

Presidência da República
AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS
Coordenação-Geral de Normatização

Nota Técnica nº 36/2022/CGN/ANPD

Assunto: Encaminhamento da minuta de Regulamento de comunicação de incidente de segurança com dados pessoais à Procuradoria da Autoridade Nacional de Proteção de Dados.

Referência: processo nº 00261.000098/2021-67

1. RELATÓRIO

1.1. Trata-se de proposta de Regulamento de comunicação de incidente de segurança com dados pessoais, que tem por objetivo a regulamentação da comunicação de incidentes de segurança, incluindo a especificação do prazo de notificação nos termos do § 1º do art. 48 da Lei nº 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD).

1.2. O referido tema encontra-se previsto no item 6 da Agenda Regulatória da Autoridade Nacional de Proteção de Dados (ANPD) para o biênio 2021/2022, aprovada pela Portaria nº 11, de 27 de janeiro de 2021.

1.3. O processo de regulamentação teve início por meio de assinatura de Termo de Abertura de Projeto em 22 de fevereiro de 2021 e conta com os seguintes integrantes em sua equipe de projeto: Fabrício Guimarães Madruga Lopes/CGN e Rodrigo Santana dos Santos/CGN, além de outros servidores indicados posteriormente.

1.4. Diante da complexidade do tema, optou-se pela realização de Tomada de Subsídios por meio do recebimento de contribuições escritas nos termos da Nota Técnica nº 3/2021/CGN/ANPD (SEI 2398694), de modo a possibilitar a participação da sociedade acerca de questões relacionadas à comunicação de incidentes de segurança. Nesse sentido, foram disponibilizadas 13 (treze) perguntas (SEI 2398738) à sociedade, sobre as quais esta Coordenação-Geral de Normatização (CGN) recebeu as respostas no período de 22/02/2021 e 24/03/2021.

1.5. Além disso, entre os dias 15 e 18/03/2022, foram realizadas Reuniões Técnicas com 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) (SEI nº 2474721); representantes do Laboratório de Políticas Públicas e Internet (LAPIN) e

Instituto de Referência em Internet e Sociedade (IRIS-BH) (SEI nº 2475226); 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 (SEI nº 2475465) e representantes do ITS Rio e Internet Lab (SEI nº 2483002).

1.6. Após análise das 98 (noventa e oito contribuições) recebidas durante a tomada de subsídios e das discussões realizadas no âmbito das reuniões técnicas, elaborou-se, no âmbito da equipe de projeto, a primeira versão da minuta, que foi submetida a consulta interna de 08 a 29 de julho de 2022 (SEI nº 3616715).

1.7. Feita a análise das contribuições internas, a minuta foi ajustada e debatida com o Conselho Diretor por meio de Seminário Interno dividido em quatro reuniões, realizado nos dias 28 de julho de 2022, e em 2, 4 e 12 de agosto do mesmo ano (SEI nº 3616751, 3616753, 3616757 e 3616768).

1.8. Após a realização de ajustes na minuta, resultado da discussão com o Conselho Diretor, a presente minuta com a proposta de regulamentação, devidamente acompanhada do Relatório de Análise de Impacto Regulatório (AIR), segue para avaliação da Procuradoria da ANPD. Na sequência, o processo será enviado ao Conselho Diretor para deliberação da matéria e autorização de submissão da proposta normativa à consulta pública.

1.9. É o relatório.

2. ANÁLISE

2.1. Da fundamentação legal

2.1.1. Inicialmente, cumpre destacar que em fevereiro de 2022, a Emenda Constitucional nº 115, de 2022 alçou o direito à proteção de dados pessoais, para o rol dos direitos e garantias fundamentais, além de ter fixado a competência privativa da União para legislar sobre o tema.

2.1.2. De fato, 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 a autarquia federal responsável por dar efetividade à LGPD no País.

