# RELATÓRIO DE ANÁLISE DE IMPACTO REGULATÓRIO

CONSTRUÇÃO DO MODELO REGULATÓRIO PARA COMUNICAÇÃO E TRATAMENTO DE INCIDENTES DE SEGURANÇA

SETEMBRO/2022

# RELATÓRIO DE ANÁLISE DE IMPACTO REGULATÓRIO

CONSTRUÇÃO DO MODELO REGULATÓRIO PARA COMUNICAÇÃO E TRATAMENTO DE INCIDENTES DE SEGURANÇA


**EQUIPE DE PROJETO:**

**ANDRESSA GIROTTO VARGAS – CGN/ANPD**

**BRUNO DUARTE GARCIA – CGF/ANPD**

**CAMILA FALCHETTO ROMERO – CGF/ANPD**

**CLEORBETE SANTOS – CGTP/ANPD**

**CRISTIANE LANDERDAHL DE ALBUQUERQUE – CGF/ANPD**

**DIEGO VASCONCELOS COSTA – GP/ANPD**

**FABRÍCIO GUIMARÃES MADRUGA LOPES – CGF/ANPD**

**GERALDO LOPES DA CONCEIÇÃO CUNHA – CGF/ANPD**

**ISABELA MAIOLINO – CGN/ANPD**

**IVAN TUYOSHI MORI KAKIMOTO – CGF/ANPD**

**JEFERSON DIAS BARBOSA – GP/ANPD**

**MARCELO SANTIAGO GUEDES – CGTP/ANPD**

**RAISSA ALENCAR DE SA BARBOSA – CGF/ANPD**

**RODRIGO SANTANA DOS SANTOS – CGN/ANPD**

**ROSEMARY DE FATIMA ANDRADE – CGF/ANPD**

**SABRINA FERNANDES MACIEL FAVERO – CGN/ANPD**

**THIAGO GUIMARÃES MORAES – CGTP/ANPD**

# RELATÓRIO DE ANÁLISE DE IMPACTO REGULATÓRIO

CONSTRUÇÃO DO MODELO REGULATÓRIO PARA COMUNICAÇÃO E TRATAMENTO DE INCIDENTES DE SEGURANÇA

**ELABORADO POR:**

**ANDRESSA GIROTTO VARGAS – CGN/ANPD**

**CRISTIANE LANDERDAHL DE ALBUQUERQUE – CGF/ANPD**

**ISABELA MAIOLINO – CGN/ANPD**

**RODRIGO SANTANA DOS SANTOS – CGN/ANPD**

**SABRINA FERNANDES MACIEL FAVERO – CGN/ANPD**

**Nota:**

Esse Relatório de Análise de Impacto Regulatório é um instrumento de análise técnica, cujas informações e conclusões são fundamentadas nas análises promovidas pela equipe técnica da ANPD responsável pelo tema. Assim, não reflete necessariamente a posição final e oficial da ANPD, que somente se firma pela decisão de seu Conselho Diretor.

ANPD Autoridade Nacional de Proteção de Dados

**SUMÁRIO**

# 1 SUMÁRIO EXECUTIVO

Este Relatório de Análise de Impacto Regulatório (AIR) tem por objetivo a análise de alternativas regulatórias e seus impactos com vistas à regulamentação do art. 48 da Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados (LGPD), o qual determina que o controlador deverá comunicar à autoridade nacional e ao titular de dados pessoais a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante a estes.

Embora a LGPD estabeleça critérios mínimos quanto ao conteúdo da comunicação e que algumas providências poderão ser determinadas para salvaguardar os direitos dos titulares de dados pessoais, o §1º do art. 48 institui obrigação de que a ANPD defina a forma e o prazo para cumprimento do dever de comunicação.

Assim, a fim de facilitar a identificação dos incidentes de segurança que necessariamente deverão ser comunicados à autoridade, conferir segurança jurídica com a fixação de prazo para notificação e a delimitação clara, objetiva e transparente de todos os ritos e critérios a serem adotados pela ANPD quanto à análise das notificações recebidas, neste AIR são apresentadas as alternativas regulatórias quanto ao escopo dos incidentes de segurança de notificação obrigatória; definição de quais incidentes acarretam risco ou dano relevante; prazos para comunicação de incidentes e o tratamento dos incidentes comunicados à ANPD.

Quanto aos critérios para definição de incidentes que possam acarretar riscos ou danos relevantes aos titulares de dados pessoais, a alternativa escolhida foi a combinação de critérios com base no contexto do incidente, levando-se em consideração a natureza e categoria dos dados pessoais, bem como o possível impacto aos interesses e direitos desses titulares.

Em relação ao prazo para notificação, definiu-se o prazo de até 3 (três) dias úteis para que o controlador comunique a ocorrência de incidente, nos termos do art. 48 da LGPD, à ANPD e ao titular de dados pessoais. Quanto à comunicação à ANPD estabeleceu-se, ainda, prazo adicional para complementação dessas informações, mediante justificativa.

No tocante à implementação, a norma proposta será implementada por meio de resolução da ANPD, a qual será objeto de consulta e audiência pública, nos termos da Portaria nº 16, de 8 de julho de 2021. Uma vez que o art. 48 da LGPD, objeto da regulamentação proposta, encontra-se em vigor desde 14 de agosto de 2020, propõe-se que a resolução entre em vigor na data de sua publicação, não havendo razão para que se prolongue a produção de efeitos do regulamento de comunicação de incidentes, nos termos do art. 4º do Decreto nº 10.139, de 28 de novembro de2019, que dispõe sobre a revisão e a consolidação dos atos normativos inferiores a Decreto.

Ainda quanto à implementação, contar-se-á com um de um plano de comunicação para sua divulgação aos agentes de tratamento, de modo a trazer transparência e clareza em relação às obrigações a eles impostas.

Relativamente ao monitoramento da norma, sugere-se a utilização de indicadores, os quais visam mensurar a ocorrência de incidentes que acarretam risco aos titulares de dados pessoais; a aderência à norma e a conformidade à LGPD.

Por fim, o que se espera com a AIR é que se possa trazer maior segurança jurídica na relação com os agentes regulados, além de trazer benefícios para os titulares de dados pessoais tendo em vista que a proposta normativa visa conduzir o agente regulado à conformidade à Lei, os regulamentos e aos deveres decorrentes dos demais atos administrativos de efeitos concretos expedidos pela Autoridade.

## 2 IDENTIFICAÇÃO DO PROBLEMA REGULATÓRIO

A LGPD dispõe que o controlador deverá comunicar à autoridade nacional e ao titular de dados pessoais a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante a estes.

Muito embora a lei estabeleça critérios mínimos sobre o conteúdo da comunicação e algumas providências que poderão ser determinadas para salvaguardar os direitos dos titulares de dados pessoais, também traz, no §1º do art. 48, a obrigação de que a ANPD defina a forma e o prazo para cumprimento da obrigação de comunicação, *in verbis*:

> Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.
> § 1º A comunicação será feita em prazo razoável, **conforme definido pela autoridade nacional**, e deverá mencionar, **no mínimo**:
> 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.
> (...)

Adicionalmente, em vista da determinação do *caput* do art. 48, verifica-se a necessidade de que a ANPD esclareça quais incidentes deverão ser comunicados, ou seja, quais podem acarretar risco ou dano relevante aos titulares de dados pessoais.

Regulamentar a aplicação do artigo 48 da LGPD é necessário para que o controlador tenha clareza e segurança jurídica para cumprir com a obrigação de comunicação que lhe foi imposta, bem como para a ANPD exercer sua competência fiscalizadora e sancionadora nos termos dos seus §§2º e 3º e do art. 52 caso seja verificada infração às normas previstas na Lei. Neste ponto, recorde-se:

> (...)
> § 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como:
> I - ampla divulgação do fato em meios de comunicação; e
> II - medidas para reverter ou mitigar os efeitos do incidente.
> § 3º 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.

Assim, observa-se três questões a serem regulamentadas:

I. Escopo dos incidentes de segurança de notificação obrigatória: definição de quais incidentes acarretam risco ou dano relevante;
II. Processo de comunicação de incidentes de segurança: prazos para comunicação à ANPD e ao titular de dados pessoais; e

III. Tratamento dos incidentes de segurança notificados à ANPD, a depender do caso concreto.

## 3 IDENTIFICAÇÃO DOS GRUPOS AFETADOS

A transversalidade da LGPD alcança todas as operações de tratamento de dados pessoais, independentemente do meio adotado, do país sede do agente de tratamento, ou do país em que estejam localizados os dados pessoais, conforme dispõe o artigo 3º da referida lei. A norma de comunicação de incidentes de segurança ora avaliada, apesar de tratar de obrigação imposta ao controlador, interessa a toda e qualquer agente que realize operações de tratamento envolvendo dados pessoais, bem como aos titulares desses dados.

Os controladores serão afetados pela norma a ser editada na medida em que deverão cumprir os critérios para comunicação de incidentes à ANPD. Os titulares de dados pessoais também são impactados pela proposta normativa na medida em que seus dados pessoais poderão ter sido afetados pelo incidente e deverão ter seus direitos resguardados, bem como eventuais danos mitigados. Ao mesmo tempo, operadores e demais envolvidos no tratamento de dados poderão estar envolvidos nas obrigações derivadas da norma, auxiliando na prestação das informações requeridas e na adoção de providências necessárias.

Assim, os grupos a seguir foram identificados como mais impactados:

I. Agentes de tratamento de dados;
II. Titulares de dados pessoais; e
III. Encarregados.

## 4 FUNDAMENTAÇÃO LEGAL

O direito à proteção de dados pessoais consta expressamente no rol de direitos e garantias fundamentais ao cidadão estabelecidos no art. 5º da Constituição Federal. Ainda, a Carta Magna fixou, em seu art. 21, a competência da União em organizar e fiscalizar a proteção

e o tratamento de dados pessoais, nos termos da lei, bem como a competência privativa para legislar sobre proteção e tratamento de dados pessoais.

A LGPD inaugurou um novo regime jurídico referente ao tratamento de dados pessoais no país, conferindo prerrogativas à ANPD para zelar, implementar e fiscalizar o cumprimento da lei em todo o território nacional. Desta forma, a ANPD é o órgão federal responsável por dar efetividade à LGPD no país. Dentre as competências da ANPD, consta o estabelecimento de normas e diretrizes para a interpretação e implementação da LGPD.

Quanto a esse ponto, destaca-se que o art. 48 da LGPD dispõe que agentes de tratamento devem comunicar a ANPD e ao titular de dados pessoais a ocorrência de incidente de segurança que possam acarretar riscos ou danos relevantes titulares estes, nos seguintes termos:

> Art. 48. O controlador deverá comunicar **à autoridade nacional** e **ao titular** a ocorrência de **incidente de segurança** que possa **acarretar risco ou dano relevante aos titulares.**
> § 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:
> 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.
> § 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como:
> I - ampla divulgação do fato em meios de comunicação; e
> II - medidas para reverter ou mitigar os efeitos do incidente.
> § 3º 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, a Agenda Regulatória da ANPD para o biênio 2021-2022, aprovada pela Portaria nº 11, de 27 de janeiro de 2021, previu, em seu item 6, iniciativa regulatória para regulamentar o dispositivo relativo à notificação de incidentes a Autoridade e ao titular de

dados pessoais. Tal regulamentação deve ser precedida de AIR, nos termos do art. 55-J, §2º da LGPD.

## 5 OBJETIVOS A SEREM ALCANÇADOS

O objetivo imediato da intervenção regulatória é regulamentar o dispositivo legal de notificação de incidentes de segurança, nos termos do art. 48 da LGPD, de modo a definir o prazo razoável em que deverá ser realizada, quais incidentes são passíveis de acarretarem risco ou dano relevante aos titulares de dados pessoais e qual será o tratamento das notificações recebidas pela ANPD.

Por sua vez, os objetivos mediatos são: facilitar a identificação dos incidentes de segurança que necessariamente deverão ser comunicados à autoridade, conferir segurança jurídica com a fixação de prazo para notificação e a delimitação clara, objetiva e transparente dos ritos e critérios a serem adotados pela ANPD quanto à análise das notificações recebidas.

## 6 TOMADA DE SUBSÍDIOS

Tendo em vista a necessidade de coleta de informações sobre o tema, decidiu-se realizar Tomada de Subsídios por meio de intercâmbio documental a fim de possibilitar a participação da sociedade acerca de questões relacionadas à comunicação de incidentes de segurança, nos termos da Nota Técnica n° 3/2021/CGN/ANPD (SEI 2398694). O documento SEI 2398738 foi então elaborado com 13 (treze) perguntas e espaço para sugestão de normativo. O recebimento de subsídios ocorreu entre os dias 22/02/2021 e 24/03/2021[1].

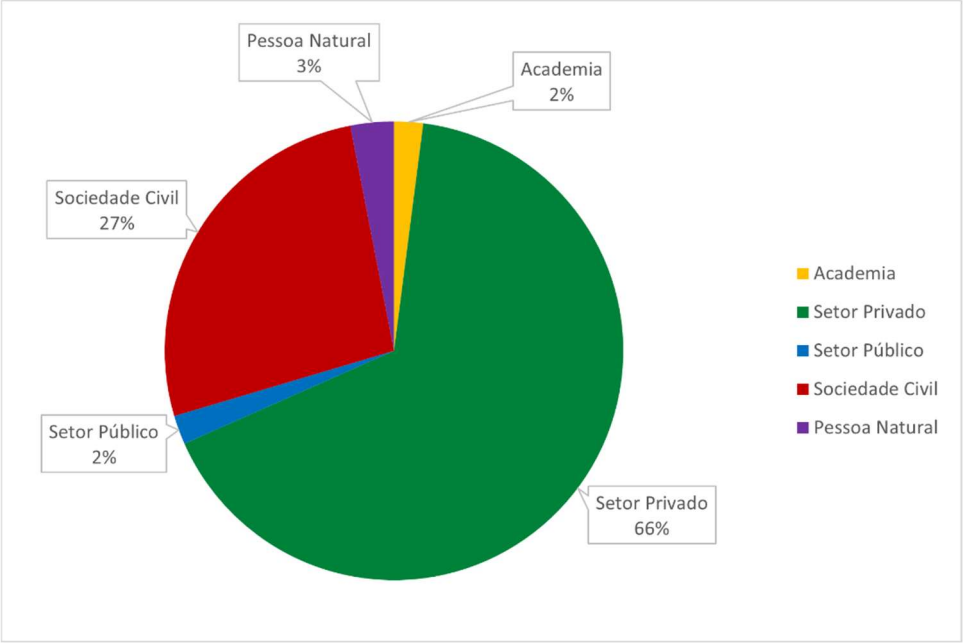
Foram recebidas 98 (noventa e oito) contribuições para a Tomada de Subsídios dentro do prazo estabelecido. Outras 10 (dez) contribuições foram recebidas fora do prazo e, portanto, não foram consideradas.

