", são incidentes internos (ou externos mas de impacto controlado) que tenham sido resolvidos sem efeitos colaterais pelas equipes envolvidas

	(muito bem documentado e armazenado para consulta futura em caso de reincidentes* ou casos similares em outros locais). 24. Alguém considerou reincidência?
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	25. Idem.
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	26. Idem item9.
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	27. IRM – Incident Responde Methodology) ajuda mensurar o problema de acordo com as fases listadas no item16. Tornar isso “relevante/qualitativo” varia de acordo com ferramentas e modelos utilizados (diversos listados anteriormente, e parte deles utilizam não apenas plataformas de Tecnologia mas indicadores de Processos e fatores Humanos/Pessoas presentes no evento). Adicionalmente, FAIR ajuda aproximar o contexto de Incidentes com o de Riscos, OCTAVE pode ser utilizado para uma abordagem mais ágil mas é fato que os componentes/atributos envolvidos na temática (ao longo desse documento) deverão ser utilizados na equalização.
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	28. Uma vez que o relatório tenha o padrão mínimo esperado (uma conclusão do momento e respeite o faseamento do item16, a pergunta que deve ser feito é se sobrou algum “risco residual” que deva ser endereçado pela área da cia ou se haverá “plano de ação” para correções pontuais (e de curto prazo ou imediato).
Extras?	29. Sim. Consultem padrões “de-facto”, normais e modelos maduros para qualquer tipo de atividade/disciplina existente (em 2021 é quase impossível criar algo novo). Evitem criar modelos específicos que servirão somente a ANPD. O maior problema dos profissionais de Segurança/Dados atualmente é atender pedidos diversos, da mesma necessidade, em momentos distintos, escritos de formas diferentes, em formatos diferentes, prazos diferentes para órgãos diferentes que não se conversam (e se houvesse essa conversa, reduziria em muito o tempo e esforço de todos os envolvidos). 30. Avaliaram a ISOs 27001 e 27002 que são ótimos subsídios 27.701? Pois é, o que não existe nelas está na 27003, 27004, 27005, 27006, 27007, 27008, 27009, 27009, 27010, 27011...

SUGESTÃO DE NORMATIVO, SE HOUVER	
Não é mais o momento, mas seria muito mais fácil, rápido, barato e menos complexo se a LGPD tivesse sido full-copy/paste da GDPR (à la FCPA-12.846).	
Art. Xxxx	

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº2/2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: JOSÉ ANTONIO MAURILIO MILAGRE DE OLIVEIRA

CPF/CNPJ: [redacted]

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como, critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

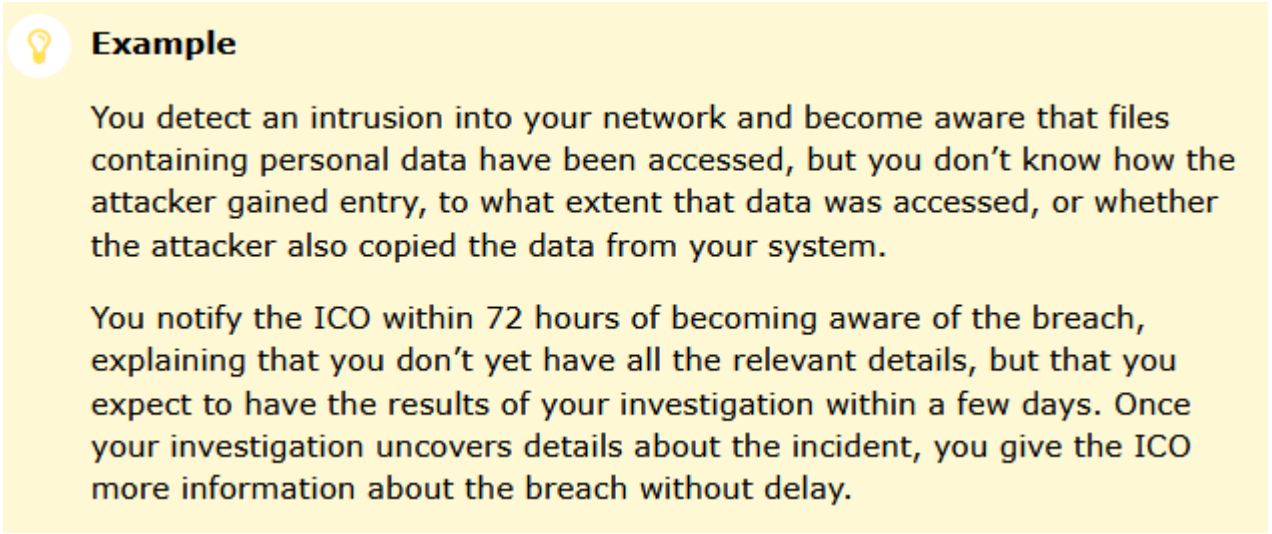
CONTRIBUIÇÕES RECEBIDAS	
IMPORTANTE: Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	**Um incidente deve ser considerado de risco ou dano relevante ao titular quando os dados pessoais envolvidos forem minimamente suficientes para criação de cadastros, autenticação em serviços ou promoção de alterações nos mesmos, como o uso indevido de identidade, a exemplo: *A partir dos dados seja possível contratar planos de Internet ou alterar o número telefônico para outro chip* ou exista potencial para usos danosos. A ANPD poderá regulamentar critérios a serem observados pelos Agentes de tratamento, para que, diante de um incidente de segurança, ajam objetivamente. Estes critérios, a serem avaliados pelos Agentes de Tratamento, envolvem: a) origem dos datasets, b) período a que os dados se referem, c) agente responsável; d) vulnerabilidade explorada, e) modus operandi do atacante, f) medidas técnicas existentes que impediriam ou não o acesso aos dados e possíveis danos.**
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	**Sim, isso já decorre de análises de risco básica:** **Alto: Dados em texto plano suficientes ou sem medidas de proteção aplicadas, com alta probabilidade de utilização indevida, individualização do titular e aplicação de golpes.** **Médio: Dados em texto plano ou com pseudonimização considerada de relativa possibilidade de reversão, suficientes para usos indevidos, porém, com média probabilidade de utilização indevida, individualização do titular e aplicação de golpes, considerando medidas utilizadas e o contexto do vazamento, após análise pericial.** **Baixo: Dados pessoais pseudonimizados, ou dados anonimizados, ou em granularidade insuficiente para utilização indevida, individualização do titular e aplicação de golpes.** **Risco ou Dano baixo poderá ser considerado relevante ou não, desde que se considere a possibilidade de associação destes dados a outros, com a geração de inferências (dados inferidos).**

Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	**<u>Risco ao titular:</u> Risco é a probabilidade de uma ameaça explorar uma ou várias vulnerabilidades, causando prejuízos. Deste modo, para que ocorra risco ao titular, não existe a necessidade de concretização da ameaça e dano, mas a mera probabilidade.** **A partir da Análise da ANPD ou do Agente de tratamento, conclui-se que os dados vazados podem ser utilizados para aplicação de golpes e fraudes, considerando o contexto atual de golpe cibernéticos. Nossa recomendação é que a ANPD estabeleça aos agentes de tratamento a necessidade de Gestão/Avaliação de Riscos envolvendo as fases (Avaliação do risco, tratamento do risco, aceitação do risco, comunicação do risco) A exemplo: Na fase de avaliação, o agente de tratamento buscaria ameaças comuns ao seu negócio e aos dados pessoais, logo, medida prudente para se antecipar a eventuais incidentes.** **<u>Dano ao titular:</u> Dano ao titular é a efetivação do risco. Já a questão do "dano ao titular" é de difícil prova considerando que os dados vazados podem ser utilizados futuramente, porém, sem que seja possível associar a utilização indevida dos dados ao vazamento. Razão pela qual é importante que a ANPD trabalhe com o risco, como aliás é a boa prática internacional. Um exemplo é o caso EQUIFAX, nos Estados Unidos, onde um fundo foi provisionado para que as pessoas envolvidas avaliassem sua situação, inclusive com um site específico para tratativas sobre vazamento de dados (https://www.equifaxbreachsettlement.com/)** **Ressaltamos ainda que a ANPD estabeleça padrões para que diante de vazamentos, tags permitam associar o dado a uma fonte, facilitando a autoria, a perícia técnica e a comprovação do nexo entre o vazamento e um agente de tratamento específico.**
O que deve ser considerado na avaliação dos riscos do incidente?	**A avaliação de risco pode considerar importantes aportes da norma ISO 31000 e ISO 27005 - ISO/IEC 27005 Information Security Risk Management Trainings. Em síntese as empresas deverão estabelecer um programa de análise e avaliação de riscos que considere as fases:** **a) Identificação e análise do risco (arrolamento dos riscos possíveis, com base em fontes)** **b) Avaliação do risco (evento, probabilidade, impacto)** **c) Tratamento dos riscos (medidas a serem tomadas de acordo com a avaliação. Ex: evitar, transferir, reter, reduzir ou mitigar)** **d) Aceitação do risco (Em análise de riscos, decorre de quando o custo da proteção não vale a pena. A ANPD precisa ver com cautela o documento de gestão de riscos de Agentes de tratamento que tenham aceitado o risco. Por isso, entendemos ser relevante que a análise de risco seja um dos documentos que a ANPD pode requerer dos agentes de tratamento.** **e) Comunicação do risco: Planos definidos de comunicação, a partir das disposições da ANPD e regulatórias.**

	A partir do momento em que a ANPD tomar ciência do incidente, pode considerar alguns critérios para avaliar qual foi a diligência do agente de tratamento, diante do mesmo: **a) Medidas técnicas e organizativas para dificultar o acesso ou interpretação dos dados;** **b) Responsabilidade do agente de tratamento em assumir rapidamente a responsabilidade e disponibilização de meios ao titular para mitigar e reduzir riscos ou consultar se seus dados foram comprometidos (A exemplo a EQUIFAX disponibilizou um site (https://eligibility.equifaxbreachsettlement.com/en/Eligibility) para que os cidadãos consultem se os dados foram vazados..** **c) Criticidade e natureza dos dados pessoais (Ex: dados financeiros ou sensíveis). Volume e granularidade dos dados pessoais. (Ex: muitos detalhes sobre o indivíduo). Facilidade dos dados serem usados para fraudes e golpes e acessibilidade dos dados vazados.** **d) Se a comunicação do incidente veio do próprio agente de tratamento ou a partir de terceiros.** **Com base nestes critérios, a ANPD terá elementos importantes para avaliar se o agente de tratamento foi diligente ou não em proteger os dados e em agir adotando boas práticas pós incidente, bem como sobre a gravidade do incidente.**
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	**Além dos dados previstos no parágrafo primeiro do Art. 48, elencamos os seguintes dados:** ● **Dados do operador responsável (caso a vulnerabilidade tenha sido explorada);** ● **Qual vulnerabilidade foi explorada;** ● **Qual o *modus operandi* ou técnica identificada ou de exploração;** ● **Potenciais suspeitos com base no já apurado;** ● **Laudo técnico de perícia forense digital independente (A ANPD poderá exigir um laudo técnico até para que compreenda todas as dimensões do incidente);** ● **Logs em formato estruturado sobre acessos a base comprometida;** ● **Logs em formato estruturado dos últimos compartilhamentos de dados;** ● **Medidas que estão sendo adotadas para que o titular possa reduzir a exposição (Ex: HOTSITE);** ● **Relatório atual de investigação. Acreditamos que a ANPD pode estabelecer um padrão de metadados sobre incidentes, inclusive em linguagem de descrição como RDF, o que padronizaria as comunicações de incidentes e as tornaria mais ágeis, evitando que milhões de agentes enviem dados de incidentes de formas distintas à ANPD.** ● **Apresentar mapeamento de riscos/análise atualizado, envolvendo ativo, ameaça, vulnerabilidades possíveis e medidas que estavam descritas pela empresa diante da concretização do risco. Inclusive indicando qual método foi utilizado: qualitativo ou**

	quantitativo. Lembrando que Análise e avaliação de riscos é um dos principais pilares da Gestão de Segurança da Informação **Um exemplo vem da Autoridade de Controle ICO Britânica, que em seu formulário exige muitas das informações que arrolamos aqui (https://ico.org.uk/media/for-organisations/forms/2172646/eidas-regulations-breach-notification-form.docx)**
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	**Os controladores têm se utilizado da alegação de que "não são os responsáveis" pelos dados vazados e este argumento é de difícil prova. Auditorias serão necessárias neste sentido. Portanto, o prazo não pode exceder 24 horas para incidentes de alta probabilidade de risco ou dano relevante, podendo ser de até 72 horas para riscos médios ou baixos. Lembrando que 72 horas é o prazo da GDPR. A classificação errônea do risco, para fins de notificação, poderá ser objeto de revisão pela ANPD e responsabilização do agente de tratamento. É importante que a ANPD também informe o prazo dos operadores para que comuniquem os controladores e que contratos sejam feitos entre estes, nos termos da ISO 27701. (Sistema de Gestão da Privacidade da Informação). É importante destacar que a ANPD precisa estabelecer como agirá diante das notificações de incidentes com dados que não foram feitas pelo agente de tratamento, mas por terceiros, pois é muito comum na área de segurança da informação que terceiros descubram o incidente antes da empresa e comuniquem a Autoridade. Recomendamos que diante deste cenário, o agente de tratamento seja notificado pela ANPD, após avaliação da denúncia, imediatamente, para confirmar o fato narrado.** **Uma argumentação que vem sendo utilizada pelos controladores é que não notificaram a Autoridade porque estavam "investigando", "confirmando". Porém neste ínterim, as pessoas estão sujeitas a riscos. Recomendamos que a ANPD estabeleça a comunicação de "investigação/confirmação de potencial incidente com dados pessoais" por parte dos agentes de tratamento. Assim, esta saberia tão logo um processo de investigação fosse iniciado, e após, aguardaria a confirmação ou não pelo agente de tratamento, inclusive, podendo requerer medidas já na fase de investigação, permitindo que titulares por exemplo, adotassem medidas protetivas com mais agilidade. Este aspecto, denominado "notificação em fases", considerando que é impossível investigar tudo em 72 horas, é boa prática, e previsto até mesmo nas orientações do ICO: *"What if we don't have all there quired information available yet? The UK GDPR recognises that it will not always be possible to***

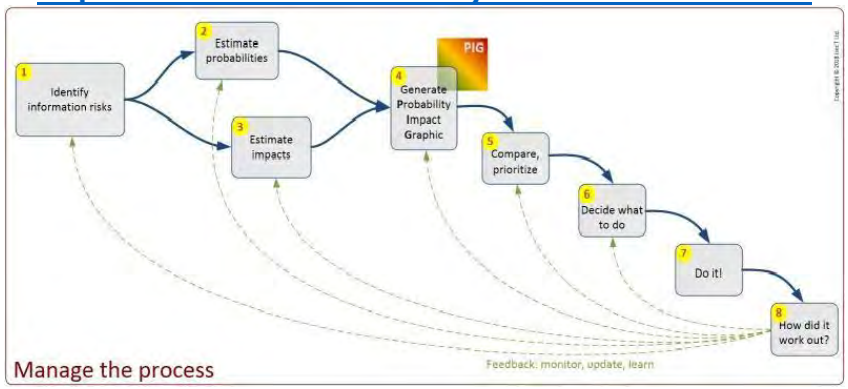
investigate a breach fully within 72 hours to understand exactly what has happened and what needs to be done to mitigate it. So its Article 33(4) allows you to provide the required information in phases, as long as this is done without undue further delay.However, we expect controllers to prioritise the investigation, give it adequate resources, and expedite it urgently. You must still notify us of the breach when you become aware of it, and submit further information as soon as possible. If you know you won't be able to provide full details within 72 hours, it is a good idea to explain the delay to us and tell us when you expect to submit more information.



Fonte: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/#whatinformationmust

Por fim, no que diz respeito à priorização de incidentes, a norma NIST-800-61 (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf) estabelece que um incidente não pode ser tratado no modelo *"firt-come – firt served"* mas deve considerar 3 critérios para decisão sobre qual incidente priorizar:
Impacto funcional: atacam a funcionalidade do negócio.
Impacto informacional do incidente: atacam os dados e os atributos de privacidade.
Impacto na recuperação: o tempo que deverá ser considerado.
Aconselhamos que a ANPD preze pelo impacto informacional do incidente ou relativo aos riscos aos titulares de dados envolvidos.

Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	**A comunicação ao titular de dados deve ser imediata, tão logo a empresa tenha as informações necessárias. A empresa deverá estabelecer um time de resposta a incidentes para avaliação deste contexto, agindo rapidamente. As informações mínimas necessárias são, data, hora do incidente, dados comprometidos, riscos associados, vulnerabilidade explorada, possíveis suspeitos e sites, ou locais em que o titular pode saber mais sobre seus dados e adotar medidas para redução do risco (orientações, cartilhas, manuais e vídeos). Detalhamos mais na sugestão de normativo, anexa ao presente.**
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	**A comunicação deverá ser direta e individual e em casos de alto risco, também publicada ostensivamente. De outro modo, a ANPD poderá utilizar de um padrão de transferência de dados de notificação de incidentes, incluindo linguagem de descrição, como RDF por exemplo (Estabelecendo uma ontologia ou descrição padronizada), facilitando a padronização, organização, leitura por máquina e recuperação de dados sobre as notificações de incidentes. Desencorajamos que formulários em Word continuem sendo usados para estas finalidades. A ANPD pode, por exemplo, fazer chamadas para startups e pesquisadores para soluções e para a contribuição com o desenvolvimento de padrões para transferência e compartilhamento de dados entre a ANPD e agentes de tratamento, que facilitem a interoperabilidade, padronização, encontrabilidade e leitura dos dados. Os padrões online de descrição de informações para comunicação a ANPD poderão, inclusive, serem estabelecidos em outros casos e situações, não apenas na comunicação de incidentes, mas por exemplo, na geração de registros sobre compartilhamento de dados pessoais, trazendo mais transparência à Autoridade e titulares de dados.**
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	**A ANPD precisa saber de todos os incidentes de segurança envolvendo dados pessoais, ainda que seja apenas para registro, estatística, e extração de inferências sobre quais ações precisa focar e as principais vulnerabilidades que estão em exploração. O que pode ser diferente é a formalidade entre um incidente de alto risco, médio e baixo. Empresas também podem notificar algo como baixo risco e a ANPD entender ser alto risco o que demandará uma nova análise/reclassificação e adoção de medidas. Porém, se agentes de tratamento não informarem, estas hipóteses não seriam conhecidas jamais. Recomendamos que apenas os riscos considerados inexistentes sejam considerados exceção à regra da obrigatoriedade de informação.**
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	**Apenas nos casos em que, comprovado por análise forense independente, ficar registrado que os dados vazados não se originaram da base de dados do agente de tratamento ou diante de incidentes considerados de risco inexistente.**

Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	**Criticidade, volume, sensibilidade dos dados e potencial para danos aos titulares; Mora do agente de tratamento em reconhecer responsabilidade; Mora do agente de tratamento em adotar medidas técnicas para mitigar, reduzir, eliminar o risco ou medidas investigativas forenses para apurar o modus operandi e possível autoria/responsabilidade pelos ataques/ameaças. Não disponibilização de meios para que o titular consulte se foi comprometido e informe-se como minimizar possíveis danos de usos indevidos de seus dados. Não disponibilizar instruções claras ao titular para reduzir danos. Não oferecer um canal dedicado ao titular para esclarecer dúvidas.**
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	**ISO 27005, norma dedicada a avalição de riscos de segurança https://www.iso27001security.com/html/27005.html**  **Privacy Incident Handling Guidance - https://www.dhs.gov/sites/default/files/publications/047-01-008%20PIHG%20FINAL%2012-4-2017_0.pdf Data Breach Response Guide https://iapp.org/media/pdf/resource_center/Experian_Data_Breach_Response_Guide.pdf Computer SecurityIncident Handling Guide https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf Página "personal data breaches ICO" (A ANPD poderia criar uma página como a ICO – A página contém um checklist de preparação para uma personal data breach e como responder) inclusive com instruções sobre medidas que devem ser passadas aos titulares de dados, como a troca de senhas: *"If possible, you should give specific and clear advice to individuals on the steps they can take to protect themselves, and what you are willing to do to help them. Depending on the circumstances, this may include such things as:forcing a password reset; advising individuals to use strong, unique passwords; and***

	telling them to look out for phishing emails orfraudulent activity on their accounts" **Traz também guias para contratos entre controladores e operadores, que abordem a questão dos vazamentos de dados: https://ico.org.uk/media/about-the-ico/consultations/2014789/draft-gdpr-contracts-guidance-v1-for-consultation-september-2017.pdf https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/ ISO 29134:2017: Information technology — Security techniques — Guidelines for privacy impact assessment https://www.iso.org/standard/62289.html**
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	**A ANPD pode orientar os controladores a seguirem especificamente a ISO 27701 (Sistema de Gestão da Privacidade da Informação), sobretudo na gestão de incidentes de segurança da informação, coleta de evidências forenses, avaliação, e implementação dos controles, comunicando a ANPD das medidas que foram adotadas. Ex: troca de senhas dos acessos dos titulares, conscientização, área para informações ao titular. Também é recomendável que o controlador conduza uma investigação digital, com compartilhamento dos resultados para a ANPD. Estabelecimento de hot site ou ponto para esclarecimentos ao titular sobre o incidente demonstra-se boa prática. Comprovação da ciência dos titulares sobre o incidente, também. Adoção das medidas de segurança para evitar que a vulnerabilidade não seja novamente explorada.**
Educação	**Autoridades do mundo todo dispõem em seus sites exemplos didáticos sobre, por exemplo, exemplos de violações de dados pessoais. Tal medida organizativa/educacional ajuda na maturidade dos agentes de tratamento (controladores) para estas finalidades, o que recomenda-se seja adotado no Brasil. Ex: https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-breach-examples/**
SUGESTÃO DE NORMATIVO, SE HOUVER	
EM ANEXO AO PRESENTE DOCUMENTO – SUGESTÃO BÁSICA E INICIAL DE NORMATIVO.	

Processo nº 00261.000098/2021-67

PRESIDÊNCIA DA REPÚBLICA
AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS
Coordenação-Geral de Normatização Nota Técnica nº 3/2021/CGN/ANPD

SUGESTÃO DE NORMATIVO

REGULAMENTAÇÃO DO DEVER DE COMUNICAÇÃO DE INCIDENTES DE SEGURANÇA

Autor: Msc. José Antonio Maurilio Milagre de Oliveira

Advogado, Mestre e Doutorando em Ciência da Informação – UNESP, pesquisador do Núcleo de Estudos em Web Semântica e Análise de Dados Newsda-BR USP, Diretor de Políticas Públicas do Instituto de Defesa do Cidadão na Internet – IDCI Brasil

Contato: [redacted]

Data: 02/03/2021

Observações: Pelo presente, apresentamos nossa sugestão de normativo elaborada a partir dos questionamentos e itens formulados por esta R. Coordenação-Geral de Normatização, no Processo em epígrafe, com escopo de início da redação de regulamentação dos dispositivos relativos à comunicação de incidentes de segurança. Desde já registramos que se trata de versão basilar, estrutural e que reflete conceitos e práticas adotadas por Autoridades de Controle Internacionais, sendo imprescindível, logicamente, o debate com vários atores e óticas, para enriquecimento da estrutura, ajustes e para que se possa chegar a um normativo considerado adequado, claro, efetivo e proporcional.

REGULAMENTAÇÃO XX/2021

DISPÕE SOBRE A REGULAMENTAÇÃO DO DEVER DE COMUNICAÇÃO DE INCIDENTES DE SEGURANÇA ENVOLVENDO DADOS PESSOAIS, AVALIAÇÕES DE RISCOS DE INCIDENTES E DÁ OUTRAS PROVIDÊNCIAS.

DEFINIÇÕES E CONCEITOS

Art. X. Para efeitos deste regulamento, considera-se:

a) Risco: Probabilidade de uma ameaça explorar uma ou várias vulnerabilidades, causando exposição ou tratamento indevido de dados pessoais;

b) Dano ao titular: A efetivação concreta do risco de acesso ou tratamento indevido de dados pessoais.

DA AVALIAÇÃO DE RISCOS DE INCIDENTES COM DADOS PESSOAIS

Art. X. A atividade de tratamento de dados pessoais pressupõe a realização de Avaliação de Riscos por parte dos agentes de tratamento. Para elaboração da Avaliação de Riscos, poderão os agentes de tratamento se valerem de melhores práticas e normas internacionalmente conhecidas.

Art. X. Os agentes de tratamento deverão, na realização da avaliação de riscos, considerar a probabilidade de uma ameaça prevista se concretizar, diante das possíveis vulnerabilidades sobre ativos e mecanismos que suportam ou protegem os dados pessoais.

Art. X A ANPD poderá requerer dos agentes de tratamento, a qualquer momento, a apresentação da Avaliação de Riscos de Incidentes com Dados Pessoais. A avaliação de riscos de incidentes com dados pessoais, inserida no contexto de um programa de gerenciamento de riscos de dados pessoais, de implementação obrigatória pelos agentes de tratamento, conterá:

a) Identificação do risco: Arrolamento dos riscos possíveis, com base em fontes de pesquisa;

b) Avaliação do risco: Utilização de metodologias reconhecidas e práticas que considerem o evento, a probabilidade e o impacto, associados aos titulares de dados pessoais;

c) Tratamento de riscos: Medidas a serem tomadas de acordo com a avaliação realizada, incluindo ações como transferir, reter, reduzir ou mitigar o risco;

d) Comunicação do risco: Elaboração de planos definidos de comunicação aos interessados, autoridades e titulares de dados pessoais, nos moldes das disposições da Lei Geral de Proteção de Dados e demais regulamentos expedidos pela Autoridade Nacional de Proteção de Dados.

Art. X Um incidente envolvendo dados pessoais poderá acarretar risco ou dano relevante ao titular de dados pessoais quando os dados pessoais envolvidos forem suficientes para exploração indevida, incluindo:

a) Criação de cadastros;

d) Autenticação em serviços ou alteração dos dados pessoais de titulares;

c) Uso indevido de identidade para autenticação em locais, sistemas e serviços;

d) Discriminação, ações indevidas, decisões equivocadas, maliciosas e danosas aos titulares de dados pessoais.

DA CLASSIFICAÇÃO DO RISCO OU DANO RELEVANTE AOS TITULARES DE DADOS PESSOAIS

Art. X O risco ou dano relevante a titulares de dados poderá ser mensurado, conforme resultados da realização de análise de riscos e considerando as probabilidades de uma ameaça se concretizar, de acordo com as seguintes classificações:

a) Alto: Dados não protegidos por medidas de segurança preventivas ou reativas, e com alta probabilidade, consideradas as medidas aplicáveis e categorias de dados, de execução de ameaça, exploração ou utilização indevida, individualização do titular, discriminação ou uso de dados pessoais para finalidades nocivas ou prejudiciais ao mesmo;

b) Médio: Dados protegidos por medidas de segurança preventivas ou reativas consideradas de relativa possibilidade de reversão ou violação e com média probabilidade, consideradas as medidas aplicáveis e categorias de dados, de execução de ameaça, exploração ou utilização indevida, individualização do titular, discriminação ou uso para finalidades nocivas ou prejudiciais ao mesmo;

c) Baixo: Dados anonimizados ou dados pessoais protegidos por medidas de segurança consideradas de difícil reversão ou violação e com baixa probabilidade, consideradas as medidas aplicáveis e categorias de dados, de execução de ameaça, exploração ou utilização indevida, individualização do titular, discriminação ou uso para finalidades nocivas ao mesmo;

d) Inexistente: Incidentes que não comprometam dados pessoais, comprovados por meio de avaliação técnica de responsabilidade do agente de tratamento.

DA COMUNICAÇÃO DE INCIDENTES COM DADOS PESSOAIS

Art X. A informação à ANPD sobre incidentes de segurança que comprometam dados pessoais, nos termos do parágrafo 1º. do Art. 48 da LGPD, deverá ser feita:

a) Em até 24 (vinte e quatro) para incidentes envolvendo possibilidade de alto risco ou dano relevante aos titulares de dados;

b) Em até 72 (setenta e duas) horas para incidentes envolvendo possibilidade de médio ou baixo risco aos titulares de dados;

Parágrafo primeiro. Os incidentes considerados de risco inexistente ficarão dispensados de serem informados à ANPD, ressalvadas as obrigações do agente de tratamento na manutenção de dados e dos registros. A ANPO poderá, a qualquer momento, requerer o registro de incidentes considerados de risco inexistente, podendo ordenar medidas caso entenda haver riscos aos titulares ou classificação de riscos errônea.

Parágrafo segundo. Caso o agente de tratamento ainda esteja apurando os riscos ou não tenha todos os elementos para caracterização do mesmo, deverá, ainda assim, comunicar à ANPD, nos prazos previstos no caput do artigo, informando estimativa de prazo para complementação das apurações.

Art. X. Complementarmente às disposições do §1º do art. 48 da Lei 13.708/2019, deverão os controladores, diante de um incidente envolvendo dados pessoais, instruir, preferencialmente, notificação à ANPD, contendo:

a) Dados do co-controlador ou operador responsável, caso o incidente tenha se dado na estrutura destes, incluindo todas as análises e avaliações feitas por estes;

b) Indicação clara e precisa de qual vulnerabilidade técnica, humana ou física foi explorada, e quais mecanismos de segurança incidiam sobre a vulnerabilidade;

c) Indicação do *modus operandi* utilizado para exploração e um registro do tempo da exploração, caso possível;

d) Indicação de potenciais suspeitos, caso já apurado;

e) Indicação se o controlador ainda está confirmando a sua responsabilidade e se os dados comprometidos são de sua base ou não;

f) Laudo técnico de perícia forense digital independente, sobre as investigações realizadas;

g) Registros (logs) em formato estruturado sobre acessos a base de dados comprometida;

h) Registros (logs) em formato estruturado relativos aos últimos compartilhamentos dos dados pessoais comprometidos;

i) Medidas que estão sendo adotadas para que o titular possa reduzir a exposição e minimizar possíveis danos;

j) Relatório atual de investigação;

k) Análise de riscos atualizada, contendo inclusive a previsão do risco explorado, ou se inexistente, a justificativa pela qual o risco não era contemplado na análise.

Parágrafo primeiro. A Autoridade Nacional de Proteção de Dados disporá sobre padrões de comunicação eletrônica e interoperabilidade de dados, visando a rápida notificação de incidentes envolvendo dados pessoais, bem como poderá

dispor ou formular novas exigências e documentos adicionais que se fizerem necessários, diante do caso concreto.

DA INFORMAÇÃO AO TITULAR DE DADOS PESSOAIS

Art X. A comunicação ao titular de dados sobre incidentes de segurança que comprometam dados pessoais, nos termos do parágrafo 1º do Art. 48 da LGPD, deverá ser feita imediatamente após o conhecimento do incidente, pelo agente do tratamento e deverá incluir, além do disposto na Lei 13.709/2018:

a) Data e hora do incidente e modus operandi do atacante;

b) Informação sobre dados comprometidos e riscos associados;

c) Possíveis causas do incidente;

d) Sites, hotsites, aplicativos, ou locais em que o titular pode saber mais sobre seus dados e adotar medidas para redução do risco;

e) Orientações, cartilhas, manuais e instruções para que o titular reduza o risco de uso indevido dos seus dados;

Parágrafo primeiro. É dever do agente de tratamento o ônus da prova de que o titular de dados teve ciência de seu comunicado acerca do incidente com dados pessoais, preferencialmente adotando meios tecnológicos para maior agilidade das comunicações e que assegurem confirmação.

Parágrafo segundo. A ANPD poderá regulamentar ou catalogar padrões ou sistemas online para fins de comunicação aos titulares de dados em casos de incidentes.

Art. X. A informação aos titulares sobre incidentes de segurança deixa de ser obrigatória quando:

a) Se tratar de risco inexistente, não ocorrendo comprometimento de dados pessoais;

b) Quando provado, por auditoria independente, que o agente de tratamento não é responsável pelo incidente ou pelos dados identificados;

Parágrafo primeiro. A ANPD poderá, a qualquer momento, requerer e revisar os registros de incidentes considerados de risco inexistente, bem como ordenar a reclassificação do risco e adoção de providências cabíveis.

DAS PROVIDÊNCIAS DIANTE DE UM INCIDENTE COM DADOS PESSOAIS

Art. X. Diante do conhecimento de um incidente de segurança envolvendo dados pessoais, poderá a ANPD determinar providências e diligências aos agentes de tratamento, incluindo, mas não se limitando a:

a) Determinar sejam comprovadas a observância às melhores práticas na gestão de incidentes de segurança de dados;

b) Determinar investigações forense, auditorias e perícias;

c) Requerer a implementação de controles imediatos diante do incidente reportado;

d) Determinar o estabelecimento de orientações aos titulares sobre melhores práticas para evitarem ou minimizarem os riscos a seus dados pessoais;

e) Determinar a criação de área, site, aplicativo ou demais meios de contato com o titular para atendimentos sobre o incidente, onde este poderá checar o comprometimento a seus dados, compreender os riscos, formas de proteção e adotar medidas de segurança;

f) Determinar que o agente de tratamento apresente comprovações de que deu ciência aos titulares de dado de forma inequívoca;

e) Determinar que medidas reparatórias sejam adotadas e providas a titulares, diante do risco do uso indevido de seus dados pessoais e potencialidade danosa.

DA AVALIAÇÃO DA GRAVIDADE DO INCIDENTE

Art. X Após conhecimento do incidente de segurança com dados pessoais, a ANPD, na apuração da gravidade do incidente, deverá considerar:

a) Natureza, volume, sensibilidade dos dados e potencial danoso que o uso indevido possa gerar aos titulares de dados pessoais;

b) Mora do agente de tratamento em reconhecer responsabilidade pelo incidente;

b) A mora do agente de tratamento em comunicar a ANPD e informar os titulares, quando esta não for justificada;

c) Os resultados da classificação da possibilidade do risco ou dano relevante ao titular de dados, conforme disposto no art. X, desde regulamento;

d) A mora ou não adoção, pelo agente de tratamento, de medidas técnicas e organizativas para mitigar, reduzir, eliminar o risco ou adotar medidas investigativas forenses para apurar o *modus operandi* e possível autoria/responsabilidade pelos ataques ou exploração das vulnerabilidades;

e) A mora ou não disponibilização, pelo agente de tratamento, de meios para que o titular consulte informações sobre o incidente e conheça se foi comprometido ou não;

f) A mora ou não disponibilização de instruções claras ao titular para reduzir danos diante do incidente;

e) A não elaboração de Avaliação de Riscos de Incidentes com Dados Pessoais;

f) O descumprimento das disposições da Lei 13.709/2018 na aplicação da conformidade do Agente de tratamento;

e) A reincidência do agente de tratamento, em incidentes da mesma natureza, em um intervalo não superior a 3 (três) meses.

DA PRIORIZAÇÃO DE INCIDENTES

Art. X Os agentes de tratamento, na priorização do atendimento de incidentes de segurança da informação, considerarão sempre o nível de risco aos dados pessoais e potenciais danos aos titulares de dados.

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: KELY CRISTINA GENEBRA

CPF/CNPJ: [redacted]

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS

IMPORTANTE: Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.

