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 cenário atual de incidentes de segurança nos permite confirmar que o risco existe sempre que houver posse indevida de qualquer dado pessoal, sensível ou não. Não obstante, o dano relevante somente se materializa quando efetivamente ocorrer alteração, destruição, divulgação, perda, roubo ou uso indevido dos dados, seja em mídia física ou eletrônica, gerando prejuízo ao titular. A mensuração do dano deve levar em consideração critérios objetivos de classificação de gravidade e cálculo da extensão do dano efetivo ao titular. Nesse contexto, sugerimos a adoção da Tabela de Severidade abaixo, a qual se baseia em determinados critérios para classificação de incidentes e análise de impactos, levando em consideração o risco potencial de incidentes e a materialidade do dano:

TABELA DE SEVERIDADE

Classificação de Impacto	Baixo 5	Médio 4	Moderado 3	Alto 2	Crítico 1
Regulatório	Sem impacto Regulatório	Baixo impacto Regulatório	Médio Impacto Regulatório	Risco de fiscalização/investigação/pedido de explicação por parte da Autoridade	Risco de suspensão ou perda de licença por parte da Autoridade
Reputacional	sem publicidade e/ou com baixa publicidade interna	Publicidade baixa (para fórum externo restrito)	Publicidade em mídia nacional e/ou internacional, por pequeno período de tempo	Publicidade em mídia nacional e/ou internacional, por período de tempo médio	Publicidade em mídia nacional e/ou internacional, por período de tempo longo
Impacto para o titular do Dado	Poucos Dados Pessoais não Sensíveis	Vários Dados Pessoais não Sensíveis	Muitos Dados Pessoais não Sensíveis	Muitos Dados Pessoais não Sensíveis e/ou poucos Dados Pessoais Sensíveis, atingindo a maior parte dos clientes, Terceiros, Parceiros de Negócios	Muitos Dados Pessoais não Sensíveis e/ou vários Dados Pessoais Sensíveis, atingindo todos os clientes, Terceiros, Parceiros de Negócios

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 seja subdivido de acordo com a matriz de risco e a governança de cada instituição. Conforme a Tabela de Severidade acima, sugerimos a divisão em 5 categorias de gravidade e risco: Baixo, Médio, Moderado, Alto e Crítico. A instituição deverá informar, com base nos critérios de relevância definidos e de acordo com as categorias contidas na Tabela de Severidade, quais situações deverão ser reportadas à ANPD, ao Titular dos dados ou a ambos. Para tanto, sugerimos a adoção de uma escala baseada nos critérios contidos na tabela, com base em um score obtido a partir da classificação em cada um dos critérios.
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	O risco é relacionado à potencial gravidade de um incidente. O dano ao titular é a materialização do risco, com efetivo prejuízo ao titular. Para fins de mitigação de risco, diversas ações podem ser tomadas conjuntamente pelo regulador e instituições processadoras de dados.
O que deve ser considerado na avaliação dos riscos do incidente?	A avaliação de risco de incidente deve ser conduzida diretamente por cada instituição, dentro de sua governança, tomando por base, inclusive, o tipo de cliente e o mercado no qual a instituição está inserida. Critérios de severidade específicos e setoriais podem ser considerados, sobretudo em decorrência de regulações específicas como incidentes que possam afetar o sistema financeiro, por exemplo.
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	Não é necessário nenhum acréscimo, entendemos serem suficientes aquelas 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)	A depender da materialidade do dano (tabela item 01), a comunicação deve seguir os mesmos critérios, sendo que a com maior gravidade deve ser comunicada em prazo menor, ainda que de forma preliminar. Após a ciência do Controlador, para os casos aplicáveis, o vazamento deverá ser notificado para a ANPD em até 72 horas seguindo o mesmo padrão da 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?	A comunicação deve ocorrer somente após a confirmação de que houve um incidente de segurança relevante ao titular, de acordo com os critérios contidos na Tabela de Severidade, até para que a instituição tenha tido tempo hábil para concluir seus procedimentos internos de apuração e investigação do incidente e tenha uma dimensão mais apurada sobre a extensão, gravidade e impactos do incidente de segurança envolvendo os dados pessoais do(s) titular(es). Nos casos em que houver necessidade de comunicação somente ao(s) titular(es), sugerimos que o prazo seja definido com base na quantidade de titulares que deverão ser comunicados, conforme definido de acordo com as políticas e procedimentos de comunicação de incidentes de cada instituição. Nos casos em que o Regulador também deva ser comunicado, sugerimos a adoção da mesma tabela de prazos para comunicação aos titulares, conforme previsto nas políticas e procedimentos de cada instituição e um prazo fixo para comunicação ao Regulador, de até 7 (sete) dias contados da ciência do incidente de segurança. Alternativamente, a depender, inclusive, da gravidade do incidente, o prazo pode ser definido em conjunto com o Regulador, bem como a forma e conteúdo da comunicação. De qualquer forma, a comunicação deverá ser feita na base dos melhores esforços utilizando os dados dos contatos existentes nos cadastros dos titulares junto aos Controladores. No mais, a comunicação de todo o detalhamento relacionado no §1º do art. 48 pode não ser eficaz, mas as instituições devem se assegurar de que as informações sejam suficientes para que o titular tenha conhecimento acerca do(s) dado(s) comprometido(s) e que seja estabelecido um canal de comunicação para sanar eventuais dúvidas e questionamentos que possam surgir.
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.)?	Para proporcionar a segurança e a agilidade da comunicação dos incidentes à ANPD sugerimos o uso do e-mail cadastrado no CERT.br como contato de segurança, assim como o cadastro do incidente em um website seguro da ANPD. De tal forma que o próprio titular consiga consultar se houve vazamento de seus dados e obter maiores informações sobre o incidente.
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	Conforme Tabela de Severidade acima.

Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	Conforme Tabela de Severidade acima.
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	Critérios contidos na Tabela de Severidade acima.
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	NIST ou quaisquer normas utilizadas como prática de mercado: 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/ - nist.gov/cyberframework/risk-management-framework https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-55r1.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?	Seguir as medidas já previstas na lei considerando, (art. 52) observada a proporcionalidade e análise de risco e dano efetivamente materializado.
SUGESTÃO DE NORMATIVO, SE HOUVER	
Art.	
Art.	

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: RODOIL DISTRIBUIDORA DE COMBUSTÍVEIS S.A.

CPF/CNPJ: 07.520.438/0001-40

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 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 identificado vazamento, destruição, alteração de dados de pessoa física, contendo: CPF, contatos do titular, cartão de crédito, senhas, padrões de consumo ou dados sensíveis 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, ambos devem ser classificados. O dano pode ser em duas categorias, levando em consideração a quantidade de dados de um mesmo titular, bem como se o mesmo é sensível ou não. (As categorias poderiam ser Alto e Baixo). O nível baixo entendemos não ser relevante. Quanto risco sugere-se a utilização da classificação definida na ISO 27000.**
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	**O risco se caracteriza pela análise da probabilidade x impacto que aquele vazamento pode ocasionar ao titular. O dano se caracteriza pelo prejuízo financeiro ou moral, causado pelo incidente. Espera-se a definição de um nível mínimo de comprovação dos referidos prejuízos pelo titular do dado e a vinculação com a empresa que forneceu o dado.**
O que deve ser considerado na avaliação dos riscos do incidente?	**a) Que tipos de danos o incidente ocasionou ao titular (e qual sua classificação – Baixo ou Alto);** **b) Quantidade de dados do mesmo titular;** **c) Natureza dos dados pessoais;** **d) Se houve reclamação do titular perante a ANPD ou outro órgão;** **e) Impacto que o incidente pode ocasionar ao titular;**

Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	**Entendemos suficientes as listas no §1º do art. 48.**
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	**5 (cinco) dias (úteis), ressalvadas ações que dependam exclusivamente de operadores ou co-controladores (terceiros), o que deverá ser analisado de forma específica, quando comprovado que o controlador tomou todas as medidas estabelecidas 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 comunicação? As mesmas do §1º do art. 48?	**No mesmo prazo de informar a ANPD (5 dias úteis), desde que sejam permitidas formas de comunicação em massa e mídias digitais. As informações não seriam as mesmas, o que deveríamos passar seriam quais informações foram vazadas e quais medidas foram tomadas para reverter ou mitigar os efeitos do prejuízo. No caso de possível vazamento de senhas, deveríamos instruir aos titulares a realizar a imediata alteração de senha.**
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.)?	**E-mail, telefone, site institucional ou outras mídias digitais oficiais (ficando a escolha a critério da empresa). Ou seja, sendo permitida a comunicação pública.**
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	**Somente informar quando os riscos e os danos forem altos (respeitando a classificação supra citada).**
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	**Idem acima.**

Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	**Idem acima, ou seja, quando o risco foi classificado como Alto.**
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?	**Apresentação de plano de ação para correção da vulnerabilidade e comunicação aos titulares.**
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: Sociedade Beneficente Israelita Brasileira Hospital Albert Einstein – SBIBHAE

CPF/CNPJ: 60.765.823/0001-30

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?	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	

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

NOME DA INSTITUIÇÃO/PESSOA FÍSICA:

SINDUSFARMA – SINDICATO DA INDÚSTRIA DE PRODUTOS FARMACÊUTICOS

CPF/CNPJ: 62.646.633/0001-29

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
Apresentação Preliminar	A **INTERFARMA** – Associação da Indústria Farmacêutica de Pesquisa, é uma entidade setorial, sem fins lucrativos, criada em 1989. A associação representa mais de 50 empresas que promovem e incentivam a pesquisa, o desenvolvimento e a inovação voltada para a produção de insumos farmacêuticos, matérias-primas, medicamentos e produtos para a saúde humana. Mesmo pertencentes a grupos internacionais, nossas associadas têm instalações no Brasil e, geram emprego, renda e tributos ao país. São condições para fazer parte da INTERFARMA: conduzir atividades privadas de pesquisa, desenvolvimento e inovação no setor farmacêutico. Empresas associadas também são compelidas a aderir ao Código de Conduta da Associação, que estabelece princípios e normas para assegurar a conduta ética e as boas práticas no setor. Maiores informações sobre laboratórios associados, nosso código e iniciativas, visite nossa página www.interfarma.org.br .

	O **SINDUSFARMA** foi fundado em 26 de abril de 1933 e tem como associados fabricantes, importadoras e exportadoras de produtos farmacêuticos, correlatos e afins, destinados à saúde humana, que atualmente sumam mais de 200 empresas em todo o Brasil. Entre outras, são atividades institucionais do Sindicato, nos termos da lei e de seu estatuto social, a realização de estudos, representação dos direitos e interesses gerais da categoria perante as autoridades públicas, celebração de convenções coletivas do trabalho, atuação como órgão técnico, consultivo, educacional e social.
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?	As Entidades entendem, sob este aspecto, que um incidente de segurança da informação envolvendo a violação de dados pessoais (Art. 48), de fato pode acarretar dano relevante ao titular quando o incidente expuser o titular do dado a riscos de uso inadequado e mal-intencionado de seus dados pessoais e/ou sensíveis, e que possam acarretar danos materiais (financeiros), morais/psicológicos (discriminação e reputação) ou ainda risco de sequestro, violação de direitos e liberdade fundamentais. Critérios a serem considerados: tipo e quantidade de informação exposta, contexto da exposição (ataque cibernético, phishing, malware, má conduta etc.), tempo e local de exposição da informação (divulgação em fóruns de venda dark web), qualificação do titular (idoso, criança, incapazes), probabilidade de materialização**.**
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, as Entidades entendem que se faz necessária a subdivisão entre categorias de danos para avaliar devidamente quando ele se mostra relevante. Neste sentido, nosso entendimento é de que o risco será: • **Muito Baixo** – Nas situações em que o vazamento de dados pseudoanonimizados e/ou dados já tornados públicos pelo titular de dados e/ou disponíveis na internet e/ou outros dados que não possam gerar ao titular de dados nenhum dano ou inconvenientes mínimos sobre os direitos e liberdade fundamentais, e que podem ser superados sem maior complexidade (ex. tempo gasto para inserir informações novamente, aborrecimentos, irritação etc.). • **Baixo** – Nas situações em que os dados pessoais de nível 2 (ver conceito na pergunta 11 abaixo) envolvidos gerem dano ou inconvenientes moderados sobre os direitos e liberdade

	fundamentais dos titulares dos dados, e que podem ser superados com pouca dificuldade/complexidade (ex. medo, falta de compreensão, custos extras etc.). • **Médio** – Nas situações em que houver comprovadamente danos repercutindo em inconvenientes significativos sobre os direitos e liberdade fundamentais dos titulares dos dados, e que podem ser superados, mas com algumas dificuldades/complexidade (ex. ansiedade ou angústia, pequenas doenças físicas, negação de acesso a serviços comerciais etc.). • **Alto** – Nas situações em que houver comprovadamente danos significativos sobre os direitos e liberdade fundamentais dos titulares dos dados, e que podem ser superados, mas com sérias dificuldades/alta complexidade (ex. perda de emprego, intimação, piora da saúde etc.). • **Muito alto** - Nas situações em que houver comprovadamente danos significativos sobre os direitos e liberdades fundamentais dos titulares dos dados, e que podem não ser superados (ex. graves dificuldades financeiras, doenças fisiológicas ou físicas de longo prazo, morte etc.).
3.Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	As Entidades entendem, em síntese, que riscos podem não acarretar danos ao titular dos dados concretamente. A existência de eventual dano precisa ser analisada caso a caso, a fim de avaliar se houve de fato prejuízo aos titulares de dados. Apenas a avaliação entre agentes e autoridade poderá concluir que o risco, eventualmente concretizado, gerou de fato dano (e em que medida indenizável).
4. O que deve ser considerado na avaliação dos riscos do incidente?	As Entidades entendem que os critérios para essa avaliação foram apresentados na resposta 2 acima. Cabe ainda a avaliação de que tipo de danos os titulares podem estar expostos e a probabilidade do risco se materializar (raro/incomum, improvável, possível, provável ou quase certo).
5. Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	As Entidades acreditam que, para que a ANPD tenha informações suficientes para avaliar o nível de gravidade do incidente e em que medida o agente de tratamento em questão estava preparado para proteger os dados, nossa proposta é que os controladores informem, de acordo com as informações disponíveis no momento da notificação, adicionalmente: a) Dia e Hora da ocorrência do incidente; b) Duração do incidente; c) Breve descrição do incidente - Informações sobre a natureza e o possível impacto do incidente para os agentes de tratamento e os titulares; d) Status do incidente- indicar se (i) ainda em andamento; (ii) encerrado ou (iii) em andamento, porém gerenciado e contido;

	e) Causa do incidente, se conhecida e em que extensão conhecida; f) Informação sobre eventual comunicação já enviada aos titulares dos dados que foram comprometidos com o incidente; g) Descrição de eventuais medidas já adotadas para evitar que futuros incidentes semelhantes venham a ocorrer; h) Dados de contato do Encarregado.
6. Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	A experiencia compartilhada pelas associadas das Entidades demonstra que a (in)determinação de prazo específico para notificação à autoridade competente acerca de um incidente de segurança não é algo exclusivo do Brasil. Nesse sentido, países como EUA, Australia e os europeus sob GDPR não tem cravado prazo razoável para tal comunicação pela complexidade que a sua compreensão e investigação pode tomar no caso concreto. Logo, definir um prazo adequado e razoável, mas não obrigatório em qualquer circunstância, pode ser solução mais adequada, uma vez que o controlador mantenha compromisso de munir a autoridade de demais informações tão logo estas sejam investigadas e compreendidas. Fundamental, a nosso ver, é que haja harmonização e alinhamento a padrões internacionais, uma vez que hoje vivemos economias globalizadas e as empresas estão cada vez mais conectadas, mesmo que sujeitas a autoridades locais em diversos territórios. Dessa forma, é impraticável que cada regulamento decida o seu “prazo mínimo” que entenda razoável, o que minaria a cadeia de contratos internacionais entre agentes de processamento, hoje imprescindível para o bom andamento da economia. Da mesma forma que existem mínimos globais para regulamentar direitos de propriedade intelectual, é altamente recomendável o mesmo para regras de proteção de dados. Portanto, pelo cenário internacional ora posto que coloca GDPR como referência já estabelecida, entende-se que o prazo de 72 horas do conhecimento do incidente é o mais adequado para melhor inserir o país no contexto internacional e facilitar a adequação das empresas que atuam no Brasil e em demais países.

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?	Quanto ao prazo para notificação ao titular de dados, a posição das Entidades conforme apresentada aqui é no sentido de que tal notificação nem sempre se fará necessária. No mais, ela deve sempre pautar pela individualidade e buscar não expor o titular publicamente. Cada situação, portanto, merece devido discernimento quanto às medidas a serem tomadas e, neste raciocínio, nos parece adequado que a definição quanto ao prazo e as formas para notificação dos titulares seja algo a ser pactuado diretamente entre autoridade e controlador envolvido. Por fim, avaliando o rol de itens do §1º do art. 48, sob a perspectiva do titular, entendemos que é relevante a inclusão das seguintes informações:(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.
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.)?	Na visão das Entidades é recomendável que a comunicação possa ser direta / individual e/ou pública a critério do controlador, considerando que em alguns casos é possível que não sejam localizados os dados de contato atualizados do titular para a comunicação de forma que este possa vir a tomar conhecimento do incidente por meio de comunicação pública e, assim, tomar providências para se resguardar. Entendemos ser salutar que esta decisão se de entre o controlador afetado e a ANPD caso a caso, frente as particularidades da situação conforme avaliada no momento (extensão, gravidade, número de titulares envolvidos, sensibilidade dos dados e da comunicação, possíveis consequências da comunicação, meios disponíveis etc.). Em nenhum caso deveria ser permitido que a comunicação seja em si uma violação de outros dados pessoais e/ou uma indevida exposição de sua privacidade.
9. Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	Mais uma vez, a avaliação de padrões adotados em outras jurisdições é relevante para respondermos. Essa avaliação demonstra que, a despeito de um alinhamento global robusto, as medidas postas sempre se voltam para avaliação de risco, ou seja, se realmente o fato a ser reportado pode gerar risco (e eventual dano) ao titular envolvido (exemplos consultados Canadá, UK e Califórnia).

	As Entidades se alinham a esse posicionamento e, como trazido neste documento, advoga que para incidentes de segurança que não representem risco relevante aos titulares a comunicação a autoridade não deve ser necessária.
10. Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	As Entidades entendem ser adequado que incidentes de muito baixo e baixo risco, devidamente e comprovadamente controlados, através das ações corretivas e preventivas adotadas não devam ser obrigatoriamente comunicados aos titulares. A depender, como dito do tipo de dados vazados e número de pessoas afetadas.
11. Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	As Entidades defendem que critérios internacionalmente reconhecidos, sejam adotados pela autoridade nessa avaliação para, dentre outras razões, tornar mais fácil a harmonização dos critérios, metodologias e processos internos. Neste sentido, a sugestão das Entidades é pela adoção dos critérios da European Union Agency of CyberSecurity (ENISA) disponíveis em https://www.enisa.europa.eu/risk-level-tool/methodology . Em consonância com tal sugestão, as Entidades entendem que os critérios a serem adotados pela ANPD deveriam levar em conta os aspectos abaixo relacionados: 1. CT - Categoria de titulares de dados e a quantidade de dados individuais (Dados cadastrais, Dados Sensíveis) Art. 5º § I e II a. Dados simples (peso = 1 ou 2) considerando o tipo e a quantidade b. Dados sensíveis (peso = 3 ou 4) levando em conta o tipo e a quantidade 2. CVP - Circunstâncias da violação de dados pessoais – Possíveis impactos negativos a Confidencialidade, Integridade ou Disponibilidade do dado pessoal a. Confidencialidade = 0, 0,25 e 0.50 i. 0 - risco de confidencialidade sem evidência de processamento ilegal. ii. 0,25 – dados expostos para um número de pessoas conhecido. iii. 0,50 – dados expostos para um número desconhecido de pessoas (redes sociais, dark web). b. Integridade = 0, 02,5 e 0,50 i. 0 - dados alterados, mas sem qualquer uso incorreto ou ilegal comprovado.

	ii. 0,25 - dados alterados e possivelmente usados de forma incorreta ou ilegal, mas com possibilidade de recuperação. iii. 0,50 - dados alterados e possivelmente usados de forma incorreta ou ilegal, sem possibilidade de recuperação. c. Disponibilidade = 0, 0,25 e 0,50 i. 0 - os dados podem ser recuperados sem qualquer dificuldade. ii. 0,25 - indisponibilidade temporal dos dados, cuja disponibilidade poderá ser reconstruída a partir de outras bases de dados. iii. 0,50 - indisponibilidade total (os dados do controlador ou dos indivíduos não podem ser recuperados). 3. FI - Determinar a facilidade com que os dados pessoais envolvidos identificam diretamente o individuo a. FI = 0,25 – Insignificante b. FI = 0,50 - Limitado c. FI = 0,75 - Significante d. FI = 1 – Impacto direto Com as informações acima seria, portanto, possível calcular o potencial de dano ao indivíduo através da equação: **GV - Gravidade = CT x CVP + FI.** E como critérios de avaliação, teríamos: GV < 2 = **Risco baixo**: Os indivíduos não serão afetados ou podem encontrar alguns inconvenientes. GV >= 2 e <3 **Risco Médio**: Os indivíduos podem encontrar inconvenientes significativos, que serão capazes de superar, apesar de algumas dificuldades. GV >=3 e <4 **Risco Alto:** Os indivíduos podem enfrentar consequências significativas, que devem ser capazes de superar, embora com sérias dificuldades. GV = ou > 4 **Risco muito alto:** Os indivíduos podem enfrentar consequências significativas, ou mesmo irreversíveis, que podem não superar. Dado que no contexto desta consulta também se discute os critérios a serem adotados na tomada de decisão quanto a reporte aos indivíduos, as Entidades entendem que a metodologia acima pode igualmente servir para criar tais parâmetros. Logo, a ANPD poderia considerar os níveis de reporte seguindo a ordem:

	• GV <2 – Reportar a ANPD sem necessidade de notificação aos titulares de dados. O reporte deve conter a análise de riscos deste documento e as medidas tomadas para mitigação do risco ao titular. • GV >2 e <3 – Reportar a ANPD e avaliar a necessidade de notificação aos titulares de dados. O reporte deve conter as mesmas análises mencionadas acima e, também, as medidas tomadas para mitigação do risco ao titular incluindo monitoramento de dados ativo na internet e deep web, além de serviços de análise de uso de documentos como Serasa, Consumidor Positivo. • GV >3 – Reportar a ANPD e aos titulares de dados. O reporte deve conter a análise de riscos deste documento e, também, as medidas tomadas para mitigação do risco ao titular incluindo monitoramento de dados ativo na internet e deep web, serviços de análise de uso de documentos como Serasa, Consumidor Positivo. A organização deve vincular as ações em canais de grande acesso como TV e Internet. Deve disponibilizar um número de contato com a empresa através de website próprio e deve dispor um formulário de contato com a empresa.
12. Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	No mesmo sentido, as Entidades defendem que a mesma fonte metodológica da European Union Agency of CyberSecurity (ENISA). Esta metodologia trata incidentes de segurança da informação com violação de dados pessoais. Desta forma, sob essa avaliação, os critérios que deveriam ser adotados pela ANPD a nosso ver levariam em conta os aspectos abaixo relacionados: 1. CT - Categoria de titulares de dados e a quantidade de dados individuais (Dados cadastrais, Dados Sensíveis) (Art. 5º § I e II) a. Dados simples (peso = 1) b. Dados sensíveis (peso = 3) 2. CVP - Circunstâncias da violação de dados pessoais – Possíveis impactos negativos a Confidencialidade, Integridade ou Disponibilidade do dado pessoal. a. Confidencialidade = 0, 0,25 e 0.50 i. 0 - risco de confidencialidade sem evidência de que ocorreu processamento ilegal. ii. 0,25 – Dados expostos para um número de pessoas conhecidos

	iii. 0,50 – Dados expostos para um número desconhecido de pessoas (Redes sociais, dark web) b. Integridade = 0, 02,5 e 0,50 i. 0 - dados alterados, mas sem qualquer uso incorreto ou ilegal identificado ii. 0,25 - dados alterados e possivelmente usados de forma incorreta ou ilegal, mas com possibilidade de recuperação iii. 0,50 - dados alterados e possivelmente usados de forma incorreta ou ilegal, sem possibilidade de recuperação: c. Disponibilidade = 0, 0,25 e 0,50 i. 0 - os dados podem ser recuperados sem qualquer dificuldade ii. 0,25 - indisponibilidade temporal e pode ser reconstruído a partir de outras bases de dados iii. 0,50 - Indisponibilidade total (os dados não podem ser recuperados do controlador ou dos indivíduos 3. FI - Determinar a facilidade com que os dados pessoais envolvidos identificam diretamente o individuo a. FI = 0,25 – Insignificante b. FI = 0,50 - Limitado c. FI = 0,75 - Significante d. FI = 1 – Impacto direto Com as informações acima seria, portanto, possível calcular o potencial de dano ao indivíduo através da equação: **GV - Gravidade = CT x CVP + FI.** E como critérios de avaliação, teríamos: **GV < 2 = Risco Baixo** - Os indivíduos não serão afetados ou podem vivenciar alguns inconvenientes. **GV >= 2 e <3 Risco Médio** - Os indivíduos podem vivenciar inconvenientes significativos, que serão capazes de superar, apesar de algumas dificuldades. **GV >=3 e <4 Risco Alto** - Os indivíduos podem enfrentar consequências significativas, que devem ser capazes de superar, embora com sérias dificuldades. Reforçamos que a metodologia mencionada aqui está disponível no link abaixo: https://op.europa.eu/en/publication-detail/-/publication/dd745e70-efb8-4329-9b78-79020ec69da5

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 Entidades compreendem ser fundamental a atuação da ANPD como promovedora da cultura de proteção de dados no país. Nesta linha, vemos que é importante à Autoridade elaborar documentos e guias para implementação de controles de segurança da informação aptos a proteger os dados em todo o ciclo de vida desde a coleta, uso, armazenamento e descarte. Estas medidas a serem encorajadas devem proteger os dados e informações de maneira proativa, evitando ou diminuindo a probabilidade de ocorrência de incidentes de segurança da informação ou que, caso ocorram, tragam impactos diminuídos com ações rápidas e monitoramento ativo. Ademais, medidas técnicas e administrativas preventivas incluiriam: • Aplicação de políticas estruturantes de proteção de dados e de procedimentos técnicos e de usuários. • Análises de vulnerabilidades técnicas contemplando os ativos de informações como hardware, sistemas operacionais, bancos de dados, sistemas e aplicativos. • Análise de testes intrusivos também conhecidos como *Pentests* (simulação controlada de um ataque) com o objetivo de entender se as proteções adotadas estão aptas a proteger e permitir que correções sejam implementadas. Este teste pode ser executado em frequências regulares e de acordo a criticidade dos dados (quantidade de dados *versus* tipo de dado). • Programas de *Bug Bounty* que visam oferecer pagamentos a quem descobrir vulnerabilidades nos sistemas da organização. Esta medida já é adotada largamente por grandes empresas de tecnologia e pelo mercado corporativo internacional, majoritariamente. • Medidas a serem adotadas após um comunicado de incidente. Por fim, medidas técnicas e administrativas após a comunicação de incidentes de segurança incluiriam: • Se necessário, suspender temporariamente o serviço ou reduzir as funcionalidades disponíveis (a análise deverá considerar o tipo de serviço e o dano aos titulares de dados).

	• Se necessário, acionar o plano de continuidade de negócios (se o sistema principal for comprometido) para que a organização continue operando com o mínimo necessário de serviços. • Análise forense digital e legal para entender como o ataque ocorreu e assim permitir que medidas técnicas sejam providenciadas para evitar outros ataques semelhantes. Esta análise pode evoluir para uma investigação criminal caso seja detectada a ação de atacantes externos (considere que somente autoridade policiais investigativas podem exercer tal atividade). • Revisão das políticas de segurança da informação e privacidade e proteção de dados para atualização com as lições aprendidas na análise forense com foco na gestão de acessos e aplicação de correções de vulnerabilidades e atualizações de hardware e software. • Recomendação de monitoramento através de SOC – Security Operations Centers em busca de possíveis correlações a violação de dados pessoais. • Estabelecer contato com CSIRT BR - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. • Treinar os times de resposta a incidentes considerando as lições aprendidas. • Treinar todo o time para prevenir novos incidentes de segurança da informação. Mais uma vez, nossas sugestões estão suportadas por iniciativas da ENISA, encontradas através do link https://www.enisa.europa.eu/publications/good-practice-guide-for-incident-management
SUGESTÃO DE NORMATIVO, SE HOUVER	
As Entidades não têm sugestão no momento.	

CONTRIBUIÇÃO TOMADA DE SUBSÍDIO ANPD Nº 2/2021

Asshaias Felippe [redacted]

ter 23/03/2021 18:21

Para: ANPD - Consulta Publica <consultapublica@anpd.gov.br>; [redacted]

1 anexo

CONTRIBUIÇÃO TOMADA DE SUBSÍDIOS ANPD N 2 -2021 INCIDENTE DE SEGURANÇA.pdf;

Prezados,

Venho por meio deste, enquanto Sócio Fundador e atual Conselheiro da empresa SOLINTEL – SOLUÇÕES INTELIGENTES EM TELECOMUNICAÇÕES LTDA, pessoa jurídica inscrita no CNPJ nº 08.429.293/0001-39, respeitosamente à presença dessa Autoridade Nacional de Proteção de Dados Pessoais – ANPD, apresentar contribuição referente à Tomada de Subsídios nº 02/2021.

A SOLINTEL é empresa de assessoria técnica-regulatória para provedores de telecomunicações com aproximadamente 15 anos de mercado e uma carteira de clientes de mais de 2000 provedores de internet, de pequeno a médio porte.

Sempre atenta aos impactos do setor de telecomunicações e com cultura preventiva e orientativa, a SOLINTEL tem buscado, antes mesmo da LGPD entrar em vigor, orientar seus clientes para que se adequem em relação às obrigações da nova lei.

É evidente que o setor de telecomunicações movimenta robustos bancos de dados pessoais e, cabe aqui pontuar, que os provedores de internet de pequeno porte, hoje, juntos, formam a maior prestadora do país.

Por outro lado, tratam-se de pequenas empresas, que não diferente de outros ramos, possuem dúvidas, incertezas, e dificuldades em operacionalizar as obrigações contidas na LGPD.

Motivo pelo qual, além da SOLINTEL buscar a conscientização de seus clientes em relação à proteção de dados pessoais, não poderia essa empresa deixar de se manifestar neste momento oportuno em que esta Autoridade, brilhantemente, abre a palavra para que o público em geral se manifeste sobre a regulação aplicável para microempresas e empresas de pequeno porte em relação à LGPD.

Desde já, a SOLINTEL parabeniza e agradece a conduta da ANPD na abertura desta Tomada de Subsídios e se coloca à disposição para o que for necessário.

Asshaias Felippe
Conselho
[redacted]

ANPD Autoridade Nacional de Proteção de Dados

CONTRIBUIÇÃO REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2021

NOME DA INSTITUIÇÃO: SOLINTEL - SOLUÇÕES INTELIGENTES EM TELECOMUNICAÇÕES LTDA

CNPJ: 08.429.293/0001-39

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?	**Assim como no cenário internacional, entende-se que para se verificar se um incidente pode acarretar risco ou dano relevante ao titular é necessário realizar a avaliação do risco, tendo por princípio que risco relevante é aquele decorrente de violação suscetível de afetar direitos e liberdades do titular de dados, podendo resultar em perda de controle sobre seus dados, limitação de direitos, discriminação, roubo ou usurpação da identidade, perdas financeiras, danos para reputação, entre outros. Assim, é preciso, mediante avaliação, 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?	**Defende-se que, assim como se dá na União Europeia é necessário que se considere 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 deverá ser ponderada como critério na avaliação do risco, haja vista que se acredita que dependendo da natureza dos dados**

	pessoais afetados uma violação (por exemplo dados sensíveis, bancários, etc) o dano poderá ser particularmente severo, é o caso de roubo, usurpação de identidade, entre outros.
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 esta regra seja medida de regulação assimétrica, para que pequenas, médias empresas possuam um prazo superior ao de grandes empresas para envio da comunicação, sendo esse o caso, aponta-se o prazo de 05 (cinco) dias úteis.** **Ainda, defende-se que seria necessário que a regulação brasileira abordasse a possibilidade de entrega parcial de informações à ANPD, em situações específicas quando o levantamento de informações depende de prazo superior ao próprio prazo fixado para notificação 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 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. Caso não seja este o entendimento da ANPD, sugere-se que esta regra seja medida de regulação assimétrica, para que pequenas, médias empresas possuam um prazo superior ao de grandes empresas para envio da comunicação, sendo esse o caso, aponta-se o prazo de 05 (cinco) dias úteis.** **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 determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	**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. Por sua vez, acredita-se que independentemente da situação, deve esta matéria ser tema de regulação assimétrica em favor de pequenas e médias empresas, de modo que essas empresas não necessitem realizar a comunicação de forma individualizada em qualquer hipótese que seja, sendo, então, estabelecido que a comunicação se dará de forma pública.** **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.** **No caso dessas medidas serem adotadas na regulação brasileira, que seja oportunizado ao controlador manifestar na própria notificação do incidente à ANPD a adoção de medidas técnicas, a fim de informar a dispensa da comunicação aos titulares, podendo a ANPD, em um segundo momento solicitar documentação complementar se entender pertinente.**
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 dano. 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 serem apresentados à ANPD.**

ANPD Autoridade Nacional de Proteção de Dados

CONTRIBUIÇÕES REFERENTES À TOMADA DE SUBSÍDIOS Nº 02 /2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: Clientes do setor de óleo e combustíveis, GLP, armazenagem de granéis líquidos, Indústria de especialidades químicas, plataforma de pagamentos digitais e varejo farmacêutica.

CPF/CNPJ: não se aplica.