2.1.3. Entre as competências da ANPD, consta o estabelecimento de normas e diretrizes para a interpretação e implementação da LGPD. Para além da competência normativa, a LGPD também atribuiu à ANPD a competência fiscalizatória e sancionatória em matéria de tratamento de dados pessoais, prevalecendo, no que se refere à proteção de dados pessoais, sobre as competências correlatas de outras entidades ou órgãos da administração pública, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito ao recurso, *in verbis* (grifo nosso):

Art. 55-J. Compete à ANPD:

(...)

XIII - **editar regulamentos** e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei; (Incluído pela Lei nº 13.853, de 2019)

2.1.4. Ademais, destaca-se que o Regimento Interno da ANPD (RIANPD), aprovado pela Portaria nº 1, de 8 de março de 2021, em seu art. 16, atribuiu a esta Coordenação-Geral de Normatização (CGN) as competências de elaboração de guias e recomendações, bem como proposições normativas, regulamentos, orientações e procedimentos simplificados, nos termos da LGPD, a serem submetidas à aprovação pelo Conselho Diretor.

2.1.5. No tocante ao objeto de regulamentação, o art. 48 da LGPD ao prever que o controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, determinou, em seu §1º que tal comunicação deverá ser realizada em prazo razoável, a ser definido pela Autoridade, e estabeleceu requisitos mínimos para que a mesma fosse realizada:

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.

2.1.6. Ademais, o item 6 da Agenda Regulatória do biênio 2021/2022, aprovada pela Portaria nº 11, de 27 de janeiro de 2021, prevê a regulamentação do art. 48 da LGPD, conforme tabela a seguir.

Tema	Descrição
Comunicação de incidentes e especificação do prazo de notificação	De acordo com o art. 48 da LGPD, 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. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações.

2.1.7. Existe, assim, previsão legal para regulamentação do tema.

2.2. Da Tomada de Subsídios

2.2.1. No que se refere à Tomada de Subsídios, conforme supramencionado, consoante teor da Nota Técnica nº 3/2021/CGN/ANPD (SEI nº 2398694), optou-se pela sua realização por meio do recebimento de contribuições escritas, de modo a obter insumo para elaboração de minuta de normativo e AIR. Nesse sentido, foram disponibilizadas as 13 (treze) perguntas abaixo discriminadas (SEI nº 2398738), as quais puderam receber contribuições no período de 22/02/2021 a 24/03/2021.

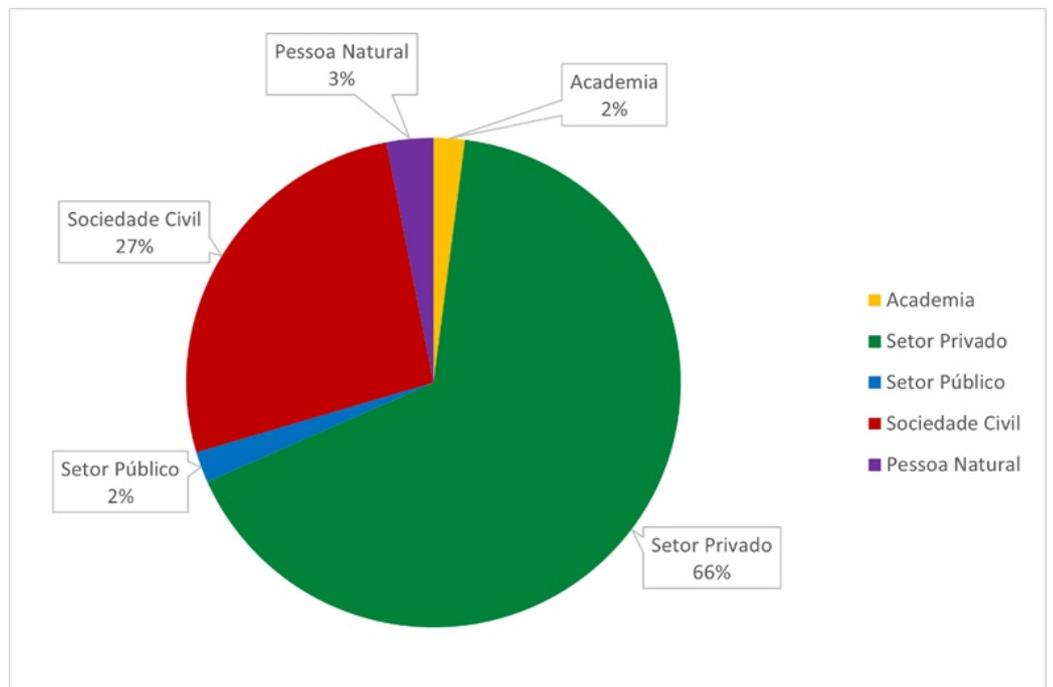
1. Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?
2. O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto, etc)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?
3. Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?
4. O que deve ser considerado na avaliação dos riscos do incidente?
5. Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?