Quanto aos participantes, 66% identificaram-se como representantes do setor privado; 27% classificaram-se como represente da Sociedade Civil; 3%, identificaram-se como pessoas

[1] Conforme nota à imprensa disponível em < https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-inicia-processo-de-regulamentacao-sobre-incidentes-de-seguranca-com-tomada-de-subsidios> Acesso em 13 mai. 2022.

naturais e 2% dos participantes identificaram-se como representantes do setor público e como membros da academia. Uma breve síntese das contribuições recebidas dentro do prazo é feita seguir.

Gráfico 1: Relação de participantes – Tomada de Subsídios




Fonte: Elaboração própria (Coordenação-Geral de Normatização)

A primeira pergunta do formulário da Tomada de Subsídios tratou da definição de risco ou dano relevante e dos critérios que deveriam ser utilizados para avaliar se o risco ou o dano é relevante. Várias contribuições foram no sentido de que risco ou dano relevante está relacionado à probabilidade de danos concretos, ao tipo de dado pessoal afetado, ao tipo de direito afetado e ao impacto em liberdades e direitos do titular de dados pessoais. Algumas contribuições sugeriram que fosse criada análise quantitativa de danos e impactos, bem como uma metodologia para a avaliação de riscos.

Em relação aos critérios, algumas contribuições sugeriram que a ANPD estabeleça critérios claros e objetivos do que constituiria risco ou dano relevante ao titular de dados pessoais, enquanto outras sugeriram que não se defina critérios taxativos e sim orientações gerais. Algumas contribuições propuseram que a norma preveja critérios objetivos, mas que também tivesse flexibilidade para que as especificidades de cada caso sejam consideradas.

Além disso, houve contribuições que afirmaram que é o controlador quem deve escolher uma metodologia para avaliar o risco ou dano de um incidente. Ainda no tocante aos critérios a serem utilizados, os mais frequentes nas contribuições foram: tipo de incidente (disponibilidade, integridade, confidencialidade); natureza dos dados; volume dos dados; facilidade de identificação dos titulares; gravidade das consequências aos titulares; características dos titulares; aspectos do setor econômico ou do controlador; medidas tomadas para reverter ou mitigar as consequências; medidas de segurança tomadas previamente ao incidente; possível intenção de quem perpetrou o ataque; publicidade prévia dos dados; natureza do risco ou dano advindo do incidente. Houve contribuições, contudo que se opuseram à utilização de certos critérios, como o volume de titulares afetados.

Nessa questão, várias contribuições também levantaram a necessidade de a ANPD definir o conceito de incidente de segurança e diferenciá-lo de incidentes que não envolvam dados pessoais.

A segunda pergunta relacionou possíveis categorias de risco ou dano relevante e questionou se tal critério deveria ser subdividido em mais categorias. A maioria das respostas concordou que o risco ou dano relevante deveria ser dividido em categorias como baixo, médio, alto e muito alto. Algumas contribuições sugeriram criar categorias para a gravidade do incidente, mas não para risco e dano. Outras sugestões propuseram separar as categorias de risco e de dano, enquanto outras sugeriram tratar risco e dano em conjunto. Ainda outras poucas sugestões foram no sentido de que subcategorias não seriam necessárias, mas apenas a definição do que seria ou não relevante.

Em relação a como realizar a distinção de cada nível, várias contribuições sugeriram critérios como impacto para o titular; tipo de dado; tipo de titular; volumetria; características do incidente; pessoa ou organização que teve acesso aos dados pessoais de forma não autorizada; extensão geográfica dos dados e medidas adotadas pelo controlador. Houve algumas sugestões no sentido de se estabelecer método para aferir a probabilidade e o impacto do incidente de segurança. Outras sugeriram que o controlador é quem deveria definir a metodologia que será utilizada para classificar o risco ou dano. A maioria das contribuições informou que incidentes com risco ou dano baixo não deveriam ser de comunicação obrigatória à ANPD.

A terceira pergunta questionou a respeito distinção entre risco e dano ao titular e como os dois conceitos se relacionam. A maioria das contribuições sinalizou que o risco seria a probabilidade de acontecer algum impacto ao titular, enquanto o dano seria o impacto materializado. Algumas contribuições sugeriram que o dano deveria ser comprovado, já outras afirmaram que a depender do tipo e qualidade do dado vazado, já seria possível caracterizar o dano. Algumas contribuições destacaram que a diferenciação poderia se dar para fins de responsabilização do agente de tratamento. Contudo, para fins de notificação do incidente de segurança, deve-se considerar tanto o risco quando o dano relevante. Algumas contribuições associaram o risco à gestão do controlador e o dano ao momento em que o incidente de segurança ocorreu. Outras sugeriram que o dano deveria ser comprovado, enquanto outras julgam que tal comprovação não seria factível, tendo em vista, por exemplo, que o dano pode se dar no futuro. Além disso, contribuições propuseram que, para fins do art. 48 da LGPD, risco e dano poderiam ser equiparados, já que a própria violação de segurança poderia causar um dano ao violar o direito da privacidade e da autodeterminação afirmativa.

A quarta pergunta questionou o que deveria ser considerado na avaliação dos riscos do incidente. Os fatores mais citados nas contribuições foram: contexto do tratamento de dados; contexto do incidente; medidas técnicas adotadas; tipo de dados, volume de dados afetados; possibilidade de identificação dos titulares afetados; publicização anterior dos dados afetados; número de indivíduos afetados; características especiais dos titulares afetados; gravidade dos efeitos para o titular; autor do incidente; fato gerador do incidente; se o dano foi concretizado; a duração do incidente; porte da empresa; intenções de terceiros que tiveram acesso aos dados; eventual relatório de impacto à proteção de dados pessoais; eventual reclamação do titular à ANPD.

A quinta pergunta questionou quais informações o controlador deveria notificar à ANPD além daquelas listadas no §1º do art. 48. Aproximadamente 30% das contribuições afirmaram que as informações listadas no dispositivo legal citado são suficientes. Além disso, algumas contribuições sugeriram retirar do formulário de notificação de incidentes a possibilidade de o operador realizar a comunicação.

Aqueles que afirmaram que outras informações poderiam ser adicionadas citaram principalmente: nível do impacto do incidente; plano de ação do controlador; prazo para

conclusão do plano; informações de contato do controlador e do encarregado; descrição do incidente de segurança; método de comunicação dos titulares afetados; plano de governança pré-estabelecido; tipo do incidente; número de titulares afetados; informações temporais do incidente; volume de dados afetados; possíveis consequências em decorrência do incidente; extensão geográfica; se dados são compartilhados com terceiros. Algumas contribuições sugeriram a disponibilização de formulário simplificado, bem como a diferenciação da comunicação à ANPD e ao titular.

Outras contribuições afirmaram que a ANPD deveria permitir flexibilidade aos controladores para que eles pudessem decidir a melhor forma de atender o dispositivo legal. Também houve contribuições no sentido de o rol de informações não ser obrigatório. Houve contribuições também que sugeririam a criação de formulário automatizado. Várias contribuições levantaram também a importância de a ANPD manter a confidencialidade das informações prestadas e algumas afirmaram que as informações prestadas não poderiam ser usadas contra os controladores. Algumas contribuições ainda sugeriram que a ANPD detalhasse as informações dispostas no §1º do art. 48.

A sexta pergunta questionou qual prazo seria razoável para que os controladores comunicassem a ANPD sobre incidentes de segurança. Os prazos sugeridos foram diversos. Várias contribuições sugeriram 72 horas, conforme estabelecido no Regulamento Geral de Proteção de Dados (RGPD), da União Europeia. Outras mencionaram o Decreto n° 9.936, de 24 de julho de 2019, art. 18, §1º, que determina que incidentes de segurança que possam causar "riscou ou prejuízo relevante aos cadastrados" sejam notificados à ANPD em dois dias úteis. Houve ainda sugestão de prazos mais curtos (24 horas) e mais longos (de até 30 dias, conforme adotado pela autoridade australiana). Várias contribuições sugeriram adotar a notificação em etapas, por meio das quais o controlador fornece informações à ANPD em pelos menos duas fases, a primeira imediatamente após a ciência do incidente e a segunda depois que o controlador possui mais informações a respeito do ocorrido.

Houve contribuições no sentido de permitir justificativa para a comunicação atrasada, prazos diferenciados a depender de fatores como gravidade do incidente e porte da empresa. Algumas contribuições também levantaram a importância em se definir a "ciência do incidente", momento a partir do qual o prazo começaria a ser contado.

A sétima pergunta, relativa à comunicação ao titular de dados pessoais, questionou qual seria o prazo razoável para realizar tal comunicação e quais informações deveriam ser ali apresentadas. Foram sugeridos prazos diversos, de 72 horas até 60 dias. Algumas contribuições sugeriram que o prazo deveria ser diferenciado de acordo com a gravidade do incidente e/ou porte da empresa. Também foi sugerido que o prazo para notificação ao titular de dados pessoais comece a contar a partir da notificação à ANPD, enquanto outras sugeriram que essa comunicação se dê em paralelo com a comunicação à ANPD. Houve também sugestões de se dissociar a comunicação à ANPD da comunicação ao titular.

Em relação ao conteúdo da comunicação, várias contribuições afirmaram que ela deve ser em linguagem fácil e clara e deve conter: descrição do incidente; riscos associados ao incidente; dados afetados; canal de comunicação; dados do encarregado; medidas a serem tomadas pelo titular; medidas já tomadas pela ANPD; se o incidente de segurança foi comunicado à ANPD.

A oitava pergunta questionou qual seria a forma mais adequada de comunicar o titular de um incidente de segurança. A maioria das contribuições afirmou que a comunicação direta e individualizada é preferível. Contudo, se esse tipo de comunicação requerer esforço desproporcional, se não for possível e/ou se envolver grande número de indivíduos, a comunicação pública pode ser mais adequada. Várias contribuições também pontuaram que a comunicação deve ser escolhida conforme o caso e pode depender do número de titulares. Algumas contribuições sustentaram que o controlador está em melhor posição para definir que tipo de comunicação é mais adequada para cada caso. Foi sugerido ainda que a ANPD disponibilize ambiente próprio em seu site para disponibilizar esse tipo de informação.

A nona pergunta referiu-se a eventuais exceções de obrigatoriedade de informar a ANPD. Grande parte das contribuições afirmou que incidentes de segurança com risco ou dano baixo não deveriam ser comunicados e algumas também sugeriram que fosse dado o mesmo tratamento para risco ou dano médio. No mesmo sentido, várias contribuições afirmaram que não deveriam ser notificados incidentes que não afetassem direitos e liberdades dos titulares. Outros fatores citados que desobrigariam uma notificação são: ausência de dano; adoção de medidas de segurança pelo controlador; dados afetados ininteligíveis; dados previamente públicos; dados não estruturados; incidentes prontamente solucionados. Outras

características para dispensar a notificação são aquelas relativas ao volume de dados afetados, ao tipo de titular e tipo de dado e ao porte da empresa. Houve ainda contribuições que afirmaram que não deveria haver exceções.

A décima pergunta tratou das possíveis exceções da obrigatoriedade de informar os titulares. Assim como na pergunta anterior, a maior parte das contribuições citou incidentes com risco baixo como possível exceção. Também foram citados incidentes em que é necessário um esforço desproporcional para comunicação dos titulares afetados. Algumas contribuições também sugeriram dispensar a comunicação ao titular quando a divulgação pode afetar a investigação relacionada ao incidente. Outros fatores mencionados foram: quando o controlador adotou medidas de segurança para proteger os dados antes do incidente; quando o controlador adotou medidas para impedir o dano; quando o incidente foi causado pelo próprio titular; no caso de dados ininteligíveis; no caso de dados que já eram públicos; conforme a quantidade de titulares ou conforme o porte do controlador. Por outro lado, houve contribuições que sustentaram que não deveria haver exceções.

A décima primeira pergunta questionou quais seriam os possíveis critérios a serem adotados pela ANPD na análise de gravidade de incidentes de segurança, conforme o §2° do art. 48 da LGPD. Várias contribuições fizeram referência às respectivas respostas às perguntas um a quatro. Dessa forma, a maior parte dos critérios citados foram idênticos aos mencionados na avaliação de relevância do risco ou dano. Outros fatores citados foram: a existência de relatório de impacto à proteção de dados pessoais; comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais ininteligíveis; características de governança do controlador; reincidência do controlador; histórico de incidentes da mesma natureza de outros controladores; nível de preparo do controlador para lidar com incidentes; boa-fé e intenção de terceiros que tiveram acesso aos dados; consequências transfronteiriças e número de acessos aos dados afetados.

A décima segunda pergunta questionou se haveria metodologias recomendadas para a análise de gravidade do incidente de segurança. Várias metodologias foram citadas, entre elas: *Recommendations for a methodology of the assessment of severity of personal data breaches* da *European Union Agency for Network and Information Security* (ENISA); *Opinion 03/2014 on Personal Data Breach Notification* do *Working Party 29; Guidelines on Personal*

*data breach notification under Regulation 2016/679*, da Comissão Europeia; *Examples regarding data breach* notification, da *European Data Protection* Board; *Guía para la notificación de brechas de datos personales* da *Agencia Española de Protección de Datos (AEPD)*; matriz elaborada pelo *National Health System* (NHS) do Reino Unido; ISO 31000 e 27000; framework de cyber security *do National Institute of Standards and Techonology*; Circular nº 3978/2020 do Banco Central do Brasil. Vários desses documentos são sintetizados na seção 7 deste relatório.

Por fim, a décima terceira pergunta, referiu-se as providências a serem determinadas pela ANPD aos controladores após a comunicação de um incidente de segurança. Várias contribuições afirmaram que as providências variarão conforme o controlador e o incidente. Diversas mencionaram tanto a remediação do incidente comunicado como planos de ação preventivos para corrigir eventuais falhas que resultaram no incidente. Houve menção também a solicitação de evidências do tratamento do incidente, ações de minimização de danos aos titulares e implementação de contramedidas e ações educativas. Outras providências citadas foram a de notificar o titular e determinar auditoria e certificação dos sistemas de gestão de segurança da informação. Algumas contribuições também afirmaram que a providências determinadas pela ANPD não devem se confundir necessariamente com as sanções previstas na LGPD.

Além das perguntas acima listadas, houve, ainda, um campo específico para contribuições adicionais em que alguns agentes realizaram sugestões relacionadas a temas não abordados nas questões. Além disso, foram realizadas reuniões técnicas com especialistas sobre o tema entre os dias 15 e 18/03/2022. Foram ouvidos representantes do Núcleo de Informação e Coordenação do Ponto BR (NIC.br), Centro de Direito, Internet e Sociedade (CEDIS) e Instituto Brasileiro de Defesa do Consumidor (IDEC); representantes do Laboratório de Políticas Públicas e Internet (LAPIN) e Instituto de Referência em Internet e Sociedade (IRIS-BH); representantes do Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.REC) e Coding Rights (SEI nº 2475382); representantes do Data Privacy Brasil e Privacy Academy e representantes do ITS Rio e Internet Lab.

Os principais pontos abordados nessas reuniões estão listados nas Memórias de Reunião nº 2474721, 2475226, 2475382, 2475465, 2483002.