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 pode acarretar risco ou dano relevante para os titulares principalmente quando o incidente envolver: **(i)** dados pessoais sensíveis ou que possam levar ao conhecimento de um dado pessoal sensível; **(ii)** dados de crianças e adolescentes); **(iii)** dados que tenham 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; **(iv)** dados que possam gerar risco a liberdade e direitos fundamentais; ; **(vi)** eventos cuja volumetria (quantidade de indivíduos afetados) tenha sido elevada de acordo com a metodologia indicada na resposta à pergunta 11.. Links para acesso às fontes internacionais: • Diretrizes ICO – Personal Data Breaches (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/) • Guideline – Article 29 Working Party - Guidelines on Personal data breach notification under Regulation 2016/679 (https://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49827)

	• EDPB – Guidelines 01/2021 on Examples regarding Data Breach Notification (https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2021/guidelines-012021-examples-regarding-data-breach_pt)
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, via de regra, o risco pode ser classificado em 4 (quatro) níveis: **1- RISCO BAIXO**: Quando o incidente não gera qualquer possibilidade de dano relevante ao titular, tendo em vista inexistência de dados pessoais sensíveis, informações financeiras e dados pessoais de crianças e adolescentes, sendo remota qualquer possibilidade de danos de natureza física, psíquica, material ou imaterial; **2- RISCO MÉDIO**: Quando o incidente não gera possibilidades concretas de dano relevante ao titular, podendo existir informações financeiras, mas que não permitem inferências significativas sobre a condição econômica do indivíduo, nem possibilitam qualquer tipo de fraude. Ademais, incidentes de risco médio também não envolvem dados pessoais sensíveis e dados de crianças e adolescentes, sendo remota qualquer possibilidade de danos de natureza física, psíquica, material ou imaterial; **3- RISCO ALTO**: Quando o incidente gera possibilidades dano relevante ao titular, tendo em vista a presença de dados pessoais financeiros, viabilizando denotar o status social do indivíduo, ou quando é possível presumir dados sensíveis, mas sem que necessariamente tenham sido expostas informações sensíveis, permitindo uma inferência; **4- RISCO MUITO ALTO**: Quando o incidente gera possibilidade concreta de dano relevante e/ou grave, devido ao vazamento de informações sensíveis, de crianças e adolescentes e/ou informações financeiras, viabilizando situações possíveis de danos de natureza física, psicológica, material ou imaterial. Pelo racional acima, entendemos que somente os riscos enquadrados como ALTO e MUITO ALTO apresentam possibilidade de “risco ou dano relevante” ao titular, ensejando a notificação. Por outro lado, os riscos avaliados como BAIXO ou MÉDIO não representam qualquer tipo de ameaça de “risco ou dano relevante”, desnecessitando, em tese, de notificação para a ANPD e os Titulares.
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	O Risco é que uma situação ou operação de tratamento suscetível de ocasionar danos efetivos ao titular (situações lesivas), no âmbito material, imaterial, físico ou psicológico. O dano, por sua vez, é a materialização e efetivação do risco que ocorre quando há efetiva perda de dados que tenha ocasionado prejuízos concretos ao titular, sejam eles pecuniários ou não, materiais ou morais, físicos ou psicológicos.
O que deve ser considerado na avaliação dos riscos do incidente?	A avaliação de riscos faz parte do processo de gestão de riscos e possibilitará a criação de um plano de contingência para avaliar suas consequências e as medidas a serem adotadas. Devem ser considerados, observadas as especificidades do caso em análise: (i) o contexto em que se deu o incidente; (ii) a existência de mecanismos de controles internos, tais como controles técnicos e organizacionais, segurança da

	informação, segurança física, existência de políticas e procedimentos e de mecanismos de gestão de incidentes; (iii) o tipo de ameaça, a origem da ameaça, o contexto em que a ameaça foi detectada; (iv) o nível de vulnerabilidade de segurança dos sistemas afetados; (v) o perfil e a volumetria dos titulares afetados; (vi) o impacto sobre os indivíduos afetados; (vii) a categoria dos dados afetados (por exemplo: dados cadastrais, dados comportamentais, dados financeiros, dados sensíveis e dados de crianças e adolescentes). (Guideline da Autoridade Espanhola de Proteção de Dados) Links para acesso às fontes internacionais: • Agencia Española de Protección de Datos – Guide on Personal Data Breach Management and Notification (https://www.aepd.es/sites/default/files/2019-09/Guide-on-personal-data-breach.pdf)
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	Além dos itens mencionados no art. 48, § 1º da LGPD, é importante, ainda, que a notificação contenha informações sobre: ▪ O contato do Encarregado pela Proteção de Dados da Companhia ou de outra pessoa junto à qual seja possível obter maiores detalhes sobre o ocorrido; ▪ Informações sobre a notificação estar completa ou parcial e justificativas sobre o motivo de ser parcial, se for o caso. Deve ser identificado, ainda, se se trata da primeira notificação ou se se trata de uma notificação adicional (complementar). ▪ Informações sobre a data/hora em que ocorreu o Incidente e data/hora da ciência pelo Controlador; ▪ Informações sobre as circunstâncias nas quais se deu o incidente (roubo, violação, fraude, cópia etc.), bem como fazer um resumo do incidente. ▪
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	03 dias úteis a partir do momento em que o Controlador confirmou o Incidente envolvendo dados pessoais, e gradativamente caso não tenha informações suficientes na ocasião da notificação, justificando o envio parcial e promovendo o envio completo de informações o mais rapidamente possível.
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	03 dias úteis a partir do momento em que o Controlador confirmou o Incidente envolvendo dados pessoais. Sugerimos que a notificação contenha as seguintes informações: **(a)** o Contato do Encarregado pela proteção de dados ou outra pessoa junto à qual seja possível obter informações sobre o evento; **(b)** a descrição dos dados envolvidos; **(c)** a data do incidente; **(d)** possíveis consequências do Incidente; **(e)** medidas mitigadoras adotadas; **(f)** recomendações aos Titulares sobre quais medidas adotar para que possam se proteger das consequências do Incidente.

comunicação? As mesmas do §1º do art. 48?	A critério do controlador, avaliado o risco e a categoria do titular , o controlador poderá adotar medidas de , notificação também gradativagradativasgradativa, caso não se tenha informações suficientes na ocasião da notificação, justificando o envio parcial e promovendo o envio completo de informações o mais rapidamente possível. No caso o Controlador deverá avaliar se a notificação gradativa possibilitará ao titular adotar alguma medida eficaz para mitigação de riscos decorrentes 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.)?	A comunicação deve se dar de forma clara e simples, respeitada a expectativa do titular, bem como a necessidade de formalização do contato. Assim, sugerimos que a regra de envio seja, em um primeiro momento, por meio postal ou e-mail, com confirmação de recebimento (nunca por telefone), com preferência pela notificação em meios digitais. Caso não seja comprovado o recebimento da comunicação, ou realiza-la envolva esforço desproporcional, a sugestão é que seja feita comunicação de forma pública. No caso de comunicação pública, esta não deve conter detalhes sobre o Incidente, mas apenas o contato do encarregado pela proteção de dados a fim de que o titular busque informações detalhadas sobre o ocorrido. Se necessário a comunicação pública, sugerimos que a ANPD disponibilize um ambiente próprio no seu site para disponibilização da referida comunicação, a exemplo do que acontece com o recall, que possui ambiente especifico no site do Procon onde os consumidores podem também consultar empresas que estão promovendo recall: http://www.procon.rj.gov.br/index.php/publicacao/listar/4/1
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	a) Situações nas quais o risco seja classificado como baixo ou médio; b) Situações nas quais as medidas corretivas adotadas posteriormente ao incidente tiverem sido eficazes, revertendo os riscos de dano relevante ou **minorando-os**; c) Situações nas quais comprovadamente o Incidente não gerará danos aos titulares (vide GDPR); d) Situações nas quais os dados estejam codificados e sejam ininteligíveis (vide WP29);
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	a) Situações nas quais as medidas corretivas adotadas posteriormente ao incidente tiverem sido eficazes, **eliminando** o risco de dano ao titular; (vide GDPR) b) Situações nas quais comprovadamente o Incidente não gerará danos aos titulares, observadas as especificidades do caso em análise (vide GDPR); c) Situações nas quais os dados estejam codificados e sejam ininteligíveis (vide WP29); d) Situações em que envolva esforço desproporcional para a notificação Links para acesso às fontes internacionais: • Guideline – Article 29 Working Party - Guidelines on Personal data breach notification under Regulation 2016/679 (https://ec.europa.eu/newsroom/article29/document.cfm?doc_id=49827)

	• Regulation 679 / 2016 GDPR (Arts 33 e 34)
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	A análise de gravidade pode ser realizada através do cálculo da severidade pode ser dado a partir da seguinte fórmula: S=CPD×FI+CI -> S*FV = SF Sendo: **S – Severidade do incidente**: o grau de severidade do incidente, que vai definir quais incidentes devem ser priorizados para o ato de remediação. A severidade pode ser classificada de acordo com o resultado da equação da seguinte forma: ▪ 0,00 a 1,99 – Baixa ▪ 2,00 a 2,99 – Média ▪ 3,00 a 3,99 – Alta ▪ 4,00 para cima – Muito alta **CPD – Contexto do processamento de dados**: Criticidade da informação, tendo em conta o contexto específico do processamento de dados e sua categoria. **FI – Facilidade de identificação**: Facilidade de um terceiro acessar um conjunto de informações e fazer a correspondência de certo indivíduo. **CI – Circunstâncias do incidente**: Circunstâncias específicas do incidente. Assim, para verificação da gravidade do incidente, é necessário que os critérios previstos na fórmula sejam pontuados com notas que variem de 0 a 4, considerando as criticidades baixa, média, alta e muito alta. SF – Severidade Final do Incidente: o grau final de severidade considerando o volume de dados envolvidos no respectivo incidente, calculado através da multiplicação da Severidade do incidente com o Fator de Volume. FV – Fator de Volume: fator de agravamento de severidade, calculado a partir da quantidade de titulares envolvidos no incidente e do nível de criticidade do incidente.

<table>
<tr>
<td></td>
<td>
<table>
<tr><th>Quantidade de titulares</th><th>Nível CritividadeCritividadeCriticidade</th><th>Fator de Volume</th></tr>
<tr><td>Até 450 titulares</td><td>1</td><td>1</td></tr>
<tr><td>Até 4500 titulares</td><td>2</td><td>1,2</td></tr>
<tr><td>Entre 4.501 e 450.000</td><td>3</td><td>1,5</td></tr>
<tr><td>Mais de 450.001</td><td>4</td><td>1,8</td></tr>
<tr><td>Acima de 4.5 M</td><td>5</td><td>2</td></tr>
</table>

* inspirado, com certo grau de distinção, no racional do Anexo 3 do Guia de Incidentes com Dados Pessoais da Agência Espanhola de Proteção de Dados (fonte abaixo)

Nesse sentido, considerando a população do Brasil, maior em 4,5 vezes do que a população espanhola, chegamos na quantidade de titulares de dados pessoais, associada a nível de criticidade, a partir do qual será considerado fator de multiplicação do score final de risco

Links para acesso às fontes internacionais:

• European Union Agency for Cybersecurity - "Recommendations for a methodology of the assessment of severity of personal data breaches" (https://www.enisa.europa.eu/publications/dbn-severity
• Autoridade Española de Proteção de Dados – AEPD – “Guide on personal data breach management and notification” (https://www.aepd.es/sites/default/files/2019-09/Guide-on-personal-data-breach.pdf)
</td>
</tr>
<tr>
<td>Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?</td>
<td>A sugestão é que seja utilizada metodologia similar àquela adotada na Europa, elaborada pela ENISA (European Union Agency for Cybersecurity), por meio do documento denominado "Recommendations for a methodology of the assessment of severity of personal data breaches, a qual foi detalhada no item acima.

Links para acesso às fontes internacionais:

• European Union Agency for Cybersecurity - "Recommendations for a methodology of the assessment of severity of personal data breaches" (https://www.enisa.europa.eu/publications/dbn-severity</td>
</tr>
</table>

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 um primeiro momento, entendemos que deverá, a ANPD, contribuir para disseminar medidas educativas à população e às Organizações empresariais como um todo. Sugerimos, ainda: - Que a ANPD oriente o Controlador em termos de Treinamentos a serem fornecidos internamente na Companhia para que se institua uma cultura empresarial de proteção de dados. - Que sugira medidas organizacionais tais como: limitações de acesso aos dados pessoais, medidas para manter a confiabilidade de funcionários que necessitarem acessar dados, instituição de meios de autenticação de acessos. - Que sugira a adoção de medidas de segurança da informação que sejam suficientes contra fraudes, cópias e invasões, no geral, tais como pseudonimização e encriptação; -; - Que sugira a promoção de avaliações de riscos e checagens periódicas; - Que sugira a promoção de registros e elaboração de relatórios de todos os Incidentes de Segurança vivenciados e as medidas adotadas; - Que disponibilize diretrizes para que as Organizações elaborem suas políticas e procedimentos; - Que disponibilize diretrizes a serem seguidas quando da ocorrência de incidentes de segurança. (vide ICO); - As recomendações da ANPD devem considerar prazos factíveis para sua respectiva implementação, os quais deverão ser, preferencialmente, alinhados junto ao agente de tratamento, considerando a necessidade de investimentos, acesso à tecnologia adequada, e outros fatores como estrutura, modelo de negócio, faturamento, e demais aspectos quem impactem no tempo e meios para implantação de uma eventual recomendação.
Sugestão Adicional:	A Autoridade Nacional de Proteção de Dados Pessoais, deverá guardar e proteger o sigilo das informações que lhes são comunicadas, em especial os segredos comerciais e industriais, inclusive se abstendo de divulgar as informações recebidas, salvo quando houver decisão judicial, pedido ou requerimento de alguma autoridade pública, ou seja estritamente necessário para o cumprimento de qualquer das suas atividades previstas na LGPD.

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: TozziniFreire, Teixeira e Silva, Freire Advogados

CPF/CNPJ: 48.109.110/0001-12

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**
PONDERAÇÃO INICIAL	De início, é importante referir quer o simples fato de ter ocorrido incidente de segurança não significa, necessariamente, que as medidas técnicas e organizacionais de segurança implantadas pelo controlador, tenham sido insuficientes. A perfeição não é padrão atingível em matéria de segurança da informação. Em outras palavras, a ocorrência de um incidente de segurança não é, por si só, indicador de fato quanto à proteção insuficiente dos dados pessoais ou ainda indicador de que uma empresa não empregou medidas razoáveis de proteção aos dados pessoais ou agiu de forma inadequada neste tocante. Cada incidente e as medidas de segurança implantadas precisam ser considerados individualmente haja vista os contornos do caso concreto. Também é importante separar incidentes de segurança com violação de dados pessoais de usuários e relacionados ao controlador: de outros cenários em que os dados de um usuário possam ter sido acessados por terceiros não autorizados em decorrência de autocomprometimento, ou seja, comprometimento dos dados por parte do próprio usuário, como ocorre, por exemplo, em casos de *phishing*. Entende-se que os casos de autocomprometimento de dados pessoais, decorrente de ação por parte do próprio usuário afetado, com violação de seus dados pessoais em decorrência disso, devem ficar excluídos das obrigações de notificação à ANPD e aos titulares afetados, por não se tratarem, tais casos, de incidentes de segurança relacionáveis ao controlador.

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?	Preliminarmente, à medida em que a distinção entre risco e dano será abordada no item 3, a presente questão se limita a uma análise conjunta de risco e dano relevante enquanto "impacto" aos titulares. Nesta discussão vale ressaltar a premissa elencada pelo Grupo de Trabalho do Artigo 29º para a Proteção de Dados Pessoais: "enquanto todas as violações de dados pessoais são incidentes de segurança, nem todos os incidentes de segurança são necessariamente violações de dados pessoais".
	
	Estabelecidas estas considerações iniciais, entendemos que alguns são os critérios do que deve ser considerado pela ANPD enquanto risco ou dano relevante:
	• **Parâmetro 01: Comprometimento da confidencialidade ou integridade dos dados pessoais** - Um incidente pode acarretar em risco ou dano relevante ao titular (ou seja, lhe impactará), à medida em que os titulares de dados forem atingidos por meio da sua **(i) divulgação não autorizada** (ou seja, na hipótese de comprometimento da confidencialidade dos dados tratados), ou ainda da sua **(ii) alteração não autorizada** (ou seja, na hipótese de comprometimento da integridade dos dados tratados).
	  • Exemplos pontuais:
	  • **1.1. Comprometimento da confidencialidade dos dados pessoais**
	  • A perda de confidencialidade ocorre quando as informações são acessadas por terceiros não autorizados (ou seja, que não possuem uma base legal ou finalidade legítima para acessá-las), o que varia de acordo com o escopo da divulgação.
	  • Ex. a disponibilização dos dados vazados em mercados exclusivos para tanto, podendo resultar em fraudes financeiras ou roubo de identidade.
	  • **1.2. Comprometimento da integridade dos dados pessoais**
	  • A perda de integridade ocorre quando a informação original é alterada trazendo prejuízo para o indivíduo no processo.
	  • Ex. Uma alteração não autorizada aos dados pessoais se faz presente na hipótese de perda irreversível de dados pessoais (ex. em função de um ransomware, um backup desatualizado da base de dados dos

	titulares da controladora é utilizado e, nesse processo, são perdidos os dados coletados entre a data do último backup e a data do incidente em si). • **Parâmetro 02: Perda de acesso aos dados quando necessários para atender a solicitações de titulares (ou seja, comprometimento da disponibilidade dos dados pessoais)** - Em regra, um incidente de segurança que resulte na perda de acesso aos sistemas do controlador por algum período de tempo (ou seja, que o torne temporariamente indisponível), mas que não envolve o comprometimento dos dados nele retidos, não será considerado como passível de risco ou dano relevante ao titular. De todo modo, é possível que o dano ao titular diga respeito à impossibilidade de se atender aos seus direitos ou demais reivindicações frente aos seus dados pessoais, o que pode configurar este cenário de perda de acesso como hipótese de impacto para estes indivíduos. • **Parâmetro 03: Configuração de hipótese prevista no art. 46 da LGPD de incidente de segurança (que resultem em riscos ou danos relevantes para os titulares, conforme delineado no art. 48 da LGPD) -** Estes cenários incluem situações acidentais ou ilícitas de destruição, perda, alteração, comunicação dos dados pessoais. Ressaltamos que a relevância do incidente que resulte em comprometimento da confidencialidade, integridade ou disponibilidade dos dados pessoais independe de quem tenha dado causa para o incidente em si (seja o Controlador ou Operador).
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?	À medida em que a LGPD preza por uma análise da "relevância" do impacto aos titulares, faz-se interessante que haja uma subdivisão dos riscos para os titulares entre (i) Baixo, (ii) Médio, (iii) Alto e (iv) Muito Alto. Esta classificação servirá não apenas como um norte para a elaboração de estratégias para mitigar o incidente de segurança, como ainda enquanto baliza para o dever de notificar os titulares afetados e a Autoridade (à medida em que um risco baixo poderá ser considerado não relevante e, portanto, configurar enquanto hipótese de exclusão do dever de comunicação citado).

	Para a distinção citada, os mesmos parâmetros para a análise de gravidade do incidente de segurança podem ser considerados (conforme apresentado na questão 11 abaixo), cuja mensuração dependerá da adoção de metodologia de análise apta para tanto (conforme delineada na questão 12 abaixo).
3. Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	É possível definir dano como **qualquer desvantagem econômica significativa para os titulares decorrente da materialização dos riscos envolvidos no incidente**. A título exemplificativo, é possível mapear neste cenário potenciais danos materiais aos titulares que tenham se concretizado gerando prejuízos a eles, tais como danos emergentes ou lucros cessantes decorrentes da perda de controle sobre seus dados pessoais, de danos reputacionais, do roubo ou usurpação de sua identidade, da perda de confidencialidade de seus dados pessoais protegidos por sigilo profissional, dentre outras formas que resultem em perdas financeiras concretas. O debate sobre riscos, por sua vez, diz respeito ao **impacto potencial para os direitos e liberdades do titular, ou seja, sobre as consequências potencialmente negativas sob os direitos dos titulares envolvidos**. Esta análise demanda, portanto, uma avaliação sobre a estrutura de governança dos agentes de tratamento para averiguar se foram aplicadas as medidas técnicas e administrativas de segurança aptas a proteger os dados pessoais antes do incidente (ex. a adoção de técnicas de criptografia que inviabilizam a leitura dos dados vazados), bem como em momento posterior ao incidente (para mitigar o potencial de dano concreto para os titulares, reduzindo, portanto, o risco envolvido com o incidente).
4. O que deve ser considerado na avaliação dos riscos do incidente?	Entendemos que a avaliação dos riscos aos titulares deve seguir dois conjuntos de métricas: (i) aquelas relacionadas às medidas de segurança adotadas pelo agente de tratamento para mitigar, preliminarmente, os impactos de um incidente de segurança; e (ii) aquelas referentes à avaliação de gravidade dos incidentes. No que diz respeito às métricas de prevenção de impacto de incidentes, devem ser levados em consideração fatores tais como a existência de:

	• Procedimentos de deleção automática de dados pessoais (para mitigar a possibilidade de vazamento de dados retidos de forma desnecessária); • Controles de acesso aos dados pessoais com medidas de anonimização (quando cabível) e criptografia dos dados tratados (para mitigar a possibilidade de identificabilidade dos titulares); e • Protocolos de pseudonimização dos dados pessoais tratados (para mitigar a potencial identificabilidade dos dados pessoais tratados). Já em relação às métricas de avaliação da gravidade de incidentes, os mesmos parâmetros detalhados na questão 11 devem ser considerados, o que inclui, em linhas gerais: • A possibilidade de leitura dos dados pessoais objeto do vazamento; • A sensibilidade dos dados vazados; • A vulnerabilidade dos titulares a quem se referem, ou seja, se são dados de titulares menores, em especial se referentes a crianças (em atenção à faixa etária delineada no Estatuto da Criança e do Adolescente - ECA); • O grau de atualização dos dados vazados (avaliando quando foi a última atualização desses dados); • O grau de disponibilidade pública desses dados antes do vazamento (ex. eram dados públicos coletados de redes sociais); e • O grau de identificabilidade dos titulares a partir dos dados vazados. Adicionalmente, enquanto parâmetro adicional, o volume dos dados sujeitos ao incidente pode ser considerado como parâmetro subsidiário para a análise de gravidade em questão.
5. Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	O art. 48, §1º da LGPD dispõe que a comunicação a ser enviada pelo controlador à ANPD em caso de incidente de segurança que implique em *"risco ou dano relevante aos titulares"* de dados pessoais afetados, deve conter, no mínimo: (i) a descrição da natureza dos dados pessoais afetados; (ii) informações sobre os titulares dos dados envolvidos; (iii) indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; (iv) 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, cumpre ressaltar que o guia preliminar publicado pela ANPD para informação à autoridade acerca de incidentes de segurança ocorridos até a oportuna regulamentação do art. 48 da LGPD, dispõe que esse informe deve abarcar, para além daquelas informações objeto do art. 48, §1º da LGPD e referidas no parágrafo precedente também as seguintes: (i) identificação e dados de contato da entidade ou pessoa responsável pelo tratamento de dados pessoais objeto do incidente, bem como identificação e dados de contato do respectivo encarregado de dados ou outra pessoa de contato no âmbito da entidade notificante; (ii) indicação se a notificação é completa ou parcial; (iii) data e hora de detecção do incidente; (iv) data e hora do incidente e sua duração; (v) circunstâncias em que ocorreu a violação de segurança de dados pessoais (por exemplo, perda, roubo, cópia, vazamento, dentre outros); (vi) descrição dos dados pessoais e informações afetadas, como conteúdo dos dados pessoais, categoria e quantidade de dados e de titulares afetados; (vii) resumo do incidente de segurança com dados pessoais, com indicação da localização física e meio de armazenamento; (viii) medidas de segurança, técnicas e administrativas preventivas tomadas pelo controlador de acordo com a LGPD; (ix) possíveis problemas de natureza transfronteiriça e (x) outras informações úteis às pessoas afetadas para proteger seus dados ou prevenir possíveis danos. Entende-se que parte das informações adicionais demandadas pelo guia preliminar publicado pela ANPD para informação à autoridade acerca de incidentes de segurança, são pertinentes, quais sejam: identificação e dados de contato do controlador e respectivo encarregado; indicação se a notificação é completa ou parcial; data e hora de detecção do incidente; descrição dos dados pessoais afetados; quantidade de dados e de titulares afetados; medidas de segurança, técnicas e administrativas preventivas tomadas pelo controlador de acordo com a LGPD; e resumo do incidente de segurança. Não obstante, entendemos que algumas dessas informações adicionais cujo fornecimento é demandado no guia preliminar publicado pela ANPD não poderiam ser exigidas, vez que possivelmente indisponíveis ou inviáveis de serem precisadas em casos concretos de incidentes, quais sejam: data e hora do incidente e sua duração exatos; circunstâncias precisas em que ocorreu

	a violação de segurança de dados pessoais (por exemplo, perda, roubo, cópia, vazamento); ou ainda localização física dos dados pessoais objeto do incidente de segurança. Ademais, entendemos que o *"conteúdo dos dados pessoais"* que tenham sido objeto de incidente, não deveria ter fornecimento demandado à autoridade tal como consta do guia preliminar por esta publicado, uma vez que a investigação acerca do incidente de segurança ocorrido prescindiria do fornecimento da íntegra dos dados pessoais envolvidos à autoridade (descrição destes, acompanhada dos demais elementos cuja informação se mostra pertinente conforme abordado nos parágrafos precedentes, seriam suficientes para fins de investigação). Dessa forma, **propomos que as informações adicionais acerca de incidentes de segurança constantes do guia preliminar publicado pela ANPD, mas não do §1º do artigo 48 da LGPD, sejam incluídas como informações de prestação opcional pelo controlador de dados**. Propomos, ainda, **seja esclarecido quais exatas informações a ANPD visa obter no item "*problemas de natureza transfronteiriça*",** constante do guia preliminar publicado pela autoridade.
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 estabelece que os controladores devem informar à ANPD e aos titulares de dados pessoais afetados acerca de incidente de segurança que implique em *"risco ou dano relevante aos titulares"* de dados, dentro de *"prazo razoável"*. Referido dispositivo legal deixa de estabelecer o que se entende por *"prazo razoável"*, e a partir de que momento tal prazo passa a fluir. Dito isso, o guia preliminar publicado pela ANPD para informação à autoridade acerca de incidentes de segurança, estabelece, como prazo nesse sentido, o de 2 (dois) dias úteis, contados a partir do momento em que o controlador tome conhecimento acerca do incidente de segurança. Referido prazo foi proposto com base no Decreto nº 9.936/2019, que regulamenta a Lei Federal nº 12.714/11. No que diz respeito ao prazo para informação de incidentes de segurança à autoridade competente, o art. 33 do GDPR 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 acerca do incidente. Na mesma esteira, o art. 26-D da Lei de

	Proteção de Dados Pessoais de Cingapura determina que os controladores devem comunicar incidente de segurança sobre dados pessoais à autoridade de proteção de dados daquele país 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. Diante desse panorama, quanto ao início de fluição do prazo para informação de incidente de segurança, pelo controlador, à ANPD, **propomos que referido prazo tenha início a partir do momento em que o incidente de segurança tenha sido confirmado pelo controlador**. Avaliamos que outros critérios para definição de início desse prazo, a partir de elementos em certa medida subjetivos possivelmente abriria espaço para discussões extensivas caso a caso sobre se referido prazo foi cumprido pelo controlador, ou não. No mais, avaliamos ser essencial que a ANPD permita que a primeira comunicação à autoridade pelo controlador acerca de incidente de segurança constatado, a ser feita em curto prazo, seja comunicação preliminar. Passível de ser posteriormente complementada conforme avancem as investigações acerca do incidente. **Assim, propomos que ANPD fixe o prazo de 03 (três) dias úteis para uma comunicação à autoridade acerca da ocorrência de incidente de segurança. Se, dadas as características do incidente de segurança sob exame, não for possível comunicação de forma completa com todas as informações exigidas pela regulamentação no prazo inicial de 03 (três) dias úteis, o controlador poderá requerer a apresentação de informações complementares no prazo de 30 (trinta) dias úteis, prazo esse prorrogável mediante solicitação**. Apresentamos tal proposta uma vez que, na prática, os controladores dificilmente serão capazes de reunir todas as informações solicitadas no §1º do art. 48 da LGPD no prazo de apenas dois ou três dias. As informações disponíveis no momento da comunicação inicial acerca do incidente de segurança constatado dependerão das diferentes circunstâncias de cada incidente de segurança. Avaliamos que a proposta ora apresentada está de acordo com o posicionamento da ANPD, uma vez que o guia preliminar publicado pela autoridade já assinala como campo de preenchimento pelo controlador, se a notificação prestada acerca de incidente de segurança constatado é do tipo parcial/preliminar, ou já completa: "*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". Cumpre ressaltar que o GDPR também prevê a possibilidade de comunicação acerca de incidente de segurança, por fases. O artigo 85 do GDPR consigna que "*Se não for possível efetuar essa comunicação* [à autoridade acerca de incidente de segurança] *no prazo de 72 horas, a comunicação deverá ser acompanhada dos motivos do atraso, podendo as informações serem fornecidas por fases sem demora injustificada*". Além disso, no Brasil, por meio da Resolução ANP nº 44 de 22/12/2009 a Agência Nacional do Petróleo, Gás Natural e Biocombustíveis ("ANP") adota o modelo de comunicação inicial e preliminar, seguida de uma comunicação posterior com mais detalhes, em caso de incidentes de petróleo: com (i) comunicação inicial acerca do incidente, que deve ser imediata e (ii) relatório detalhado acerca do incidente, a ser apresentado em 30 dias, prazo que é prorrogável mediante fundamentação técnica apresentada nesse sentido. Seguindo a mesma linha, mediante a Instrução CVM 505/2011 a Comissão de Valores Mobiliários ("CVM") já prevê esse modelo de comunicação faseada para incidentes de segurança cibernética: conforme o disposto em seu art. 35-I, o intermediário deve apresentar comunicação preliminar de forma tempestiva e, em um segundo momento, relatório completo.
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 estabelece que os controladores devem informar à ANPD e aos titulares de dados pessoais afetados, acerca de incidente de segurança que implique em *"risco ou dano relevante aos titulares"* de dados, em *"prazo razoável"*. Como já mencionado nos comentários ao item precedente, referido dispositivo legal deixa de estabelecer o que se entende por *"prazo razoável"*, e a partir de que momento tal prazo passa a fluir. Entende-se que o objetivo da comunicação ao titular dos dados acerca de incidente de segurança constatado é informá-lo sobre um incidente de segurança relevante e, também, fornecer recomendações para viabilizar que adote as precauções necessárias para evitar maiores riscos ou

	danos. Nesse sentido, a comunicação aos titulares de dados deve contemplar informações claras sobre o incidente de segurança e as recomendações para mitigar potenciais efeitos adversos. No que diz respeito ao prazo para a realização de tal comunicação aos titulares de dados, entendemos que, na prática, os controladores não serão capazes de reunir todas as informações necessárias para fornecer clareza suficiente aos titulares dos dados, com descrição do incidente e recomendação quanto aos próximos passos a serem tomados para proteger os dados pessoais envolvidos, dentro do prazo de dois dias úteis referido no guia preliminar publicado pela ANPD, prazo este contado a partir do momento em que o controlador tenha tomado conhecimento acerca do incidente de segurança. Avaliamos que o fornecimento de informações genéricas e imprecisas, apenas para cumprir o prazo de dois dias úteis, geraria desinformação e alarde entre os titulares dos dados, o que seria mais prejudicial do que útil, gerando desinformação e violando o dever de adequada informação aos consumidores conforme determina o CDC (como bem reconheceu a ANPD ao firmar o acordo de cooperação técnica nº 01/2021 com a SENACON, boa parte das relações entre controladores e titulares de dados são, também, relações de consumo). Dito isso, **propomos a adoção de diferentes regimes de comunicação - à ANPD e aos titulares de dados afetados -, cada qual com prazos próprios. Avaliamos que a comunicação adequada aos titulares de dados pessoais afetados deve ser enviada <u>após a coleta de todas as informações necessárias para fornecer um cenário claro ao titular de dados, com as medidas correspondentes a serem tomadas para proteger os dados envolvidos no incidente de segurança</u>.** A fim de reiterar o argumento de que são pertinentes prazos diferentes para informação à autoridade e aos titulares de dados pessoais afetados, acerca de incidente de segurança constatado, veja-se que o art. 33 do GDPR estabelece que o controlador deve, sem demora injustificada e, sempre que possível, até 72 horas após ter tomado conhecimento acerca de incidente de segurança, comunicá-lo <u>à autoridade nacional</u>; enquanto o art. 34 do GDPR estabelece que o controlador deve comunicar <u>ao titular dos dados</u> sobre o incidente de segurança, <u>sem demora injustificada</u> - nenhum prazo ou parâmetro específico é mencionado.

	Além disso, ressaltamos que 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.*" Por sua vez, com relação ao conteúdo da comunicação a ser enviada aos titulares de dados pessoais afetados por determinado incidente, **propomos que as informações que deverão constar de referida comunicação, considerando o teor do art. 48, §1º da LGPD e o dever de adequada informação aos consumidores, sem informações excessivamente técnicas, sejam as seguintes: (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; e (iv) medidas que devem ser adotadas pelo próprio titular dos dados para reverter ou mitigar os efeitos do prejuízo (por exemplo, alterar senha).**
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 à 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, **propomos 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, propomos 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?	Conforme o disposto no art. 48, *caput* da LGPD, o controlador de dados só deve comunicar à ANPD aqueles incidentes de segurança que possam impor risco ou dano relevante aos titulares de dados

	afetados – o que se propõe seja avaliado de acordo com a metodologia e os critérios sugeridos na questão 2 acima. Sem prejuízo disso, visando a conferir maior segurança jurídica aos controladores de dados pessoais, a ANPD pode também listar exemplos de casos em que não se afiguraria presente risco ou dano relevante aos titulares de dados pessoais afetados, dispensando-se notificação à autoridade, por exemplo nos seguintes casos: quando os dados pessoais objeto de incidente consistem apenas em informações de contato profissional (que já estiverem disponíveis publicamente - por exemplo, no site de uma empresa); quando os dados pessoais objeto de incidente se referem apenas a informações da "lista telefônica" que já são de domínio público, ou ainda outros dados já integralmente públicos; além de quando o incidente de segurança envolver apenas dados criptografados ou pseudoanomimizados; sem prejuízo de outros exemplos possíveis, na mesma linha.
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 dano aos 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)	**Em linhas gerais, entendemos que a gravidade de um incidente está diretamente relacionada com os efeitos negativos que este cenário pode causar para os titulares. A mensuração deste impacto, por sua vez, pode considerar alguns critérios objetivos.** **Preliminarmente, é importante levar em consideração a (i) possibilidade de leitura dos dados vazados**: A LGPD já começa a delinear parâmetros para uma análise de gravidade em seu artigo 48, §3º ao definir 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, entende-se que uma baliza para a análise de gravidade de incidentes reside na possibilidade de que os dados objeto do vazamento sejam lidos. Como resultado, será considerada menos grave a hipótese de incidente em que os dados envolvidos estejam criptografados (considerando as técnicas de criptografia disponíveis no momento do vazamento) de modo a impossibilitar sua leitura. **Uma vez identificado que os dados objeto de vazamento são legíveis, cumpre avaliar demais critérios sobre o que está em jogo no incidente:** • **(I) Qual a sensibilidade dos dados vazados**: É possível classificar os dados pessoais em 4 categorias: (i) dados simples; (ii) dados comportamentais; (iii) dados financeiros; e (iv) dados sensíveis. • **(II) Qual o contexto dos dados vazados**: Para além da sensibilidade, é importante avaliar qual o impacto do incidente, o que inclui aspectos tais como:

	○ (a) A **vulnerabilidade dos titulares** a quem se referem, ou seja, se são dados de titulares menores, em especial se referentes a crianças (em atenção à faixa etária delineada no Estatuto da Criança e do Adolescente - ECA) ○ (b) O grau de **atualização dos dados vazados** (avaliando quando foi a última atualização desses dados); ○ (c) O grau de **disponibilidade pública desses dados antes do vazamento** (ex. eram dados públicos coletados de redes sociais) • **(III) Qual o grau de identificabilidade dos titulares a partir dos dados vazados**: à luz do conceito expansivo de "dados pessoais", é possível que haja dados pessoais que identifiquem um titular direta ou indiretamente. Nesse sentido, será considerado um cenário de maior impacto para o titular o incidente que envolver o vazamento e dados que mais facilitam a identificabilidade do titular isoladamente (sem a necessidade, portanto, de muitas informações adicionais para que a partir de determinado contexto se identifique esse indivíduo). • **(IV) Qual o tipo de incidente de segurança (circunstâncias do incidente em si)**: é possível vislumbrar o impacto do incidente analisando se ele envolveu, de forma isolada ou em conjunto, o comprometimento da confidencialidade, da integridade ou da disponibilidade dos dados pessoais. Ainda, essa análise leva em consideração se o incidente decorreu de um atentado contra as bases de dados do agente de tratamento. • **(V) O volume dos dados vazados**: como parâmetro subsidiário, vale avaliar qual o volume dos dados afetados, o que se apresenta enquanto variável objetiva sobre a escala e potencial impacto do incidente.
12. Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	A título exemplificativo, a Agência Europeia para Segurança de Redes e da Informação (ENISA) apresenta sua própria metodologia para a avaliação da gravidade de um incidente de segurança. Nessa abordagem, são levados em consideração três critérios: • (i) O contexto do tratamento de dados pessoais ("Data Processing Context" ou "DPC") ○ *Contempla os itens I e II da questão acima.* • (ii) A facilidade de identificação dos titulares ("Ease of Identification" ou "EI" ○ *Contempla o item III da questão acima*

	• (iii) As circunstâncias do incidente ("Circumstances of the Breach" ou "CB" – ○ *Contempla o item IV da questão acima.* Como resultado, a fim de avaliar se a gravidade do incidente ("severity" ou "SE") será baixa, média, alta ou muito alta, a ENISA toma como cálculo a seguinte fórmula "SE = DPC x EI + CB". A ENISA conta ainda com um anexo que ilustra a "nota" atribuída para cada cenário possível, o que tido em conjunto irá compor cada componente da fórmula acima (mais detalhes sobre esta métrica, podem ser encontrados no relatório "Recommendations for a methodology of the assessment of severity of personal data breaches" da ENISA no seguinte link: https://www.enisa.europa.eu/publications/dbn-severity). Uma vez calculado o valor de "Severity" do incidente, é possível subdividi-lo em: • **Incidente de Baixa Gravidade**, ou seja, os titulares não serão afetados ou ainda poderão vir a encontrar alguns inconvenientes que serão facilmente superados (como tempo gasto para reintroduzir informações, ou eventuais aborrecimentos); • **Incidente de Média Gravidade**, ou seja, os titulares podem encontrar inconvenientes significativos que serão capazes de superar apesar de algumas dificuldades (o que envolve custos extras, ou recusa de acesso aos serviços, por exemplo); • **Incidente de Alta Gravidade**, os titulares podem enfrentar consequências significativas em suas vidas em função do incidente, estes que devem ser capazes de superar, embora com sérias dificuldades (como danos materiais ou reputacionais); e ainda • **Incidente de Muito Alta Gravidade,** em que os titulares podem enfrentar consequências significativas, ou mesmo irreversíveis em função do incidente.
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 acerca de incidente de segurança, a ANPD poderá determinar que o controlador adote medidas visando a reverter ou a mitigar os efeitos decorrentes deste. Entendemos que as medidas a serem determinadas pela ANPD nesse sentido, dependerão das circunstâncias de cada incidente de segurança. Não obstante, apresentamos abaixo alguns exemplos de medidas que poderiam ser determinadas pela ANPD aos controladores, sendo importante enfatizar que uma lista exaustiva de tais medidas não seria praticável:

	• Solicitar ao controlador que aumente a conscientização sobre a proteção de dados pessoais entre os seus colaboradores, mediante treinamentos a serem realizados nesse sentido; • Solicitar ao controlador que se atente às condições contratuais ao envolver terceiros no tratamento de dados pessoais sob seus cuidados; • Solicitar ao controlador a correção – se viável - do vício técnico específico que tenha ensejado o incidente de segurança objeto de notificação; • Solicitar ao controlador que informações adicionais sobre a resolução do incidente sejam apresentadas com determinada frequência (até que seja constatado que todos os impactos da ocorrência foram devidamente endereçados) a fim de garantir que serão adotadas as melhores medidas técnicas a mitigar os impactos do incidente. Ainda, em função do seu futuro contato com o contexto de diferentes incidentes de segurança (desde a sua origem até resolução), entendemos que a Autoridade contará com um repertório de estratégias aptas a contribuir com a série de medidas adotadas pelo controlador frente ao ocorrido, podendo então orientá-lo com recomendações pertinentes para seu contexto (enquanto um efetivo diálogo no processo de resolução do incidente). Ademais, em atenção ao disposto no art. 48, §2º, I, da LGPD e aos comentários objeto do item 8 acima, propomos que a hipótese de determinação pela ANPD de divulgação do incidente de segurança constatado, de forma ampla *"em meios de comunicação"*, fique restrita ao cenário excepcional de inviabilidade ou impossibilidade de comunicação direta e individualizada aos titulares de dados pessoais afetados acerca de determinado incidente.
	<u>Outro(s) tema(s) relevante(s):</u> **(I) Notificação de incidente de segurança por operador de dados pessoais:** Quando a ANPD publicou a consulta pública objeto dos presentes comentários, também publicou (i) um guia preliminar sobre incidentes de segurança, em que referiu 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. A esse respeito, entendemos que o art. 48, §1º da LGPD é claro ao estabelecer que o controlador deve notificar à ANPD sobre incidentes de segurança envolvendo dados pessoais. Nesse sentido, entendemos que a ANPD não pode permitir que os operadores notifiquem incidentes de segurança, pois isso seria contrário ao texto legal. **(II) Incidente de segurança não configura ilícito *per se*:** Perfilhando o regime adotado na Europa, entendemos que a Lei Geral de Proteção de Dados Pessoais (LGPD) articulou a segurança da informação como uma obrigação de meio, e não de resultado. Uma análise sistemática da Lei, e em especial dos artigos 43, incisos II e III, 44, caput e parágrafo único, e 46, caput e §§ 1º e 2º torna clara essa percepção. Nos termos desses artigos da lei, deve-se observar a conduta adotada pelo agente de tratamento de dados pessoais ao longo do período que antecedeu o *data breach*, para definir se possui responsabilidade sobre o ocorrido. Ou seja, os esforços prévios e contínuos envidados pelo agente são determinantes para aferir se estarão obrigados a reparar eventuais danos sofridos pelos usuários que tiveram seus dados acessados de forma indevida. Caso o agente de tratamento forneça a segurança que o titular possa esperar - considerados o modo pelo qual é realizado o tratamento dos dados pessoais, os resultados e riscos que razoavelmente dele se espera, e as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado -, ainda que ocorra um acesso indevido de terceiros, defendemos que o agente não está obrigado a reparar os titulares, justamente porque cumpriu as obrigações que lhe foram impostas. Precedentes judiciais proferidos antes da LGPD confirmam essa opinião. Para o Tribunal de Justiça do Rio de Janeiro no julgamento da Apelação nº 0024968-52.2013.8.19.0061, "(...) Nenhum sistema

	informatizado é imune a esse tipo de invasão. O que o administrador de rede deve promover é o cuidado necessário com o uso de tecnologias que visem dificultar tais invasões, visto que a complexidade e alcance das fraudes cibernéticas andam sempre à frente da especialização tecnológica dos sistemas de segurança de rede, o que é demonstrado pelas constantes notícias de descoberta de novas fraudes e invasões, inclusive em grandes corporações. Assim, para que ficasse caracterizada a responsabilidade do Estado, seria necessário demonstrar sua negligência quanto aos aspectos de proteção de rede. Todavia, não há prova nos autos de que o Estado negligenciou a ponto de facilitar a invasão de seu sistema." Nesse mesmo sentido, o Superior Tribunal de Justiça reconheceu no julgamento do Recurso Especial nº 1.398.985/MG que não há sistemas infalíveis e, por isso mesmo *"(...) Também não significa que se deva exigir um processo de cadastramento imune a falhas. A mente criminosa é astuta e invariavelmente encontra meios de contornar até mesmo os mais modernos sistemas de segurança. O que se espera dos provedores é a implementação de cuidados mínimos, consentâneos com seu porte financeiro e seu know-how tecnológico – a ser avaliado casuisticamente, em cada processo – de sorte a proporcionar aos seus usuários um ambiente de navegação saudável e razoavelmente seguro."* Se o agente de tratamento de dados atua em conformidade com a LGPD, empregando os melhores esforços na segurança da informação, adotando medidas eficazes e necessárias para a proteção dos dados pessoais armazenados, eventual vazamento de dados não se configura, *per se*, uma falha na prestação de seus serviços. **(II) Coordenação e concentração do procedimento de comunicação de incidentes de segurança, e suspensão de procedimentos administrativos com trâmite perante outras autoridades competentes conforme o caso:** Entendemos que, sob o ponto de vista procedimental, em linha com as práticas adotadas pela SENACON em processos recall, a ANPD, enquanto órgão central para a implementação e fiscalização de atendimento da LGPD, deverá coordenar e concentrar o procedimento de comunicação de incidentes de segurança, envolvendo as demais autoridades competentes conforme

	o caso, inclusive para solicitar suspensão de procedimentos que estejam conduzindo em paralelo acerca de incidente de segurança também informado à ANPD, suspensão que deverá perdurar, ao menos, até a conclusão de investigação do incidente pela ANPD.
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: Tramontina Central de Administração Ltda.