<table>
<tr><th>TÓPICO/QUESTÃO</th><th>CONTRIBUIÇÃO/INSTITUIÇÃO</th></tr>
<tr><td>Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?</td><td>Para os 2 questionamentos, poderia ser utilizada uma tabela de nível de sensibilidade, conforme exemplo abaixo:

<table>
<tr><th>Nível de Sensibilidade</th><th>Operações de Compartilhamento</th></tr>
<tr><td>Baixo</td><td>Quando há compartilhamento de Dados Pessoais Anonimizados ou Pseudonimizados que não possibilitam a identificação de um Titular de Dados.</td></tr>
<tr><td>Intermediário</td><td>Quando há compartilhamento de Dados Pessoais, como por exemplo nome, endereço, CPF, e-mail etc., salvo se a operação de compartilhamento envolver Dados Pessoais classificados no nível Alto ou Crítico.</td></tr>
<tr><td>Alto</td><td>Quando há Compartilhamento de Dados Pessoais classificados como: (i) Dados Pessoais Sensíveis; (ii) Dados Pessoais de criança e adolescente; (iii) Dados Pessoais Financeiros; (iv) Dados Pessoais de Comportamento.</td></tr>
<tr><td>Crítico</td><td>Quando há Compartilhamento/Transferência Internacional de Dados Pessoais de operações de tratamento consideradas como críticas.</td></tr>
</table></td></tr>
<tr><td>O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?</td><td>Sim, conforme tabela anterior e também a tabela abaixo considerando a quantidade de titulares envolvidos.</td></tr>
</table>

<table>
<tr><td></td><td>
<table>
<tr><th>Quantidade de Titulares Envolvidos</th><th>Classificação dos Dados</th><th>Grau de criticidade do Incidente</th></tr>
<tr><td rowspan="3">Menos de 1.000</td><td>Simples</td><td>Não crítico</td></tr>
<tr><td>Financeiros e/ou Comportamentais, combinados ou não com Dados Simples</td><td>Criticidade baixa</td></tr>
<tr><td>Sensíveis (combinados ou não com outros tipos de dados)</td><td>Criticidade média</td></tr>
<tr><td rowspan="3">Entre 1.000 e 10.000</td><td>Simples</td><td>Criticidade baixa</td></tr>
<tr><td>Financeiros e/ou Comportamentais, combinados ou não com Dados Simples</td><td>Criticidade média</td></tr>
<tr><td>Sensíveis (combinados ou não com outros tipos de dados)</td><td>Criticidade alta</td></tr>
<tr><td rowspan="2">Entre 10.000 e 100.000</td><td>Simples, Financeiros ou Comportamentais, combinados ou não</td><td>Criticidade média</td></tr>
<tr><td>Sensíveis (combinados ou não com outros tipos de dados)</td><td>Criticidade alta</td></tr>
<tr><td>Mais de 100.000</td><td>Indiferente</td><td>Criticidade alta</td></tr>
</table>
</td></tr>
<tr><td>Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?</td><td></td></tr>
<tr><td>O que deve ser considerado na avaliação dos riscos do incidente?</td><td></td></tr>
<tr><td>Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?</td><td>• Além daquelas listadas na Lei, o controlador deveria apresentar toda a jornada de maturidade da adequação à LGPD (treinamentos, ações de conscientização, ferramentas, fluxos dos processos, etc).</td></tr>
<tr><td>Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)</td><td>• 30 dias corridos a contar da data de notificação que deve ser enviada quando se tenha informações confiáveis sobre o Incidente, capazes de abordar os tópicos mencionados no §1º do art. 48.</td></tr>
<tr><td>Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que</td><td>• O prazo poderia ser o mesmo acima, ou seja, informou à ANPD no mesmo momento informa ao titular, com as mesmas informações. Como titular, sabemos que incidentes ocorrem de diversas formas, mas eu gostaria de saber sobre os esforços do controlador quanto à proteção e privacidade dos meus dados.</td></tr>
</table>

informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	• Sim, por e-mail de forma direta e individual e em casos mais críticos e de maiores impactos para os titulares (seguindo a volumetria da tabela acima, por exemplo) poderia ser feita a comunicação pública.
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	• Acredito que o volume de dados envolvidos no incidente
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	• Casos individuais e de pequeno volume (conforme tabela acima) de incidentes ocorridos por erro de processo interno por exemplo.
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	• Para casos críticos de com volumetria significativa, poderia ser feita auditoria (de processos e de sistemas) no controlador sobre o programa de privacidade e proteção de dados, considerando uma pontuação sobre a adequação à LGPD (Insatisfatório / Necessita melhorias / Satisfatório, por exemplo).
SUGESTÃO DE NORMATIVO, SE HOUVER	

Art. Xxxx ....
Art. Xxxx ....

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: KPMG Auditores Independentes
CPF/CNPJ: 57.755.217/0001-29

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

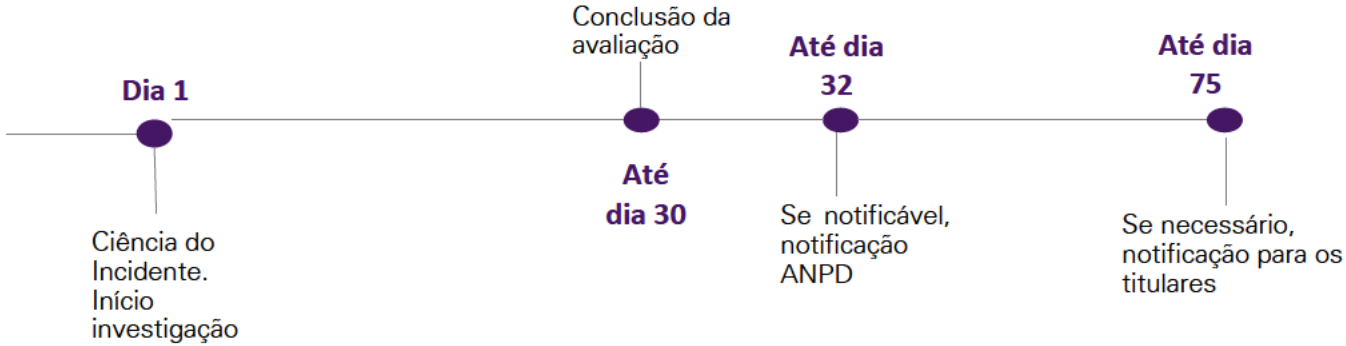
Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS **IMPORTANTE:** Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	Relevante seria algo capaz de alterar de forma significativa o status *quo*. No caso, riscos e danos relevantes aos titulares, seriam aqueles com um potencial acarretar algum tipo de dano físico, material ou imaterial, de forma irreversível ou com alto grau de gravidade em relação aos seus direitos e liberdades fundamentais. Nesse sentido, sugerirmos que sejam adotados critérios objetivos, por meio da adoção de metodologia de avaliação de riscos, de forma a afastar a subjetividade do conceito, posto que, a ausência de critérios objetivos poderá ensejar em (i) insegurança jurídica, (ii) excesso de notificações desnecessárias e (iii) impossibilidade operacional de tratar o que efetivamente precisa ser tratado. Abaixo, apresentamos sugestão de alguns critérios e referências de metodologias: 1.**Insignificante**: os titulares dos dados não serão afetados ou podem encontrar alguns inconvenientes, que serão superados sem problemas (tempo gasto para reinserir informações, aborrecimentos, irritações, etc.) ou as medidas mitigatórias adotadas conseguem minimizar de forma significativa os impactos aos titulares. 2. **Limitada**: os titulares dos dados podem encontrar inconvenientes significativos, capaz de superar com algumas dificuldades (custos extras, negação de acesso aos serviços, medo, falta de compreensão, estresse, pequenas doenças físicas, etc.) ou as medidas mitigatórias conseguem minimizar de forma significativa os impactos. 3. **Significativo**: os titulares dos dados podem encontrar consequências significativas, que deve ser capaz de superar, embora com sérias dificuldades (apropriação indébita de fundos, lista negra de bancos, danos materiais, perda de emprego, intimação, agravamento do estado de saúde, etc.). 4. **Extremo**: os titulares dos dados podem encontrar resultados significativos, ou mesmo irreversíveis, consequências, que eles não podem superar (dificuldades financeiras, como

	substanciais dívidas ou incapacidade para trabalhar, doenças físicas ou psicológicas de longo prazo, discriminações, morte, etc.). A título de referência, existem diversas metodologias disponíveis como por exemplo a metodologia sugerida pela ENISA - *European Union Agency for Network and Information Security* desenvolvida em parceria com as Autoridades de Proteção de Dados Pessoais da Grécia e Alemanha para avaliação da severidade de riscos em incidentes https://www.enisa.europa.eu/publications/dbn-severity ou a ISO 31000 que trata de gestão de riscos de forma geral https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en .
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	Conforme sugerido acima, entendemos que o desenvolvimento de uma metodologia única, com critérios objetivos seria a melhor forma de se garantir segurança jurídica tanto para as empresas quanto para os titulares. Ademais possibilitará à ANPD direcionar esforços para aqueles incidentes que, de fato, necessitem avaliação e tratamento, caso contrário a ANPD poderá estar sujeita a toda sorte de notificações de incidentes que não representam de fato riscos ou danos relevantes ao titulares.
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	O risco é a possibilidade de materialização de um dano ou impacto, já o dano é o resultado da materialização do risco. A ISO 31000 também apresenta conceito de risco versus danos dentro do contexto de gestão de riscos: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en
O que deve ser considerado na avaliação dos riscos do incidente?	Conforme experiência europeia, sugerimos os seguintes critérios para tal avaliação dos riscos, sendo que, conforme mencionamos no item de avaliação de riscos e danos aos titulares, a adoção de uma matriz de classificação tornaria a definição mais objetiva e, consequentemente, mais padronizada, de forma a garantir que o entendimento das empresas quanto a gravidade de um incidente esteja alinhado ao entendimento da ANPD: ▪ Tipo de violação (perda de confidencialidade, perda de integridade, indisponibilidade) ▪ Tipo do incidente (cibernético, físico etc.) ▪ Tipo de potencial risco ou dano

	▪ Gravidade do potencial risco ou dano de acordo com a classificação indicada na primeira pergunta ▪ Quantidade de titulares envolvidos ▪ Natureza dos dados pessoais envolvidos ▪ Capacidade de identificação direta dos titulares ▪ Volume de dados pessoais envolvidos ▪ Tipo do negócio da empresa e operação envolvida no incidente ▪ Identificação da causa raiz do incidente ▪ Descoberta própria do incidente ▪ Status do incidente ▪ Duração do incidente e exposição ▪ Distribuição geográfica da base de dados / dados expostos ▪ Relacionamento com Operadores de Dados ▪ Ações fora do Brasil (Cross Border) ▪ Disponibilidade dos dados para conhecimento público (estão à venda ou foram publicados) ▪ O incidente pode trazer prejuízos a segurança pública ou causar perda de vidas ▪ O incidente pode colocar em risco as operações da Empresa ou sua continuidade ▪ Medidas adotadas para mitigação dos potencias riscos ou danos
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	Entendemos que as informações contidas na LGPD já são suficientes.
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	Incialmente, sugerimos que sejam estabelecidos conceitos para incidentes de segurança e incidentes de segurança com dados pessoais. Incidentes de segurança podem não expor dados pessoais ou trazer prejuízos, o que não deveria ser tratado no âmbito da ANPD. Após isto devemos avaliar o marco inicial para contagem do prazo para notificação tendo em vista os seguintes fatores: a. O report de um possível incidente não significa necessariamente que houve a ocorrência de uma violação de dados pessoais, e ainda, se tal violação de dados pessoais possui o condão de gerar riscos ou danos relevantes aos titulares; e

	b. Para que se tenha uma conclusão quanto a (i) se houve uma violação de dados pessoais e (ii) se esta violação é reportável é necessário um processo de investigação e avaliação do incidente, o que, demanda uma série de ações a depender do tipo de incidente. Nesse sentido, após o report um incidente, deverá haver uma investigação e análise, que segundo as melhores práticas é composta pelas fases de Identificação e Análise, Contingenciamento, Erradicação, Recuperação e Lições Aprendidas. Estas fases são ações indicadas por diversos institutos e entidades que abordam o tema, como por exemplo o *National Institute of Standarts and Technology* – NIST e o SANS *Institute*. Logicamente que o tempo para conclusão de cada etapa acima indicada dependerá do tipo e amplitude do incidente. Assim, nossa sugestão é que haja a especificação de dois prazos, sendo um para a investigação do incidente e outro para a efetiva notificação à ANPD. A exemplo do *Australian Privacy Act* 1988 (https://www.legislation.gov.au/Details/C2021C00139) o prazo sugerido é de até 30 (trinta) dias para a investigação. Caso o incidente seja reportável nos termos a serem definidos, 02 (dois) dias úteis para a notificação. Adicionalmente a isto, considerando a ampla diversidade de tipos de incidentes, sugerimos que o Controlador deva justificar a razão pela qual utilizou determinado período de tempo, desta forma teremos uma ponderação quanto ao tipo do incidente versus sua gravidade e o tempo decorrido para sua investigação, para se garantir que incidentes menos complexos ou cujo riscos aos titulares é evidente sejam tratados da forma mais rápida possível. E, ainda, caso haja uma publicização do incidente, a ANPD poderá solicitar informações sobre o processo de investigação do incidente.
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa	A comunicação aos titulares demanda um esforço operacional e a organização de capacidade de atendimento a todos os titulares, nesse sentido, sugerimos que seja definido um prazo que garanta que as instituições tenham capacidade de se organizar para gerar a comunicação e garantir que o atendimento a todos os titulares se dará de forma eficaz.

comunicação? As mesmas do §1º do art. 48?	Nesse sentido, considerando que poderão haver incidentes que envolvam uma quantidade significativa de titulares, seja definido um prazo máximo de 45 dias contados da conclusão da investigação, para a notificação e atendimento aos titulares. E, da mesmo forma indicada acima, o prazo utilizado para a realização da comunicação e atendimento aos titulares deverá ser justificado. Abaixo indicamos uma linha do tempo considerando os seguintes prazos: investigação, notificação a ANPD e notificação para os titulares:  Quanto as informações a serem fornecidas aos titulares, considerando que a comunicação tem por objetivo comunicar o titular quanto ao incidente bem como possibilitar que o titular adote medidas para mitigar e evitar danos, sugerimos que sejam informados: a. Quais dados pessoais foram objeto do incidente; b. Indicação de quais terceiros tiveram ou podem ter acesso a tais dados; c. Indicação das medidas que a empresa adotou para mitigar os riscos, se houver; d. Indicação de recomendações ao titular, se houver; e e. Dados do Encarregado e/ou canal de atendimento.
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em	Entendemos que a forma de comunicação deverá ser definida a partir do tipo de incidente e de acordo com o volume de titulares envolvidos, posto que, a depender da quantidade de titulares envolvidos algumas formas podem se tornar inviáveis ou até mesmo ineficientes. Nesse sentido sugerimos que seja fornecida a possibilidade de mais de uma forma de comunicação.

determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	Considerando que a LGPD já determinou o critério de que apenas violação de dados pessoais capazes de ensejar em riscos ou danos relevantes aos titulares deverão ser notificadas, entendemos que a exceção serão aquelas que a partir da análise e aplicação da metodologia proposta não estiverem enquadradas na natureza de riscos ou danos relevantes.
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	Além dos casos acima citados, deve-se considerar se a notificação aos titulares poderá prejudicar eventual investigação quanto ao incidente.
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	Conforme experiência europeia, recomendamos que sejam considerados os seguintes critérios para tal avaliação: ▪ Tipo de violação (perda de confidencialidade, perda de integridade, indisponibilidade) ▪ Tipo do incidente (cibernético, físico etc.) ▪ Tipo de potencial risco ou dano ▪ Gravidade do potencial risco ou dano de acordo com a classificação indicada na primeira pergunta ▪ Quantidade de titulares envolvidos ▪ Natureza dos dados pessoais envolvidos ▪ Capacidade de identificação direta dos titulares ▪ Volume de dados pessoais envolvidos ▪ Tipo do negócio da empresa e operação envolvida no incidente ▪ Identificação da causa raiz do incidente ▪ Descoberta própria do incidente ▪ Status do incidente ▪ Duração do incidente e exposição ▪ Distribuição geográfica da base de dados / dados expostos ▪ Relacionamento com Operadores de Dados ▪ Ações fora do Brasil (Cross Border)

	▪ Disponibilidade dos dados para conhecimento público (estão à venda ou foram publicados) ▪ O incidente pode trazer prejuízos a segurança pública ou causar perda de vidas ▪ O incidente pode colocar em risco as operações da Empresa ou sua continuidade ▪ Medidas adotadas para mitigação dos potencias riscos ou danos *https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052* *https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2021/guidelines-012021-examples-regarding-data-breach_en*
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	Considerando que há diferentes tipos de incidentes, com graus de complexidade e resultados diferentes, sugerimos que sejam recomendadas medidas de forma a analisar os seguintes aspectos: O que a equipe e a gerência fariam de forma diferente na próxima ocorrência de um incidente semelhante? Como o compartilhamento de informações com outras organizações pode ser melhorado para evitar o vazamento de dados? Quais ações corretivas podem evitar incidentes semelhantes no futuro? Quais indicadores podem ser observados no futuro para detectar incidentes semelhante?
SUGESTÃO DE NORMATIVO, SE HOUVER	
Art. Xxxx	
Art. Xxxx	

2021 | MARÇO

CONTRIBUIÇÃO À ANPD

TOMADA DE SUBSÍDIOS Nº 2/2021 DA ANPD

INCIDENTES DE SEGURANÇA, PROCESSO DE COMUNICAÇÃO E ANÁLISE DE RISCO

LAPIN

LABORATÓRIO DE POLÍTICAS PÚBLICAS E INTERNET

LABORATÓRIO DE POLÍTICAS PÚBLICAS E INTERNET

Realização:

Laboratório de Políticas Públicas e Internet - LAPIN

Autoria:

Cynthia Picolo Gonzaga de Azevedo

Gustavo Henrique Luz Silva

Isabela Maria Rosal Santos

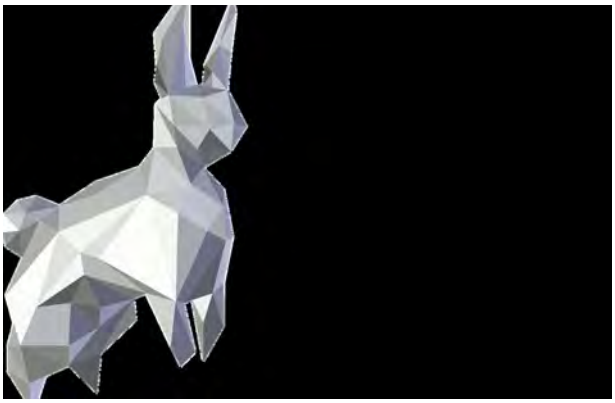
Revisão:

Amanda Espiñeira

José Renato Laranjeira de Pereira

Imagem de Capa:

anyaberkut, Getty Images



lapin.org.br

@lapin.br

/lapinbr

/lapinbr

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2/2021

NOME DA INSTITUIÇÃO: Laboratório de Políticas Públicas e Internet - LAPIN[1]

O Laboratório de Políticas Públicas e Internet (LAPIN) é um think tank de composição multidisciplinar com sede na capital federal brasileira. Seu objetivo é apoiar o desenvolvimento de políticas públicas voltadas para a regulação das tecnologias digitais por meio da pesquisa e da conscientização da sociedade. Para maiores informações sobre nossa atuação, visite nosso site: <https://lapin.org.br/>.

CNPJ: 36.965.428/0001-16

1 [redacted]

CONTRIBUIÇÕES RECEBIDAS	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO - LAPIN**
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	**Um incidente de segurança pode acarretar risco ou dano relevante ao titular quando há um aumento de risco de roubo de identidade, fraude ou danos à reputação[2], ainda que esses não se concretizem a ponto de configurar danos.** Isso está de acordo com a ideia que direciona, por exemplo, o GDPR[3], no sentido de que o risco relevante sobre o tema de incidente de segurança é o risco adverso para o titular[4]. Um elemento de extrema relevância na avaliação do risco relacionado a um incidente de segurança é a consideração das possíveis consequências negativas para os indivíduos. Já o dano é a concretização dessas

[2] SOLOVE, D; CITRON, D. K. **Risk and Anxiety: A theory of data-breach harms**. Texas Law Review 737. 2018. Disponível no SSRN: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2885638>. Acesso em 22 mar. 2021.

[3] O Considerando 75 do GDPR traz o conceito de risco: "O risco para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, poderá resultar de operações de tratamento de dados pessoais suscetíveis de causar danos físicos, materiais ou imateriais, em especial quando o tratamento possa dar origem à discriminação, à usurpação ou roubo da identidade, a perdas financeiras, prejuízos para a reputação, perdas de confidencialidade de dados pessoais protegidos por sigilo profissional, à inversão não autorizada da pseudonimização, ou a quaisquer outros prejuízos importantes de natureza econômica ou social; quando os titulares dos dados possam ficar privados dos seus direitos e liberdades ou impedidos do exercício do controle sobre os respetivos dados pessoais; quando forem tratados dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas e a filiação sindical, bem como dados genéticos ou dados relativos à saúde ou à vida sexual ou a condenações penais e infrações ou medidas de segurança conexas; quando forem avaliados aspectos de natureza pessoal, em particular análises ou previsões de aspectos que digam respeito ao desempenho no trabalho, à situação econômica, à saúde, às preferências ou interesses pessoais, à confiabilidade ou comportamento e à localização ou às deslocações das pessoas, a fim de definir ou fazer uso de perfis; quando forem tratados dados relativos a pessoas singulares vulneráveis, em particular crianças; ou quando o tratamento incidir sobre uma grande quantidade de dados pessoais e afetar um grande número de titulares de dados".

[4] CIPL. **Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR**. 2016. Disponível em: <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf>. Acesso em 23 mar. 2021.

	possíveis consequências. Tais conceitos devem ser interpretados de maneira extensiva, abrangendo efeitos morais, patrimoniais, individuais e coletivos, conforme o art. 42 da LGPD. A interpretação dos efeitos negativos ao titular deve ser feita da maneira mais abrangente possível, uma vez que a compensação por danos na esfera informacional de um indivíduo é de difícil realização, pois um vazamento de dados muitas vezes é irreversível em sua completude. Por essa razão, o regime de proteção de dados brasileiro se utiliza de instrumentos preventivos, a fim de evitar possíveis riscos ou danos para não ser necessário alcançar a fase indenizatória[5]. A interpretação extensiva dos resultados de um incidente também está prevista no *caput* do art. 42 da LGPD, que prevê que "o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados, é obrigado a repará-lo". A ideia de consequências negativas para o titular para fins de avaliação de riscos e gravidade também é adotada em outros momentos na LGPD e deve ser o foco central na avaliação dos riscos, considerando a probabilidade de concretização do risco e sua gravidade. Isso consta inclusive no teste de balanceamento do legítimo interesse, previsto no art. 7º, IX da LGPD: quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

[5] A prevenção é um princípio básico para o tratamento de dados, previsto no art. 6º, inciso VIII, da LGPD. Nesse mesmo sentido, no GDPR: Article 29 Working Party. **Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC**. Disponível em: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf> p. 30-33; p. 37. Acesso em 23 mar. 2021.

	Outro fator que gera presunção de risco ou dano relevante ao titular é a **categoria** dos dados pessoais afetados pelo incidente. Se **dados sensíveis** ou **dados de crianças e adolescentes** forem afetados, já deve existir uma presunção de risco ou dano relevante ao titular. Nesse sentido, também deve haver a consideração de **grupos minoritários** ou **grupos em situação de vulnerabilidade** (como indivíduos com condenações penais ou até refugiados). Se os dados afetados contarem com informações sobre esses grupos, maior a relevância do risco ou dano. Além disso, para mensuração do risco ao titular, também deve ser considerada a **probabilidade de o dano se concretizar**. Quanto mais altas as chances de concretização de dano, mais grave ou relevante deve ser considerado o incidente de segurança. Nesse sentido, também devem ser considerados possíveis danos morais relevantes aqueles relacionados ao estresse e ao medo, mas há gravidade evidente quando houver risco de prejuízos financeiros ou à integridade física, por exemplo. Também se mostra necessária a avaliação do **volume de dados** afetados. De maneira geral, quanto mais dados são afetados, maior a relevância desse incidente. Cabe ressaltar que um alto volume de um único tipo de dado pode vir a ser menos grave do que um incidente que afete vários dados sobre um determinado indivíduo, possibilitando a sua completa identificação, incluindo a revelação de seu perfil comportamental ou inferências feitas por determinado algoritmo. Por isso, é essencial a **avaliação do contexto** em que se encontram os dados impactados, para entender o que esse volume significa para os titulares de dados afetados. Esses pontos estão relacionados com a metodologia para gestão de risco (2012)[6] e a metodologia para a formulação de relatório de impacto de dados pessoais (2018 — ver questão sobre metodologias)[7] apresentadas pela

[6] Disponível em: <https://www.cnil.fr/sites/default/files/typo/document/CNIL-ManagingPrivacyRisks-Methodology.pdf>. Acesso em 22 mar. 2021.
[7] Disponível em: <https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf>. Acesso em 22 mar. 2021.

autoridade francesa de proteção de dados, a *Commission Nationale de l'Informatique et des Libertés* – CNIL, e sintetizadas através das seguintes imagens (em tradução livre):

[Figura 1 - metodologia de gestão de risco]

[Figura 2 - relatório de impacto à proteção de dados pessoais]

Esses dois ciclos demonstram a importância da consideração dos riscos na gestão da proteção de dados. A avaliação do contexto e das consequências, possíveis ou concretas, nessa gestão de riscos e impactos é crucial para garantir a observância dos princípios e direitos do titular. Além disso, devem ser considerados os eventos esperados e as possíveis ameaças. Pretende-se endereçar todos esses pontos ao longo da tomada. A experiência

	francesa, inclusive, demonstra a importância da formulação de materiais didáticos sobre esse tema por parte da ANPD.[8] A prática australiana nos mostra o mesmo; a legislação australiana também prevê a necessidade de comunicação se um incidente de segurança tiver probabilidade de causar dano relevante e, em seu site, traz **exemplos de situações que configuram dano relevante**[9]: roubo de identidade que possa afetar finanças e relatório de crédito; perda financeira por fraude; um provável risco de dano físico, como por exemplo, por um ex-parceiro abusivo; danos psicológicos graves; e danos sérios à reputação de um indivíduo. Em síntese e diante do exposto, o LAPIN acredita que os **seguintes critérios devem ser utilizados para avaliar o risco ou dano como relevante**: ● A **categoria dos dados afetados** pelo incidente (dados sensíveis e dados de crianças e adolescentes já configurariam risco ou dano relevante — é necessário considerar o contexto dos dados para fazer essa análise) em conjunto com o **volume de dados** afetados; ● Se **terceiros não autorizados têm acesso aos dados afetados** (o fato desses terceiros serem desconhecidos agravaria o resultado da avaliação — p. ex., a divulgação dos dados afetados em listas ou a venda dos dados já traria a relevância do risco ou dano);

[8] Nesse sentido, o relatório do *Global Privacy Enforcement Network* (GPEN) demonstra que organizações sem políticas internas sobre incidentes de segurança utilizavam os guias das autoridades quando necessário. Disponível em: <https://privacy.org.nz/publications/statements-media-releases/gpen-sweep-finds-significant-awareness-of-managing-data-breaches-concerns-regarding-low-engagement>. Acesso em 23 mar. 2021.

[9] Disponível em: <https://www.oaic.gov.au/privacy/data-breaches/what-is-a-notifiable-data-breach/>. Acesso em 22 mar. 2021.

	• A **probabilidade de concretização do dano** (essa avaliação deve considerar as possíveis consequências do incidente, sem menosprezar danos de natureza moral, como estresse e medo); • A **gravidade** dos possíveis danos; • **Características específicas** sobre os titulares afetados (se pertencem a algum grupo minoritário ou em situação de vulnerabilidade, se existe algum perigo relacionado à violação daqueles dados etc.); • O contexto da **origem** do incidente (considerando, inclusive, se a entidade já adotava um programa de *compliance* à proteção de dados e se a ameaça foi interna ou externa).
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto etc.)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	É bem-vinda a adoção de gradação das categorias de risco e de dano. Essa categorização possibilitará a compreensão sobre a urgência de comunicação à ANPD e também sobre a necessidade de comunicação do titular. A experiência internacional também utiliza dessa gradação para avaliar os riscos de incidentes de segurança, como a apresentada pela autoridade francesa[10], demonstrada pela imagem a seguir, em tradução livre:

[10] Disponível em: <https://www.cnil.fr/sites/default/files/typo/document/CNIL-ManagingPrivacyRisks-Methodology.pdf>. p. 18. Acesso em 22 mar. 2021.

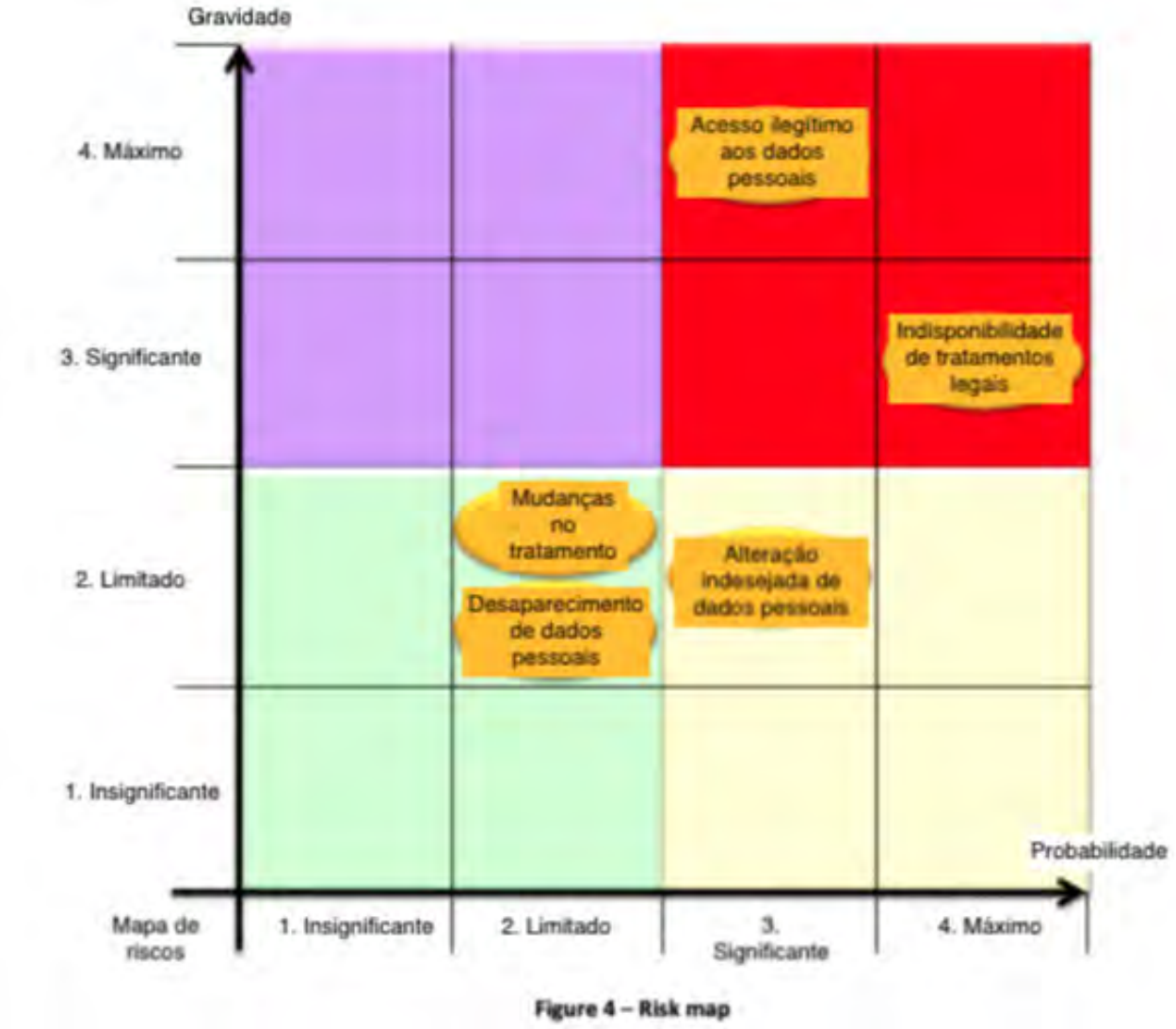


Figure 4 – Risk map

[Figura 3 - gráfico sobre gradação de riscos, a partir de avaliação de gravidade dos riscos e probabilidade de concretização dos riscos]

O gráfico apresentado demonstra a relação entre gravidade e probabilidade de concretização de um risco para classificar o risco em algumas das subdivisões – risco máximo, significante, limitado ou insignificante. Ou seja, riscos baixos têm probabilidade de concretização e gravidade das possíveis consequências também insignificantes. Assim, resta clara a relação direta da classificação do risco com a questão da gravidade do incidente de segurança, uma vez que, quanto mais grave o incidente, maior o risco relacionado a esse fato.

O GDPR também traz previsões sobre um "elevado risco", demonstrando certa subdivisão do risco, inclusive enumerando tratamentos de alto risco[11] em seu artigo 35(3):

a) Avaliação sistemática e completa dos aspectos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado, incluindo a definição de perfis, sendo com base nela adotadas decisões que produzem efeitos jurídicos relativamente à pessoa singular ou a afetem significativa de forma similar;

b) Operações de tratamento em grande escala de categorias especiais de dados a que se refere o art. 9 (1), ou de dados pessoais relacionados a condenações penais e infrações a que se refere o art. 10; ou

c) Controle sistemático de zonas acessíveis ao público em grande escala.

Com isso em mente, **propõe-se a seguinte distinção de níveis de risco**:

- **Irrelevante** → não existem possíveis consequências negativas para o titular (p. ex.: os dados afetados já eram públicos e não é possível nenhuma inferência adicional a partir do contexto em que os dados se inserem);

[11] CIPL. **Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR**. 2016. Disponível em: <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_gdpr_project_risk_white_paper_21_december_2016.pdf>. Acesso em 23 mar. 2021.

	• **Baixo** → as possíveis consequências negativas para o titular têm pouco impacto e ainda são reversíveis (p. ex.: basta o recadastramento do titular ou atualização de seus dados para reverter o dano gerado); • **Médio** → as possíveis consequências negativas para o titular podem gerar impactos maiores, mas ainda reversíveis (p. ex.: atualização do cadastro em vários meios ou necessidade de pedido de exclusão de bancos de dados em que as informações foram adicionadas); • **Alto** → as consequências negativas são mais severas e sua reversão depende do gasto de recursos de tempo e financeiros (p. ex.: intimações judiciais ou extrajudiciais, mudanças em scores de crédito); • **Alarmante** → as possíveis consequências são significantes e não são passíveis de reversão (p. ex.: dificuldades financeiras, dificuldades em conseguir ou manter uma relação de trabalho). Ainda é importante verificar tanto o **critério quantitativo** (relacionado ao número de titulares afetados e a quantidade de dados afetados em relação a cada indivíduo) quanto o **critério qualitativo** (análise contextual dos titulares e dados afetados, além da consideração de características específicas do controlador e de como se deu o incidente). Esses critérios, que merecem definição detalhada pela ANPD, também vão possibilitar que somente incidentes relevantes sejam comunicados à ANPD, evitando uma enxurrada de comunicações, o que impediria a análise efetiva por parte da Autoridade. Essa ideia ainda está completamente de acordo com o art. 52, §7º, da LGPD, que possibilita a conciliação direta do controlador com o titular afetado em caso de incidentes individuais. A classificação do risco é aplicável à categorização do dano, uma vez que o dano é a concretização do risco, excluído o dano irrelevante, uma vez que é impossível existir dano sem consequências negativas ao titular. **Então, a subdivisão de dano será equivalente a dano baixo, médio, alto ou alarmante,** a partir da avaliação de quais riscos efetivamente se concretizaram. É importante ressaltar, no entanto, que, independentemente de sua classificação,

	uma vez comprovado dano, de qualquer natureza, ao titular, já há relevância nos efeitos do incidente de segurança, considerando que o dano é a concretização do risco. Dessa forma, o risco irrelevante não deve ser considerado como passível de ser comunicado à ANPD ou ao titular; o risco baixo, por sua vez, só poderá ser considerado relevante se houver fatores adicionais que agravem a situação (p. ex.: a volumetria dos dados afetados); já os riscos médio, alto e alarmante devem ser considerados todos como relevantes, gerando obrigação de comunicação à ANPD. Além disso, pelo menos os incidentes que gerem riscos alto ou alarmante devem ser comunicados também diretamente aos titulares. Por fim, nas situações em que houver dano, ou seja, risco concretizado, deverá haver, ao menos, comunicação à ANPD. Além disso, deve-se comunicar ao titular informações sobre o incidente no caso de dano médio, alto ou alarmante.
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	O risco é equivalente às consequências negativas hipotéticas, possíveis, oriundas do incidente de segurança. A avaliação dos riscos deve ser feita de forma abrangente a fim de se considerar riscos que podem gerar danos morais, materiais, individuais ou coletivos. Já o dano consiste na concretização do risco. É o momento em que a consequência hipotética se torna real. Por isso, o risco gera dever de prevenção, transparência e prestação de contas. Já o dano, além desses, também gera o dever de indenização, conforme dispõe o art. 42 da LGPD. Portanto, os conceitos se relacionam, uma vez que tratam de momentos diferentes de um mesmo efeito negativo ao titular: o risco em um momento anterior, a partir de avaliação hipotética; e o dano, algo posterior, que é a efetivação da probabilidade. Um exemplo dessa diferenciação seria um incidente envolvendo o funcionário de um escritório de advocacia que perdeu uma mochila que continha seu laptop e arquivos de papel com informações de clientes. O funcionário

	disse a seu gerente que acreditava que o laptop estava criptografado e que os dados nos arquivos em papel haviam sido marcados com caneta preta para evitar que pudessem ser lidos. O gerente, então, relatou o incidente ao departamento de TI, que limpou remotamente o laptop. Pelo fato de o risco, nessa situação, ser considerado baixo, já que a proteção contra invasão de seu computador era forte e os arquivos em papel não poderiam ser lidos, o controlador muito provavelmente não necessitaria informar o incidente à Autoridade. Ocorre que, posteriormente, o departamento de TI descobriu que o funcionário estava trabalhando em um laptop antigo, que não era criptografado nem protegido por senha. O funcionário também confirmou que os arquivos em papel eram de um julgamento criminal que se aproximava e que os dados pessoais, relacionados a condenações criminais e informações de saúde, talvez ainda pudessem ser lidos, porque descobriu que uma cópia dos documentos, dessa vez sem deleções, também estava na mochila perdida. Com isso, houve um aumento expressivo de risco de dano nessa situação, bem como uma potencial presunção de dano, já que muito provavelmente a pessoa que localizou o computador e os arquivos físicos pôde visualizá-los e ter amplo acesso aos dados pessoais ali presentes[12].
O que deve ser considerado na avaliação dos riscos do incidente?	Devem ser consideradas as características do incidente, do contexto do tratamento dos dados, dos titulares afetados e da entidade controladora. Além disso, é necessário considerar a gravidade das possíveis consequências e a possibilidade de concretização dessas. Esses pontos permitem uma avaliação completa e extensa dos riscos ao titular e à sociedade, ou seja, as possíveis consequências negativas oriundas do incidente.