# 7 TEMA 1: CRITÉRIOS PARA DEFINIÇÃO DE INCIDENTES QUE POSSAM ACARRETAR RISCOS OU DANOS RELEVANTES AOS TITULARES

## 7.1 Experiência Internacional

Os artigos 33 e 34 do RGPD regulamentam a comunicação de violações de dados pessoais à autoridade e ao titular.

Já o art. 34 da RGPD estabelece as condições para que os titulares de dados sejam comunicados:

> 1. Quando a violação dos dados pessoais for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento comunica a violação de dados pessoais ao titular dos dados sem demora injustificada.[2]

O mesmo artigo também estabelece as hipóteses em que a comunicação a titulares não é necessária.

> 3. A comunicação ao titular dos dados a que se refere o n. 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 nº 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.[3]

O art. 34 estabelece, ainda, que a autoridade pode determinar que o titular seja comunicado caso entenda que o incidente de segurança gera um elevado risco e o controlador não tiver feito tal comunicação.

O Considerando 75 do RGPD esclarece o conceito de risco:

---

[2] COMISSÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).** Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj Acesso em: 25 jul.2022.

[3] *Ibidem*.

> (75) 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 económica ou social; quando os titulares dos dados possam ficar privados dos seus direitos e liberdades ou impedidos do exercício do controlo 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 aspetos de natureza pessoal, em particular análises ou previsões de aspetos que digam respeito ao desempenho no trabalho, à situação económica, à saúde, às preferências ou interesses pessoais, à fiabilidade 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]

Por sua vez, o Considerando 76 da RGPD indica critérios a serem considerados na avaliação de risco e que eles devem ser aferidos com base em uma avaliação objetiva:

> (76) A probabilidade e a gravidade dos riscos para os direitos e liberdades do titular dos dados deverá ser determinada por referência à natureza, âmbito, contexto e finalidades do tratamento de dados.
> Os riscos deverão ser aferidos com base numa avaliação objetiva, que determine se as operações de tratamento de dados implicam risco ou risco elevado.[5]

Por sua vez, o *Working Party 29* ("WP29") publicou, em 2014, parecer sobre a notificação de incidentes de segurança (*Opinion 03/2014 on Personal Data Breach Notification*[6]). O objetivo do parecer é auxiliar controladores na decisão de quando notificar titulares da ocorrência de um incidente de segurança (*data breach*).

---

[4] COMISSÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).** Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj Acesso em: 25 jul. 2022

[5] *Ibidem*.

[6] ARTICLE 29 DATA PROTECTION WORKING PARTY. **Opinion 03/2014 on Personal Data Breach Notification. 2014**. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf. Acesso em: 23 mai. 2022.

O documento faz referência à Diretiva 2002/58/EC, já que o RGPD ainda não havia sido promulgado. Segundo essa diretiva, incidentes de segurança deveriam ser notificados à autoridade competente. Incidentes em que os dados são ininteligíveis não precisavam ser comunicados aos titulares, já que não afetariam sua privacidade. Contudo, o parecer do WP29 sustenta que mesmo se tratando de dados ininteligíveis, os titulares deveriam ser comunicados se o incidente causou alteração ou perda de dados.

O parecer também explica que caso medidas de segurança de dados pessoais fossem adotadas e se o controlador tivesse um plano para lidar com incidentes de segurança, seria possível minimizar os danos aos titulares. Ademais, controladores deveriam ter em mente que um dos principais benefícios de notificar o titular é fornecer informação para que ele adote as medidas cabíveis para reduzir o risco do incidente.

Segundo o WP29, incidentes de segurança que poderiam causar efeitos adversos a dados pessoais ou à privacidade deveriam ser comunicados aos titulares. A violação de dados pode ser de confidencialidade, integridade ou disponibilidade. O documento lista exemplos de tais tipos de incidentes e medidas técnicas que, se adotadas, poderiam evitar a obrigatoriedade de notificação aos titulares.

O documento ainda discorre sobre cenários em que a notificação a titulares não era obrigatória. Ao final, há perguntas e respostas sobre temas específicos, como incidentes que envolvem apenas um indivíduo, dados públicos e quando o controlador não possui dados de contato dos indivíduos afetados. Nesse último caso, o WP29 afirma que o controlador deveria envidar esforços razoáveis para comunicar os titulares, por exemplo, por meio de comunicação pública. Em relação a dados públicos, o texto afirma que os titulares deveriam ser notificados sempre que o incidente alterasse a disponibilidade ou a publicidade dos dados pessoais.

Posteriormente, em 2018, o WP29 também emitiu as Orientações sobre a notificação de uma violação de dados pessoais no âmbito do Regulamento (UE) 2016/679[7]. Esse documento já faz recomendações baseadas no RGPD e explica os requisitos obrigatórios de

[7] ARTICLE 29 DATA PROTECTION WORKING PARTY**. Guidelines on Personal data breach notification under Regulation 2016/679**. 2018. Disponível em: https://ec.europa.eu/newsroom/article29/redirection/document/49827. Acesso em: 25/05/2022.

notificação e medidas que o controlador e o operador podem tomar para cumprirem as obrigações. Também são fornecidos vários exemplos.

Segundo o documento, violação de dados pessoais é uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.

O WP29 recomenda que, ao avaliar o risco, o controlador considere a gravidade do impacto e a probabilidade de o incidente ocorrer. Na avaliação, recomenda que se avalie os seguintes critérios:

I. Tipo de violação;
II. Natureza, sensibilidade e volume dos dados pessoais;
III. Facilidade de identificação de pessoas singulares;
IV. Gravidade das consequências para as pessoas afetadas;
V. Características especiais das pessoas afetadas;
VI. Características especiais do controlador;
VII. Número de pessoas afetadas; e
VIII. Elementos gerais.

A **Agencia Española de Protección de Datos (AEPD), autoridade da Espanha,** publicou o *Guía para la notificación de brechas de datos personales*[8], que busca estabelecer diretrizes para a notificação de incidentes de segurança. O documento esclarece que nem todos os incidentes serão considerados como um incidente de segurança que afeta dados pessoais. Por exemplo, se os dados não são identificáveis ou se são dados tratados por pessoas físicas em âmbito doméstico. Além disso, o documento afirma que todas as organizações que tratem dados pessoais devem possuir um processo de gerenciamento de incidentes de segurança.

Ainda segundo o guia da AEPD, apenas os incidentes que possuam risco de afetar os direitos e liberdades dos titulares devem ser notificados à autoridade. Os incidentes que

[8] AGENCIA ESPAÑOLA PROTECCIÓN DATOS**. Guía para la notificación de brechas de datos personales.** 2021. Disponível em: https://www.aepd.es/sites/default/files/2019-09/guia-brechas-seguridad.pdf. Acesso em: 25/05/2022.

possuam alto risco devem ser notificados também aos titulares de dados pessoais. Os fatores a serem considerados para avaliar o risco de um incidente são: (i) tipo de incidente de segurança; (ii) natureza, sensibilidade e volume de dados pessoais; (iii) facilidade de identificação dos indivíduos; (iv) gravidade das consequências para os direitos e liberdades dos indivíduos; (v) características particulares do controlador; (vi) número de indivíduos afetados; (vii) considerações gerais.

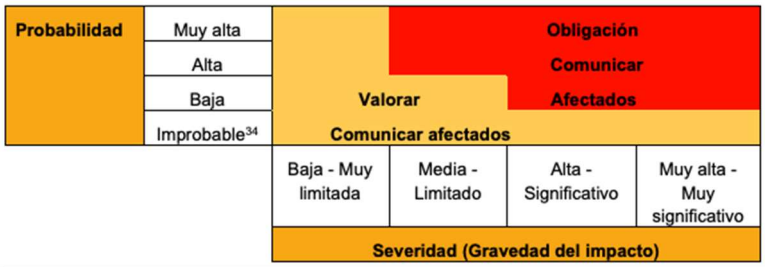
Se o operador tomar conhecimento de um incidente de segurança, ele deverá avisar o controlador de forma que ele possa cumprir com suas obrigações. O guia sugere, inclusive, que tal aviso e seu prazo estejam estabelecido no contrato entre controlador e operador. Além disso, é possível que qualquer pessoa denuncie um incidente de segurança por meio de um formulário de apresentação de reclamação.

O guia estabelece ainda que o controlador deve ser capaz de determinar a categoria dos dados pessoais afetados, o número de indivíduos e seu perfil para poder determinar o nível de risco. O documento lista dezenove categorias de dados pessoais e suas respectivas descrições. O documento lista ainda oito perfis de titulares, como clientes, empregados, pacientes e usuários. O controlador deve avaliar também quais são as possíveis consequências para os titulares de dados pessoais derivadas do incidente de segurança. O documento lista oito tipos de consequências:

I. Impossibilidade de exercer algum direito ou acesso a um serviço;
II. Roubo de identidade;
III. *Phishing* ou *spamming*;
IV. Perdas financeiras;
V. Danos reputacionais;
VI. Perda de confidencialidade de dados afetados por sigilo profissional;
VII. Danos psicológicos ou físicos; e
VIII. Perda de controle sobre seus dados pessoais.

O guia espanhol ainda divide o nível de gravidade do incidente de segurança em quatro categorias: baixo, médio, alto e muito alto, de acordo com as possíveis consequências para os titulares. Quando a gravidade for alta ou muito alta, o controlador deverá comunicar o incidente aos titulares afetados. Além disso, mesmo que a gravidade seja baixa ou média, se a probabilidade de materialização for alta ou muito alta, o titular também deverá ser comunicado. A Figura 1 a seguir ilustra a obrigatoriedade de notificação.

Figura 1 - Quadro de obrigação de notificação de incidentes de segurança da AEPD




Fonte*: Guía para la notificación de brechas de datos personales da AEPD*

**A *Data Protection Commission* (“DPC”) da Irlanda** publicou alguns documentos relativos à notificação de incidentes de segurança. O primeiro é *o Quick Guide to GDPR Breach Notifications*[9]*,* de agosto de 2019. O objetivo desse documento é ajudar controladores a entender suas obrigações básicas relativas a incidentes de segurança perante a autoridade e os titulares.

Esse guia está organizado em forma de perguntas e respostas e a primeira pergunta é relacionada ao conceito de incidente de segurança, ou violação de dados pessoais, que seria “uma violação de segurança em que ocorreu a destruição, perda, alteração ou divulgação não autorizada ou acesso a dados pessoais, de maneira acidental ou ilegal”. O documento também afirma que uma violação de dados pessoais afeta negativamente a confidencialidade, integridade ou disponibilidade de dados pessoais e, portanto, quando o incidente acontece, o controlador não pode mais garantir o atendimento aos princípios de proteção de dados pessoais elencados no art. 5 da RGPD.

[9] DATA PROTECTION COMMISSION**. A Quick Guide to GDPR Breach Notifications**. 2019. Disponível em: https://www.dataprotection.ie/sites/default/files/uploads/2019-08/190812%20GDPR%20Breach%20Notification%20Quick%20Guide.pdf. Acesso em: 15/07/2022.

Em relação à notificação à autoridade, o guia irlandês explica que o controlador é obrigado a notificar qualquer incidente de segurança que envolva dados pessoais, a não ser que ele consiga demonstrar que o incidente não gerou riscos para os direitos e liberdades dos titulares. O controlador também deve registrar toda a informação relevante pertinente ao incidente (de acordo com o art. 33 da RGPD), inclusive em que momento tomou conhecimento do incidente. O DPC recomenda que essa informação também seja apresentada na notificação à autoridade, além das informações determinadas pela RGPD.

O guia ainda explica que a obrigação de comunicação aos titulares tem um critério mais elevado, já que o controlador só tem a obrigação de comunicar os titulares incidentes de segurança que causem risco elevado. Além disso, o guia cita as exceções de comunicação ao titular dispostas no RGPD, bem como descreve o conteúdo da comunicação.

Por fim, o guia rápido da DPC afirma que o controlador pode notificar incidentes que não gerem risco caso entendam apropriado, a depender do contexto específico.

O segundo documento emitido pelo DPC é o "*A Pratical Guide do Personal Data Breach Notifications under the GDPR*"[10], de outubro de 2019. O objetivo desse documento é o de prover recomendações práticas a controladores de como lidar com incidentes de segurança e como proceder à notificação à autoridade. O guia foi produzido depois de uma análise de tendências e estatísticas realizada dos incidentes comunicados no primeiro ano desde que a notificação passou a ser obrigatória.

Além das orientações já trazidas no guia rápido, o documento também fornece orientações de como avaliar o risco de um incidente de segurança. Nesse sentido, lista os seguintes fatores que devem ser considerados pelos controladores:

I. O tipo e natureza do dado pessoal;
II. As circunstâncias do incidente de segurança;
III. Se os dados pessoais estavam protegidos com medidas técnicas de segurança;
IV. A facilidade de identificação dos titulares direta ou indiretamente;

[10] DATA PROTECTION COMMISSION. **A Practical Guide to Personal Data Breach Notifications under the GDPR.** 2019. Disponível em: https://www.dataprotection.ie/sites/default/files/uploads/2019-10/Data%20Breach%20Notification_Practical%20Guidance_Oct19.pdf. Acesso em: 13/07/2022.

V. A probabilidade de reversibilidade de pseudoanonimização ou perda de confidencialidade;

VI. A probabilidade de roubo de identidade, perda financeira, ou outras formas de uso inadequado dos dados pessoais;

VII. Se os dados pessoais podem ser usados de forma maliciosa;

VIII. A probabilidade de o incidente causar dano material, físico ou imaterial e a gravidade desse dano; e

IX. Se o incidente pode resultar em discriminação, dano reputacional ou prejuízo a direitos fundamentais dos titulares.

O guia da DPC esclarece que se o controlador deixar de considerar todos os fatores, pode avaliar o risco inadequadamente e, por conseguinte, pode haver subnotificação.

Por fim, na página na Internet da DPC sobre incidentes de segurança, a autoridade lista quatro categorias de risco:

i. Risco baixo: é improvável que o incidente tenha impacto nos indivíduos ou o impacto é mínimo.

ii. Risco médio: pode haver um impacto aos indivíduos, mas é improvável que o impacto seja substancial.

iii. Risco alto: o incidente pode ter impacto considerável nos indivíduos afetados.

iv. Risco grave: o incidente pode ter impacto crítico, extenso ou perigoso nos indivíduos afetados.

***A Commission Nationale de l'Informatique et des Libertés*** **(CNIL),** Autoridade de Proteção de Dados da França, em documento de 2018[11], relaciona os incidentes de segurança com a violação de dados definida no artigo 4.12 da RGPD, ou seja, "uma violação de segurança, acidental ou ilícita, que acarreta a destruição, a perda, a alteração, a divulgação não

[11] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS. **Security of Personal Data. The CNIL Guide's** - 2018. Disponível em: https://www.cnil.fr/sites/default/files/atoms/files/guide_security-personal-data_en.pdf. Acesso em: 02 jul. 2022.

autorizadas de dados pessoais transmitidos, armazenados ou tratados, ou acesso não autorizado a tais dados". Para o órgão, a violação de dados se refere a todo incidente de segurança, malicioso ou não, intencional ou não, que traga como consequência o comprometimento da integridade, da confidencialidade ou da disponibilidade de dados pessoais.