CPF/CNPJ: 90.114.299/0001-06

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 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 identificado vazamento, destruição, alteração de dados de pessoa física, contendo: Informação contendo o CPF, contato do titular, senhas, cartão de crédito, dados sensíveis 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, ambos devem ser classificados. O dano pode ser em duas categorias, levando em consideração a quantidade de dados de um mesmo titular, bem como se o mesmo é sensível ou não. (As categorias poderiam ser Alto e Baixo). O nível baixo entendemos não ser relevante. Quanto risco sugere-se a utilização da classificação definida na ISO 27000.**
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	**O risco se caracteriza pela análise da probabilidade *x* impacto que aquele vazamento pode ocasionar ao titular. O dano se caracteriza pelo prejuízo financeiro ou moral, causado pelo incidente. Espera-se a definição de um nível mínimo de comprovação dos referidos prejuízos pelo titular do dado e a vinculação com a empresa que forneceu o dado.**

O que deve ser considerado na avaliação dos riscos do incidente?	a) **Que tipos de danos o incidente ocasionou ao titular (e qual sua classificação – Baixo ou Alto);** b) **Quantidade de dados do mesmo titular;** c) **Natureza dos dados pessoais;** d) **Se houve reclamação do titular perante a ANPD ou outro órgão;** e) **Impacto que o incidente pode ocasionar ao titular.**
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	**Entendemos ser suficiente.**
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	**5 dias (úteis), ressalvadas ações que dependam exclusivamente de operadores ou co-controladores (terceiros), o que deverá ser analisado de forma específica, quando comprovado que o controlador tomou todas as medidas estabelecidas 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 comunicação? As mesmas do §1º do art. 48?	**No mesmo prazo de informar a ANPD (5 dias úteis), desde que sejam permitidas formas de comunicação em massa e mídias digitais. As informações não seriam as mesmas, o que deveríamos passar seriam quais informações foram vazadas e quais medidas foram tomadas para reverter ou mitigar os efeitos do prejuízo. No caso de possível vazamento de senhas, deveríamos instruir aos titulares a realizar a imediata troca de senha.**
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.)?	**E-mail, telefone, site institucional ou outras mídias digitais oficiais (ficando a escolha a critério da empresa). Ou seja, sendo permitida a comunicação pública.**

Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	**Somente informar quando os riscos e danos forem altos (respeitando a classificação supracitada).**
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	**Idem acima.**
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	**Idem acima, ou seja, quando o risco foi classificado como Alto.**
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?**Apresentação de plano de ação para correção da vulnerabilidade e comunicação aos titulares.**	**Apresentação de plano de ação para correção da vulnerabilidade e comunicação aos titulares.**

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: Tudo-Sobre-IoT – GTL - Grupo Técnico LGPD

CPF/CNPJ: diversos - Prof. João Peres

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?	Quando um **risco pré-estabelecido ou não,** se materializar ou ocorrer, portanto, produzindo um incidente de segurança envolvendo dados pessoais identificáveis (IS-PII). Risco é um tipo de evento possível, que durante o tratamento de dados pessoais possa causar VIOLAÇÃO de dados, acarretando efetivamente um IS-PII. 1) Segundo o RGPD europeu – Um incidente PII pode acarretar riscos e produzir danos aos Titulares de Dados Pessoais, quando representar uma **VIOLAÇÃO** aos critérios de segurança da informação **CID** (Confidencialidade – Integridade – Disponibilidade), que possa caracterizar um ou mais riscos ou produza efetivamente danos ou impactos. A violação deve causar «*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**» 2) **CRITÉRIOS –** Refere-se à extensão dos danos ou impactos diretos e/ou indiretos causados aos titulares de dados pessoais. O nível de dano aos Titulares, produzido por um IS-PII deverá ser metrificado com uma estrutura escalar, partindo do "Inócuo ao Catastrófico". Todo Risco que possa produzir um IS-PII envolvendo a CID de PII, cuja a probabilidade e impacto (dano) sejam classificados como "**Alto ou Muito Alto**", (escala de 0 (zero) até 100 (cem)), devem ser considerados RELEVANTES, independente da probabilidade.  *Documento1 disponível em 10/03/21 - https://www.cnpd.pt/media/zgkec1q0/data-breach-_wp250rev01_pt.pdf

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?	Os riscos devem sempre serem associados com a criticidade dos dados pessoais que estão sendo tratados e com as perdas, danos e consequências (diretas e indiretas) das suas concretizações para os titulares de dados pessoais. Volumes de dados pessoais tratados também podem elevar os riscos, em função do aumento da extensão das perdas eventualmente causadas a mais titulares de dados pessoais. Acreditamos que a metrificação do Impacto deva ser escalar (escala de 0 (zero) até 100 (cem)), com categorias; Muito Baixo, Baixo, Médio, Alto, Muito Alto – de forma que seja possível ampliar a precisão da avaliação. (Categorias/Níveis com base no Manual Gestão de Riscos TCU 2020*). As cinco categorias (níveis) de impacto deverão ser calculadas com base na pontuação escalar da Matriz de Riscos, ajustada as reais necessidade de garantir a CID PII, para contemplar todos os tipos de IS-PII identificáveis, em sua avaliação inicial. Devem ser avaliadas durante a captura de dados e tratamentos posteriores, considerando as metodologias internacionais PIA* e DPIA**, para a manutenção "viva ou contínua" do relatório RIPD, de impacto à proteção de dados pessoais. O RIPD corresponde ao definido no art. 5º, XVII da LGPD, proposto como: «*documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco*». Riscos com probabilidade rara e danos muito baixos, não devem ser considerados como relevantes inicialmente, mas devem ser monitorados e avaliadas as possibilidades de produzirem outros riscos secundários e estes escalarem gradativamente para níveis maiores. Os demais riscos que exijam investimento em mitigação, deverão ter uma forte avaliação de riscos residuais e monitoração continua em sua gestão, ou seja, todos os riscos de IS-PII devem ser monitorados e gerenciados. *PIA - Privacy Impact Assessment é uma tradicional metodologia (desde 1990) de Avaliação de Impacto de Privacidade de dados pessoais, composta por processos que auxiliam as organizações na identificação e gerenciamento dos riscos de privacidade decorrentes de captura de novos dados, novos projetos, iniciativas, sistemas, processos, estratégias, políticas, relações comerciais, etc. *(base wikipedia)* **DPIA - Data Protection Impact Assessments é um padrão metodológico seguido pela comunidade europeia, fundamentado na metodologia PIA, com objetivo de avaliar não só o impacto de Privacidade de Dados, mas em especial as características de "proteção de dados" adotadas, que possam mitigar a probabilidade e ocorrência de riscos e na redução de danos (impactos), além de outros aspectos. Entendemos que estas duas metodologias não deveriam ser confundidas, mesmo possuindo bases similares. *Documento 2 disponível em 10/03/21: - https://portal.tcu.gov.br/data/files/46/B3/C6/F4/97D647109EB62737F18818A8/Manual_gestao_riscos_TCU_2_edicao.pdf

3 - Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	**Distinguir** – Risco sobre o tratamento de PII é um evento caracterizado como IS-PII (Incidente de segurança CID-PII), que tem a probabilidade de ocorrer em algum momento do tratamento e produzir Danos (impactos negativos) aos titulares de dados pessoais. Danos são as consequências, caso os fatos previstos no evento de Risco IS-PII venham a ocorrer. **Como se relacionam** – Não existe Risco IS-PII sem Dano (impactos negativos) – o problema é temporal na relação "Causas x Efeitos" – A identificação de Riscos de IS-PII e das prováveis consequências da sua ocorrência são normalmente previstas/estimadas, com antecedência por uma Avaliação Contínua de Riscos PII (ACR PII). A verificação dos Danos reais só acontecerá depois do Risco ser materializado ou ocorrido. O processo de "ACR PII" deve, portanto, ser revisto e ajustado após cada ocorrência de IS-PII em um ciclo PDCA. Riscos IS-PII podem ser entendidos como a: Probabilidade não concreta de se tornarem realidade. Exigem que sejam identificados e reconhecidos previamente, bem como, previstas as medidas mitigatórias (para redução dos riscos). Devem ser identificadas as probabilidades e impactos negativos das suas eventuais ocorrências, bem como, quais serão os eventuais riscos residuais após à aplicação das medidas mitigatórias. Danos estão associados à ocorrência concreta de um episódio de violação de segurança, com a contabilização dos prejuízos e das perdas causadas, diretas e/ou indiretas, em curto, médio e longo prazo para os titulares de dados pessoais.
4 - O que deve ser considerado na avaliação dos riscos do incidente?	**Todos os riscos empresariais** que possam estar direta ou indiretamente ligados a eventos danosos que impactem a CID (Confidencialidade, Integridade e Disponibilidade) de dados, em especial aos ligados ao dados PII. Um IS-PII é uma VIOLAÇÃO dos padrões de segurança estabelecidos. No RGPD da UE, a definição de IS-PII é indicada como «*uma violação da segurança CID 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**». Uma Avaliação Contínua de Riscos PII "ACR PII", deve considerar todos os eventos / episódios em relação a sua gravidade e extensão dos danos, que violem as regras da LGPD (conformidade), não só as de segurança estabelecidas, envolvendo Informações de Identificação Pessoal (PII), portanto, as Políticas de Segurança (PoSIC), em seu capítulo "Riscos de Segurança PII", as regras devem estar alinhadas a todos os artigos da LGPD, que enderecem obrigações aos Agentes de Tratamento

	de Dados pessoais, não se limitando ao CAPÍTULO VII da LGPD, que trata da segurança e das boas práticas. Uma Avaliação Contínua de Riscos sobre dados pessoais ACR-PII, deve minimamente considerar: a) Identificar a origem e da causa do episódio de risco, a fim de que se possa garantir a retomada da continuidade dos negócios/operação da empresa com segurança, e com o menor risco possível da repetição do mesmo tipo de episódio de violação de segurança, no futuro; b) Apurar quais foram os dados envolvidos; c) Assegurar se houve ou não dados pessoais envolvidos; d) Quantificar o volume de dados pessoais envolvidos; e) Qualificar os tipos de dados pessoais envolvidos; f) Estimar danos imediatos e desdobramentos de novos riscos eventuais, para os titulares de dados pessoais produzidos pelo episódio – Estabelecer o nível de Gravidade do IS-PII. g) Verificar as falhas das medidas técnicas e administrativas, que possibilitaram a materialização do risco PII e dos impactos negativos; h) Qualificar a necessidade de informar imediatamente a ANPD e aos Titulares sobre a ocorrência do episódio. i) Ajustar as ações mitigatórias e preventivas no ciclo de aperfeiçoamento PDCA. Documento1 disponível em 10/03/21 - https://www.cnpd.pt/media/zgkec1g0/data-breach-_wp250rev01_pt.pdf
5 - Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	Poderiam ser reportadas diversas outras informações de caráter mais aprofundado e tecnicamente importantes, para uma avaliação preliminar mais assertiva pela ANPD, no entanto, há de se estabelecer por regra regulamentar da ANPD, que essas informações **não serão utilizadas em prejuízo dos informantes**. A transparência necessária para informar a ANPD poderá ser uma barreira vista pelos Agentes de Tratamento de Dados, para informar dados corretamente. Ao documentar no formulário de comunicação de incidente de segurança, se poderá produzir provas contra eles mesmos. **Proposta:** Poderia ser adicionado no atual formulário no Bloco “Critério para a comunicação”, que se requer estimar a gravidade da ocorrência, respondendo - “Estimativa da Gravidade do IS-PII – de zero a dez = _____” – isso ajudaria a ANPD imediatamente compreender a possível classificação dos “riscos x danos” estimados pelo informante. Nesta questão, existem diversos pontos que poderiam ser adicionados aos questionamentos no formulário de comunicação, de forma que as próprias perguntas poderiam ser orientadoras de ações práticas preventivas. Por exemplo: No bloco do formulário “Incidente de Segurança” poderia ser questionado:

	a) Ao se analisar a ocorrência do incidente reportado, foram tomadas todas as providências para registrar e garantir a cadeia de custódia* dos dados analisados? b) A sua empresa possui processos de Forense Computacional Empresarial**, em caso de incidentes PII? c) Para chegar as conclusões do incidente PII, sua empresa contou com a colaboração de pessoal técnico qualificado em Segurança da Informação ou em operações de CSIRTs***? d)... *- Documentação cronológica ou histórica que registra a sequência de custódia (tutela ou guarda de dados), controle, transferência, análise e disposição de evidências físicas ou eletrônicas obtidas. **- Forense Computacional Empresarial é uma atividade realizada por profissionais de segurança da informação capacitados para realizar um tipo de "perícia forense digital" com o intuito determinar a materialidade, a dinâmica e autoria de ilícitos associados ao âmbito da computação, tendo a identificação e o processamento de evidências como provas materiais dos desvios de segurança ocorridos na organização, que inclusive poderão ser revistas por um perito judicial. ***- CSIRT é o acrônimo de "Computer Security Incident Response Team", ou grupo de resposta a incidentes de segurança, que são profissionais altamente proficientes em Tecnologia da Informação, Telecomunicações e Segurança da Informação, especializados em identificar, investigar e resolver incidentes computacionais e cibernéticos.
6 - Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	A ANPD requer 2 (dois) dias úteis, o RGPD 3(três) dias – acreditamos que deveríamos ter um alinhamento internacional. 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), possam atender a LGPD no prazo estabelecido de 48 horas. As demais que representam 99,9% do mercado, não terão condições de cumprir o prazo, em mais de 90% dos casos de IS-PII. No art. 48, § 1º, V, há a indicação de que a comunicação **deve ser imediata** (há uma CONTRADIÇÃO com o caput do § 1º, que diz: **A comunicação será feita em prazo razoável**,... Acreditamos que o **prazo de até 30 dias uteis** possa ser razoável para as **empresas de pequeno porte**. Dificilmente uma ME ou MEI que não seja da área de tecnologia, terá condições de identificar um IS-PII de origem na Internet em 48 horas, a não ser que o caso seja muito evidente. Alguns incidentes graves são complexos de identificar, mesmo para grupos CSIRTs experientes, como os possíveis ataques: **APT**s (Advanced Persistent Threat) de alto impacto PII, que podem levar meses para serem efetivamente descobertos, mesmo havendo evidências no curto prazo.

	PONDERAÇÃO - VELOCIDADE X RISCO: Quanto tempo é necessário para identificar que uma ameaça explorou uma vulnerabilidade de segurança de dados PII na empresa? Uma vez identificado o incidente PII, quanto tempo se leva para avaliar o prejuízo (sistêmico, financeiro e reputacional, ...)? Uma vez tendo ocorrido a quebra de segurança, o risco materializado em danos, já estará presente. Nesse caso, a velocidade de reação de contenção e mitigação, servirá como parâmetro para determinar a dosimetria da sanção que deverá ser julgada e aplicada. Se os Agentes de Tratamento de Dados demorarem em reagir e informar aos Titulares, a ANPD poderá entender que houve tentativa de ocultar o incidente (quando o objetivo é dar publicidade para que todos tomem conhecimento do ocorrido, até porque os dados não pertencem ao controlador/operador) e, por sua vez, majorar a pena a ser aplicada. É um beco sem saída. A questão não é saber se IS-PII vão ocorrer, mas quando vão ocorrer, e se será possível com atual cultura empresarial identificá-los. A situação de 99,9% das empresas brasileira vai se complicar, por ausência de cultura e de práticas metodológicas e normativas no uso cotidiano de SI (Segurança da Informação). O fato vai impossibilitar atender aos prazos estabelecidos. A grande maioria sequer vai informar suspeitas de IS-PII até por ingenuidade e ou falta de preparo. Entendemos que a ANPD deva levar o fato em consideração, mas também, produzir campanhas de conscientização e publicação de materiais de orientação que objetivem estabelecer uma cultura mínima de prevenção, para a proteção de dados PII. Podemos colaborar, com apoio a ANPD, na busca de divulgar e alcançar a melhoria contínua da cultura básica de SI nas empresa brasileiras.
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?	Nossa proposta é seguir os padrões internacionais, onde os Titulares devem ser informados imediatamente após a constatação e avaliação do IS-PII com Danos “Alto ou Muito Alto” e só depois informar a Autoridade ANPD, na sequência de maiores investigações e fundamentações sobre os fatos reais. Os dados fornecidos aos titulares, além dos previstos no art.48,§1º, poderão ser complementados com propostas de ações preventivas, corretivas e ou saneadoras, que possam colaborar na redução dos possíveis danos**.** Propostas: para colaborar no atendimento das questões 06 e 07 quanto a prazos: a) Todo o website empresarial deveria ter uma página dedicada a “Comunicação de Incidentes de Segurança PII” da respectiva empresa, mesmo que nunca tenha ocorrido. Nessa página e na “home page”, as empresas poderiam divulgar IMEDIATAMENTE suspeitas ou fatos de IS-PII

	em seu ambiente operacional. Isso poderia alcançar seus clientes habituais e manteria o registro de ocorrências e justificativas. b) Preventivamente nessa página, poderiam ser divulgados procedimentos padronizados aos Titulares, para a mitigação de riscos de exposição ou vazamentos de PII em suas máquinas. c) Poderiam, ainda, criar um formulário de denúncia de suspeita de vazamentos, onde os Titulares possam informar, questionar, validar, indicar evidências que permitam uma investigação de origem de um IS-PII, mesmo que a empresa ainda não os tenham identificados. Essa proposta é complementar ao processo de comunicação aos Titulares, já previsto na Lei.
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.)?	Vai depender da abrangência (volume de dados) do IS-PII comprovado, e dos prováveis níveis de impactos (danos negativos) aos Titulares. Para os casos de menor impacto poderia haver uma comunicação na “Homepage exposta por 30 dias” e em página específica – como proposto - no website do Controlador, onde se mantem o registro das ocorrências. Se houver condições a comunicação, deveria ser por escrito, enviada ao endereço de correspondência dos titulares de dados pessoais e em paralelo ser direta por e-mail específico, e só em casos de muito grande impacto a publicização por mídias de grande alcance, deveria ser adotada como medida imposta pela ANPD, com base no art. 48, §2 da LGPD.
9 - Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	Quando a investigação de um Incidente de Segurança de dados pessoais IS-PII comprovar que não se produziu 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, mesmo que isso ocorra de modo acidental ou ilícito. **Exemplo internacional:** Houve uma invasão séria na Rede da empresa X, a Base de Dados “BDC” de 3 milhões de Clientes foi furtada (copiada) pelos invasores. O fato foi comprovado. A análise documentada, a conclusão foi da não necessidade de comunicar a Autoridade de Proteção de Dados nem aos Titulares – motivo: a BDC estava criptografada no padrão FIPS-197 com chave de 256 bits, e a investigação interna comprovou que não houve comprometimento da chave criptográfica correspondente, portanto, a margem de risco de acesso indevido ao conteúdo da BCD seria quase nulo. Mesmo assim, os dados do incidente foram reportados ao FIRST.ORG (similar ao nosso CERT.br para registro de incidentes) e os desdobramentos do incidente continuaram com a monitoração contínua.

10 - Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	**As mesmas para não informar a ANPD.** Como já proposto - seria altamente recomendável que as empresas que já vivenciaram algum IS-PII, incluíssem em seus websites páginas dedicadas a orientação ao Titulares, com indicação clara de algumas sugestões de providências, caso haja suspeita de eventuais vazamentos, inclusive há a oportunidade de criar um "**Canal de Denuncia IS-PII**", de forma a favorecer uma cultura de investigação preliminar, por parte dos Titulares, antes de afirmarem que seus dados vazaram a partir de determinada fonte.
11 - Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	A "gravidade" dos episódios de violação de segurança CID de PII, estariam sempre ligadas com a extensão dos riscos, seus desdobramentos e as consequências dos danos diretos e ou indiretos, possivelmente causados à curto, médio e longo prazo aos titulares de dados pessoais por um IS-PII. A ANPD ao receber o formulário de Comunicação de IS-PII, e iniciar a verificação das suas respostas, a partir de uma rápida análise, de certa forma, já poderá identificar o potencial de gravidade do IS-PII, em ocasionar danos materiais, financeiros, fraudes, roubo de identidade, ou danos morais, violação do direito à imagem e à reputação, entre outros. Para se estabelecer critérios de análise de gravidade de um IS-PII, deveríamos primeiro estabelecer um padrão mínimo adequado de Identificação, Avaliação e Gestão de Riscos de IS-PII (metodologia padrão ANPD a ser criada, para "Avaliação Contínua de Riscos PII" (ACR PII)), que fosse compreensível e facilmente aplicável, pelos Agentes de Tratamento de dados. A adoção de um padrão de ACR PII ANPD, iria uniformizar e facilitar a análise de gravidade dos IS-PII. Para uma devida análise da gravidade de um IS-PII no atendimento a LGPD em seu art. 48, §2º, se faz necessário desenvolver uma metodologia própria de avaliação escalar padronizada, dos níveis de "Gravidade/Severidade" de um IS-PII, que possa estar apoiada em referências internacionais de fundamentação. Aqui nos propomos em colaborar com a ANPD, se aprovado, no desenvolvimento metodológico de uma proposta de solução tanto para ACR PII quanto para avaliar a Gravidade IS-PII, que teria apoio do nosso corpo técnico especializado. O resultado seria ajustado pelas áreas técnicas da ANPD, como julgarem adequado. Obs.: Está colaboração foi aceita pela ANPD, em nossa reunião por videoconferência em 22/03/2021.

12- Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	A referência, mas significante, metodológica*, que encontramos, para avaliar a Gravidade/Severidade ou magnitude de um IS-PII já é antiga e foi publicada pela ENISA (The European Union Agency for Network and Information Security) em 2013. Encontramos em pesquisas WEB muitas metodologias que tratam o tema Avaliação de Riscos, mas são poucas as que qualificam de alguma maneira a "gravidade de IS-PII", de forma coerente. Reforçamos a nossa proposta de desenvolver uma metodologia integrada de "Avaliação de Riscos e Análise de Gravidade de IS-PII", que possa vir a ser ajustada e adotada pela ANPD. *Incluímos aqui a visão "kernel" metodológica da publicação ENISA, do documento nominado "Recommendations for a methodology of the assessment of severity of personal data breaches**" de dezembro de 2013, traduzida para o português, como segue: **Metodologia ENISA** **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: • **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) > • 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: $$SE = DPC \times EI + CB$$ • **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. **É importante entender o contexto da proposta que notoriamente indica não haver consenso entre a DPAs (Autoridades de Proteção de Dados) na EU.** **Documento disponível em 10 de março de 2021, através do link: - https://www.enisa.europa.eu/publications/dbn-severity (documento com 27 páginas). Entendemos que a visão da Metodologia AGIS-PII (Avaliação da Gravidade IS-PII) poderá ser aperfeiçoada e ganhar maior precisão, conforme nossa proposta de desenvolvimento.
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?	Além das providências previstas em Lei, a ANPD poderia requisitar, conforme a gravidade e abrangência do fato reportado, uma **análise de terceira parte**, a documentação das **evidências forense** de preservação dos fatos, e diversas outras medidas técnicas e administrativas, mas tudo vai depender de como se regulamenta a estrutura como um todo, na busca da equidade. A ANPD poderia recomendar "**checklists de verificação**" detalhadas, indicados para as empresas conforme o segmento de atuação e porte. Solicitar medidas técnicas e administrativas mais aprofundadas, poderá ser positivo e necessário, no entanto, mais de 90% das empresas brasileiras, não praticam ou dispões do mínimo necessário em Políticas, Procedimentos, infraestrutura de Hardware/Software, pessoal capacitado em SI, IS ou CSIRT, entre outros, para tratar IS-PII adequadamente ou condições de evoluir para um nível de maturidade maior, com brevidade no tema IS-PII. Para as grandes organizações - Visando a melhoria contínua dos "SGSI/SGIP" (Sistemas de Gerenciamento de Segurança da Informação (ISO 27001) e Sistema de Gerenciamento de Informações de Privacidade (ISO 27701)) das corporações, a ANPD poderia publicar no seu portal web um "RESUMO DAS OCORRÊNCIAS DOS EPISÓDIOS DE VIOLAÇÃO DE SEGURANÇA REPORTADOS PELAS CORPORAÇÕES" (sem citar os nomes), com uma sinopse sobre as

	conduções realizadas nos incidentes acompanhados pela ANPD, em todas as suas fases e com os detalhes mais importantes, a fim de servir como aprendizado para as demais corporações.
COLABORAÇÃO NOSSA 14 - Como seriam identificados os níveis de gravidade de Incidentes de Segurança PII em transito de dados ou tratamento de dados internacionais, considerando os artigos, 33,34,35 e 36?	Neste caso a identificação de responsabilidade de todos os envolvidos em um IS-PII internacional, pode ficar comprometida e alcançar um grau de dificuldade de avaliação de impacto (gravidade), muito mais elevado. Seria necessário que a ANPD possa publicar a lista das DPAs (Autoridades de Proteção de Dados – internacionais) com as quais o Brasil se alinha – exemplo das DPAs da EU*, por questões de jurisdição e colaboração na solução de incidentes PII, que envolvam transito de dados internacionais. Isso ajudaria os Controladores em saber que poderiam contar com a ANPD na busca de elucidar eventos adversos de IS-PII. Temos uma situação objetiva a ser ponderada – a maioria das empresas de pequeno porte que possuem contratos de uso de recursos em nuvem " IaaS, PaaS e SaaS, entre outros", não sabem responder em qual (is) local (is) no mundo, estão hospedados os seus dados empresariais que incluem os PIIs. Qualquer IS-PII que envolva recursos de serviços em nuvem poderá ter uma grande dificuldade de mitigação ou controle sobre ela, independentemente de haver responsabilidades definidas em contrato. Esse fato impacta nas inciativas dos "Agentes de Tratamento de dados pessoais", comunicarem os reais dados de IS-PII a ANPD e inclusive no saneamento dos incidentes. O fato também tem impacto para que a ANPD possa cumprir o determinado no art. 48, §2, II - "determinar ao controlador a adoção de providência como; medidas para reverter ou mitigar os efeitos do incidente." Entendemos que seria importante uma definição da ANPD, de que dados capturados, armazenados ou que sofram qualquer tratamento em nuvens, os datacenters devam estar em território nacional. Isso facilitaria o acesso e a autonomia da ANPD, atendendo ao art. 3º.
15 – Qual a importância de se determinar um padrão de avaliação de Riscos e da Gravidade de IS-PII? O quanto isso impacta à sociedade?	Sem um padrão para avaliação de riscos e da gravidade de IS-PII, os Controladores terão uma grande dificuldade em atender ao art. 50, § 1º e §2º, em especial no tocante a estabelecer regras e boas práticas (Governança), sobre os aspectos ligados à "sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados." Teremos muitas definições distorcidas.

	Da mesma forma em atender ao art.50, §2, I, g) “conte com planos de resposta a incidentes e remediação; ” - Estes planos dependerão em muito da identificação, avaliação, e gestão de riscos, bem como, da qualificação de gravidade de incidentes envolvendo PII. Outros pontos afetados: • No caso das sanções administrativas com base no Art. 52 - §1º - I - **a gravidade e a natureza das infrações e dos direitos pessoais afetados;** - Ser não houver um padrão ficará complicado estabelecer critérios justos. • Art. 54. “O valor da sanção de multa diária aplicável às infrações a esta Lei deve observar a **gravidade da falta e a extensão do dano ou prejuízo causado** e ser fundamentado pela autoridade nacional.” Entendemos que aqui se faz a exigência de se estabelecer um padrão.
SUGESTÃO DE NORMATIVO, SE HOUVER	
Art. Xxxx	
Art. Xxxx	

Não incluímos objetivamente Anexos – Estamos disponíveis para prestar esclarecimentos quando necessário.
Por favor faça contato com Prof. João Peres – [redacted]

Contribuição GTL – Grupo Técnico LGPD apoio comunidade “TUDO SOBRE IOT”

Instituição colaboradora – “Tudo-sobre-IoT” – Dra. Thelma Troise

Coordenação – Prof. Dr. João Peres – Komp Security Brasil™

Corpo Técnico/Jurídico
Dr. Alípio Badeque Junior - Uberconsult®
Dra. Cristina Hang - Kaunerth Direito Digital
Dra. Janne Kaurnet - Kaunerth Direito Digital
Dr. João Adolfo de Rezende Ponchio - Uberconsult®
Dr. Josmar Giovannini - Conformidados®
Dr. Orlando Arnaud - Uberconsult®
Dr. Sergio Takeo Kofuji - IBE-USP / LSI-TEC
Dr. Wagner Pozzer - Rubens Naves Santos Jr. Advogados

Apoio *(tema apresentado e discutido com esses grupos)*
Dr. Coriolano Camargo - Digital Law Academy
Dra. Luciana Nunes Freire - Grupo de Direito Digital e Compliance FIESP
Dra. Regina Inoue - OAB-Grupo de Direito Digital e Compliance – OAB sec. Butantã-SP.

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: UNIMED BELO HORIZONTE COOPERATIVA DE TRABALHO MÉDICO

CPF/CNPJ: 16.513.178/0001-76

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?	A interpretação da GDPR (https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG), uma referência internacional – equivalente europeia à nossa LGPD – permite concluir que o incidente (de violação de dados pessoais) é aquele que pode provocar, 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. Primeiramente, cabe ponderar que em 2020 e 2021 foram noticiados vazamentos maciços de dados, os quais, segundo a mídia especializada, seguem comercializados na deep web. Assim, no cenário atual, cabe avaliarmos que tipo de incidente é realmente passível de causar dano, considerada toda essa exposição já ocorrida e, possivelmente, que se prolongará no tempo. O incidente acarreta em dano nos casos em que ocorre um efetivo prejuízo, sempre comprovado. Ou seja, quando há um dano material ou moral ao titular. Além disso deve haver nexo causal entre a ação ou a omissão do controlador e o

	prejuízo/dano. Assim, no caso de dano, o mais provável é que o controlador já tenha tido contado com o titular, pois necessário a efetiva comprovação do dano/prejuízo, do nexo causal, da conduta. O dano é aquele causado a partir de um incidente no qual, “se não forem adotadas medidas adequadas e oportunas”, a violação cause “danos físicos, materiais ou imateriais às pessoas singulares, como a perda de controle sobre os seus dados pessoais, a limitação dos seus direitos, a discriminação, o roubo ou usurpação da identidade, perdas financeiras (...) 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” (Considerando 85 e art. 33, da já referenciada GDPR). Já o risco está vinculado a um potencial dano. Não há o dano nesta situação; não há prejuízo concreto; mero risco, situação fática na qual não se sabe se haverá dano ou prejuízo. Segundo a GDPR (Considerando 76), “Os riscos deverão ser aferidos com base numa avaliação objetiva, que determine se as operações de tratamento de dados implicam risco ou risco elevado”. Entende-se que devem ser comunicados incidentes (comprovação dos mesmos critérios do dano, exceto o prejuízo) nos casos em que: (i) há divulgação pública; (ii) envolva grande volume de dados (percentual, considerados a atividade do controlador e o volume total de tratamento) pessoais, a saber, identificados os titulares; (iii) e nos dois casos, se não houve meios de contenção da divulgação ou se ela não se deu a tempo. No caso de dados em saúde, deve-se ponderar que, mero percurso assistencial, a saber, mas não se limitando, dados relacionados a agenda de consultas ou procedimentos, não devem ser considerados como passíveis de causar dano ou risco de dano. Eventuais sanções devem ser aplicadas com base no dano causado, e não no risco. Afinal, o risco é uma situação de exposição ou vulnerabilidade na qual não ocorreu o dano concreto, como já mencionado. Assim, a imposição de sanção com base em mera situação de risco fere postulados básicos do ordenamento. A comunicação de risco à ANPD deve servir para cooperação, auxílio na prevenção desse risco e monitoramento do cenário nacional pela Agência; nunca para punir o informante por algo que, efetivamente não gerou danos. ***INSTITUIÇÃO: UNIMED BELO HORIZONTE COOPERATIVA DE TRABALHO MÉDICO***

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 essa divisão seria salutar. Podem ser combinados critérios para a definição do que é risco baixo, médio e alto. Mas, risco e dano baixo não devem ser considerados como relevantes para os efeitos da lei geral de proteção de dados e, portanto, não passíveis de comunicação. Na europeia GDPR (https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG), art. 83, há indicativo de reconhecimento de níveis (graus) dos incidentes para aplicação das penalidades, considerando aquela normativa para a cominação de multas a gravidade (alínea a), o grau de responsabilidade do controlador (alínea d) e, até mesmo, o grau de cooperação com a autoridade de dados (no nosso caso, a ANPD – alínea f). Sugerimos a adoção de uma classificação que leve em conta a métrica probabilidade x impacto, para aferição de níveis de risco. Nível de risco alto: O evento poderá ocorrer com frequência, alcançando um número elevado de titulares e dados sensíveis (probabilidade), que necessariamente cause impacto severo no bem jurídico tutelado pela Lei (privacidade), com dano efetivamente materializado, quebrando o pacto firmado entre controlador e titular para o tratamento e uso daqueles dados, ou para a finalidade pretendida. Para se aferir a probabilidade a avaliação perpassa também pela consistência das ações tomadas pelo controlador para prevenir e conter o vazamento. Nível de risco moderado: O evento poderá ocorrer em algum momento (probabilidade), podendo alcançar dados pessoais e/ou dados pessoais sensíveis, que necessariamente cause dano moderado ao bem jurídico tutelado pela norma (privacidade). Para se aferir a probabilidade a avaliação perpassa também pela consistência das ações tomadas pelo controlador para prevenir e conter o vazamento. Nível de risco baixo: O evento poderá ocorrer em circunstâncias excepcionais (probabilidade), podendo alcançar dados pessoais (impacto) ou mesmo dados sensíveis cujo dano à privacidade é baixo (tal como, mas não se limitando, a marcação de consultas e agenda) e trará baixo impacto ao titular. Com relação à categorização do dano, é possível adotar métrica semelhante, que utilize parâmetros objetivos para delimitar situações de dano alto, moderado ou baixo: (i) há divulgação pública; (ii) se envolveu grande volume de dados (percentual, considerados a atividade do controlador e o volume total de tratamento) pessoais ou titulares, a saber, identificados os titulares; (iii) e nos dois casos, se não houve meios de contenção da divulgação ou se ela não se deu a tempo.