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

2.2.2. A análise das 98 (noventa e oito) contribuições recebidas foi realizada de forma consolidada no Relatório de AIR (SEI nº 3632342).

2.2.3. No tocante aos participantes, 66% identificaram-se como representantes do setor privado^[1]; 27% classificaram-se como representantes da Sociedade Civil^[2]; 3%, identificaram-se como pessoas naturais^[3] e 2% dos participantes identificaram-se como representantes do setor público^[4] e como membros da academia.^[5]

Gráfico 1: Relação de participantes na Tomada de Subsídios



Fonte: Elaboração própria (Coordenação-Geral de Normatização)

2.3. Da Análise de Impacto Regulatório (AIR)

2.3.1. Nesta seção são apresentados os temas mais relevantes do relatório de AIR de construção do modelo regulatório para comunicação e tratamento de incidentes de segurança (SEI nº 3632342). Maiores esclarecimentos podem ser obtidos diretamente no documento.

2.3.2. O relatório de AIR identificou os possíveis problemas ou questões a serem enfrentadas para atender ao comando legal disposto no art. 48 da LGPD de regulamentação de comunicação de incidentes de segurança à ANPD e ao titular.

2.3.3. As questões seriam:

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

2.3.4. Foi realizada pesquisa de experiências internacionais para identificar mecanismos regulatórios para endereçar os problemas identificados. Além dos organismos vinculados à União Europeia, foram pesquisadas autoridades e legislações de outros seguintes países: Espanha,

Irlanda, França, Austrália, Canadá e Japão.

2.3.5. Para endereçar os problemas regulatórios foram identificadas as seguintes alternativas, pormenorizadas no relatório de AIR: (i) tema 1 - critérios para definição de incidentes que possam acarretar riscos ou danos relevantes aos titulares; (ii) tema 2 - prazo de envio das comunicações de incidentes de segurança à ANPD e ao titular de dados; e (iii) tema 3 - tratamento de incidentes notificados à ANPD.

2.3.6. No que se refere ao tema 1, concluiu-se que a combinação de critérios com base no contexto do incidente é a melhor alternativa a ser escolhida, levando em conta a natureza e categoria dos dados, e possível impacto aos interesses e direitos dos titulares.

2.3.7. Este modelo dispõe 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.

2.3.8. 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. Por sua vez, no que se refere ao tema 2, concluiu-se que a previsão da 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, é a melhor alternativa.

2.3.9. Essa alternativa propõe, em que pese haja a fixação de prazo inicial comum para comunicação à ANPD e ao titular, que em relação àquela seja previsto prazo para, excepcionalmente, ocorrer a complementação das informações solicitadas, mediante justificativa.

2.3.10. Sugere-se igualmente 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 à ANPD e ao titular.

2.3.11. 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.

2.3.12. 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 prazo de 30 (trinta) dias para complemento.

2.3.13. 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 da ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, exceto quando 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.

2.3.14. Já no que se refere ao tema 3, 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.

2.3.15. 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.

2.3.16. 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.