A CNIL cita como exemplos: a supressão acidental de dados médicos armazenados por um estabelecimento de saúde sem *backup* (disponibilidade); a perda uma chave USB, sem senha, com a cópia da base de dados de uma sociedade (confidencialidade), e a introdução maliciosa em uma base de dados escolar com a modificação dos resultados obtidos pelos alunos (integridade).

A avaliação do risco é feita conforme o caso concreto pelo controlador e deve considerar os seguintes elementos:

I. O tipo de violação (integridade, confidencialidade ou disponibilidade);
II. A natureza, a sensibilidade e o volume dos dados pessoais envolvidos;
III. A facilidade de se identificar as pessoas afetadas pela violação;
IV. As possíveis consequências aos titulares;
V. As características dos titulares (crianças, vulneráveis, etc.); e
VI. As características do controlador (natureza, papel, atividades).

**Na Austrália, o *Privacy Act 1988***[12] estabelece que um incidente de segurança deve ser notificado ("incidente elegível", traduzido livremente de "*eligible data breach*") se (i) ocorreu acesso não autorizado, divulgação não autorizada, ou perda de dados pessoais e (ii) o acesso, divulgação ou perda resultou em sério prejuízo para qualquer dos indivíduos afetados. A legislação também prevê exceções de notificação se o controlador adotar medidas que remediam o risco de prejuízo ao titular, bem como outras exceções relacionadas a setores e contextos específicos.

[12] OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER. **Privacy Act 1988.** Disponível em: https://www.legislation.gov.au/Series/C2004A03712. Acesso em: 10 ago.2022.

Ainda segundo o *Privacy Act* 1988, os seguintes fatores devem ser considerados na avaliação de se um incidente pode ou não resultar em sério prejuízo:

I. O tipo de dado;
II. A sensibilidade do dado;
III. Se os dados são protegidos por uma ou mais medidas de segurança;
IV. Caso o item anterior seja positivo, a probabilidade de que alguma dessas medidas possa ser superada;
V. As pessoas ou o tipo de pessoas que obtiveram ou podem obter os dados;
VI. Metodologias ou tecnologias de segurança usadas;
VII. A natureza do prejuízo; e
VIII. Qualquer outra questão relevante.

O ***Office of the Australian Information Commissioner*** **(OAIC)**, autoridade Australiana, também publicou o documento ***Data breach preparation and response – A guide to managing data breaches in accordance with the Privacy Act 1988***[13]***,*** de julho de 2019. O guia tem o objetivo de orientar controladores no gerenciamento de incidentes de segurança, inclusive em relação ao cumprimento da legislação.

Segundo o documento, um incidente de segurança envolvendo dados pessoais pode gerar prejuízos substanciais, sejam eles físicos ou psicológicos. O guia lista os seguintes exemplos:

I. Fraude financeira, incluindo transações não autorizadas com cartões de crédito ou fraude de crédito;
II. Roubo de identidade que cause perda financeira ou dano emocional e psicológico;
III. Violência familiar;

[13] OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER. **Data breach preparation and response A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth**). Disponível em: https://www.oaic.gov.au/ data/assets/pdf file/0017/1691/data-breach-preparation-and-response.pdf. Acesso em: 11 ago 2022.

IV. Dano físico ou intimidação.

O guia pontua também que um incidente de segurança pode afetar negativamente também a reputação do controlador. Contudo, o controlador pode reduzir o impacto reputacional se adotar medidas adequadas para minimizar o potencial dano.

Conforme o guia, toda entidade deve ter um plano de resposta a incidentes de segurança. Um plano de resposta, por sua vez, é o plano que estabelece as responsabilidades envolvidas no gerenciamento de um incidente de segurança e descreve os passos a serem tomados quando o incidente ocorre. O plano deve ser testado com frequência e atualizado quando necessário. O guia também detalha o que o plano de resposta a incidentes deve conter.

O guia resume a obrigação de notificar em três critérios:

I. Houve acesso não autorizado ou divulgação não autorizada de dados pessoais ou perda de dados;
II. É provável que resulte em prejuízo severo a um ou mais indivíduos;
III. O controlador não conseguiu evitar o risco de prejuízo severo com ações de remediação.

Em relação à etapa de avaliação, a OAIC explica em maior detalhe alguns dos fatores que devem ser levados em consideração ao se avaliar o risco. Sobre o tipo de dados pessoais, o guia lista os seguintes que podem aumentar o risco de prejuízo severo aos titulares:

I. Dados sensíveis, como dados de saúde;
II. Documentos geralmente usados para roubo de identidade;
III. Dados financeiros;
IV. A combinação de dados que permite saber mais sobre os indivíduos afetados.

Sobre as circunstâncias do incidente de segurança, a OAIC sugere que o controlador avalie o seguinte:

I. O tipo de pessoa cujo dado foi afetado, por exemplo, grupos vulneráveis;

II. A quantidade de indivíduos afetados. Quanto maior o número de indivíduos afetados por um incidente de segurança, maior a chance de pelo menos alguns deles sofrerem prejuízo severo.

III. Se as características do incidente revelam dados sensíveis, tanto pela natureza dos dados, quanto pela natureza do controlador. Se o controlador é, por exemplo, um prestador de serviço de saúde mental, a simples divulgação do nome de indivíduos pode gerar dano significativo;

IV. O período em que os dados pessoais ficaram acessíveis;

V. Se os dados pessoais estavam adequadamente encriptados, anonimizados ou de alguma outra maneira inacessíveis;

VI. Que pessoas ou entidades tiveram acesso aos dados.

Em relação à natureza do possível dano para o titular, a OAIC lista os seguintes exemplos:

I. Roubo de identidade;

II. Perda financeira significativa para o indivíduo;

III. Ameaça à segurança física do indivíduo;

IV. Perda de oportunidade de negócios ou de emprego;

V. Humilhação, dano à reputação ou a relacionamentos;

VI. Assédio moral no trabalho ou na vida social.

O guia australiano também explica que se o controlador adotou medidas para evitar danos ao titular, o incidente deixa de ser um "incidente elegível" *(eligible data breach*) e não há obrigação de notificação. São oferecidas também orientações a respeito de suspeitas de incidentes de segurança. Nesse sentido, se o controlador acredita que um incidente ocorreu e ele pode causar prejuízos severos a titulares, o incidente deve ser notificado. No caso de suspeitas, o controlador tem até 30 dias para completar a avaliação para concluir se houve ou não um incidente de segurança envolvendo dados pessoais. O guia aconselha, contudo, que a

análise seja feita com a maior brevidade possível para que potenciais danos possam ser mitigados.

Em relação à comunicação ao titular, o guia esclarece que sempre que houver um "incidente elegível", o controlador deve notificar tanto a autoridade quanto o titular. São listadas três opções para notificação ao titular:

I. Notificar todos os indivíduos afetados, caso não seja possível identificar aqueles que possuem maior probabilidade de sofrer danos;
II. Notificar apenas os indivíduos que podem sofrer prejuízos severos em decorrência do incidente, caso seja possível identificá-los;
III. Realizar notificação pública, por meio da publicação de sua notificação à autoridade em sua página na Internet, e tomar medidas para publicizar seu conteúdo.

O ***Amended Act on the Protection of Personal Information***[14] do Japão, no art. 22-2, estabelece que o controlador deve informar a Personal Information Protection Commission (PIPC), autoridade japonesa, quando houver vazamento, perda ou danos e outra situação de segurança no tratamento de dados pessoais em que existe uma grande possibilidade de prejuízo aos direitos e interesses dos titulares.

Segundo a legislação japonesa, o controlador também deve notificar o titular, a não ser que a comunicação se mostre difícil ou que o controlador tenha adotado as medidas necessárias para proteger os direitos e interesses dos titulares.

**O *Personal Information Protection and Electronic Documents Act* (PIPEDA) do Canadá**[15] exige que todos os incidentes de segurança envolvendo dados pessoais que tragam "riscos reais de danos significativos" aos titulares (independentemente do número de titulares afetados) sejam notificados à autoridade canadense (*Office of the Privacy Comissioner of Canada* - OPC) e aos titulares afetados, bem como sejam registrados pelas empresas.

[14] PERSONAL INFORMATION PROTECTION COMMISSION. **Amended Act on the Protection of Personal Information**. Disponível em: https://www.ppc.go.jp/files/pdf/APPI_english.pdf. Acesso em: 10 ago.2022.
[15] OFFICE OF THE PRIVACY COMISSIONER OF CANADA**. Personal Information Protection and Electronic Documents Act.** Disponível em: https://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html. Acesso em: 18 jul. 2022.

A legislação canadense define um incidente de segurança como sendo a perda, o acesso não autorizado ou vazamento não autorizado de dado pessoal resultante de uma violação das medidas de segurança de uma determinada empresa ou de uma falha na implementação dessas medidas.

A PIPEDA também define “dano significativo” como sendo dano físico, humilhação, prejuízo à reputação ou relacionamentos, perda de emprego ou de oportunidades de negócio ou profissionais, perda financeira, roubo de identidade, efeitos negativos em informações de crédito e danos ou perda de propriedade. A sensibilidade dos dados pessoais envolvidos no incidente e a probabilidade de que tenham sido, estão sendo ou serão objeto de uso indevido são fatores relevantes a ser considerados na avaliação de risco real de dano significante.

No que tange a sensibilidade, ao tratar do princípio do consentimento, a lei canadense traz, sem seu artigo. 4.3.4, que dados de saúde e financeiros são geralmente considerados sensíveis, enquanto todos os outros dependem do contexto. O OPC orienta que dados sobre origem étnica e racial, sobre opinião política, sobre vida e orientação sexual e sobre crenças religiosas ou filosóficas devem ser consideradas sensíveis de modo geral, bem como dados genéticos e biométricos.

Para a avaliação da probabilidade de uso indevido dos dados objetos de um incidente, o OPC relaciona diversas questões a serem consideradas, tais como quem e por quanto tempo teve acesso aos dados, se há indícios de intenções maliciosas, se os dados estão sob controle de alguém que possa oferecer risco reputacional, se os dados foram expostos a quem representa baixa probabilidade de fazer uso indevido, entre outras.

### 7.2 Alternativas possíveis ao enfrentamento do problema

Preliminarmente, cabe analisar o termo trazido pela LGPD no art. 48 que diz respeito ao incidente que possa acarretar “risco ou dano relevante aos titulares”.

Na tomada de subsídios foi abordado que poderia ser realizada uma definição separada de risco e dano, ao mesmo tempo que também houve contribuição no sentido de que a definição poderia ser feita de forma conjunta. No caso, a equipe de projeto optou por considerar a definição de forma conjunta do risco ou dano relevante.

O fato é que incidentes que “possam” ocasionar risco ou dano relevante ainda estão na contextualização e abrangência dos riscos que poderiam causar impacto aos interesses e direitos dos titulares, não sendo necessário a concretude do dano.

Ademais, a definição de forma conjunta facilita o entendimento a definição de risco que possa causar risco ou dano relevante.

Sobre os critérios para definição de risco ou dano relevante, tiveram contribuições na tomada de subsídios no sentido de manter alinhamento às experiências internacionais, considerando que existe vasta produção de documentos sobre o tema.

Nesse sentido, para a definição de incidentes que possam ocasionar risco ou dano relevante aos titulares, considerando a experiência internacional apresentada no item 7.1 deste relatório, podem ser utilizados os seguintes critérios:

- **Possibilidade de afetar significativamente interesses e direitos fundamentais dos titulares, sendo aqueles que possam:** i) impedir o exercício de direitos ou a utilização de um serviço; ou ii) ocasionar danos materiais ou morais aos titulares, tais como discriminação, violação à integridade física, ao direito à imagem e à reputação, fraudes financeiras ou roubo de identidade.
- **Dados em larga escala:** sendo caracterizados quando abrangerem número significativo de titulares, considerando, ainda, o volume de dados envolvidos e a extensão geográfica de localização dos titulares;
- **Dados sensíveis:** aqueles definidos no art. 5º, II da LGPD;
- **Dados de crianças, de adolescentes ou de idosos;**
- **Dados financeiros**: dado pessoal relacionado à vida financeira do titular, inclusive para contratação de serviços e aquisição de produtos;
- **Dados de autenticação:** considerando que seja qualquer dado pessoal utilizado em um processo para determinar se um usuário tem acesso permitido a um

sistema e/ou para confirmar a identidade de um usuário, tais como contas de login e senhas".[16]

Observa-se que vários critérios foram utilizados no regulamento de aplicação da LGPD ao agente de tratamento de pequeno porte para a definição de tratamento de alto risco. No entanto, por mais que a abordagem esteja fundamentada nos riscos que podem impactar interesses e direitos dos titulares, o contexto no presente caso é distinto, notadamente, os riscos que o incidente pode ocasionar ao titular de dados pessoais.

**Alternativa A: não regulamentação**

A alternativa C propõe que não haja intervenção regulatória, de modo que seja mantido o cenário regulatório atual.

Nesse sentido, não haveria definição de incidente que possa ocasionar risco ou dano relevante aos titulares.

[16]"Authentication is a process used for determining whether or not users are allowed access. In addition, authentication is a process used for confirming the identity of a user. That is, once a username is entered, the user must prove that this username really belongs to them." Extraído de: BOONKRONG, Sirapat. Authentication and Access Control: Practical Cryptography Methods and Tools. Berkeley: Apress, 2021, p. 46. Além disso, Chris Clifton afirma que "[…] authentication is used to ensure that an individual performing an action matches the expected identity. Authentication can be accomplished by a variety of mechanisms, each with advantages and drawbacks. These mechanisms fall into four main categories: 1. What you know—secret knowledge held only by the individual corresponding to the identity; 2. What you have—authentication requires an object possessed by the individual; 3. Where you are—the location matches the expected location; 4. What you are—biometric data from the individual" CLIFTON, Chris. Identity and Anonymity. In: BREAUX et al. Introduction to Privacy for Technology Professionals. Pourtsmouth: Hyde Park Publishing Services, 2020, p. 271. Por fim, outros autores listam uma série de dados pessoais que, a depender do contexto, podem ser considerados dados de autenticação: senhas, perguntas de segurança, foto de identificação (documentos oficiais), tokens, captcha, biometria (face, retina, digital), atributos comportamentais (ritmo da voz, forma de andar, ritmo de datilografia), localização, entre outros. Ver mais em: DASGUPTA, Dipankar; ROY, Arunava; NAG, Abhijit. Advances in User Authentication. Cham: Springer International Publishing, 2017, p. 2-36.