	INSTITUIÇÃO: UNIMED BELO HORIZONTE COOPERATIVA DE TRABALHO MÉDICO
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	O dano tem de estar relacionado a um prejuízo e deve ser comprovado. O risco é potencial. O dano pode ocorrer ou não. Por isso entende-se que o dano se configura quando já atingiu a esfera patrimonial do titular, com o efetivo prejuízo, mas deve haver a triangulação com ação/omissão, nexo causal. O risco é uma situação hipotética. **Pode** anteceder o dano e, desde já, deve-se acrescer que o simples risco não é indenizável, pelo que necessário, efetivamente, o dano, para que haja dever de indenizar, segundo normas de responsabilidade civil nacional, exceto em teorias do risco, a qual entende-se não se aplicar à presente. Se o risco é comunicado, antes que haja efetivo prejuízo, entende-se que o controlador adotou medidas de saneamento e controle. ***INSTITUIÇÃO: UNIMED BELO HORIZONTE COOPERATIVA DE TRABALHO MÉDICO***
O que deve ser considerado na avaliação dos riscos do incidente?	Conforme já se argumentou, risco pode anteceder o dano; é potencial de dano. Assim, deve ser aferido se no incidente houve controle do risco; houve zelo e medidas concretas por parte do controlador para evitar que ele ocorresse; se haveriam meios razoáveis e esperáveis para que aquele risco fosse evitado; bem como deve-se considerar a comunicação do risco como uma etapa de cooperação para prevenir um dano futuro, ou outros riscos similares. ***INSTITUIÇÃO: UNIMED BELO HORIZONTE COOPERATIVA DE TRABALHO MÉDICO***
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	Esse item vai depender de como a ANPD desenvolver os itens acima, mas sugerimos: • Informações sobre o próprio incidente em si, quando foi identificado, qual sua natureza; • Medidas tomadas para preservação das evidências, procedimentos seguidos para a contenção da crise; • Apresentação do Comitê de Crise e de suas ações em relação ao incidente; • Funções elaboradas pelos colaboradores envolvidos; • Questionamentos e demandas externas, como requerimentos de titulares de dados, autoridades e imprensa, bem como suas respostas; • Medidas de correção técnicas e de Governança adotadas; • Balanço geral do incidente, danos causados, etc.

	Considerando o disposto no §1º do art. 48, entende-se que as informações sobre o risco relevante são praticamente suficientes, podendo ser acrescido montante de dados relativo à quantidade de titulares afetados e dentro das possibilidades a categoria desses titulares. Neste ponto, cabe sugerir que a quantidade de titulares afetados pode-se ser um dos itens ou subitens balizadores para estabelecimento da categorização ou graduação do risco quanto a relevância. ***INSTITUIÇÃO: UNIMED BELO HORIZONTE COOPERATIVA DE TRABALHO MÉDICO***
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	Somente devem ser comunicados os considerados relevantes, conforme itens discutidos acima. O prazo deve permitir que o controlador faça as apurações e tome as medidas corretivas adequadas. Ainda, mostra-se positivo, na esteira do que faz a GDPR (art. 33) permitir uma flexibilidade deste prazo, desde que o não cumprimento da comunicação dentro dele se dê mediante apresentação de justificativa. Sugere-se que o termo inicial seja o conhecimento do fato, e que seja concedido um **prazo de 5 dias úteis, quando possível** (e, em não sendo possível, que seja feita o mais rápido possível e de maneira fundamentada sobre o não cumprimento do prazo estabelecido). A GDPR europeia apresenta um Guia de "*Orientações sobre a notificação de uma violação de dados pessoais ao abrigo do Regulamento (UE) 2016/679*", disponível em inglês e outras línguas (dentre as quais o português) no link https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052. Para além de sugerirmos a elaboração de guia similar pela ANPD, especialmente após a edição da Resolução Normativa para a qual se está tomando subsídios nesta ocasião, indicamos que neste guia há um trecho de especial atenção ao tema ora comentado: Após ter sido informado de uma potencial violação por um indivíduo, uma organização de comunicação ou outra fonte, ou ao detetar ele próprio um incidente de segurança, o responsável pelo tratamento pode realizar um curto período de investigação para apurar se ocorreu ou não uma violação. Durante este período de investigação o responsável pelo tratamento não deve ser considerado como tendo «conhecimento». No entanto, é expectável que a investigação inicial comece o mais rapidamente possível, para apurar, com razoável grau de certeza, a ocorrência de uma violação; pode seguir-se uma investigação mais aprofundada. (pág 12). Mostra-se, portanto, como viável estabelecer um tempo eventual entre o conhecimento do incidente e o início do prazo para comunicação à ANPD e ao titular, buscando permitir uma melhor apuração e levantamento de informações. ***INSTITUIÇÃO: UNIMED BELO HORIZONTE COOPERATIVA DE TRABALHO MÉDICO***

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?	Somente devem ser comunicados os considerados relevantes, conforme itens discutidos acima. O prazo deve, também, permitir que o controlador faça as apurações e tome as medidas corretivas adequadas. E, no caso da comunicação ao titular, há um dever de cuidado especial para evitar incompreensão ou pânico desnecessário por parte do recebedor da informação. Assim, sugere-se que o termo inicial seja o conhecimento do fato, e que seja concedido um **prazo de 10 dias úteis para a comunicação, quando possível** (e, em não sendo possível, que seja feita o mais rápido possível e de maneira fundamentada sobre o não cumprimento do prazo estabelecido). As informações devem seguir o padrão estabelecido para comunicação à Autoridade, com linguagem a mais clara e compreensível que for possível, destacando eventuais medidas que aquele titular pode adotar (por exemplo, no caso de vazamento de senhas, sugerir a troca destas). ***INSTITUIÇÃO: UNIMED BELO HORIZONTE COOPERATIVA DE TRABALHO MÉDICO***

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.)?	Quanto mais eletrônica e digital, melhor. Aliás, deve-se permitir a liberdade de forma de comunicação, desde que ela seja efetiva. A comunicação deve ser realizada de forma segura entre o Controlador e o Titular dos Dados, e de forma genérica para sociedade. A comunicação deve ser realizada com cautela para não atrapalhar a investigação do incidente. A título exemplificativo, a GDPR (https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG) destaca que há situações em que a comunicação é extremamente difícil ou custosa, podendo ser feita uma comunicação pública geral; confira-se o dispositivo pertinente: Artigo 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). 3. A comunicação ao titular dos dados a que se refere o n.o 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 aceder a esses dados, tais como a cifragem; 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 n.o 1 já não é suscetível de se concretizar; c) 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. 4. Se o responsável pelo tratamento não tiver já comunicado a violação de dados pessoais ao titular dos dados, a autoridade de controlo, tendo considerado a probabilidade de a violação de dados pessoais resultar num elevado risco, pode exigir-lhe que proceda a essa notificação ou pode constatar que se encontram preenchidas as condições referidas no n.o 3. ***INSTITUIÇÃO: UNIMED BELO HORIZONTE COOPERATIVA DE TRABALHO MÉDICO***
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	Se não houver relevância. Se for de baixo risco. Se o dado for público. Se já tiver sido divulgado em vazamentos anteriores que não tenham sido acarretados pelo controlador. ***INSTITUIÇÃO: UNIMED BELO HORIZONTE COOPERATIVA DE TRABALHO MÉDICO***

Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	Se não houver relevância. Se for de baixo risco. Se o dado for público. Se já tiver sido divulgado em vazamentos anteriores que não tenham sido acarretados pelo controlador. Destacamos, a título ilustrativo, as situações previstas pela GDPR europeia (https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG) para dispensa de comunicação ao titular: Art. 34. (...) 3. A comunicação ao titular dos dados a que se refere o n.o 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 aceder a esses dados, tais como a cifragem; 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 n.o 1 já não é suscetível de se concretizar; c) 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. ***INSTITUIÇÃO: UNIMED BELO HORIZONTE COOPERATIVA DE TRABALHO MÉDICO***
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	Somente devem ser comunicados, claro, incidentes de risco médio e alto – a serem definidos critérios pela ANPD. Para análise da gravidade do incidente: volume de dados; se foi um incidente que expos o dado a um incontável número de pessoas; se havia, por parte do controlador, medidas preventivas, processos e técnicas de proteção e contenção. ***INSTITUIÇÃO: UNIMED BELO HORIZONTE COOPERATIVA DE TRABALHO MÉDICO***
Existe alguma metodologia recomendada para a análise de gravidade do incidente de	A categorização em níveis (graus), que considere fatores objetivos (tais como volume de dados envolvidos, segmento de atuação daquele fluxo de tratamento de dados) permite uma maior objetividade na análise dos incidentes. ***INSTITUIÇÃO: UNIMED BELO HORIZONTE COOPERATIVA DE TRABALHO MÉDICO***

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?	Vai depender do caso concreto, sempre. Sugerimos a adoção de um rol exemplificativo de medidas, que envolvam, por exemplo (mas não se limitando): • Estabelecimento de comitê de crise; • Auditoria; • Mecanismos internos de controle (*Compliance*); • Envio de relatório de informações, com periodicidade podendo ser definida, até eventual solução do incidente; • Procedimentos internos de verificação. ***INSTITUIÇÃO: UNIMED BELO HORIZONTE COOPERATIVA DE TRABALHO MÉDICO***
Comentários adicionais da Participante	No caso do incidente é recomendável que se pondere, por exemplo, alguns itens, a serem discutidos com os segmentos econômicos, de forma particularizada, para que se possa compreender as particularidades de cada um, relativa ao tratamento de dados. Isso pois, os setores possuem diferenças entre si, particularidades que devem ser consideradas. (i) Tipo de violação; (ii) Natureza dos dados; (iii) Volume dos dados tratados pelo agente x volume dos dados envolvidos no incidente; (iv) Com que facilidade os titulares dos dados podem ser identificados por meio do incidente; (v) Quais as medidas técnicas adotadas para a proteção dos dados; (vi) Se for vazamento, onde ele se deu; (vii) Quais as medidas tomadas para minorar os efeitos do incidente; (viii) Há efetiva exposição ou risco de dano, com o incidente? (ix) Se já houve incidente/vazamentos anteriores, envolvendo os mesmos titulares e os mesmo dados, há risco de dano nos incidentes subsequentes ao primeiro? (x) Atenuantes; ***INSTITUIÇÃO: UNIMED BELO HORIZONTE COOPERATIVA DE TRABALHO MÉDICO***

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: USINA TERMELÉTRICA NORTE FLUMINENSE SA

CPF/CNPJ: 03.258.983/0001-59

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 identificado vazamento, destruição, alteração de dados de pessoa física, contendo: Informação contendo o CPF, contatos do titular, senhas, padrões de consumo ou dados sensíveis 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, ambos devem ser classificados. O dano pode ser em duas categorias, levando em consideração a quantidade de dados de um mesmo titular, bem como se o mesmo é sensível ou não. (As categorias poderiam ser Alto e Baixo). O nível baixo entendemos não ser relevante. Quanto risco sugere-se a utilização da classificação definida na ISO 27000.**
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	**O risco se caracteriza pela análise da probabilidade x impacto que aquele vazamento pode ocasionar ao titular. O dano se caracteriza pelo prejuízo financeiro ou moral, causado pelo incidente. Espera-se a definição de um nível mínimo de comprovação dos referidos prejuízos pelo titular do dado e a vinculação com a empresa que forneceu o dado.**
O que deve ser considerado na avaliação dos riscos do incidente?	**a) Que tipos de danos o incidente ocasionou ao titular (e qual sua classificação – Baixo ou Alto);** **b) Quantidade de dados do mesmo titular;** **c) Natureza dos dados pessoais;** **d) Se houve reclamação do titular perante a ANPD ou outro órgão;** **e) Impacto que o incidente pode ocasionar ao titular;**

Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	**Entendemos ser suficiente.**
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	**5 dias (úteis), ressalvadas ações que dependam exclusivamente de operadores ou co-controladores (terceiros), o que deverá ser analisado de forma específica, quando comprovado que o controlador tomou todas as medidas estabelecidas 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 comunicação? As mesmas do §1º do art. 48?	**No mesmo prazo de informar a ANPD (5 dias úteis), desde que sejam permitidas formas de comunicação em massa e mídias digitais. As informações não seriam as mesmas, o que deveríamos passar seriam quais informações foram vazadas e quais medidas foram tomadas para reverter ou mitigar os efeitos do prejuízo. No caso de possível vazamento de senhas, deveríamos instruir aos titulares a realizar a imediata troca de senha.**
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.)?	**E-mail, telefone, site institucional ou outras mídias digitais oficiais (ficando a escolha a critério da empresa). Ou seja, sendo permitida a comunicação pública.**
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	**Somente informar quando os riscos e os danos forem altos (respeitando a classificação supra citada).**
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	**Idem acima.**

Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	**Idem acima, ou seja, quando o risco foi classificado como Alto.**
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?	**Apresentação de plano de ação para correção da vulnerabilidade e comunicação aos titulares.**
SUGESTÃO DE NORMATIVO, SE HOUVER	
Art. Xxxx	
Art. Xxxx	

Comentado [SM|DSA1]: Falar com o Carlos.

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:
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**	**SITE**
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 quando este apresenta riscos de dano físico, material ou não material ao titular, como por exemplo fraude, perda de controle sobre os dados, limitação de seus direitos, discriminação, constrangimento, prejuízo financeiro, danos a imagem e reputação, perda de confidencialidade de dados protegidos ou outra desvantagem social ou financeira (Consideranda 85 da GDPR). Os critérios analisados devem ser os seguintes: 1. Tipo de incidente (Grupo de Trabalho Artigo 29) 2. Natureza dos dados envolvidos (sensíveis?) 3. Volume de dados envolvidos (Grupo de Trabalho Artigo 29) 4. Possibilidade ou facilidade de identificação do titular (Grupo de Trabalho Artigo 29) 5. Qual o constrangimento sofrido pelo homem médio. O vazamento era tido como remoto, possível ou provável?; 6. Idade dos titulares e profissão;	https://gdpr-text.com Working Party do Artigo 29. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjW1efC15fvAhWaDrkGHSzTDHUQFjAAegQIBBAD&url=https%3A%2F%2Fec.europa.eu%2Fnewsroom%2Farticle29%2Fdocument.cfm%3Fdoc_id%3D49827&usg=AOvVaw2uhYsKyRzJ6lwhQyiMURJF

	7. Possibilidade de utilização dos dados vazados (por exemplo, podemos usar dados de cartão de crédito para fazer compras de valores altos, mas não podemos usar a idade do titular para muita coisa).	
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?	Risco: baixo, médio e alto. Dano: relevante ou não relevante. O risco se refere à possibilidade de ocorrer o dano, e a relevância do dano tem a ver com o quanto o dano vai afetar o seu titular.	
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	O risco decorre do incidente. Ou seja, ocorrido o incidente já existe risco de dano. Por outro lado, o dano pode ou não ocorrer, a depender do incidente e dados envolvidos, sendo que a extensão do dano deve ser verificada na prática.	
O que deve ser considerado na avaliação dos riscos do incidente?	O potencial de dano apresentado pelo dado vazado, se houve vazamento de dados sensíveis, a quantidade de dados vazados de cada titular, a quantidade de titulares afetados, a amplitude de acesso aos dados. Por exemplo, se foi um ataque de hacker, mas que não vazou dados, então o risco é menor do que um efetivo vazamento de dados para o público.	
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	· Nome dos agentes de tratamento envolvidos; · Data e horário (ou estimativa) ou incidente e data e hora da descoberta do incidente. · Resumo do incidente, com circunstâncias do incidente (furto, perda, etc) e local físico e servidores envolvidos. · Conteúdo dos dados pessoais afetados · Informações e número de titulares envolvido, em especial, se havia menores de idade e se residentes de outros países foram afetados	(sugestões com base nas instruções da ICO (Information Commissioner`s Officer – Reino Unido) https://ico.org.uk/for-organisations/report-a-breach/

	· Informação sobre notificação aos titulares e conteúdo desta notificação	
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	Até e não mais que 48 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?	Até e não mais que 72 horas. As mesmas do §1º do art. 48 e da GDPR.	
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.)?	Para comunicação direta, por e-mail preferencialmente, ou outro dado que o Controlador possua (telefone, endereço). Caso o risco de dano seja muito alto, então publicação na página da internet da ANPD e Diário Oficial.	
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	Se o incidente for referente a dados já públicos ou de conhecimento geral, e que não resultem em risco aos direitos e liberdade dos titulares (artigo 33 (1) da GDPR), ou, ainda, quando os dados pessoais forem ininteligíveis para partes não autorizadas e houver cópia ou backup.	https://gdpr-text.com
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	Quando o incidente não envolver dados pessoais Quando for improvável que o incidente afete o dado pessoal ou a privacidade do titular - conforme verificado em relatório de análise realizado pela ANPD Quando for verificado que o agente de tratamento tomou todas as medidas necessárias aos dados pessoais envolvidos no	Opinião 3/2014 da Working Party do Artigo 29. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

	incidente (exemplo, uso de criptografia não permite que o dado vazado seja acessado ou compreendido) De toda forma, notificação ao titular deveria ser incluída como uma boa prática, ainda que não obrigatório e deve ser levado em conta na eventual aplicação de sanção.	
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	Contexto do tratamento do Dado Pessoal (DPC) - tipo de dado pessoal envolvido no incidente cou outros fatores linkados ao contexto geral do tratamento Facilidade na identificação dos titulares pelos dados envolvidos no incidente (EI) Circunstancias do incidente (culpa, dolo, falta de medidas de segurança, etc) (CB)	Documento elaborado em Dezembro de 2013 pelas autoridades da Grécia e Alemanha com a ENISA - European Union Agency for Network and Information Security https://iapp.org/media/pdf/resource_center/ENISA-breach-severity-methodology.pdf
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	Cálculo da gravidade do incidente: DPC avalia a criticidade de determinado dado o contexto específico do tratamento EI é o fator corretor do DPC. A combinação entre os dois da o score inicial de gravidade do incidente (SE). CB quantifica circunstancias específicas, então só pode adicionar à gravidade do incidente. A formula desenvolvida pelas autoridades da Grécia e Alemanha é a seguinte: "SE - DPC x EI + CB"	Documento elaborado em Dezembro de 2013 pelas autoridades da Grécia e Alemanha com a ENISA - European Union Agency for Network and Information Security https://iapp.org/media/pdf/resource_center/ENISA-breach-severity-methodology.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?	Tomada imediata de medidas para minimizar o incidente. Reforço das medidas de segurança e tomada de novas medidas mais robustas para fins do tratamento realizado - inclusive medidas administrativas (treinamento, políticas internas e externas, controle de acesso, etc) e tecnológicas. Retratação referente ao incidente, comunicação pública, reparação de danos.	
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: VILARINHO SCAREL SOCIEDADE DE ADVOGADOS ("Vilarinho Advogados")

CPF/CNPJ: 26.263.072/0001-15

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 pode acarretar risco ou dano ao titular dos dados pessoais quando envolver: (i) dados sensíveis; (ii) dados de indivíduos em situação de vulnerabilidade, menores de idade e idosos; e (iii) dados que possam ocasionar danos materiais ou morais, tais como fraudes financeiras e/ou roubo de identidade. Os critérios para avaliar a relevância do incidente devem ser: (i) o volume de dados envolvidos no incidente de segurança; (ii) a quantidade de indivíduos afetados; e (iii) quais tipos de dados vazaram.
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?	Todo tipo de incidente que envolva dados pessoais deve ser tratado como relevante. No caso de classificação de um incidente os seguintes critérios devem ser considerados: (i) tipo de dados envolvidos; (ii) número de titulares afetados pelo incidente; e (iii) riscos e eventuais danos que podem vir a ser suportados pelo titular em decorrência do incidente.
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	O risco é algo que enseja incerteza, acarretando uma probabilidade de ocorrência de situações que possam acarretar algum tipo de dano ao titular de dados, e, por consequência, prejuízo a este. Dano, por sua vez, é uma lesão de caráter patrimonial ou moral ocasionada ao titular de dados após um vazamento. Os conceitos se relacionam na medida em que um risco pode vir a gerar um dano, na medida em que os dados sejam utilizados de forma indevida, seja em decorrência de um vazamento ou pelo uso em desconformidade com as finalidades informadas ao titular.

O que deve ser considerado na avaliação dos riscos do incidente?	O responsável pelo tratamento de dados deve considerar: (i) as possíveis consequências e efeitos negativos que recairão sobre os titulares dos dados afetados; (ii) a quantidade de titulares afetados; (iii) quais tipos de dados foram expostos em decorrência do incidente; e (iv) quais medidas imediatas podem ser adotadas para mitigar e/ou reverter a situação, se possível.
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	Os controladores devem informar: (i) data e hora da detecção do incidente; (ii) possíveis consequências e efeitos negativos sobre os titulares dos dados afetados; (iii) dados do agente responsável pelo tratamento e do encarregado (caso aplicável); (iv) estimativa de quando e como serão notificados os titulares; (v) indicar se a notificação é completa (ou seja, se foi possível ou não apurar o incidente, incluindo causas, dados afetados e se houve de fato o acesso por terceiros) ou parcial. Caso seja parcial, é necessário indicar, além das medidas que estão sendo adotadas para a investigação do incidente, a estimativa de conclusão das investigações.
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	A ANPD deve ser informada com a maior brevidade possível, não devendo ultrapassar 2 (dois) dias úteis, contados a partir da data do conhecimento 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 comunicação? As mesmas do §1º do art. 48?	Os titulares de dados devem ser informados no prazo de 2 (dois) dias úteis, contados a partir do momento de comunicação do incidente à ANPD, de modo a avaliar, conjuntamente com esta, a necessidade de informação aos titulares. Na comunicação devem constar, além dos requisitos do §1º do artigo 48, a indicação de um canal de atendimento para sanar eventuais dúvidas e/ou disponibilizar informações úteis aos titulares de dados e, caso a investigação sobre o ocorrido ainda esteja em andamento, informar o prazo estimado para sua conclusão.
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 com o titular deve ser feita através do envio de comunicação pessoal destinada ao titular (por e-mail, envio de mensagem) e através de nota pública divulgada nos canais oficiais do responsável pelo vazamento ou veículo de comunicação de grande repercussão.
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	Pode haver exceção da obrigatoriedade de informar a ANPD quando for constatado que, dentro das primeiras 48 (quarenta e oito) horas após a descoberta do incidente, não houve o vazamento de dados pessoais.

Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	Pode haver exceção da obrigatoriedade de informar os titulares quando for constatado que, dentro das primeiras 48 (quarenta e oito) horas após a descoberta do incidente, não houve o vazamento de dados pessoais.
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	Entendemos que os seguintes critérios devem ser considerados: (i) tipo de dados envolvidos; (ii) número de titulares afetados pelo incidente; e (iii) riscos e eventuais danos que podem vir a ser suportados pelo titular em decorrência do incidente.
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?	Realizar uma análise interna e pormenorizada do incidente, de forma a identificar as causas e mensurar a extensão do dano. Verificar quais medidas adicionais de segurança podem ser implementadas com base no incidente, para mitigar os riscos de novos incidentes no futuro.
SUGESTÃO DE NORMATIVO, SE HOUVER	
Art. Xxxx	
Art. Xxxx	

Zetta

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

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: ZETTA

CPF/CNPJ: 37.253.906/0001-28

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

Zetta

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?	Em primeiro lugar, a fim de oferecer uma orientação precisa, consideramos importante que o conceito de incidente esteja claramente definido. Em consonância com as orientações prévias da ANPD, publicadas no dia 22 de janeiro de 2021[1], considera-se, em primeiro lugar, que incidente *"é qualquer evento adverso, confirmado 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"*. Ressaltamos que as orientações prévias da ANPD citam "qualquer evento adverso" e listam as situações de maneira exemplificativa. Ainda que tal abertura seja desejável do ponto de vista do regulador, a existência de um rol exemplificativo de situações pode gerar incerteza jurídica quanto à obrigação de comunicar um "evento adverso". Considera-se aqui que a própria ideia de "evento adverso" é de difícil conceituação. Dessa forma, sugere-se respeitosamente que a ANPD trace uma definição clara e objetiva sobre o que pode caracterizar um incidente de segurança. Com vistas a definições mais precisas, sugere-se a adoção das definições propostas pelo Grupo de Trabalho Artigo 29 da UE[2]. Nesse sentido: *destruição* indica casos nos quais os dados não mais existem, ou ao menos não existem em um formato que podem ser usado pelo controlador; *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, *vazamento* ou *tratamento inadequado ou ilícito* referem-se às situações de recebimento (ou acesso) aos dados por parte de pessoas ou entidades não autorizadas. Feitas essas definições, é importante traçar uma distinção entre risco e dano relevante ao titular, bem como definir de que forma cada um dos casos deverá ser informado à ANPD.

[1] Disponível em: https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca. Acesso em 24 de março de 2021.
[2] Disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052 . Acesso em 24 de março de 2021.

	Entende-se aqui que há importantes diferenças entre risco e dano efetivo. Nesse sentido, destacamos que é da própria natureza da evolução tecnológica dedicar um esforço constante para manter sistemas e ambientes seguros. O mesmo vale para a proteção de dados pessoais. Uma determinada técnica de proteção de informações pode ser considerada segura até o momento em que se descobre uma nova vulnerabilidade. A descoberta de novas vulnerabilidades, certamente, representa algum tipo de risco. Entretanto, a atualização tempestiva e diligente de sistemas de segurança a partir do momento que uma vulnerabilidade é conhecida pela comunidade técnica não deve ser considerada uma infração às normas de proteção de dados pessoais e, portanto, sujeita a penalidades. Dessa forma, é importante que as ideias de risco e dano possuam gradações que permitam distinguir situações. A noção de risco ou dano "relevante", nesse sentido, cumpre um importante papel.
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?	Com vistas a tornar o processo de notificação de incidentes eficiente para todos os envolvidos, é interessante que a obrigação de notificação seja ponderada pelo risco do incidente vir a causar danos (ou pela relevância dos danos efetivos) aos direitos e liberdades do titular dos dados pessoais. Para elaborar essa métrica, e seguindo as recomendações do Grupo de Trabalho Artigo 29, recomenda-se a utilização de uma matriz que pondere a relevância do incidente com base na sua *gravidade* e *probabilidade*. Recomenda-se que a ANPD consulte a matriz elaborada pelo National Health System (NHS) do Reino Unido, com base nas recomendações do Grupo de Trabalho Artigo 29[3]. Em linhas gerais, incidentes com *gravidade* e *probabilidade* conjuntamente baixos, nos quais os risco não se materializará em um dano, e que não sejam contemplados pelos critérios indicados na resposta às perguntas 1 e 4, não seriam considerados incidentes relevantes, e portanto não deveriam ser necessariamente reportados à ANPD ou aos titulares dos dados pessoais.

[3] Disponível em: https://www.dsptoolkit.nhs.uk/Help (ponto 8 - "incident report" -, páginas 12 a 14). Acesso em 24 de março de 2021.

	Por fim, ressaltamos a importância de dar autonomia ao controlador para classificar os incidentes de acordo com seu modelo de negócios, levando em conta os parâmetros aqui sugeridos e os critérios a serem definidos pela ANPD.
3. Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	Considera-se que há existência de risco ao titular nos eventos que são de alguma forma relacionados à segurança de dados, mas que, embora ainda não haja evidência de materialização de impacto ao usuário, existe a probabilidade de materialização de dano enquanto o evento não for mitigado ou resolvido. Considera-se um dano ao titular quando um evento passa a ser considerado um incidente de segurança; ou seja, quando há evidências de que o risco ao usuário foi materializado, afetando portanto seus direitos. Dessa forma, entende-se que os conceitos de "risco" e "dano" representam dois momentos distintos da ocorrência de um incidente de segurança, com "risco" sendo a probabilidade de ocorrência de um dano, e o "dano" a materialização do risco. Para fins de obrigatoriedade de comunicação de incidentes, e de acordo com a resposta à primeira questão, entende-se que devem ser comunicados apenas os incidentes que apresentem um dano relevante aos titulares de dados.
4. O que deve ser considerado na avaliação dos riscos do incidente?	Além de identificar se o incidente pode levar a situações que possam representar risco de danos (ou tenham causado risco relevante) para os direitos e liberdades do titular dos dados pessoais, conforme descrito na resposta à primeira pergunta, e em consonância com a Publicação da ANPD do dia 22 de janeiro de 2021, sugere-se abaixo os seguintes critérios para a avaliação da relevância e do grau de risco de um incidente: ● Volume de dados pessoais envolvidos; ● Natureza dos dados pessoais envolvidos; ● Possibilidade de os dados envolvidos no incidente permitirem com que o titular seja identificado de forma inequívoca;

	● Possibilidade de o dados envolvidos no incidentes podem ser acessados sem a necessidade de medidas técnicas por parte de terceiros; ● Número aproximado de indivíduos afetados ou potencialmente afetados; ● A boa-fé e as intenções dos terceiros que obtiveram acesso aos dados em função do incidente; ● 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 / reversibilidade da situação que gerou o risco/dano. Ressalta-se que os pontos acima mencionados têm pesos variáveis, e devem ser ponderados caso a caso. Ou seja, por vezes, é possível que o volume de titulares afetados será alto, mas os dados envolvidos no incidente de segurança não serão relevantes, como por exemplo listas de e-mails corporativos. Algumas situações claramente representam riscos ou danos relevantes para os titulares de dados pessoais, em casos de incidentes. Como exemplo, e com base nas orientações prévias da ANPD, publicadas no dia 22 de janeiro de 2021, citamos aquelas situações que: ● envolvam dados pessoais sensíveis, incluindo crianças e adolescentes; ● tenham o potencial de ocasionar danos materiais ou morais, tais como discriminação, violação do direito à imagem e à reputação, fraudes ou perdas financeiras e roubo de identidade. ● coloquem a vida de pessoas em risco a depender de quem tiver acesso aos dados vazados ou a que tipo de informação tiverem acesso; Para além destes casos mais extremos, a relevância de um incidente de segurança deve ser medida observando os critérios de mensuração da gravidade de um incidente, apresentados nas respostas às questões 2 e 3.

5. Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	Entende-se que, em linhas gerais, as informações sugeridas no no §1º do art. 48 da LGPD são suficientes para os propósitos de avaliar possível incidente e adotar medidas necessárias. Reforçamos o princípio de minimização, conforme sugerido pelo Information Commissioner's Office do Reino Unido (ICO)[4], que defende que quaisquer informações a serem comunicadas, principalmente outras informações para além daquelas previstas 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. ● Mínimo Necessário - as informações compartilhadas devem corresponder ao mínimo necessário para que a comunicação seja eficiente. Seguindo esses princípios, e de acordo com exposto nas orientações prévias da ANPD, publicadas no dia 22 de janeiro de 2021, recomenda-se que caso a notificação do incidente à ANPD necessite de outras informações para além daquelas previstas no §1º do art. 48, essas informações devem ser: ● Entidade ou pessoa responsável pelo tratamento. ● Encarregado de dados ou outra pessoa de contato. ● Indicação se a notificação é completa ou parcial. Admite-se a possibilidade de uma comunicação parcial nos casos os quais não seja possível fornecer todas as informações listadas previamente dentro prazo de 72 horas, conforme defendido na questão abaixo Nesse caso, as informações faltantes poderão ser fornecidas posteriormente. ● Informações sobre o incidente em si, como por exemplo a data e a hora do incidente, duração do incidente, e a data e hora da detecção do incidente. ● Junto às informações acerca dos titulares (art. 48, §1º, inciso II), destacar os casos em que o titular pertence a grupo vulnerável (nos termos da resposta à primeira pergunta).

[4] Disponível em: https://ico.org.uk/for-organisations/report-a-breach/ . Acesso em 24 de março de 2021.

	• Possíveis problemas de natureza transfronteiriça. 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. Ainda, no que diz respeito aos meios para comunicação à ANPD, entende-se que a comunicação feita via Peticionamento eletrônico, por meio do preenchimento de um formulário disponível no site da autoridade, conforme disposto nas orientações prévias da ANPD, publicadas no dia 22 de janeiro de 2021, é um meio eficiente e seguro para realização da comunicação, desde que seja mantida a confidencialidade do formulário. Ainda, destaca-se, que é preferível que o formulário seja devidamente padronizado e que possa ser preenchido de forma eletrônica, com vistas a garantir mais segurança e eficiência ao fluxo de comunicação.

6. Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	Em consonância com o estabelecido na GPDR (art. 33, §1º)[5], sugere-se que o controlador tenha um prazo de até 72 horas para informar à ANPD sobre o incidente de segurança, a partir do momento no qual o controlador tenha a confirmação da sua ocorrência. 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 existe.

[5] Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 . Acesso em 24 de março de 2021.

	Ainda de acordo com o Grupo de Trabalho Artigo 29, entende-se que a falta conhecimento de informações precisas acerca do incidente (como por exemplo o número exato de titulares afetados) não deve ser impeditivo para a notificação dentro do prazo de 72 horas. O controlador deve reportar dentro deste prazo todas as informações que são do conhecimento no presente momento, e uma vez esclarecidos os motivos pelos quais ele não tem total ciência da extensão completa do incidente, a ele deve ser concedida a possibilidade de reportar o restante das informações acerca do incidente de modo faseado, conforme vá tomando ciência das mesmas.
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?	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 graves aos direitos e liberdade individuais seja baixo. Ainda, nos casos em que o risco de causar danos graves aos direitos e liberdade individuais seja alto, é também mandatório que os titulares sejam avisados. 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. Assim, defende-se que a notificação aos titulares seja feita assim que possível, uma vez que a ANPD tenha sido notificada ela mesma acerca do incidente e em seguida emitir o entendimento de que naquele caso os titulares também devem ser informados. Nessa situação o controlador tem até 72 horas, após o parecer da ANPD, para comunicar os titulares. Em consonância com o disposto na GPDR (art. 34), a comunicação para os titulares deve conter, de forma clara, 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. ● Dados do titular estão envolvidos no incidente. ● Ações que o titular pode realizar para mitigar possíveis riscos/danos (como atualização de senha, por exemplo).

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.)?	Com base nas recomendações do *European Data Protection Board* (EDPB)[6] e do Grupo de Trabalho do Artigo 29, a comunicação deve ser preferencialmente individual, de forma transparente, e desacompanhada de outras informações não relativas ao incidente (como atualizações acerca de algum produto ou serviço, por exemplo). Meios de comunicação individuais legítimos incluem e-mails e SMS, por exemplo. Ressalta-se, contudo, que 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. Em casos nos quais a comunicação individual se mostre onerosa, a comunicação pública é permitida, desde que também seja transparente e desacompanhada de outras informações não relativas ao incidente. Meios de comunicação pública legítimos incluem anúncios proeminentes no *website* do controlador e anúncios na mídia impressa. Considera-se que a comunicação individual é onerosa nos casos em que os esforços técnicos para a comunicação forem demasiados altos, tendo como critérios o números de titulares afetados, bem como os custos da comunicação. Por fim, defende-se que caso o risco já tenha sido mitigado, sem que tenha havido qualquer impacto para o titular, a comunicação pelo controlador deveria ser facultativa. Nesse sentido, a GDPR também já dispõe sobre essa possibilidade em seu artigo 34.
9. Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	Defende-se a não obrigatoriedade de informar à ANPD em casos nos quais o incidente não seja classificado como relevante, nos termos da resposta à primeira pergunta, bem como com base nos critérios aventados nas respostas às perguntas 2 e 4.
10. Quais seriam as possíveis exceções da obrigatoriedade de informar	Com base nos critérios estabelecidos pela GPDR (art.34), entende-se que não deve haver a obrigatoriedade de informar aos titulares nos casos em que:

[6] Disponível em: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf . Acesso em 24 de março de 2021.

os titulares?	• Antes do incidente, o controlador tenha implementado medidas técnicas e organizacionais adequadas à proteção os dados pessoais, em especial aquelas medidas que buscam tornar os dados pessoais não inteligíveis para qualquer pessoa que não esteja autorizada a acessá-los; • Imediatamente após o incidente, o controlador tome medidas com vistas a garantir que o risco de danos para os direitos e liberdades dos indivíduos não se materialize; • A comunicação individual com os titulares demande esforços desproporcionais. Nesses casos, conforme exposto na resposta à pergunta 9, deve ser possível a comunicação pública. Os controladores devem ser capazes de comprovar os pontos acima mencionados. Ressalta-se que, embora em um primeiro momento a ANPD possa determinar que não há a necessidade de informação dos titulares, fica aberta a possibilidade de mudanças nesse parecer caso, com o passar do tempo, novas investigações ou informações comprovem que a relevância do incidente é maior do que se supunha a princípio.
11. 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 análise da gravidade do incidente se dê com base em critérios estabelecidos em um espectro de gravidade e probabilidade, conforme demonstrado na resposta à segunda questão, bem como os critérios aventados na resposta à quarta questão.
12. 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.