2.3.17. 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.

2.3.18. Por fim, foram identificados os seguintes indicadores para monitoramento do resultado regulatório do regulamento:

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

2.3.19. As informações detalhadas sobre cada um dos temas podem ser consultadas no relatório de AIR (SEI 3632342).

2.4. Da proposta de ato normativo

2.4.1. A elaboração da proposta de resolução foi baseada na adequação à Lei Complementar nº 95, de 26 de fevereiro de 1998, que dispõe

sobre a elaboração, a redação, a alteração e a consolidação das leis, conforme determina o parágrafo único do art. 59 da Constituição Federal, e estabelece normas para a consolidação dos atos normativos que menciona.

2.4.2. A parte preliminar contém a epígrafe, a ementa, o preâmbulo, o enunciado do objeto e a indicação do âmbito de aplicação das disposições normativas.

2.4.3. No presente caso, a epígrafe contém o título designativo da espécie, qual seja, a Resolução. A ementa sintetiza seu conteúdo e explicita, de modo conciso o seu objeto, se tratando, neste caso, da aprovação do Regulamento de Comunicação de Incidente de Segurança com Dados Pessoais. O preâmbulo, por sua vez, esclarece que o Conselho Diretor é a autoridade competente com os fundamentos legais.

O CONSELHO DIRETOR DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD), com base nas competências previstas no art. 55-J, inciso XIII, da Lei nº 13.709, de 14 de agosto de 2018, no art. 2º, inciso XIII, do Anexo I do Decreto nº 10.474, de 26 de agosto de 2020, no art. 5º, inciso I do Regimento Interno da ANPD, aprovado pela Portaria nº 1, de 8 de março de 2021, tendo em vista a deliberação tomada no Circuito Deliberativo nº XX/2022, e pelo que consta no processo nº 00261.000098/2021-67, **RESOLVE:**

Art. 1º Aprovar o Regulamento de comunicação de incidente de segurança com dados pessoais na forma do anexo desta Resolução.

Art. 2º Esta Resolução entra em vigor na data de sua publicação.

WALDEMAR GONÇALVES ORTUNHO JUNIOR

Diretor-Presidente

2.4.4. Em relação à estrutura da minuta, adotou-se a seguinte divisão:

2.5. Disposições preliminares

2.5.1. Nas disposições preliminares aborda-se questões gerais como escopo, objetivos e definições descritos na norma.

2.5.2. Com relação ao escopo, o regulamento, em observância ao art. 48 da LGPD, trata da comunicação de incidente de segurança com dados pessoais que possa acarretar risco ou dano relevante aos titulares, à Autoridade Nacional de Proteção de Dados (ANPD) e ao titular de dados pessoais, bem como os procedimentos internos necessários para apuração e eventual determinação de adoção de providências nos termos do art. 48, § 2º e art. 55-J, inciso XIII, da Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD).

2.5.3. Ressalta-se que está fora do escopo do regulamento o tratamento de dados pessoais realizado por pessoa natural para fins

exclusivamente particulares e não econômicos, bem como às demais hipóteses previstas no art. 4º da LGPD.

2.5.4. Os objetivos estão aderentes aos princípios da LGPD e demonstram importantes pilares para o processo, como por exemplo, proteção de direitos e interesses dos titulares, estímulo a promoção de cultura de dados e responsabilização e prestação de contas por parte do agente de tratamento de dados.

2.5.5. Ademais, os objetivos alinham-se as principais bases de atuação do ANPD no que tange ao processo de comunicação de incidente de segurança.

2.5.6. Dessa forma, a redação do Capítulo I ficou redigida nos seguintes termos:

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Art. 1º Este regulamento tem por objetivo normatizar a comunicação de incidente de segurança com dados pessoais que possa acarretar risco ou dano relevante aos titulares, à Autoridade Nacional de Proteção de Dados (ANPD) e ao titular de dados pessoais, bem como os procedimentos internos necessários para apuração e eventual determinação de adoção de providências, nos termos do art. 48 da Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD).