[12] Disponível em: <https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-breach-examples/>. Acesso em 24 mar 2021.

	Esse direcionamento está de acordo com o guia sobre incidentes de segurança elaborado pelo Article 29 Working Party (ou WP29), órgão responsável por lançar guias sobre a aplicação da proteção de dados na Europa antes da entrada em vigor do GDPR, que recomenda a consideração dos seguintes pontos na **análise de risco**[13]: 1. o tipo de incidente; 2. a natureza, a sensibilidade e o volume de dados afetados - considerando as características especiais dos indivíduos afetados; 3. o número de indivíduos afetados. 4. a facilidade de identificação de indivíduos; 5. a gravidade das consequências para os indivíduos; e 6. as características do controlador. Já a *Agencia Española de Protección de Datos*[14] defende que os seguintes fatores devem ser considerados na **análise de risco** de um incidente: o tipo de ameaça; contexto ou origem da ameaça — interna ou externa; categoria de segurança dos sistemas utilizados; dados afetados; perfis dos titulares afetados; número e classificação dos sistemas afetados; impacto do incidente na organização; exigências legais e regulatórias; vetor ou método do ataque. Trazemos essas experiências internacionais por considerarmos que tais critérios, por garantirem uma abordagem objetiva para a avaliação de riscos do incidente, também podem ser adotados pela ANPD.

[13] Article 29 Working Party, **Guidelines on Personal data breach notification under Regulation 2016/679.** Disponível em: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052> p. 24-26. Acesso em 16 mar. 2021.
[14] Agencia Española de Protección de Datos. **Guide on personal data breach management and notification.** Disponível em: <https://www.aepd.es/sites/default/files/2019-09/Guide-on-personal-data-breach.pdf>. Acesso em 16 mar. 2021.

Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	As primeiras orientações trazidas pela ANPD através da disponibilização de formulário para comunicação de incidente de segurança[15] são oportunas, inclusive porque detalham melhor as informações necessárias a serem comunicadas. Destaca-se a necessidade de identificação do encarregado ou equivalente como ponto de contato com a ANPD, as circunstâncias em que ocorreu a violação de segurança de dados pessoais, possíveis problemas de natureza transfronteiriça, além da quantidade de dados e de titulares afetados. Esse último ponto é de suma importância para compreensão dos possíveis riscos oriundos do incidente, porque pode ser mais arriscado o vazamento de várias informações sobre um indivíduo do que o de um só tipo de informação menos sensível sobre diversos titulares — tal avaliação dependerá do caso concreto e por isso é importante a discriminação dessas informações na comunicação. Sendo assim, é fundamental a descrição da categoria dos dados afetados e o contexto que os dados estavam inseridos. Por exemplo: uma informação como o nome de um titular não parece ser tão prejudicial, mas se considerado o contexto do incidente, como um vazamento de pessoas diagnosticadas com uma doença, passa a ser uma informação sensível. Para melhor compreensão do período entre a data e hora da detecção e a comunicação, também pode ser requisitada como informação adicional maior detalhamento sobre o processo de comunicação interna de incidentes da organização. Essa informação pode justificar a demora em notificar a ANPD, porque o incidente pode ter ocorrido em uma área de baixo risco, por exemplo, e esse detalhamento de processos internos pode ajudar na compreensão de como se deu o incidente e sobre o nível de *compliance* da organização que sofreu o incidente. O LAPIN também apoia a ideia de possibilitar uma comunicação preliminar e outra completa, como já proposto pela ANPD. A comunicação preliminar deve contar com algumas informações mínimas: natureza dos dados pessoais afetados; os riscos relacionados ao incidente; uma estimativa do prazo para envio da comunicação

[15] ANPD, Comunicação de Incidentes de Segurança. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca>. Acesso em 22 mar. 2021.

	completa; e informações sobre os titulares envolvidos, como a quantidade de pessoas, as regiões geográficas afetadas, o perfil geral dos afetados com informações que permitam um titular compreender as chances de ele estar envolvido nesse determinado incidente - principalmente nos casos em que não há comunicação individual e direta. A possibilidade de uma comunicação parcial tem por ponto positivo permitir que o controlador forneça informações sobre o incidente posteriormente à comunicação imediata, já que, dependendo do tipo de incidente, a investigação e avaliação internas serão mais complexas, e nem sempre informações relevantes estarão disponíveis rapidamente e com um grau de certeza mais elevado. Além disso, podem ser enviadas outras comunicações parciais até o envio da comunicação completa definitiva. Já a comunicação completa deve conter as demais informações já detalhadas no formulário preliminar da ANPD e, a depender do caso, o processo de comunicação interna de incidentes. Deve-se questionar em quanto tempo uma comunicação parcial deva ser completada, tendo em vista que um procedimento muito demorado aumenta as chances de concretizar riscos ou de agravar o dano, impactando diretamente nos direitos dos titulares (ver tópico seguinte). Ressalta-se que, da perspectiva do titular, o objetivo da comunicação é justamente limitar os danos. De qualquer forma, para possibilitar que as comunicações sejam feitas de modo adequado, a ANPD deve fornecer maiores orientações sobre o que será enquadrado como incidente de segurança — inclusive se será adotada a definição da Administração Pública federal trazida pelo Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo, por exemplo. Isso é fundamental, já que a possível definição que pode ser retirada do art. 46 da LGPD é muito ampla e pode afastar comunicações relevantes ou fazer com que sejam notificados incidentes que não apresentam riscos ao

	titular, aumentando de forma expressiva o número de notificações e impossibilitando uma verificação adequada por parte da ANPD. Considerando que as informações constantes da comunicação devem respaldar a averiguação do incidente de segurança pela ANPD, é essencial que elas proporcionem o máximo de clareza e entendimento sobre o fato. Essa compreensão não somente guiará a ANPD quando da análise da gravidade do incidente, mas também permitirá maior celeridade na solução dos problemas, na implementação de estratégias para mitigação de riscos e na eventual responsabilização, lembrando que em diversas circunstâncias a ANPD agirá em conjunto com outros atores. Em síntese, para além daquelas já solicitadas no formulário disponibilizado pela ANPD, as seguintes informações complementares devem constar na comunicação de incidentes de segurança à Autoridade: ● Indicação de **prazo estimado** para completar a comunicação parcial; ● Uma referência clara para que se informe o **período aproximado de ocorrência da violação** de dados no tópico "Quando o incidente ocorreu?" nos casos em que não se possa delimitar com exatidão a data/período do incidente; ● Detalhes de **quem potencialmente teve acesso aos dados pessoais**, quando possível. Essa informação ajudaria na avaliação de gravidade; o risco pode ser maior ou menor considerando o agente que possivelmente acessou os dados; ● Detalhes sobre o **processo de comunicação interna** de incidentes da organização;

	• Informações de quais **técnicas para segurança** dos dados haviam sido utilizadas, como anonimização, pseudonimização ou criptografia; • Detalhes sobre a **avaliação** feita para determinação da existência de risco ou dano relevante aos titulares, especialmente nos casos em que, a princípio, não for possível identificar com clareza o tipo de violação de dados; • Mais informações em relação ao **conteúdo da comunicação aos titulares**, já que é imprescindível que o controlador adote postura preventiva e forneça meios para que os titulares afetados possam, de fato, adotar medidas de mitigação de risco, incluindo através de canais disponibilizados pelo controlador. A depender do que foi ou pretende ser informado aos titulares, a ANPD poderá recomendar ações. Ademais, estas informações ajudarão a embasar a decisão da ANPD sobre a adoção de medidas complementares para a salvaguarda dos direitos dos titulares previstas no art. 48, §2º, da LGPD; • Informações sobre **organizações e/ou outras autoridades a serem notificadas**, especialmente considerando o cenário em que a ANPD atuará em conjunto com outras entidades.
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	O primeiro ponto a ser discutido é a partir de quando começa a correr o prazo para o controlador comunicar a ANPD. No âmbito do GDPR, o controlador deve comunicar o incidente à autoridade em até 72 horas a partir do *conhecimento do fato*, e muito se discutiu sobre quando seria este momento. De acordo com o Article 29 Working Party, o controlador deve ser considerado 'ciente' do fato quando existe um **grau razoável de certeza** que ocorreu um incidente de segurança que comprometeu dados pessoais[16].

[16] Article 29 Working Party, **Guidelines on Personal data breach notification under Regulation 2016/679.** Disponível em: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052> p. 11. Acesso em 16 mar. 2021.

	O WP29 discorre, ainda, que o momento exato em que o controlador pode ser considerado ciente de uma violação de dados dependerá das circunstâncias, que poderão ser mais ou menos claras. No entanto, o WP29 orienta que **a ênfase deve ser na ação imediata para investigar o incidente para determinar se os dados pessoais foram realmente comprometidos** e, em caso afirmativo, tomar medidas corretivas e comunicar, se necessário.[17] Na impossibilidade de determinar com precisão o momento em que o controlador toma ciência de um incidente que deva ser comunicado à ANPD, é importante que especialmente os princípios da boa-fé (art. 6º, *caput*), da segurança (art. 6º, VII), da prevenção (art. 6º, VIII) e da responsabilização e prestação de contas (art. 6º, X) sejam rigidamente observados. Além disso, deve-se ponderar que os agentes de tratamento são obrigados a utilizar sistemas que atendam aos requisitos de segurança (art. 49), o que pressupõe certa estruturação para lidar com incidentes de segurança de dados pessoais. Por fim, e seguindo a linha do WP29, um "grau razoável de certeza" que ocorreu um incidente de segurança de dados pessoais pode ser considerado como o ponto de partida no processo de comunicação. De qualquer forma, havendo dúvidas sobre comunicar ou não a ANPD, é importante que seja adotada uma abordagem baseada no risco e que o controlador elabore, pelo menos, uma comunicação parcial, reservando-se o direito de fornecer informações mais precisas em um segundo momento[18]. Em relação ao prazo razoável para comunicar a ANPD sobre o incidente de segurança, o LAPIN sugere o prazo de 72 horas a partir do conhecimento do incidente — pelo menos para o envio da comunicação parcial. O prazo sugerido segue a experiência internacional sobre o tema, como as seguintes:

[17] ibid.

[18] No entanto, não podemos deixar de pontuar que a comunicação à ANPD sem um grau de certeza razoável pode levar ao *notification fatigue* – conceito bastante utilizado na Europa para indicar a fadiga causada a controladores, autoridades de proteção de dados e titulares de dados quando não há critérios bem definidos para comunicações de incidentes de segurança, levando a um alto volume de incidentes comunicados.

	• União Europeia → comunicação deve ocorrer imediatamente e, se possível, em até 72 horas após o conhecimento da violação[19]; • Uruguai → em até 72 horas após o conhecimento da violação[20]; • Argentina → a Lei de Proteção de Dados Pessoais nº 25.326, em vigor na Argentina desde 2000, não prevê a obrigação de notificar incidentes de segurança aos titulares de dados pessoais ou à autoridade de controle. Porém, um projeto de lei em discussão prevê que a comunicação do incidente seja feita imediatamente ou, no mais tardar, em até 72 horas do conhecimento do fato[21]; • Singapura → imediatamente ou, no mais tardar, em até 72 horas da determinação que o incidente é passível de notificação[22]. Além disso, é importante a definição de um prazo para a apresentação da comunicação completa e, nesse caso, sugere-se o prazo adicional de 10 dias (equivalente ao prazo da Portaria do Ministério da Justiça e Segurança Pública nº 618/2019[23], que disciplina o *recall*), contados a partir do protocolo da comunicação parcial. Este prazo é importante pois, dependendo do tipo de incidente, a investigação e avaliação internas serão mais complexas, e nem

[19] Regulamento Geral sobre Proteção de Dados, art. 33(1). Disponível em: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>. Acesso em 22 mar. 2021.
[20] Decreto n° 64/020, art. 4°. Disponível em: <www.impo.com.uy/bases/decretos/64-2020>. Acesso em 22 mar. 2021.
[21] Diputados Argentina, Dirección Secretaría – Tramite Parlamentario n. 171, Proyecto de Ley de Protección de Los Datos Personales, art. 20. Disponível em: <https://www4.hcdn.gob.ar/dependencias/dsecretaria/Periodo2020/PDF2020/TP2020/6234-D-2020.pdf>. Acesso em 22 mar. 2021.
[22] Personal Data Protection Commission. **Advisory Guidelines on Key Concepts in the Personal Data Protection Act**, p. 141. Disponível em: <www.pdpc.gov.sg/-/media/Files/PDPC/PDF-Files/Advisory-Guidelines/AG-on-Key-Concepts/Advisory-Guidelines-on-Key-Concepts-in-the-PDPA-1-Feb-2021.pdf?la=en>. Acesso em 22 mar. 2021.
[23] Art. 2º, §10 da Portaria: A investigação do fornecedor de produtos e serviços, para determinar a comunicação de que trata o art. 3º desta Portaria não deve ultrapassar o prazo de dez dias úteis, a menos que o fornecedor demonstre circunstanciadamente que a extensão do prazo é necessária para a conclusão dos trabalhos.

	sempre informações relevantes estarão disponíveis rapidamente e com um grau de certeza mais elevado para constarem na comunicação imediata. Mas, de qualquer forma, a ANPD deve esclarecer perfeitamente quais casos podem contar com essas duas fases de comunicação — parcial e completa —, de forma a não incentivar a utilização da comunicação parcial como regra para todos os casos de incidente. Além disso, o prazo deve ser passível de flexibilização, a depender das justificativas apresentadas pela organização na comunicação. Outra solução possível apoiada pelo LAPIN é a definição de **prazos diferenciados,** talvez mais flexíveis, para determinados controladores. Alguns dos critérios que podem ser utilizados são: (i) a composição ou tamanho do controlador (relação com o tratamento diferenciado para PMEs) e (ii) o tratamento de dados ser atividade fundamental à organização. De qualquer forma, é muito importante a **adoção de uma forma de comunicação online,** que funcione ininterruptamente, para que os prazos sejam contados de forma corrida. Um prazo definido em dias úteis[24] pode causar mais demora no processo de comunicação do incidente já que não se consideram sábados, domingos e feriados. A celeridade na comunicação do incidente de segurança envolvendo dados pessoais garante uma tutela mais efetiva aos direitos dos titulares. Nesse sentido, ressaltamos que o sistema SEI não traz funcionalidades suficientes para garantir a agilidade que esse processo requer. A ANPD ainda deverá considerar formas de retorno do prazo em situações de instabilidade de seu próprio sistema ou por qualquer limitação imposta pelo próprio processo de comunicação (por exemplo: demora em conceder acesso ao SEI). Além disso, o LAPIN incentiva a adoção de outros meios de

[24] Como o da Lei do Cadastro Positivo, mencionado na Nota Técnica nº 3/2021/CGN/ANPD, que é de dois dias úteis a partir da data do conhecimento do incidente.

	comunicação que não dependam da utilização dos canais do SEI, principalmente para os titulares, como algum local para denúncias diretas no site. Ainda deve-se levar em conta que o descumprimento não justificado dos prazos definidos poderá impactar na aplicação, pela ANPD, dos critérios de definição de sanções administrativas previstos no parágrafo primeiro do artigo 52 da LGPD no caso concreto.
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	Em relação ao prazo para que os controladores informem os titulares de dados sobre o incidente de segurança, sugerimos que seja o mesmo para a ANPD, ou seja, de 10 dias, contados a partir da comunicação parcial. No entanto, recomendamos que a ANPD seja comunicada primeiro nos casos envolvendo dados sensíveis, para que a Autoridade eventualmente forneça orientações mais específicas ao caso concreto. A comunicação com o titular deve conter as informações listadas no §1º do artigo 48 da LGPD, mas essas informações devem ser apresentadas de forma simplificada e em linguagem acessível, de modo a não constarem informações excessivas que tornem o processo de compreensão do incidente extremamente complexo. Como referência, o site do OAG[25] da Califórnia conta com vários exemplos interessantes de comunicação ao titular. Além dos pontos já elencados, o controlador também deve informar quais precauções o titular deve tomar para evitar golpes ou fraudes ou qualquer outro risco oriundo do incidente e qual o contato do encarregado ou equivalente para esclarecimentos adicionais. Tais informações, inclusive, devem ser fornecidas de forma imediata, ainda dentro do prazo para comunicação parcial, preferencialmente. Também pode ser interessante a menção aos dados que **não** foram afetados pelo incidente para o titular ter real controle dos seus dados. Em suma, as

[25] Office of the Attorney General. Disponível em: <https://oag.ca.gov/privacy/databreach/list>. Acesso em 22 mar. 2021.

	informações a serem fornecidas ao titular devem ser aquelas essenciais para o exercício dos direitos previstos na LGPD e para compreensão do risco envolvido no incidente. Além disso, ao se considerar os custos relacionados à comunicação individual e direta, uma forma de atender a essa necessidade de comunicação direta é o envio de mensagens padronizadas simplificadas para os titulares**,** mas com direcionamentos caso o indivíduo queira maiores informações sobre o incidente. Para que esse tipo de comunicação seja suficiente para cumprir os critérios legais, é necessário que a organização disponibilize informes mais detalhados sobre o incidente, além de disponibilizar um sistema de respostas aos direitos do titular adequado (como em uma página facilmente acessível de perguntas frequentes), considerando que em um momento pós-incidente o número de requisições deve aumentar consideravelmente (seria o caso, p. ex., de envio de link que redireciona para página que possibilita o exercício de direitos do titular). Por fim, o LAPIN acredita que devem constar as seguintes informações na comunicação de incidentes de segurança aos titulares de dados[26]: ● Informações elencadas no §1º do art. 48, apresentadas **maneira de simplificada e em linguagem acessível**; ● Indicações de quais **medidas podem ser tomadas para mitigar riscos** (como evitar golpes ou fraudes, ou qualquer outro risco oriundo do incidente); ● O **contato do encarregado** ou equivalente para esclarecimentos adicionais;

[26] Essas indicações são próximas das recomendações trazidas pela Autoridade Australiana, que defende que a comunicação ao titular deve incluir: (i) o nome e as informações de contato da entidade controladora; (ii) as categorias de dados pessoais envolvidos no incidente; (iii) uma descrição do incidente; e (iv) recomendações de medidas que podem ser adotadas pelo titular como resposta ao incidente. Disponível em: <https://www.oaic.gov.au/privacy/data-breaches/what-is-a-notifiable-data-breach/>. Acesso em 23 mar. 2021.

	• Quando cabível, informações sobre os **dados que <u>não</u> foram afetados** pelo incidente; e • Para comunicações simplificadas, incluir o **canal disponibilizado pela organização** para fornecimento de detalhes adicionais sobre o incidente de segurança.
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	A forma mais adequada de comunicação de incidentes entre a organização e o titular seria comunicação direta e individual, principalmente através de e-mails, SMS ou até mensagem de WhatsApp[27]. A escolha do meio deve manter a expectativa de relacionamento já estabelecido com aquele titular. Ou seja, se o titular fez o cadastro ou mantém comunicação com o controlador via e-mail, a comunicação deve ser feita por e-mail; agora, se a organização já dialoga por WhatsApp com aquele titular, pode escolher esse meio para informar o indivíduo do incidente ocorrido. O importante é garantir um meio hábil para informar o titular sobre quais medidas de segurança ele deve tomar e quais dados pessoais foram afetados e quais não foram. Dessa forma, há certo empoderamento do titular, impedindo que ele se coloque em maior risco através de qualquer atitude precipitada e movida pelo medo, insegurança ou falta de informação. Essa orientação veio da experiência dos megavazamentos que ocorreram nos últimos meses no Brasil, quando foram proliferados sites que supostamente ajudariam o titular, mas que na realidade coletavam mais dados, e o titular não conseguia diferenciar qual site tinha qual finalidade. Por isso, e até aproveitando da prática consumerista, o LAPIN acredita que a comunicação pública voltada para a conscientização deve ser incentivada em mais casos, visando o incentivo à cultura de privacidade, a observância do princípio da autodeterminação informativa, devendo ser considerada inclusive como uma prática

[27] Nesse sentido, temos a experiência da adoção de uso de WhatsApp para intimação em algumas jurisdições no Brasil, como a Justiça Federal de Pernambuco ou, ainda, o TJDFT. Disponível em: <https://www.cnj.jus.br/uso-de-whatsapp-para-intimacao-e-regulado-na-justica-federal-de-pe/> e <https://www.tjdft.jus.br/institucional/imprensa/destaques/intimacoes-por-whatsapp>. Acesso 22 mar. 2021.

	para mitigação de danos. Mesmo nos casos em que a comunicação à ANPD e aos indivíduos não seja obrigatória, a comunicação pública deve ser considerada como uma boa prática, inclusive mediante anúncios publicitários como disposto no art. 10 do Código de Defesa do Consumidor. Além disso, o LAPIN entende que a comunicação pública também poderá ser admitida em determinadas circunstâncias, como nos casos em que a comunicação direta possa gerar um esforço desproporcional à organização ou quando o controlador não possuir informações individualizadas de contato dos titulares de dados afetados.

Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	Sugere-se como exceção para a obrigação de comunicação do incidente à ANPD a situação em que não houver risco ou dano, ou quando o risco for baixo. Isso dependerá dos critérios definidos pela ANPD para a gradação de risco, porém em alguns casos o baixo risco é notório. Para melhor exemplificar tal exceção[28]: um agente de insolvência de dívida enviou por e-mail o arquivo de um novo cliente por engano para um colega em um departamento diferente. O arquivo continha uma lista das dívidas pendentes do cliente, seus detalhes de contato, histórico financeiro básico, informações sobre sua saúde mental e motivos para buscar apoio para sua situação financeira. A organização considera o cliente vulnerável devido ao seu estado mental. O colega que recebeu o arquivo imediatamente apagou o e-mail e informou ao remetente o erro. Nesse caso, apesar de haver o compartilhamento de dados sensíveis para um remetente incorreto, foi realizado para um funcionário da mesma organização e, portanto, sujeito às mesmas políticas de governança de dados, o que reduz o risco significativamente. Ademais, o recipiente do e-mail o deletou e informou ao remetente sobre o erro, possibilitando ações corretivas.
Quais seriam as possíveis exceções da	Não é qualquer tipo de incidente de segurança que deve ser comunicado aos titulares de forma obrigatória. Deve existir uma análise de risco prévia por parte do controlador, de modo que não haja um excesso de comunicações enviadas aos titulares de dados, de forma a causar fadiga. Não há como existir a presunção de risco

[28] Disponível em: <https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-breach-examples/>. Acesso em 15 mar. 2021.

obrigatoriedade de informar os titulares?	ou dano relevante em todos os incidentes de segurança. Contudo, é relevante que haja critérios para que as comunicações gerem, inclusive, consequências educacionais. Sugere-se que não haja a obrigatoriedade de comunicação do incidente de segurança ao titular quando o risco for baixo ou médio combinado à não ocorrência de dano. Por outro lado, deve haver a obrigatoriedade da comunicação nos casos em que haja a ocorrência de dano ou alto ou alarmante risco. Após a comunicação à ANPD, eventual comunicação ao titular poderá ser recomendada ou determinada pela própria ANPD, caso se entenda pela não obrigatoriedade de comunicar aos titulares automaticamente. De qualquer modo, somente deve haver comunicação ao titular quando este deva se prevenir ou tomar ações para mitigar risco ou dano que possa ser ocasionado em razão do incidente, ou seja, nos casos em que haja a ocorrência de dano ou alto risco.
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	A gravidade do incidente deverá ser avaliada tanto pelo controlador, antes da comunicação, quanto pela autoridade, após o processo de comunicação. Essa resposta trará um enfoque para a avaliação realizada pela ANPD, que inclusive poderá contar com a análise dos registros, relatórios e avaliações do controlador. Durante o processo de adequação, o controlador deve ter definido quem será responsável por administrar o procedimento relacionado ao incidente de segurança, incluindo a avaliação da gravidade. Sugere-se que a

	responsabilidade seja direcionada para o encarregado ou equivalente (podendo ser uma única pessoa ou um time)[29]. Essa definição auxiliará o diálogo com a ANPD[30]. Como já mencionado, a análise do risco perpassa a avaliação da gravidade do incidente, havendo relação de proporcionalidade entre esses conceitos - quanto maior a gravidade dos riscos do incidente, maior o risco em si e vice e versa. Mas, especificamente, a gravidade representa a magnitude do risco, se relacionando diretamente à natureza das possíveis consequências do incidente. Com isso em mente, o LAPIN entende que os seguintes critérios devem fazer parte da análise de gravidade do incidente de segurança por parte da ANPD, além daqueles que são considerados na análise dos riscos[31]: ● A **impossibilidade de reversão do incidente** (p. ex., se os dados forem alterados, não existir forma de atualização, ou se eles forem excluídos e não existir backup); ● A adoção de medidas de segurança da informação e de boas práticas **antes do incidente** (p. ex.: utilização de *softwares* certificados, utilização de tipos de criptografia, ter realizado um processo de adequação etc.), como mencionado no art. 46 e 50 da LGPD; ● Se agentes não autorizados têm acesso aos dados; ● O **contexto da ameaça** - origem externa ou interna;

[29] Esse é o direcionamento dado pelo Information Commissioner's Office - ICO - na página sobre "personal data breaches". Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/>. Acesso em 16 mar. 2021.

[30] Sobre o tema, ver o relatório produzido pelo *Global Privacy Enforcement Network* (GPEN), disponível em: <privacy.org.nz/publications/statements-media-releases/gpen-sweep-finds-significant-awareness-of-managing-data-breaches-concerns-regarding-low-engagement/>. Acesso em 23 mar. 2021. Apesar da baixa adesão das empresas em participar respondendo o questionário, 84% (oitenta e quatro por cento) das entidades participantes haviam apontado time ou grupo responsável pelo gerenciamento de incidentes de segurança.

[31] Esses critérios também deverão ser considerados na análise de gravidade.

	• As **regiões** afetadas, levando em consideração se há possibilidade de consequências em outros países; ○ Se houver alguma possibilidade de consequência transfronteiriça, avaliar se tais jurisdições contam com um sistema de proteção de dados equivalente; • As medidas de **mitigação de dano** que serão adotadas no momento pós-incidente (ver as indicações sobre comunicação com o titular); • Se a organização irá adotar alguma forma de **comunicação aos titulares** (seja a comunicação direta ou alguma campanha de conscientização mais relacionada à mitigação dos danos); • O **impacto aos direitos e liberdades** do titular; e • A **facilidade de identificação dos indivíduos**.
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	A gravidade do incidente está diretamente relacionada com os riscos oriundos desse fato. A gravidade do incidente depende das consequências negativas que podem surgir desse fato, sejam potenciais ou efetivas, sejam consequências físicas, materiais ou imateriais, individuais ou coletivas[32]. Como disposto pela autoridade francesa, o nível de risco é mensurado a partir da gravidade e da probabilidade de concretização desse risco e a gravidade representa a magnitude do risco, se relacionando diretamente à natureza dos potenciais impactos[33].

[32] Article 29 Working Party. **Guidelines on Personal data breach notification under Regulation 2016/679.** Disponível em: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052>. Acesso em 16 mar. 2021.
[33] COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS (CNIL). **Privacy Impact Assessment (PIA) methodology**. Disponível em: <https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-1-en-methodology.pdf> p. 6.. Acesso em 16 mar. 2021.

Em relação à metodologia de análise da gravidade do incidente de segurança, a *European Union Agency for Network and Information Security* (ENISA)[34] propôs o seguinte modelo:

- **DPC x EI + CB = SE**
    - **DPC** (*data processing context*), que é a avaliação da sensibilidade dos dados em um contexto específico de tratamento de dados. Essa avaliação deve passar por 2 passos: (1) definição e classificação dos tipos de dados pessoais afetados; (2) ajustes a partir de fatores contextuais relacionados ao tratamento de dados pessoais. O *score* pode ser representado por 1, 2, 3 ou 4 (importante ressaltar que dados sensíveis começam com a classificação 4 e pode ter o valor minorado a partir da avaliação das circunstâncias concretas, ou dados financeiros começam com o valor 3 e também podem ter o *score* minorado ou majorado, o que demonstra a preocupação anterior relacionada a sensibilidade dos dados);
    - **EI** (*ease of identification*), que representa a facilidade de terceiro não autorizado acessar dados e conseguir identificar uma determinada pessoa. A classificação do EI segue critérios de relevância com atribuição de um valor para cada um, como se segue: insignificante (1); significante (2); e máximo (3). Para essa definição, também devem ser considerados fatores de majoração e de minoração.
        - **Fatores de majoração**: (i) o volume de dados afetados relacionados ao mesmo indivíduo; (ii) características específicas do controlador; e (iii) características específicas dos titulares afetados.

[34] ENISA. **Recommendations for a methodology of the assessment of severity of personal data breaches.** Disponível em: <https://www.enisa.europa.eu/publications/dbn-severity>. Acesso em 16 mar. 2021.

- **Fatores de minoração**: (i) invalidade/imprecisão dos dados afetados; (ii) disponibilização pública (considerar se os dados já eram públicos); e (iii) natureza dos dados afetados.

- **CB** (*circumstances of the breach*), que considera a perda de segurança (confidencialidade, integridade e disponibilidade) e intenção criminosa/ilícita. A partir dessa análise, a pontuação equivalente pode ser acrescentada de 0.25 ou 0.5, podendo alcançar valores representados por 0 a 2.

- **SE** (severity *of a data breach*) é o valor final alcançado, que representa a gravidade do incidente e segue a seguinte classificação:

Gravidade do incidente de segurança		
SE < 2	**Baixa**	Os titulares ou não serão afetados ou poderão encontrar alguns pequenos inconvenientes, os quais serão superados sem qualquer problema (tempo gasto reentrando informações, aborrecimentos, irritações etc.).
2 ≤ SE < 3	**Média**	Os titulares podem encontrar inconvenientes significativos, que eles podem superar apesar de algumas dificuldades (custos extras, dificuldade de acesso a serviços comerciais, medo, falta de compreensão, stress, doenças físicas não-graves etc.).
3 ≤ SE < 4	**Alta**	Os titulares podem encontrar consequências significativas, as quais são passíveis de superação, embora com sérias dificuldades (apropriação indevida de fundos, scores de crédito negativos, danos materiais, perda de emprego,intimação, agravamento da saúde etc.).
4 ≤ SE	**Muito alta**	Os titulares podem se deparar com consequências significativas, ou mesmo irreversíveis, que não podem ser superadas (dificuldades financeiras, tais como dívida substancial ou incapacidade de trabalhar, doenças físicas e psicológicas graves, morte etc.).

Já a *Advisera*, companhia especializada em normas ISO de segurança da informação, através de publicação da *EU GDPR Academy*[35], propôs o seguinte modelo metodológico (aproximando-se de uma versão simplificada do modelo apresentado pela ENISA):

- **DPC x EI + CB = SE**
    - **DPC** (*data processing context*) é a avaliação da sensibilidade dos dados em um contexto específico de tratamento de dados e pode ser representado por 1, 2 ou 3, a depender da categoria dos dados pessoais envolvidos no incidente. Se o incidente só envolve dados não sensíveis, o **DPC deve ser igual a 1**. Se o incidente só afeta dados não sensíveis, mas os dados podem ser utilizados para compreensão do perfil dos titulares de dados afetados, o **DPC deve ser igual a 2**. Agora, se o incidente envolve dados sensíveis, **o DPC deve ser igual a 3**.
    - **EI** (*ease of identification*) reflete a facilidade de identificação dos titulares; ou seja, o EI avalia quão fácil será para uma parte não autorizada, mas com acesso aos dados afetados, identificar os titulares. O EI pode ser representado por 1 ou 2, a depender do tipo de criptografia utilizado para proteção dos dados pessoais. Se os dados pessoais afetados forem protegidos por um tipo de criptografia forte (como AES, RSA, Twofish etc.), dificultando a identificação dos titulares, o **EI deve ser igual a 1.** Em compensação, se as informações sobre o titular estão dispostas de modo compreensível e possibilitam a identificação de um titular específico, o **EI deve ser igual a 2**.

[35] ADVISERA. **Assessing the severity of personal data breaches according to GDPR.** Disponível em: <https://info.advisera.com/eugdpracademy/free-download/assessing-the-severity-of-personal-data-breaches-according-to-gdpr>. Acesso em 16 mar. 2021.

	○ **CB** (*circumstances of breach*) trata da avaliação das circunstâncias do incidente, considerando o tipo de incidente, a perda de segurança e controle dos dados afetados e qualquer intenção maliciosa (criminosa, danosa, ilícita) envolvida no incidente. O **CB deve ser igual a 1** se: (i) os dados são vazados para agentes não autorizados, mas conhecidos/identificados; (ii) os dados pessoais são alterados e utilizados incorretamente ou ilegalmente, mas tais alterações podem ser revertidas; ou (iii) o acesso aos dados foi perdido, mas os dados podem ser restaurados. Contudo, o **CB deve ser igual a 2** nas seguintes situações: (i) os dados são vazados para agentes não identificados; (ii) os dados pessoais são alterados ou utilizados de forma incorreta ou ilegal e tais alterações não podem ser restauradas; (iii) o acesso foi perdido e os dados não podem ser restaurados; ou (iv) o incidente foi causado por comportamento malicioso que afeta os titulares. No cálculo, somente uma circunstância deverá ser tomada em consideração, ou seja, o **CB será sempre igual a 1 ou a 2**. ● **SE** é a gravidade do incidente. ○ Se o resultado final for menor ou igual a 3 (**SE igual ou menor a 3**), o incidente provavelmente não causará riscos ao titular. Assim, tal incidente só deveria ser registrado, não sendo obrigatória a comunicação. ○ Quando o **SE for igual a 4,** é provável que o incidente resulte em algum risco relevante para o titular. Dessa forma, o incidente deve ser reportado para a Autoridade competente. ○ Nos casos em que o **SE for igual ou maior a 5,** existe uma alta probabilidade de riscos para o titular. Por isso, o incidente deve ser notificado para a Autoridade competente e para os titulares afetados.