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?	Sugere-se que ao recomendar providências após a comunicação de incidentes por parte dos controladores, essas recomendações levem em consideração as medidas de segurança já adotadas pelo controlador e tomar como base o incidente em questão, revisando riscos já mapeados, controles implementados e eventuais novos riscos. Defende-se também que as recomendações considerem o impacto que elas podem vir a ter no modelo de negócio da empresa, bem como a possibilidade técnica e financeira de implementação. Nesse sentido, seria razoável que o controlador pudesse propor alternativas e um prazo razoável para cumprir as recomendações da ANPD.
Outras sugestões	Defende-se as seguintes sugestões complementares: ● Um controlador deve poder reportar casos, mesmo que não qualificados como incidentes ou como incidentes relevantes, quando o reporte contemplar informações relevantes para que a comunidade técnica tome conhecimento de novas vulnerabilidades em sistemas de segurança e tecnologias de proteção de dados pessoais. Tais informações podem ser úteis para que a ANPD tome ações no sentido de promover ações educativas e melhorias no ambiente de segurança no País. ● Deve haver isenção de penalidades no caso de o controlador ter adotado todas 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. ● Como a obrigação de reportar o incidente recai sobre o controlador e, por vezes, o controlador 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.

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 Brasileira Online To Offline
CPF/CNPJ: 24.030.490/0001-37

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 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?	- Considerar como risco ou dano relevante apenas aqueles que puderem de fato oferecer um risco para os direitos e liberdades das pessoas individuais, conforme se tem observado no direito estrangeiro. - A definição de “relevante” deve ser bastante objetiva e o mais restritiva possível, de modo a garantir a segurança jurídica na aplicação da LGPD. Ainda que o Recital 75 da GDPR defina “dano relevante”, a definição é ainda muito ampla e pode gerar interpretações descentralizadas. *Referências*: Lei nº 25.326: A Lei prevê como infração grave a violação do dever de sigilo de dados sensíveis. Esse critério poderia ser analogicamente utilizado para definir um potencial risco em caso de incidentes. **-** Quando o usuário é impedido de acessar informações de sua conta ou mesmo utilizá-la por um período prolongado,

	desde que comprovado que tal impedimento decorre do incidente. -Quando envolver dados sensíveis comprometidos em virtude de uma falha na segurança do controlador. - Quando o cliente for vítima de fraude utilizando a plataforma. - Um critério para avaliar um incidente como relevante é a quantidade de dados comprometidos, atrelados à sua criticidade/sensibilidade.

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 diferenciar as definições de risco e dano. O dano é o risco que de fato se materializou e o risco é a probabilidade de uma ameaça se materializar. Nesse sentido, deveriam ser reportados apenas os danos materializados, sendo que o impacto do dano poderia ser medido a partir de uma análise de riscos. - Para fins da análise de risco, pode-se dividir os riscos de acordo com os seguintes listados abaixo, sendo que somente os riscos classificados como “altos” e “críticos” deveriam ser considerados como “relevantes” na análise. - Crítico - Alto - Médio - Baixo O impacto do dano gerado pelo o incidente deveria ser avaliado após ponderar os seguintes aspectos: - Quantidade de registros/dados comprometidos - Tipos dos registros/dados comprometidos - Tipo e quantidade de usuários afetados - Pilar de Segurança afetado (Confidencialidade/Disponibilidade/Integridade) - Exposição do incidente - Tempo de inatividade/impacto do serviço alvo - Métricas organizacionais principais afetadas - Monetização associada - Possibilidade de relacionar a informação ao indivíduo - Possibilidade de o dado ser utilizado de forma indevida e de fato gerar dano ao titular - Verificar se o dado está de fato acessível ou se seria exigida alguma medida técnica para fazê-lo - Analisar a natureza das atividades atreladas ao incidente

	- Incidentes cujo impacto seja baixo/médio não devem ser reportados necessariamente, principalmente se o controlador tiver adotado as medidas para mitigar os danos. - Adotar como base as orientações do Conselho Europeu de Proteção de Dados (EDPB).
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	- Se considera um risco ao titular os casos que estejam marcados como eventos de segurança: quando não há evidência de materialização de impacto ao usuário, mas que existe o risco de materialização enquanto o evento não for mitigado/resolvido. - Se considera um dano ao titular quando um caso passa a ser considerado um incidente de segurança; ou seja, quando há evidências de que o risco ao usuário foi materializado (o que afeta os seus direitos). Importante mencionar que só deveriam ser reportados os incidentes que eventualmente afetem dados pessoais e tragam impacto negativo relevante ao titular.

O que deve ser considerado na avaliação dos riscos do incidente?	- Como mencionado acima, o ideal seria que a obrigação de reportar tivesse relação com o dano efetivamente causado ao titular e não somente os riscos (não materializados). Algumas variáveis a se considerar são: - Impacto interno (organização) a áreas/processos/plataformas - Impacto a usuários/clientes - Quantidade e qualidade dos registros/dados comprometidos - Monetização ou perdas relacionadas - Tipos dos registros/dados comprometidos - Tipo e quantidade de usuários afetados - Pilar de Segurança afetado (Confidencialidade/Disponibilidade/Integridade) - Exposição do incidente - Tempo de inatividade/impacto do serviço alvo - Métricas organizacionais principais afetadas - Possibilidade de relacionar a informação ao indivíduo - Possibilidade de o dado ser utilizado de forma indevida e de fato gerar dano ao titular - Verificar se o dado pessoal está de fato acessível ou se seria exigida alguma medida técnica para fazê-lo
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	-Unicamente as sugeridas pela norma, as quais já são suficientes para avaliar eventual incidente e adotar as medidas necessárias.

Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	-O prazo de 10 (dez) dias úteis a partir do momento em que o incidente de segurança é detectado de forma inequívoca. 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 regulamentação) para comunicar o incidente. - Em virtude da estrutura reduzida da ANPD, o mais razoável seria reportar apenas as suspeitas efetivamente confirmadas, já que o controlador terá de fato um dano materializado para apontar à Autoridade. -Ressalte-se que é importante que sejam adotadas medidas para restringir a publicidade das investigações em curso, para não afetar desnecessariamente a reputação da empresa. Tais medidas também protegem os titulares de dados, pois pode haver vulnerabilidades que ainda estão sendo analisadas pelo controlador.
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 a constatação inequívoca do incidente e a sua respectiva comunicação à ANPD, os titulares afetados deveriam ser comunicados no prazo de 72 (setenta e duas) horas. -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.

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 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. - 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, conforme abaixo. "*A comunicação ao titular dos dados a que se refere o n.o 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 aceder a esses dados, tais como a cifragem;* *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 n.o 1 já não é suscetível de se concretizar; ou* *c) 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."*

Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	- Hipóteses nas quais os controladores não deveriam ter a obrigação de comunicar o incidente aos usuários: (i) Se, antes da violação, o controlador tiver implementado medidas técnicas e organizacionais aptas a proteger os dados pessoais, tornando-os inteligíveis 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; (iii) Se a comunicação com os indivíduos demandar esforços desproporcionais.
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	- Idem resposta acima.
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	- Idem critérios mencionados no item 2. O ideal seria que tais critérios fossem explorados para a criação de gradações de riscos (baixo, médio, alto, crítico), para que fique claro ao controlador o que de fato seria considerado como crítico, possibilitando que a ANPD indique medidas adicionais a serem adotadas pelo controlador para garantir a segurança do titular.
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	- Para o processo de resposta a incidentes, poderia ser utilizado o processo do NIST - Gestão de riscos (ISO 31000)

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 recomendações da ANPD devem levar em consideração as medidas de segurança já adotadas pelo controlador e tomar como base o incidente em questão, revisando riscos já mapeados, controles implementados e eventuais novos riscos. - Considerar o impacto das recomendações no modelo de negócio da empresa, bem como a possibilidade técnica e financeira de implementar as recomendações. Nesse sentido, seria razoável que o controlador pudesse propor alternativas e um prazo razoável para cumprir à recomendações da ANPD.
Outras Sugestões	- Deve haver isenção de penalidades no caso de o controlador ter adotado todas 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 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.

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: ALEXANDRE RIBEIRO DANTAS

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 acarreta danos relevantes quando ameaça ou limita os direitos e as liberdades individuais previstos em legislação nacional (necessário fazer um levantamento jurídico sobre isso).** **Recomendo utilizar uma taxonomia de dano como a proposta pelo prof. Daniel Solove (ver 3ª questão a seguir).** **Adicionalmente, recomendo alinhamento quanto aos critérios definidos no âmbito da União Europeia. Em especial, Guidelines 01/2021.**
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?	**Sim, os riscos/danos devem ter, ao menos, uma escala de 3 níveis.** **Sugiro que os riscos/danos de baixa criticidade não sejam considerados relevantes e que haja tratamento diferenciado em termos de prazos e sanções conforme a gradação do risco.** **Os critérios para avaliar a criticidade do dano/risco podem incluir, mas não se limitar a:** **- Quantidade de titulares afetados.** **- Quantidade de registros afetados/expostos.**

	- Categoria dos dados afetados/expostos, especialmente, dados pessoais sensíveis e de vulneráveis (crianças e adolescentes). **- Abrangência territorial** **- Se limitam a riscos ou já materializaram danos aos titulares** **Ainda, sugiro considerar os tipos de danos associados à violação (com base na taxonomia do Daniel Solove) – por exemplo, um dano é altamente relevante se envolver roubo de identidade, perdas financeiras, chantagem, negação de serviços/produtos/direitos, dano reputacional, etc.** **Pode ser construída uma escala numérica para cada fator de risco e uma fórmula que consolide o grau de risco a partir dos fatores, em média aritmética ou ponderada.**
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	**O dano pode ser entendido como a materialização do risco. Os riscos devem ser avaliados em relação ao seu potencial de levar a um ou mais danos aos titulares.** **Recomendo considerar os danos objetivos e subjetivos, para isso, sugiro o artigo do M. Ryan Calo. Já o artigo do Daniel J. Solove poderia ser a base para as categorias de risco/dano aos titulares (extrato sumarizado na figura anexa).**

	A. *Information Collection* 1. Surveillance 2. Interrogation B. *Information Processing* 1. Aggregation 2. Identification 3. Insecurity 4. Secondary Use 5. Exclusion C. *Information Dissemination* 1. Breach of Confidentiality 2. Disclosure 3. Exposure 4. Increased Accessibility 5. Blackmail 6. Appropriation 7. Distortion D. *Invasion* 1. Intrusion 2. Decisional Interference **Solove, Daniel J (2006) "A Taxonomy of Privacy", University of Pennsylvania Law Review, Vol. 152 Nº 3** **Calo, M. Ryan (2011) "The Boundaries of Privacy Harm", Indiana Law Journal: Vol. 86:3, Article 8.**
O que deve ser considerado na avaliação dos riscos do incidente?	**Devem considerar se os riscos materializaram ou não danos aos titulares.**
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	**Sugiro alinhamento com a legislação da União Europeia, em especial, destaco a da autoridade britânica:** **- Descrição e natureza dos dados pessoais afetados** **- Categoria e número aproximado de titulares afetados** **- Categoria e número aproximado de registros afetados** **- Informações de contato do Encarregado** **- Descrição dos danos materializados ou possíveis consequências (riscos) do incidente**

	- Descrição das medidas tomadas ou propostas para lidar com a violação e para mitigar efeitos adversos
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	**Sugiro alinhamento com a legislação da União Europeia, mantendo prazo inicial de até 72 horas da identificação do incidente para a primeira comunicação.** **Nota-se que essa comunicação não se extingue com o primeiro contato, devendo abrir-se um canal contínuo de comunicação enquanto o incidente estiver em análise e contenção, até o seu fechamento.**
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?	**Sugiro prazo inicial de até 72 horas após a identificação da criticidade/relevância do incidente, ou seja, esse prazo pode ser superior ao prazo de informe para a ANPD, pois requer uma etapa adicional de análise 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.)?	**A comunicação deve seguir uma ordem de prioridade, dentro do que for viável, senão justificar:** **- Comunicação direta com o titular e de forma digital (e-mail, SMS)** **- Comunicação ampla (nota) em veículos de comunicação/imprensa** **A comunicação postal pode não ser adequada em relação aos prazos e a telefônica de difícil rastro.**
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	**Todos os incidentes de violação de dados devem ser comunicados a ANPD.**
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	**Para os incidentes de criticidade/relevância baixa, conforme escala e metodologia definida anteriormente.**

Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	**Se aplicam os mesmos critérios da questão 2ª anterior.**
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	**ISO/IEC 27035 — Information security incident management** **ISO/IEC 27035-1 — Information security incident management - Part 1 Principles of incident management** **ISO/IEC 27035-2 — Information security incident management - Part 2 Guidelines to plan and prepare for incident response** **ISO/IEC 27043 — Incident investigation**
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	**Isso vai variar caso a caso dependendo de uma análise preliminar 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: Federação das Associações das Empresas Brasileiras de Tecnologia da Informação – FEDERAÇÃO ASSESPRO
CPF/CNPJ: 42.581.264/0001-26

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 ocorrência de um incidente não necessariamente pode trazer danos aos titulares de dados. Incidentes de dados relacionados às questões financeiras (exigidas no país tais como CPF, data de nascimento, RG e outras conforme resolução nº 2025 de 1993) bem como dados sensíveis podem trazer severos danos. Geralmente estes incidentes trazem como consequência o uso dos dados para perpetração de fraudes financeiras (roubo de identidade, extorsão, roubos digitais, sequestro de dados etc.) Cabe aqui ressaltar que a ASSESPRO, em consonância com seus valores, ideais e objetivos, sugere um sistema simplificado de classificação de riscos pois, grande parte das empresas (MEI, microempresa, pequena empresa e startups – ultrapassa 20 milhões de CNPJ) possui um baixo grau de maturidade de gestão tanto do negócio quanto da segurança da informação.

	Os critérios para mensuração de risco que sugerimos, a serem avaliados pela ANPD, levando-se em conta que o Nível de Risco é a "magnitude de um risco, expressa em termos da combinação das consequências e de suas probabilidades" conforme a ISO 31000:2018:
	
	• **Categoria do risco: Alto**
	  ○ Dados financeiros (dados bancários, dados de cartão de crédito, IRPF, CPF, remuneração, data de nascimento, filiação, situação patrimonial, dívidas etc.)
	  ○ Dados sensíveis: orientação sexual, filiação partidária, religião, entre outros conforme a LGPD, dados que possam gerar discriminação,
	  ○ Dados de saúde;
	  ○ Dados legais da medicina do trabalho (exames admissionais e demissional)
	  ○ Dados pessoais de acesso: senhas de banco, e-mail, senhas e códigos de acesso e/ou segurança, dados de biometria etc.
	  ○ Dados genéticos, DNA, análise hereditária e de família
	
	• **Categoria do risco: Médio**
	  ○ Dados referentes a localização
	  ○ Dados relativos às condenações e às infrações penais
	
	• **Categoria do risco: Baixo:**
	  ○ Dados genéricos (histórico de compras, histórico de navegação)
	  ○ Dados que não possibilitem lesão patrimonial ou financeira, discriminação de nenhuma forma ou perpetração de crimes a terceiros.
	
	Os critérios para avaliação de risco dependem de metodologia ou *framework* a ser utilizado, por isso, apontamos aqui os critérios sugeridos para a mensuração e elaboração de uma matriz de riscos. A avaliação de risco em segurança da informação consiste em levantar as principais ameaças que possam impactar o ambiente, ou seja, gerar um impacto indesejável e muitas vezes crítico para as organizações. Devem ser avaliados os seguintes critérios:
	
	• **Ameaça** (causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização);
	• **Probabilidade** (possibilidade de algo acontecer que seja determinada, medida ou estimada, objetiva ou subjetivamente, frequências ou probabilidade matemáticas);

	O método de avaliação de ameaças, ativos e vulnerabilidade operacional críticas (OCTAVE) é amplamente utilizado e pode ser empregado em controladores de todos os portes (desde MEI até grandes corporações).
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?	Temos que primeiramente nos atentar ao conceito de cada palavra, onde, um risco não necessariamente gera um dano, seja ele físico, financeiro ou moral. O termo risco provém do italiano risico ou rischio que, por sua vez, deriva do árabe clássico rizq ("*aquilo que se depara com a providência*"). O termo faz referência à proximidade ou contingência de um possível dano. Considerando o conceito adotado pelo COSO (*Framework de negócios para governança e gestão de TI*), temos a seguinte definição: "**Risco é a possibilidade de que um evento ocorra e impacte negativamente a condição da empresa de atingir objetivos previamente estabelecidos**." Quanto ao termo dano, temos a seguinte definição: "*Dano é toda lesão a um bem juridicamente protegido, causando prejuízo de ordem patrimonial ou extrapatrimonial*". No dicionário da língua portuguesa encontramos a seguinte definição: "1. Estrago; prejuízo. 2. Prejuízo sofrido ou causado por alguém (*ex.: danos físicos; danos morais; danos patrimoniais*)". Podemos ainda encontrar a seguinte definição de dano quando consideramos a segurança da informação associada ao termo: Os danos são as possíveis consequências de um incidente, exatamente as consequências que desejamos evitar. Os danos podem ser **diretos** (como a indisponibilidade de um e-commerce ou um acesso a informações confidenciais de uma empresa) e **Indiretos** (como a queda das ações da empresa na bolsa de valores ou perda de clientes). Classificar o dano é algo complexo, pois depende de inúmeras variáveis e depende do impacto causado. Podemos definir o impacto para as empresas, para os titulares de dados, o CPC (artigo 1045 da Lei 13105 de 2015 e o CC (artigos 186, §5° do Artigo 292 e 944 da Lei 10406 de 2002) além das súmulas 37 e 387 do Superior Tribunal de Justiça definem diversas penalidades aos responsáveis pelos danos causados. Estes danos dependem da percepção (lesão de interesses não patrimoniais de pessoa natural ou jurídica conforme o CC, art. 52; Súmula nº 227 do STJ) de casa titular de dados e as consequentes infrações perpetradas utilizando seus dados obtidos no incidente de segurança da informação. Cabe ainda ressaltar que, quando nos referimos a incidentes, eles podem de ser de ordem digital ou física.

	Para fins de regulamentação de normas, vimos por meio desta consulta sugerir que os riscos sejam somente registrados juntamente ao Encarregado de Dados (DPO) responsável na empresa em ferramenta adequada (*seja ela em relatório físico ou em plataforma digital*). Para empresas de micro e pequeno porte, em não exigindo-se a contratação de um DPO, sugerimos que a ANPD forneça em seu sítio eletrônico, por meio de download, modelo de relatório, simplificado, a ser preenchido pelo responsável legal da empresa a fim de manter histórico de riscos e possibilitar o subsídio de informações para um modelo de gestão de riscos que venha a ser implantado nestas empresas. Cabe ressaltar que, exigir investimentos significativos em modelos de gestão de segurança da informação, governança e risco (GRC) em empresas do tipo MEI, Micro Empresa, Pequena Empresa e Startups pode dificultar a operação destas, sendo assim, recomendamos somente o fornecimento por meio da autoridade instituída, o fornecimento de relatórios padronizados para a documentação e quando oportuno (considerando-se a maturidade das empresas no Brasil), o desenvolvimento de mecanismos de gestão para estas organizações. Para os controladores que já tem implementados modelos de governança e risco da tecnologia da informação, sejam eles de qualquer porte, recomenda-se que apenas continuar gerindo a segurança da informação e a privacidade de dados conforme método escolhido.
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	Podemos entender conforme o conceito de risco (fonte ISO 31000:2018) e dano exposto no quesito anterior que, um risco baseia-se em ameaças e fatores inerentes ao negócio, e podem ser mensurados através de metodologias e frameworks apropriados para esta mensuração. Os danos por sua vez são mais complexos de serem avaliados, pois depende da percepção de cada pessoas e principalmente dos dados alvo do incidente, da sua propagação, das consequências deste incidente e da possibilidade de corrigi-lo entre outras inúmeras variáveis. Desta forma, o dano é uma consequência do incidente de mensuração empírica e o risco é um fator inerente à operação mensurável pelo controlador de dados.
O que deve ser considerado na avaliação dos riscos do incidente?	Quando falamos de riscos do incidente, devemos ter o entendimento que a violação dos direitos do titular de dados já ocorreu, desta forma cabe ao controlador de dados comunicar aos titulares envolvidos, à ANPD, aos operadores e tomar medidas para corrigir o incidente. Basicamente as ações iniciais devem ser:

	1. Identificar a origem do incidente 2. Categoria do Incidente 3. Autoria do incidente 4. Identificar quais dados, sua classificação e direitos dos titulares foram alvo do incidente 5. Corrigir os métodos, processos, ações e políticas de segurança da informação para evitar a recorrência do incidente 6. Documentar todo o caso do incidente 7. Reparar os danos causados aos titulares conforme CPC e demais legislações brasileiras pertinentes ao ocorrido. Quando falamos de mitigação destes riscos, estamos falando de um modelo de gestão de riscos que deve incluir a identificação, análise, avaliação, tratamento, aceitação, comunicação, monitoramento e revisão do risco em seu processo, em que se deve analisar todos os riscos inerentes 'as atividades de uma determinada organização, processo ou atividade. Na ISO 31000:2018 são sugeridos os seguintes aspectos para avaliar a significância dos riscos: • A natureza e os tipos de causas e de consequências que podem ocorrer e como elas serão medidas; • Como a probabilidade será definida; • A evolução no tempo da probabilidade e/ou consequência(s); • Como o nível de risco deve ser determinado; • Os pontos de vista das partes interessadas; • O nível em que o risco se torna aceitável ou tolerável; e • Se convém que combinações de múltiplos riscos sejam levadas em consideração e, em caso afirmativo, • Como e quais combinações convém que sejam consideradas.
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	A ASSESPRO entende que além dos dados já solicitados no §1º do art. 48 da LGPD, são necessários pelo menos mais três dados muito importantes para que a ANPD tenha condição de avaliar o incidente de acordo com o §2º e §3º do art. 48 da referida lei e desta forma determinar ações e realizar juízo de gravidade: • Se o incidente(tipo e categoria) já ocorreu antes • A frequência que este mesmo incidente tem • Período do incidente (*pelo menos do início estimado até a detecção*)

Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	Entendemos que os prazos devem considerar o porte das empresas, pois como é sabido (pesquisa realizada pelo IDC com matéria publicada em https://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=54806&sid=5), no Brasil empresas do tipo MEI, microempresa, pequena empresa e startups tem um nível de maturidade baixo quanto à sua gestão de segurança da informação, gestão de processos e capacidade de investimento para implantar sistemas adequados de gestão de riscos. • Para médias e grandes empresas, este comunicado deve ocorrer em até 48horas úteis, a contar da detecção do incidente; Para Micro, pequena, startups e MEI este prazo deverá ser de até 72 horas úteis, a contar da detecção 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 comunicação? As mesmas do §1º do art. 48?	Devemos levar em consideração não somente a legislação de proteção de dados, mas outras que de forma indireta definem prazos, como por exemplo a Lei nº 8.078, de 11 de setembro de 1990 ("Código de Defesa do Consumidor") no §1° do artigo 10 determina que: "*O fornecedor de produtos e serviços que, posteriormente à sua introdução no mercado de consumo, tiver conhecimento da periculosidade que apresentem, deverá comunicar o fato imediatamente às autoridades competentes e aos consumidores, mediante anúncios publicitários*." Por esta razão, constatado um incidente de segurança os consumidores (titulares de dados) devem ser avisados uma vez que a depender do caso pode haver risco à segurança destes indivíduos. Entendemos que assim que constatado um incidente de segurança, ele seja reportado aos titulares de dados em meios de comunicação (telefone, e-mail, etc) e/ou mídias sociais e para empresas de médio e grande porte, também em jornais de grande circulação.
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	Pesquisas recentes (Pnad Contínua TIC 2019 realizada pelo Cetic.br - https://cetic.br/pt/publicacao/pesquisa-sobre-o-uso-das-tecnologias-de-informacao-e-comunicacao-nos-domicilios-brasileiros-tic-domicilios-2019/) mostram que muitos cidadãos brasileiros têm acesso à internet (*conforme a pesquisa, três em cada quatro brasileiros têm acesso à internet*) e à dispositivos móveis com internet (*smartphones e dispositivos móveis representam 99% das ferramentas de*

admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	*conexão*). Entendendo que esta realidade ainda não alcança a todos os cidadãos, sugerimos um modelo misto de comunicação, considerando-se sempre duas variáveis: a) o porte do controlador; b) severidade do incidente. • Todos os incidentes de grande severidade, onde o risco avaliado para de perpetração de crimes contra os titulares de dados é alto, a comunicação deve ser direta e por meio de comunicação pública (*os meios de comunicação seguem a sugestão fornecida no item anterior desta tomada de subsídios*). • Os incidentes de menor severidade, mas ainda assim de médio risco podem ser comunicados por meios eletrônicos de comunicação pública. • Incidentes de baixa severidade e baixo risco para os titulares de dados podem ser apenas informados através de mídias sociais, site do controlador ou site de associações a quem o controlador esteja ligado (exemplo: cooperativas), sem a necessidade de comunicação individual.
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	Em análise de legislação pertinente, a ASSESPRO não identificou nenhuma possível situação em que o controlador não comunique à ANPD obrigatoriamente qualquer tipo de incidente ocorrido. Entendemos que qualquer tipo de exceção se trataria de uma ilegalidade, mesmo que aplicada para ente público, de qualquer autarquia.
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	Considerando a legislação vigente no Brasil (leis número 13709, 12965 e 12737 além do CPC), a ASSESPRO entende que somente casos em que o próprio titular de dados é o responsável pelo incidente e única e exclusivamente ele é afetado por tal incidente, não se faz necessário nenhum tipo de comunicação obrigatória por parte do controlador ao titular de dados.
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	Quando falamos de gravidade do incidente de segurança, temos que observar dois entes fundamentais na análise: o titular de dados e o controlador dos dados. Mensurar a o dano e a gravidade do incidente para o titular de dados é complexo, pois cada pessoa tem uma percepção do ocorrido, sendo assim, muito difícil chegar a um denominador comum. Para um melhor atendimento das percepções dos titulares de dados, recomendamos que eles busquem junto à legislação brasileira (CC, CPC, LGPD, Marco Civil da Internet e demais legislações vigentes) a reparação e mensuração de perdas e danos.

	No caso dos controladores, pode-se avaliar com maior acuracidade tanto a gravidade quanto a origem do incidente e desta forma utilizar metodologias e normas para aferir o quão grave um incidente é. Existem algumas metodologias que são reconhecidas mundialmente para gestão de segurança da informação. Uma vez levantados ou elicitados os ativos de informação de uma organização, estes precisam ser valorados, isto é, ordenados dos mais críticos ao menos críticos, segundo o julgamento dos analistas, que deve ser o menos subjetivo possível. Na GRSI (Gestão de Risco da Segurança da Informação), essa valoração é inicialmente estabelecida em dois passos: a. Levantamento de consequências operacionais da perda de segurança em ativos; b. Estimativa de impacto sobre negócios relacionados à perda de proteção para cada ativo A ISO 27005:2018 apresenta, no seu Anexo B, um conjunto de critérios que podem ser empregados para atribuição de valores de criticidade aos ativos na ocorrência de eventos em geral. A recomendação é que se defina uma base comum de análise, e duas formas são indicadas: a. pela análise das consequências operacionais resultantes da perda de confidencialidade, integridade, disponibilidade, não repúdio, contabilização, autenticidade ou confiabilidade dos ativos; e b. de forma mais simples, pela avaliação direta dos impactos sobre os negócios da organização, em decorrência do comprometimento dos ativos. Acerca da primeira abordagem, algumas consequências operacionais a considerar são (ISO/IEC, 27005:2018): a. violação da legislação, regulamentos ou contratos; b. redução no desempenho de negócios; c. perda de confiança e reputação de clientes e sociedade; d. vazamento de informação pessoal; e. aumento de perigos para os colaboradores; f. efeitos adversos no cumprimento da lei; g. brechas de confidencialidade;

	h. brechas na ordem pública; i. perdas ou custos financeiros; j. riscos e crises ambientais; k. crise governamental; l. interrupção de serviços; m. perda de vantagem competitiva. Abordagens qualitativas são usualmente adotadas para avaliar as consequências de comprometimento dos ativos, uma vez que a atribuição de valores financeiros a ativos nem sempre é possível. Uma escala de pelo menos três valores pode ser usada: alta, média e baixa. A ISO 27005 propõe, para a avaliação do impacto operacional direto e indireto, a consideração dos seguintes efeitos: a. custo financeiro de substituição de um ativo; b. custo de aquisição, configuração e instalação de um novo ativo ou de seu backup; c. custo de operações suspensas devido ao acidente, até que o serviço seja restaurado; d. resultados devido a brechas na segurança da informação; e. violação de obrigações; f. violação de códigos de conduta, entre outros A ASSESPRO recomenda a utilização dos critérios adotados na metodologia OCTAVE ALLEGRO para adoção de critérios de análise e mensuração da gravidade do incidente. Esta metodologia é conhecida e faz parte das soluções apontadas pela ENISA (The European Union Agency for Cybersecurity) para utilização na Europa. A abordagem OCTAVE está focada na identificação dos ativos críticos e das ameaças que incidem sobre esses ativos, das vulnerabilidades ambas organizacionais e tecnológicas que expõem essas ameaças e criam um risco para o controlador. O OCTAVE usa uma metodologia com três fases para examinar a organização e os recursos tecnológicos. Os resultados obtidos nas três fases fornecem um gráfico de informações úteis para a identificação das necessidades de segurança da organização:

	Fase 1 - Construção do perfil das ameaças baseado em ativos: esta fase dá o conhecimento necessário sobre os ativos, ameaças e estratégias de proteção. Essa etapa consiste dos seguintes processos: 1. Identificação de informações no contexto do gerenciamento sênior: gerentes seniores são selecionados para identificar ativos importantes, ameaças, requerimentos de segurança, práticas atuais de segurança e vulnerabilidades organizacionais; 2. Coleta do conhecimento do gerenciamento da área operacional: gerentes da área operacional são selecionados para identificar ativos importantes, ameaças, requerimentos de segurança, práticas atuais de segurança e vulnerabilidades organizacionais; 3. Obtenção de informações referente ao conhecimento dos funcionários: são selecionados membros de diversas áreas de TI para identificar ativos importantes, ameaças, requerimentos de segurança, práticas atuais de segurança e vulnerabilidades organizacionais; 4. Elaboração dos perfis das ameaças: a equipe de análise avalia as informações do processo 1 a 3, selecionando os ativos críticos, refina os requisitos de segurança associados e identifica as ameaças a esses ativos, criando perfis da ameaça. Fase 2 - Identificação da infraestrutura das vulnerabilidades: A equipe de análise examina os principais componentes para deficiências operacionais (tecnologia e vulnerabilidades) que podem conduzir a uma ação não autorizada contra os ativos. Os processos da fase 2 são: 5. Identificação dos componentes chaves de segurança: a equipe de análise identifica os componentes e sistemas de tecnologia da informação chaves para cada ativo crítico; 6. Avaliação dos componentes selecionados: são analisados os componentes e sistemas chaves para as fragilidades de tecnologia. Os resultados são examinados para identificar a relevância dos ativos e os perfis das ameaças. Fase 3 - Desenvolvimento de planos e estratégias de segurança: Durante essa avaliação são identificados os riscos para os ativos da organização e são decididas as medidas de proteção. Os processos da fase 3 são: 7. Condução da análise de riscos: são identificados os impactos das ameaças sobre os ativos, são criados critérios para a avaliação desses riscos e avaliados os impactos baseados nesses critérios. O processo 7 reproduz o perfil dos riscos; 8. Desenvolvimento de uma estratégia de proteção: é criada uma estratégia de proteção para a organização e planos de mitigação para ativos críticos, baseados na análise de

	informações obtidas. Esta recomendação baseia-se na premissa de que o incidente só pode ser mensurado e seu impacto no controlador, conforme já mencionado anteriormente. A avaliação desta gravidade para o titular de dados é subjetiva e deve ser amparada em legislação já apontada neste documento.
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	Existem diversas normas e frameworks reconhecido mundialmente para a gestão de riscos e incidentes focados em segurança da informação e controles internos. Descrevemos as principais e de maior relevância para a análise da ANPD. Não há apenas uma única que atende somente ao objetivo de analisar a gravidade de um incidente, pois o mesmo, não se restringe somente a um departamento da empresa, mas sim permeia por toda organização e por várias vezes extrapola suas fronteiras, atingindo todo ecossistema em que a organização está inserida. Dentre os frameworks citados abaixo, a ASSESPRO recomenda a utilização do OCTAVE por ser uma metodologia que pode ser facilmente utilizada por pequenas empresas e por grandes corporações. **ISO** - Trata-se de um conjunto de práticas para a gestão de riscos que as organizações enfrentam, tendo como foco boas práticas e padrões internacionais de gestão de risco. Normas ISO voltadas à Segurança da Informação: A norma tem como princípio geral a adoção pela organização de um conjunto de requisitos, processos e controles, que visam gerir adequadamente o risco presentes nas organizações. Um elevado número de organizações no mundo utiliza as práticas documentadas na ISO 27001:2013 e usufruem dos benefícios da sua adoção pela certificação. Além disso, essas organizações exigem que seus fornecedores ou parceiros detenham certificações da ISO 27001, como garantia do cumprimento dos princípios de idoneidade e um nível extra de conforto quanto à Segurança da Informação. • ISO 27001 – consiste em padrão de referência Internacional para a gestão da segurança da informação (ISMS – Information Security Management System), assim como a ISO 9001 é a referência Internacional para a certificação de gestão em Qualidade.

	A implementação da norma ISO 27001 providencia um elevado compromisso com a proteção da informação, o que representa um nível considerável de conforto para as organizações que interagem com a entidade certificada. • ISO 27002 - O principal objetivo da ISO 27002 é estabelecer diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. Isso também inclui a seleção, a implementação e o gerenciamento de controles, levando em conta os ambientes de risco encontrados na empresa. • A ISO 27005 - Fornece diretrizes para o processo de gestão de riscos de segurança da informação (SI). Visa a facilitar a implementação eficaz da SI tendo como base a gestão de riscos. • ISO 27006 - Norma de requisitos para a acreditação de organizações que oferecem serviços de certificação de sistemas de gestão da SI. • ISO 27031 - Esta Norma descreve os conceitos e princípios da prontidão esperada para a tecnologia de comunicação e informação (TIC) na continuidade dos negócios e fornece uma estrutura de métodos e processos para identificar e especificar todos os aspectos (como critérios de desempenho, projeto e implementação) para fornecer esta premissa nas organizações e garantir a continuidade dos negócios. • ISO 27701 – Sistema de Gestão de Segurança Privada – é uma extensão da norma 27001, e tem como objetivo adicionar novos controles no sistema de gestão para garantir a total privacidade especificamente dos dados pessoais. **COSO** (The Comitee of Sponsoring Organizations) - é uma entidade sem fins lucrativos, dedicada à melhoria dos relatórios financeiros através da ética, efetividade dos controles internos e governança corporativa. As recomendações do COSO são tidas como referência para controles internos. Por controle interno, o COSO entende como sendo todo processo conduzido pela diretoria, conselheiros, ou outros empregados de uma companhia, no intuito de prover uma razoável garantia com relação ao cumprimento das metas de organização.