Parágrafo único. Este regulamento não se aplica ao tratamento de dados pessoais realizado por pessoa natural para fins exclusivamente particulares e não econômicos, bem como às demais hipóteses previstas no art. 4º da LGPD.

Art. 2º O processo de comunicação de incidente de segurança à ANPD atenderá aos seguintes objetivos:

I - proteger os direitos dos titulares e assegurar a adoção das medidas necessárias para mitigar ou reverter os danos gerados;

II - incentivar a responsabilização e a prestação de contas pelos agentes de tratamento;

III - promover a adoção de regras de boas práticas e de governança e de medidas de prevenção e segurança adequadas;

IV - estimular a promoção da cultura de proteção de dados pessoais;

V - garantir que os agentes de tratamento atuem de forma transparente, visando ao estabelecimento de relação de confiança com o titular; e

VI - fornecer subsídios para as atividades regulatórias, de fiscalização e sancionadora da ANPD.

2.6. Das definições

2.6.1. Neste capítulo são abordadas as definições necessárias para a operacionalizar e proporcionalizar maior entendimento ao processo de comunicação de incidentes de segurança.

2.6.2. Um dos pontos considerados relevantes é a definição de “ampla divulgação do incidente em meios de comunicação” disposto no art. 48, § 2º, I da LGPD, o qual exemplifica os possíveis meios dessa divulgação, como por exemplo, Internet e redes sociais.

2.6.3. Outro destaque é a definição de “categoria de dados pessoais”, como sendo a classificação dos dados de acordo com o contexto da sua utilização, tais como identificação pessoal, financeiro, saúde, educação, dentre outros.

2.6.4. Essa classificação é importante para identificar tipos de dados que podem trazer mais riscos aos titulares no contexto do incidente de segurança, como é o caso de dados financeiros, que podem ocasionar danos materiais aos titulares de dados.

2.6.5. Além disso, existem os dados sensíveis que são definidos pela LGPD como de origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

2.6.6. É importante ressaltar que os dados sensíveis também se inserem no contexto de analisar o potencial de riscos ou danos que o incidente pode causar aos titulares, entretanto, a sua definição fica restrita ao definido no art. 5º, II da LGPD.

2.6.7. Nota-se que um dado pode ser de determinada categoria e estar incluído no rol de dados sensíveis, como é o caso de dados de prontuários médicos, mas outras não, como é o caso de dados financeiros.

2.6.8. Ademais, criou-se a definição de “natureza de dados” que abarca classificação de dados pessoais em gerais e sensíveis.

2.6.9. Outro destaque seria a definição do relatório de tratamento do incidente, como sendo o relatório fornecido pelo controlador que contém cópias de documentos, físicos ou digitais, dados e informações relevantes para descrever o incidente e as ações tomadas para o seu tratamento, tais como evidências e cronologia do incidente, metodologia de investigação e ferramentas utilizadas, e medidas de segurança adotadas.

2.6.10. Ainda que não esteja previsto na LGPD, este relatório é utilizado na prática na atividade de tratamento de incidente de segurança, e auxilia a ANPD na análise do incidente.

2.6.11. Nesse sentido, a redação do Capítulo II ficou redigida da seguinte forma:

CAPÍTULO II

DAS DEFINIÇÕES

Art. 3º Para efeitos deste regulamento são adotadas as seguintes definições:

I - ampla divulgação do incidente em meios de comunicação: providência que pode ser determinada pela ANPD ao controlador, nos termos do art. 48, § 2º, I, da LGPD, no âmbito do processo de comunicação de incidente de segurança com dados pessoais, tais como, publicação no sítio da Internet e nas redes sociais do controlador ou em outros meios de grande alcance;

II - categoria de dados pessoais: classificação dos dados pessoais de acordo com o contexto de sua utilização, tais como, identificação pessoal, autenticação em sistemas, financeiro, saúde, educação, judicial e criminal;