**Alternativa B: definição com base no contexto do tratamento e do incidente, que estabelece o risco ou dano com base em fatores como tipo de dado pessoal afetado, categoria de dados, quantidade de dados pessoais e/ou titulares afetados, dentre outros.**

A alternativa B consiste em estabelecer abordagem orientada com base em critérios relacionados aos dados envolvidos no incidente. Nesse sentido, a abordagem fica restrita a natureza e ao tipo de dado pessoal, como por exemplo, dados de saúde, dados financeiros, dados de autenticação em sistemas, dados de criança, de adolescentes e de idosos, bem como o número de titulares envolvidos, volume de dados, dentre outros.

**Alternativa C: definição com base no possível impacto aos interesses e direitos dos titulares.**

A alternativa C consiste em definir critérios unicamente relacionados diretamente ao impacto ao titular de dados pessoais, como por exemplo, dano material ou moral e impedimento de exercício de direitos e serviços. Observa-se que essa alternativa tem como único elemento o impacto aos interesses e direitos dos titulares para a definição de incidente com risco ou dano relevante.

**Alternativa D: combinação de critérios com base no contexto do incidente, levando em conta a natureza e categoria dos dados, e possível impacto aos interesses e direitos dos titulares.**

A alternativa D estabelece que seja necessária a ocorrência do critério central, ou seja, o possível dano material e moral ao titular e impedimento ao exercício de direitos ou à utilização de um serviço e além desse critério central, deve-se atender ao menos um critério específico relacionado à natureza e ao tipo de dado pessoal, como por exemplo, dados de

saúde, dados financeiros, dados de autenticação em sistemas, dados de criança, de adolescentes e de idosos. Inclui-se também como critério específico o incidente em larga escala, que leva em conta o número de titulares envolvidos, volume de dados, dentre outros.

### 7.3 Impactos regulatórios das alternativas identificadas

O impacto regulatório das alternativas está relacionado à abrangência da definição de acordo com os critérios definidos, ou seja, caso a definição seja mais abrangente, em tese, mais incidentes deverão ser comunicados à ANPD e ao titular ou, no caso contrário, menos comunicações deverão ser comunicados à ANPD e ao titular.

As análises devem considerar o impacto do custo operacional aos agentes de tratamento e ANPD, bem como a proteção de dados e privacidade do titular.

Observa-se que os incidentes comunicados à ANPD deverão ser analisados para avaliar a necessidade de determinações de providências, nos termos do art. 48, § 2º da LGPD, que por sua vez deverão ser acompanhadas pela Autoridade.

Dessa forma, diante do elevado custo operacional de acompanhamento pela ANPD dos incidentes notificados, bem como dos agentes de tratamento de dados, a LGPD adotou a abordagem de comunicação de incidentes que possam ocasionar risco ou dano relevante ao titular.

Na alternativa B, diante dos critérios com base no contexto do tratamento e do incidente, que estabelece o risco ou dano com base em fatores como tipo de dado pessoal afetado, categoria de dados, quantidade de dados pessoais e/ou titulares afetados, avalia-se que é bastante abrangente e pode causar fadiga ao processo de comunicação de incidentes de segurança, tanto pelos controladores quanto pelos titulares. No caso, essa alternativa pode trazer como consequência um elevado número de comunicações de incidentes que os agentes de tratamento deverão notificar à ANPD e ao titular sem possiblidade de acarretar risco ou dano relevante ao titular.

A título exemplificativo, o vazamento de tipos sanguíneos (dado sensível) de uma pessoa deveria ser comunicado à ANPD e ao titular. Cabe observar que esse dado, em tese, não tem potencial de causar risco ou dano relevante ao titular.

Além disso, o impacto gerado ao processo de comunicação de incidentes não garante uma atuação mais efetiva na garantia de proteção de dados e privacidade dos titulares.

Na alternativa C, diante do critério único de afetar aos interesses e direitos dos titulares, o impacto operacional aos agentes e à ANPD pode ser elevado, considerando a subjetividade desse critério. Por exemplo, o vazamento de dado qualquer que, teoricamente, possa ocasionar perda de exercício de direito ou cause algum dano, deve ser notificado à ANPD e ao titular.

Sob o aspecto do titular, a subjetividade pode levar a dificuldade na compreensão sobre o incidente que possa ocasionar risco ou dano relevante.

Na alternativa D, considerando a combinação de critérios com base no contexto do incidente, levando em conta a natureza e categoria dos dados, e possível impacto aos interesses e direitos dos titulares, observa-se equilíbrio maior entre a avaliação do incidente e o impacto que pode causar ao titular.

Sob o aspecto dos agentes de tratamento e a ANPD, a clareza dessa definição reduz o escopo dos incidentes considerados com risco ou dano relevante por meio de critérios mais objetivos, como por exemplo, dados financeiros e dados sensíveis, tende a colocar esforço e atuação em incidentes mais relevantes.

Sob o aspecto do titular, a condição primária de ser incidente que possa afetar significativamente interesses e direitos fundamentais dos titulares, orienta o tratamento de incidentes que realmente tem potencial de impacto aos titulares pela ANPD.

Por sua vez, a alternativa A, ao prever que não haja intervenção regulatória da matéria acarretaria maior insegurança jurídica aos regulados ante à utilização de conceito indeterminado pela LGPD, qual seja, “incidente de segurança que possa acarretar risco ou dano relevante aos titulares”. Ademais, a citada definição no regulamento decorre da necessidade para implementar a determinação legal (art. 48 da LGPD), de modo que a não emissão de ato regulatório representaria descumprimento da Lei. Diante do exposto, esta alternativa não será considerada para fins de comparação com as demais.

### 7.4 Comparação das alternativas consideradas

As comparações das alternativas serão realizadas por meio de tabela comparativa de avaliação dos modelos, com base em critérios considerados relevantes sob aspecto de impacto aos atores e construção do modelo.

Tabela 1: Comparação entre as alternativas

| Critério | Alternativa B (Contexto incidente) | Alternativa C (Contexto impacto ao titular) | Alternativa D (Contexto impacto ao titular + incidente) |
|---|---|---|---|
| **Impacto operacional na ANPD** | Risco de ter elevado número de comunicações de incidentes de baixo impacto aos titulares | Risco de ter elevado número de comunicações de incidentes, considerando a subjetividade do critério de o impacto aos interesses e direitos fundamentais | Maior equilíbrio no que concerne à abrangência de incidentes considerados com risco ou dano relevante ao titular<br>Possível redução de comunicação de incidentes, considerando o critério central de impactar interesses e direitos fundamentais |
| **Impacto aos titulares de dados** | Falta de elemento para avaliar o impacto aos interesses e direitos fundamentais dos titulares | Falta da abordagem do incidente, por exemplo, tipo de dados ou tipo de titulares, na definição | Orienta o modelo a considerar o incidente que cause impacto aos interesses e direitos fundamentais dos titulares, mas considera outros critérios relacionados aos incidentes |
| **Impacto ao agente de tratamento** | Modelo mais objetivo<br>Risco operacional de obrigação de comunicar elevado número de incidentes de baixo impacto aos titulares | Maior subjetividade ao modelo de definição de incidente com risco ou dano relevante<br>Risco operacional de ter elevado número de obrigações | Maior complexidade devido ao maior número de critérios<br>Possível redução do número de comunicação de incidentes para notificar |

| | | | |
|---|---|---|---|
| **Complexidade** | Complexidade mais baixa, tendo em vista critérios mais objetivos | Complexidade média, considerando a subjetividade do modelo | Complexidade considerável, tendo em vista o maior número de critérios |
| **Flexibilidade** | Modelo mais rígido, devido aos critérios objetivos | Maior flexibilidade devido à subjetividade o modelo | Maior flexibilidade devido a inclusão de critério subjetivo como elemento central. |
| **Dificuldade na construção e operacionalização do modelo** | Fácil operacionalização devido aos critérios mais objetivos | Média dificuldade de operacionalização devido ao caráter subjetivo do critério de impacto ao titular | Média dificuldade de operacionalização devido ao caráter subjetivo do critério de impacto ao titular |

Fonte: Elaboração própria (Coordenação-Geral de Normatização)

Diante da comparação dos modelos, observa-se que a alternativa D tem maior equilíbrio em refletir na regulamentação os incidentes que possam ocasionar maior risco ou dano relevante aos titulares, estando, portanto, mais aderente ao art. 48 da LGPD.

# 8 TEMA 2: DEFINIÇÃO DE PRAZOS

## 8.1 Experiência Internacional

Os artigos 33 e 34 do RGPD regulamentam a comunicação de violações de dados pessoais à autoridade e ao titular, respectivamente. O artigo 33 estabelece o seguinte em relação à obrigatoriedade de notificação e prazo:

> Em caso de violação de dados pessoais, o responsável pelo tratamento notifica desse fato a autoridade competente nos termos do artigo 55.o, sem demora injustificada e, sempre que possível, até 72 horas após ter tido conhecimento da mesma, a menos que a violação dos dados pessoais não seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares. Se a notificação à autoridade de controlo não for transmitida no prazo de 72 horas, é acompanhada dos motivos do atraso.
> O subcontratante notifica o responsável pelo tratamento sem demora injustificada após ter conhecimento de uma violação de dados pessoais. [17]

[17] COMISSÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à**

Assim, é estabelecido o prazo de 72 horas para que a autoridade seja comunicada de um incidente de segurança. Contudo, o art. 33 também estabelece que, caso todas as informações não estejam disponíveis, elas podem ser fornecidas por fases.

Em relação ao prazo de notificação de 72 horas, o ***Working Party 29*** **("WP29")** em parecer sobre a notificação de incidentes de segurança (*Opinion 03/2014 on Personal Data Breach Notification*)[18], explica que a contagem de tal prazo se inicia a partir do conhecimento do incidente pelo controlador. O conhecimento, por sua vez, ocorre quando o controlador "tem um grau razoável de certeza de que ocorreu um incidente de segurança que afetou dados pessoais". No caso de controladoria conjunta, o WP29 recomenda que esteja disposto em acordos contratuais quem será o responsável por comunicar incidentes de segurança. Já o operador deve notificar o controlador de uma violação de dados, conforme art. 33, n° 2, e o controlador deverá avaliar seu risco e obrigatoriedade de notificação. O documento recomenda que o operador notifique o controlador imediatamente para que este possa cumprir o prazo de 72 horas.

Além disso, o Considerando 85 explicita a importância da comunicação à autoridade no prazo de 72 horas:

> (85) Se não forem adotadas medidas adequadas e oportunas, a violação de dados pessoais pode causar danos físicos, materiais ou imateriais às pessoas singulares, como a perda de controlo sobre os seus dados pessoais, a limitação dos seus direitos, a discriminação, o roubo ou usurpação da identidade, perdas financeiras, a inversão não autorizada da pseudonimização, danos para a reputação, a perda de confidencialidade de dados pessoais protegidos por sigilo profissional ou qualquer outra desvantagem económica ou social significativa das pessoas singulares.
> Por conseguinte, logo que o responsável pelo tratamento tenha conhecimento de uma violação de dados pessoais, deverá notificá-la à autoridade de controlo, sem demora injustificada e, sempre que possível, no prazo de 72 horas após ter tido conhecimento do ocorrido, a menos que seja capaz de demonstrar em conformidade com o princípio da responsabilidade, que essa violação não é suscetível de implicar um risco para os direitos e liberdades das pessoas singulares.

**livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).** Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj Acesso em: 25/07/2022.

[18] ARTICLE 29 DATA PROTECTION WORKING PARTY. **Opinion 03/2014 on Personal Data Breach Notification. 2014**. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf. Acesso em: 19/07/2022

> Se não for possível efetuar essa notificação no prazo de 72 horas, a notificação deverá ser acompanhada dos motivos do atraso, podendo as informações ser fornecidas por fases sem demora injustificada. [19]

Em relação ao conteúdo da notificação, o artigo 33 estabelece que deve conter, pelo menos:

> I. 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;
> II. Comunicar o nome e os contatos do encarregado da proteção de dados ou de outro ponto de contacto onde possam ser obtidas mais informações;
> III. Descrever as consequências prováveis da violação de dados pessoais;
> IV. 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. [20]

O art. 33 estabelece, ainda, que o controlador deverá documentar quaisquer violações de dados pessoais, incluindo os fatos "relacionados com as mesmas, os respectivos efeitos e a medida de reparação adotada".

O Considerando 86 estabelece diretrizes para a comunicação ao titular:

> (86) O responsável pelo tratamento deverá informar, sem demora injustificada, o titular dos dados da violação de dados pessoais quando for provável que desta resulte um elevado risco para os direitos e liberdades da pessoa singular, a fim de lhe permitir tomar as precauções necessárias.
> A comunicação deverá descrever a natureza da violação de dados pessoais e dirigir recomendações à pessoa singular em causa para atenuar potenciais efeitos adversos.
> Essa comunicação aos titulares dos dados deverá ser efetuada logo que seja razoavelmente possível, em estreita cooperação com a autoridade de controlo e em cumprimento das orientações fornecidas por esta ou por outras autoridades competentes, como as autoridades de polícia.
> Por exemplo, a necessidade de atenuar um risco imediato de prejuízo exigirá uma pronta comunicação aos titulares dos dados, mas a necessidade de aplicar medidas

[19] COMISSÃO EUROPEIA. **Regulamento(UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados).** Disponível em: https://eur-lex.europa.eu/legalcontent/PT/TXT/HTML/?uri=CELEX:32016R0679&from=PT. Acesso em: 10/08/2022.
[20] *Ibidem*.

> adequadas contra violações de dados pessoais recorrentes ou similares poderá justificar um período mais alargado para a comunicação.[21]

O Considerando 87 fornece, ainda, outros esclarecimentos em relação à notificação de incidentes de segurança e a possibilidade de intervenção da autoridade

> (87) Há que verificar se foram aplicadas todas as medidas tecnológicas de proteção e de organização para apurar imediatamente a ocorrência de uma violação de dados pessoais e para informar rapidamente a autoridade de controlo e o titular.
> Para comprovar que a notificação foi enviada sem demora injustificada importa ter em consideração, em especial, a natureza e a gravidade da violação dos dados pessoais e as respetivas consequências e efeitos adversos para o titular dos dados.
> Essa notificação poderá resultar numa intervenção da autoridade de controlo em conformidade com as suas funções e competências, definidas pelo presente regulamento.[22]

A ***Agencia Española de Protección de Datos (AEPD)*** publicou o ***Guía para la notificación de brechas de datos personales***[23], que busca estabelecer diretrizes para a notificação de incidentes de segurança, que recorda que o RGPD estabelece o prazo de 72 horas e prevê, ainda, que caso não seja possível prestar todas as informações em nesse prazo, o controlador deverá completar sua notificação em até 30 dias úteis.

A comunicação do incidente à autoridade deverá ser feita eletronicamente e o controlador poderá receber pedido de novas informações e/ou determinação de que notifique os titulares afetados. A confirmação de notificação deverá se dar por registro eletrônico e o controlador terá, em regra, 30 dias para executá-la, podendo esse prazo ser diminuído em função do nível de risco.

---

[21] COMISSÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/LSU/?uri=CELEX:32016R0679. Acesso em: 19 jul. 2022.

[22] *Ibidem*.