	COBIT (Objetivos de Controle de Informação e Tecnologia Relacionada) - é uma estrutura criada pela ISACA (Associação de Auditoria e Controle de Sistemas de Informação) para governança e gerenciamento de TI. Ele deve ser uma ferramenta de suporte para os gerentes e permite aproximar o fosso existente entre questões técnicas, riscos comerciais e requisitos de controle. É um modelo de controle que garante a integridade do sistema de informação mundialmente reconhecida que pode ser aplicada a qualquer organização em todas as indústrias. No geral, a COBIT garante qualidade, controle e confiabilidade dos sistemas de informação na organização. **OCTAVE ALLEGRO** - a Avaliação de Ameaças, Ativos e Vulnerabilidades Operacionalmente Críticas (OCTAVE) é uma estrutura para identificar e gerenciar riscos de segurança da informação. Ele define um método de avaliação abrangente que permite a uma organização identificar os ativos de informação que são importantes para a missão da organização, as ameaças a esses ativos e as vulnerabilidades que podem expor esses ativos às ameaças. Ao reunir os ativos de informação, ameaças e vulnerabilidades, a organização pode começar a entender quais informações estão em risco. Com esse entendimento, a organização pode projetar e implementar uma estratégia de proteção para reduzir a exposição geral ao risco de seus ativos de informação. **ITIL** - é o padrão de boas práticas para gerenciamento de serviços de tecnologia da Informação mais amplamente empregado no mundo. A ITIL é uma biblioteca que reúne as melhores práticas Gestão de Serviços de Tecnologia da Informação (TI). estruturada por processos, funções e outras habilidades requeridas para entregar e suportar serviços de TI. São as melhores práticas mais reconhecidas a nível mundial para este segmento. A ITIL pode ser utilizada por empresas de quaisquer segmentos de negócio que sejam suportadas por provedores de serviços de tecnologia, isso é, por qualquer empresa, já que dificilmente uma organização atual dispensaria a tecnologia da informação. A ITIL pode ser adaptada para empresas de qualquer porte.
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos	O entendimento e sugestão da ASSESPRO no tocante a recomendações posteriores à ocorrência de incidentes se foca em prazos para resposta e resolução do mesmo para sanar ou mitigar possíveis danos aos titulares de dados:

controladores após a comunicação do incidente de segurança?	1. Cabe a ANPD determinar prazos para que o controlador corrija/solucione o incidente (recomendamos baseados na NIST 800-6 r21 e ISSO 27001:2013 anexo A.16, neste caso prazos de até 30 dias para empresa de micro e pequeno porte, startups e MEIs e prazo de 15 dias para empresas de médio e grande porte); 2. Determinação de medidas de comunicação aos titulares conforme sugestão presente neste documento e a fiscalização de sua a execução por parte do controlador. A ANPD deverá publicar em seu sítio eletrônico, todas as ações, sanções, determinações técnicas e/ou administrativas referentes à processo oriundo de incidentes ocorridos e sob fiscalização a fim de dar transparência. Recomendados área específica no site da agência para este fim.
Sugestão ASSESPRO de questionário para comunicação de incidente de segurança (Baseado na ISO 27001:2013)	1. Descreva que tipo de incidente de segurança da informação ocorreu, relacionado a dados pessoais: 2. Existe um risco ou dano relevante aos direitos individuais dos titulares afetados em razão do incidente de segurança da informação? 3. O notificante é titular ou controlador? a) Dados do agente de tratamento: i. Nome ou razão social: ii. CPF ou CNPJ: iii. Natureza da organização: iv. Endereço: v. Cidade: vi. Estado: vii. CEP: viii. Telefone ix. E-mail 4. Dados do notificante: a) Nome: b) E-mail: c) Telefone: 5. Dados do encarregado: a) Nome: b) E-mail: c) Telefone:

	6. Descreva de forma resumida como o incidente de segurança da informação com dados pessoais ocorreu: 7. Data e hora da ocorrência do incidente: 8. Quando a organização teve ciência do incidente de segurança da informação? 9. Descreva como a organização teve ciência do incidente: 10. Se a notificação inicial do incidente não foi encaminhada no prazo sugerido de 2 dias úteis após ter tomado ciência do incidente, justifique os motivos: 11. Se o incidente não foi comunicado de forma imediata após a sua ciência, justifique os motivos da demora: Qual a natureza dos dados afetados? a) Informações contidas no AD (Active Directory); b) Informações contidas em uma caixa de e-mail corporativa; c) Informações contidas em um serviço de disco virtual (nuvem); d) Informações contidas em um diretório de rede; e) Informações contidas em um dispositivo da rede; f) Informações contidas em um sistema corporativo (ERP, CIGAM, outros); g) Banco de dados; h) Outros; Descreva: 12. Qual a categoria dos dados afetados: a) Funcionários; b) Prestadores de serviços; c) Clientes; d) Pacientes; e) Outros; Descreva se outros: 13. Quis os dados afetados? a) Nomes de usuário ou senhas de sistemas de informação. b) Origem racial ou étnica. c) Convicção religiosa. d) Opinião política. e) Filiação a sindicato. f) Filiação a organização de caráter religioso, filosófico ou político. g) Dado referente à saúde. h) Dado referente à vida sexual. i) Dado genético ou biométrico. j) Dado de comprovação de identidade oficial (Por exemplo, nº RG, CPF, CNH).

	k) Dado financeiro. l) Dado de geolocalização. m) Outros. Descreva: 14. Quais medidas de segurança, técnicas e administrativas, foram tomadas para prevenir a recorrência do incidente de segurança da informação? 15. Quais medidas de segurança, técnicas e administrativas, foram tomadas após a ciência do incidente de segurança da informação? 16. Quais medidas de segurança, técnicas e administrativas, foram ou serão adotadas para reverter ou mitigar os efeitos do prejuízo do incidente de segurança da informação aos titulares dos dados? 17. Quais as prováveis consequências do incidente de segurança da informação para os titulares afetados? 18. Os titulares foram comunicados sobre o incidente de segurança da informação com dados pessoais? Descreva: 19. Caso os titulares não tenham sido comunicados, descreva o motivo: 20. Que tipo de serviço é prestado pela organização? 21. Qual o ramo da organização? 22. O serviço prestado é terceirizado? 23. Dentro da organização existe empresas terceirizadas? 24. No caso de a empresa ser uma prestadora de serviços, a mesma terá acesso aos sistemas do contratante? a) A empresa irá trocar, enviar ou receber dados ou informações da Contratante? Se sim, onde serão armazenados? (Em caso de nuvem, especificar se está fora do Brasil) b) Tem a intenção de subcontratar empresas para a realização do serviço? c) Já fornece o mesmo serviço para outras empresas? 25. A empresa possui uma política de segurança da informação alinhada aos interesses de negócio da empresa mas que observe as melhores práticas de mercado em relação a segurança da informação, segurança cibernética e a proteção de dados pessoais? 26. A empresa possui um conjunto de normas e procedimentos que oriente todas as atividades relativas a segurança da informação, segurança cibernética e proteção de dados pessoais?

	27. Existe um processo e procedimentos estabelecidos orientando a análise crítica da política de segurança da informação e de suas normas? 28. As responsabilidades e papéis relativos a segurança da informação estão formalmente atribuídos e devidamente previstos na política de segurança da informação e suas normas? 29. A política de segurança da informação prevê segregação de funções objetivando evitar os conflitos internos e de interesses? 30. A empresa mantém contato com autoridades, grupos especiais, associações profissionais e/ou outros fóruns especializados em segurança da informação? 31. Existem procedimento e processos que garantam a segurança da informação na gerência de projetos? 32. A política encontra-se devidamente atualizada, divulgada e disponível para todos os colaboradores? 33. A empresa realiza periodicamente auditoria interna ou tem um processo de supervisão de seus processos internos objetivando zelar pela segurança da informação? 34. É feito algum tipo de auditoria por uma empresa independente, visando avaliar os controles de Segurança da Informação em seu ambiente? 35. Existe um processo periódico para acompanhamento das não conformidades identificadas durante o processo de auditoria? Os planos de ação são acompanhados? 36. A empresa realiza a análise de capacidade de infraestrutura e tecnologia? 37. A empresa dispõe de alguma certificação aceita internacionalmente que firme seu compromisso com a Segurança da Informação? (Ex.: ISO 27001, SSAE16 (SOC I, II, III), ISAE3402, PCI DSS, EU-US Safe Harbor Framework)? 38. A empresa possui controles e políticas para combater hacktivismo, espionagem, crimes cibernéticos, insiders e APT (Advanced Persistente Threats)? 39. A empresa possui iniciativas para para garantir o cumprimento com a LGPD (Lei Geral de Proteção de Dados)? Quais são? 40. Existe um departamento ou processos que busquem constantemente identificar legislação aplicável, requisitos contratuais, regulamentações aplicáveis ao negócio? 41. A empresa tem norma e/ou procedimentos claros sobre a proteção de direitos de propriedade intelectual? 42. Existe uma área ou responsável pela Segurança da Informação na empresa?

	43. A empresa o possui política, norma e/ ou procedimento para gerenciar e controlar o acesso de funcionários e terceiros aos ativos de TI (sistemas, banco de dados, entre outros)? 44. A política de acesso prevê que os acessos de administrador de sistemas sejam limitados somente ao mínimo necessário para execução das atividades? 45. A empresa permite o acesso remoto ao ambiente de operação? Em caso positivo, esses acessos são gerenciados? 46. Para os sistemas que armazenam ou processam informações/ dados fora da Contratante, existe um sistema de gerenciamento de autenticação? Qual é a parametrização de senha? (quantidade de caracteres, período de troca de senha, etc.). Existem procedimentos estabelecidos de registro e cancelamento de contas de usuários? 47. O uso de contas e credenciais privilegiadas é monitorado? 48. Os provisionamentos de privilégios são controlados e monitorados? 49. Há registros dos logs de acesso físico de entrada e saída das áreas exclusivas da empresa? A empresa deverá fornecer, em até 48 horas, registros (logs) contendo pessoa, data e hora de entrada e saída. 50. Os registros de acesso físico e o controle de credenciais de acesso são armazenados? Se sim, por quanto tempo estes registros são mantidos? 51. A empresa possui geradores de energia e "no- breaks" instalados para garantir a continuidade de energia elétrica dos ambientes críticos da operação? Se sim, são realizados testes periódicos? 52. Existem procedimentos e processos formalizados de cópias de segurança (back-up's)? 53. Existem procedimentos e processos formalizados que garantam a rastreabilidades nas operações (gestão de logs, garantia de sincronismo de relógios da rede...)? 54. Os procedimentos e processos formalizados sobre a segurança da informação estão devidamente formalizados e são conhecidos pelas equipes? 55. A empresa possui controle de softwares ou ferramenta que não pode sofrer atualização para novas versões? (Ex. Java, etc). Quais são os softwares/ferramentas? 56. Existem processos estabelecidos e procedimentos definidos para acompanhar a evolução e surgimento de novas vulnerabilidades tecnológicas? 57. A empresa executa periodicamente scans de vulnerabilidade em suas redes?

	58. A empresa tem uma metodologia estabelecida para execução de testes de invasão objetivando avaliar a maturidade de sua segurança cibernética? 59. A empresa executa regularmente testes de invasão internos e externos? Se sim, Qual a periodicidade? 60. Os sistemas que são normalmente suscetíveis a infecção de softwares maliciosos tem soluções antivírus instalados? a) Caso sim, este antivírus é controlado por um servidor central? b) Está configurado para executar atualizações automáticas? c) O scans estão configurados para executar automaticamente em períodos pré-definidos? 61. Os sistemas que não são normalmente suscetíveis a ações de softwares maliciosos tem antivírus instalados? a) Caso não tenham, e feito uma análise técnica e periódica a fim de garantir que continua não sendo necessário o uso de recursos deste tipo? 62. Há um processo formalizado de gestão para a continuidade do negócio (GCN)? 63. A empresa possui uma equipe de contingência responsável pelo processo, disponível e regularmente treinada? 64. Os planos de continuidade do negócio e treinamentos são revisados e testados regularmente? 65. Os planos de continuidade do negócio (PCN) foram determinados por uma análise de riscos e impacto? 66. Os backups dos equipamentos críticos são realizados e testados periodicamente para garantir a integridade e capacidade de restauração sendo armazenados fora das dependências da empresa?
Sugestões técnicas	O universo de associados é composto de empresas privadas nacionais possuindo os maiores acervos da experiência profissional brasileira na área da tecnologia e inovação fora da tutela do Estado e das grandes corporações privadas, atendendo a um universo de clientes de médio e grande porte, como a um incontável número de micro e pequenas empresas em todo os recantos do Brasil. Assim, podemos afirmar que 90% das empresas independentes têm sua presença assinalada na Assespro. Desta forma entendemos como necessárias algumas sugestões técnicas para a ANPD • Sugerimos que a ANPD crie uma API para interoperabilidade de modo que as empresas possam submeter e gerenciar incidentes de maneira automática evitando assim a burocracia de notificações manuais - Cada controlador poderia se registrar na ANPD para obter uma chave de API. • Recomendamos a criação de um canal de acompanhamento de adequação para micro e pequenas empresas. A ANPD criaria em seu sistema um local para as pequenas empresas e

	startups se cadastrarem e nesse portal existiria um cronograma de acompanhamento onde as empresas podem ir registrando o andamento da sua adequação e dentro de prazos diferenciados. • Sugerimos a criação de um padrão de interoperabilidade para a portabilidade de dados pessoais entre empresas (controladores de dados). Na GDPR existem iniciativas entre empresas como a https://opengdpr.org/ que visa criar padrões abertos de comunicação para facilitar a troca de dados pessoais entre agentes de tratamento de uma maneira segura e padronizada, facilitando assim o cumprimento legal. • A ASSESPRO ainda vem por meio desta tomada sugerir a classificação e categorização dos controladores de dados, visando implementar normativas e ações de fiscalização que visam organizar e otimizar os esforços desta agência no que se refere ao cumprimento da Lei Geral de Proteção de Dados. • Sugerimos ainda a adequação do normativo às seguintes legislações: ○ Lei nº 8.078, de 11 de setembro de 1990. Artigo 10, §1°. ○ Lei nº 10.406 de 10 de janeiro de 2002. Artigos 52, 186, 292 inciso §5° e 944. ○ Lei nº 12.737, de 30 de novembro de 2012. Artigos 2 e 3. ○ Lei nº 12.965, de 23 de abril de 2014. Artigos 10, 11, 18, 19, 20 e 21. ○ Lei nº 13.105, de 16 de março de 2015. Artigo 1045. ○ Lei nº 13.709, de 14 de agosto de 2018. Artigo 48 do §1° ao 3º.
Referência Bibliográficas	Banco Central do Brasil. Resolução nº 2025/1993. Disponível em: https://www.bcb.gov.br/pre/normativos/res/1993/pdf/res_2025_v6_L.pdf. Acesso em: 22/03/2021. Cetic.br. Pnad Contínua TIC 2019. Disponível em: https://cetic.br/pt/publicacao/pesquisa-sobre-o-uso-das-tecnologias-de-informacao-e-comunicacao-nos-domicilios-brasileiros-tic-domicilios-2019. Acesso em 23/03/2021. COBIT. Framework COBIT. Disponível em: https://www.fm2s.com.br/o-que-e-cobit/#:~:text=COBIT%20significa%20Objetivos%20de%20Controle,governan%C3%A7a%20e%20gerenciamento%20de%20TI. Acesso em 22/03/2021.

COSO. Framework CASO. Disponível em: https://portaldeauditoria.com.br/coso-gerenciamento-de-riscos-corporativa-estrutura-integrada/. Acesso em 23/03/2021.

IDC. Pesquisa de maturidade digital. Disponível em: https://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?UserActiveTemplate=site&infoid=54806&sid=5. Acesso em: 26/03/2021.

ISO. Família de normas ISO 27.000. Disponível em: https://www.portalgsti.com.br/2013/12/as-normas-da-familia-iso-27000.html. Acessado em: 22/03/2021.

ITIL. Framework ITIL. Disponível em: https://www.isaca.org. Acesso em: 23/03/2021.

OCTAVE. Metodologia OCTAVE ALLEGRO. Disponível em: https://resources.sei.cmu.edu/asset_files/TechnicalReport/2007_005_001_14885.pdf. Acesso em 24/03/2021.

COALIZÃO DIREITOS NA REDE

contato@direitosnarede.org.br
DIREITOSNAREDE.ORG.BR

Brasília, 30 de março de 2021

À
Autoridade Nacional de Proteção de Dados (ANPD)

Assunto: Tomada de subsídios para regulamentação do dever de comunicação de incidentes de segurança

Prezados Diretores,

A Coalizão Direitos na Rede (CDR), articulação que reúne 44 entidades da sociedade civil e organizações acadêmicas que trabalham em defesa dos direitos digitais, vem a público cumprimentar a iniciativa da ANPD em realizar a tomada de subsídios para regulamentação do dever de comunicação de incidentes de segurança, conforme seu planejamento da agenda regulatória bianual corrente. Consideramos que é uma etapa importante e que será ainda mais qualificada a partir das contribuições dos diversos atores envolvidos através do processo encerrado na última semana.

Diversas das entidades que compõem a Coalizão participaram da consulta, cada qual com sua especificidade e especialidade, a fim de ampliar ainda mais o leque de subsídios. Aproveitamos aqui para reunir, de forma consolidada, todos estes esforços, destacando a nossa disposição e disponibilidade para ampliar o diálogo com a Autoridade.

A fim de sistematização, nas próximas páginas seguem as contribuições feitas pelas seguintes organizações da CDR à consulta:

1. Associação Data Privacy Brasil de Pesquisa
2. Coding Rights
3. Instituto Brasileiro de Defesa do Consumidor - IDEC
4. Instituto de Tecnologia e Sociedade do Rio de Janeiro - ITS-Rio
5. Instituto de Pesquisa em Direito e Tecnologia do Recife – IP.Rec
6. Instituto de Referência em Internet e Sociedade – IRIS
7. Instituto Brasileiro de Defesa do Consumidor - IDEC
8. LAPIN – Laboratório de Pesquisa em Políticas Públicas e Internet

Agradecemos desde já a atenção dispensada na avaliação das contribuições da nossa articulação e reiteramos novamente nossa disposição ao diálogo contínuo e profícuo.

Nossos cumprimentos,

Coalizão Direitos na Rede

Contatos:

Secretaria Executiva:

Fabricio Solagna
E-mail: secretariaexecutiva@direitosnarede.org.br
Telefone: [redacted]

Imprensa:

Ênio Lourenço
E-mail: imprensa@direitosnarede.org.br
Telefone: [redacted]

Entidades que fazem parte da Coalizão Direitos na Rede

- Actantes
- Ação Educativa
- Artigo 19
- Associação Brasileira de Pesquisadores e Profissionais em Educomunicação – ABPEducom
- Associação de Consumidores PROTESTE
- Associação Mundial de Rádios Comunitárias – Amarc Brasil
- Associação Data Privacy Brasil de Pesquisa
- Associação Software Livre – ASL.Org
- Casa da Cultura Digital de Porto Alegre
- Casa Hacker
- Centro de Estudos da Mídia Alternativa Barão de Itararé
- Ciranda da Comunicação Compartilhada
- Coding Rights
- Colaboratório de Desenvolvimento e Participação-COLAB-USP
- Coletivo Digital
- Creative Commons Brasil
- Fórum Nacional pela Democratização da Comunicação – FNDC
- Garoa Hacker Clube
- Grupo de Pesquisa em Políticas Públicas para o Acesso a Informação/GPoPAI da USP
- Idec-Instituto Brasileiro de Defesa do Consumidor
- Instituto Alana
- Instituto Bem-Estar Brasil
- Instituto Beta: Internet & Democracia
- Instituto de Pesquisa em Direito e Tecnologia do Recife – IP.rec
- Instituto Educadigital
- Instituto Igarapé
- Instituto Iris
- Instituto Nupef
- Instituto de Tecnologia e Sociedade do Rio de Janeiro - ITS-Rio
- Instituto Telecom
- Internet Sem Fronteiras Brasil
- InternetLab – Centro de pesquisa em direito e tecnologia
- Intervozes-Coletivo Brasil de Comunicação Social
- Laboratório Cooperativista de Tecnologias Comunitárias – Coolab
- Laboratório de Políticas de Comunicação da UnB – LAPCOM/UnB
- Laboratório de Pesquisa em Políticas Públicas e Internet – LAPIN
- Rede latina-americana de estudos sobre vigilância, tecnologia e Sociedade – LAVITS
- Me Representa
- Movimento Mega
- Núcleo de Pesquisas em Direitos Fundamentais, Relações Privadas e Políticas Públicas — NUREP
- Observatório da Ética Jornalística – objETHOS
- Open Knowledge Brasil
- Transparência Brasil
- Wiki Movimento Brasil

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 ....

CODING RIGHTS
www.codingrights.org
contact@codingrights.org

Rio de Janeiro, 24 de março de 2021.

À Coordenação-Geral de Normatização
Autoridade Nacional de Proteção de Dados

Assunto: Regulamentação de notificação de incidentes de segurança (Tomada de Subsídios nº 2/2021 - reunião técnica)

O convite para contribuir com o trabalho da Coordenação-Geral de Normatização por meio da reunião técnica realizada no âmbito da tomada de subsídios nº 2/2021 teve como enfoque responder às seguintes perguntas:

a. Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?
b. Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?

Levando-se em conta o disposto no artigo 48 da Lei Geral de Proteção de dados (LGPD), que trata da obrigação do controlador de comunicar à Autoridade Nacional de Proteção de Dados (ANPD) e ao titular de dados a ocorrência de incidentes de segurança que possam acarretar em risco ou dano, a Coding Rights faz as seguintes contribuições às duas perguntas acima.

Medidas preventivas de incidentes de segurança que possam acarretar em risco ou dano para o titular dos dados

A Lei Geral de Proteção de Dados (LGPD) prevê a implementação **de medidas técnicas e organizacionais para a segurança e sigilo do processamento de dados pessoais, levando-se em consideração a natureza das informações tratadas, o estado da tecnologia e as propriedades distintivas do processamento,** tais como **escala, contexto e objetivo** *(*Art 46 § 1º*)*. Em particular, estas **medidas devem proteger os dados pessoais** de acessos não-autorizados e **de incidentes de segurança tanto acidentais quanto propositais** capazes de **comprometer a confidencialidade, a integridade e a disponibilidade dos dados** *(*CNSSI 4009 Committee on National Security Systems (CNSS) Glossary*)*.[1] As medidas técnicas

[1]https://www.serdp-estcp.org/Tools-and-Training/Installation-Energy-and-Water/Cybersecurity/Resources-Tools-and-Publications/Resources-and-Tools-Files/CNSSI-4009-Committee-on-National-Security-Systems-CNSS-Glossary

mencionadas a seguir são sugestões para assegurar a conformidade aos três pilares da segurança de dados.

(i) A **Confidencialidade** pode ser garantida por meio de:

(i.1) Pseudonimização para o tratamento de dados, que pode ser realizada através da modificação dos dados pessoais por códigos aleatórios.

(i.2) Política de controle de acesso, que garante que apenas pessoas autorizadas tenham acesso aos dados.

(i.3) Política de monitoração interna para garantir que agentes internos estejam em conformidade com as políticas de segurança.

(i.4) Descentralização do processamento dos dados para que o corrompimento de um sistema não comprometa integralmente os dados dos titulares.

(i.5) Encriptação de comunicação de dados sensíveis, de discos rígidos, de mídias de armazenamento e de dados confidenciais.

(ii) A **Integridade** pode ser garantida por meio de:

(ii.1) Segurança de transferência de dados, que pode ser garantida pela geração de certificados de "websites" e por conexões criptografadas.

(ii.2) Controle de entrada para garantir que todas as entradas feitas nos sistemas sejam registradas e para que os "logs" sejam arquivados.

(ii.3) Política de transparência e documentação do tratamento de dados.

(iii) A **Disponibilidade** pode ser garantida por meio de:

(iii.1) Instauração de mecanismos abrangentes e regulares de replicação de dados ("backups") para evitar a perda de dados.

(iii.2) Arquitetura de redes implementada de forma redundante.

(iii.3) Plano de continuidade para a rápida recuperação dos dados em casos de perda acidental ou de incidentes de segurança comprometedores.

Também é interessante o emprego regular de testes para avaliar a eficácia das medidas técnicas e institucionais adotadas, como testes de intrusão. Auditorias realizadas por autoridades externas também são aconselháveis.

É, portanto, de responsabilidade dos agentes de tratamento de dados **tomar medidas técnicas e organizacionais para PREVER e AVERIGUAR a ocorrência de incidentes de segurança envolvendo dados pessoais, REAGIR para mitigar danos e INFORMAR** rapidamente a Autoridade Nacional de Proteção de Dados e os titulares dos dados.

De acordo com posicionamento[2] do Article 29 Working Party[3], agentes de tratamento de dados devem também **ter uma avaliação preliminar de riscos de incidentes de segurança como parte da sua avaliação de impacto na proteção de dados antes de iniciadas as operações de processamento.** Este posicionamento, posteriormente incorporado na "Regulation(EU) 2018/1725" da União Europeia e esclarecido pelas diretrizes do "European Data Protection Supervisor", tem ressonância com o artigo 32 da Lei Geral de Proteção de Dados, que também deve ser regulamentado.

Obrigatoriedade de notificar a Autoridade Nacional de Proteção de Dados

O artigo 48 da LGPD assim dispõe: "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." Entendemos que **qualquer incidente de segurança que envolva comprometimento de confidencialidade, integridade ou disponibilidade de dados pessoais acarreta risco aos titulares e, como tal, a comunicação entre agentes de tratamento e a Autoridade Nacional de Proteção de Dados é imprescindível. Isso porque** é a partir da **comunicação entre agentes de tratamento e o governo brasileiro que serão traçadas estratégias efetivas de proteção de dados e que trabalhos preventivos** serão desenvolvidos para evitar novos riscos e incidentes de segurança.

A relação entre a **ocorrência de incidentes de segurança de informação e o desenvolvimento de mecanismos de defesa tanto jurídicos quanto técnicos que assegurem a proteção de informações é dialética,** isto é, a evolução de métodos capazes de assegurar a proteção de dados é o resultado do constante conflito entre forças contraditórias que podem ser classificadas em eventos sócio-digitais disruptivos e recursos defensivos. Portanto, a **notificação serve também para a capacitação adequada de profissionais de Segurança da Informação das esferas pública e privada e para o fortalecimento dos sistemas tecnológicos, responsáveis pela proteção de dados.**

Nesse sentido, **não deve haver exceções para a obrigatoriedade de notificar a Autoridade Nacional de Proteção de Dados sobre incidentes de segurança que envolvam dados**

[2] "Guidelines on Personal data breach notification under Regulation 2016/679", disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

[3] O Article 29 Working Party, cuja denominação completa é "The Working Party na Proteção de Indivíduos no Processamento de Dados Pessoais", foi um conselho consultivo formado por representantes das autoridades de proteção de dados de cada estado membro da União Européia, da Supervisão Europeia de Proteção de Dados e da Comissão Europeia.

pessoais, seja visando a **coleta de informações sobre a evolução do ecossistema de segurança da informação no país,** seja para que agentes de tratamento de dados sejam orientados para a melhor forma de atuar em coerência com a proteção de dados dos titulares. **Não deve ficar apenas a cargo do agente de tratamento de dados pessoais a avaliação sobre se o incidente de segurança causou risco ou dano ao titular do dado, pois ele é o principal interessado em negar riscos ou danos.** Normalmente incorre, portanto, em conflito de interesse nesse tipo de avaliação. **Tal avaliação deve caber à ANPD.**

Qualquer argumentação contra a notificação mandatória de qualquer tipo de incidente que seja pautada pelo argumento de um possível excesso de notificações deve ser comprovada com dados que comprovem tal temor. Aqui, cabe relembrar o **caráter educativo da ANPD, nos termos do artigo 55-J da LGPD.**

Necessidade da ANPD estabelecer uma matriz de classificação de riscos de incidentes de segurança que envolvem dados pessoais

Com base nos incidentes relatados[4], acreditamos que a ANPD deva estabelecer uma **matriz de classificação de risco de incidentes de segurança** para que esta possa estabelecer melhores diretrizes de atuação e mitigação e para deliberar pela obrigatoriedade de relatório de impacto à proteção de dados pessoais para determinados tipos de tratamento de dados, nos termos do artigo 32 da LGPD.

De acordo com sugestão do WP29:

"The GDPR does not define categories of data subjects or personal data records. However, WP29 suggests ***categories of data subjects*** *to refer to the various types of individuals whose personal data has been affected by a breach: depending on the descriptors used, this could include, amongst others,* ***children and other vulnerable groups, people with disabilities, employees or customers.*** *Similarly,* ***categories of personal data records can refer to the different types of records that the controller may process, such as health data, educational records, social care information, financial details, bank account numbers, passport numbers and so on.***
Recital 85 makes it clear that one of the purposes of notification is limiting damage to individuals. ***Accordingly, if the types of data subjects or the types of personal data indicate a risk of particular damage occurring as a result of a breach (e.g. identity theft, fraud, financial loss, threat to professional secrecy), then it is important the notification indicates these categories.*** *In this way, it is linked to the requirement of describing the likely consequences of the breach."*[5]

[4] E em proximidade com as medições do CERT.br: https://www.cert.br/stats/incidentes/
[5] Article 29 Data Protection 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

Em conformidade com essa visão, as diretrizes[6] que interpretam o artigo 34 da Regulation(EU)2018/1725 da União Europeia determinam que os riscos identificados previamente no estudo de impacto à proteção de dados (DPIA) podem servir de ponto de partida para classificação de riscos de incidentes.

Obrigatoriedade de notificar o titular de dados

Consideramos que **qualquer incidente de segurança que envolva dados pessoais pode acarretar em risco ou dano para o titular do dado**. Portanto, o titular deve ser notificado sempre, mesmo que medidas técnicas e organizacionais preventivas tenham sido adotadas pelo agente de tratamento. Desta forma, o titular se torna ciente dos riscos envolvidos no manuseio de seus dados e poderá buscar amparo legal, inclusive para avaliar pedidos de indenização por danos, quando cabível, bem como terá mais informações para avaliar se o agente de tratamento tem sido capaz de resolver incidentes e ser digno de alguma confiança. Visando respaldar a privacidade e evitar maior dano, o aviso de incidentes deve ser feito em comunicação direcionada para o titular do dado sempre que possível.

De acordo com The Working Party on the Protection of Individuals with regard to the Processing of Personal Data": *Communicating a breach to individuals* ***allows the controller to provide information on the risks*** *presented as a result of the breach and the* ***steps those individuals can take to protect themselves from its potential consequences.*** *The focus of any breach response plan should be on protecting individuals and their personal data. Consequently,* ***breach notification should be seen as a tool enhancing compliance in relation to the protection of personal data.***[7]

Diferença nos tipos de notificações enviadas para a ANPD e o titular de dados

Entendemos que, por motivos de segurança, podem existir situações extraordinárias em que a ANPD deva ser comunicada antes do titular de dados sobre incidentes de segurança que estão em andamento, inclusive para orientar o controlador sobre medidas de mitigação.

Nesse sentido, novamente, o **desenvolvimento por parte da ANPD de uma classificação de risco dos diferentes incidentes de segurança que envolvem dados pessoais** pode ser **importante também para estabelecer o fluxo e formato de comunicação de incidentes para titulares de dados.** Tal classificação seria importante inclusive para evitar um fluxo excessivo de comunicações de incidentes com os titulares de dados. Com efeito, incidentes resolvidos e que incorreram baixo risco podem ser notificados de maneira agregada, apenas a título de

[6] European Data Protection Supervisor. "Guidelines on personal data breach notification For the European Union Institutions and Bodies", disponível em: https://edps.europa.eu/sites/default/files/publication/18-12-14_edps_guidelines_data_breach_en.pdf
[7] Article 29WP Guidelines, conforme mencionado acima.

informação, por exemplo, em relatórios periódicos, enquanto incidentes graves, nos quais titulares também podem tomar medidas de mitigação, devem ter notificação em formato mais alarmante.

Portanto, entendemos que, ainda que o artigo 48 da LGPD não estabeleça diferenças entre a notificação da ANPD e do titular, em conformidade com o modelo europeu, é necessário regulamentar possível considerar dois tipos de notificação de acordo com o notificado (ANPD ou titular), cabendo, portanto, à ANPD estabelecer as diretrizes e formato de ambas.

Estímulo à denúncias (whistle blowers) em caso de incidentes não notificados

Além das notificações por parte dos agentes de tratamento de dados, em conformidade também com sugestões do Article 29 WP, acreditamos que a ANPD deva criar canais para permitir denúncias anônimas sobre incidentes de segurança que envolvam dados pessoais. Desta forma, empregados, clientes e jornalistas investigativos poderão notificar a ANPD sobre possíveis vazamentos subnotificados ou irregularidades cometidas por agentes de tratamentos de dados. Nesse caso, caberá à ANPD iniciar investigações de conformidade.

Agradecemos a oportunidade de contribuir com as duas questões propostas na tomada de subsídios nº 2/2021. Seguimos à disposição para mais contribuições e esclarecimentos.

Contribuição por

Joana Varon
Diretora executiva da Coding Rights, Fellow de Direitos Humanos e Tecnologia do Carr Center for Human Rights Policy da Harvard Kennedy School. Afiliada ao Berkman Klein Center for Internet and Society at Harvard University. Advogada, com experiência em direitos humanos e segurança digital, opera em fóruns técnicos na intersecção de debates legais e de desenvolvimento de códigos para a proteção de direitos, entre eles, iniciou o grupo de trabalho sobre Considerações de Direitos Humanos para Standards e Protocolos no Internet Engineering Task Force (IETF).

Rafaella Nunes
Estudante de Ciência da Computação da Universidade de São Paulo e consultora em cibersegurança para a Coding Rights. Realizou intercâmbio acadêmico focado em

Cybersecurity na Far Eastern Federal University (Vladivostok, Rússia) e, atualmente, é estudante de “Game Theory and Operations Research (Master program)” na Saint Petersburg State University (São Petersburgo, Rússia).

OUTROS LINKS DE REFERÊNCIA

(i) Classificação de incidentes

European Union Agency for Cybersecurity:
https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy

European Commission:
https://ec.europa.eu/information_society/newsroom/image/document/2018-30/cybersecurity_incident_taxonomy_00CD828C-F851-AFC4-0B1B416696B5F710_53646.pdf

(ii) Notificações e definição de incidente de segurança

NIST: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
NIST: https://csrc.nist.gov/glossary/term/security_categorization
CERT.br: https://www.cert.br/docs/whitepapers/notificacoes/

(iii) “Confidentiality, integrity, availability”

O NIST utiliza, explicitamente, a terminologia adotada pelo documento abaixo:

CNSSI 4009 Committee on National Security Systems (CNSS) Glossary - https://www.serdp-estcp.org/Tools-and-Training/Installation-Energy-and-Water/Cybersecurity/Resources-Tools-and-Publications/Resources-and-Tools-Files/CNSSI-4009-Committee-on-National-Security-Systems-CNSS-Glossary

"COMPUTER SECURITY: Measures and controls that ensure confidentiality, integrity, and availability of the information processed and stored by a computer."

(iv) Estatísticas do CERT.br

https://www.cert.br/stats/incidentes/

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.

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) <u>Canadá</u>** 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.

CHAMADA DE SUBSÍDIOS N º 02 - INCIDENTES DE SEGURANÇA - AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD)

Instituto de Pesquisa em Direito e Tecnologia do Recife - IP.rec

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?**

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 está 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 **garantista** à ANPD, tendo em vista a centralidade do titular dos dados na dinâmica da notificação de incidentes.

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?**

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 altíssimo.**

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, **critérios qualitativos** 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 os 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.

3. 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).

4. 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.

5. 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.

6. 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.

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?

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.

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 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.

9. Quais seriam as eventuais exceções da obrigatoriedade de informar à ANPD?

O comando legal do art. 48 da LGPD expressa 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.” 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.

10. 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.

11. 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.

12. 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.

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 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 etapas 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.

Tomada de Subsídios 2/2021 da Autoridade Nacional de Proteção de Dados

Contribuições do IRIS sobre incidentes de segurança

INSTITUTO
DE REFERÊNCIA
EM INTERNET
E SOCIEDADE

Tomada de Subsídios 2/2021 da Autoridade Nacional de Proteção de Dados

Contribuições do IRIS sobre incidentes de segurança

AUTORIA
Gustavo Ramos Rodrigues
Odelio Porto Júnior
Luiza Couto Chaves Brandão
Victor Barbieri Rodrigues Vieira

PROJETO GRÁFICO, CAPA E DIAGRAMAÇÃO
Felipe Duarte

INSTITUTO
DE REFERÊNCIA
EM INTERNET
E SOCIEDADE

APRESENTAÇÃO

Para contribuir com o maior alcance possível das contribuições oferecidas à Autoridade Nacional de Proteção de Dados (ANPD) no Brasil, o IRIS torna públicas as respostas oferecidas à Tomada de Subsídios nº 2/2021 referente a incidentes de segurança que envolvem dados pessoais. Conforme a missão do Instituto, buscamos nutrir o debate público a partir da perspectiva acadêmica e baseada em referências, tanto da experiência internacional quanto de uma perspectiva multidisciplinar.

Entendemos, por fim, que a consolidação de um sistema nacional de proteção de dados ainda apresenta muitos desafios no contexto brasileiro, mas acreditamos que a colaboração de diferentes setores, bem como a fundamentação consistente das diretrizes da ANPD guardam grande potencial para a garantia dos direitos e liberdades dos titulares de dados pessoais. O amadurecimento das discussões é bem-vindo e consideramos que esta contribuição não esgota, necessariamente, o tema. Esperamos, na verdade, que sirvam para o avanço das discussões e da representatividade de diversos setores na consolidação regulatória da proteção de dados pessoais no Brasil. A seguir, encontram-se a apresentação e as questões elaboradas pela ANPD na Tomada de Subsídios nº 2/2021 e as respectivas reflexões oferecidas pelo IRIS.

Belo Horizonte, 24 de março de 2021.

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.

TOMADA DE SUBSÍDIOS Nº 2 /2021

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

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.

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 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 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).

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.

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. 6º, 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).

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 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

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.

(RGPD) da União Europeia.[7] Na referida norma, o responsável pelo tratamento é compelido a notificar todos os incidentes, a menos 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

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>

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 conceitos se relacionam?

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 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:

> "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 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:

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.

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.

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. 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

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

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"

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 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.

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

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.

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 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.

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.

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.

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

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.

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.

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 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 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

20 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.

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]

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.

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 Ac**t. 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.

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.

INSTITUTO
DE REFERÊNCIA
EM INTERNET
E SOCIEDADE

2021 | MARÇO

CONTRIBUIÇÃO À ANPD

TOMADA DE SUBSÍDIOS Nº 2/2021 DA ANPD

INCIDENTES DE SEGURANÇA, PROCESSO DE COMUNICAÇÃO E ANÁLISE DE RISCO

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

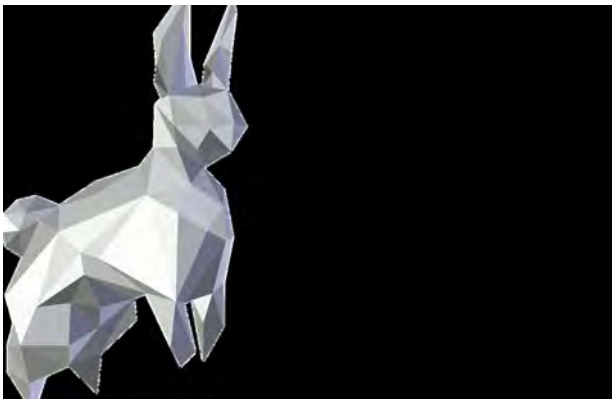
Revisão:

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] Essa contribuição foi desenvolvida pelos seguintes membros do LAPIN: [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.