III - comunicação de incidente de segurança: ato do controlador que comunica à ANPD e ao titular de dados a ocorrência de incidente de segurança com dados pessoais que possa acarretar risco ou dano relevante aos titulares;

IV - confidencialidade: propriedade pela qual se assegura que o dado pessoal não esteja disponível ou não seja revelado à pessoa, à sistema, à órgão ou entidades não autorizadas e nem credenciadas;

V - dado de autenticação em sistemas: qualquer dado pessoal utilizado como credencial para determinar o acesso a um sistema ou para confirmar a identificação de um usuário, tal como contas de login, tokens e senhas;

VI - dado financeiro: dado pessoal relacionado à vida financeira do titular, inclusive para contratação de serviços e aquisição de produtos;

VII - dado pessoal afetado: dado pessoal cuja confidencialidade, integridade ou disponibilidade tenha sido comprometida em um incidente de segurança;

VIII - disponibilidade: propriedade pela qual se assegura que o dado pessoal esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;

IX - incidente de segurança com dados pessoais: qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais;

X - integridade: propriedade pela qual se assegura que o dado pessoal não seja modificado ou destruído de maneira não autorizada ou acidental;

XI - medidas de segurança relacionadas a dados pessoais: medidas técnicas e administrativas adotadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de

tratamento inadequado ou ilícito;

XII - natureza dos dados pessoais: classificação de dados pessoais em gerais e sensíveis;

XIII - procedimento de apuração de incidente de segurança: procedimento realizado pela ANPD para apurar a ocorrência de incidente de segurança com dados pessoais capaz de gerar risco ou dano relevante ao titular que não lhe tenha sido comunicado pelo controlador;

XIV - processo de comunicação de incidente de segurança: processo no âmbito da ANPD que abrange a comunicação do incidente com dados pessoais e a avaliação da necessidade de determinação de adoção de providências;

XV - relatório de tratamento do incidente: relatório fornecido pelo controlador que contém cópias de documentos, físicos ou digitais, dados e informações relevantes para descrever o incidente e as ações tomadas para o seu tratamento, tais como, evidências e cronologia do incidente, metodologia de investigação e ferramentas utilizadas, e medidas de segurança adotadas.

2.7. Das disposições processuais

2.7.1. O art. 4º dispõe sobre o alinhamento necessário com as previsões das Seções I, II e IV do Capítulo IV do Título I do Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador, aprovado pela Resolução CD/ANPD nº 01, de 28 de outubro de 2021.

2.7.2. Esses dispositivos no Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador tratam de contagem de prazos, da comunicação dos atos administrativos e do regime de tramitação prioritária.

2.7.3. Preliminarmente, ressalta-se que foi adotada a contagem de prazo em “dias úteis” na minuta, para buscar harmonização com o previsto no Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador.

2.7.4. Além disso, no art. 5º foi destacado que os agentes de tratamento de pequeno porte têm direito a prazos em dobro, nos termos do art. 14, II do Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) aos agentes de tratamento de pequeno porte, aprovado pela Resolução CD/ANPD nº 2, de 27 de janeiro de 2022, exceto quando houver potencial comprometimento à integridade física ou moral dos titulares ou à segurança nacional.

2.7.5. O art. 6º dispõe sobre a divisão do processo de comunicação de incidente em:

- I - comunicação do incidente de segurança com dados

personais; e

II - avaliação da necessidade de adoção de providências para a salvaguarda dos direitos dos titulares.

2.7.6. O objetivo desse artigo é trazer luz e esclarecimento sobre as duas etapas do processo de comunicação de incidentes.

2.7.7. Já o art. 7º trata da possibilidade de a ANPD poder analisar os incidentes comunicados de forma agregada, e sobre como as eventuais providências deles decorrentes poderão ser adotadas de forma padronizada. Esse aspecto é importante para que a ANPD possa tratar os incidentes comunicados com mais eficiência. Pelo histórico de comunicados recebidos pela ANPD e por outras autoridades de outros países, o alto volume de incidentes comunicados pode se tornar um gargalo operacional para a sua análise.