[23] AGENCIA ESPAÑOLA PROTECCIÓN DATOS**. Guía para la notificación de brechas de datos personales**, 2021. Disponível em : https://www.aepd.es/sites/default/files/2019-09/guia-brechas-seguridad.pdf Acesso em:18 fev. 2022.

O ***Personal Information Protection and Electronic Documents Act*** [24] **(PIPEDA) do Canadá** exige que todos os incidentes de segurança envolvendo dados pessoais que tragam "riscos reais de danos significativos" aos titulares (independentemente do número de titulares afetados) sejam notificados ao ***Office of the Privacy Comissioner of Canada*** **(OPC)**, a autoridade canadense e aos titulares afetados, bem como sejam registrados pelas empresas.

A notificação deve ser feita "tão logo que possível", sem definição concreta do prazo, por meio de formulário eletrônico que poderá ser aditado no caso de novas informações e enviado por qualquer meio de comunicação seguro. Para os titulares, deverá ser feita de forma clara e direta. Exceções para a comunicação direta estão elencadas na lei e incluem: (i) possibilidade de maior dano ao titular; (ii) dificuldade excessiva para a organização, ou (iii) indisponibilidade dos dados de contato do titular afetado. A comunicação indireta deverá ser feita por comunicação pública ou modo similar que possa alcançar todos os titulares envolvidos, tais como anúncios em jornais online e offline e avisos destacados no site da organização ou em outro tipo de presença digital/online.

Na legislação canadense, as empresas também são obrigadas a notificar outras empresas ou órgãos governamentais que possam reduzir o risco de dano ou o dano resultante do incidente de segurança, como autoridades policiais ou uma empresa que processa os pagamentos da organização afetada, por exemplo.

O conteúdo da notificação, conforme definido em regulamento, deverá conter:

> (a) descrição das circunstâncias do incidente e a causa, caso conhecida;
> (b) dia ou período durante o qual o incidente ocorreu (podendo ser aproximado, caso não seja identificado);
> (c) descrição dos dados pessoais afetados;
> (d) número exato ou aproximado de titulares afetados (apenas nas notificações à OPC);
> (e) descrição das medidas tomadas pela organização para reduzir o risco de dano ou o dano aos titulares afetados;
> (f) descrição das medidas tomadas ou a serem tomadas pela organização para notificar os titulares, no caso de notificação à OPC, ou das medidas que os titulares poderão tomar para reduzir o risco de dano ou o dano que poderá se resultar do incidente, no caso de notificação aos titulares, e

[24] OFFICE OF THE PRIVACY COMISSIONER OF CANADA. **Personal Information Protection and Electronic Documents Act.** Disponível em: https://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html. Acesso em: 05 ago. 2022.

(g) dados de contato para mais informações. [25]

A legislação também obriga que o controlador mantenha registro de todos os incidentes de segurança por dois anos, o que deverá ser analisado pelo OPC no caso de uma fiscalização, até mesmo para avaliar se foi considerada a necessidade de notificação, ou seja, o risco real de dano significante. Os registros devem conter, no mínimo: (i) data exata ou estimada do incidente; (ii) descrição geral das circunstâncias em que o incidente ocorreu; (iii) natureza dos dados envolvidos, e (iv) se o incidente foi notificado ao OPC e aos titulares.

A responsabilidade por notificar incidentes cabe ao controlador, conforme orientação da autoridade canadense. Ocorre que a legislação determina que uma organização deve notificar, nos casos cabíveis, os incidentes de segurança com dados pessoais sob seu controle, sem definir claramente "controle", o que gera ambiguidade. Assim, em uma leitura conjunta com o que dispõe o art. 4.1.3, no que concerne o princípio de *accountability*, e considerando as práticas de negócios existentes, a autoridade nacional interpreta ser o controlador o responsável pela notificação e sugere que haja dispositivos contratuais suficientes com o processador para que o controlador possa cumprir suas obrigações de notificação e de registro de incidentes. De qualquer forma, o OPC ressalta que a avaliação deverá ser feita no caso concreto tendo em vista as complexidades das relações comerciais atuais.

Na mesma linha, o *Privacy Act 1988*[26] estabelece que o controlador deve notificar o ***Office of the Australian Information Commissioner*** **(OAIC), autoridade australiana,** assim que possível depois que o controlador tomar conhecimento do incidente. O controlador também deve notificar os titulares individualmente, se factível, do conteúdo de sua notificação à autoridade. Caso contrário, deve fazer anúncio público em sua página na Internet ou tomar outras medidas para publicizar o conteúdo de sua notificação. O OAIC também pode determinar que um controlador a notifique de um incidente de segurança ou notifique o titular.

[25] OFFICE OF THE PRIVACY COMISSIONER OF CANADA. **Personal Information Protection and Electronic Documents Act.** Disponível em: https://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html. Acesso em: 05 ago. 2022.

[26] OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER. **Privacy Act 1988**. Disponível em: https://www.legislation.gov.au/Series/C2004A03712. Acesso em 06/08/2022.

A forma da notificação ao titular pode ser modificada conforme a necessidade, mas ela deve conter o conteúdo da notificação à autoridade. Não há prazo específico para a comunicação ao titular, mas ela também deve ser feita assim que possível e pode, inclusive, ser feita antes da notificação ao OAIC.

A notificação ao OAIC deve incluir:

> I. A identificação e informação de contato do controlador;
> II. A descrição do incidente de segurança, que, por sua vez, pode conter:
> III. A data e período do incidente
> IV. A data em que o controlador identificou o incidente
> V. As circunstâncias do incidente
> VI. Quem obteve acesso ou pode obter acesso aos dados pessoais
> VII. Informações relevantes sobre as medidas tomadas pelo controlador para remediar o incidente;
> VIII. O tipo de dado pessoal afetado pelo incidente de segurança;
> IX. Que medidas o controlador recomenda que os titulares adotem em resposta ao incidente.[27]

Quando outras entidades estiverem envolvidas no incidente, é útil incluir na notificação sua identificação e a maneira como elas estão envolvidas no incidente.

O OAIC sempre acusará o recebimento de notificações de incidente de segurança e pode requisitar mais informações ou orientar o controlador a respeito do incidente. Para isso, levará em consideração:

> I. Se o incidente de segurança foi contido ou está em processo de ser contido;
> II. Se o controlador está adotando medidas para mitigar o impacto do incidente nos indivíduos afetados;
> III. Se o controlador está adotando medidas para evitar que um incidente similar ocorra novamente.

O OAIC também tem poderes para aceitar um acordo oferecido pelo controlador, determinar medidas, solicitar uma liminar e solicitar que penas pecuniárias sejam aplicadas ao controlador. Contudo, o OAIC afirma que prefere trabalhar em conjunto com os agentes para incentivar e facilitar a conformidade com a legislação de privacidade.

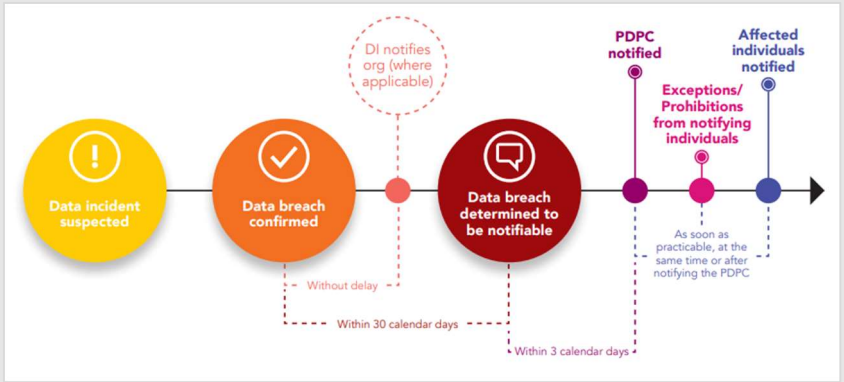
[27] *Ibidem.*

O OAIC pode, ainda, determinar que um incidente de segurança seja notificado ou declarar que um incidente não precisa ser notificado.

Por fim, o guia afirma que o OAIC oferece orientações gerais sobre o *Privacy Act,* mas não presta orientações sobre casos de incidentes específicos.

Em Singapura, o ***Personal Data Protection Act 2012***[28] prevê que a notificação do incidente deve ser realizada à ***Personal Data Protection Commission*** assim que for possível, mas, em qualquer caso, em até três dias corridos após a avaliação de que aquele incidente seja notificável. É informado, ainda, que as organizações devem avaliar se o incidente é notificável em um prazo de 30 dias corridos a partir da data que tomou conhecimento do fato. Em relação à notificação aos titulares afetados, é previsto que ocorra assim que possível no mesmo momento em que for notificada a autoridade ou após.

Figura 2: Notificação de Incidentes - *Personal Data Protection Act 2012*




Fonte: *Personal Data Protection Commission* (2021)

**A *Commission Nationale de l'Informatique et des Libertés* (CNIL), autoridade de proteção de dados da França,** determina que a obrigação de notificação das violações de dados mencionadas observará o definido nos artigos 33 e 34 da RGPD e, portanto, dependerá do risco que possa acarretar aos direitos e liberdades individuais. Se não houver riscos, o controlador deve apenas registrar internamente a violação, o que poderá ser objeto de fiscalização posterior pela CNIL.

[28] Art. 26 D (1) **Personal Data Protection Act 2012**. Disponível em: https://sso.agc.gov.sg/Act/PDPA2012?ProvIds=P16A-#pr26D-https://www.msn.com/pt-br/?pc=ACTE. Acesso em: 05/08/2022.

A autoridade francesa relaciona os itens que devem estar contidos no registro interno de incidentes:

I. A natureza do incidente;
II. As categorias e o número aproximado de titulares envolvidos;
III. As categorias e o número aproximado de bancos de dados envolvidos;
IV. As possíveis consequências do incidente;
V. As medidas tomadas para remediar o incidente e, caso aplicável, limitar suas consequências negativas;
VI. A justificativa da não notificação, caso aplicável.

Quando há risco, além do registro, o controlador deve notificar a CNIL em até 72 horas. Nos casos de risco elevado, os titulares também deverão ser comunicados com a brevidade possível, a não ser que:

I. Os dados estejam protegidos por medidas apropriadas e estejam incompreensíveis para pessoas sem autorização de acesso;
II. O controlador tenha tomado medidas posteriores que garantam que o risco elevado não poderá se materializar, e
III. A comunicação exigirá esforços desproporcionais, bastando, nesse caso, uma comunicação pública ou medida similar.

A CNIL ilustra casos para os quais não seria necessária a notificação: a divulgação de dados já públicos, a supressão de dados protegidos e imediatamente restaurados, a perda de dados protegidos por um algoritmo de encriptação desde que a senha do código não esteja comprometida e uma cópia dos dados esteja disponível. Adicionalmente, a autoridade se dispõe a esclarecer dúvidas sobre a necessidade de se notificar os titulares.

A notificação deve conter, no mínimo, os mesmos elementos do registro interno de incidentes, além dos dados de contato da pessoa responsável (encarregado ou outro) e é feito por meio de formulário digital exclusivo, nos prazos determinados pelo RGPD. A CNIL ressalta que casos de ataque cibernético devem ser reportados às autoridades de segurança pública competentes.

No que se refere ao operador, este deve notificar o controlador sobre qualquer incidente tão logo tenha conhecimento de forma que o último possa cumprir com suas obrigações em relação à matéria. Na prática, a autoridade recomenda que tal obrigação do operador em relação ao controlador esteja prevista no contrato celebrado entre ambos.

O operador também poderá agir em nome do controlador (a seu pedido) para notificar à CNIL nos casos em que o controlador avalie que o incidente pode representar um risco aos

titulares envolvidos. Ainda assim, a obrigação do operador de informar o controlador permanece, bem como a obrigação do controlador de efetuar os registros internos cabíveis e avaliar a necessidade de notificação em função do risco estimado.

Após a notificação, a CNIL instrui o processo e poderá encerrá-lo caso constate que: i) o incidente não atingiu os dados pessoais ou não coloca em risco direitos e liberdades individuais; ii) os titulares foram devidamente informados, e iii) as medidas técnicas de segurança, aplicadas anteriormente ao incidente, foram adequadas.

A CNIL também poderá determinar que os titulares sejam informados caso perceba que não o foram e/ou as medidas de segurança aplicadas anteriormente ao incidente não foram adequadas.

De forma geral, no que se refere a incidentes de segurança, cabe à CNIL exercer o papel de acompanhamento dos controladores que receberão orientações sobre medidas de segurança a serem implementadas para encerrar o incidente ou minimizar seus efeitos, e sobre a necessidade de notificação aos titulares, bem como o papel de fiscalização das obrigações do controlador, tais como o registro interno, a avaliação de risco, o cumprimento dos prazos e do conteúdo da notificação. Caso necessário, poderão ser aplicadas sanções e determinar que o controlador notifique os titulares.

Nos dois casos, a avaliação da CNIL poderá se debruçar sobre o nível geral de segurança do tratamento de dados que o incidente vier a revelar.

Por fim, a CNIL esclarece que, no caso de tratamento de dados transfronteiriço, a notificação deverá ser feita à autoridade supervisora principal. De qualquer forma, ao informar, no formulário eletrônico da CNIL, se tratar de um incidente que afeta um tratamento de dados transfronteiriço, deverá ser indicado quais outros países da União Europeia estão envolvidos e a CNIL se encarregará de informar as demais autoridades.

### 8.2 Alternativas possíveis ao enfrentamento do problema

Inicialmente, cumpre analisar o termo trazido pelo §1º do art. 48 da LGPD ao tratar do prazo para comunicação à autoridade nacional e ao titular quanto a ocorrência de incidente que possa acarretar risco ou dano ou risco relevante a este. Consoante a lei, a referida

comunicação deverá ser realizada em prazo “razoável”, conforme definido pela autoridade nacional e deverá mencionar no mínimo os elementos elencados no §1º.

No tocante à fixação de prazo razoável para tal comunicação perante a ANPD, na tomada de subsídios várias contribuições sugeriram 72 horas, conforme estabelecido no RGPD da União Europeia. Outras contribuições mencionaram o Decreto n° 9.936, de 24 de julho de 2019, art. 18, §1º, que determina que incidentes de segurança que possam causar “riscou ou prejuízo relevante aos cadastrados” sejam notificados à ANPD em dois dias úteis. Houve, ainda, sugestão de prazos mais curtos (24 horas) e mais longos (de até 30 dias, conforme a autoridade australiana). Além disso, muitas contribuições sugeriram que a notificação fosse realizada em etapas, em que o controlador pudesse fornecer informações à ANPD em pelos menos duas fases, a primeira imediatamente após a ciência do incidente e a segunda depois que o controlador possuísse mais informações a respeito do ocorrido. Em relação ao termo inicial, sugeriu-se a “ciência do incidente”.

Na definição do que possa ser considerado como “prazo razoável” para comunicação do incidente, verifica-se que essa deverá ocorrer o mais breve possível, considerando, ainda, a necessidade de avaliação prévia por parte do controlador no tocante à classificação do incidente quanto ao risco ou dano relevante que possa ocasionar.