	O *Information Commissioner's Office* (ICO)[36] disponibiliza um teste para definição da gravidade do incidente para compreender se esse fato deve ou não ser notificado ao ICO. As perguntas do teste, em tradução livre, são as seguintes: ● Uma violação de dados pessoais pode ser definida amplamente como um incidente de segurança que tenha afetado a confidencialidade, integridade ou disponibilidade de dados pessoais. Você já determinou se ocorreu uma violação de dados pessoais? ● Fazendo sua própria avaliação, a violação envolve os dados pessoais de indivíduos vivos? ● Após sua própria avaliação, é provável que haja um alto risco para os direitos e liberdades individuais? ○ Nesse ponto, você precisará avaliar tanto a gravidade do impacto potencial ou real sobre os indivíduos como resultado de uma violação e a probabilidade de que isso ocorra. Se o impacto da violação for mais severo, o risco é maior; se a probabilidade das consequências for maior, então novamente o risco é maior. O WP29 diz que "Este risco existe quando a infração pode levar a danos físicos, materiais ou não materiais para as pessoas cujos dados foram violados" e essa definição deve ser considerada. Para ajudá-lo a avaliar a gravidade de uma violação, foram selecionados exemplos retirados de várias violações relatadas à ICO[37]. Estes também incluem conselhos úteis sobre os próximos passos a serem tomados ou coisas a serem pensadas. Este link será aberto em uma nova guia do navegador.

[36] Disponível em: <https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach-assessment/>. Acesso em 16 mar. 2021.
[37] Documento disponível em: <https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-breach-examples/>. Acesso em 16 mar. 2021.

	● Se você diz sim a todas as perguntas do ICO, você recebe a seguinte orientação[38]: ○ É preciso dizer às pessoas afetadas pela violação sem demora. Você deve informá-las sobre quaisquer medidas que esteja tomando para mitigar os efeitos da violação e dar-lhes conselhos sobre o que fazer para se protegerem; Como você fez uma avaliação, é provável que haja um risco elevado, então você também deve notificar a ICO. Isto deve ser feito dentro de 72 horas após tomar conhecimento da infração. Você pode ligar para nossa Linha de Ajuda[39] para obter orientação sobre como administrar a violação, mitigar o efeito da violação e relatar a violação. A menos que você não possa acessar seu sistema, você deve reportar incidentes cibernéticos online[40]. Alternativamente, se você estiver confiante de que está gerenciando os efeitos da violação e não precisar de aconselhamento, você pode relatar os detalhes da violação on-line. As metodologias apresentadas são adequadas, já que apresentam critérios objetivos a serem considerados. Como é um processo que depende da atuação do controlador, a adoção de metodologias simples e objetivas é positiva e incentivada. Além disso, os modelos metodológicos levam em consideração questões de suma importância, como o contexto do tratamento de dados que foi afetado pelo incidente; a facilidade de identificação de determinado indivíduo, o que se relaciona com a probabilidade de dano; e, ainda, as circunstâncias do incidente. Esse processo ainda avaliará a categoria dos dados afetados e as características dos titulares afetados, o que representa uma síntese das propostas oferecidas pelo LAPIN nessa tomada de subsídios.

[38] Tradução livre.
[39] Iniciativas como essa, um SAC para sanar dúvidas, também podem ser adotadas pela ANPD para aprimorar o procedimento de comunicação.
[40] Essa preferência pelo procedimento e processo eletrônico também é positiva, gera menos burocracia e menos gastos.

	Sugere-se a adoção de critérios semelhantes aos adotados internacionalmente para facilitar o *enforcement* da LGPD tendo em vista o contexto de grande fluxo transnacional de dados. Para facilitar a compreensão de tais modelos, devem ser disponibilizados questionários como o oferecido pelo ICO na página da ANPD.
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	Uma forma interessante de atuação da ANPD é a consideração de que o incidente de segurança se relaciona diretamente com a segurança da informação (necessária a observância e reforço do princípio da segurança, previsto no art. 6º, VII, LGPD). Por isso, é possível aproveitar desse momento para garantir que novos incidentes não ocorram. Para entender qual seriam as melhores indicações por parte da ANPD, trazemos algumas experiências internacionais, que podem ser adotadas pela Autoridade. *Agencia Española de Protección de Datos Personales* recomenda[41] (essas medidas não ajudam necessariamente a mitigar ou reverter os efeitos do incidente, mas podem servir de inspiração para atitudes imediatas que o controlador poderá tomar): ● Uso de senhas seguras (incluindo o estabelecimento de política de senhas) e autenticação de dois fatores; ● Adoção de cópias de backup; ● Ter sistemas sempre atualizados, tanto o sistema operacional de equipamentos de trabalho e servidores, quanto programas utilizados em dispositivos. Além disso, deve ser estabelecida uma rotina de atualizações frequentes que seja documentada e rastreável; ● Adoção de política rígida dos serviços expostos na Internet. Da mesma forma, os acessos remotos devem sempre ocorrer por meio de sistemas VPN, proxy reverso ou medidas igualmente eficazes; e

[41] Disponível em: <https://www.aepd.es/en/prensa-y-comunicacion/blog/breaches-top-5-measures>. Acesso em 23 mar. 2021.

	• Tornar obrigatória a criptografia, pelo menos para dispositivos portáteis, que podem ser facilmente perdidos ou roubados, e levar em consideração a minimização de dados nos dispositivos. Já o ICO recomenda as seguintes medidas adicionais[42]: • Condução de treinamento obrigatório sobre proteção de dados; • Atualização de políticas e procedimentos e desenvolvimento de uma cultura de confiança para que os funcionários se sintam capazes de relatar casos de falhas de segurança; • Adoção interna do princípio "verificar duas vezes, enviar uma vez"; • Implementação de restrição de acesso a sistemas; • Desativação do preenchimento automático. **Outros endereçamentos possíveis e indicados pelo LAPIN são:** • Organização de uma equipe de resposta especializada que possa conter a violação, identificar e remover as vulnerabilidades; • Remoção imediata de conteúdo exposto de maneira indevida; • Proteção da área física e dos sistemas (tanto para conter o incidente quanto para fins de inspeção posterior); • Condução de investigação imediata junto ao funcionário que deu causa ao incidente; • Estabelecimento de canal de suporte aos titulares afetados para ajudá-los na redefinição de senhas; • Revisão dos softwares e programas utilizados internamente, impondo a utilização de programas com reconhecimento de segurança; e

[42] Disponivel em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/>. Acesso em 22 mar. 2021.

	• Acordos de prevenção (motivando novo processo de *compliance* para evitar novos incidentes).

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: LGPD Acadêmico – representado por Angela Maria Rosso, Marcia Muniz, Remilina Yun, Fernanda Maia, Marcel Leonardi

CPF/CNPJ: [redacted]

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS **IMPORTANTE:** Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	Compreender quando um incidente pode acarretar risco ou dano relevante implica avaliar uma série de fatores que envolvem o contexto em que o evento ocorreu. Nesse sentido, o *European Data Protection Board* (EDPB), ao se posicionar sobre o tema, orienta que para analisar o impacto de um incidente para o titular de dados sejam considerados os seguintes critérios: a) O tipo do incidente e em qual nível ele pode afetar o indivíduo; b) A natureza, sensibilidade e o volume dos dados pessoais envolvidos; c) Facilidade com que os indivíduos podem ser identificados; d) Gravidade das consequências para o titular de dados; e) Características especiais do titular de dados; f) Características especiais do controlador; e g) O número de indivíduos afetados. A adoção dos critérios acima permitiria que tanto a ANPD quanto o controlador que sofreu o incidente conheçam a gravidade do evento. Desta forma teriam a capacidade de determinar qual a probabilidade de dano aos titulares e qual a extensão do dano que pode vir a ser causado aos titulares de dados atingidos. Além dos fatores mencionados, a boa prática no tratamento de incidentes sugere que podem ser acrescentados à lista os seguintes pontos de análise: a) Se o incidente foi interno ou externo; b) Nível de confidencialidade dos dados violados; e c) Efetividade da contenção do incidente.

<table>
<tr><td></td><td>Referência: European Data Protection Board. Guideline on Personal data breach notification under Regulation 2016/679. Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052.</td></tr>
<tr><td>O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc.)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?</td><td>O framework NIST 800 - 37 define que o nível de risco é obtido em função da probabilidade da ocorrência de um evento adverso e o impacto proveniente desta ocorrência, permitindo assim, que se subdivida o risco em níveis. Padronizar os itens que compõem essa função (probabilidade x impacto) é algo recomendável.

A European Union Agency for Cybersecurity (ENISA) apresenta uma metodologia para encontrar o nível de risco envolvido em um incidente de segurança de dados. A metodologia utilizatrês critérios base que permite calcular a gravidade do incidente.

As variáveis são as seguintes:
(1) Contexto do tratamento de dados pessoais – que considera o tipo do incidente e outras características contextuais do evento;
(2) A facilidade de identificação do indivíduo cujos dados foram violados pelo incidente; e
(3) Circunstâncias do incidente, composta por questões de segurança da informação envolvidas na ocorrência do incidente.

Resumidamente, a metodologia apresentada, permite que a partir dessas variáveis na fórmula: Gravidade = Contexto do tratamento de dados x Facilidade de identificação + Circunstâncias do incidente é possível obter o valor da Gravidade, que é uma forma de atribuir um valor para o risco dentre os níveis baixo, médio, alto e muito alto calculado para o incidente de segurança de dados que ocorreu.

Para aplicar a fórmula é preciso que as variáveis Contexto do tratamento de dados, Facilidade de Identificação e Circunstâncias do incidente tenham seus valores conhecidos previamente. Isso é possível a partir da criação de tabelas de referência em que se atribuem scores à situações específicas para serem utilizadas nessas situações.

Utilizando o modelo descrito, é possível criar uma tabela de scores da seguinte maneira:

<table>
<tr><td>Gravidade < 2</td><td>Baixo</td><td>Indivíduos não seriam afetados ou enfrentariam poucas inconveniências.</td></tr>
</table>
</td></tr>
</table>

<table>
<tr>
<td></td>
<td>
<table>
<tr><td>2<=gravidade<3</td><td>Médio</td><td>Indivíduos podem ter problemas significantes</td></tr>
<tr><td>3<=gravidade<4</td><td>Alto</td><td>Indivíduos podem enfrentar problemas significantes e dificuldades sérias.</td></tr>
<tr><td>4<=gravidade</td><td>Alto Risco</td><td>Indivíduos podem enfrentar problemas irreversíveis.</td></tr>
</table>

Adotando essa metodologia, riscos baixos, com baixa probabilidade de dano, não seriam considerados relevantes.

Referências: NIST 800-37r2. Disponível em: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

Recomendations for a methodology of the assessment of severity of personal data breaches Disponível em: https://www.enisa.europa.eu/publications/dbn-severity
</td>
</tr>
<tr>
<td>Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?</td>
<td>
O framework NIST 800-37 define o risco como a medida em que uma entidade é ameaçada por uma circunstância ou evento potencial.

No contexto do Código Civil brasileiro dano é toda lesão que causa prejuízo.

Assim, risco e dano, no contexto de incidentes de segurança de dados, são conceitos que se complementam, mas não se confundem. Enquanto o risco representa a probabilidade de o dano ocorrer, o dano representa a consequência da concretização do risco.

O Information Comissioner's Office (ICO) define que os riscos relativos à privacidade se relacionam à exposição ou utilização indevida dos dados pessoais do titular de dados. O risco é a probabilidade potencial de ocorrência de consequências negativas para o titular caso seus dados tenham a segurança violada. Já o dano é a consequência da exposição indevida. Dessa forma, a existência do risco não implica necessariamente na existência do dano.

Os critérios para avaliação do risco devem considerar o potencial de dano que o incidente pode vir a causar ao titular do dado. Entre os danos possíveis, existem os danos morais, materiais e/ou físicos.
</td>
</tr>
</table>

	As consequências de um incidente de segurança de dados pessoais, que seria o dano, podem ser, portanto, mas não se resumem a: perda do controle dos dados pessoais, limitação ao exercício de direitos, discriminação, roubo de identidade ou fraude, perdas financeiras, danos reputacionais ou ainda outras desvantagens econômicas ou sociais que possam causar preocupações aos indivíduos. **Referência:** NIST 800-37r2. Disponível em: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf *Personal data breaches.* Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/
O que deve ser considerado na avaliação dos riscos do incidente?	Avaliar as consequências de um incidente exige considerar todos os fatores contextuais do evento. A ICO, por exemplo, orienta que na avaliação dos riscos do incidente deve-se levar em consideração as possíveis consequências do evento. Isso significa identificar como e em que grau o incidente pode afetar os indivíduos envolvidos e qual a probabilidade dessas consequências acontecerem. O EDPB ao se posicionar sobre o tema, orienta que se considerem os seguintes critérios: a) O tipo do incidente e em qual nível ele pode afetar o indivíduo; b) A natureza, sensibilidade e o volume dos dados pessoais envolvidos. Nesse ponto atenção especial deve ser dada para incidentes que envolvam dados sensíveis nos termos da lei. Em regra, quanto maior a sensibilidade do dado, maior o dano que sua exposição indevida pode causar ao titular dos dados. Nesse ponto, também é preciso avaliar o contexto da violação, quanto mais informações sobre o mesmo titular forem expostas, maior o risco do dano se concretizar e também maior o risco de ser um dano relevante; c) Facilidade com que os indivíduos podem ser identificados. Existe diferença no impacto causado por um incidente envolvendo dados criptografados e incidentes envolvendo dados em texto plano. No primeiro caso certamente a probabilidade de que haja dano ao titular do dado é menor do que no segundo caso; d) Gravidade das consequências para o titular de dados. Quando um incidente envolver a exposição indevida de dados pessoais que possam resultar em roubo de identidade ou fraude, em riscos à integridade física ou psíquica, humilhação ou prejuízo à reputação a probabilidade de dano será alta e se o dano se concretizar será grave, logo impactará na valoração do risco, atingindo um grau muitas vezes catastrófico. Ainda na análise desse critério deve-se incluir a temporalidade do dano.

	Dadas as características do meio digital em que grande parte dos incidentes acontecem, o dano poderia perpetuar-se no tempo tornando-o mais grave; e) Características especiais do titular de dados. Outro fator que contribui para a gravidade do incidente é o envolvimento de indivíduos vulneráveis. No Brasil, por força da própria LGPD e do Estatuto da Criança e do Adolescente fariam parte desse grupo crianças e adolescentes. f) Características especiais do controlador. A própria natureza do negócio que exige o tratamento de dados pessoais interfere na análise do risco de o incidente causar um dano relevante. Negócios que atuam de forma preponderante com dados sensíveis por si só já tem um nível de risco elevado; e g) O número de indivíduos afetados. Esse critério tem influência relativa na construção do valor do risco. Obviamente, incidentes envolvendo um grande número de indivíduos gera a desconfiança de que o dano será automaticamente relevante. Entretanto, pequenos incidentes com dados especialmente sensíveis podem causar impactos catastróficos na vida dos titulares de dados atingidos. Nesse caso, é preciso ponderar em conjunto, a natureza dos dados expostos e o contexto em que o incidente ocorreu. A análise de todos esses critérios possibilitará visualizar o contexto em que o evento ocorreu, tornando mais assertiva a abordagem na contenção ou mesmo mitigação dos danos provenientes do evento. **Referência:** EDPB - Guideline on Personal data breach notification under Regulation 2016/679. Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052.
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	A boa prática da gestão de incidentes indica que além das informações listadas no art. 48, §1º da LGPD poderiam subsidiar a ANPD saber: a) Qual o tipo do incidente; b) Quais características do incidente: violação da confidencialidade, da disponibilidade ou da integridade dos dados. Essas informações auxiliariam a ANPD na análise do contexto em que o incidente ocorreu e também sobre a sua gravidade.
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	O prazo de 72 horas nos parece razoável para o primeiro comunicado para a ANPD, desde que efetivamente compreendido o que ocorreu e suas consequências. Analisando a legislação comparada, temos que Regulamento Europeu e a Lei do Uruguai preveem 72 horas após o conhecimento do evento de violação de segurança dos dados como prazo para realização do comunicado. Regulamento Europeu - https://gdpr-info.eu/

	Lei do Uruguai - https://www.impo.com.uy/bases/leyes/18331-2008/29
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	Idealmente a comunicação aos titulares deve ser realizada somente após a confirmação de três condições: a) o incidente envolveu dados pessoais; b) o incidente representa realmente um risco relevante ou um dano relevante; e c) após a correta identificação de quem são os indivíduos atingidos. Não há um prazo exato para que se consiga levantar essas informações, prevalece o entendimento de que a comunicação deve ser feita o mais brevemente possível, sem atrasos injustificados. Em relação ao comunicado para os titulares ele deve conter: a) Indicação da data que a empresa teve conhecimento da ocorrência do incidente; b) Se o incidente ocorreu no ambiente do controlador ou em um parceiro; c) Uma breve narrativa da ocorrência contemplando o tipo do incidente e quem são os titulares atingidos; d) Medidas que foram tomadas para solucionar ou mitigar as consequências do incidente; e) Quais dados foram afetados; f) Quais os riscos concretos para o titular dos dados pessoais e qual a gravidade do risco; g) Eventuais medidas adotadas para mitigar os possíveis prejuízos para o titular dos dados; h) Orientações sobre medidas que o titular pode adotar para evitar maiores prejuízos; e i) Dados de contato para que o titular possa obter maiores informações. O conteúdo sugerido para o comunicado é mais completo do que aquele adotado no contexto do Regulamento Europeu. O *Guideline on Personal data breach notification under Regulation* 2016/679 do EDPB orienta que a comunicação aos titulares dos dados pessoais deve minimamente conter as seguintes informações: a) Descrição da natureza do incidente; b) O nome e o contato do DPO/ Encarregado ou outro contato; c) A descrição das consequências do incidente; e d) A descrição das medidas tomadas ou propostas pelo controlador para resolver o incidente e mitigar efeitos adversos, se necessário.

	Entendemos que informações mais detalhadas possibilitam aos titulares compreender melhor o alcance do incidente e quais medidas podem tomar para saber mais sobre o evento bem como para mitigar consequências derivadas do incidente. **Referência:** European Data Protection Board. Guideline on Personal data breach notification under Regulation 2016/679. Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052.
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	A modalidade de comunicação a ser adotada depende do contexto que envolve o incidente. Incidentes com um alto nível de gravidade (probabilidade de dano alta ou muito alta) devem ser comunicados diretamente aos titulares por canais que permitam esse contato, como o e-mail, por exemplo. Entretanto, quando o incidente envolver um grande número de pessoas e o risco de dano envolvido não for alto ou muito alto, pode ser feito divulgado via comunicação pública. É necessário ainda considerar o nível de esforço que a organização terá que realizar para comunicar o incidente aos titulares de dados, para não inviabilizar o próprio negócio. Não faz sentido, por exemplo, ter de obter dados pessoais complementares para fazer a notificação.
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	O *Guideline on Personal data breach notification under Regulation* 2016/679 do EPDB orienta que a notificação das autoridades supervisoras não seria necessária nas seguintes situações: a) Quando o incidente não resultar em risco para os direitos e liberdades dos titulares de dados pessoais; e b) Quando os dados estiverem em formatos ininteligíveis para partes não autorizadas. Seguindo esse entendimento, incidentes envolvendo dados pessoais já disponíveis publicamente em listas públicas não exigiriam notificação para a ANPD bem como a exposição de dados criptografados sem que a chave de segurança tenha sido violada também não devem ser notificados. Acrescente-se a isso situações de incidente internos, como por exemplo, acessos indevidos, por eventuais falhas no controle de acessos, envolvendo os próprios colaboradores da organização, por ocorrerem em ambiente restrito e com baixo potencial de dano ao titular dos dados pessoais também não mereceriam ser notificados para a ANPD. **Referência:** Guideline on Personal data breach notification under Regulation 2016/679 - EDPB. Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052.

Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	O Guideline on Personal data breach notification under Regulation 2016/679 do EPDB orienta que a comunicação aos titulares dos dados não é necessária nas seguintes situações: a) Quando os dados expostos estão protegidos de tal forma que não podem ser lidos; b) Quando imediatamente após o incidente o controlador conseguiu mitigar o alto risco tornando improvável a ocorrência de danos ao titular dos dados; c) Quando o esforço a ser adotado para fazer o comunicado é desproporcional. No contexto da LGPD, faz sentido aplicar as mesmas exceções. Seria possível acrescentar à lista de exceções incidentes com baixo risco de dano aos titulares, como destacado anteriormente. **Referência:** Guideline on Personal data breach notification under Regulation 2016/679 - EDPB. Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052.
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	Para garantir o tratamento isonômico para todas as organizações, a ANPD deve adotar uma metodologia que permita compreender a probabilidade do dano aos titulares de dados pessoais atingidos pelo incidente. Nesse sentido, aplicar a metodologia adotada pela ENISA, anteriormente mencionada, utilizando as variáveis **Contexto do tratamento de dados, Facilidade de identificação e Circunstâncias do incidente** a partir de scores previamente determinados permite contemplar todos os fatores envolvidos no incidente. Inclusive se a organização adotava boas práticas de segurança da informação antes do evento ocorrer, fator contido na variável **Circunstâncias do incidente**.
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	ISO 27.000, em especial ISO/IEC 27035-1 — Information Security Incident management, onde há uma referência para priorização e categorização de incidentes de segurança da informação. Recommendations for a methodology of the assessment of severity of personal Data Breaches – The European Union Agency For Network and Information Security (ENISA). Disponível em: https://www.enisa.europa.eu/publications/dbn-severity.
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	O cabimento das medidas sempre dependerá da análise do cenário em que o incidente ocorreu. Incidentes internos, por exemplo, demandariam treinamentos de reciclagem em segurança da informação, enquanto incidentes externos demandariam realização de testes de vulnerabilidades. De toda forma, algumas medidas devem sempre ser implementadas após um incidente: a) Registro da ocorrência com todos os detalhes pertinentes; b) Monitoramento do ambiente para evitar novos incidentes; c) Treinamentos de segurança da informação e proteção de dados;

	d) Análise de segurança das tecnologias incorporadas ao negócio (hardware e softwares); e e) Revisão do plano de gestão de incidentes.
Outras considerações importantes:	O formulário para comunicação de incidentes abre a possibilidade do Operador realizar a notificação da ocorrência de um incidente ainda que o Controlador não tenha autorizado ou não tenha se mostrado negligente na comunicação. Entendemos que tal situação pode representar um risco para o Controlador, que em última instância é que quem assume o risco da atividade de tratamento realizada. No sistema europeu, há bastante clareza nos seguintes pontos: a) controladores é que têm a responsabilidade de decidir notificar, porque estão em posição de avaliar o risco do incidente em si; b) operadores devem se limitar a notificar controladores sobre incidentes, e não têm qualquer dever nem prerrogativa de fazer notificação direta à autoridade - pelo contrário, só podem fazê-lo se o contrato com o controlador assim permitir; c) operadores não têm qualquer responsabilidade se o controlador, recebendo o aviso do incidente, deixar de notificar a autoridade - não há espaço para imposição de responsabilidade subsidiária nesse cenário. As guidelines "*On personal data breach notification do WP29*", referendadas pelo EDPB, inclusive destacam que a única responsabilidade do Operador é comunicar ao Controlador quando o incidente ocorreu, no menor prazo possível, possibilitando que este tome as medidas que entender adequadas, inclusive, se necessário for, comunicar a autoridade supervisora. **Referência:** *On personal data breach notification do WP29* EDPB https://edps.europa.eu/sites/default/files/publication/18-12-14_edps_guidelines_data_breach_en.pdf (art. 54)
SUGESTÃO DE NORMATIVO, SE HOUVER	

Art. Xxxx ....
Art. Xxxx ....

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: LIMA ≡ FEIGELSON SOCIEDADE DE ADVOGADOS

CPF/CNPJ: 13.403.313/0001-32

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente algumas disposições, como por exemplo, o prazo para que tal comunicação seja feita, defina o formulário, bem como a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079/2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS **IMPORTANTE:** Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	Um incidente de segurança pode causar uma série de efeitos adversos aos titulares que vão desde sofrimento emocional a danos físicos e materiais.[1] O *Recital 75 do GDPR* traz um conceito de risco associado aos seus possíveis resultados danosos. O texto elenca as hipóteses nas quais o tratamento de dados pode trazer danos aos titulares: 1. Quando o tratamento der origem a discriminação, roubo de identidade ou fraude, perda financeira, danos à reputação, perda de confidencialidade de dados pessoais protegidos por sigilo profissional, reversão não autorizada de pseudonimização ou qualquer outra desvantagem econômica ou social significativa 2. Nos casos em que os titulares dos dados possam ser privados dos seus direitos e liberdades ou impedidos de exercer controlo sobre os seus dados pessoais; 3. Nos casos nos quais os dados pessoais tratados revelem origem racial ou étnica, opiniões políticas, religião ou crenças filosóficas, filiação sindical e o processamento de dados

[1] Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/. Acessado em 19 de março de 2021.

	genéticos, dados relativos à saúde ou dados relativos à vida sexual ou condenações criminais e infrações ou medidas de segurança relacionadas; 4. Nos casos em que são avaliados aspectos pessoais, designadamente analisando ou prevendo aspectos relativos ao desempenho no trabalho, situação económica, saúde, preferências ou interesses pessoais, fiabilidade ou comportamento, localização ou movimentos, com vista à criação ou utilização de perfis pessoais; 5. Nos casos nos quais dados pessoais de pessoas singulares vulneráveis, em particular de crianças, são tratados; 6. Quando o tratamento envolve uma grande quantidade de dados pessoais e afeta a muitos titulares de dados. No universo da privacidade e proteção de dados, comumente entende-se que o risco equivaleria à probabilidade de uma atividade de processamento de dados resultar em um impacto, ameaça ou perda de um bem jurídico (por exemplo, direitos e liberdades). Um risco inaceitável, portanto, seria a impossibilidade de mitigação de uma ameaça ou perda de um bem jurídico[2]. Pode-se afirmar, portanto, que um incidente de segurança tratará risco ou dano quando envolver qualquer uma das hipóteses acima.
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	1. Risco baixo: Nessa hipótese, o incidente ocorreria internamente, isto é, dentro da estrutura do controlador ou operador. Além disso, o incidente de segurança não envolveria dados sensíveis. 2. Risco médio ou moderado: O risco médio ou moderado geraria efeitos para fora da organização e, assim como o risco baixo, não envolveria dados sensíveis. 3. Risco alto: A hipótese de risco alto envolveria necessariamente dados sensíveis e causaria impactos para além da organização. A título de exemplo, a Autoridade de Proteção de Dados da Espanha (AEPD) determinou que sempre que houver dado sensível existe a obrigação de comunicação à autoridade, o que reforça o tratamento diferenciado conferido aos dados

[2] Dispoível em: https://iapp.org/media/pdf/resource_center/cipl_gdpr_risk_21_dec_2016.pdf. Acessado em 10 de março de 2021.

	sensíveis em razão do seu potencial discriminatório e os riscos trazidos por eventuais tratamentos abusivos ou ilícitos.
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	A noção de risco apresenta diferentes significados para diferentes pessoas. Contudo, pode-se afirmar que a ideia de "ameaça" está comumente presente quando se pensa em risco. O conceito de risco pode ser compreendido também como alta probabilidade de dano. A título de exemplo, alguns Estados norte-americanos dispensam os controladores do dever de notificação caso não haja **probabilidade de danos** aos titulares, ou seja, caso inexista risco[3]. O *Recital 91* do GDPR trata do Relatório de Impacto à Proteção de Dados que é exigido nas hipóteses de operações de tratamento que possam afetar um grande número de titulares e que são suscetíveis de resultar em alto risco. De acordo com o documento, a noção de "alto risco" envolveria, por exemplo: (1) grau de sensibilidade dos dados pessoais, (2) operações de tratamento que possam afetar os direitos e liberdades dos titulares dos dados, especialmente, quando essas operações tornam mais difícil para os titulares dos dados o exercício dos seus direitos e (3) quando de acordo com o estado de conhecimento tecnológico alcançado, uma nova tecnologia é utilizada em grande escala. Resta evidente que o risco sempre envolve a probabilidade do dano, bem como o potencial lesivo do tratamento aos direitos e liberdades do titular. Por sua vez, o dano representa o prejuízo ou a lesão já configurada. Para Sergio Cavalieri Filho, dano é a subtração ou diminuição de um bem jurídico, qualquer que seja a sua natureza, quer se trate de um bem patrimonial, quer se trate de um bem integrante da própria personalidade da vítima, como a sua honra, a imagem, a liberdade etc.[4] Portanto, o dano consiste em uma lesão a um bem jurídico, desvalorizando-o. De acordo com a Autoridade Mexicana (Instituto Nacional de Transparência, Acesso à Informação e Proteção de Dados Pessoais - INAI), **um incidente de segurança representa um risco**

[3] Disponível em: https://iapp.org/media/pdf/resource_center/Data_Breach_Notification_United_States_Territories.pdf. Acessado em 08 de março de 2021.
[4] CAVALIERI FILHO, Sérgio. *Programa de Responsabilidade Civil*. 8. ed. São Paulo: Atlas, 2008. pág. 71.

	materializado[5] , mas que não necessariamente gera um dano. Em nosso entendimento, para que um incidente de segurança enseje responsabilização do agente de tratamento, não basta a alegação abstrata de que houve dano ao titular, devendo restar demonstrado um prejuízo fático, como nas hipóteses de vazamento de dados sensíveis, em decorrência de seu potencial discriminatório.
O que deve ser considerado na avaliação dos riscos do incidente?	Dentre os parâmetros para avaliação dos riscos do incidente, com base no art. 33 do GDPR, destacam-se: 1. O volume e fluxo de dados tratados, de modo a dimensionar a categoria dos titulares de dados e o número aproximado dos respectivos titulares; 2. A verificação quanto à existência de dados pessoais sensíveis e suas respectivas possibilidades de discriminação; 3. A possibilidade de um Encarregado pela proteção de dados ficar responsável por aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências, nos termos do art. 41, I da LGPD; 4. Consultar o acervo documental quanto a Políticas e documentos adequados à proteção de dados, tais como Política de Retenção e Descarte, Política de Respostas a Incidentes, Política de Segurança da Informação, Relatório de Impacto à Proteção de Dados (DPIA) e Avaliação do Legítimo Interesse do Controlador (LIA); 5. Verificar se é utilizada alguma medida técnica e organizacional para prevenção de incidentes, tais como a adoção de sistemas de segurança da informação, senhas fortes e criptografias.
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	1. A janela de tempo do incidente, ou seja, por quanto tempo perdurou o incidente até que medidas fossem tomadas para cessar e conter o dano; 2. A natureza do incidente; 3. O número aproximado e a categoria dos titulares afetados, quando informações precisas não estiverem disponíveis (por exemplo, número exato de titulares de dados afetados). Frise-se que isso não deve impedir que a notificação da violação se dê em tempo hábil.[6]

[5] Disponível em: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/Recomendaciones_Manejo_IS_DP.pdf. Acessado em 08 de março de 2021.

[6] Guidelines on Personal data breach notification under Regulation 2016/679. Working Party Article 29. Disponível em: https://www.datenschutzstelle.li/application/files/7115/3621/9381/wp250rev01_en.pdf#:~:text=%E2%80%9CIn%20the%20case%20of%20a,unlikely%20to%20result%20in%20a. Acessado em 02 de março de 2021.

	4. O nome e informações de contato do Encarregado; 5. Data e hora da detecção do incidente; 6. Data e hora do incidente. Quanto ao **procedimento de notificação** à ANPD, entendemos que a criação de um conselho específico dentro da Autoridade brasileira seria uma alternativa válida para conferir maior eficiência às respostas aos incidentes. No Uruguai, por exemplo, quando o responsável pelo tratamento de dados tomar conhecimento de alguma violação de segurança, deverá comunicá-la imediatamente, juntamente com as medidas adotadas, tanto ao titular dos dados como à Autoridade uruguaia, que coordenará com o Centro Nacional de Resposta a Incidentes de Segurança Informática do Uruguai (CERTuy)[7]. Na mesma linha, a Argentina criou, mediante a *Resolução 1107-E / 2017*, o Comitê de Resposta a Incidentes de Segurança Informática, que faz parte do Ministério da Segurança. A função do Comitê é proteger os ativos de informação de sua comunidade-alvo e promover a conscientização da segurança da informação, tentando reduzir a probabilidade e gravidade de incidentes que podem comprometer significativamente a segurança de sistemas e redes.
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	O *General Data Protection Regulation* (GDPR) estabelece um prazo de 72 (setenta e duas) horas, contados do momento em que se tem conhecimento do incidente (Article 33 (1)). No mesmo sentido, está tramitando no Senado argentino Projeto de Lei (Proyecto de Ley nº 283/2018) que visa incluir na lei de proteção de dados argentina dispositivo sobre incidentes de segurança. O projeto fala igualmente no prazo de 72 (setenta e duas) horas contados do momento em que se tem conhecimento do incidente para notificar à Autoridade. De acordo com o projeto, o dever de notificação somente é dispensado caso "seja improvável que o incidente de segurança constitua risco para os direitos dos titulares de dados." Ambas normativas podem levantar questões acerca do que seria "ter conhecimento", momento crucial em que se começa a contar o prazo para notificação à ANPD. Ora, o *Article 29 Working Party* afirma

[7] Disponível em https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/publicaciones/cambios-recientes-legislacion-sobre-proteccion-de-datos-personales-en. Acessado em 08 de março de 2021.

	que “ter conhecimento” significa que o controlador tem um grau razoável de certeza de que houve um incidente de segurança que levou ao comprometimento dos dados[8].
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	• **Quanto ao prazo:** Embora a legislação europeia adote o parâmetro de 72 (setenta e duas) horas para comunicar à Autoridade, ela não define um prazo para comunicação aos titulares. No *Recital 86*, estabelece-se somente que **a comunicação deve ser feita o mais rapidamente possível** e em cooperação com a Autoridade supervisora. Destaca-se que o Regulamento afirma que a comunicação deve se dar o mais rápido possível, uma vez que o principal objetivo da notificação aos indivíduos é fornecer informações específicas sobre as medidas que devem seguir para se proteger. A tempestividade da comunicação aos titulares é fundamental, haja vista que dependendo da natureza da violação e do risco apresentado, a comunicação oportuna ajudará os indivíduos a tomar medidas para se proteger de quaisquer consequências negativas da violação. Entretanto, este critério deve considerar a capacidade técnica e financeira dos agentes de tratamento em analisar o ocorrido e identificar os possíveis danos. Naturalmente, no tocante à identificação e mitigação de incidentes de segurança, não se pode exigir de uma pequena ou média empresa o mesmo que se espera de uma empresa altamente estruturada e com vastos recursos destinados à adequação da LGPD. Portanto, o “mais rapidamente possível” não deve desprezar a realidade de cada agente e sim levar em conta as suas limitações para apresentar informações exatas e implementar medidas de mitigação de danos. Segundo a Autoridade mexicana (Instituto Nacional de Transparência, Acesso à Informação e Proteção de Dados Pessoais - INAI), recomenda-se notificar os titulares (i) **no menor tempo possível**, (ii) quando já houver informações específicas sobre o incidente e (iii) quando não houver mais exposição dos ativos envolvidos na violação. Dentro do processo de resposta a incidentes, isso ocorre no final do Contenção, ou no início da etapa de Mitigação. No que tange ao prazo, a *Ley Federal de Protección de Datos Personales en Posesión de Los Particulares* do México dispõe, no artigo 20 que “*[as] violações de segurança ocorridas em qualquer fase do tratamento que afetem significativamente os direitos econômicos ou morais dos titulares,*

[8] Ibid.

	serão informados de forma imediatamente pelo responsável ao titular, para que este tome as providências cabíveis para defender seus direitos." Como se pode observar, não há uma determinação precisa quanto ao prazo, abrindo margem para interpretação acerca do que seria "imediatamente" ou "no menor tempo possível". Ainda no cenário latino-americano, a Agencia de Protección de Datos de los Habitantes (Prodhab), autoridade de proteção de dados da Costa Rica, adota posição diversa. De acordo com o *Reglamento a la Ley n.° 8.968*, o responsável pelo tratamento de dados deve informar o titular de qualquer irregularidade no tratamento ou armazenamento de seus dados, como perda, destruição, extravio, entre outros, em decorrência de vulnerabilidade de segurança ou por ter conhecimento do fato, pelo qual terá **cinco dias** úteis a partir do momento em que ocorreu a vulnerabilidade, para que os titulares dos dados pessoais afetados possam tomar as medidas cabíveis. Ante o exposto, entendemos que o cenário ideal consiste na indicação exata do prazo, evitando-se a utilização de expressões vagas e imprecisas que geram controvérsia e, consequentemente, insegurança para os titulares, bem como para os controladores. Assim, consideramos o prazo de **5 (cinco) dias** contado da notificação à ANPD dialoga com a realidade brasileira. ● **Quanto às informações:** Tendo em vista que o *Recital 85 do GDPR* destaca que um dos objetivos da notificação é a contenção de danos ao indivíduo, entendemos ser necessário, além das informações previstas no art. 48, §1º da LGPD, acrescentar **instruções para as pessoas atingidas de como mitigar eventuais efeitos adversos**, conforme previsto no *Recital 86 do GDPR.* Ademais, entendemos ser necessário indicar: 1. **O nome e informações de contato do Encarregado**: Consonante com o princípio da boa-fé e transparência, norteadores da atividade de tratamento de dados pessoais, as informações de contato do Encarregado devem estar disponíveis para caso os titulares desejem maiores detalhes sobre o incidente.