2.7.8. Dessa forma, a redação do Capítulo III dispõe o seguinte:

CAPÍTULO III

DAS DISPOSIÇÕES PROCESSUAIS

Art. 4º Aplicam-se aos processos e procedimentos regidos por este regulamento as disposições das Seções I, II e IV do Capítulo IV do Título I do Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador, aprovado pela Resolução CD/ANPD nº 01, de 28 de outubro de 2021.

Art. 5º Os prazos contidos neste regulamento serão concedidos em dobro aos agentes de tratamento de pequeno porte, nos termos do art. 14, II do Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) aos agentes de tratamento de pequeno porte, aprovado pela Resolução CD/ANPD nº 2, de 27 de janeiro de 2022, exceto quando houver potencial comprometimento à integridade física ou moral dos titulares ou à segurança nacional.

Art. 6º O processo de comunicação de incidente de segurança possui as seguintes fases:

I – comunicação do incidente de segurança com dados pessoais; e

II - avaliação da necessidade de adoção de providências para a salvaguarda dos direitos dos titulares.

Art. 7º Os processos de comunicação de incidente de segurança, de que trata este regulamento, poderão ser analisados de forma agregada, e as eventuais providências deles decorrentes poderão ser adotadas de forma padronizada.

Parágrafo único. Os processos referidos no caput serão analisados e, se for o caso, arquivados, em conformidade com o planejamento da atividade de fiscalização e os critérios de priorização definidos no Relatório de Ciclo de Monitoramento de que trata o art. 20 do Regulamento do Processo de Fiscalização e do Processo

2.8. Dos critérios para comunicação de incidentes de segurança

2.8.1. Os critérios para comunicação de incidentes de segurança são um importante aspecto relacionado à identificação dos incidentes que possam ocasionar risco ou dano relevante aos titulares de dados e, portanto, devem ser comunicados à ANPD e ao titular.

2.8.2. Como pode ser observado no item 7.1 do relatório de AIR (SEI nº 3632342), que analisou o modelo regulatório para comunicação e tratamento de incidentes de segurança, existe considerável número de experiências internacionais sobre os critérios para definição dos incidentes que devem ser notificados às autoridades e aos titulares.

2.8.3. No relatório supramencionado avaliou-se quais os critérios utilizados pelas autoridades pesquisadas, bem como aqueles já utilizados pela regulamentação, notadamente os critérios para definição de tratamento de alto risco, nos termos do art. 4º do Regulamento de aplicação da LGPD aos agentes de tratamento de pequeno porte, aprovado pela Resolução CD/ANPD nº 2, de 27 de janeiro de 2022

2.8.4. Destaca-se que o contexto de tratamento de alto risco é diferente da definição de incidentes de segurança que possam acarretar risco ou dano relevante aos titulares. No entanto, ainda que diferentes, ambos se baseiam em riscos que possam causar impedimento no exercício de direitos e serviços ou danos aos titulares de dados.

2.8.5. Sobre os critérios adotados, transcreve-se parte do relatório de AIR (SEI nº 3632342) que tratou sobre o tema:

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”.

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

2.8.6. A minuta proposta visa constituir critérios que, com base na alternativa escolhida do tema 1, qual seja, critérios para definição de incidentes que possam acarretar riscos ou danos relevantes aos titulares, conforme consta no relatório de AIR, possam proporcionar a comunicação do incidente de segurança à ANPD e aos titulares de dados.

2.8.7. Esse modelo se diferencia de algumas experiências internacionais no que se refere à distinção do notificado, considerando que alguns incidentes seriam notificados aos titulares e não à Autoridade. No presente caso, entende-se que todo incidente que se enquadre no critério definido no art. 9º da minuta deve ser notificado tanto à ANPD quanto aos titulares.