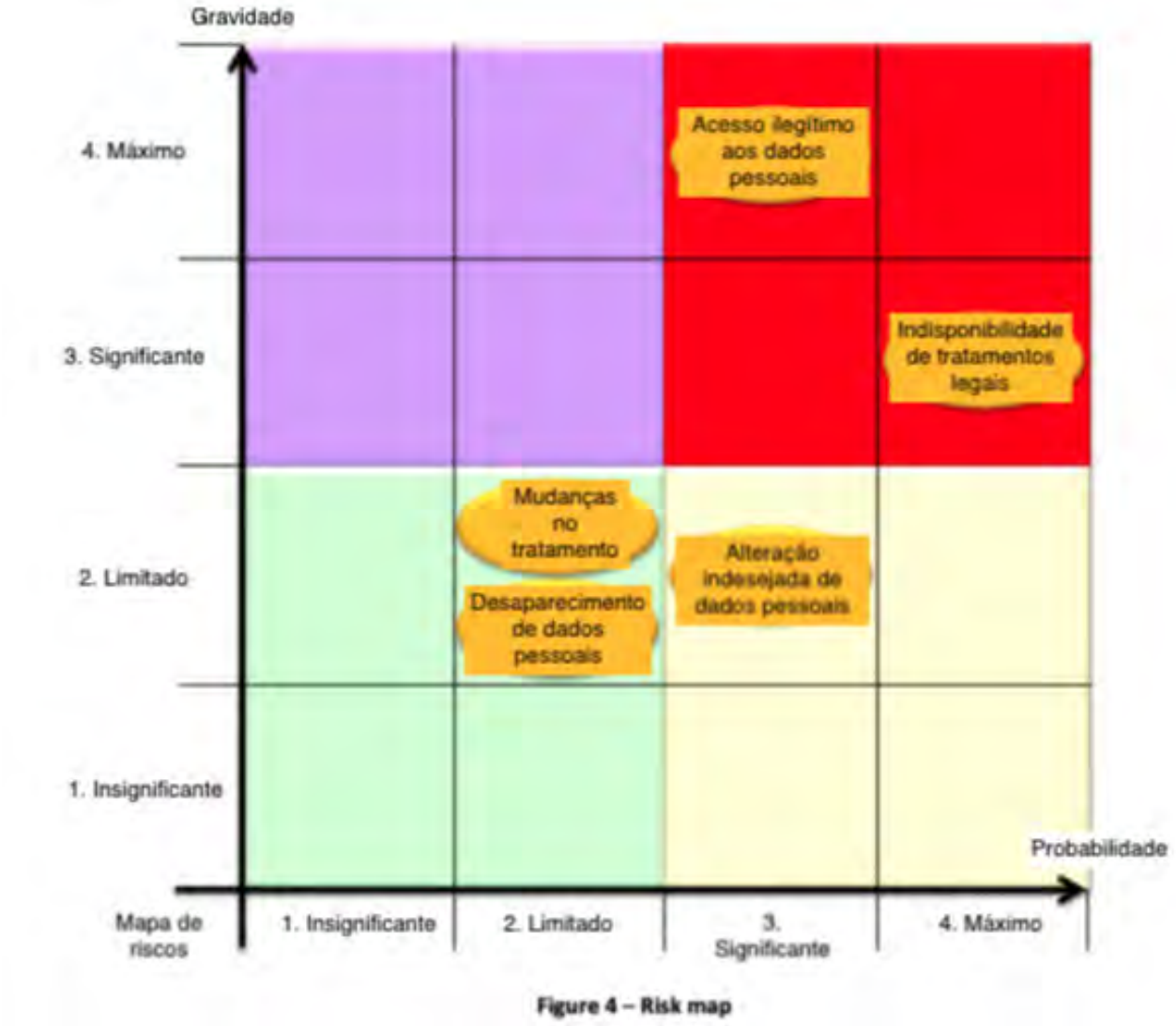


Figure 4 – Risk map

[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).

CODING RIGHTS
www.codingrights.org
contact@codingrights.org

Rio de Janeiro, 24 de março de 2021.

À Coordenação-Geral de Normatização
Autoridade Nacional de Proteção de Dados

Assunto: Regulamentação de notificação de incidentes de segurança (Tomada de Subsídios nº 2/2021 - reunião técnica)

O convite para contribuir com o trabalho da Coordenação-Geral de Normatização por meio da reunião técnica realizada no âmbito da tomada de subsídios nº 2/2021 teve como enfoque responder às seguintes perguntas:

a. Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?
b. Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?

Levando-se em conta o disposto no artigo 48 da Lei Geral de Proteção de dados (LGPD), que trata da obrigação do controlador de comunicar à Autoridade Nacional de Proteção de Dados (ANPD) e ao titular de dados a ocorrência de incidentes de segurança que possam acarretar em risco ou dano, a Coding Rights faz as seguintes contribuições às duas perguntas acima.

Medidas preventivas de incidentes de segurança que possam acarretar em risco ou dano para o titular dos dados

A Lei Geral de Proteção de Dados (LGPD) prevê a implementação **de medidas técnicas e organizacionais para a segurança e sigilo do processamento de dados pessoais, levando-se em consideração a natureza das informações tratadas, o estado da tecnologia e as propriedades distintivas do processamento,** tais como **escala, contexto e objetivo** *(*Art 46 § 1º*)*. Em particular, estas **medidas devem proteger os dados pessoais** de acessos não-autorizados e **de incidentes de segurança tanto acidentais quanto propositais** capazes de **comprometer a confidencialidade, a integridade e a disponibilidade dos dados** *(*CNSSI 4009 Committee on National Security Systems (CNSS) Glossary*)*.[1] As medidas técnicas

[1]https://www.serdp-estcp.org/Tools-and-Training/Installation-Energy-and-Water/Cybersecurity/Resources-Tools-and-Publications/Resources-and-Tools-Files/CNSSI-4009-Committee-on-National-Security-Systems-CNSS-Glossary

mencionadas a seguir são sugestões para assegurar a conformidade aos três pilares da segurança de dados.

(i) A **Confidencialidade** pode ser garantida por meio de:

(i.1) Pseudonimização para o tratamento de dados, que pode ser realizada através da modificação dos dados pessoais por códigos aleatórios.

(i.2) Política de controle de acesso, que garante que apenas pessoas autorizadas tenham acesso aos dados.

(i.3) Política de monitoração interna para garantir que agentes internos estejam em conformidade com as políticas de segurança.

(i.4) Descentralização do processamento dos dados para que o corrompimento de um sistema não comprometa integralmente os dados dos titulares.

(i.5) Encriptação de comunicação de dados sensíveis, de discos rígidos, de mídias de armazenamento e de dados confidenciais.

(ii) A **Integridade** pode ser garantida por meio de:

(ii.1) Segurança de transferência de dados, que pode ser garantida pela geração de certificados de "websites" e por conexões criptografadas.

(ii.2) Controle de entrada para garantir que todas as entradas feitas nos sistemas sejam registradas e para que os "logs" sejam arquivados.

(ii.3) Política de transparência e documentação do tratamento de dados.

(iii) A **Disponibilidade** pode ser garantida por meio de:

(iii.1) Instauração de mecanismos abrangentes e regulares de replicação de dados ("backups") para evitar a perda de dados.

(iii.2) Arquitetura de redes implementada de forma redundante.

(iii.3) Plano de continuidade para a rápida recuperação dos dados em casos de perda acidental ou de incidentes de segurança comprometedores.

Também é interessante o emprego regular de testes para avaliar a eficácia das medidas técnicas e institucionais adotadas, como testes de intrusão. Auditorias realizadas por autoridades externas também são aconselháveis.

É, portanto, de responsabilidade dos agentes de tratamento de dados **tomar medidas técnicas e organizacionais para PREVER e AVERIGUAR a ocorrência de incidentes de segurança envolvendo dados pessoais, REAGIR para mitigar danos e INFORMAR** rapidamente a Autoridade Nacional de Proteção de Dados e os titulares dos dados.

De acordo com posicionamento[2] do Article 29 Working Party[3], agentes de tratamento de dados devem também **ter uma avaliação preliminar de riscos de incidentes de segurança como parte da sua avaliação de impacto na proteção de dados antes de iniciadas as operações de processamento.** Este posicionamento, posteriormente incorporado na "Regulation(EU) 2018/1725" da União Europeia e esclarecido pelas diretrizes do "European Data Protection Supervisor", tem ressonância com o artigo 32 da Lei Geral de Proteção de Dados, que também deve ser regulamentado.

Obrigatoriedade de notificar a Autoridade Nacional de Proteção de Dados

O artigo 48 da LGPD assim dispõe: "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." Entendemos que **qualquer incidente de segurança que envolva comprometimento de confidencialidade, integridade ou disponibilidade de dados pessoais acarreta risco aos titulares e, como tal, a comunicação entre agentes de tratamento e a Autoridade Nacional de Proteção de Dados é imprescindível. Isso porque** é a partir da **comunicação entre agentes de tratamento e o governo brasileiro que serão traçadas estratégias efetivas de proteção de dados e que trabalhos preventivos** serão desenvolvidos para evitar novos riscos e incidentes de segurança.

A relação entre a **ocorrência de incidentes de segurança de informação e o desenvolvimento de mecanismos de defesa tanto jurídicos quanto técnicos que assegurem a proteção de informações é dialética,** isto é, a evolução de métodos capazes de assegurar a proteção de dados é o resultado do constante conflito entre forças contraditórias que podem ser classificadas em eventos sócio-digitais disruptivos e recursos defensivos. Portanto, a **notificação serve também para a capacitação adequada de profissionais de Segurança da Informação das esferas pública e privada e para o fortalecimento dos sistemas tecnológicos, responsáveis pela proteção de dados.**

Nesse sentido, **não deve haver exceções para a obrigatoriedade de notificar a Autoridade Nacional de Proteção de Dados sobre incidentes de segurança que envolvam dados**

[2] "Guidelines on Personal data breach notification under Regulation 2016/679", disponível em: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

[3] O Article 29 Working Party, cuja denominação completa é "The Working Party na Proteção de Indivíduos no Processamento de Dados Pessoais", foi um conselho consultivo formado por representantes das autoridades de proteção de dados de cada estado membro da União Européia, da Supervisão Europeia de Proteção de Dados e da Comissão Europeia.

pessoais, seja visando a **coleta de informações sobre a evolução do ecossistema de segurança da informação no país,** seja para que agentes de tratamento de dados sejam orientados para a melhor forma de atuar em coerência com a proteção de dados dos titulares. **Não deve ficar apenas a cargo do agente de tratamento de dados pessoais a avaliação sobre se o incidente de segurança causou risco ou dano ao titular do dado, pois ele é o principal interessado em negar riscos ou danos.** Normalmente incorre, portanto, em conflito de interesse nesse tipo de avaliação. **Tal avaliação deve caber à ANPD.**

Qualquer argumentação contra a notificação mandatória de qualquer tipo de incidente que seja pautada pelo argumento de um possível excesso de notificações deve ser comprovada com dados que comprovem tal temor. Aqui, cabe relembrar o **caráter educativo da ANPD, nos termos do artigo 55-J da LGPD.**

Necessidade da ANPD estabelecer uma matriz de classificação de riscos de incidentes de segurança que envolvem dados pessoais

Com base nos incidentes relatados[4], acreditamos que a ANPD deva estabelecer uma **matriz de classificação de risco de incidentes de segurança** para que esta possa estabelecer melhores diretrizes de atuação e mitigação e para deliberar pela obrigatoriedade de relatório de impacto à proteção de dados pessoais para determinados tipos de tratamento de dados, nos termos do artigo 32 da LGPD.

De acordo com sugestão do WP29:

"The GDPR does not define categories of data subjects or personal data records. However, WP29 suggests ***categories of data subjects*** *to refer to the various types of individuals whose personal data has been affected by a breach: depending on the descriptors used, this could include, amongst others,* ***children and other vulnerable groups, people with disabilities, employees or customers.*** *Similarly,* ***categories of personal data records can refer to the different types of records that the controller may process, such as health data, educational records, social care information, financial details, bank account numbers, passport numbers and so on.***
Recital 85 makes it clear that one of the purposes of notification is limiting damage to individuals. ***Accordingly, if the types of data subjects or the types of personal data indicate a risk of particular damage occurring as a result of a breach (e.g. identity theft, fraud, financial loss, threat to professional secrecy), then it is important the notification indicates these categories.*** *In this way, it is linked to the requirement of describing the likely consequences of the breach."*[5]

[4] E em proximidade com as medições do CERT.br: https://www.cert.br/stats/incidentes/
[5] Article 29 Data Protection 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

Em conformidade com essa visão, as diretrizes[6] que interpretam o artigo 34 da Regulation(EU)2018/1725 da União Europeia determinam que os riscos identificados previamente no estudo de impacto à proteção de dados (DPIA) podem servir de ponto de partida para classificação de riscos de incidentes.

Obrigatoriedade de notificar o titular de dados

Consideramos que **qualquer incidente de segurança que envolva dados pessoais pode acarretar em risco ou dano para o titular do dado**. Portanto, o titular deve ser notificado sempre, mesmo que medidas técnicas e organizacionais preventivas tenham sido adotadas pelo agente de tratamento. Desta forma, o titular se torna ciente dos riscos envolvidos no manuseio de seus dados e poderá buscar amparo legal, inclusive para avaliar pedidos de indenização por danos, quando cabível, bem como terá mais informações para avaliar se o agente de tratamento tem sido capaz de resolver incidentes e ser digno de alguma confiança. Visando respaldar a privacidade e evitar maior dano, o aviso de incidentes deve ser feito em comunicação direcionada para o titular do dado sempre que possível.

De acordo com The Working Party on the Protection of Individuals with regard to the Processing of Personal Data": *Communicating a breach to individuals* ***allows the controller to provide information on the risks*** *presented as a result of the breach and the* ***steps those individuals can take to protect themselves from its potential consequences.*** *The focus of any breach response plan should be on protecting individuals and their personal data. Consequently,* ***breach notification should be seen as a tool enhancing compliance in relation to the protection of personal data.***[7]

Diferença nos tipos de notificações enviadas para a ANPD e o titular de dados

Entendemos que, por motivos de segurança, podem existir situações extraordinárias em que a ANPD deva ser comunicada antes do titular de dados sobre incidentes de segurança que estão em andamento, inclusive para orientar o controlador sobre medidas de mitigação.

Nesse sentido, novamente, o **desenvolvimento por parte da ANPD de uma classificação de risco dos diferentes incidentes de segurança que envolvem dados pessoais** pode ser **importante também para estabelecer o fluxo e formato de comunicação de incidentes para titulares de dados.** Tal classificação seria importante inclusive para evitar um fluxo excessivo de comunicações de incidentes com os titulares de dados. Com efeito, incidentes resolvidos e que incorreram baixo risco podem ser notificados de maneira agregada, apenas a título de

[6] European Data Protection Supervisor. "Guidelines on personal data breach notification For the European Union Institutions and Bodies", disponível em: https://edps.europa.eu/sites/default/files/publication/18-12-14_edps_guidelines_data_breach_en.pdf
[7] Article 29WP Guidelines, conforme mencionado acima.

informação, por exemplo, em relatórios periódicos, enquanto incidentes graves, nos quais titulares também podem tomar medidas de mitigação, devem ter notificação em formato mais alarmante.

Portanto, entendemos que, ainda que o artigo 48 da LGPD não estabeleça diferenças entre a notificação da ANPD e do titular, em conformidade com o modelo europeu, é necessário regulamentar possível considerar dois tipos de notificação de acordo com o notificado (ANPD ou titular), cabendo, portanto, à ANPD estabelecer as diretrizes e formato de ambas.

Estímulo à denúncias (whistle blowers) em caso de incidentes não notificados

Além das notificações por parte dos agentes de tratamento de dados, em conformidade também com sugestões do Article 29 WP, acreditamos que a ANPD deva criar canais para permitir denúncias anônimas sobre incidentes de segurança que envolvam dados pessoais. Desta forma, empregados, clientes e jornalistas investigativos poderão notificar a ANPD sobre possíveis vazamentos subnotificados ou irregularidades cometidas por agentes de tratamentos de dados. Nesse caso, caberá à ANPD iniciar investigações de conformidade.

Agradecemos a oportunidade de contribuir com as duas questões propostas na tomada de subsídios nº 2/2021. Seguimos à disposição para mais contribuições e esclarecimentos.

Contribuição por

Joana Varon
Diretora executiva da Coding Rights, Fellow de Direitos Humanos e Tecnologia do Carr Center for Human Rights Policy da Harvard Kennedy School. Afiliada ao Berkman Klein Center for Internet and Society at Harvard University. Advogada, com experiência em direitos humanos e segurança digital, opera em fóruns técnicos na intersecção de debates legais e de desenvolvimento de códigos para a proteção de direitos, entre eles, iniciou o grupo de trabalho sobre Considerações de Direitos Humanos para Standards e Protocolos no Internet Engineering Task Force (IETF).

Rafaella Nunes
Estudante de Ciência da Computação da Universidade de São Paulo e consultora em cibersegurança para a Coding Rights. Realizou intercâmbio acadêmico focado em

Cybersecurity na Far Eastern Federal University (Vladivostok, Rússia) e, atualmente, é estudante de “Game Theory and Operations Research (Master program)” na Saint Petersburg State University (São Petersburgo, Rússia).

OUTROS LINKS DE REFERÊNCIA

(i) Classificação de incidentes

European Union Agency for Cybersecurity:
https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy

European Commission:
https://ec.europa.eu/information_society/newsroom/image/document/2018-30/cybersecurity_incident_taxonomy_00CD828C-F851-AFC4-0B1B416696B5F710_53646.pdf

(ii) Notificações e definição de incidente de segurança

NIST: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
NIST: https://csrc.nist.gov/glossary/term/security_categorization
CERT.br: https://www.cert.br/docs/whitepapers/notificacoes/

(iii) “Confidentiality, integrity, availability”

O NIST utiliza, explicitamente, a terminologia adotada pelo documento abaixo:

CNSSI 4009 Committee on National Security Systems (CNSS) Glossary - https://www.serdp-estcp.org/Tools-and-Training/Installation-Energy-and-Water/Cybersecurity/Resources-Tools-and-Publications/Resources-and-Tools-Files/CNSSI-4009-Committee-on-National-Security-Systems-CNSS-Glossary

"COMPUTER SECURITY: Measures and controls that ensure confidentiality, integrity, and availability of the information processed and stored by a computer."

(iv) Estatísticas do CERT.br

https://www.cert.br/stats/incidentes/

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: FEDERASUL – Federação das Entidades Empresariais do Rio Grande do Sul

CPF/CNPJ: 88.015.771/0001-01

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?	**O incidente pode acarretar risco ou dano relevante quando expuser publicamente dados pessoais sensíveis, dados que permitam o acesso a conteúdo controlado e restrito dos titulares (tais como senhas pessoais), especialmente dados bancários e de cartão de crédito (por exemplo), além de dados pessoais patrimoniais. Além disso, haverá risco ou dano relevante quando o incidente ocasionar adulteração, comprometimento da integridade de tais dados ou perda definitiva.** **A avaliação do risco ou dano deve considerar, especialmente, o tipo de dado pessoal que foi objeto do incidente, por quanto tempo os dados permaneceram expostos, qual a extensão da disseminação da informação, ou seja, em quais canais / plataformas / meios os dados foram veiculados. Em caso de adulteração dos dados, a ANPD deve ponderar**
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 divisão em categorias, dependendo da criticidade do risco ou dano pode ser favorável.** **Critérios para distinção dos níveis de criticidade: (i.) baixo – ocorrência de incidente de segurança que não comprometeu, nem redundou na divulgação dos dados pessoais a terceiros ou o controlador tomou providências que impediram tais efeitos; (ii.) médio – ocorrência de incidente que comprometeu ou acarretou a divulgação de dados pessoais não sensíveis e sem significativa potencialidade lesiva; (iii.) alto – ocorrência de incidente que comprometeu ou acarretou a divulgação de dados pessoais sensíveis e dados que permitam**

	o acesso a conteúdo controlado e restrito dos titulares ou que possuam potencialidade lesiva contra o titular. **Risco ou dano baixo deve ser considerado não relevante, dispensando, inclusive, a comunicação a ANPD e aos titulares.**
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	**O risco consiste em uma exposição em potencial, enquanto que o dano corresponde a uma perda ou prejuízo efetivo, que tenha efetivamente se concretizado em termos práticos.**
O que deve ser considerado na avaliação dos riscos do incidente?	**O efetivo potencial lesivo, a quantidade de titulares atingidos, a extensão da disseminação.**
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	**As condições para a ocorrência e os tipos de controles existentes, tanto para questões cibernéticas como físicas.**
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	**A informação preliminar deve ocorrer em até 96 horas após o conhecimento da ocorrência do incidente, podendo ser complementada em 15 dias úteis após a apresentação da primeira comunicação, caso não tenha sido possível apurar todas as informações até essa oportunidade.**
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?	**Incidentes de risco baixo não precisam ser comunicados. Incidentes de risco médio devem ser comunicados em até 15 dias úteis do conhecimento do incidente. Já incidentes de risco alto devem ser comunicados em até 96 horas do conhecimento.** **Além das informações constantes do art. 48, §1º, o controlador deverá informar eventuais recomendações de segurança que se façam necessárias diante do incidente detectado.**
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 aos titulares deve ser direta e da maneira mais eficaz para que o destinatário seja alcançado, podendo se dar pela via postal, e-mail, SMS, sítio eletrônico do controlador, mensagem de WhatsApp.**

à imprensa, publicação na internet etc.)?	
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	**Os incidentes de baixo risco de dano não precisariam ser informados, da mesma forma que incidentes de risco médio que tenha atingido menos de 10.000 titulares.**
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	**Os incidentes de baixo risco de dano não precisariam ser informados.**
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	**A verificação da extensão do incidentes, a postura cooperativa do controlador, a adoção de medidas técnicas que tornem os dados pessoais afetados ininteligíveis a terceiros e o potencial lesivo aos titulares (potencial efeito adverso que pode ser causado aos titulares).]**
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	**A European Union Agency of Cybersecurity estabelece critérios para avaliação e classificação da severidade dos incidentes de vazamento de dados: 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?	**Investimento em capacidade de mitigação e resposta em tempo real, baseado em estruturas para processos, tecnologias e pessoas.**

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:
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?	Até o presente momento, ainda não existe uma definição ou parâmetro exato sobre o que é um risco/dano relevante. Os riscos envolvidos no incidente serão analisados pela equipe responsável quando da avaliação do problema, considerando fatores como tipos e sensibilidade dos dados afetados, número de titulares, se há dados de crianças ou adolescentes e a gravidade das consequências. Para ser considerado como relevante, entende-se os riscos/danos que possam expor dados sensíveis, de localização e identificação, que possam levar o titular a ser vítima de cyber crimes, como o roubo de identidade ou fraudes financeiras, por exemplo. Logo após ter conhecimento de um incidente, é muito importante que o responsável pelo tratamento procure não só contê-lo, mas também avaliar o risco que dele pode resultar. Existem duas razões importantes para isso: em primeiro lugar, conhecer a probabilidade e a potencial gravidade do impacto sobre os titulares afetados, o que irá ajudar a tomar medidas eficazes para conter e dar resposta ao evento; e, em segundo lugar, irá ajudar a determinar se é exigida notificação à autoridade e, se necessário, aos 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?	Os Considerandos 75 e 76, da GDPR, sugerem que, de um modo geral, ao avaliar o risco, devem ser levados em conta a probabilidade e a gravidade do risco para os direitos e liberdades dos titulares de dados. Declaram, ainda, que o risco deve ser aferido com base numa avaliação objetiva. Assim, a graduação do risco em mais categorias é uma boa opção para distinguir uma classificação da outra, de modo que poderia-se pensar em adotar critérios como a volumetria de dados, categoria dos titulares, tipo de dados atingidos (por exemplo, se sensíveis ou não, se incluem dados financeiros ou não, se dados de menores ou não, etc), buscando deixar a identificação mais objetiva possível. Nesse sentido, riscos relevantes devem ser considerados apenas os que estiverem incluídos na faixa de médio-alto ou alto.

Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	O risco é a combinação da probabilidade de um evento vir a ocorrer e de suas consequências. É a ideia de correr perigo. Já o dano, trata-se efetivamente do prejuízo sofrido. Desse modo, o relacionamento entre ambos se dá no seguinte sentido: quando o incidente de dados envolver elevado risco ao titular, deverão ser adotadas as medidas suficientes para impedir que a projeção do perigo se concretize (seja por meio do acesso indevido, da alteração dos arquivos, etc), ao passo em que, tendo ocorrido o evento (sendo ele previsível ou não) que leve à exposição de dados pessoais do titular, o agente de tratamento deverá indicar as medidas que são necessárias para conter, mitigar e, se possível, reverter os prejuízos que podem advir daquela violação.
O que deve ser considerado na avaliação dos riscos do incidente?	A primeira ação a ser tomada no planejamento de análise de riscos é realizar uma avaliação global do cenário, no qual se observam e pontuam os perigos e riscos que determinada atividade pode gerar e indicam-se as medidas preventivas a serem aplicáveis em cada situação. A avaliação deve observar tanto a atividade realizada, quanto o ambiente que ela está inserida. Há casos em que a atividade em si não apresenta grandes riscos, mas o perigo externo pode ampliar a probabilidade. Ao realizar a avaliação, é preciso entender que a análise será feita a partir de números e dados gerais, podendo, ainda, fazer uso de equipamentos e *frameworks* que possibilitem compreender o cenário, adotando, por exemplo, um plano de resposta de incidentes. Após a avaliação, segue-se para a implementação das medidas que foram identificadas como necessárias, levando-se em conta a complexidade da empresa e os diversos setores necessários, uma vez que cada setor/processo precisará de uma medida específica. Todas as ações devem tomar como fundamentação os dados extraídos dos processos anteriores, mediante o registro da medida e a confirmação da eficácia das ações diante da prevenção dos riscos.
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	Ao comunicar a ANPD sobre os incidentes, recomenda-se que os agentes de tratamento possam 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 registros de dados pessoais. Além disso, comunicar o nome e os contatos do Encarregado da Proteção de Dados ou de outro ponto de contato onde possam ser obtidas mais informações sobre o evento. Descrever as consequências prováveis da violação de dados pessoais e 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)	Em atendimento ao princípio da transparência, a LGPD atribui ao controlador o dever de notificar os titulares de dados pessoais e a ANPD a ocorrência de um incidente de segurança "que possa acarretar risco ou dano relevante aos titulares" (art. 48, caput). A comunicação, portanto, é de incidente de segurança que já ocorreu; não de uma mera ameaça. Não se trata, também, de um incidente qualquer, mas de um incidente que possa acarretar um risco ou dano de caráter relevante. Verifica-se, portanto, que o legislador já estabeleceu um parâmetro para o referido prazo: a razoabilidade. Assim, a ANPD poderá se socorrer do direito comparado: a General Data Protection Regulation - GDPR, que define o prazo de 72 horas para a comunicação à autoridade como regra geral, podendo flexibilizar e elastecer o prazo caso seja comprovado pelo controlador que o prazo é insuficiente para reunir toda a documentação e informações necessárias. Em todo o caso, sugere-se que o prazo para envio dos documentos e informações iniciais seja de 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?	Com relação ao prazo para comunicação aos titulares, sugerimos a adoção do mesmo prazo e critérios mencionados para a comunicação à ANPD, ressalvada a utilização de linguagem que possibilite fácil compreensão por parte do titular.
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.)?	Entende-se que a melhor forma de comunicar o titular é individualizando-o quanto aos demais, permitindo que ele tenha conhecimento sobre quais dados, especificamente sobre ele, foram atingidos. Tal providência deve ser considerada especialmente nos casos em que hajam dados diversos de cada titular sendo atingidos pelo incidente. Nos demais casos, quando o tipo de dados for o mesmo, sugerimos que seja oportunizado ao controlador realizar a comunicação ao titular por meio de uma nota pública, sem o prejuízo de que, ao ser diretamente demandado por ele, esclareça de forma individualizada, quais informações foram atingidas. Além disso, o principal objetivo da comunicação aos titulares é fornecer informações específicas sobre as medidas que eles devem tomar para se protegerem, como, por exemplo, redefinição de senha. A notificação pode ser distribuída por e-mail, aviso em redes sociais, chamadas telefônicas ou qualquer outro meio de comunicação que normalmente seja usado com as partes afetadas.
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	Analisando o direito comparado, temos no art. 33, nº 1, da GDPR, a desobrigação de que o controlador realize a comunicação à autoridade quando as violações "não sejam suscetíveis de resultar num risco para os direitos e liberdades das pessoas singulares". Como exemplo, podemos deixar de notificar quando os dados pessoais já se encontram disponíveis ao público e uma

	divulgação desses dados não constitui um risco provável para o titular. Outra situação seria quando a violação não for suscetível de pôr em risco os direitos e liberdades dos titulares, ou seja, o titular também não necessitaria de ser informado quando não existir risco elevado, o que não impede que seja reavaliado pela equipe técnica do controlador e, ao constatar que há risco naquele incidente, façam a comunicação adequada.
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	Quando o agente de tratamento tiver adotado medidas técnicas e organizacionais adequadas para proteger os dados pessoais antes do incidente, em especial quando, por meio de tais medidas, os dados pessoais se tornem incompreensíveis para pessoas não autorizadas (como o caso da utilização de encriptação de ponta-a-ponta ou utilização de codificação). Ou ainda, quando após o incidente, o agente de tratamento tiver adotado as medidas adequadas para corrigir eventuais falhas deixadas no processo, e que pela utilização de tais medidas consiga comprovar que não há mais riscos elevados aos 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)	Poderão impactar na avaliação da gravidade e risco, os incidentes que: (i) possam envolver dados sensíveis, (ii) envolvam indivíduos em situação de vulnerabilidade, incluindo crianças e adolescentes, (iii) tenham potencial de ocasionar danos materiais ou morais, tais como discriminação, violação do direito à imagem e à reputação, fraudes financeiras e roubo de identidade, (iv) possuam volume significativo de dados envolvidos, (v) possuam quantitativo significativo de indivíduos afetados, (vi) demonstrem falta de boa-fé e más intenções de quem teve acesso, e (vii) facilidade de identificação dos titulares.
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	A metodologia desenvolvida pela ENISA (European Union Agency for Network and Information Security) para identificar gravidade de incidentes de segurança pode ser aplicada para verificar se o conteúdo do arquivo e as circunstâncias do incidente levam à conclusão de que este incidente poderá ou não causar risco ou dano relevante aos titulares de dados. Recommendations for a methodology of the assessment of severity of personal data breaches - ENISA. Disponível em: 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	Após a devida análise pela ANPD, ao considerar como grave o incidente, deve ser levado em consideração se, em razão do evento, os dados pessoais atingidos poderão ser objeto de tratamento desautorizados por terceiros, razão pela qual deverão ser divulgados amplamente pelos agentes de tratamento, além de determinar a utilização de medidas que possam, sempre que possível, reverter ou mitigar os efeitos ao titular.

controladores após a comunicação do incidente de segurança?	
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: Petróleo Brasileiro S.A. - PETROBRAS

CPF/CNPJ: 33.000.167/0001-01

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?	**Os critérios a serem considerados para avaliar risco ou dano podem ser: 1) categorias do dado pessoal (se incluiu ou não dado pessoal sensível); 2) facilidade de sua identificação; 3) se envolve dados pessoais de menores de idade; 4) salvaguardas adotadas pelos agentes de tratamento; 5) potencial impacto financeiro ou reputacional ao titular.** **Tais critérios devem ser objetivos e quantificáveis quanto à abrangência, quantidade e criticidade.** **Quando o titular de dado pessoal for menor de idade, o risco ou dano será relevante, em virtude de o titular ainda não ter o discernimento completo para entender as consequências do incidente.** **As salvaguardas adotadas pelo agente de tratamento devem servir de parâmetro para a definição da relevância do dano ou risco ao qual o titular de dados está submetido.** **Dependendo do número de pessoas em potencial ao qual os dados foram expostos, o risco ou dano poderá ou não ser relevante (como regra).**
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, pois a ausência de graduação dos riscos ou danos acaba por nivelar incidentes com potenciais danosos diversos, além de equiparar agentes de tratamento que atuaram de forma diferente na proteção dos dados dos titulares. Portanto, como sugestão: muito baixo, baixo, médio, alto e muito alto.** **Poderiam servir de critérios para a graduação do risco ou dano do incidente: 1) o número de titulares envolvidos, em conjunto com a classificação dos dados pessoais (exemplo: o vazamento "apenas" do nome dos alunos maiores de idade de uma turma de Universidade);**

	2) o acesso ou não dos dados por terceiros sem relação com a controladora (exemplo: supondo que determinada sociedade empresária seja a controladora dos dados pessoais, um incidente envolvendo o acesso indevido dos dados de RH por um funcionário da área de Marketing, sem que tais dados tenham sido compartilhados com terceiros fora da organização). **Assim, alternativamente, sugere-se considerar relevante apenas os riscos e danos graduados como graves.**
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	**O risco envolve um cenário mais brando que não acarreta necessariamente um prejuízo imediato ao titular diverso do próprio vazamento, como no caso dos vazamentos de login e *hash* de senha, que submetem o titular a um risco de roubo de identidade, por exemplo.** **No caso de uma senha forte, dificilmente haverá a concretização do risco. Todavia, caso o usuário tenha utilizado uma senha fraca, o risco poderá se concretizar, se não for alterada a senha ou utilizada autenticação multifatorial.** **No caso do dano, pode-se entender que o incidente já acarretou um prejuízo imediato ao titular diverso da própria violação, como no caso dos recentes vazamentos de dados pessoais ocorridos no Brasil, em que não é possível desfazer o vazamento e sujeitam o titular à abertura de contas e a contratação de serviços em seu nome. Outros exemplos são o vazamento do nome e histórico de doença, outros dados sensíveis, dados de geolocalização, antecedentes criminais, endereço residencial etc.** **Ainda acerca do dano, poderiam ser utilizadas referenciais teóricos sobre sua taxonomia, tornando-o mais objetivo e passível de categorização e análise, inclusive para o grau de impacto de uma violação. Assim, as categorias de potenciais danos seriam elementos de análise e gradação do risco.** **A diferença entre o risco e o dano, no caso dos incidentes, seria que neste último caso, o titular pouco pode fazer para mitigar os efeitos danosos. Nos exemplos dados para o dano, acima, como vazaram dados do titular que são imutáveis (CPF, nome, identidade etc.), não há como mitigar a contratação de serviços indevidamente em seu nome, por exemplo.**
O que deve ser considerado na avaliação dos riscos do incidente?	**As salvaguardas adotadas pelo agente de tratamento previamente ao incidente; o contexto do tratamento; as informações constantes no RIPD (nos casos de sua obrigatoriedade); a categoria do dado pessoal; o volume de registros; a facilidade de identificação do titular; o número de pessoas em potencial ao qual os dados foram expostos; os potenciais desdobramentos da violação em si (já existe um problema, que pode ser agravado).**

	Portanto, as considerações para a primeira pergunta são igualmente aqui aplicáveis, com a observação de que as salvaguardas são mais pertinentes para justificar o incidente do que para avaliar seu risco.
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	**Para art. 48, §1º, II, ponderar sobre esclarecer "informações" dos titulares, como quantidade de titulares afetados e quantidade de registros violados, abrangência territorial, titulares brasileiros ou estrangeiros e se há menores incluídos.**
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	**Nos casos de obrigatoriedade da notificação, sugere-se que deva ocorrer em até 3 dias da ciência do ocorrido (ou seja, da identificação do incidente), semelhante ao que é previsto no GDPR (72 horas).** **Há de se ponderar que tal prazo não seja razoável para tratar o incidente em si ou obter informações com completude suficiente. Desta forma, o prazo para reunir estas informações poderia ser maior, sem prejuízo de uma primeira notificação no prazo estabelecido.**
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?	**Não vislumbramos razão para que os titulares dos dados sejam comunicados em prazo diverso daquele previsto para a comunicação à ANPD, nos casos em que tal comunicação é obrigatória. Ponderar sobre a possibilidade de solicitar justificativa caso o prazo seja maior do que o sugerido para o item anterior.** **Além disso, entendemos que o §1º do art. 48 já prevê as informações necessárias e relevantes à comunicação 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 à imprensa, publicação na internet etc.)?	**Dever-se-ia sempre levar em consideração o contexto em que ocorreu o incidente. Caso o agente de tratamento possua as informações necessárias para a comunicação direta (e-mail, SMS, mensagem por aplicativo etc.) do incidente aos titulares afetados, ela deveria ser priorizada.** **No entanto, nem sempre será possível a comunicação direta dos titulares, caso em que deveria ser priorizada a comunicação em canal específico do agente de tratamento (exemplo: se for necessário que todos os titulares acessem um site do agente de tratamento para realizar determinada atividade, a comunicação deverá ser feita por meio do referido site).** **Apenas nos casos em que as situações anteriores não forem possíveis, poder-se-ia comunicar publicamente por meio de nota à imprensa ou outras formas com menor potencial de atingir o público ao qual se destina a comunicação.** **Contudo, sugere-se primeiramente definir em que cenários a comunicação vai seria feita, por exemplo, só em casos de riscos altos (critérios). Neste contexto, poderia seguir uma ordem de prioridade de canais (contato digital direto com os titulares e divulgação de nota na**

	imprensa/Internet), caso se entenda ser inefetivo e/ou ruim operacionalmente comunicados via telefone ou por correio. **Outra ponderação pertinente é definir ser a comunicação pública admitida ou se será obrigatória. Para alguns segmentos de negócio talvez não faça sentido sua obrigatoriedade e não haveria necessidade de a comunicação ser pública. Adicionalmente, nem todos os negócios exigem dados de contato, mas sim outros dados pessoais (portanto, não possuem forma de contatar. Nestes casos não haveria uma alternativa senão a comunicação pública.**
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	**Ponderar volume de registros.** **Adicionalmente, quando for possível a eliminação do risco ou a reversão do dano ao titular, a ANPD não precisaria de ser informada** **Por fim, após definição de critério de risco, incidentes de impacto baixo, muito baixo e talvez médio não precisassem ser comunicados.**
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	**Sempre que não houver acesso dos dados pessoais por terceiros, isto é, sempre que o incidente com os dados pessoais se restringir ao próprio ambiente do agente de tratamento (exemplo: no caso de uma sociedade empresária, o acesso indevido dos dados pessoais por outra sociedade empresária do mesmo grupo), entendemos que a comunicação aos titulares não deve ser obrigatória.** **Por fim, após definição de critério de risco, incidentes de impacto baixo, muito baixo e talvez médio não precisassem ser comunicados.**
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	**A capacidade de identificação do titular; as salvaguardas adotadas pelo agente de tratamento previamente ao incidente; as medidas mitigatórias adotadas pelo agente de tratamento após o incidente; o número de pessoas em potencial ao qual os dados foram expostos.**
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	Norma Complementar nº 05/IN01/DSIC/GSIPR**, e seu Anexo, disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal. (Publicada no DOU Nº 156, de 17 Ago 2009 - Seção 1).** Norma Complementar nº 08/IN01/DSIC/GSIPR**, estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal. (Publicada no DOU Nº 162, de 24 Ago 2010 - Seção 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?	**Depende da análise casuística da violação ocorrida.** **A título de contribuição, ponderar sobre melhorias dos controles (são diversos, a família ISO 27000 tem bom conjunto) e sobre melhoria do RIPD, se nele não foram detectados de antemão os riscos.**
SUGESTÃO DE NORMATIVO, SE HOUVER	
ISO 27035 e normas complementares da IN01 da GSI.	