	2. **As possíveis consequências do incidente**, além dos riscos relacionados, conforme previsto no art. 48, §1º, IV. 3. **Categoria dos titulares e dos dados afetados**: O GDPR não define as categorias de titulares de dados, tampouco as de registro de dados pessoais. Contudo, o *Article 29 Working Party*, grupo de trabalho independente que lidou com as questões relacionadas com a proteção de dados pessoais e privacidade até a entrada em vigor do GDPR[9], recomenda que as categorias considerem os variados tipos de indivíduos que possam ter seus dados violados. Assim, deve-se levar em conta crianças e outros grupos vulneráveis, pessoas deficientes, empregados e consumidores. Similarmente, as categorias de registros de dados pessoais podem envolver diferentes tipos de registros que o como dados de saúde e educação, informações de assistência social, dados financeiros e bancários, número de passaporte e assim por diante[10]. Caso o incidente implique desdobramentos como perda de controle sobre dados pessoais ou limitação de seus direitos, discriminação, roubo de identidade ou fraude, prejuízo financeira, reversão não autorizada de pseudonimização, danos à reputação, perda de confidencialidade de dados pessoais protegidos por sigilo profissional ou qualquer outra desvantagem econômica ou social significativa para o titular[11], é imprescindível que a notificação aos titulares indique a categoria dos sujeitos e dados atingidos.
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota	A comunicação acerca de incidente de segurança deve ser feita de maneira **clara e transparente** de modo que não é recomendável que o comunicado se dê via *newsletter*, por exemplo. Justamente por se tratar de um incidente que implica risco ou danos aos titulares, a comunicação deve ser específica para as hipóteses de incidentes, não sendo recomendado um comunicado geral disparo de forma automática. A título de exemplo, a Autoridade mexicana[12] elenca três hipóteses nas quais se pode optar por **notificação indireta genérica** por meio de sites ou mídia de massa: 1. quando a notificação direta ao titular puder causar mais danos; 2. quando for muito custoso ou;

[9] Disponível em: https://edpb.europa.eu/our-work-tools/article-29-working-party_pt. Acessado em 08 de março de 2021.
[10] Guidelines on Personal data breach notification under Regulation 2016/679
[11] Recital 85 do GDPR. Disponível em: https://gdpr-info.eu/recitals/no-85/. Acessado em 03 de março de 2021.
[12] Disponível em: https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPrivado/Recomendaciones_Manejo_IS_DP.pdf. Acessado em 08 de março de 2021.

à imprensa, publicação na internet etc.)?	3. quando não houver informações de contato. Assim, sugerimos que a comunicação seja feita direta e individualmente por *e-mail*, postal ou até mesmo via SMS, desde que seja possível acessar mais informações a partir da mensagem de texto. De acordo com o *Article 29 Working Party*, *e-mail*, SMS, mensagem direta, *banners* ou notificações no site, comunicações postais e anúncios na mídia impressa são métodos adequados de comunicação. Uma notificação confinada exclusivamente a um comunicado à imprensa ou blog corporativo não seria um meio eficaz de comunicar uma violação a um indivíduo. Os controladores devem escolher um meio que maximize a chance de comunicar as informações de maneira adequada a todos os indivíduos afetados. Portanto, ao invés de recorrer a somente um canal de comunicação, **a utilização de mais de um método é a alternativa adequada a fim de potencializar o alcance do comunicado aos titulares**. Na mesma linha, a Autoridade mexicana (Instituto Nacional de Transparência, Acesso à Informação e Proteção de Dados Pessoais) aconselha utilizar mais de um método de comunicação simultaneamente[13]. Vale destacar ainda dois pontos quanto ao método de comunicação: 1- A notificação deve ser independente e personalizada, e não deve incluir informações não relacionadas ao incidente de segurança, pois pode causar confusão; 2- Os controladores devem estar atentos para não utilizar um canal de comunicação comprometido pelo incidente. Quanto à linguagem empregada na comunicação, esta deve ser simples de fácil compreensão. **Os controladores devem garantir que os titulares compreendam a natureza do incidente e suas repercussões, além das medidas a serem tomadas para se proteger.** É recomendável que os controladores entrem em contato com a ANPD no intuito de determinar a mensagem e canal mais apropriados para informar os titulares. Nesse ponto, cabe à ANPD auxiliar os controladores de modo a orientá-los, exercendo, portanto, um papel consultivo.

[13] Ibid.

	No tocante à comunicação pública, esta deve ser excepcional, uma vez que traz consideráveis danos reputacionais às empresas. Até porque, o simples fato de a comunicação se dar por via pública não significa que o titular afetado pelo incidente a verá, desnaturando a finalidade primeira da comunicação. Assim, entendemos que representa um último recurso, devendo ser utilizado quando não for possível identificar os titulares ou quando a volumetria do incidente for muito elevada, de modo a impossibilitar ou dificultar significativamente a comunicação individual. Contudo, pode haver circunstâncias em que a própria comunicação pública não será suficiente. Em maio de 2020, o Instituto Nacional de Seguridade Social italiano ("INPS") sofreu um incidente em seu portal *on-line*, expondo os dados dos contribuintes e de menores. Dada a natureza delicada destes dados, a autoridade italiana *Garante per La Protezione dei Dati Personali* entendeu que a comunicação pública no site do Instituto não bastava de modo que de foi exigido que uma nova comunicação fosse realizada diretamente aos titulares.
Quais seriam as eventuais exceções da obrigatoriedade de informar à ANPD?	Considerando a ausência de moldura regulatória, entendemos que comunicação à ANPD não será necessária se o incidente não for capaz de causar dano efetivo ao titular. A título de exemplo, os dados sensíveis referentes à origem étnica e racial apresentam um potencial lesivo considerável e podem efetivamente ensejar práticas discriminatórias, caso vazados. Desse modo, a exceção se configura na hipótese em que o incidente se mostrar inofensivo, não causando maiores transtornos aos titulares. Contudo, se poderia ventilar a possibilidade de criação de uma categoria ou lista de dados pessoais que, quando objeto de incidentes, necessariamente gerariam a obrigação de notificação à ANPD. Nessa linha, a exceção à obrigatoriedade de notificação seria quando o incidente envolvesse dados não incluídos nesta categoria. Outra possível hipótese de dispensa ao dever de informar seria se a própria Autoridade levasse ao conhecimento do agente o incidente de segurança. Entretanto, para a *Comission Nationale de l'Informatique et Libertés* (CNIL), o fato da Autoridade ter informado o agente a respeito do incidente não o exonera da obrigação de notificar. Por outro lado, em nosso entendimento, a comunicação do incidente pelo agente, mesmo quando este já é de conhecimento da Autoridade, é um ato de

	demonstração de boa-fé do infrator que certamente deve ser observado no momento do arbitramento da sanção administrativa.
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	O GDPR enumera as hipóteses nas quais o controlador não tem a obrigação de comunicar o incidente aos titulares *(Article 34(3))*: 1. Se o responsável pelo tratamento tomou medidas subsequentes que garantam que o elevado risco para os direitos e liberdades das pessoas já não seja provável de se concretizar. Por exemplo, dependendo das circunstâncias do caso, o controlador pode ter identificado imediatamente quem acessou os dados pessoais, tomando medidas para neutralizá-lo. 2. Se antes da violação, o controlador tiver implementado medidas técnicas e organizacionais aptas a proteger os dados pessoais (ex. criptografia), tornando-os inteligíveis para qualquer pessoa que não fosse autorizada a acessar o banco de dados; 3. Se a comunicação fosse demandar esforços desproporcionais. Nesse caso, uma campanha de informação pública ou medidas semelhantes devem ser adotadas para que os indivíduos afetados possam ser efetivamente informados Poder-se-ia acrescentar ainda, a hipótese na qual a ANPD elaboraria um lista ou categoria de dados que, quando objeto de incidente de segurança, geraria para o controlador a obrigação de notificar aos titulares. Nesta categoria, incluir ia-se, por exemplo, dados sensíveis, bancários e financeiros, dados relativos ao CPF e RG, filiação e endereço. Assim, todo vazamento que envolvesse estes dados deveria ser comunicado. Por exemplo, todos os 50 estados dos EUA, Washington, DC e a maioria dos territórios dos EUA (incluindo Porto Rico, Guam e as Ilhas Virgens) aprovaram leis de notificação de incidentes que exigem dos controladores que notifiquem os titulares sobre violação de segurança envolvendo categorias de informações mais sensíveis, como o *Social Security Number* e outros identificadores governamentais, dados bancários e de cartão de crédito, dados médicas ou de saúde, identidade de seguro, identificação fiscal, data de nascimento, bem como credenciais de conta online, assinaturas digitais e/ou biometria.[14] Desse modo, a possível quarta exceção à obrigatoriedade de informar aos titulares seria se os dados objeto do incidente não estiverem incluídos nesta categoria.

[14] Disponível em: https://www.dlapiperdataprotection.com/index.html?t=breach-notification&c=US. Acessado em 08 de março de 2021.

Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	Dentre os critérios para análise objetiva da ANPD, quanto à gravidade do incidente de segurança, destacam-se: 1. A quantidade aproximada de titulares afetados, bem como as respectivas categorias de dados pessoais; 2. A janela temporal na qual o incidente ficou produzindo efeitos; 3. A origem dos dados pessoais; 4. As categorias de titulares afetados; 5. A base legal utilizada; 6. A existência de meios disponíveis e factíveis para evitar que o incidente não ocorresse – ou ocorresse em menor grau –, observada a capacidade financeira da empresa e a atividade por ela desempenhada; 7. A existência de documentos regulatórios de compliance de dados, como Registro das Operações de Tratamento de Dados (RoPA); Políticas de: (i) Privacidade, (ii) Retenção e Descarte de Dados, (iii) Segurança da Informação e, (iv) Resposta a Incidentes; Relatório de Impacto à Proteção de Dados (RIPD); 8. A adoção de medidas técnicas e organizacionais de treinamento para efetiva mitigação de riscos; 9. A adequada comunicação e oferecimento de suporte aos titulares de dados afetados com o incidente; 10. A existência de mecanismos de Segurança da Informação, tais como criptografia, senhas fortes e backup.
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	A análise da gravidade do incidente deve ser feita em etapas: 1. A primeira questão a ser avaliada deve ser a conduta do agente de tratamento diante do incidente de segurança, analisando, conforme acima, a sua postura antes, durante e após o incidente.

	2. Caso o agente de tratamento tenha enviado comunicação nos termos do art. 48, LGPD, deverá ser avaliado o nível de cooperação com a autoridade; Em sequência, passa-se à análise do incidente em si: 1. Em primeiro, deve ser avaliada a possibilidade de delimitação dos titulares e dos dados envolvidos; 2. Em sequência, deve ser realizada a análise quantitativa do incidente (perguntando, por exemplo, quantos titulares foram envolvidos e quais informações destes foram comprometidas), sempre levando em conta a cooperação demonstrada pelo agente, principalmente, porque em certas situações o detalhamento do incidente pode se mostrar difícil, indo de encontro à "comunicação mais rápida possível" mencionada acima. Munido destas informações, é possível analisar as seguintes questões: previsibilidade do incidente, conduta do agente de tratamento e gravidade do incidente.
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	As medidas a serem impostas pelos agentes de tratamento após a comunicação de segurança devem ser avaliadas de acordo com a gravidade do incidente, podendo variar significativamente de acordo com a magnitude do ocorrido. Naturalmente, devem ser adotadas medidas técnicas para a interrupção do incidente e mitigação das consequências, que devem ser indicadas casuisticamente. Entretanto, dentre as medidas de natureza administrativa, a ANPD deverá sugerir a elaboração (ou, caso haja, a efetiva aplicação ou adaptação) de políticas internas, especialmente de: ● Segurança da Informação; ● Resposta a Incidentes; ● Retenção e descarte de dados; ● Diretrizes de proteção de dados direcionadas aos colaboradores.

SUGESTÃO DE NORMATIVO, SE HOUVER
Art. Xxxx. Comunicação aos titulares - O controlador ou operador, quando ciente do incidente de segurança, deve informar os titulares de qualquer incidente que possa efetiva e concretamente causar dano ao titular, pelo qual terá cinco dias úteis a partir do conhecimento do fato, para que os titulares dos dados pessoais afetados possam tomar as medidas cabíveis.
Art. Xxxx .... Comunicação à ANPD - Em caso de violação de dados pessoais, o controlador ou operador, deve em até 72 horas após ter tido conhecimento do fato, notificar o incidente à Autoridade Nacional de Proteção de Dados, exceto se for improvável que a violação de dados pessoais resulte em efetivo prejuízo ao titular.

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA:

Loeser e Hadad Advogados

CPF/CNPJ:60.527.520/0001-89

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

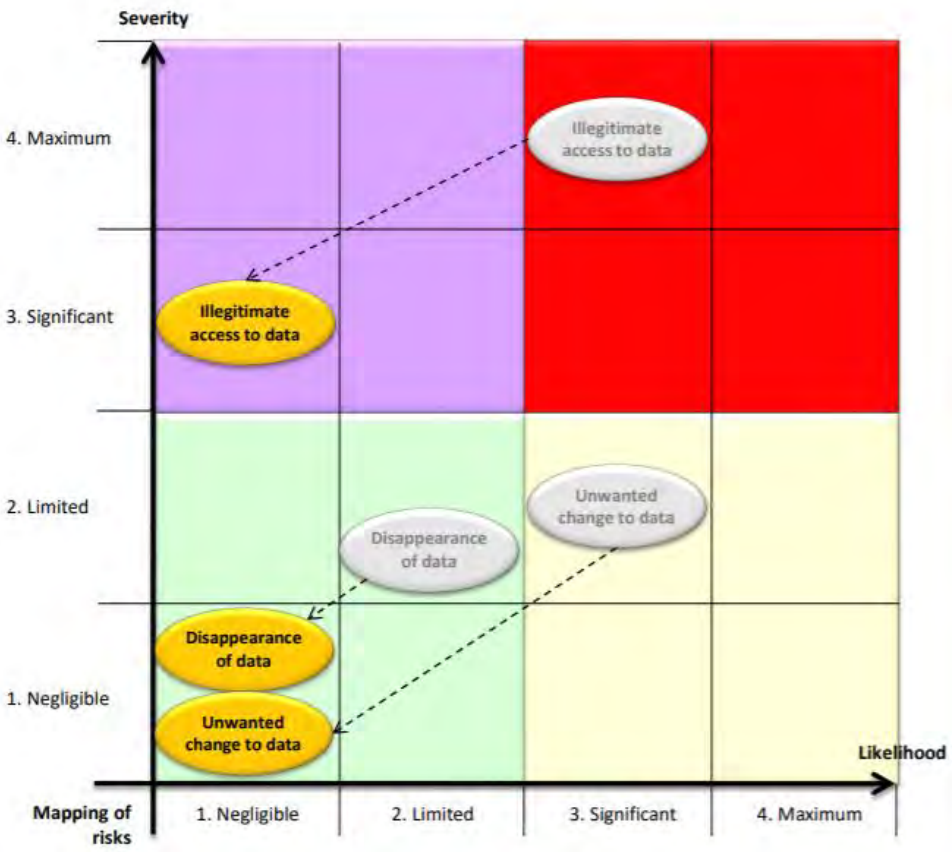
São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS

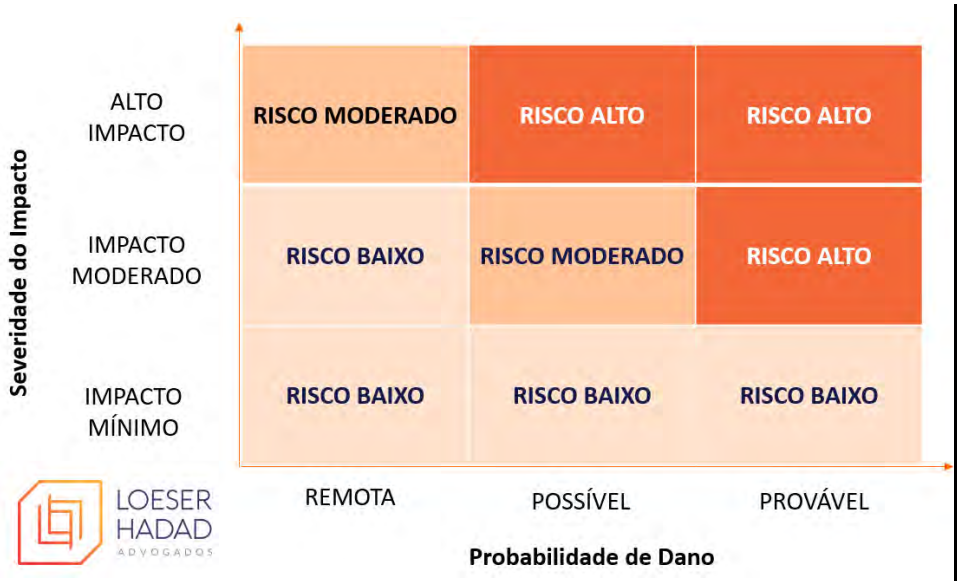
IMPORTANTE: Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.

TÓPICO/QUESTÃO	CONTRIBUIÇÃO/INSTITUIÇÃO

Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	De acordo com a GDPR, danos relevantes são aqueles que podem gerar desvantagens pessoais, como discriminação ou danos à reputação do titular (vide Recital 85), que dependem do impacto causado no caso concreto. Fonte: https://gdpr-info.eu/recitals/no-85/ Em outras legislações da América Latina, como a do Equador, não é necessário que o dano seja relevante para comunicar a autoridade. Entendemos que adotar metodologia semelhante à apresentada pela autoridade francesa *(Commission Nationale Informatique & Libertés (CNIL)* representa uma boa opção para a ANPD avaliar se o risco é relevante. Incluímos na resposta ao próximo item um gráfico que pode servir de base para auxiliar a ANPD avaliar a relevância do risco. A metodologia adotada pela autoridade francesa consiste em avaliar duas variáveis conjuntamente: a **severidade** do risco caso o mesmo ocorra, e a **probabilidade** do risco se concretizar:  Fonte: Guideline Privacy Impact Assessment - Pág. 23 - https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-2-en-templates.pdf

	Além disso, em relação aos eventuais danos, é importante que a ANPD avalie se dados pessoais sensíveis foram afetados pelo incidente, se dados de crianças ou adolescentes foram afetados e, ainda, se os dados envolvidos no incidente têm capacidade de gerar discriminação, violação do direito à imagem e à reputação, fraudes financeiras, roubo de identidade ou violação aos direitos fundamentais previstos na Constituição Federal. A título exemplificativo, em um caso julgado pela autoridade italiana, um hospital teve que pagar multa de EUR 50.000,00 por dois incidentes onde, por erro interno, exames de um paciente foram enviados para a pessoa errada, incluindo um menor. O caso e a decisão podem ser consultados através dos links: https://www.enforcementtracker.com/ETid-561 (inglês) e https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9544092 (italiano). Os critérios utilizados para a gradação neste caso foram: a presença de dados de um menor, a presença de dados pessoais sensíveis e a repetição do incidente, considerando que o ocorrido se repetiu em um pequeno prazo. A autoridade considerou ainda a **cooperação da empresa** e a **falta de voluntariedade do ocorrido** para a aplicação da pena. Além da multa mencionada, o hospital teve que publicar o ocorrido em seu site. Assim, entendemos que caso o incidente de segurança envolva dados pessoais sensíveis, dados de criança ou adolescente, ou qualquer uma das condicionantes supracitadas, aumenta-se a severidade do possível impacto.

O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	A autoridade francesa de proteção de dados, *Commission Nationale Informatique & Libertés (CNIL),* classifica o risco em 4 categorias: 1- insignificante; 2- limitado; 3- significante; e 4- máximo. Como mencionado no tópico anterior, a avaliação é realizada tomando como base duas variáveis: a **severidade** do possível dano que o risco representaria caso ocorresse e a **probabilidade** do risco ser concretizado. Fonte: Guideline Privacy Impact Assessment - Pág. 23 - https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-2-en-templates.pdf O *EDPB (European Data Protection Board),* por outro lado, categoriza o risco em "risco baixo" e "risco alto". Apesar desta diferença, assim como a autoridade francesa, o EDPB indica que a **severidade** do possível dano e a **probabilidade** de concretização do risco são dois elementos que devem ser levados em consideração para avaliar os riscos. Fonte: Article 29 of Directive 95/46/EC - Statement of WP29 on the role of a risk-based approach in data protection legal frameworks, Págs. 2 e 4. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf A autoridade do Reino Unido, *Information Commissioner's Office (ICO),* segue o mesmo entendimento apresentado pelo EDPB, indicando que deve ser avaliada a **probabilidade** e a **severidade** de um potencial dano aos titulares. Fonte:https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/when-do-we-need-to-do-a-dpia/#when3 Compatibilizando o quanto determinado pelas autoridades mencionadas e levando em conta o mercado brasileiro, entendendemos que a ANPD deve categorizar o risco como baixo, moderado e alto, levando em conta a severidade do impacto e a probabilidade de dano, utilizando gráfico semelhante ao adotado pela autoridade francesa, conforme sugestão abaixo:

	 Em resposta à terceira pergunta, entendemos que **risco baixo** deve ser considerado como **não relevante**. No entanto, o mesmo não deve ser aplicado ao dano, pois levando em conta os fundamentos e princípios da LGPD, podemos observar o caráter protetivo da legislação em relação ao titular de dados. Desta forma, entendemos que **mesmo que o dano seja baixo, ainda assim pode ser considerado como relevante**, já que independentemente da intensidade, houve algum prejuízo ao titular de dados, seja de ordem material ou moral, o que viola os fundamentos e princípios da LGPD (arts. 2º e 6º).
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	Risco é a **probabilidade** de um evento acontecer, seja ele uma ameaça quando negativo, ou oportunidade, quando positivo. Juridicamente, "risco" possui via de regra conotação negativa, uma vez que é considerado como um evento futuro e incerto, insubmisso à vontade das partes, que pode ocasionar dano a outrem. Corroborando com esta perspectiva, tem-se o entendimento de Sílvio Venosa de que: "o risco consiste no acontecimento **futuro** e **incerto** previsto no contrato, **suscetível de causar dano**". (VENOSA, Sílvio de Salvo. Direito Civil: Contratos em espécie. São Paulo: Editora Atlas, 2002, v. III, 2ª Ed., 373.) A definição de risco está diretamente atrelada ao estudo da responsabilidade civil, bem como a compreensão de que a "culpa" não é (e não seria), de acordo com a "Teoria do Risco", elemento suficiente para atribuição de responsabilidade em alguns casos,

uma vez que há situações que naturalmente criam risco *per si, e os agentes que cientes de tais riscos, decidissem por executar tal atividade, deveriam assumir sua responsabilidade em ressarcir eventual "dano" causado a terceiro.*

Nesse sentido, alguns doutrinadores como Carlos Alberto Gonçalves, entendem que a partir do momento em que um agente exerce uma atividade "que possa oferecer algum perigo, representa **um risco, que o agente assume**, **de ser obrigado a ressarcir os danos que venham resultar a terceiros dessa atividade**" (GONÇALVES, Carlos Roberto. Direito Civil Brasileiro: Responsabilidade Civil. 12. ed. São Paulo: Saraiva, 2017. v.4, p. 28.)

Esta teoria vem inserida no art. 927, parágrafo único, do Código Civil Brasileiro, em que resta certo que, independentemente de culpa e, dos casos especificados em lei, haverá obrigação de reparar o ato lesivo quando a atividade normalmente desenvolvida pelo autor dos danos implicar, **por sua natureza, risco para os direitos de outrem.**

Enquanto o dano é um prejuízo (de fato) causado por alguém a outrem, detentor de um bem juridicamente protegido. Assim, o dano ocorre quando esse bem é diminuído, inutilizado ou deteriorado. Conforme, definição da doutrina majoritária:

> *"(...). Conceitua-se, então, o dano como sendo a subtração ou diminuição de um bem jurídico, qualquer que seja a sua natureza, quer se trate de um bem patrimonial, quer se trate de um bem integrante da própria personalidade da vítima, como a sua honra, a imagem, a liberdade etc.* ***Em suma, dano é lesão de um bem jurídico,*** *tanto patrimonial como moral, vindo daí a conhecida divisão do dano em patrimonial e moral" (CAVALIERI F.º, 2005, p. 95-96).*
>
> *"****Dano consiste no prejuízo sofrido pelo agente****. Pode ser individual ou coletivo, moral ou material, ou melhor econômico e não econômico. (...)* ***Na noção de dano está sempre presente a noção de prejuízo****. Nem sempre a transgressão de uma norma ocasiona dano. Somente haverá possibilidade de indenização, como regra, se o ato ilícito ocasionar dano. Cuida-se, portanto, do dano injusto, aplicação do princípio pelo qual a ninguém é dado*

	prejudicar outrem (neminem laedere)." (VENOSA, Silvio de Salvo, 2004, p. 33 -34). Esses dois conceitos estão diretamente relacionados, uma vez que a LGPD surge com o propósito de proteger os dados de um titular, criando ferramentas para que o risco de violação de seus direitos, e efetivo dano não ocorram. E, ainda, a LGPD indica possibilidades de responsabilização daquele que feriu tal direito, bem como cria possibilidades de o titular receber o ressarcimento adequado pelos danos sofridos.
O que deve ser considerado na avaliação dos riscos do incidente?	A avaliação de riscos do incidente de segurança deverá levar em consideração os seguintes fatores: ● Natureza dos dados pessoais envolvidos no incidente; ● Se houve fluxo de saída de dados não criptografados para fora do banco de dados da empresa; ● Categoria de pessoa e/ou entidade que obteve acesso aos dados pessoais envolvidos no incidente; ● Categoria dos titulares dos dados pessoais envolvidos no incidente; ● Quantidade de titulares de dados pessoais afetados no incidente; ● Impacto para os titulares de dados. Para referência, indicamos os guias a seguir: "*Understanding and assessing risk in personal data breaches*" produzido pelo Information Commissioner's Office - ICO e disponibilizado no link: https://ico.org.uk/for-organisations/data-protection-advice-for-small-organisations/understanding-and-assessing-risk-in-personal-data-breaches/ e "*Guidelines 01/2021 on Examples regarding Data Breach Notification*" produzido pelo European Data Protection Board - EDPB e disponibilizado no link: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf
Quais informações os controladores devem notificar à ANPD, além	O parágrafo 1º do Art. 48 da LGPD deixa de mencionar alguns detalhes importantes para a comunicação, sendo eles: - Quantidade de titulares

daquelas já listadas no §1º do art. 48?	- Volume de dados pessoais afetados - Nome e contato do encarregado de proteção de dados ou outro canal de comunicação com o controlador, e - Se houve fluxo de saída de dados não criptografados para fora do banco de dados da empresa (ou seja, se o terceiro obteve acesso aos dados em si). Entendemos que a ANPD deve complementar a legislação com essas informações.
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	No regulamento europeu o prazo para informar a autoridade é de 72 horas (muito embora não de maneira peremptória, porém acompanhada de uma justificativa pelo atraso). Art. 33(1) da GDPR: https://gdpr-info.eu/art-33-gdpr/ No entanto, algumas empresas, mesmo no âmbito da GDPR, adotam o **prazo de dois dias úteis**, como forma de prevenir ainda mais danos. Exemplo disto está no procedimento para reportar incidentes da empresa *Mopinion*, conforme documento: https://www.mopinion.com/wp-content/uploads/2020/02/procedure-for-data-breach.pdf As leis americanas que tratam de incidentes de dados, por sua vez, também deixam o prazo em aberto, sendo que a legislação do estado do Arkansas considera o prazo de **2 dias** como razoável. Sugerimos considerar prazos maiores para startups, microempresas e empresas de pequeno porte que não tenham no tratamento dos dados a sua principal atividade, considerando o quadro enxuto de funcionários e, na maioria dos casos, a falta de capacidade técnica para investigar o incidente.

Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	A GDPR não estabelece um prazo específico para a comunicação de incidente de segurança ao titular. Apenas determina que o mesmo deve ser informado "sem atraso indevido" - Art. 34(1) do GDPR: https://gdpr-info.eu/art-34-gdpr/ Ainda neste sentido, o *Recital 86* (disponível em: https://gdpr-info.eu/recitals/no-86/) demonstra que na europa o prazo razoável para a notificação dos titulares não é fixo, mas se altera de acordo com o caso concreto. Por exemplo, em caso de necessidade de mitigar um dano imediato haveria a necessidade de realizar uma comunicação imediata aos titulares. Enquanto em casos onde há incerteza com relação aos danos ou risco de dano ao titular, um prazo superior seria justificável. Entendemos que, caso o incidente não se encaixe nos casos mencionados acima, o prazo para a comunicação aos titulares deve seguir o mesmo prazo de comunicação à ANPD. No caso da GDPR, recomenda-se que as informações que constarão da notificação ao titular sejam: - o nome e contato do encarregado de proteção de dados ou outro ponto de contato onde mais informações poderão ser obtidas; - as possíveis consequências do incidente; e - as medidas tomadas ou pretendidas para remediar o incidente e seus efeitos. O mencionado *Recital* 86 recomenda que a natureza do incidente e recomendações de possíveis medidas que podem ser tomadas pelo titular para mitigar os eventuais danos também sejam comunicadas. Entendemos que a comunicação ao titular não deve conter informações de cunho altamente técnico, como a comunicação à ANPD. Isto porque estas informações poderiam gerar mais dúvidas, o que impactaria diretamente a atividade do Encarregado, que é essencial em caso de incidentes. Não há necessidade de informar também a quantidade de dados afetados, somente que

	os dados do titular estavam envolvidos em um incidente e a natureza dos mesmos. Seria interessante prever recomendações para garantir uma linguagem fácil e acessível ao titular dos dados, principalmente considerando grupos mais vulneráveis, como por exemplo, crianças e idosos.
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	Entendemos que a comunicação deve ser realizada pelas formas que mais tenham probabilidade de atingir o titular dos dados, considerando inclusive a utilização de mais de uma forma de contato. Desta feita, cenários em que a coleta de dados foram realizados por meio de um aplicativo, a comunicação deveria ser realizada tanto pelo email cadastrado pelo titular quanto pela própria interface do aplicativo. Titulares que têm uma relação presencial com o controlador, por exemplo, pacientes médicos, devem ser informados por e-mail e, se possível, por telefone. Ao utilizar a notificação por email ou pela própria interface da plataforma, seria possível direcionar o titular dos dados para que reforce a segurança de sua conta, por exemplo, possibilitando que troque sua senha ou que insira outras formas de segurança disponibilizadas pelo controlador (dupla autenticação, atualização de seus dados, dentre outros). Por fim, a regulamentação deveria admitir a possibilidade de uma comunicação geral para os titulares de dados afetados em situações pré-determinadas, por exemplo: quando há dificuldade por parte do controlador de identificar qual titular teve seus dados envolvidos no incidente, ou, ainda, em incidentes que comprometem um extenso número de titulares.
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	A única exceção de comunicação à autoridade constante na GDPR é caso não exista a probabilidade de que o incidente ocasione riscos aos direitos e liberdades dos titulares. Esta exceção consta no artigo 33 da GDPR, disponível em: https://gdpr-info.eu/art-33-gdpr/

	Neste sentido, o controlador deve ser capaz de demonstrar esta condição, de acordo com o princípio da prestação de contas. Assim, entendemos que seguindo a metodologia exposta anteriormente, quando o **risco for considerado baixo**, levando em consideração a **severidade** e **probabilidade** de concretização de dano aos titulares, o agente de tratamento deve ser desobrigado a informar a ANPD, de modo que a autoridade seja informada somente quando o risco for **relevante** (moderado e alto). Este também é o posicionamento da autoridade europeia EDPB, em seu Guideline 01/2021. Fonte:https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf Em contrapartida, caso haja **dano** ao titular, independentemente da intensidade, entendemos que a ANPD e o titular devem ser informados, pois nesta hipótese houve um prejuízo ao titular de dados, seja de ordem material ou moral, o que viola os fundamentos e princípios da LGPD, especialmente os contidos nos artigos 2º e 6º da lei.
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	Para este ponto, podemos tomar como exemplo a legislação europeia e equatoriana. A primeira dispõe, em seu art. 34, que não há necessidade de comunicar o titular se uma das seguintes condições for preenchida: - Se o controlador implementou medidas técnicas e organizacionais apropriadas e estas foram aplicadas aos dados pessoais envolvidos no incidente, principalmente as medidas que fazem com que os dados sejam ininteligíveis para as pessoas não autorizadas (Ex: Criptografia) - Se o controlador tomou medidas subsequentes que garantem que os riscos aos direitos e liberdades dos titulares não tenham chances de acontecer; ou - Se a notificação necessita de esforços desproporcionais. Caso em que deve haver comunicação pública ou similar.