Uma vez ponderados tais fatores, discute-se se a notificação deva ocorrer em etapa única, valendo-se de um prazo mais longo para tanto, ou se poderia ocorrer em prazo mais exíguo, mas com a previsão de complementação em caso de impossibilidade de fornecimento das informações no prazo previsto, mediante justificativa, ou, ainda, em etapa única valendo-se de um prazo exíguo.

Nesse sentido, para a definição do prazo para notificação perante a Autoridade, considerando a experiência internacional apresentada no item 8.2 deste relatório, podem ser utilizados as seguintes alternativas:

**Alternativa A: não regulamentação**

A alternativa A propõe que não haja intervenção regulatória, de modo que seja mantido o cenário regulatório atual.

Vale mencionar que enquanto pendente de regulamentação, recomendou-se, a título indicativo, que o prazo para comunicação de incidente que pudesse causar risco ou dano relevante aos titulares fosse de 2 dias úteis [29]contados da data do conhecimento do incidente, à semelhança do parâmetro definido no Decreto nº 9936, de 24 de julho de 2019, o qual regulamenta a Lei nº 12.414, de 9 de junho de 2011, que disciplina a formação e a consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito.

**Alternativa B: fixação de prazo comum para comunicação à ANPD e ao titular em etapa única.**

A alternativa B propõe que haja a fixação de prazo para a realização de notificação em etapa única.

No que tange à definição do prazo para comunicação do controlador de dados à ANPD e ao titular, busca-se a fixação de prazo que seja suficientemente célere, de modo a mitigar os danos gerados pelo incidente aos titulares, considerando, ainda, previsão de análise do incidente por parte do controlador quanto a classificação deste quanto ao risco e relevante.

Considerando a análise da experiência internacional ora realizada, e, para fins de harmonização da forma de contagem de prazo prevista na Resolução CD/ANPD nº 1, de 28 de outubro de 2021, a qual aprova o Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados, sugere-se a determinação do prazo de até 3 (três) dias úteis, a contar da ciência do incidente que possa acarretar risco ou dano ou risco relevante ao titular, para que seja realizada a comunicação perante a ANPD, bem como ao titular.

Aos agentes de tratamento de pequeno porte, em regra, aplica-se o disposto no art. 14, III, da Resolução CD/ANPD nº 2, de 27 de janeiro de 2022, a qual aprova o Regulamento de aplicação da LGPD, para agentes de tratamento de pequeno porte, de modo que será concedido prazo em dobro para comunicação à ANPD e ao titular de dados pessoais da

[29] AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Comunicação de incidentes de segurança. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca. Acesso em: 01 set. 2022.

ocorrência de incidente de segurança que possa acarretar risco ou dano relevante a estes, exceto caso houver potencial comprometimento à integridade física ou moral dos titulares ou à segurança nacional, devendo, nesses casos, a comunicação atender aos prazos conferidos aos demais agentes de tratamento.

**Alternativa C: fixação de prazo inicial comum para comunicação à ANPD e ao titular, acrescido de previsão para complementação da notificação, mediante justificativa, para comunicação à ANPD.**

A alternativa C propõe a fixação de prazo inicial comum para comunicação à ANPD e ao titular de dados pessoais, mas com possibilidade de que seja previsto prazo para, excepcionalmente, ocorrer a complementação das informações solicitadas pela Autoridade, mediante justificativa.

Sugere-se igualmente a determinação do prazo inicial de até 3(três) dias úteis a contar da ciência do incidente que possa acarretar risco ou dano ou risco relevante ao titular, para que seja realizada a comunicação à ANPD e ao titular de dados pessoais.

Todavia, em relação à comunicação à ANPD, excepcionalmente, as informações poderão ser complementadas no prazo de 20 (vinte) dias úteis, prorrogável uma vez, por igual período, mediante justificativa.

Esse prazo justifica-se pelas experiências internacionais, quando abordam a complementação das informações, bem como se harmoniza com a prática atual da ANPD em conceder um prazo de 30 (trinta) dias para envio de complemento de informações.

Aos agentes de tratamento de pequeno porte, aplica-se o disposto no art. 14, III, da Resolução CD/ANPD nº 2, de 27 de janeiro de 2022, a qual aprova o Regulamento de aplicação da LGPD, para agentes de tratamento de pequeno porte, de modo que será concedido prazo em dobro para comunicação à ANPD e ao titular de dados pessoais da ocorrência de incidente de segurança que possa acarretar risco ou dano relevante a estes, exceto quando houver potencial comprometimento à integridade física ou moral destes ou à segurança nacional, devendo, nesses casos, a comunicação atender aos prazos conferidos aos demais agentes de tratamento.

## 8.3 Impactos regulatórios das alternativas identificadas

O impacto regulatório das alternativas está relacionado com a razoabilidade do prazo da comunicação e seus efeitos para o titular de dados pessoais, bem como a viabilidade de cumprimento da comunicação do controlador a ele e à ANPD.

Dessa forma, avaliam-se a seguir as alternativas regulatórias.

Na alternativa B, propõe-se que haja a de prazo comum para comunicação à ANPD e ao titular em etapa única, isto é, sem possibilidade de prorrogação de prazo para fins de complementação das informações ora exigidas.

Considerando a adoção do prazo de até 3 (três) dias úteis para notificação, tal alternativa, se adotada, pode eventualmente se mostrar insuficiente para casos de incidentes mais complexos, em que o controlador necessite de prazo maior para avaliação e encaminhamento das informações ora solicitadas. Ainda que se observe a necessidade de uma comunicação com a maior brevidade possível, a comunicação imediata de incidente, sem que haja tempo hábil para análise do controlador quanto à classificação do incidente, isto é, se este é passível de causar risco ou dano relevante ao titular, os quais são fatores determinantes para que surja o dever de comunicação, pode acarretar volume de comunicações desnecessárias perante a Autoridade, de modo a inviabilizar a sua atividade fiscalizatória.

Além disso, corre-se o risco de que uma vez não avaliado o incidente quanto a tais aspectos, a comunicação possa até mesmo gerar maior ansiedade aos titulares, diante da falta de informações adequadas. Por outro lado, supondo que houvesse a definição de um prazo mais longo para a realização de comunicação em etapa única, poderia se revelar igualmente prejudicial tanto sob a perspectiva de atuação da ANPD, quanto para o titular, considerando que a demora na comunicação poderia ensejar o agravamento dos riscos e danos ocasionados pelo incidente perante ele. Assim, a atuação do controlador deve ser célere o suficiente para que a Autoridade possa adotar medidas para salvaguardar os direitos dos titulares ante a gravidade do incidente.

Nesse sentido, a alternativa C propõe que haja prazo inicial comum para comunicação à ANPD e ao titular, acrescido de previsão para complementação da notificação, mediante justificativa, para comunicação à ANPD.

Tal alternativa parte do pressuposto de que há incidentes cujo grau de complexidade não permitiria a identificação de todas as informações mínimas exigidas no art. 48, §1º da LGPD em um prazo de até 3 (três) dias úteis. Assim, a fixação de um prazo único, sem possibilidade de dilação, não seria capaz de contemplar diferentes graus de complexidade de incidentes, o que, eventualmente, poderia até mesmo inviabilizar o objetivo previsto na lei, uma vez que prevê obrigação de notificação somente quanto aqueles incidentes passíveis de acarretar dano ou risco relevante aos titulares e não a todo e qualquer incidente de segurança com dados pessoais.

Vale observar que tal medida se aplicaria apenas no que tange à comunicação do controlador à ANPD, não incidindo sobre a comunicação aos titulares, a qual deve ocorrer impreterivelmente no prazo de até 3 (três) dias úteis, a contar da ciência do incidente por parte do controlador.

Por sua vez, a alternativa A, ao prever que não haja intervenção regulatória da matéria acarretaria maior insegurança jurídica aos regulados ante à utilização de conceito indeterminado pela LGPD, qual seja, “prazo razoável”. Ademais, a necessidade de definição de referido prazo por parte da ANPD decorre de determinação legal (art. 48, §1º), de modo que a não emissão de ato regulatório representaria descumprimento da Lei. Diante do exposto, esta alternativa não será considerada para fins de comparação com as demais.

### 8.4 Comparação das alternativas consideradas

As comparações das alternativas serão realizadas por meio de tabela comparativa de avaliação dos modelos, com base em critérios considerados relevantes sob aspecto de impacto aos atores e construção do modelo.

Tabela 2: Comparação entre as alternativas

| Critério | Alternativa B | Alternativa C |
|---|---|---|
| **Impacto operacional na ANPD** | Risco de haver elevado número de comunicações contendo informações incompletas e/ou que não se enquadrem na classificação prevista no art. 48 da LGPD.<br><br>Risco de ter elevado número de descumprimento do prazo de comunicação de incidentes que não se enquadrem na classificação prevista no art. 48 da LGPD. | Maior robustez dos elementos informativos encaminhados à ANPD por meio da comunicação.<br><br>Risco de morosidade do tratamento do incidente comunicado à ANPD. |
| **Impacto aos titulares de dados** | Risco de recebimento de volume expressivo de comunicações que não necessariamente causem risco ou dano relevante. | Risco semelhante à alternativa A.<br><br>(Não se aplica o prazo para complementação de informações no que tange à comunicação do controlador aos titulares, mas tão somente à ANPD.) |
| **Impacto ao agente de tratamento** | Risco de impossibilidade de obtenção das informações necessárias no prazo estabelecido e consequentemente de classificação do incidente. | Possibilidade de prazo adicional para complementação de comunicação à ANPD, mediante justificativa. |
| **Flexibilidade** | Maior rigidez, devido à realização de comunicação em etapa única, sem possibilidade de dilação de prazo para complementação das informações exigidas. | Maior flexibilidade, diante da possibilidade de complementação das informações em prazo determinado. |

Fonte: Elaboração própria (Coordenação-Geral de Normatização)

Diante da comparação das alternativas, observa-se que a alternativa C proporciona maior equilíbrio ao possibilitar que haja complementação da comunicação à ANPD, não aplicando-se tal prorrogação de prazo quanto à comunicação aos titulares. Entende-se que tal alternativa é mais razoável, quando comparada com a alternativa B, e, portanto, mais aderente ao art. 48 da LGPD.

# 9 TEMA 3: TRATAMENTO DOS INCIDENTES NOTIFICADOS À ANPD

## 9.1 Experiência Internacional

O art. 34 do RGPD estabelece que a autoridade pode determinar que o titular seja comunicado caso entenda que o incidente de segurança gera um elevado risco e o controlador não tiver feito tal comunicação.

Em relação a como avaliar a gravidade do incidente de segurança, a ***European Union Agency for Network and Information Security*** **(ENISA)** [30] publicou em 2013 documento com recomendações para uma metodologia de avaliação da gravidade de um incidente de segurança. Em tal documento, a gravidade do incidente é definida como a estimativa da magnitude do impacto potencial do incidente para os titulares de dados. Assim, três elementos devem ser levados em consideração:

- O contexto de tratamento dos dados pessoais – tipo de dados pessoais ajustado ao contexto em que são tratados
- Facilidade de identificar indivíduos com base no incidente de segurança
- Circunstâncias do incidente de segurança

A pontuação final da gravidade do incidente de segurança é dada pela seguinte equação:

| |
|---|
| GRAVIDADE DO INCIDENTE DE SEGURANÇA = CONTEXTO DO TRATAMENTO DE DADOS PESSOAIS x FACILIDADE DE IDENTIFICAÇÃO DE INDIVÍDUOS + CIRCUNSTÂNCIAS DO INCIDENTE |

Em relação ao contexto do tratamento de dados pessoais, os dados seriam primeiro classificados em uma de quatro categorias: simples, comportamental, financeiro e sensível. Cada categoria tem uma nota padrão atribuída (1, 2, 3 e 4, respectivamente), que é ajustada de acordo com fatores específicos, como características do controlador e/ou do titular,

[30] EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY. **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 fev. 2022.

natureza e volume dos dados ou se os dados pessoais já eram públicos. Dessa forma, a nota pode ser aumentada ou diminuída de acordo com fatores específicos do tratamento de dados.

A facilidade de identificação possui quatro níveis: negligenciável, limitada, significante e máxima, que pode tomar valores de 0,25, 0,5, 0,75 e 1, respectivamente. Esse fator deve ser considerado de acordo com o contexto do incidente e do tratamento de dados pessoais. O documento da ENISA apresenta uma série de exemplos de dados pessoais e seus valores considerando diferentes contextos.

Os elementos que são considerados na "Circunstâncias do Incidente" são: perda de confidencialidade, perda de integridade, perda de disponibilidade e intenção maliciosa. A depender das circunstâncias concretas do incidente de segurança, o valor desse fator pode ser de 0, 0,25 ou 0,5. O último elemento, "intenção maliciosa", é considerado um fator que aumenta as chances de dados pessoais serem usados de maneira danosa, já que quando há uma intenção maliciosa, o uso prejudicial de dados pessoais geralmente é o propósito do incidente de segurança. Nesse caso, acrescenta-se o valor de 0,5.

Aplicando os valores descritos na fórmula, obtém-se uma nota para a gravidade do incidente. A nota indicará o nível de gravidade, conforme a Figura 3 abaixo.

Figura 3 - Gravidade do Incidente de Segurança - metodologia ENISA

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

Fonte: Recommendations for a methodology of the assessment of severity of personal data breaches[31].

Após a aferição do nível de gravidade, alguns indicadores ("flags", como chamado no documento) podem ser acrescentados para sinalizar a importância do incidente de segurança. O documento da ENISA lista dois indicadores: (i) número de indivíduos afetados ultrapassa 100; e (ii) dados ininteligíveis.

A ENISA afirma que a metodologia desenvolvida pode ser utilizada por controladores para comunicar às autoridades incidentes de segurança e para que as autoridades determinem se é necessário comunicar os titulares de dados pessoais envolvidos.

A ***Agencia Española de Protección de Datos (AEPD)*** publicou o ***Guía para la notificación de brechas de datos personales***,[32] no qual informa que o controlador poderá receber pedido de novas informações e/ou determinação de que notifique os titulares

[31] EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY. **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 fev. 2022.

[32] AGENCIA ESPAÑOLA PROTECCIÓN DATOS. **Guía para la notificación de brechas de datos personales**. 2021. Disponível em: https://www.aepd.es/sites/default/files/2019-09/guia-brechas-seguridad.pdf Acesso em: 03 ago.2022.

afetados. A confirmação de notificação deverá se dar por registro eletrônico e o controlador terá, em regra, 30 dias para executá-la, podendo esse prazo ser diminuído em função do nível de risco.

**A *Commission Nationale de l'Informatique et des Libertés* (CNIL)**, por sua vez, após receber a notificação do incidente, instrui o processo e poderá encerrá-lo caso constate que: i) o incidente não atingiu os dados pessoais ou não coloca em risco direitos e liberdades individuais; ii) os titulares foram devidamente informados, e iii) as medidas técnicas de segurança, aplicadas anteriormente ao incidente, foram adequadas.