CONTRIBUIÇÕES DO ESCRITÓRIO PRADO VIDIGAL ADVOGADOS À TOMADA DE SUBSÍDIOS Nº 2/2021 SOLICITADA PELA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD)

Dados da instituição:

PRADO E VIDIGAL SOCIEDADE DE ADVOGADOS
CNPJ: 38.491.410/0001-55

Autores:

PAULO VIDIGAL
LUIS FERNANDO PRADO

PRADO VIDIGAL
Privacidade & Digital

BREVES CONSIDERAÇÕES INICIAIS

No contexto de crescente digitalização de organizações, notória ocorrência de incidentes ao redor do mundo (incluindo significativos acontecimentos no Brasil) e oportuna valorização do tema da privacidade por parte dos titulares de dados, o tema objeto da presente tomada de subsídios assume extrema relevância.

Se de um lado há, evidentemente, preocupação com a segurança dos dados pessoais e salvaguarda de direitos de titulares, por outro há a necessidade de se garantir um mínimo de segurança jurídica aos agentes de tratamento de dados pessoais.

Nesse sentido, ao nosso ver, a regulamentação a ser editada pela ANPD deve trazer clareza, ao menos, quanto (a) às noções de risco e dano relevante que ensejariam o dever de comunicação de que trata o artigo 48; e (b) ao que configuraria "prazo razoável" para notificação à ANPD e aos titulares envolvidos.

Em vista disso, prestamos nossas homenagens em relação à presente iniciativa lançada pela ANPD e esperamos que nossas contribuições a seguir possam ser oportunas para a regulamentação do tema. Evidentemente, não se pretendeu exaurir os temas abordados ou produzir provas de conhecimento ou experiência dos signatários deste, mas – sim – colacionar entendimentos, formulações e materiais que possam servir de fonte para o trabalho de construção que será desenvolvido pela autoridade, a serem somados a outros que serão trazidos pelos demais colaboradores.

No mais, perceberá o leitor reiteradas referências à legislação dos EUA, o que, a primeira vista, poderia causar estranheza, considerando a ausência de tradição regulatória deste país em termos de privacidade e proteção de dados pessoais. No entanto, os EUA, embora não contem com normatização completa, rigorosa e abrangente sobre o direito em referência, regulam intensamente, por meio de leis setoriais e dos estados, o tema da notificação de incidentes, gerando, assim, importantes referências ao debate brasileiro sobre o tema.

Por fim, colocamo-nos à disposição para os desdobramentos desta contribuição, certos de que a participação da sociedade na construção da regulamentação é o melhor caminho para termos normatizações equilibradas, eficazes e plenamente exequíveis.

Cordialmente,

Prado Vidigal Advogados

ÍNDICE

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 levantamento de legislações mundo afora, percebe-se que se revela árdua a tarefa de se estabelecer conceituação fechada do que seria "risco" ou "dano" a titulares de dados. As leis ou autoridades que o pretendem fazer, normalmente acabam por adotar via exemplificativa, em que são expostas hipóteses não excludentes de "risco" e "dano", para que não se venha a afastar, de pronto, a obrigação de comunicação de alguma situação crítica, que possa resultar em modalidades de "risco" ou "dano" não imaginados quando da concepção dos conceitos regulatórios, o que poderia ocasionar decréscimo de proteção da lei.

Ocorre que, mesmo não sendo possível encontrar rol taxativo de situações, a nosso ver, é necessário trazer algum nível de previsibilidade e objetividade para a análise do impacto de incidentes que envolvam dados pessoais, em especial para que esta possa ser reproduzida de forma sistemática e consistente pelos agentes de tratamento de dados pessoais, pois é crucial que se tenham parâmetros mínimos de segurança jurídica para a tomada da deliciada decisão de comunicação da ANPD e titulares de dados.

Para tanto, observa-se que, de modo geral, os seguintes critérios são amplamente admitidos como fatores de risco a serem considerados:

NATUREZA DOS DADOS	Dados sensíveis são fatores de acréscimo de risco para autoridades europeias, em metodologia desenvolvida pela entidade europeia ENISA , no âmbito da legislação australiana, canadense e de Singapura.
INTENÇÃO MALICIOSA	A intenção maliciosa de terceiros que potencialmente tenham acessado os dados afetados figura como critério de risco para autoridades europeias, em metodologia desenvolvida pela entidade europeia ENISA, no âmbito da legislação australiana e canadense.
MEDIDAS DE SEGURANÇA	A existência de medidas de segurança que mitiguem o potencial de mau uso dos dados por terceiro funciona como critério atenuante de risco para autoridades europeias, o que também ocorre no âmbito da legislação australiana e canadense.
NÚMERO DE TITULARES	O número de titulares afetados surge como critério relevante de risco, sendo que legislações dos Estados Unidos (em alguns casos) e Singapura excluem a obrigação de comunicação caso o incidente não tenha afetado ao menos 500 indivíduos. No Japão o limite é de 1.000 titulares. Inclusive, algumas legislações (como no norte-americano HIPPA) impõem apenas dever de documentação e reporte anual nesses casos em que o volume de titulares afetados é menos significativo.

A nosso ver, à luz dos critérios expostos e sem prejuízos de outros, a regulamentação da ANPD deveria se inspirar na metodologia desenvolvida pela instituição europeia, ENISA, a qual, na medida do possível, torna a análise de impactos incidentes objetiva, traçando critérios para obtenção de score matemático que aponte a criticidade do incidente.

O passo a passo para a avaliação do incidente, conforme a referida entidade, é o seguinte:

I. ANÁLISE DO CONTEXTO (DPC)

1. Identificam-se os dados envolvidos no incidente;

2. Classificam-se os dados em simples, comportamentais, financeiros e sensíveis, o que resulta em *score* base;

3. Verificam-se fatores agravantes ou atenuantes;

4. Aplicam-se os fatores encontrados no passo 3 e, assim, aumenta-se ou diminui-se o *score* de risco base.

II. AVALIAÇÃO DA FACILIDADE DE IDENTIFICAÇÃO (EI)

5. Define-se o grau de potencialidade de identificação do titular, entre irrelevante, limitada, significativa e máxima.

III. APURAÇÃO DAS CIRCUNSTÂNCIAS (CB)

6. Apuram-se as circunstâncias do incidente, conforme atributos de segurança de informação afetados (confidencialidade, integridade e disponibilidade), bem como se trata-se de incidente malicioso ou não-malicioso, a exemplo de acidentes, erros humanos ou falhas de tecnologia.

Após a atribuição de pontuação individual para cada um desses três passos, conforme a metodologia proposta pela ENISA, aplica-se a seguinte fórmula para se chegar ao *score* final do risco do incidente:

SE (*score* final) = DPC (contexto) x EI (facilidade de identificação) + Circunstâncias (CB)

Para se chegar à avaliação final do risco, aplica-se a matriz abaixo:

SE < 2	BAIXO
2 ≤ SE < 3	MÉDIO
3 ≤ SE < 4	ALTO
4 ≤ SE	MUITO ALTO

REFERÊNCIAS

O GDPR, em sua Consideranda 85, elucida os eventuais danos decorrentes de incidentes de segurança envolvendo dados pessoais, quais sejam: danos físicos, materiais ou imateriais, como perda de controle sobre os dados pessoais ou limitações a direitos, discriminação, fraude de identidade, perda financeira, reversão não autorizada de pseudonimização, danos à reputação, perda de confidencialidade de dados protegidos por sigilo profissional ou qualquer desvantagem econômica ou social significativa. Acessível em: https://gdpr-info.eu/recitals/no-85/.

O Working Party 29 (órgão consultivo europeu que deu lugar ao European Data Protection Board) recomenda a avaliação dos seguintes critérios: (i) tipo de incidente: (ii) natureza e volume dos dados pessoais afetados: (iii) potencial de identificação dos titulares afetados; (iv) gravidade das consequências para os titulares; (v) titulares envolvidos; (vi) natureza da atividade do controlador; e (vii) número de titulares afetados. Ver: Working Party 29. Guidelines on Personal data breach notification under Regulation 2016/679, p. 25/26. Acessível em https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052. Acesso em 23.03.2021.

A European Union Agency for Network and Information Security (ENISA) desenvolveu reconhecida metodologia para análise de impacto de incidentes de segurança envolvendo dados pessoais que considera os seguintes elementos: (I) contexto do tratamento de dados e tipos de dados envolvidos; (II) possibilidade de identificação do titular a partir do incidente; e (III) circunstâncias do incidente. Disponível em https://www.enisa.europa.eu/publications/dbn-severity. Acesso em 22.03.2021.

Conforme a lei australiana de proteção de dados, devem ser notificados incidentes de segurança que importem em "sérios danos" aos titulares envolvidos, os quais incluem danos físicos, psicológicos, emocionais, financeiros e reputacionais. O risco de danos dessa natureza deve ser avaliado de maneira holística, a partir de variados critérios delineados pela autoridade competente. Disponível em: https://www.oaic.gov.au/privacy/guidance-and-advice/data-breach-preparation-and-response/part-4-notifiable-data-breach-ndb-scheme/#identifying-eligible-data-breaches. Acesso em 22.03.2021.

No caso da legislação canadense PIPEDA, incidentes de segurança devem ser comunicados em caso de risco real ou dano significativo aos titulares envolvidos. Danos significativos incluem danos corporais, humilhação, danos à reputação ou relacionamentos, perda de emprego, negócios ou oportunidades profissionais, perda financeira, fraude de identidade, prejuízos em registro de créditos ou danos ligados à propriedade. Os critérios a serem analisados são (i) sensibilidade dos dados envolvidos; e (ii) probabilidade de tais dados estarem ou vir a serem mal utilizados. 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_6. Acesso em 22.03.2021.

Boa parte das leis esparsas norte-americanas trabalham com noções subjetivas de risco (a serem avaliadas pelas organizações envolvidas ou em conjunto com autoridades), porém admitem como critério para obrigação de notificação de incidentes o volume de titulares afetados, sendo que se inferior a 500 indivíduos afasta-se tal dever. Disponível em: https://www.dlapiperdataprotection.com/index.html?t=breach-notification&c=US&c2=. Acesso em 22.03.2021.

A legislação de Singapura define que é obrigatória a notificação de incidentes que ocasionem "danos significativos", os quais incluem "danos significativos", que incluem danos físicos, psicológicos, emocionais, econômicos, financeiros e reputacionais, não excluídos eventuais outros. A fim de simplificar essa tarefa, a legislação traz um cardápio extenso de dados cuja combinação em incidente demanda a notificação (denominados "prescribed data"). Além disso, a lei prevê que incidentes que afetem 500 ou mais indivíduos necessariamente precisam ser comunicados. Disponível em: https://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 22.03.2021.

Levantamento internacional, sobre critérios para *data breach notification* disponível em: https://www.dlapiperdataprotection.com/index.html?t=breach-notification&c=JP&c2=. Acesso em 23.03.2021.

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?

Tomando por base a recomendação realizada no item anterior, tem-se que seria salutar definir metodologia que pudesse resultar em *score* de risco segmentado em níveis. Por mais que a LGPD não tenha trazido expressamente gradações de risco ao tratar da questão da comunicação de incidentes, se mostra importante, para fins de governança, a existência de orientação oficial que subdivida o risco em diferentes níveis, já que, a depender do grau de risco envolvido, as respostas ao incidente se tornam mais ou menos complexas, de acordo com os planos de respostas existentes nas organizações.

Sem prejuízo das definições próprias da ANPD, sopesados os critérios que entender cabíveis em metodologia a ser desenvolvida, sugere-se que os níveis finais sejam próximos daqueles definidos pela ENISA na metodologia ora recomendada. Nesse sentido, poderá ser entendido que incidentes de risco baixo, de acordo com os parâmetros de classificação a seguir expostos, não caracterizam "risco ou dano relevante" e, portanto, não ensejam dever legal expresso de comunicação (nem à ANPD, nem aos titulares):

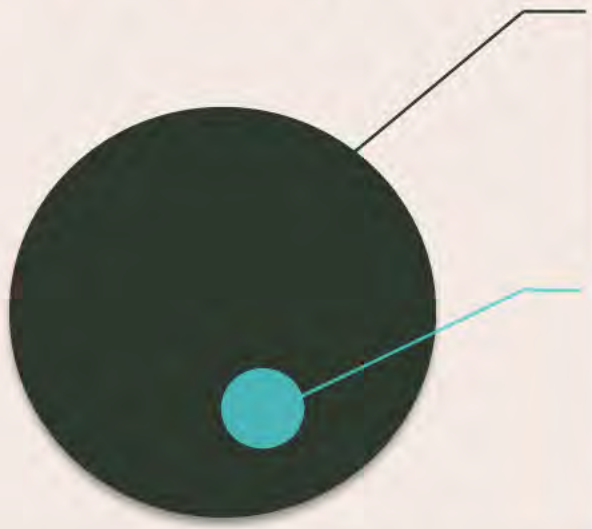
"RISCO NÃO RELEVANTE" — Não se aplica dever de comunicação do art. 48 da LGPD	**BAIXO**	Os titulares não serão afetados ou poderão sofrer apenas alguns inconvenientes, os quais poderão ser superados sem muitas dificuldades (ex.: pequenos desperdícios de tempo, aborrecimentos, irritações).
"RISCO RELEVANTE" — Aplica-se dever de comunicação do art. 48 da LGPD	**MÉDIO**	Os titulares poderão sofrer inconvenientes significativos, os quais poderão ser superados ainda que com certa dificuldade (ex.: custos extras, negação de serviço temporária, medo, stress, desconfortos físicos).
	ALTO	Os titulares poderão sofrer consequências significativas, os quais poderão ser superadas, mas com sérias dificuldades (ex.: perdas financeiras, inclusão em listas restritivas, danos a propriedades, perda de emprego, piora em estado de saúde etc.)
	MUITO ALTO	Os titulares poderão sofrer consequências significativas ou até irreversíveis, as quais não poderão ser superadas (ex.: dificuldades financeiras como dívidas substanciais, incapacidade de trabalho, doenças físicas ou psicológicas de longo prazo, morte etc.)

COMO DISTINGUIR O RISCO AO TITULAR DO DANO AO TITULAR? COMO ESSES CONCEITOS SE RELACIONAM?

No contexto do que se colocou anteriormente, entende-se que embora a lei mencione risco e dano, tais conceitos naturalmente se confundem quando da análise de impacto de incidentes. É que, em nosso entender, para a lógica da legislação (principalmente à luz do princípio da prevenção, disposto no artigo 6º, VIII), basta que se afigure risco relevante, para que o agente de tratamento tenha de tomar as medidas dispostas na lei (dentre elas, a comunicação), não havendo que aguardar que eventual dano de fato ocorra (sendo este nada mais do que a materialização do risco).

De certo modo, pode-se dizer que a LGPD acolheu a concepção moderna de responsabilidade preventiva (responsabilidade civil independente do dano), de modo que o mero risco (se relevante), engloba a possibilidade de dano e, como tal, é suficiente para disparar o dever de comunicação, assim como as demais obrigações legais da LGPD. Evidentemente que a apuração do dano será relevante, em momento posterior, se e quando vierem a se aplicar penalidades ou for determinado o ressarcimento de titulares de dados em decorrência do incidente, mas nesse momento anterior – de análise do dever de comunicação – risco e dano devem ser mensurados a partir de uma mesma régua, tendo por protagonista o risco (já que o dano muitas vezes não será conhecido desde logo).

De maneira ilustrativa, nossa sugestão de interpretação se resume ao seguinte:



RISCO

O risco é mais abrangente que o dano. Se houver dano, é porque o risco já existia em momento anterior.

DANO

O potencial danoso está envolvido pelo risco. Uma vez concretizado o risco, uma de suas consequências poderá ser o dano.

O QUE DEVE SER CONSIDERADO NA AVALIAÇÃO DOS RISCOS DO INCIDENTE?

Questão respondida no primeiro tópico da presente contribuição.

QUAIS INFORMAÇÕES OS CONTROLADORES DEVEM NOTIFICAR À ANPD, ALÉM DAQUELAS JÁ LISTADAS NO §1º DO ART. 48?

Entendemos que as informações contidas do artigo 48 são suficientes para atender aos propósitos da legislação. Além disso, ressalvamos que a atividade da ANPD não deve extrapolar seu poder regulamentar, o que, nesse ponto, traz a impossibilidade de se impor, via regulamentação, nova obrigação aos controladores para além daquilo já disposto na LGPD (sob pena de violação do princípio constitucional da legalidade).

QUAL O PRAZO RAZOÁVEL PARA QUE CONTROLADORES INFORMEM A ANPD SOBRE O INCIDENTE DE SEGURANÇA? (ART. 48, §1º)

Entendemos que o prazo razoável tem de ser disciplinado à luz das experiências internacionais. Assim, trazemos abaixo referências que podem pautar essa definição:

72 hrs (GDPR)

30 dias para avaliar gravidade + notificar

30 dias para avaliar gravidade + 3 dias corridos para notificar

5 dias úteis

Sem demora indevida (PIPEDA e PIPA Alberta)

Legislação esparsa, com prazos variados. Vide materiais inseridos nas referências.

Ainda sobre o prazo para se comunicar a ANPD, perceba-se que o exemplo do GDPR, nesse ponto, mostra-se excessivamente rigoroso, ainda mais se consideramos a novidade do tema no Brasil. Há de se levar em conta, desde logo, que prazo demasiadamente exíguo compromete a necessária avaliação de risco do incidente, que, a nosso ver, consiste na etapa mais vital do plano de respostas da organização, vez que guiará todas as ações dali em diante, inclusive e principalmente em termos de adequada mitigação de risco aos titulares.

Um prazo tão exíguo como vimos nos exemplos vindo da Europa em um país com dimensão continental como o Brasil pode, inclusive, trazer entraves operacionais para a própria ANPD, vez que o prazo reduzido se mostra como convite para que mera suspeitas sejam de pronto notificadas, o que, considerando a quantidade de controladores de dados no país, potencialmente geraria número de comunicações à ANPD impossível de se gerenciar/processar. Vale lembrar que lá na EU, há, pelo menos, uma autoridade nacional de proteção de dados para cada país-membro, sendo que, no caso de empresas como atuação em vários países da UE, deve a empresa contatar, se o caso, apenas sua "autoridade mãe", o que certamente alivia a carga de trabalho para as autoridades locais.

No Brasil, embora não se desconheça disposição do artigo 18, § 1º do Decreto 9.936/2019, que regulamenta a Lei do Cadastro Positivo e estabelece o prazo de 2 (dois) dias úteis para que o gestor de banco de dados realize comunicação de incidentes de risco ou prejuízo relevante aos cadastrados, há de se considerar a necessidade de, como regra geral, estabelecer prazo razoavelmente superior a 2 dias ou 72 horas pra as comunicações à ANPD, sob pena de se criar sistema de comunicação e resposta a incidentes ineficiente e excessivamente moroso por excesso de volume de comunicações. No mais, a nosso ver, a pretexto de se viabilizar uma rápida comunicação com a ANPD, não se deve prejudicar o correto e adequado desenvolvimento das avaliações de risco, ou seja, não devemos incentivar os controladores de dados a pularem etapas e motivar o envio de comunicações incompletas ou incabíveis, que mais prejudicarão do que auxiliarão os trabalhos da ANPD. Registra-se, portanto, nossa visão crítica em relação à estratégia regulatória de simplesmente importar aquele prazo previsto na Europa, pois, especificamente quanto às comunicações de incidentes, as realidades fática, cultural e regulatória são bastante distintas.

REFERÊNCIAS

Art. 33, GDPR. Disponível em: https://gdpr-info.eu/art-33-gdpr/. Acesso em 23.03.2021.
Personal Data Security Breach Code of Practice, disponível em: https://www.ics.ie/news/view/255. Acesso em 23.03.2021.
Conforme informação contida de levantamento internacional, disponível em https://www.dlapiperdataprotection.com/index.html?t=breach-notification&c=AU&c2=. Acesso em 23.03.2021.
Informações da autoridade de proteção de dados de Singapura: https://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 22.03.2021.
THOMAS. Lisa, M. A Practical Guide to Handling Data Breach Notifications Worldwide, 2019, p. 205/206. FOLEY. State Data Breach Notificaiton Laws, disponível em: https://www.foley.com/en/-/media/18d91d3de9b94e98b526efa2e27c6faa.ashx. Acesso em 23.03.2021.

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 para notificação de titulares, nos parece prudente recomendar que esta se opere em prazo superior àquele definido para notificação para a ANPD. Isso porque o ato de notificar o titular demandaria ainda maior nível de assertividade de informações do que o de comunicação do regulador. Não nos parece que faça sentido impor, desde logo, exíguo prazo para notificação de titulares, de tal sorte que os controladores teriam curto tempo para reunir informações precisas sobre o ocorrido, sob pena dos titulares serem impactados com informações confusas, inconclusivas ou até equivocadas. Ademais, nos parece que o cenário ideal aponta para o alinhamento da comunicação de titulares entre controlador e regulador, o que apenas seria factível caso o prazo ora estabelecido fosse superior àquele para comunicação da ANPD.

A esse respeito, lembra-se que o GDPR embora estabeleça prazo radicalmente curto (de apenas 72h) para comunicação do incidente à autoridade competente (o qual, como expusemos, não deveria ser simplesmente importado ao ordenamento jurídico brasileiro sem as devidas reflexões e ponderações), ao tratar do prazo para comunicação do incidente aos titulares não chega a estabelecer prazo fixo, fazendo constar que, quando for o caso, tal comunicação deve ocorrer sem demora indevida. Lembre-se que, no direito europeu, não é qualquer incidente de risco ou dano relevante que deve ser notificado aos titulares, mas somente aqueles de risco elevado, o que, lamentavelmente, não foi reproduzido na LGPD sendo este um fato que sujeita o cenário brasileiro a conviver com a fadiga da notificação e até mesmo possível banalização do instituto, o que seria temerário do ponto de vista da tutela aos titulares. De qualquer forma, o próprio GDPR se utilizou do racional regulatório ora exposto, no sentido de separar os prazos da notificação à autoridade e comunicação aos titulares, de modo que, pelos motivos expostos neste tópico e no anterior, defendemos que o prazo para comunicação aos titulares seja, no mínimo, 15 dias superior àquele que será estabelecido para notificação do incidente à ANPD.

Quanto ao conteúdo da comunicação, entendemos que as seguintes informações do artigo 48, §1º, não fazem sentido de serem comunicadas aos titulares:

Informação do art. 48, §1º que não deveriam constar da comunicação aos titulares	Justificativa
II - as informações sobre os titulares envolvidos;	Sob pena de que a própria comunicação sobre o incidente exponha os titulares a risco adicional, entendemos que não devem os titulares destinatários da comunicação receber qualquer informação sobre os demais envolvidos.
III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;	De modo a se priorizar a clareza na transmissão de informações aos titulares (não técnicos no assunto), não devem constar em tais comunicações informações técnicas e de segurança utilizadas para a proteção de dados.

A título de referência, trazemos abaixo quadro que explicita os elementos presentes em legislações europeia (GDPR) e norte-americanas (considerando o compilado de exigências das legislações esparsas e já com as devidas adaptações para o cenário brasileiro). Perceba-se que em nenhum dos cenários de direito comparado ora examinados constam as informações do artigo 48, §1º, da LGPD que apontamos anteriormente como não pertinentes aos titulares:

Em linguagem clara e acessível:

(a) nome e contato do Encarregado ou outro ponto de contato que poderá prestar maiores informações;

(b) descrição das possíveis consequências do incidente; e

(c) descrição das medidas tomadas pelo controlador para mitigar os efeitos do incidente.

(a) descrição do incidente;

(b) detalhamento dos dados comprometidos;

(c) potenciais consequências do incidente;

(d) resultado de investigações e mitigações realizadas;

(e) meios para que o titular possa se proteger;

(f) informações de contato da autoridade;

(g) informações de contato do controlador.

REFERÊNCIAS

Ver artigos 33 e 34 do GDPR. Acessíveis em: https://gdpr-info.eu/art-33-gdpr/. Acesso em 23.03.2021.
THOMAS. Lisa, M. A Practical Guide to Handling Data Breach Notifications Worldwide, 2019, p. 171

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.)?

Entende-se que deve ser admitida comunicação de maneira ampla em qualquer situação em que o controlador de dados não tenha relação direta com o titular, ou, ainda que o tenha, não disponha de informações de contato individualizadas, sem excluir aquelas situações em que a comunicação individualizada imporia esforços desproporcionais. Tal racional segue a lógica disposta no artigo 34, 3, c, do GDPR: "A comunicação ao titular dos dados a que se refere o n.o 1 não é exigida se for preenchida uma das seguintes condições: 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".

Quanto aos meios de comunicação direta, quando for o caso de sua aplicação, considerando que a LGPD não trouxe qualquer restrição nesse sentido, entendemos que se deve admitir a possibilidade de utilização de qualquer meio que possa gerar prova válida do ato.

QUAIS SERIAM AS EVENTUAIS EXCEÇÕES DA OBRIGATORIEDADE DE INFORMAR A ANPD?

Em nosso entender, deveriam ser consideradas as seguintes exceções, sem prejuízo de outras:

MERAS SUSPEITAS

Ao nosso ver, as organizações não deveriam estar obrigadas ao dever de comunicação ante a mera "suspeita" de ocorrência de incidentes, mas somente após a efetiva confirmação. Isso não é dizer, é claro, que as organizações podem agir com desídia e falhar em seu dever de investigação, com a devida agilidade e diligência, de suspeitas de incidentes.

Na Europa, opinião do Working Party 29 expõe que o controlador se torna ciente quando adquire razoável grau de certeza quanto à ocorrência do incidente que comprometeu dados pessoais e, mais, que em alguns casos pode-se levar algum tempo até que seja possível estabelecer que o incidente de fato ocorreu, sendo que se deve dar ênfase à pronta reação e investigação da suspeita.

APLICAÇÃO DE MEDIDAS TÉCNICAS

Entendemos que a aplicação de medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis desconfigura o incidente de segurança para fins de LGPD, pois afasta risco ou dano relevante.

Na Europa, o Working Party 29 é da opinião de que se os dados pessoais foram tornados ininteligíveis para terceiros não-autorizados e havendo cópias ou backups, incidente que afete a confidencialidade de dados criptografados não precisaria ser comunicado à autoridade competente, já que é improvável de significar risco aos direitos e liberdades dos titulares de dados.

MANUTENÇÃO DA CONFIDENCIALIDADE

Defendemos a não-obrigatoriedade de comunicação à ANPD no caso em que eventual acesso não autorizado se deu, de maneira acidental, por pessoa ou organização com quem o agente de tratamento tem relação, desde que vigore dever de confidencialidade e não haja mau uso dos dados indevidamente acessados.

Entendemos que se o caso descrito se trata de incidente contido, que pode ser revertido pelo agente de tratamento sem que venha a ensejar consequências aos titulares de dados. Exceção similar, conhecida como "good faith exception", existe em diversas leis esparsas norte-americanas. Nesses casos, o incidente deverá ser mitigado prontamente e devidamente documentado. Ainda, caso o agente de tratamento não venha, em tempo razoável, a obter do terceiro as devidas comprovações que atestem a confirmação da mitigação, deverá (se o caso, a depender do score) retomar o processo natural de comunicação.

REFERÊNCIAS

Working Party 29. Guidelines on Personal data breach notification under Regulation 2016/679, p. 10/11 e 19.
THOMAS. Lisa, M. A Practical Guide to Handling Data Breach Notifications Worldwide, 2019, p. 90/92. .

QUAIS SERIAM AS POSSÍVEIS EXCEÇÕES DA OBRIGATORIEDADE DE INFORMAR OS TITULARES?

Considerando que a LGPD não distingue os critérios para comunicação à ANPD ou aos titulares, entendemos que as exceções para comunicação à Autoridade, independentemente de quais sejam, também devem se aplicar ao contexto dos titulares, razão pela qual fazemos remissão à nossa contribuição apresentada no item anterior.

QUAIS SÃO OS POSSÍVEIS CRITÉRIOS A SEREM ADOTADOS PELA ANPD NA ANÁLISE DA GRAVIDADE DO INCIDENTE DE SEGURANÇA? (ART. 48, §2°)

Questão respondida no primeiro tópico do presente documento.

EXISTE ALGUMA METODOLOGIA RECOMENDADA PARA A ANÁLISE DE GRAVIDADE DO INCIDENTE DE SEGURANÇA? SE SIM, QUAL(IS)?

Como mencionamos anteriormente, destacamos a metodologia da instituição europeia ENISA.

COMENTÁRIOS ADICIONAIS

Para além das contribuições ora expostas, antes mesmo da edição da regulamentação em referência, sugere-se que a ANPD remova de seu "formulário de comunicação de incidente de segurança com dados pessoais" o campo que indica a possibilidade de que a comunicação tenha sido enviada por agente de tratamento na condição de operador de dados, conforme print abaixo:

Isso porque, à luz da LGPD, não compete ao operador enviar comunicação de incidente à ANPD, tendo em vista que não cabe a tal parte realizar a avaliação necessária para se diagnosticar "risco ou dano relevante" aos titulares (critério para ser devida a comunicação). Referido ônus cabe exclusivamente ao controlador, que, inclusive, é a parte que, na prática, deterá todos os elementos relevantes para que tal avaliação aconteça de maneira adequada.

Entendemos que, embora nítida a boa-fé e o senso de pró-atividade da ANPD ao mencionar expressamente o operador no formulário, referida medida tem alto potencial de ser interpretada como algum tipo de orientação do órgão para que notificações aconteçam por parte do operador, o que gera imensa confusão (e potenciais litígios) entre os agentes de tratamento, especialmente no atual momento de ausência de clareza da sociedade e escassez de diretrizes oficiais sobre o tema (o que nem de longe se atribui à ANPD em si, mas à demora na sua constituição por quem de direito).

Portanto, em homenagem à segurança jurídica, e até para se evitar o acúmulo de notificações impertinentes junto à ANPD que sequer deveriam existir, sugere-se a pronta adequação do formulário para exclusão da menção ao operador.

SÃO PAULO/SP, 24 DE MARÇO DE 2021.

PRADO VIDIGAL

Privacidade & Digital

contato@pradovidigal.com.br
www.pradovidigal.com.br

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: ThoughtWorks Brasil Software Ltda.

CPF/CNPJ: 10.564.976/0001-40

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 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?	Neste caso, o que deve ser considerado é o impacto objetivo e material para o titular. Dentro desse contexto, há que se considerar não apenas o número de dados ou titulares afetados pelo incidente em questão, mas também a sensibilidade (para além da definição de dados sensíveis imposta pela LGPD) e profundidade de tais dados. Recomenda-se, ainda, a inspiração no seguinte documento relativo à GDPR: Recital 75.
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?	Deveria, sim, existir mais de uma categoria. Para tal, sugerimos uma escala que leve em consideração, especialmente: (i) quantidade de pessoas afetadas; (ii) quão afetadas essas pessoas são. É primordial que se leve em consideração o contexto diante da análise de risco ou dano relevante: quão provável de o incidente ocorrer; o que foi feito para mitigá-lo; como se deu a resposta ao incidente; quão efetivos foram os meios de adequação utilizados. Risco ou dano baixo não deve ser completamente irrelevante, mas há, sim, que se sobrepesar os interesses envolvidos, uma vez que o contexto brasileiro de proteção de dados ainda é muito incipiente.
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	Dano é o risco efetivado/realizado/concretizado. Para tanto, entendemos que o dano não deve ser presumido e sim comprovado (e entendemos que é essa correlação que deve existir entre os dois conceitos). Uma sequência como risco -> risco efetivado -> dano efetivamente causado (consequências). Em termos de risco, também entendemos que é necessário quantificar a probabilidade de o risco ser, inicialmente, efetivado e, novamente, quais foram as medidas tomadas para mitigá-lo. Para tanto, há de se considerar o risco de uma maneira objetiva. Decisões sobre casos concretos devem ser tomadas individualmente e mediante comprovação, em adição aos outros dispositivos legais aplicáveis, conforme o caso.

O que deve ser considerado na avaliação dos riscos do incidente?	Pontos que, na nossa visão, devem ser priorizados: - Se o incidente já aconteceu antes; - Se havia um risco óbvio que foi assumido e/ou desconsiderado; - Se medidas de mitigação foram tomadas e quais; - Evidências de que as partes tentaram evitar o incidente de segurança (e isso deve ser considerado para diminuir ou majorar a penalidade); - A criticidade dos dados/sistemas envolvidos; - O número de titulares (potencialmente) afetados; - A probabilidade de um acesso indevido; - Se estaríamos falando de um dado pessoal direto ou pseudoanonimizado (embora a LGPD não fale em pseudoanonimização, o critério da possibilidade de relação direta do dado com a pessoa pode ser considerado para avaliação de riscos em si).
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	Sugerimos que, neste primeiro momento, a necessidade de notificação se dê exclusivamente nos casos já apontados pela LGPD. Como é uma lei muito nova, entedemos que este não é o momento para falarmos em amplificação – com o tempo e com os aprendizados, a ANPD pode e deve emitir outros entendimentos.
Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	A GDPR prevê 72h e, pela nossa experiência atuando na União Europeia, é um prazo razoável considerando as diferentes variáveis (riscos, investigação interna mínima requerida, etc). Importante ressaltar que esse prazo deve começar a contar a partir do conhecimento, pela parte, do potencial incidente (e não do acontecimento em si). Nesse sentido, sugerimos que o prazo seja contado apenas em 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?	Se for suficientemente grave, de forma que necessite a informação aos titulares dos dados, entendemos que depende de quão imediatos são os riscos. Se exige alguma ação do titular de dados, especialmente em sentido de precaução para danos mais graves, os controladores deveriam avisá-los imediatamente, antes mesmo de decorrer o prazo para informar à ANPD. Se a gravidade não for tão alta (portanto, média), entendemos que o prazo de 07 dias úteis seria razoável. Ou, em caso de risco muito baixo, a comunicação aos titulares não precisaria ser feita.
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	Depende do nível de ameaça, conforme comentários da pergunta acima. Sobre o meio de comunicação, sugerimos que seja sempre o mesmo meio que os controladores normalmente se comunicam com o titular de dados em questão. A depender do nível da ameaça e da extensão dos danos, se altos, a comunicação pública também deverá ser feita, inclusive em termos de confiança da sociedade em geral relacionado àquele controlador em específico.

à imprensa, publicação na internet etc.)?	
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	Incidentes considerados de baixo risco para os direitos e liberdades dos titulares de dados, havendo a obrigação, entretanto, de manter registros internos para eventuais fiscalizações ou em casos de repetição de incidentes.
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	Incidentes considerados de baixo risco para os direitos e liberdades dos titulares de dados, havendo a obrigação, entretanto, de manter registros internos para eventuais fiscalizações ou em casos de repetição de incidentes.
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	É importante ressaltar que existem diferenças entre incidente de segurança de forma ampla e incidentes de segurança que envolvem dados pessoais. Nesse sentido, recomendamos também a inspiração na WP 29 da GDPR, para considerar critérios como: natureza, sensibilidade (em sentido amplo) dos dados, *accountability* do controlador (o que foi feito para a prevenção do risco no primeiro momento; quão efetivo isso foi; diferenças entre descaso do controlador e risco inerente, quando o controlador efetivamente tentou evitar), se o incidente se deu por um ator interno ou externo ao controlador, se os processos estavam bem definidos e as pessoas representantes do controlador bem treinadas (necessária a apresentação de evidências).
Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	Sugerimos a adoção do CREST como 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?	- Consideração de risco x responsabilidade; - Medidas educativas primeiro; - Análise de causas e posterior compartilhamento de recomendações, com follow ups das ações; - Auditorias e auditorias de acompanhamentos posteriores; - Formalização de processo interno para toda análise do incidente.

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