	A equatoriana, por sua vez, possui os mesmos três pontos para dispensa de notificação, sendo que existe uma diferença de redação, onde esta dispõe que "**não se deve** notificar os titulares caso uma das seguintes condições seja preenchida", enquanto a europeia diz que "**não é necessário**". Um dos pontos levantados recentemente nos Guidelines 01/2021 do EDPB é a dispensa da comunicação quando não houve qualquer dano efetivo ao titular. Neste existem alguns exemplos práticos de incidentes com que a autoridade teve que lidar em seu tempo de atuação. Uma das recomendações do documento é que, caso após o incidente o controlador verifique, através de uma avaliação de riscos, que não houve riscos e nem há a possibilidade destes ocorrerem no futuro, não é necessária comunicação aos titulares ou à autoridade. Há ainda um exemplo que demonstra que, em casos onde somente parte dos titulares foram afetados, não há necessidade de comunicar todos constantes no banco de dados. Somente uma comunicação direta àqueles afetados deve ser realizada.
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	Segundo o *European Data Protection Board,* entre os critérios a serem adotados para análise da gravidade, estão: ● O impacto e a severidade dos efeitos do incidentes de segurança; ● A vulnerabilidade subjacente dos titulares, o método de infiltração (quando aplicável) e se o código malicioso ainda está presente, a fim de compreender as consequências; ● Se as informações afetadas estavam protegidas do restante dos dados pessoais tratados pelo agente de tratamento; ● Se existe uma forma de mitigar os danos aos titulares e se essa medida de mitigação está sendo adotada. Fonte:https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf Além disso, deve ser levado em consideração, entre outros aspectos: ● Gravidade do dano causado ao titular;

	● A boa-fé do agente de tratamento, que pode ser identificada por meio da apresentação, pelo agente à ANPD, de evidências que comprovem que a empresa implementou um Programa de Governança em Proteção e Privacidade de Dados, constituiu um Comitê (a depender do porte), adotou medidas para resguardar a privacidade dos titulares, alterou processos internos para torná-los mais transparentes, elaborou Política de Privacidade condizente com o tratamento dos dados que realiza, elaborou Código de Boas Práticas, Relatórios de Impactos para as operações que representam risco aos titulares ou aquelas legitimadas pelo Legítimo Interesse, entre outras ações que demonstrem que o agente de tratamento, apesar de ter sofrido incidente de segurança, agiu com boa-fé, sem tentar obter vantagem ilícita perante os titulares. Em resumo, a demonstração do comprometimento do agente de tratamento em adotar processos e políticas internas que assegurem o cumprimento de normas e boas práticas relativas à proteção de dados pessoais é o que entendemos que deve ser levado em consideração na análise da gravidade do incidente e no balanceamento da aplicação de eventual sanção. ● A vantagem auferida ou pretendida pelo agente de tratamento relacionado ao incidente; ● A condição econômica do agente de tratamento; ● Reincidência; ● A adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do §2º do art. 48; ● A pronta adoção de medidas corretivas; ● A proporcionalidade entre a gravidade da falta e a intensidade da sanção.
Existe alguma metodologia recomendada para a análise de gravidade do	Existem diversas metodologias para análise de gravidade de um incidente de segurança e seus riscos. Estas variam de metodologias simples, como a apresentada pelo ICO e disponível em: https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach-assessment/, a metodologias complexas, com

incidente de segurança? Se sim, qual(is)?	diversas classificações dos riscos, como a apresentada pela ISO/IEC 27005 (páginas 66 - 69) e pelo IAPP. A primeira propõe a possibilidade de avaliar as consequências de várias maneiras, podendo ser quantitativa (considerando uma unidade monetária), qualitativa (como “risco moderado” ou “severo”), ou mista, sendo uma junção das anteriores. Para definir a probabilidade de ocorrência de uma ameaça, a norma explica que devemos considerar a atratividade do ativo ou do potencial impacto, a facilidade de se converter a exploração destes ativos em recompensas, a capacitação técnica do agente da ameaça e a suscetibilidade da vulnerabilidade à exploração. Uma das opções apresentadas é a avaliação com base em uma matriz com valores pré-definidos. Nesta, as medidas quantitativas são valoradas conforme o custo de reposição, reconstrução, aquisição ou desenvolvimento de eventuais ativos físicos e software. Desta forma, o valor e “sensibilidade” dos dados em uso, armazenados, sendo processados ou acessados é determinado, com base em diretrizes para valoração da informação, que cobre temas como segurança física das pessoas envolvidas, informações pessoais, obrigações legais e regulatórias, ordem pública, dentre outras. Estas diretrizes servem para facilitar a identificação dos valores em uma escala numérica. Em seguida, questionários para cada tipo de ameaça são preenchidos, objetivando permitir uma avaliação da probabilidade de ocorrência de ameaças e a facilidade com que uma ameaça pode explorar as eventuais vulnerabilidades e provocar consequências. Desta forma, o nível da ameaça pode ser identificado numa escala de “alto” a “baixo”. Assim, os valores dos ativos e níveis de ameaça e vulnerabilidade são colocados em uma matriz utilizada para medir o risco, em uma escala de 0 a 8, conforme exemplo abaixo:

	Probabilidade da ocorrência – Ameaça	Baixa			Média			Alta		
	Facilidade de Exploração	B	M	A	B	M	A	B	M	A
Valor do Ativo	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

As vulnerabilidades e ameaças respectivas são levadas em consideração para cada ativo. Caso exista uma vulnerabilidade sem ameaça correspondente (ou vice-versa), não há risco no momento. Como exemplo, em um ativo de valor 1, com ameaça alta e vulnerabilidade (Facilidade de Exploração) alta, a medida do risco é 5.

Existe também uma matriz que relaciona a probabilidade de um cenário de incidente, com seu impacto estimado. Sendo a primeira a probabilidade de uma ameaça vir a explorar uma vulnerabilidade e o risco medido em uma escala de 0 a 8, conforme abaixo:

	Probabilidade do cenário de incidente	Muito Baixa (Muito improvável)	Baixa (Improvável)	Média (Possível)	Alta (Provável)	Muito Alta (Frequente)
Impacto ao Negócio	Muito Baixo	0	1	2	3	4
	Baixo	1	2	3	4	5
	Médio	2	3	4	5	6
	Alto	3	4	5	6	7
	Muito Alto	4	5	6	7	8

A metodologia apresentada pelo IAPP (https://iapp.org/resources/article/personal-data-breach-severity-assessment-methodology/), por sua vez, determina que os principais critérios considerados no momento de avaliação da severidade de um incidente são:
- O Contexto do Tratamento de Dados (DPC): Este define o tipo de dado envolvido no incidente, assim como diversos fatores relacionados ao contexto do tratamento;
- A Facilidade de Identificação (EI): Este define a facilidade de

	identificar a identidade dos indivíduos através dos dados envolvidos no incidente; e - As circunstâncias do incidente (CB): Define as circunstâncias específicas do incidente, relacionadas ao tipo do mesmo, incluindo a perda de segurança dos dados envolvidos, assim como alguma intenção maliciosa. Com base nos critérios acima, a metodologia segue a seguinte abordagem: O Contexto do Tratamento é o núcleo da metodologia e avalia o quão críticos são os dados em um contexto de tratamento específico. A Facilidade de identificação é o fator de correção do contexto, de modo que o valor desta pode diminuir o quão críticos os dados são. As circunstâncias do incidente, por sua vez, quantificam as circunstâncias específicas do vazamento que podem estar presentes ou não em uma situação específica. Estas circunstâncias só aumentam a severidade do incidente. Para determinar o valor final da gravidade do incidente, a seguinte fórmula seria utilizada: Gravidade = DPC x EI + CB. O resultado, por sua vez, pertence a um dos quatro níveis de gravidade, sendo eles: baixo, médio, alto e muito alto. Ao fim da avaliação, outros critérios relevantes, como quantidade de indivíduos e inteligibilidade dos dados são levados em consideração e apresentados à autoridade. O documento apresenta uma série de pontuações para valoração dos critérios acima, servindo para quantificar seu valor de forma objetiva e enquadrá-lo na seguinte tabela de gravidade:

	<table><tr><th colspan="3">Severity of a data breach</th></tr><tr><td>SE < 2</td><td>Low</td><td>Individuals either will not be affected or may encounter a few inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).</td></tr><tr><td>2 ≤ SE < 3</td><td>Medium</td><td>Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).</td></tr><tr><td>3 ≤ SE< 4</td><td>High</td><td>Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by banks, property damage, loss of employment, subpoena, worsening of health, etc.).</td></tr><tr><td>4 ≤ SE</td><td>Very High</td><td>Individuals may encounter significant, or even irreversible, consequences, which they may not overcome (financial distress such as substantial debt or inability to work, long-term psychological or physical ailments, death, etc.).</td></tr></table> https://iapp.org/resources/article/personal-data-breach-severity-assessment-methodology/
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	Após a comunicação do incidente de segurança, entendemos que a ANPD poderá determinar medidas que auxiliem na proteção do titular de dados pessoais, possibilite a investigação e resolução do incidente pelos controladores e auxilie a própria Agência na apuração do incidente ocorrido. Assim, entendemos que as medidas abaixo poderão ser cabíveis: ● Documentação do incidente de segurança; ● Apresentação do(s) plano(s) de resposta a incidentes e remediação; ● Envio de notificação aos titulares de dados pessoais, se cabível; ● Envio de notificação a órgãos de proteção do consumidor (e.g. PROCON); ● Apresentação das medidas efetivamente tomadas pelos controladores após a constatação do incidente de segurança (ex: paralisação da atividade de tratamento de dados,

	suspensão de acessos ao sistema do controlador, bloqueio de acessos, eliminação de dados pessoais).

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: Luciane Joana Quipers

CPF/CNPJ: [redacted]

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS **IMPORTANTE:** Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	**Quando ocorre o vazamento de dados considerados sensíveis e que estes possam identificar ou tornar a pessoa identificável, visto que, geralmente são utilizados em práticas discriminatórias. Um critério a ser utilizado é justamente a conceituação de dado pessoal sensível prevista no art. 5º, inciso II da LGPD, de modo que, ocorra a sua interpretação restritiva, ou seja, considerado rol taxativo, visando facilitar a sua identificação, não havendo margem para interpretações.** **Com relação ao vazamento de dados pessoais comuns, demonstra-se risco ou dano relevante quando há o vazamento de informações atinentes às restrições de acesso, como por exemplo, usuário, senhas, PINs, frases de acesso, etc., visto que tais dados possibilitam o acesso a eventuais outros dados dos quais não se tem conhecimento sobre sua natureza. Portanto, um incidente pode acarretar risco ou dano relevante ao titular quando na ocasião, o titular fica exposto às práticas discriminatórias, que possam lhe causar abalo moral e/ou dano patrimonial, por exemplo, e quando os dados afetados possam proporcionar o acesso a outros dados e informações pessoais do titular .**
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	**Sim. A distinção dos níveis pode ocorrer através da análise da natureza dos dados afetados, se são sensíveis, se pertencem a criança ou adolescente e se são comuns, neste último, verificar se podem ser utilizados para acesso a outros dados pessoais. Risco ou dano baixo não deve ser considerado relevante, pois neste caso tais dados apesar de identificar ou tornar a pessoa identificável, tais dados não serão úteis para práticas criminosas ou discriminatórias por exemplo, podendo-se considerar de baixo risco, o incidente que afete a data de nascimento, filiação, nomes dos avós, grau de escolaridade, etc. dados que se demonstrem de fácil acesso por todos, inclusive em redes sociais, podendo-se incluir os**

	dados em que o próprio titular os torna públicos, ao passo que, não haveria necessariamente nexo de causalidade com o incidente.
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	**A distinção entre estes termos pode ser realizada através da sua própria conceituação (fonte: https://webcache.googleusercontent.com/search?q=cache:8POnnss7_ucJ:https://www.dicio.com.br/risco/+&cd=10&hl=pt-BR&ct=clnk&gl=br), de modo que, o risco represente a probabilidade de dano, quando ocorre o vazamento de dados que potencialmente possam causar lesão ao titular, como, por exemplo, informações atinentes ao login de acesso, senhas, PINs, frases utilizadas para recuperação de senha, etc. Já, o dano se refere há possíveis cenários em que os dados pessoais foram totalmente perdidos, não sendo possível sua recuperação nem mesmo através de backups, não podendo haver uma retomada dos serviços, de modo que lhe cause suficientemente prejuízo, como por exemplo, a paralisação na prestação de um serviço essencial por consequência direta do incidente. Os conceitos se relacionam justamente pela estreita diferenciação, pois ambos são hipóteses de lesão ao titular, contudo, o risco se refere à possibilidade, e o dano ao prejuízo concreto. Além disso, em um incidente em um primeiro momento, pode-se ter apenas um risco ao titular, mas em seu desenrolar pode tornar-se um dano, já que um é consequência do outro.**
O que deve ser considerado na avaliação dos riscos do incidente?	**1. É possível recuperar os dados afetados, ou sua destruição, perda ou alteração é permanente? Como por exemplo, a recuperação através de backup.** **2. A natureza dos dados afetados (dados comuns, sensíveis, de criança ou adolescente);** **3. Analisar se estes dados ofertam acesso a outros dados ou informações que não possam ser resguardadas;** **4. A categoria dos dados se pertencem aos funcionários, aos prestações de serviço, a instituições financeiras;** **5. Se o dado afetado apesar de comum dependendo do contexto em que está inserido possa acarretar lesão ao titular, como por exemplo, documento que contém apenas o nome do titular, que é uma informação pública, em um cadastro de portadores de HIV, ou outras doenças infectocontagiosas, conforme Teoria do Mosaico de Fulgêncio Madrid Conesa.**
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	**1. Se o titular dos dados foi comunicado acerca do incidente, e a forma em que houve esta comunicação;** **2. Se houve a identificação do responsável pelo incidente em caso se conduta criminosa;** **3. Quando e como ocorreu o incidente;** **4. Quando o controlador/operador obteve conhecimento sobre o incidente;**

	5. Se eventualmente outra autoridade foi informada acerca do incidente, como por exemplo, organismos de defesa do consumidor, conforme art. 18, §8º da LGPD; **6. Se o incidente tornou-se notório, de modo que há sua repercussão publicamente, como por exemplo, na internet, imprensa e outros veículos de comunicação;** **7. Se os dados afetados no incidente pertencem a alguma autoridade que possa causar maiores prejuízos à população no geral, de modo que envolva interesse público nas informações;** **8. Quando possível, o cálculo dos prejuízos com o incidente, como por exemplo, a paralisação de serviços, inclusive públicos em decorrência do incidente;**
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	**Um prazo razoável para comunicação à ANPD é de 72h, conforme previsto no art. 33, inciso I da GDPR, isso por que, em caso de incidente tem-se como primordial o desempenho de ações para remediação e contenção do incidente e minimização dos riscos e prejuízos, de modo que, em um segundo momento ocorra a comunicação ao titular, dentro do prazo de 48h, tendo em vista ser o principal interessado na segurança e proteção dos dados pessoais, e posteriormente a comunicação à ANPD para que obtenha conhecimento acerca do incidente e das informações necessárias para a apuração das eventuais responsabilidades. Ou seja, inicialmente é preciso que os esforços sejam direcionados à contenção e erradicação do ataque/ameaça, evitando-se maiores prejuízos.**
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	**Um prazo razoável para comunicação ao titular é de até 2 (dois) dias úteis, conforme já previsto no art. 18, §1º do Decreto nº 9.936/19, de modo que não seja o mesmo prazo de comunicação à ANPD, justamente para que ele mesmo possa agir e se preparar para eventuais consequências do incidente, como por exemplo, a troca de senhas quando há o envolvimento deste tipo de informação, ou atento à sinais que seus dados estejam sendo utilizados de forma indevida. As informações que possam constar na comunicação são as que constam no § 1º do art. 48 da LGPD, assim como eventuais sugestões de conduta do próprio titular para que possa se precaver.**
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet	**A forma de comunicação precisa estar relacionada com a quantidade de titulares afetados, de modo que, quantidades menores possibilitem a comunicação individual, e quantidades maiores, diante da necessidade de comunicação em tempo hábil seja possível a comunicação coletiva, através de publicação no sítio eletrônico do controlador, por exemplo. Um dos parâmetros para definir este montante, pode ser o porte empresarial do controlador, visto que, incidentes que envolvam muitos titulares há uma demanda maior de quadro pessoal para realizar a comunicação individual, sendo assim, precisa haver a proporcionalidade entre titulares e possibilidade de comunicação hábil e efetiva. Contudo, a**

etc.)?	**divulgação de nota à imprensa, não se demonstra "merecida" neste momento, já que seria uma espécie de publicização do incidente que é justamente uma das sanções administrativas (art. 52, inciso IV da LGPD), não haveria deste modo, o devido processo legal, acarretando em inúmeros prejuízos aos agentes de tratamento.**
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	**Quando apesar da ocorrência do incidente, este houver sido prontamente solucionado dentro do período de comunicação de 72h, sendo, contudo, necessário que a organização possa comprovar que o incidente foi solucionado e que não apresente mais nenhum risco aos titulares mantendo estas informações e documentos comprobatórios arquivados para fins de consulta caso seja necessária a sua demonstração à ANPD.**
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	**Não há motivos para não informar o titular quando o incidente possa lhe causar risco ou dano relevante, visto que os dados são de sua propriedade demonstrando-se o principal interessado, podendo auxiliar até mesmo na diminuição dos impactos que possam ser ocasionados pelo incidente, sendo imprescindível que saiba sobre as condições que se encontram suas informações.** **A única exceção seria justamente quando o incidente não possa lhe causar risco ou dano relevante, devendo ser utilizado os parâmetros a serem definidos pela autoridade nacional, justamente para ser utilizado como "régua" na orientação a cerca da (des)necessidade de comunicação, não havendo posteriormente possibilidade de qualquer foram de punição dos agentes de tratamentos, visto que agiram dentro da legalidade.**
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	**Para a análise da gravidade do incidente de segurança, um dos critérios a ser analisado se encontra na categoria e na natureza dos dados pessoais envolvidos no incidente em conjunto com o contexto em que ocorria o tratamento destes dados, justamente para analisar o potencial destes dados em eventual utilização maliciosa. Outro critério que poderia ser utilizado é se em caso de perdimento destes dados, por perda, destruição ou alteração, se é possível o seu resgate através de backups, ou outro mecanismo de cópia de segurança, visto que em alguns casos o perdimento dos dados pessoais é tão prejudicial quanto a sua utilização maliciosa, como por exemplo, dados relativos à saúde do titular, ou outros que possam ser utilizados como uma espécie de histórico para posterior utilização pelo titular, de modo que possam interferir no exercício de seus direitos fundamentais, como à saúde, por exemplo.**
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	**Não.**

Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	**Como providência administrativa, a documentação de todo o processo de contenção e erradicação do incidente, de modo a comprovar que foram tomadas todas as medidas cabíveis para a resolução do incidente, visando a minimização dos riscos e danos aos titulares, resguardados os segredos comercial e industrial.** **Sugestões técnicas por parte da ANPD seriam muito importantes, pois nem todo Controlador possui o conhecimento necessário para agir nesse momento. Seria interessante a confecção de um manual de sugestões tendo por base os incidentes de segurança que já ocorreram, como uma forma de compilar possíveis "soluções" a determinados incidentes, pois a final de contas, com esta prática se estará auxiliando pequenos e médios empresários, protegendo de forma "preventiva" os titulares dos dados, e coibindo práticas criminosas, quando o incidente se der por ato ilícito.** **Ainda se demonstra totalmente válida a elaboração de uma espécie de manual de boas práticas, onde constem ações preventivas, como identificar um incidente de segurança, pois muitos empresários de porte pequeno ou médio se quer sabem o que é um incidente de segurança, muito menos o que fazer para contê-lo e consequentemente como resguardar os direitos dos titulares.**

ANPD Autoridade Nacional de Proteção de Dados

ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: MORAIS ANDRADE, LEANDRIN, MOLINA SOCIEDADE DE ADVOGADOS

CPF/CNPJ: 36.192.399/0001-05

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

Considerando a abertura de tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, e diante da necessidade de a ANPD regulamentar alguns itens, como prazo, o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD, viemos por meio deste na condição de especialistas na temática de proteção de dados contribuir com comentários e considerações da experiência internacional, como entendimentos de autoridades de proteção de dados europeias e padrões internacionais de segurança da informação.

Para tanto, cabe ressaltar que a experiência europeia de proteção de dados pessoais, iniciada em 1985 e atualmente fundada em regulamento que teve sua vigência iniciada ainda em 2018, o General Data Protection Regulation (GDPR). O atual Regulamento Europeu além de ser a inspiração do texto da LGPD, possui entendimentos e ações das autoridades europeias como experiências consideradas

relevantes, e por isso, foram bastante consideradas e observadas pelas empresas brasileiras como boas práticas, enquanto aguardavam os entendimentos da própria Autoridade Brasileira (ANPD).

Como exemplo destes tipos de atuação a ser observado, pode-se citar a Autoridade Nacional de Proteção de Dados Pessoais do Reino Unido, Information Comissioner´s Office (ICO), a qual criou diversos checklists de operacionalização do GDPR, tendo inclusive elaborado um focado na questão da segurança da informação[1].

Em relação aos padrões internacionais, citamos a família ISO 27000, que assim como outros padrões de segurança, determina conceitos, estabelece estratégias, incentiva boas práticas, revelando uma abrangente cobertura às questões de segurança da informação. O que enfatiza a importância do incentivo a sua adesão como meio comprobatório de conformidade com os padrões mínimos de segurança da LGPD em caso de necessidade de prestação de contas, como no caso de eventual fiscalização por incidente de segurança da informação.

O procedimento de certificação traz aos que a este se submetem (i) confiança por parte do mercado, dos titulares de dados pessoais e pelas autoridades europeias; (ii) cria vantagem competitiva dentro do mercado pela transparência que a certificação garante; (iii) garante um processo de auditoria especializado e internacionalmente padronizado; (iv) reduz riscos de ataques cibernéticos e falhas humanas e (v) serve como parâmetro de validação para a transferência internacional de proteção de dados pessoais

Ademais, em termos de segurança da informação, além de reconhecido internacionalmente, o padrão ISO ganhou ainda mais relevância ao ser citado pelo o European Data Protection Board (EDPB), órgão da União Europeia que emite orientações sobre proteção de dados pessoais, em parecer proferido por este sobre os critérios necessários a serem atendidos em uma certificação[2].

Sendo assim, diante do argumentado, defendemos abaixo a aplicação de entendimentos do GDPR, decisões das Autoridades Europeias, padrões internacionais, e o incentivo à adesão a certificações como forma de boas práticas e prestação de contas em face de eventual incidente de dados pessoais perante a Autoridade Nacional de Proteção de Dados Pessoais.

CONTRIBUIÇÕES RECEBIDAS

[1] Disponível em https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/#2, acessada em 23 de março de 2021.
[2] Disponível em https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_en.pdf, acessada em 23 de março de 2021.

IMPORTANTE: Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	Para entender se o incidente possui risco ou dano relevante ao titular, conforme entendimento da Autoridade de Proteção de Dados Pessoais do Reino Unido, *Information Comissioner´s Office* (ICO), é importante que o Controlador realize avaliação do incidente, a partir da análise da gravidade do impacto potencial ou real sobre os indivíduos e a probabilidade de isso ocorrer. Seguindo esse critério, se o impacto da violação for mais grave, o risco será maior; e se a probabilidade das consequências for maior, novamente o risco é maior.[3] Além disso, aponta a ICO que pode ser levantada a possibilidade de risco ou dano relevante do titular se o incidente for suscetível de resultar em um alto risco para os direitos e liberdades dos indivíduos, e nesse caso, as medidas de comunicação devem acontecer imediatamente, sem atrasos[4]. Assim, para uma adequada análise do risco ou dano, será necessário que a Autoridade entenda a gravidade do impacto potencial ou real e a probabilidade de o incidente acontecer. Caso o resultado se demonstre alto, e consequentemente, se configure como alto risco para os direitos e liberdades dos indivíduos, o incidente deverá ser classificado como risco ou dano relevante ao titular.

[3] Disponível em https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/, acessada em 23 de março de 2021.

[4] Disponível em https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/, acessada em 23 de março de 2021.

O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	Para uma melhor dosimetria das medidas sancionatórias, será necessário realizar a subdivisão em categorias dos incidentes. Os níveis necessariamente devem levar em consideração a extensão do dano (seja por quantidade de titulares afetados ou tamanho da base de dados envolvida) e as condições de segurança da informação da empresa responsável pelo incidente. A distinção dos níveis deverá ser feita a partir da análise do resultado da violação e a sua probabilidade de ocorrer, sendo assim, através disso, encontrado o impacto real sobre os indivíduos envolvidos. Quando ambos os critérios forem considerados altos, consequentemente, o dano será alto, conforme descrito acima. No caso de riscos e danos classificados como baixos, entendemos que estes não podem ser considerados relevantes, esta consideração implicaria que o Agente de Tratamento diante de um incidente de baixo risco e dano tivesse a obrigação de notificar os titulares envolvidos e a Autoridade. À luz do previsto no art.34, 3, a) e b), do GDPR, as duas hipóteses abaixo poderiam ser consideradas como de ausência de risco ou risco baixo, não implicando na necessidade de notificação, a saber: - quando, em caso de incidente, o agente de tratamento tiver aplicado medidas de proteção adequadas e estas medidas tiverem sido eficientes em tornar os dados pessoais incompreensíveis para qualquer pessoa não autorizada a acessá-los, tais como a cifragem; - quando, em caso de incidente, o agente de tratamento tiver tomado medidas subsequentes que assegurem que o elevado risco não seja mais passível de concretização.
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	Em breve descrição, o risco trata da probabilidade de determinada situação se concretizar, enquanto o dano é a concretização da determinada situação. O relacionamento entre os dois conceitos consiste no fato de que o risco é a análise e tentativa de previsão do dano. A diferenciação desses conceitos é importante para que a penalização somente aplicada pelo dano efetivo, e não somente pela configuração do risco (potencial danoso). O GDPR (considerando 85), exemplifica tipos de danos e eventuais riscos causados por uma possível violação de dados pessoais, de modo que são enumerados: (i) perda de controle sobre os seus dados pessoais; (ii) a limitação de direitos, a discriminação, o roubo ou usurpação da identidade, perdas financeiras, a inversão não autorizada da pseudonimização, danos para a reputação, a perda

	de confidencialidade de dados pessoais protegidos por sigilo profissional ou qualquer outra desvantagem econômica ou social significativa das pessoas físicas.
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º) O que deve ser considerado na avaliação dos riscos do incidente?	Os possíveis critérios a serem adotados devem necessariamente considerar: (i) segurança da informação (infraestrutura e investimentos de hardware e software etc); (ii) governança de dados pessoais da empresa (conscientização através treinamentos, políticas internas etc); (iii) conformidade com requisitos da legislação de proteção de dados pessoais; (iv) volume de dados tratados; (vi) categoria de dados tratados (cadastrais; sensíveis; crianças e adolescentes, etc.); (v) tamanho do agente de tratamento de dados (PME ou Grandes Empresas) e (vi) capacidade técnica do agente de tratamento reverter e/ou minimizar o dano causado. Para tanto, a própria ISO 27001:2013, em seu controle A. 16.1.7 aponta as evidências para avaliação do incidente de segurança que poderiam ser consideradas em eventual análise da Autoridade, sendo eles: "Convém que os procedimentos levem em conta: a) cadeia de custódia; b) segurança da evidência; c) segurança das pessoas; d) papéis e responsabilidades das pessoas envolvidas; e) competência do pessoal; f) documentação; g) resumo do incidente. Convém que, onde disponível, certificação ou outros meios relevantes de qualificação de pessoal e ferramentas sejam buscados, para reforçar o valor da evidência preservada." Ainda sobre o controle A.16 da ISO27001:2013 é possível aplicar os critérios de seguranças mínimos determinados para avaliação dos riscos do incidente. Sendo eles: "Convém que as seguintes diretrizes para o gerenciamento de responsabilidades e procedimentos com relação à gestão de incidentes de segurança da informação sejam consideradas:

	a) convém que responsabilidades pelo gerenciamento sejam estabelecidas para assegurar que os seguintes procedimentos sejam desenvolvidos e comunicados, adequadamente, dentro da organização: 1) procedimentos para preparação e planejamento a resposta a incidente; 2) procedimentos para monitoramento, detecção, análise e notificação de incidentes e eventos de segurança da informação; 3) procedimentos para registros das atividades de gerenciamento de incidentes; 4) procedimentos para manuseio de evidências forenses; 5) procedimentos para avaliação e decisão dos eventos de segurança da informação e avaliação de fragilidades de segurança da informação; 6) procedimentos para resposta, incluindo aquelas relativas à escalação, recuperação controlada de um incidente e comunicação as pessoas ou organizações, internas e externas; b) convém que os procedimentos estabelecidos assegurem que: 1) pessoal competente trate as questões relativas a incidentes de segurança dentro da organização; 2) um ponto de contato para notificação e detecção de incidentes de segurança esteja implementado; 3) contatos apropriados sejam mantidos com autoridades, grupos de interesses externos ou fóruns que tratem de questões relativas a incidentes de segurança da informação; c) convém que procedimentos de notificação incluam: 1) preparação de formulários de notificação de evento de segurança da informação para apoiar as ações de notifi cação e ajudar a pessoa que está notificando, lembrando de todas as ações necessárias no caso de um evento de segurança da informação; 2) o procedimento a ser realizado no caso de um evento de segurança da informação, por exemplo, relatar todos os detalhes imediatamente, como tipo de não conformidade ou violação, ocorrências de mau funcionamento, mensagens na tela; e imediatamente notificar ao ponto de contato, tomando apenas ações coordenadas; 3) referência a um processo disciplinar formal estabelecido para tratar com funcionários que cometam violações de segurança da informação; 4) processo de realimentação adequado para assegurar que aquelas pessoas que notificaram um evento de segurança da informação seja informado dos resultados após o assunto ter sido tratado e encerrado.

	Convém que os objetivos para a gestão de incidentes de segurança da informação sejam acordados com a direção e garantam que as pessoas responsáveis pela gestão dos incidentes de segurança da informação entendem as prioridades da organização para tratar com os incidentes de segurança da informação." Além disso, de acordo com entendimento da Autoridade Nacional de Proteção de Dados Pessoais do Reino Unido, *Information Commissionar's Office* (ICO), o foco do risco em relação ao relatório de violação está nas possíveis consequências negativas para os indivíduos.[5] Desta forma, um dos principais pontos de avaliação do incidente deve considerar principalmente os impactos negativos aos titulares de dados. Em complementação, o considerando 85 do GDPR[6] aponta que quando um incidente de segurança ocorre, é necessário estabelecer rapidamente se ocorreu uma violação de dados pessoais e, em caso positivo, imediatamente tomar medidas para solucioná-la, sendo indispensável que para avaliação do risco, seja considerado como critério de avaliação as medidas corretivas e emergenciais para remediação do incidente descoberto. Outro parâmetro a ser levado em consideração para análise de risco, são os parâmetros de segurança da informação adotados pelo Controlador. Para tanto, a ICO desenvolveu checklists com parâmetros mínimos para direcionar o processo de adequação com a legislação de proteção de dados, sendo alguns deles: ☐ Realiza-se uma análise dos riscos apresentados pelo nosso processamento e usamos isso para avaliar o nível de segurança apropriado que precisamos implementar. ☐ Ao decidir quais medidas implementar, levou-se em consideração o estado da arte e os custos de implementação.

[5] Disponível em https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/#riskassessingdata acessado em 23 de março de 2021.

[6] Disponível em https://www.privacy-regulation.eu/en/recital-85-GDPR.htm#:~:text=(85)%20A%20personal%20data%20breach,financial%20loss%2C%20unauthorised%20reversal%20of acessado em 23 de março de 2021.

	☐ Há uma política de segurança da informação (ou equivalente) e tomamos medidas para garantir que a política seja implementada. ☐ Sempre que necessário, há políticas adicionais e garantias da existência de controles para aplicá-las. ☐ Assegura-se a revisão regular das políticas e medidas de segurança da informação e, quando necessário, o aprimoramento destas. ☐ Implementa-se controles técnicos básicos, como os especificados por estruturas estabelecidas, como o Cyber Essentials. ☐ Entende-se como necessária a implementação de outras medidas técnicas, dependendo das circunstâncias e do tipo de dados pessoais processados. ☐ Utilização de criptografia e / ou pseudonimização quando for apropriado. ☐ Entendimento dos requisitos de confidencialidade, integridade e disponibilidade para os dados pessoais processados. ☐ Garantia da restauração do acesso a dados pessoais em caso de incidentes, como por exemplo, estabelecendo um processo de backup apropriado. ☐ Realização de testes e revisões regulares das medidas para garantir que estas permaneçam eficazes e atuamos nos resultados desses testes, onde destacam as áreas a serem melhoradas[7]. Já a autoridade francesa de proteção de dados pessoais, CNIL, oferece três níveis de programas de segurança que estejam de acordo com o GDPR, os três são baseados em 17 pontos orientativos, sendo estes[8]:

[7] Disponível em https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security/#2, acessada em 23 de março de 2021, traduzida livremente.
[8] Disponível em https://www.cnil.fr/fr/principes-cles/guide-de-la-securite-des-donnees-personnelles, acessada em 23 de março de 2021, traduzida livremente.

	• Educação dos usuários • Autenticação dos usuários • Gerenciamento das autorizações • Rastreamento do acesso e Gerenciamento dos Incidentes • Proteção das Estações de Trabalho • Proteção da Computação Móvel • Proteção da Rede Interna de TI • Segurança dos Servidores • Sites Seguros • Continuidade dos negócios (back ups) • Arquivamento com segurança • Supervisão da manutenção e destruição de dados • Gerenciamento da Terceirização • Trocas seguras com outras organizações • Proteção das instalações • Supervisão do Desenvolvimento de TI • Criptografia, garantia da integridade, assinatura E por fim, ressalta-se que além das boas práticas apontadas na própria LGPD, o GDPR em seu artigo 32 também estabelece parâmetro mínimos de segurança da informação que podem ser considerados na avaliação de risco, sendo eles:

	a) A pseudonimização e a cifragem dos dados pessoais; b) A capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento; c) A capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico; d) Um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento.
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	Além das informações já listadas no §1° do art. 48, considerando a experiência europeia, o GDPR em seu artigo 33(3), que trata das informações necessárias para notificação da Autoridade, se destacam como pertinentes a solicitação de informações sobre (i) quando e como foi descoberta a violação; e (ii) indicação de quem é contato para mais informações, seja ele, o encarregado de dados ou outro ponto de contato que seja capaz de fornecer as informações necessárias. Isso pois a capacidade do Controlador de identificar o acontecimento da violação trará para a ANPD um parâmetro sobre a própria infraestrutura de segurança do Controlador, e apesar da comunicação ser entendida como competência do encarregado de dados, e provavelmente ocorrer por meio deste, a sua apresentação formal em meio a notificação é importante para uma comunicação mais transparente e para garantir mais eficiência no processo fiscalizatório.
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	Nos termos da Autoridade Nacional de Proteção de Dados Pessoais do Reino Unido, *Information Commissionar's Office* (ICO), no caso de a possibilidade de uma violação resultar em um alto risco para os direitos e liberdades dos indivíduos, o GDPR diz que o Controlador deve informar os interessados diretamente e sem atrasos indevidos. Em outras palavras, isso deve ocorrer o mais rápido possível.

	Contudo, visando uma melhor regulamentação, o GDPR determina em seu artigo 33 (1) e considerando 85[9], como um prazo razoável para comunicação sobre o incidente de segurança da informação o prazo de 72 horas[10]. O prazo estipulado garante que no caso de subcontratação, e tendo o dano se originado da subcontratação, possibilita que a subcontratada tenha ao menos um dia para informar o Controlador acerca do incidente, para que então o Controlador possua tempo hábil para informar a Autoridade Nacional.
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48? Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota	Em relação à determinação de prazo, a Autoridade poderá considerar as peculiaridades e particularidade de cada empresa e incidente, como por exemplo, as consequências da violação de dados pessoais, número de pessoas afetadas, dentre outros critérios. Apesar da comunicação individual se configurar como cenário ideal, muitas vezes, diante das dimensões da empresa, urgência na notificação, quantidade de titulares envolvidos e infraestrutura tecnológica da empresa para a comunicação, verifica-se que o esforço para a notificação individual pode se tornar desproporcional e morosa, afetando a transparência e podendo inviabilizar direitos dos titulares, sendo aplicada então a regra da comunicação pública, tal determinação é refletida no artigo 34 (3) c do GDPR. Sobre o conteúdo da notificação, considerando que a comunicação visa dar a oportunidade aos titulares de dados de tomarem medidas de proteção, devem constar as mesmas informações do §1° do artigo 48, com indicação clara do encarregado na empresa para caso o titular de dados precise de informações adicionais.

[9] Disponível em https://www.privacy-regulation.eu/en/recital-85-GDPR.htm#:~:text=(85)%20A%20personal%20data%20breach,financial%20loss%2C%20unauthorised%20reversal%20of acessado em 23 de março de 2021

[10] Article 33(1) GDPR: "Em caso de violação de dados pessoais, o responsável pelo tratamento deve, sem demora injustificada e, se possível, o mais tardar 72 horas após ter tido conhecimento, notificar a violação de dados pessoais à autoridade de supervisão competente nos termos do artigo 55.º, a menos que seja improvável que a violação de dados pessoais resulte em risco para os direitos e liberdades das pessoas físicas. Se a notificação à autoridade de controlo não for feita no prazo de 72 horas, deve ser acompanhada da justificação do atraso."