A CNIL também poderá determinar que os titulares sejam informados caso perceba que não o foram e/ou as medidas de segurança aplicadas anteriormente ao incidente não foram adequadas.

De forma geral, no que se refere a incidentes de segurança, cabe à CNIL exercer o papel de acompanhamento dos controladores que receberão orientações sobre medidas de segurança a serem implementadas para encerrar o incidente ou minimizar seus efeitos, e sobre a necessidade de notificação aos titulares, bem como o papel de fiscalização das obrigações do controlador, tais como o registro interno, a avaliação de risco, o cumprimento dos prazos e do conteúdo da notificação. Caso necessário, poderão ser aplicadas sanções e determinar que o controlador notifique os titulares.

A ***Office of the Australian Information Commissioner* (OAIC)**[33] sempre acusará o recebimento de notificações de incidente de segurança e pode requisitar mais informações ou orientar o controlador a respeito do incidente. Para isso, levará em consideração:

i. Se o incidente de segurança foi contido ou está em processo de ser contido;
ii. Se o controlador está adotando medidas para mitigar o impacto do incidente nos indivíduos afetados;
iii. Se o controlador está adotando medidas para evitar que um incidente similar ocorra novamente.

[33] OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER. **Data breach preparation and response A guide to managing data breaches in accordance with the Privacy Act 1988 (Cth).** Disponível em: https://www.oaic.gov.au/ data/assets/pdf file/0017/1691/data-breach-preparation-and-response.pdf . Acesso em: 27 jul.2022.

A OAIC também tem poderes para aceitar um acordo oferecido pelo controlador, determinar medidas, solicitar uma liminar e solicitar que penas pecuniárias sejam aplicadas ao controlador. Contudo, a OAIC afirma que prefere trabalhar em conjunto com os agentes de tratamento para incentivar e facilitar a conformidade com a legislação de privacidade.

A legislação canadense, em seu turno, obriga que o controlador mantenha registro[34] de todos os incidentes de segurança por dois anos, o que deverá ser analisado pelo OPC no caso de uma fiscalização, até mesmo para avaliar se foi considerada a necessidade de notificação, ou seja, o risco real de dano significante. Os registros devem conter, no mínimo: (i) data exata ou estimada do incidente; (ii) descrição geral das circunstâncias em que o incidente ocorreu; (iii) natureza dos dados envolvidos, e (iv) se o incidente foi notificado ao OPC e aos titulares.

### 9.2 Alternativas possíveis ao enfrentamento do problema

Comunicado o incidente de segurança à ANPD, o art. 48, §2º, da LGPD determina que o órgão verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como:

I - ampla divulgação do fato em meios de comunicação; e

II - medidas para reverter ou mitigar os efeitos do incidente.

As alternativas propostas a seguir refletem o modelo regulatório que poderia ser utilizado para o enfrentamento dessa questão.

**Alternativa A: não regulamentação**

A alternativa A contempla a opção de não se promover intervenção normativa, de modo que seja mantido o cenário regulatório atual.

[34] OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER. **What you need to know about mandatory reporting of breaches of security safeguards**. 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/ Acesso em: 15 ago.2022

Tal opção, entretanto, não se apresenta viável tendo em vista que a LGPD determina que a ANPD verificará a gravidade do incidente e, caso necessário para a salvaguarda dos direitos dos titulares, poderá determinar a adoção de providências (art. 48, § 2º). Assim, sendo obrigatória a verificação de gravidade e, no processo, concluindo-se pelo carecimento de medidas adicionais para proteger os direitos dos titulares e não havendo tal determinação por parte do órgão competente, manter-se-á a precariedade da proteção dos dados dos titulares envolvidos no incidente e poderá o agente público incorrer em improbidade administrativa por omissão.

Não sendo, portanto, possível a não regulamentação por tratar-se de ato normativo que visa disciplinar direitos ou obrigações definidos em norma hierarquicamente superior que não permite, técnica ou juridicamente, esta alternativa regulatória, cumpre apenas avaliar os contornos a serem dados às determinações possíveis de forma a promover maior segurança jurídica tanto aos regulados quanto aos agentes públicos.

**Alternativa B: Aplicação das determinações disposta no art. 48, § 2º após análise do incidente comunicado**

O art. 48, § 2º dispõe que a ANPD 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.

Nessa alternativa, a determinação de providências, caso necessário, é aplicada após a análise do incidente, que ocorre com base nas informações enviadas e nos critérios para a definição de risco ou dano relevante ao titular.

Nesse sentido, a providência de determinação de ampla divulgação em meios de comunicação ocorrerá quando a comunicação direta e individualizada se mostrar inviável e quando a comunicação realizada pelo controlador se mostrar insuficiente para alcançar parcela significativa dos titulares afetados pelo incidente. A divulgação poderá ser viabilizada

em meio físico ou digital, considerada sempre a necessidade de se atingir o maior número possível de titulares afetados, admitidos os meios de veiculação, tais como: mídia escrita impressa, radiodifusão de sons e de sons e imagens ou Internet.

Já a determinação de medidas para reverter ou mitigar os efeitos do incidente é aplicada para garantir a confidencialidade, integridade e disponibilidade dos dados pessoais afetados, bem como as medidas para minimizar os efeitos decorrentes do incidente.

**Alternativa C: Desenvolvimento de metodologia para cálculo da gravidade do incidente e adequação das providências a serem determinadas conforme o nível de gravidade identificado.**

Este modelo traz em seu bojo o desenvolvimento de metodologia para cálculo da gravidade de incidente e avaliação das providências a serem tomadas, dependendo da aplicação ao caso concreto.

Nessa alternativa, o cálculo da gravidade e adequação das providências consiste em mais uma etapa processual do incidente notificado, mas utiliza-se basicamente os mesmos critérios adotados na avaliação de incidentes com possibilidade de acarretar risco ou dano relevante aos titulares.

### 9.3 Impactos regulatórios das alternativas identificadas

Conforme avaliado anteriormente, a alternativa A, ao prever que não haja intervenção regulatória da matéria acarretaria maior risco à proteção dos direitos dos titulares de dados, bem como maior insegurança jurídica aos regulados e aos agentes públicos ante a falta de delineamentos claros e transparentes para a determinação de medidas necessárias para salvaguardar os direitos dos titulares. Destarte, esta alternativa não será considerada para fins de comparação com as demais.

A alternativa B replica a previsão legal, mas dispõe contornos adicionais de forma a esclarecer ao regulado, bem como ao agente público, quais circunstâncias ensejarão a determinação de cada uma das providências previstas em lei, principalmente quanto à ampla

divulgação do incidente, tendo em vista a determinação de que a providência será aplicável quando a comunicação realizada pelo controlador se mostrar insuficiente para alcançar parcela significativa dos titulares afetados pelo incidente, trazendo maior segurança jurídica

A alternativa C traz maiores custos administrativos para elaboração de metodologia de cálculo e morosidade ao processo de análise do incidente de segurança pela inclusão de mais uma etapa ao processo, bem como pode gerar maior insegurança jurídica ao controlador tendo em vista que alguns critérios a serem utilizados no cálculo só poderão ser avaliados no caso concreto.

Em ambas as alternativas (B e C), o maior impacto regulatório seria causado por uma desproporcionalidade nas providências a serem determinadas, gerando um custo excessivo aos controladores e aos negócios, ou mesmo minimizando o direito dos titulares à transparência. O custo referido pode ser traduzido como despesas de comunicação aos titulares e de implementação de medidas técnicas ou administrativas prescindíveis. Aos titulares, além do direito de serem notificados nos casos específicos, é importante que seus dados pessoais sejam preservados.

## 9.4 Comparação das alternativas consideradas

Tabela 3: Comparação entre as alternativas

| Critério | Alternativa B | Alternativa C |
|---|---|---|
| **Impacto operacional na ANPD** | Aplicação mais simples com opções claras e bem delimitadas. | Alto custo administrativo tanto para elaboração de metodologia, como pela duplicação ou sobreposição de esforços visto que a avaliação de risco ou dano relevante terá sido realizada em fase anterior.<br>Maior morosidade à análise do incidente comunicado. |
| **Impacto aos titulares de dados** | Equivalente (as determinações serão adotadas). | Equivalente (as determinações serão adotadas). |

| | | |
|---|---|---|
| **Impacto ao agente de tratamento** | Maior clareza dos contornos para determinação das providências e, portanto, maior segurança jurídica. | Risco de menor segurança jurídica visto que uma eventual metodologia consideraria uma diversidade de critérios que só poderão ser analisados no caso concreto ou, no caso de uma relação exaustiva, tornar-se obsoleta em pouco tempo. |

Fonte: Elaboração própria (Coordenação-Geral de Normatização)

Diante do exposto, avalia-se ser a alternativa "B" a melhor opção para o problema regulatório em análise, por conferir maior clareza e segurança jurídica, com menor custo para a administração pública. Importa observar que as circunstâncias que determinam a providência a ser adotada refletem o que foi avaliado para comunicação aos titulares e para adoção de medidas técnicas ao longo desta AIR.

Ademais, não se encontrou na experiência internacional um cálculo de gravidade pela autoridade que se diferencie da avaliação de risco ou dano relevante necessária à comunicação do incidente.

Adicionalmente, as medidas a serem determinadas para minimizar os efeitos decorrentes do incidente de segurança deverão garantir a confidencialidade, integridade e disponibilidade dos dados pessoais afetados de forma a reduzir o impacto tanto ao controlador quanto ao titular de dados pessoais.

## 10 IDENTIFICAÇÃO E DEFINIÇÃO DOS EFEITOS E RISCOS DECORRENTES DA EDIÇÃO DO ATO NORMATIVO

A publicação do regulamento é essencial para aprimorar o processo de comunicação de incidentes de segurança, principalmente quanto à definição de incidente que possa ocasionar risco ou dano relevante aos titulares, ao prazo para comunicação à Autoridade e ao titular envolvido no incidente, bem como as informações necessárias do incidente comunicado para análise pela ANPD.

Quanto a esse aspecto, entende-se necessária a atuação da ANPD na orientação, por meio de guias e ações educativas, na consolidação das definições e abordagens regulatórias propostas pela regulamentação.

Os riscos são relacionados à capacidade operacional da ANPD de analisar os incidentes notificados, bem como expedir determinações para mitigar efeitos dos incidentes e acompanhar seu cumprimento.

Outro aspecto diz respeito à necessidade de implementação de ferramenta adequada para a gestão dos incidentes notificados no âmbito da ANPD.

Deve-se observar que o regulamento tem caráter educativo no que tange à determinação de prazo e melhoria do processo de tratamento de incidentes de segurança de dados pessoais nos agentes de tratamento.

Os processos já comunicados à ANPD representam um fator crítico que deve ser analisado pela Autoridade, tendo em vista que se estes incidentes forem incluídos no escopo do regulamento, devem ser observados os casos que podem estar em irregularidade com o normativo.

## 11 IMPLEMENTAÇÃO E MONITORAMENTO

A partir das alternativas escolhidas, o regulamento para comunicação de incidentes de segurança será implementado por meio de resolução da ANPD, que será objeto de consulta pública e audiência pública nos termos da Portaria nº 16/2021 e do art. 55-J, § 2º da LGPD, e deverá entrar em vigor na data de sua publicação.

Há que se ponderar que o art. 48 da LGPD, objeto da regulamentação proposta, está em vigor desde 14 de agosto de 2020, não havendo razão para que se prolongue a produção de efeitos do regulamento de comunicação de incidentes, nos termos do art. 4º do Decreto nº 10.139/2019.

O sucesso da implementação da norma depende também de um plano de comunicação para sua divulgação aos agentes de tratamento, de modo a trazer transparência e clareza em relação às obrigações a ele impostas. Essas ações serão coordenadas pela Coordenação-Geral de Normatização (CGN), mas devem contar com a participação da

Coordenação-Geral de Fiscalização (CGF) e da Coordenação-Geral de Tecnologia e Pesquisa (CGTP), tendo em vista as competências relacionadas às ações educativas previstas no Regimento Interno da ANPD envolvem as referidas áreas.

O monitoramento da norma poderá ocorrer por meio do acompanhamento dos indicadores descritos abaixo, que buscam refletir os objetivos da elaboração da norma. Ao mesmo tempo, a necessidade de ajustes à regulamentação será avaliada continuamente e implementada em momento oportuno, levando em conta as informações fornecidas pelas áreas atuantes no processo de comunicação de incidentes.

Tabela 4: Descrição dos Indicadores de Monitoramento

| | |
|---|---|
| **Incidentes de segurança notificados (elemento a ser mensurado)** | Ocorrência de incidentes que acarretam risco aos titulares de dados (o que se pretende medir) |
| **Indicador** | **Número de Incidentes Notificados** |
| **Parâmetro do cenário inicial** | Não existe |
| **Área responsável** | CGF |
| **Fontes de dados** | SEI ou outro sistema que venha substituí-lo |
| **Frequência de coleta de dados** | Diária |
| **Frequência de cálculo do indicador** | Mensal |
| **Meta relacionada ao indicador** | NA |
| **Data alvo para atingimento da meta** | NA |

| | |
|---|---|
| **Incidentes notificados sem risco ou dano relevante ao titular** | Eficácia e clareza da norma |
| **Indicador** | **Número de Incidentes arquivados por estarem fora dos critérios de risco ou dano relevante em relação ao número de incidentes notificados (%)** |

| | |
|---|---|
| **Parâmetro do cenário inicial** | Não tem |
| **Área responsável** | CGF |
| **Fontes de dados** | SEI ou outro sistema que venha substituí-lo |
| **Frequência de coleta de dados** | Diária |
| **Frequência de cálculo do indicador** | Mensal |
| **Meta relacionada ao indicador** | NA |
| **Data alvo para atingimento da meta** | NA |

| | |
|---|---|
| **Incidentes notificados fora do prazo** | Conformidade |
| **Indicador** | **Número de Incidentes comunicados fora do prazo em relação ao número de incidentes notificados (%)** |
| **Parâmetro do cenário inicial** | Não tem |
| **Área responsável** | CGF |
| **Fontes de dados** | SEI ou outro sistema que venha substituí-lo |
| **Frequência de coleta de dados** | Diária |
| **Frequência de cálculo do indicador** | Mensal |
| **Meta relacionada ao indicador** | NA |
| **Data alvo para atingimento da meta** | NA |

| | |
|---|---|
| **Incidentes não notificados à ANPD** | Conformidade/Eficácia da norma |
| **Indicador** | **Número de procedimentos de apuração instaurados convertidos em comunicados de incidentes (%)** |

| | |
|---|---|
| **Parâmetro do cenário inicial** | x |
| **Área responsável** | CGF |
| **Fontes de dados** | SEI |
| **Frequência de coleta de dados** | Diária |
| **Frequência de cálculo do indicador** | Mensal |
| **Meta relacionada ao indicador** | NA |
| **Data alvo para atingimento da meta** | NA |

Fonte: Elaboração própria (Coordenação-Geral de Normatização)