à imprensa, publicação na internet etc.)?	
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	Conforme apontado nos questionamentos acima, a comunicação ao titular deverá ser considerada obrigatória somente quando o risco for elevado ou o dano for relevante. Entendendo-se que não haveria risco elevado ou dano relevante, a exemplo da experiência do GDPR, especificamente em seu artigo 34(3), quando: (i) O responsável pelo tratamento tiver aplicado medidas de proteção adequadas, tanto técnicas como organizativas, e essas medidas tiverem sido aplicadas aos dados pessoais afetados pela violação de dados pessoais, especialmente medidas que tornem os dados pessoais incompreensíveis para qualquer pessoa não autorizada a aceder a esses dados, tais como a cifragem; e (ii) o responsável pelo tratamento tiver tomado medidas subsequentes que assegurem que o elevado risco para os direitos e liberdades dos titulares dos dados já não é suscetível de se concretizar. No mais, caso a notificação individual dos envolvidos implique em um esforço desproporcionado, poderá ser aceita a comunicação pública ou tomada uma medida semelhante através da qual os titulares dos dados são informados de forma igualmente eficaz.
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	Existem diversas metodologias para análise de risco e incidentes em matéria de segurança da informação, a sua adoção depende do modelo de negócio e da gestão da própria empresa. As metodologias em geral possuem o mesmo objeto, que é realizar uma análise de risco e criticidade quando aplicados no âmbito da segurança da informação, mais precisamente em relação aos incidentes de segurança da informação. Dentre elas, cabe mencionar o método GUT[11] (Gravidade, Urgência e Tendência) é um método utilizado para definir prioridades e para solução de problemas. Os campos considerados na análise são: **Gravidade**: intensidade/profundidade dos danos que o incidente pode causar se não resolvido (índice de 1 (dano mínimo) a 5 (extremamente grave)); **Urgência**: considera o tempo para a eclosão de danos caso o dano não seja resolvido (índice de 1 (prazo longuíssimo – 2+ meses) a 5 (ação imediata));

[11] Disponível em https://www.pmtech.com.br/PMP/Dicas%20PMP%20-%20Matriz%20GUT.pdf acessado em 23 de março de 2021

	Tendência: Tendência da evolução da situação (índice de 1 (desaparece com o tempo) a 5 (piora muito rapidamente)). Entendidos os elementos da matriz, a criticidade é resultado do cálculo de GUT = Gravidade + Urgência + Tendência. Considerando a existência de diversas metodologias, ressalta-se que a utilização das metodologias para análise de gravidade de incidente de segurança deveriam ser consideradas boas práticas, e caso devidamente comprovadas, poderiam contribuir com a redução nas aplicações de sanções em caso de incidente de segurança.
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	Entendemos que sugestões de providências pela Autoridade devem ser direcionadas individualmente para cada evento/risco ocorrido, as medidas técnicas e administrativas devem necessariamente estar em conformidade com as particularidades do evento, principalmente, pois eventual ação corretiva depende diretamente do risco e do impacto, conforme apontado no questionamento acima.

Fernando H. Anadão Leandrin OAB/SP 286.561 | Lygia Maria M. Molina OAB/SP 317.166 | Marcelo Chiavassa OAB/SP 305.354

ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: NBF|A (NEIVA, BARROS & FIGUEIRÓ SOCIEDADE DE ADVOGADOS)

CPF/CNPJ: 13.314.640/0001-18

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS **IMPORTANTE:** Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	Sem comentários
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	Sem comentários
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	Do ponto de vista semântico, risco e dano se diferenciam na medida em que o primeiro se relaciona à *probabilidade* de perigo (ou dano) e o segundo se relaciona à ocorrência *concreta* de um dano. Reguladores europeus têm produzido interessante material a respeito dos conceitos de risco e dano no âmbito de seus programas de proteção de dados pessoais, diferenciando e correlacionando ambos os conceitos sob a perspectiva da privacidade e proteção de dados pessoais. Por exemplo, a Agência Espanhola de Proteção de Dados Pessoais ("**AEPD**") produziu o *Guia de Análise dos Riscos nos Tratamentos de Dados Pessoais*[1], no qual define que "*O risco deriva da exposição a ameaças, portanto, a partir de uma perspectiva de privacidade, é essencial compreender o que é uma ameaça e como identificar cenários de risco para os dados pessoais a partir dela.*

[1] Versão em espanhol disponível em: https://www.aepd.es/sites/default/files/2019-09/guia-analisis-de-riesgos-rgpd.pdf. Acesso em 23 de março de 2021.

	Continua a AEPD ao definir que "*uma ameaça é qualquer fator de risco com o potencial de causar danos ou prejuízos aos titulares cujos dados pessoais são tratados*". A autoridade espanhola estabelece ainda 3 categorias de ameaças: (i) Acesso ilegítimo aos dados pessoais (ameaça à confidencialidade); (ii) Modificação não autorizada dos dados pessoais (ameaça à integridade); e (iii) Eliminação não autorizada dos dados pessoais (ameaça à disponibilidade). Para auxiliar no enquadramento das ocorrências em cada uma das categorias acima mencionadas, a AEPD estabeleceu o seguinte teste: (i) Questionar e fazer uma estimativa sobre quais seriam os *danos* aos direitos e liberdades individuais de cada um dos titulares caso alguma das categorias de riscos se concretizasse, relacionando o conceito de *risco* com o conceito de *dano*. (ii) Tal análise permitiria dimensionar a *gravidade* do risco e, por conseguinte, do dano aos titulares de dados pessoais para cada tratamento identificado. (iii) A análise dos riscos e danos tem como ponto de partida os direitos e liberdades individuais dos titulares e não das organizações que tratam dados pessoais. (iv) A análise de risco, ainda, não se limita apenas à possibilidade de dano material, mas sim a *qualquer tipo de dano*, incluindo portanto qualquer tipo de *desvantagem econômica ou social significativa*, nos termos do considerando 75 do Regulamento Geral sobre a Proteção de Dados ("**RGPD**" ou "**GDPR**") europeu[2]. Tal abordagem permite a realização de uma estimativa dos danos e do tipo de danos que podem ser causados aos titulares[3].

[2] Disponível em https://gdpr-info.eu/recitals/no-75/. Acesso em 23 de março de 2021.
[3] A obrigação de analisar o risco com base no exercício lógico acima descrito é tratada em diversos dispositivos da GDPR, quais sejam: arts. 24, 25, 32 a 35 e 39. O texto completo pode ser acessado em: https://gdpr-info.eu/. Acesso em 23 de março de 2021.

	Adicionalmente, a análise do risco a partir dos direitos e liberdades individuais de cada titular está presente em outros regulamentos europeus. A Lei Orgânica de Proteção de Dados ("LOPD GDD") espanhola, por exemplo, define o princípio da responsabilidade ativa, que exige uma avaliação prévia pelos responsáveis e encarregados para a determinação de medidas técnicas e administrativas de mitigação de riscos. As organizações devem levar em conta, principalmente, quando o tratamento puder gerar situações de discriminação; *identity theft*; privar os titulares de seus direitos e garantias individuais; envolver a criação de perfis, entre outros (art. 28 da LOPD GDD). Disponível em: https://www.boe.es/boe/dias/2018/12/06/pdfs/BOE-A-2018-16673.pdf. Acesso em 23 de março de 2021.
O que deve ser considerado na avaliação dos riscos do incidente?	Sem comentários
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	Sem comentários
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	Sem comentários
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	Sem comentários
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota	De acordo com o "Guide to GDPR"[4] publicado pelo *Information Commissioner's Office* "**ICO**") do Reino Unido, certos tipos de violações de dados pessoais devem ser informados à autoridade de proteção de dados e, em alguns casos, também para os titulares afetados. Assim, em princípio, diante de um incidente de segurança que traga risco ou dano relevante ao(s) titular(es) dos dados, a definição do meio de comunicação adequado deve ser realizada de acordo

[4] Disponível em: https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr-1-1.pdf. Acesso em 23 de março de 2021

à imprensa, publicação na internet etc.)?	com a gravidade do risco ou dano, determinada a partir da avaliação do incidente (natureza, categoria e quantidade de titulares de dados afetados, categoria e quantidade dos dados afetados, consequências concretas e prováveis), conforme metodologia definida pelo órgão regulador[5]. Concluída tal análise e estabelecida a gravidade do risco ou dano de acordo com o *score* atribuído ao evento é que se pode definir se a comunicação: (i) Terá como destinatário: Apenas a autoridade reguladora, os titulares e/ou o público em geral; (ii) Quanto à forma: a. Se será enviada direta e individualmente, com a forma eletrônica (via e-mail) sendo mais desejável em razão da sua rapidez, evitando atrasos indevidos. Sendo possível adotar também a comunicação por correspondência como opção subsidiária ou complementar à comunicação eletrônica. b. A comunicação pública ou medida semelhante (nota à imprensa, publicação na internet), quando forem exigidas medidas desproporcionais para reverter ou mitigar os efeitos do incidente, bem como for verificado que se trata de risco ou dano relevante (alto/elevado).
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	No GDPR, as exceções à obrigatoriedade de informar o órgão regulador estão diretamente relacionadas à probabilidade de risco aos direitos e liberdades dos titulares. A AEPD, por exemplo, determina que não há necessidade de notificação do incidente de segurança naqueles casos em que seja improvável que a violação represente qualquer risco aos direitos e liberdades individuais. Para adotar um critério objetivo, é possível estabelecer metodologias de cálculo de gravidade do incidente, similar à definida pela Agência Espanhola de Proteção de Dados (AEPD), em seu *Guia para a Gestão e Notificação de Incidentes de Segurança,* comentada na resposta à questão "Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?" abaixo.

[5] Vide resposta à questão "Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?"

Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	Sem comentários
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	Sem comentários
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	A análise de risco é um exercício complexo, tendo em vista que, a depender de quem faça a análise e os critérios adotados, a gravidade do incidente pode ser interpretada como maior ou menor. Tendo em vista isto, bem como o comando geral da GDPR em que a análise da gravidade use parâmetros objetivos, a AEPD emitiu o *Guia para a Gestão e Notificação de Incidentes de Segurança*[6], no qual se estabelece uma metodologia para o cálculo da gravidade do incidente de segurança [7] que leva em consideração os seguintes aspectos/critérios para definir o "*score*" de gravidade do incidente de segurança: (i) Quantidade de dados pessoais afetados (se atribuí uma nota de acordo com a faixa / quantidade de dados, por exemplo, 1ª Faixa: até 100 dados, 2ª Faixa: até 1000 dados, etc); (ii) Categoria dos dados pessoais afetados (dobra-se o valor, caso sejam dados sensíveis); (iii) Exposição dos dados pessoais afetados (se os dados vazaram para dentro da organização ou se foram expostos publicamente, por exemplo – para cada uma dessas hipóteses é atribuído um valor). (iv) Também são definidas algumas "*circunstâncias qualitativas*", espécies de agravantes da gravidade do incidente de segurança. De acordo com a AEPD: (i) Deve ser notificado à agência qualquer incidente que, com a aplicação da metodologia acima, atingir um *score* próximo a 20 e conte com ao menos 2 agravantes.

[6] Disponível em: https://www.aepd.es/sites/default/files/2019-09/guia-brechas-seguridad.pdf. Acesso em 23 de março de 2021.
[7] (Risco = Volume de Dados Afetados x (Categorias de Dados Afetados x Exposição dos Dados)

	(ii) Devem ser notificados os titulares qualquer incidente que, com a aplicação da metodologia acima, atinja um *score* próximo a 40 e conte com ao menos 2 agravantes.
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	Sem comentários
SUGESTÃO DE NORMATIVO, SE HOUVER	
Sem comentários	
Sem comentários	

OURIQUES CRUZ
advocacia empresarial

ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: OURIQUES CRUZ SOCIEDADE INDIVIDUAL DE ADVOCACIA

CPF/CNPJ: 36.572.963/0001-07

TÓPICO/QUESTÃO	CONTRIBUIÇÃO/INSTITUIÇÃO
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	O Regulamento Geral sobre a Proteção de Dados (legislação europeia) aponta que o incidente deverá ser analisado sob alguns requisitos, quais sejam: **(i)** informação sobre o incidente de forma oportuna; **(ii)** se tem potencial de causar dano físico, material ou não material ao titular, como: **(ii.1)** perda do controle dos dados pessoais; **(ii.2)** limitação dos seu direitos; **(ii.3)** discriminação; **(ii.4)** roubo ou fraude; **(ii.5)** perda financeira; **(ii.6)** dano à reputação; **(ii.7)** alteração de dados originais por falsos; **(ii.8)** perda de confidencialidade dos dados protegidos por sigilo profissional; ou **(ii.9)** quaisquer danos que causem desvantagem econômica ou social ao titular[1]; **(iii)** dados de crianças, adolescentes e idosos. Isso porque, tais aspectos estão diretamente ligados a direitos fundamentais (privacidade e intimidade), a dados sensíveis e, no caso do item "iii" acima, a pessoas com certa hipossuficiência no quesito de buscar amparo legal, em decorrência de um vazamento de dados. A ANPD deverá também analisar a extensão do risco/dano, já que é determinante em relação ao impacto do que deve ou não ser feito.

[1] General Data Protection Regulation (GDPR) – Final text neatly arranged. Disponível em: <https://gdpr-info.eu/recitals/no-75/>. Acesso em: 22 mar. 2021.

	Em reforço e utilizando-se de aplicação analógica de regulamentação de outros entes do estado brasileiro, a Instrução CVM nº 505/2011[2], alterada pela Instrução CVM nº 612/2019[3], determina no seu art. 1º, XVI, como *"incidente relevante de segurança cibernética: incidente que afete processos críticos de negócios, ou dados ou informações sensíveis, e tenha impacto significativo sobre os clientes"*. Ou seja, uma vez mais deve-se ponderar o impacto e representatividade do dado vazado para saber sua relevância.
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	Considerando que o tratamento de dados se dá em um sistema operacional, o ponto chave a ser analisado é a forma de atuação do Controlador, ou seja, se este possui uma política de prevenção e Plano de Ação e Resposta, este último para adequar e corrigir os erros que o sistema constatou. Assim, todo dano deve ser avaliado pelo Controlador e devidamente tratado, ainda que não seja necessariamente noticiado à ANPD, conforme limites do art. 48 da LGPD. No tocante ao risco em si, este deve ser analisado pelos Controladores antes de levar à autoridade competente, de modo que a questão da relevância deve ser ponderada com maior atenção, para afastar uma mera ameaça, que seria um risco baixo, de um risco grave, que precisa ser noticiado. Todos esses fatores deverão ser destrinchados na política de privacidade e contenção de incidentes, assim como no plano de ação do próprio Controlador, com amparo nos limites legais e balizas ofertadas pela ANPD. A título de contribuição sobre a parametrização pela ANPD e o que deve conter em um Plano de Ação e Resposta, a Resolução CMN 4658 dispõe que (grifou-se): Art. 6º As instituições referidas no art. 1º devem estabelecer plano de ação e de resposta a incidentes visando à implementação da política de segurança cibernética. **Parágrafo único. O plano mencionado no caput deve abranger, no mínimo:**

[2] CVM. Instrução CVM 505. Disponível em: <http://conteudo.cvm.gov.br/legislacao/instrucoes/inst505.html>. Acesso em: 22 mar. 2021.
[3] CVM. Instrução CVM 612. Disponível em: <http://conteudo.cvm.gov.br/legislacao/instrucoes/inst612.html>. Acesso em: 22 mar. 2021.

	I - as ações a serem desenvolvidas pela instituição para adequar suas estruturas organizacional e operacional aos princípios e às diretrizes da política de segurança cibernética; **II - as rotinas, os procedimentos, os controles e as tecnologias a serem utilizados na prevenção e na resposta a incidentes, em conformidade com as diretrizes da política de segurança cibernética; e** **III - a área responsável pelo registro e controle dos efeitos de incidentes relevantes.** Não obstante, é interessante que haja um parâmetro de classificação de riscos mais objetivos, dado o caráter genérico da lei, o que facilita a aplicação da norma pelos agentes de tratamento e evita comunicados ou informes desnecessários, embora a avaliação final acabe sendo do Controlador.
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	O risco deverá ser analisado pela existência de uma falha no sistema, já o dano deve ser visto pela materialização do risco, ou seja, pelo efetivo vazamento de dados, que se enquadre no primeiro tópico "Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?". Assim, no primeiro caso estamos diante de uma possibilidade/expectativa de dano, no segundo, a efetivação do dano em si.
O que deve ser considerado na avaliação dos riscos do incidente?	Levando em conta que todo sistema é passível de falhas, o que deve ser considerado é a atuação do Controlador, ou seja, se este possuía um sistema de proteção de dados adequado para o serviço que presta e se este atuou de forma diligente para solucionar e comunicar o incidente. Quanto ao sistema adequado, o art. 32 da GDPR, aplicável por analogia e capaz de fornecer um conceito objetivo, dispõe que: **Artigo 32** **Segurança do tratamento** Tendo em conta as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os riscos, de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento e

	o subcontratante aplicam as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco, incluindo, consoante o que for adequado: a) A pseudonimização e a cifragem dos dados pessoais; b) A capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento; c) A capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico; d) Um processo para testar, apreciar e avaliar regularmente a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento. Ao avaliar o nível de segurança adequado, devem ser tidos em conta, designadamente, os riscos apresentados pelo tratamento, em particular devido à destruição, perda e alteração acidentais ou ilícitas, e à divulgação ou ao acesso não autorizados, de dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento. O cumprimento de um código de conduta aprovado conforme referido no artigo 40º ou de um procedimento de certificação aprovado conforme referido no artigo 42º pode ser utilizado como elemento para demonstrar o cumprimento das obrigações estabelecidas no nº 1 do presente artigo. O responsável pelo tratamento e o subcontratante tomam medidas para assegurar que qualquer pessoa singular que, agindo sob a autoridade do responsável pelo tratamento ou do subcontratante, tenha acesso a dados pessoais, só procede ao seu tratamento mediante instruções do responsável pelo tratamento, exceto se tal lhe for exigido pelo direito da União ou de um Estado-Membro. Ainda sobre esse tema, tanto a CVM quanto o BACEN abordam acerca do sistema adequado, deixando evidente a responsabilidade do Controlador em avaliar esses riscos, sem prejuízo de a ANPD dar diretrizes para tanto (grifou-se): **Instrução CVM nº 505/2011**

	Art. 35-H. A política a que se refere o art. 35-D, inciso II, deve contemplar um programa de segurança cibernética, abrangendo, no mínimo: I – a identificação e avaliação dos riscos cibernéticos internos e externos a que o intermediário esteja exposto; II – as medidas que devem ser adotadas para reduzir a vulnerabilidade da instituição contra ataques cibernéticos; III – procedimentos e controles internos que serão adotados para: a) verificar a implementação, a aplicação e a eficácia das medidas adotadas na forma do inciso II; e b) efetuar o monitoramento contínuo e a detecção de ataques cibernéticos em tempo hábil; e IV – medidas que serão adotadas para tratamento de incidentes cibernéticos e recuperação de dados e sistemas; V – periodicidade com que o programa de segurança cibernética será testado e revisado, de forma a: a) avaliar a vulnerabilidade da instituição contra ataques cibernéticos e identificar novos riscos cibernéticos; e b) verificar a necessidade de aperfeiçoar as regras, procedimentos e controles internos existentes; e **Resolução CMN nº 4.658/2018[4]** Art. 2º As instituições referidas no art. 1º devem implementar e manter política de segurança cibernética formulada com base em princípios e diretrizes que busquem assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados. § 1º A política mencionada no caput deve ser compatível com: I - o porte, o perfil de risco e o modelo de negócio da instituição; II - a natureza das operações e a complexidade dos produtos, serviços, atividades e processos da instituição; e

[4] CMN. Resolução 4658. Disponível em: < https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o&numero=4658>. Acesso em: 22 mar. 2021.

	III - a sensibilidade dos dados e das informações sob responsabilidade da instituição. § 2º Admite-se a adoção de política de segurança cibernética única por: I - conglomerado prudencial; e II - sistema cooperativo de crédito. **Art. 3º A política de segurança cibernética deve contemplar, no mínimo:** I - os objetivos de segurança cibernética da instituição; II - os procedimentos e os controles adotados para reduzir a vulnerabilidade da instituição a incidentes e atender aos demais objetivos de segurança cibernética; III - os controles específicos, incluindo os voltados para a rastreabilidade da informação, que busquem garantir a segurança das informações sensíveis; IV - o registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da instituição; V - as diretrizes para: a) a elaboração de cenários de incidentes considerados nos testes de continuidade de negócios; b) a definição de procedimentos e de controles voltados à prevenção e ao tratamento dos incidentes a serem adotados por empresas prestadoras de serviços a terceiros que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da instituição; c) a classificação dos dados e das informações quanto à relevância; e d) a definição dos parâmetros a serem utilizados na avaliação da relevância dos incidentes; VI - os mecanismos para disseminação da cultura de segurança cibernética na instituição, incluindo: a) a implementação de programas de capacitação e de avaliação periódica de pessoal; b) a prestação de informações a clientes e usuários sobre precauções na utilização de produtos e serviços financeiros; e c) o comprometimento da alta administração com a melhoria contínua dos procedimentos relacionados com a segurança cibernética; e VII - as iniciativas para compartilhamento de informações sobre os incidentes relevantes, mencionados no inciso IV, com as demais instituições referidas no art. 1º.

	§ 1º Na definição dos objetivos de segurança cibernética referidos no inciso I do caput, deve ser contemplada a capacidade da instituição para prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético. § 2º Os procedimentos e os controles de que trata o inciso II do caput devem abranger, no mínimo, a **autenticação, a criptografia, a prevenção e a detecção de intrusão, a prevenção de vazamento de informações, a realização periódica de testes e varreduras para detecção de vulnerabilidades, a proteção contra softwares maliciosos, o estabelecimento de mecanismos de rastreabilidade, os controles de acesso e de segmentação da rede de computadores e a manutenção de cópias de segurança dos dados e das informações.** § 3º Os procedimentos e os controles citados no inciso II do caput devem ser aplicados, inclusive, no desenvolvimento de sistemas de informação seguros e na adoção de novas tecnologias empregadas nas atividades da instituição. § 4º O registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes, citados no inciso IV do caput, devem abranger inclusive informações recebidas de empresas prestadoras de serviços a terceiros. **§ 5º As diretrizes de que trata o inciso V, alínea "b", do caput devem contemplar procedimentos e controles em níveis de complexidade, abrangência e precisão compatíveis com os utilizados pela própria instituição.** **Circular BACEN n° 3.978/2020[5]** Art. 2º As instituições mencionadas no art. 1º devem implementar e manter política formulada com base em princípios e diretrizes que busquem prevenir a sua utilização para as práticas de lavagem de dinheiro e de financiamento do terrorismo. I - as diretrizes para: a) a definição de papéis e responsabilidades para o cumprimento das obrigações de que trata esta Circular; b) a definição de procedimentos voltados à avaliação e à análise prévia de novos produtos e serviços, bem como da utilização de novas tecnologias, tendo em vista o risco de lavagem de dinheiro e de financiamento do terrorismo;

[5] BACEN. Circular 3978. Disponível em: <https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Circular&numero=3978>. Acesso em: 22 mar. 2021.

	Art. 10. As instituições referidas no art. 1º devem realizar avaliação interna com o objetivo de identificar e mensurar o risco de utilização de seus produtos e serviços na prática da lavagem de dinheiro e do financiamento do terrorismo. **§ 1º Para identificação do risco de que trata o caput, a avaliação interna deve considerar, no mínimo, os perfis de risco:** I - dos clientes; II - da instituição, incluindo o modelo de negócio e a área geográfica de atuação; III - das operações, transações, produtos e serviços, abrangendo todos os canais de distribuição e a utilização de novas tecnologias; e IV - das atividades exercidas pelos funcionários, parceiros e prestadores de serviços terceirizados. § 2º O risco identificado deve ser avaliado quanto à sua probabilidade de ocorrência e à magnitude dos impactos financeiro, jurídico, reputacional e socioambiental para a instituição. § 3º Devem ser definidas categorias de risco que possibilitem a adoção de controles de gerenciamento e de mitigação reforçados para as situações de maior risco e a adoção de controles simplificados nas situações de menor risco. § 4º Devem ser utilizadas como subsídio à avaliação interna de risco, quando disponíveis, avaliações realizadas por entidades públicas do País relativas ao risco de lavagem de dinheiro e de financiamento do terrorismo. Além disso, os arts. 35-D, § 2º, 35-E e 35-F, da Instrução CVM nº 505/2011[6], alterada pela Instrução CVM nº 612/2019[7], determinam que: Art. 35-D. O intermediário deve desenvolver política de segurança da informação abrangendo: § 2º A política de segurança da informação deve: I – ser compatível com: a) o porte, o perfil de risco e o modelo de negócio do intermediário;

[6] CVM. Instrução CVM 505. Disponível em: <http://conteudo.cvm.gov.br/legislacao/instrucoes/inst505.html>. Acesso em: 22 mar. 2021.
[7] CVM. Instrução CVM 612. Disponível em: <http://conteudo.cvm.gov.br/legislacao/instrucoes/inst612.html>. Acesso em: 22 mar. 2021.

	b) a natureza das operações e a complexidade dos produtos, serviços, atividades e processos do intermediário; e c) a sensibilidade dos dados e informações sob responsabilidade do intermediário; Art. 35-E. O intermediário deve desenvolver e implementar regras, procedimentos e controles internos adequados visando garantir a confidencialidade, a autenticidade, a integridade e a disponibilidade dos dados e informações sensíveis, contemplando: I – as diretrizes para a identificação e classificação dos dados e informações sensíveis; e II – os procedimentos adotados para garantir o registro da ocorrência de incidentes relevantes, suas causas e impactos. Art. 35-F. As regras, procedimentos e controles de que trata o art. 35-E devem contemplar: I – a proteção das informações de cadastro e de operações realizadas pelo cliente contra acesso ou destruição não autorizados, vazamento ou adulteração; II – a concessão e administração de acessos individualizados a sistemas, bases de dados e redes; e III – segregação de dados e controle de acesso, de forma a prevenir o risco de acesso não autorizado, de adulteração ou de mau uso das informações. Assim, a ANPD deverá considerar o tamanho e o porte das instituições envolvidas, bem como definir elementos mínimos para serem atendidos por estas. A partir disso será possível avaliar se o Controlador foi negligente ou se a falha que ocasionou o incidente ocorreu por um fator fora de seu controle[8], sendo punível somente a primeira situação.

[8] Considerações sobre a notificação de incidente de segurança da ...- Migalhas. Disponível em: <https://www.migalhas.com.br/depeso/295440/consideracoes-sobre-a-notificacao-de-incidente-de-seguranca-da-informacao-no-contexto-da-lei-geral-de-protecao-de-dados--e-alem>. Acesso em: 22 mar. 2021.

Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	O Regulamento Geral sobre a Proteção de Dados (legislação europeia) aponta que o incidente deverá ser comunicado em um prazo de 72 horas, após o conhecimento do mesmo[9]. Contudo, entendemos por não encurtar tanto o prazo, pois poderá ocorrer uma falha na avaliação pelo Controlador. Tomando por base a Circular nº 3978/2020 do BACEN, que *"Dispõe sobre a política, os procedimentos e os controles internos a serem adotados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil visando à prevenção da utilização do sistema financeiro para a prática dos crimes de "lavagem" ou ocultação de bens, direitos e valores, de que trata a Lei nº 9.613, de 3 de março de 1998, e de financiamento do terrorismo, previsto na Lei nº 13.260, de 16 de março de 2016"*, o p. único do art. 39 determina que *"O período para a execução dos procedimentos de monitoramento e de seleção das operações e situações suspeitas não pode exceder o* ***prazo de quarenta e cinco dias****, contados a partir da data de ocorrência da operação ou da situação"*. Ainda levando em consideração a Circular nº 3978/2020, no momento que se decide comunicar a Entidade Competente, isso deverá ser feito em um dia útil. Ou seja, após ocorrer toda a avaliação, a diretoria responsável se reunirá para decidir se deverá ser feita a comunicação ou não.[10] Diante disso, entendemos como salutar criar dois prazos: um para análise interna do possível incidente, de modo a permitir a avaliação efetiva e real da situação (evitando decisões precipitadas) e, após essa avaliação, que seja determinado um prazo de um a dois dias úteis, após a decisão da Diretoria de comunicar a ANPD, para que esta decisão seja concretizada.

[9] Artigo 33º - Notificação de uma violação de dados pessoais à autoridade de controlo - 1. Em caso de violação de dados pessoais, o responsável pelo tratamento notifica desse facto a autoridade de controlo competente nos termos do artigo 55.o, sem demora injustificada e, sempre que possível, até **72 horas após ter tido conhecimento da mesma**, a menos que a violação dos dados pessoais não seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares. Se a notificação à autoridade de controlo não for transmitida no prazo
de 72 horas, é acompanhada dos motivos do atraso.
(General Data Protection Regulation (GDPR) – art. 33. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT>. Acesso em: 22 mar. 2021.)

[10] Art. 48. As instituições referidas no art. 1º devem comunicar ao Coaf as operações ou situações suspeitas de lavagem de dinheiro e de financiamento do terrorismo. **§ 2º A comunicação da operação ou situação suspeita ao Coaf deve ser realizada até o dia útil seguinte ao da decisão de comunicação.**

	Cumpre destacar a orientação do GDPR, que dispõe que, nos casos de alto risco de dano aos direitos e liberdades do titular dos dados, deverá haver comunicação imediata[11], não sendo necessário, em um primeiro momento, informar todos os requisitos dispostos no § 1º, do art. 48, da LGPD. Nesse caso, a informação deve ser repassada de forma urgente, tendo em vista os aspectos principiológicos e potenciais danos envolvidos.
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	A GDPR determina no art. 34, que se houver elevado risco de dano aos titulares, o Controlador deverá comunicar em até 72 horas, sendo que obrigatoriamente a comunicação deverá conter as seguintes informações: • Comunicar o nome e os contatos do encarregado da proteção de dados ou de outro ponto de contato onde possam ser obtidas mais informações; • Descrever as consequências prováveis da violação de dados pessoais; e • Descrever as medidas adotadas ou propostas pelo responsável pelo tratamento para reparar a violação de dados pessoais, inclusive, se for caso disso, medidas para atenuar os seus eventuais efeitos negativos. Além disso, o mesmo artigo apresenta exceções para a não comunicação, quais sejam: • O responsável pelo tratamento tiver aplicado medidas de proteção adequadas, tanto técnicas como organizativas, e essas medidas tiverem sido aplicadas aos dados pessoais afetados pela violação de dados pessoais, especialmente medidas que tornem os dados pessoais incompreensíveis para qualquer pessoa não autorizada a aceder a esses dados, tais como a cifragem; • O responsável pelo tratamento tiver tomado medidas subsequentes que assegurem que o elevado risco para os direitos e liberdades dos titulares dos dados já não é suscetível de se concretizar; ou

[11] Artigo 34º - **Comunicação de uma violação de dados pessoais ao titular dos dados** - 1. Quando a violação dos dados pessoais for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento comunica a violação de dados pessoais ao titular dos dados sem demora injustificada.
(General Data Protection Regulation (GDPR) – art. 34. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT>. Acesso em: 22 mar. 2021.)

	• Implicar um esforço desproporcionado. Nesse caso, é feita uma comunicação pública ou tomada uma medida semelhante através da qual os titulares dos dados são informados de forma igualmente eficaz. **Assim, a comunicação só será feita quando houver alto risco ou dano relevante e caso não haja nenhuma das exceções supra, e em até 2 dias úteis, utilizando assim o prazo disposto no art. 18, §§1º e 2º, do Decreto nº 9.936, de 24 de julho de 2019.**
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	A comunicação deve ser da forma mais efetiva possível, visando aplicar os princípios da LGPD, notadamente livre acesso e transparência. Em casos pontuais e de possível identificação do titular dos dados afetado, que seja feita de maneira individualizada. Contudo, em casos de incidentes que causem vazamento de dados em massa, que seja feita comunicação pública, por ser mais célere e atender de forma mais efetiva ao comando legal. Tudo isso agregado à necessidade de efetiva comunicação, conforme ressaltado no tópico anterior.
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	Risco baixo e danos de menor potencial (a depender do volume e tipo de dados vazados), os quais se configurem como mera ameaça ou baixa probabilidade de prejuízos correlatos. Contudo, importante destacar que este risco/dano deverá ser documentado pelo Controlador, proporcionando aprendizados e melhorias sistêmicas.
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	O Controlador deve informar nos casos de alto risco e/ou materialização do dano, nos limites que defendemos nos itens supra.
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	Sugere-se que a ANPD foque na análise do sistema, se o Controlador estava seguindo seu plano de ação/política de privacidade, a legislação e as normas determinadas pela ANPD, bem como a qualidade e quantidade dos dados vazados. Certamente, os casos de maior gravidade são aqueles em que o incidente de segurança gerou vazamento de **dados sensíveis**, ou seja: (i) dados pessoais que revelem a origem racial ou étnica, opiniões políticas e convicções religiosas ou filosóficas; (ii)

	filiação sindical; (iii) dados genéticos, dados biométricos tratados simplesmente para identificar um ser humano; (iv) dados relacionados com a saúde; (v) dados relativos à vida sexual ou orientação sexual da pessoa.[12]
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	Para essa pergunta, podemos recorrer mais uma vez à Circular nº 3978/2020 do BACEN, que utiliza a metodologia da Abordagem Baseada em Risco ("ABR"). Essa metodologia propõe uma avaliação singular, em que os controles estejam proporcionais aos riscos que estão sendo tomados. Nessa metodologia, a Autoridade Reguladora receberá apenas as informações relevantes, tendo em vista que o Controlador será a "primeira linha de defesa", de modo que filtrará as informações e só enviará, de fato, os incidentes que possuem um risco considerável para se concretizar.[13] O objetivo dessa metodologia, portanto, é garantir qualidade e não quantidade da informação repassada para a Autoridade Competente.
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	A ideia é que os próprios Controladores já apresentem a solução em um Plano de Ação e Resposta, de modo a corrigir o seu sistema, ou seja, a sugestão é investir em autorregulação, com base em diretrizes objetivas fornecidas pela ANPD. Havendo um Plano de Ação e Resposta bem fundamentado, este poderia ser utilizado, inclusive, para evitar um Processo Administrativo Sancionador.

[12] COMISSÃO EUROPEIA. Que dados pessoais são considerados sensíveis? Disponível em: <https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_pt>. Acesso em: 22 mar. 2021.
[13] 2017. Entenda melhor o que é Abordagem Baseada em Risco - Editorial - IPLD - Instituto de prevenção à lavagem de dinheiro e ao financiamento do terrorismo. Disponível em: <https://www.ipld.com.br/editorial/entenda-melhor-o-que-e-abordagem-baseada-em-risco#:~:text=Abordagem%20Baseada%20em%20Risco%20(ABR,diretamente%20proporcionais%20aos%20riscos%20avaliados.>. Acesso em: 22 mar. 2021.

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: PDK Advogados (https://pdka.com.br/)

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS	
IMPORTANTE: Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
1. Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	Para avaliar se um incidente acarretará risco ou dano relevante, é necessário primeiro estabelecer os critérios para torná-los relevantes. Nem todo risco terá a mesma possibilidade de se concretizar e ou causar efeito idêntico. Assim também, nem todo dano terá a mesma extensão. Por isso, a necessidade de mensurar o dano ou o risco, observando-se a sua relevância. Para análise da relevância do risco ou do dano, é necessário observar a combinação **probabilidade** de ocorrência do evento e das **consequências** que dele resultarem, ou seja, o impacto que pode causar nos objetivos. Assim, teremos o seguinte cenário:

Fonte: Brasil. Tribunal de Contas da União. Referencial básico de gestão de riscos / Tribunal de Contas da União. – Brasília: TCU, Secretaria Geral de Controle Externo (Segecex), 2018.

■ **Figura 7:** Matriz de riscos simples

Para se analisar a **probabilidade**, existem os seguintes parâmetros:
Muito baixa = Improvável. Em situações excepcionais, o evento poderá até ocorrer, mas nada nas circunstâncias indica essa possibilidade.
Baixa = Rara. De forma inesperada ou casual, o evento poderá ocorrer, pois as circunstâncias pouco indicam essa possibilidade.
Média = Possível. De alguma forma, o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade.
Alta = Provável. De forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade.
Muito alta = Praticamente certa. De forma inequívoca, o evento ocorrerá, as circunstâncias indicam claramente essa possibilidade.

Já para se analisar o **impacto**, os parâmetros são os seguintes:
Muito baixo = Mínimo impacto nos objetivos (estratégicos, operacionais, de informação/ comunicação/divulgação ou de conformidade).
Baixo = Pequeno impacto nos objetivos.
Médio = Moderado impacto nos objetivos, porém recuperável.
Alto = Significativo impacto nos objetivos, de difícil reversão.
Muito alto = Catastrófico impacto nos objetivos, de forma irreversível.
A relevância, assim, será determinada pela análise conjunta dos índices de probabilidade e impacto do risco ou do dano, conforme os critérios acima expostos.

	O incidente que poderá acarretar risco ou dano relevante é aquele cujo fator de análise da probabilidade e impacto for de médio a muito alto, visto que as chances e as consequências sairão da raridade, tornando-se possível **Referências:** - Referencial básico de gestão de riscos. Tribunal de Contas da União. Brasília : TCU, Secretaria Geral de Controle Externo (Segecex), 2018. - Metodologia de gestão de riscos. Brasília: Ministério da Transparência e Controladoria-Geral da União (CGU), 2018. **-** ISO 27001 - Código Civil/2002
2.O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	Conforme visto no item '1.' dessa Tomada de Subsídios, o incidente acarreta um risco ou dano relevante ao titular quando o fator de análise de probabilidade e impacto for de médio a muito alto., O risco relevante, decorrente da execução do processo e seus reflexos, deve ser avaliado em categorias de valoração, bem como o impacto e a probabilidade subdivididas, tal divisão deve seguir o padrão do elencado no item '1.' A avaliação quanto à necessidade de subdivisão do risco relevante em categorias deve, no entanto, seguir critérios setoriais. A importância em dividir os tratamentos de acordo com seus riscos busca uma visão preditiva no que se refere ao gerenciamento dos riscos e das probabilidades atinentes ao desenvolvimento da atividade econômica da empresa. Vale ressaltar que a classificação dos tratamentos de dados de acordo com seu risco é importante instrumento na aplicação de medidas mitigadoras e na reestruturação do processo em nível organizacional e técnico.Assim, verifica-se importante a integração com os diversos setores e suas agências reguladoras correspondentes para verificar: i) a existência de análise baseada em riscos; ii) a necessidade de subdivisão do risco relevante dentro do contexto trazido pela economia dos dados e pela LGPD. No escopo da avaliação setorial quanto a necessidade da divisão do risco ou dano relevante em subcategorias os seguintes tópicos são essenciais: natureza e especificidade dos dados, fluxo dos dados, matriz técnica de segurança, matriz organizacional, matriz operacional, contexto legal/regulatório. O risco de baixo nível deve ser levado em consideração no que toca à atenção necessária para mitigar os riscos futuros e o agravamento de tal risco ao status de risco relevante. O tratamento de dados é dotado de um aspecto dinâmico, podendo evoluir no risco conforme os aspectos que o circundam.
3. Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	Inicialmente, é necessário compreender os conceitos de dano e risco. **Dano** é entendido como prejuízo ou perda que atinge um bem jurídico, ocasionando a sua subtração ou diminuição. Trata-se da lesão do bem jurídico. Dano é um fato/acontecimento.

	Risco é quando há um desvio em relação ao esperado (efeito) que causa uma deficiência (incerteza), na compreensão, no conhecimento, na consequência ou na probabilidade das informações relacionadas a um evento (objetivo). Ou seja, é o efeito da incerteza sobre os objetivos, caracterizado como potenciais acontecimentos e consequências. Assim, temos que o risco antecede o dano, podendo ou não causar dano se concretizados seus acontecimentos e consequências. Ex. O **risco** de vazamento de dados está associado ao potencial de as **ameaças** explorarem **vulnerabilidades** de um ativo da informação e, assim, causar **dano** À organização e ao titular de dados. **Referências:** - Adolpho C. De Andrade Mello Jr. O DANO RESPONSABILIDADE CIVIL. Disponível em: https://www.emerj.tjrj.jus.br/revistaemerj_online/edicoes/revista09/Revista09_46.pdf - ISO 27001 - Código Civil/2002
4.O que deve ser considerado na avaliação dos riscos do incidente?	A avaliação de riscos do incidente deve considerar métricas concretas acerca da: **I. Categoria do Dado e suas Especificidades**: Na eventualidade de um incidente, a natureza do dado impacta diretamente no risco apresentado. Portanto, é necessário entender qual é a categoria do dado, como esse dado é manipulado, de que forma o dado é armazenado e quem é o Titular. Com relação à categoria do dado, a consideração deve ser mais abrangente: dados sensíveis, dados financeiros, dados comportamentais, dados de crianças e adolescentes, dados simples entre outros. **II. Facilidade de identificação**: Na avaliação dos riscos do incidente deve-se levar em consideração a facilidade de identificação do titular a partir dos dados em questão, ou seja, possibilidade de identificar o titular a partir dos dados disponíveis ou a necessidade de um processo de cruzamento de dados ou reversão de e um processo de pseudoanonimização por exemplo. **III. Transferência de Dados**: Dentre as operações realizadas com dados pessoais, é fundamental compreender como se dá o compartilhamento, transmissão e a distribuição de dados, bem como quem são os controladores e operadores, quais agentes possuem acesso aos dados, e os meios técnicos de acesso e transferência, elementos cruciais na avaliação do risco e suas implicações. **IV. Matriz Técnica de Segurança**: A Matriz Técnica de Segurança diz respeito às medidas técnicas adotadas para mitigar vulnerabilidades a partir da identificação de potenciais ameaças, seja no armazenamento, acesso, uso ou compartilhamento dos dados pessoais em suporte eletrônico ou físico. Desta forma, a avaliação deve

	considerar a natureza do dado, o tipo de tratamento realizado e a adequação da medida a esses fatores. Nesse contexto a Política de Segurança da Informação adquire especial relevância na avaliação dos riscos. **V. Matriz Organizacional**: A Matriz Organizacional, por sua vez, diz respeito ao controle de acesso. Basicamente deve-se analisar as permissões e limitações de acesso dos usuários ao mínimo necessário para realização da atividade de tratamento. Políticas, Códigos e demais normativas internas devem ser levadas em consideração, tanto no que se refere à sua existência quanto à sua efetiva aplicação. **VI. Aspectos Jurídicos**: A avaliação dos riscos do incidente também deve considerar a correta identificação da base legal que envolve o tratamento, o período de retenção. rotinas de atendimento ao titular do dado, existência de um EDP, atenção aos diversos princípios elencados na lei e demais obrigações e deveres oriundos do sistema jurídico que envolve a atividade desempenhada pela empresa. A avaliação de riscos do incidente, deve considerar a escolha da metodologia, as dimensões jurídicas, de segurança da informação e organizacionais e as circunstâncias específicas do caso, como volume dos dados tratados, qualidade e precisão das informações, características dos titulares e disponibilidade pública das informações. A Probabilidade e o Impacto, aos moldes da norma de gestão de risco ISO 31.000, podem ser um importante guia na análise do incidente.
5. Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	Com o intuito de se ter uma descrição pormenorizada do incidente de segurança, tanto para que seja possível mensurar o nível do risco do incidente, bem como para evitar que a ANPD seja sobrecarregada com notificações que não acarretem risco ou dano relevante ou ainda com falta de informações suficientes para investigar o caso, recomenda-se que a notificação de incidente de segurança à ANPD, além dos requisitos previstos na lei, tenha os seguintes pontos: **Agentes de Tratamento:** a) comunicar o nome e os contatos do encarregado da proteção de dados; b) informar a natureza do agente do tratamento, se organização pública ou privada. **Incidente de Segurança:** a) data e hora que o incidente ocorreu, quando possível; b) data e hora da descoberta do incidente; descrição do incidente, quando possível; como foi descoberto; pessoas já informadas: i) Se houve comunicação ao titular, em caso negativo, motivar a falta de comunicação; e ii) Se o notificante for operador, informar se já comunicou o controlador. **Dos titulares:** a) volume dos dados afetados; b) quantidade de titulares afetados. **Medidas de Segurança:** a) quais medidas de segurança, técnicas e administrativas, foram tomadas para prevenir a recorrência do incidente de segurança; b) relatório de impacto à proteção de dados pessoais dos tratamentos relacionados/impactados pelo incidente. **Referências:**

	- Guidelines on Personal data breach notification under Regulation 2016/679 (wp250rev.01). Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052 - ANPD. Comunicação de incidentes de segurança. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca
6.Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	O art. 33 do GDPR determina que a notificação do incidente deve ocorrer sem atraso injustificável, sendo o prazo máximo de 72 horas após o conhecimento do incidente, exceto se improvável que o incidente cause dano a direitos e liberdades dos titulares. O prazo de 72 horas pode ser demasiadamente curto à depender da quantidade e qualidade das informações para a notificação do incidente: coleta e organização das informações sobre a análise da situação, a avaliação dos dados afetados, descrição do impacto, envolvimento de pessoas e treinamentos ministrados, medidas preventivas e ações de mitigação e dados de contato do Encarregado. Considerando casos mais complexos, quando da impossibilidade do fornecimento de todas as informações relacionadas ao incidente, verifica-se a necessidade de negociação de tal prazo com a ANPD, sempre fundamentada pelas razões dessa solicitação. Nesse caminhar, a possibilidade de apresentar o relatório de incidentes em fases deve também ser avaliada pela ANPD, principalmente quando o incidente tiver relevância alta, como por exemplo pela potencialidade de atingir direitos e liberdades fundamentais, mas existirem dificuldades na reunião de todas as informações necessárias à notificação. Nessa hipótese, pode-se vislumbrar uma notificação prévia mais célere, no intuito de mitigar riscos ao titular de dados, e uma notificação posterior, em prazo razoável, com todas as informações necessárias do incidente. Cabe ainda ressaltar que, apesar da nítida importância de um procedimento de notificação de incidente, há de se considerar que o programa de adequação à LGPD ainda está distante à realidade da maioria das empresas no Brasil. Nesse sentido, sugere-se para além da importação do padrão europeu de 72hs, seja estudado um prazo junto à organizações especializadas no assunto, como o CERT, para melhor compreender o contexto brasileiro e determinar o prazo ideal ao cenário nacional.
7.Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	O artigo 34 do GDPR determina que a notificação do incidente de segurança pelo Controlador aos Titulares deve ocorrer "sem atraso justificável". A ausência de um prazo específico se justifica pela variedade de situações possíveis. É razoável, portanto, que o prazo contenha alguma margem temporal conforme a circunstância concreta do incidente. O prazo a ser definido pode ser gradativo a depender da gravidade do incidente e/ou dos possíveis riscos decorrentes do mesmo. Essa classificação pode seguir critérios objetivos como: quantidade dos titulares, dados afetados, natureza dos dados, entre outros.

	Cabe ainda ressaltar quanto a diferenciação da comunicação pública ou particular. Caso a comunicação seja pública, é plausível que ocorra em até 24 horas após a ciência. Por outro lado, caso a comunicação seja individual, sugere-se a consideração de um prazo de até 72 horas, considerados critérios justificadores de uma eventual dilação do prazo, como: gravidade do incidente, quantidade de titulares afetados e meios de comunicação do incidente aos titulares. A comunicação ao titular do incidente de segurança deve conter as seguintes informações do art. 48 § 1º: I) descrição da natureza dos dados pessoais afetados; III) indicação das medidas técnicas e de segurança utilizadas para a proteção de dados; IV) riscos relacionados ao incidente; V) motivo da demora caso não tenha sido imediata; VI) medidas que foram ou serão adotadas para mitigar o prejuízo. Além disso, sugere-se a inserção de informações sobre medidas de segurança adicionais que podem ser tomadas pelo titular, como: alteração de senhas e logins, monitoramento de transações bancárias, ativação de autenticação de dois fatores, dentre outras. É fundamental que a comunicação direcionada ao titular, embora contemple praticamente todas as exigências do art. 48 § 1º, tenha uma linguagem mais simples, clara e de fácil compreensão para o titular, utilizando sempre que possível de elementos gráficos e legal design.
8. Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	A forma mais adequada para a realização da comunicação do incidente aos titulares é o instrumento de comunicação utilizado com o titular pela organização, seja ele por e-mail, aplicativo de mensagem, redes sociais ou via postal, sempre considerando que o Controlador possua legitimamente esses dados. Caso o controlador faça uso preferencialmente do meio físico (correios, mala direta) sugere-se que a comunicação seja também acompanhada do formato eletrônico para trazer mais celeridade quanto a informação do incidente e medidas de segurança necessárias. Em determinadas circunstâncias pode ser admitida a comunicação pública, desde que seja um vazamento de baixo a médio, e após análise da situação em concreto pela Autoridade. Isso, pois a comunicação pública em casos de impacto alto ou muito alto pode, além de não garantir que o titular específico seja comunicado, incentivar a busca clandestina por esses bancos de dados e renovar o prejuízo experimentado pelos titulares.
9. Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	No sentido de compreender as eventuais exceções da obrigatoriedade de informar a ANPD, devemos rememorar que instituição de autoridades administrativas independentes (DPAs) e a proteção de direitos fundamentais relacionados à proteção dos dados pessoais estão interligadas por natureza e, portanto, é indispensável a notificação destes entes em qualquer hipótese que houver lesão ao direito à proteção de dados pessoais. Entende-se que para evitar o sobrecarregamento e o hiper acionamento da instituição, exceção plausível se configura na hipótese de o incidente de segurança não gerar qualquer risco ou prejuízo aos direitos e

	liberdades dos titulares de dados pessoais. O ponto é, como aferir se o incidente fere direitos fundamentais relacionados aos dados pessoais e como determinar essas hipóteses de exceção? A consulta ao RIPD (Relatório de Impacto à Proteção de Dados Pessoais) pode oferecer indicadores importantes neste exame. A análise do RIPD, feita antes de realizar a operação de tratamento em questão pode, no entanto, se mostrar mais abrangente e pouco específica em comparação com as circunstâncias singulares da violação real, fazendo se necessário que o controlador realize uma avaliação apartada quanto as circunstâncias do caso concreto. Essa avaliação do caso concreto deve seguir critérios objetivos, considerando as circunstâncias específicas da violação, incluindo a gravidade do impacto potencial e o risco de ocorrência desse impacto. A WP248, recomenda que a avaliação leve em consideração os seguintes critérios[3]: • **O tipo de violação**, que pode afetar o nível de risco apresentado aos indivíduos. • **A natureza, a sensibilidade e o volume dos dados pessoais**. Normalmente, quanto mais sensíveis os dados, maior o risco de danos às pessoas afetadas, mas também devem ser consideradas as circunstâncias do vazamento. Violações envolvendo dados de saúde, documentos de identidade ou dados financeiros, como detalhes de cartão de crédito, podem causar danos por si só, mas se usados juntos, podem ser ainda mais danosos, sendo usados para roubo de identidade por exemplo. • **Facilidade de identificação de indivíduos.** Dependendo das circunstâncias, a identificação pode ser possível diretamente a partir dos dados pessoais violados, sem a necessidade de diligências especiais para descobrir a identidade do indivíduo, ou pode ser extremamente difícil fazer essa identificação, mas ainda ser possível. Esses diferentes níveis de facilidade também influenciam no nível do risco, ressaltando a importância dos métodos mitigadores como criptografia e anonimização dos dados e a pseudonimização devidamente implementada. • **Gravidade das consequências para os indivíduos:** Quando envolvidas categorias especiais de dados, o dano potencial a indivíduos pode ser especialmente grave quando a violação puder resultar em roubo de identidade ou fraude, dano físico, sofrimento psicológico, humilhação ou danos à reputação. Se a violação envolver dados pessoais sobre indivíduos vulneráveis, como pessoas menores de idade e idosos, o risco é agravado. O destinatário também influencia no nível do risco. • **Características especiais do indivíduo.** Conforme o ponto anterior, uma violação pode afetar dados pessoais relativos a crianças ou outros indivíduos vulneráveis, que podem ser colocados em maior risco.

	• **Características especiais do controlador de dados.** A natureza, o papel do controlador e suas atividades podem afetar o nível de risco para os indivíduos em uma violação. Por exemplo, uma organização médica processará categorias especiais de dados pessoais, o que significa que haverá uma ameaça maior para os indivíduos se seus dados pessoais forem violados, em comparação com uma lista de mala direta de um jornal. • **O número de indivíduos afetados.** Geralmente, quanto maior o número de indivíduos afetados, maior o impacto de uma violação. No entanto, uma violação pode ter um impacto muito grave até mesmo em um indivíduo, dependendo da natureza dos dados pessoais e do contexto em que foram comprometidos. • **Pontos gerais. O** controlador deve considerar uma combinação da gravidade do impacto potencial sobre os direitos e liberdades dos indivíduos e a probabilidade de estes ocorrerem. Em caso de dúvida, o controlador deve se apegar ao princípio da precaução e por cautela, notificar. Todavia, independentemente da comunicação ou não à autoridade, o controlador deve sempre manter registros internos relativos aos incidentes ocorridos, de modo a atender aos princípios do Accountability e Precaução. **Referências:** - WP Guidelines sobre os RIPD's. Disponível em: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137 -Guidelines sobre a notificação de incidentes de dados pessoais. Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052 - GDPR, Capítulo IV, Seção II, Razão 75.
10.Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	A obrigatoriedade de informar aos titulares já deve ser mais restrita, protegendo-os do potencial aborrecimento. De acordo com a WP29, existem 3 circunstâncias em que se pode dispensar a notificação ao titular de dados, quais sejam: 1) O responsável pelo tratamento aplicou medidas técnicas e organizacionais adequadas para proteger os dados pessoais antes da violação, em particular aquelas medidas que tornam os dados pessoais ininteligíveis para qualquer pessoa que não esteja autorizada a acessá-los. Isso poderia, por exemplo, incluir a proteção de dados pessoais com criptografia de última geração ou por tokenização. 2) Imediatamente após uma violação, o controlador tomou medidas para garantir que o alto risco representado para os direitos e liberdades dos indivíduos não seja mais provável de se concretizar. Por exemplo, dependendo das circunstâncias do caso, o responsável pelo tratamento pode ter imediatamente identificado e tomado medidas contra a pessoa que acessou os dados pessoais antes que este pudesse utilizá-los de qualquer maneira. Dependendo da natureza dos dados em questão, a mera quebra da confidencialidade já

	pode ser motivo suficiente para a necessidade de informar aos titulares, excetuados estes casos, se as devidas providências foram tomadas não há a necessidade de notificar. 3) Envolveria um esforço desproporcional para contatar indivíduos, talvez quando seus dados de contato tenham sido perdidos como resultado da violação ou não sejam conhecidos em primeiro lugar. Em vez disso, o controlador deve fazer uma comunicação pública ou tomar medida semelhante, em que as pessoas sejam informadas de forma igualmente eficaz. No caso de esforço desproporcional, arranjos técnicos também poderiam ser considerados para disponibilizar informações sobre a violação sob demanda, o que poderia ser útil para aqueles indivíduos que podem ser afetados por uma violação, mas o controlador não pode entrar em contato de outra forma. De acordo com o princípio da responsabilidade, os controladores devem ser capazes de demonstrar à autoridade de supervisão que cumprem uma ou mais destas condições. Deve-se ter em mente que, embora a notificação possa não ser exigida inicialmente se não houver risco para os direitos e liberdades das pessoas singulares, isso pode mudar com o tempo e o risco teria de ser reavaliado. **Referências:** - Guidelines on Personal data breach notification under Regulation 2016/679 (wp250rev.01). Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052
11.Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	Para avaliar a gravidade de um incidente de segurança diversos critérios devem ser considerados, entre eles, a relevância do risco e o impacto do incidente, ambos já intensamente refletidos nas perguntas anteriores., No entanto, imprescindível se faz dar relevância na análise do dano concreto, evitando assim não somente a banalização dos incidentes de segurança, mas também o mercado do dano moral. Lembramos que dano pode ser compreendido como prejuízo ou perda que atinge um bem jurídico, ocasionando a sua subtração ou diminuição, conforme exposto na resposta da questão número 3. Trata-se, portanto, da lesão ao bem jurídico. Para haver um equilíbrio e segurança jurídica quanto as consequências dos incidentes de segurança, critérios objetivos precisam ser analisados. Tais critérios devem considerar não só a possibilidade da continuidade dos riscos, em razão da não mitigação do mesmo, mas também a lesão causada pelo incidente em concreto. Os incidentes de segurança podem acarretar danos com extensões e consequências bastante variáveis, por isso é importante observar sua relevância e definir métricas objetivas. A avaliação do caso concreto deve levar em consideração os seguintes parâmetros, como podemos observar na questão 9: a) tipo de violação; b) a natureza, a sensibilidade e o volume dos dados pessoais; c) facilidade de identificação de indivíduos; d) gravidade das consequências para os indivíduos; e) características especiais do indivíduo; e) características especiais do controlador de dados; e) número de indivíduos afetados.

12.Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	O Guia da Autoridade Espanhola de Proteção de Dados traz uma metodologia que pode servir de inspiração na análise da gravidade do incidente de segurança. Conforme Guia de Notificação de Incidente de Segurança a gravidade dependerá dos seguintes fatores: **A categoria ou nível de criticidade** relacionada à segurança dos sistemas afetados. Seguindo a classificação genérica, podemos distinguir entre: - Crítico :afeta dados valiosos, grande volume e em pouco tempo. - Muito Alto :Quando tem capacidade de afetar informações valiosas, em quantidade considerável. - Alto :quando tem a capacidade de afetar informações valiosas. - Médio quando tem capacidade de afetar um volume considerável de informação. - Baixo pouca ou nenhuma capacidade de afetar um volume considerável de informações. **Natureza, sensibilidade e categorias dos dados pessoais afetados:** - Dados de baixo risco: contato, educação, família, profissional, dados biográficos. - Dados comportamentais: localização, trânsito, hábitos e preferências. - Dados financeiros: transações, posições, receitas, contas, faturas. - Dados sensíveis: saúde, biometria, dados relativos à vida sexual, etc. - Dados legíveis / ilegíveis: dados protegidos por algum sistema de pseudonimização (por exemplo, criptografia ou hash). - Volume de dados pessoais: expresso em quantidade (registros, arquivos, documentos) e / ou em períodos de tempo (uma semana, um ano, etc.). - Facilidade de identificação de indivíduos: facilidade com que a identidade de indivíduos pode ser deduzida dos dados envolvidos na violação. **Gravidade das consequências para os indivíduos:** - Baixa: As pessoas não serão afetadas ou poderão encontrar alguns inconvenientes que poderão superar sem problemas (tempo de reingresso da informação, aborrecimentos, irritações, etc.). - Médio: as pessoas podem encontrar inconvenientes significativos, que serão capazes de superar apesar de algumas dificuldades (custos adicionais, recusa de acesso a serviços comerciais, medo, falta de compreensão, estresse, pequenos males físicos, etc.). - Alta: As pessoas podem enfrentar consequências importantes, que devem ser capazes de superar, embora com sérias dificuldades (desfalque, listas negras de bancos, danos materiais, perda de emprego, intimação judicial, deterioração da saúde, etc.). - Muito alta: as pessoas podem enfrentar consequências significativas ou mesmo irreversíveis que não podem superar (exclusão ou marginalização social, dificuldades financeiras como dívidas consideráveis ou incapacidade para trabalhar, doenças físicas ou psicológicas de longo prazo, morte, etc.).

	Características especiais dos indivíduos: Se afetam indivíduos com características especiais ou com necessidades especiais. **Número de indivíduos afetados:** dentro de uma determinada escala, por exemplo, mais de 1000 indivíduos. **Características especiais do responsável pelo tratamento (da própria entidade):** Com base na atividade da entidade. **O perfil dos usuários afetados**, sua posição na estrutura organizacional da entidade e, consequentemente, seus privilégios de acesso a informações sensíveis ou confidenciais. **O número e a tipologia dos sistemas afetados.** **O impacto** que a violação pode ter na organização, do ponto de vista da proteção da informação, da prestação de Serviços, do cumprimento legal e / ou da imagem pública. Ele estará relacionado à categoria ou criticidade dos serviços afetados e das pessoas afetadas. Nesse sentido, diferenciamos os seguintes impactos: baixo (dano limitado), médio (dano sério), alto (dano muito sério). **Os requisitos legais e regulatórios:** Notificação da violação à autoridade de controle e qualquer outra obrigação de notificação ou comunicação aos Órgãos de Segurança do Estado em caso de crime. **Referências:** - AEPD. Guía para la gestion y notificación de brechas de seguridad. Disponível em; https://www.aepd.es/sites/default/files/2019-09/guia-brechas-seguridad.pdf
13.Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	Uma das possíveis sugestões seria identificar, coletar e preservar evidências sobre o incidente de segurança. Descobrir sua causa e fazer prova positiva da investigação realizada são providências importantes, não só para traçar um caminho ou rastro positivo de que, de fato, a organização tratou o incidente com em conformidade à gravidade que possui, como também para minimizar condenações civis e sanções administrativas. A identificação e responsabilização do usuário responsável pelo vazamento de dados pessoais ou ao menos a tentativa, por exemplo, pode auxiliar na redução de sanções, demonstrando, na prática, que a organização adotou as providências que estavam ao seu alcance. a empresa reagiu prontamente, informou o titular e buscou a identificação/responsabilização dos responsáveis.

	É necessário, portanto, que a identificação e coleta das evidências para provar o episódio sejam devidamente adotadas, evitando qualquer espécie de adulteração ou dúvida sobre o procedimento, sob pena de resultar na total invalidade jurídica e consequente inutilidade das provas. Recomenda-se que um plano de resposta, portanto, conte com as primeiras providências nesse sentido e com os profissionais internos e de parceiros que serão responsáveis por adotá-las. O plano de resposta deve responder a perguntas como: (i) quem identificou o incidente deve fazer o que e deve encaminhar as evidências para qual área?; (ii) as evidências devem ser preservadas como?; (iii) quem conduzirá os trabalhos de lavratura de atas notariais ou da preservação da prova em blockchain; (iv) quem elaborará um relatório técnico interno circunstanciado do incidente?; (v) o que ele deve apresentar de essencial; (vi) quais os parceiros jurídicos e técnicos externos auxiliarão nas tarefas? Outra sugestão que deve ser levada em consideração é exigência pela Autoridade quanto a elaboração e apresentação de um relatório final do incidente. devidamente circunstanciado de todas as providências que tiverem sido adotadas. Esse relatório deve apresentar, no mínimo: (i) o que aconteceu de fato;(ii) quais providências de preservação das evidências foram adotadas; (iii) quem integrou o comitê de crise responsável pelos trabalhos; (iv) quais foram as funções desempenhadas pelos colaboradores envolvidos; (v) quais os parceiros envolvidos e por quais motivos; (vi) os questionamentos dos titulares, da imprensa e das autoridades recebidos; (vii) as respostas apresentadas; e (viii) quais as medidas de correção técnicas e de Governança adotadas. Esse relatório pode ser um importante instrumento não só como consolidação das provas positivas de atuação da organização diante o incidente, para todos os fins, sobretudo aqueles dos quais já foi conversado nesse trabalho, mas também para que o episódio fique concretizado e documentado na organização, não se perdendo depois de tratado e que sirva de ponto de partida para a revisão de procedimentos internos e até do próprio plano de resposta aos incidentes. Não raramente, já se verificou casos em que a organização responde ao incidente, mas após o assunto perde força internamente, prejudicando a criação de uma cultura positiva de preservação da Proteção de Dados Pessoais. Tal relatório é capaz de trazer outros benefícios como a um lastro documental da evolução dos procedimentos de Governança em dados pessoais a cada novo fato, podendo explorar isso, inclusive de forma gráfica, em sua defesa em fiscalizações e ações judiciais.

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: Pimentel, Vega, Souza Advogados

CPF/CNPJ: 22.458.401.0001-22

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS	
IMPORTANTE: Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	
O que deve ser considerado na avaliação dos riscos do incidente?	
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	

Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	

Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	Os incidentes de segurança possuem grande potencial de litigiosidade. Sabe-se que o Poder Judiciário já está assoberbado, com grande número de ações ajuizadas todos os anos. O sistema judicial é caro, demorado e em alguns casos ineficaz. Assim, é essencial que, para casos noticiados à ANPD em que se verifique que há grande potencial de vítimas e, portanto, ações judiciais a serem ajuizadas, já haja a previsão pelo controlador de formas de lidar com as disputas que surgirão a partir do incidente. O controlador, portanto, deverá criar e implementar um sistema para prevenir, gerir e solucionar tais disputas, sem que haja necessidade de busca ao Poder Judiciário. A isso se dá o nome de Desenho de Sistemas para resolução de Disputas, que consiste na utilização de diversos métodos para resolução de disputas, como negociação direta, mediação de conflitos, entre outros. Dessa forma, mesmo que parte dos titulares dos dados ou outros atores acabem buscando o judiciário, o controlador deverá apresentar canais e formatos para que o conflito gerado pelo incidente de segurança, e as disputas dele advindas, sejam tratados adequadamente por ele próprio, sem onerar os titulares e o Poder Judiciário.
SUGESTÃO DE NORMATIVO, SE HOUVER	
Art. Xxxx .... Para incidentes de segurança em que haja grande potencial de titulares de dados afetados (*sugere-se que haja um critério objetivo de número de potenciais ações a serem ajuizadas ou de percentual de litigiosidade em referência ao número de titulares afetados*) o controlador deverá apresentar à ANPD plano de gestão de crise, cujo desenho preveja a utilização de métodos de prevenção, gestão e resolução de disputas junto aos titulares.	
Art. Xxxx	

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: PRICEWATERHOUSECOOPERS TECNOLOGIA DA INFORMAÇÃO LTDA.

CPF/CNPJ: 07.969.979/0003-11

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

CONTRIBUIÇÕES RECEBIDAS **IMPORTANTE:** Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	Um incidente pode causar desde uma inconveniência a danos de graus variados ao titular de dados. Sugere-se que o incidente seja avaliado considerando-se as seguintes dimensões: o dimensionamento do incidente, a percepção do dano e a ocorrência de dano social. **Dimensionamento do incidente e impacto materializado** No dimensionamento do incidente deve-se considerar o volume de dados, os tipos de dados envolvidos, a incidência de dados sensíveis, de crianças ou adolescentes e vulneráveis, ou confidenciais, e se os dados estão sendo utilizados em desfavor dos titulares de dados, ou seja, se já está ocorrendo o dano. **Dano social** O dano social ocorre quando o incidente afeta a coletividade, como por exemplo, impede o acesso de pacientes à rede hospitalar. **Percepção do dano ao titular** A percepção de grau de dano ou risco relevante ao titular de dados, cujo maior impacto poderá ocorrer quando afetar os direitos fundamentais de liberdade e privacidade e de livre desenvolvimento da personalidade da pessoa natural, em situações tais como exposição da vida privada, discriminação, ocorrência de fraude, restrição ou impedimento de acesso a serviços.

	O dano relevante ocorreria se o resultado do incidente enquadra-se nas três dimensões sugeridas.
O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?	Sugerimos que o risco ou dano relevante seja classificado de acordo com a seguinte escala: **Máximo** - Dano relevante (atende os 03 critérios apresentados anteriormente); **Significativo** - Dano relevante (atende pelo menos 02 critérios apresentados anteriormente); **Limitado** - Dano (atende pelo menos 01 critério apresentado anteriormente); **Mínimo** - Não atende nenhum dos critérios.
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	O risco configura uma possibilidade de que o evento danoso ocorra, podendo ou não se materializar e resulte em potenciais impactos, enquanto o dano ocorre quando há a materialização do risco, ou o prejuízo ao titular se concretiza.
O que deve ser considerado na avaliação dos riscos do incidente?	Considerar os critérios apresentados anteriormente na primeira resposta. Os riscos devem ser avaliados considerando os critérios de impacto, probabilidade e volume.
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	Além das informações listadas no §1º do art. 48, sugere-se que na medida do possível os controladores já provenham ao titular instruções de medidas que possam ser adotadas pelo mesmo na contenção do dano (por exemplo, troca de senhas, monitoramento de consultas ao seus dados etc.). Sugere-se também que os controladores apresentem à ANPD os respectivos Planos de Resposta a Incidentes, e, em setores regulados, que informem os órgãos setoriais (tais como CVM, SUSEP, BACEN) que devam ser comunicados ou foram comunicados, nos termos de seus respectivos regulamentos, sempre que aplicável. A título de ilustração de normas setoriais podemos citar:

	DECRETO Nº 9.936, DE 24 DE JULHO DE 2019, que Regulamenta a Lei nº 12.414, de 9 de junho de 2011, que disciplina a formação e a consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. *RESOLUÇÃO Nº 4.658, DE 26 DE ABRIL DE 2018 Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.* *INSTRUÇÃO CVM Nº 612, DE 21 DE AGOSTO DE 2019 COM AS ALTERAÇÕES INTRODUZIDAS PELA INSTRUÇÃO CVM Nº 618/20 Altera, acrescenta e revoga dispositivos à Instrução CVM nº 505, de 27 de setembro de 2011, e revoga a Instrução CVM nº 380, de 23 de dezembro de 2002.* *INSTRUÇÃO CVM No 358, DE 3 DE JANEIRO DE 2002. Dispõe sobre a divulgação e uso de informações sobre ato ou fato relevante relativo às companhias abertas, disciplina a divulgação de informações na negociação de valores mobiliários e na aquisição de lote significativo de ações de emissão de companhia aberta, estabelece vedações e condições para a negociação de ações de companhia aberta na pendência de fato relevante não divulgado ao mercado, revoga a Instrução CVM no 31, de 8 de fevereiro de 1984, a Instrução CVM no 69, de 8 de setembro de 1987, o art. 3o da Instrução CVM no 229, de 16 de janeiro de 1995, o parágrafo único do art. 13 da Instrução CVM 202, de 6 de dezembro de 1993, e os arts. 3o a 11 da Instrução CVM no 299, de 9 de fevereiro de 1999, e dá outras providências.*
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	Um prazo razoável para que os controladores informem a ANPD sobre o incidente de segurança com base no art. 48, §1º seria de 10 (dez) dias, o qual poderia ser escalonado da seguinte forma: - uma notificação inicial em 2 (dois) dias comunicando a identificação do incidente; e - considerando que nem todos os fatos, levantamento e conclusões estejam disponíveis no momento da comunicação inicial, as respostas, conclusão e remediação dentro do prazo de 10 (dez) dias, ou, na impossibilidade devido a complexidade ou magnitude do evento, em prazo razoável a ser acordado com a ANPD com base na criticidade do incidente e volume de titulares afetados.

	A sugestão acima se baseia nas principais fases do Cyber Security Framework do National Institute of Standards and Technology (NIST).
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	Um prazo razoável para que os controladores informem os titulares sobre o incidente de segurança com base no art. 48, §1º seria de 10 (dez) dias, o qual poderia ser escalonado da seguinte forma: - uma comunicação imediata no prazo de 2 (dois) dias nas hipóteses em a natureza do incidente permita ao titular tomar alguma medida preventiva para a proteção de seus dados (por ex., troca de senha), ou - após a devida apuração e confirmação de todo o contexto do incidente, seu impacto, causa raiz, abrangência de titulares afetados, dentro do prazo de 10 (dez) dias, ou, na impossibilidade, em prazo prazo razoável a ser acordado com a ANPD com base na criticidade do incidente e volume de titulares afetados.
Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	Sugerimos que, uma vez comprovado o incidente, seja emitido no prazo de 2 (dois) dias da comprovação do incidente um comunicado informativo inicial aos titulares no site do controlador e/ou nos canais públicos que o controlador utiliza para divulgação de informações relevantes, nas hipóteses em que esta comunicação configure a possibilidade de contenção de eventuais danos que venham a ser causados aos titulares de dados. As demais formas de comunicação deveriam ser avaliadas caso a caso, mediante a necessidade e efetividade da comunicação e a particularidade do negócio do Controlador e os meios que o mesmo tem disponíveis para acessar o titular de dados.
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	Incidentes classificados como “Mínimo” ou “Limitado” considerando que na régua proposta esse tipo de incidente não representa dano relevante ao titular.
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	Incidentes classificados como “Mínimo” ou “Limitado” considerando que na régua proposta esse tipo de incidente não representa dano relevante ao titular.
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	Impacto para o titular – usar os critérios das perguntas acima.

Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	Recomendamos o framework de Cyber Security do National Institute of Standards and Technology (NIST), uma abordagem baseada em riscos para reduzir o risco de segurança cibernética, composta de três partes: Framework Core, Framework Profile e Framework Implementation Tiers.
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	Sugere-se que o tratamento do Incidente siga as etapas indicadas no Framework do National Institute of Standards and Technology (NIST). Outras medidas sugeridas seriam: realização de avaliação Forense do ambiente tecnológico; utilização de soluções para monitorar de maneira preventiva o tráfego com a internet e neste caso, avaliar a interrupção de comunicação do ambiente comprometido com a Internet e com empresas externas, iniciando a recuperação do ambiente impactado através de imagens seguras, que já possuam controles de segurança implementados suficientes para impedir a recorrência do incidente.
SUGESTÃO DE NORMATIVO, SE HOUVER	
Art. Xxxx	
Art. Xxxx	

ANPD Autoridade Nacional de Proteção de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: BANCO RABOBANK INTERNATIONAL BRASIL S/A.

CPF/CNPJ:01.023.570/0001-60

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.