2.8.8. Nesse sentido, foi escolhido como critério central a possibilidade de o incidente de segurança afetar significativamente interesses e direitos fundamentais dos titulares, sendo subdividido em: 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.

2.8.9. Esse elemento central traz o impacto aos interesses e direitos dos titulares como grande norteador da definição de incidentes que possam ocasionar risco ou dano relevante aos titulares. Ao mesmo tempo, foram inseridos critérios específicos de forma secundária e alternativa, ou seja, deve-se atender algum dos critérios específicos que estão relacionados a riscos ao titular, sendo eles:

- 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;
- 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; ou
- Dados de autenticação em sistemas: qualquer dado pessoal utilizado como credencial para determinar o acesso a um sistema ou para confirmar a identificação de um usuário, tal como contas de login, tokens e senhas.

2.8.10. A escolha dos critérios específicos levou em consideração as experiências internacionais, amplamente divulgadas e analisadas no relatório de Análise de Impacto Regulatório, bem como buscou estabelecer parâmetros mais objetivos de forma a trazer maior segurança jurídica à proposta.

2.8.11. Além disso, caso o controlador identifique algum incidente que, por meio de boas práticas, tenha possibilidade de acarretar risco ou dano relevante ao titular, mesmo que utilize critérios distintos, deve comunicá-lo à ANPD e aos titulares.

2.8.12. Os critérios específicos, além de estarem harmonizados com as experiências internacionais, tem aspecto mais objetivo e trazem maior segurança jurídica ao processo de identificação de incidente com possibilidade de acarretar risco ou dano relevante.

2.8.13. Por fim, foi incluído um artigo que possibilita a ANPD solicitar a comunicação de incidentes de segurança, inclusive ao titular de dados, ainda que não estejam presentes os critérios descritos acima, caso conclua que o incidente possa causar risco ou dano relevante ao titular.

2.8.14. Dessa forma, a redação do Capítulo IV dispõe o seguinte:

CAPÍTULO IV

DOS CRITÉRIOS PARA COMUNICAÇÃO DE INCIDENTES DE SEGURANÇA

Art. 8º O controlador deverá comunicar à ANPD e ao titular os incidentes de segurança envolvendo dados pessoais que possam ocasionar risco ou dano relevante aos titulares.

Art. 9º Para fins deste regulamento, considera-se que um incidente de segurança com dados pessoais pode acarretar risco ou dano relevante aos titulares quando tiver potencial de afetar significativamente interesses e direitos fundamentais dos titulares e envolver:

I - dados em larga escala;

II - dados sensíveis;

III - dados de crianças, de adolescentes ou de idosos;

IV - dados financeiros; ou

V - dados de autenticação em sistemas.

§ 1º São considerados incidentes que tem potencial de afetar significativamente interesses e direitos fundamentais dos titulares, 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.

§ 2º Para aplicação deste regulamento, os incidentes de segurança envolvendo dados pessoais em larga escala serão assim caracterizados quando abrangerem número significativo de titulares, considerando, ainda, o volume de dados envolvidos e a extensão geográfica de localização dos titulares.

§ 3º O controlador deverá comunicar o incidente de segurança à ANPD e aos titulares se identificada, por meio de boas práticas, a possibilidade de acarretar risco ou dano relevante ao titular, mesmo que utilize critérios distintos daqueles descritos no caput.

Art. 10 A ANPD poderá determinar ao controlador que comunique o incidente de segurança, inclusive ao titular de dados, ainda que não presentes os critérios descritos nos incisos do caput art. 9º deste regulamento, caso conclua que o incidente possa causar risco ou dano relevante ao titular.

2.9. Da comunicação do incidente à ANPD

2.9.1. O capítulo V da minuta trata da comunicação dos incidentes de segurança que possam acarretar risco ou dano relevante, nos termos do art. 48 da LGPD, perante a ANPD.

2.9.2. Para tanto, o art. 11 define o prazo de até 3 (três) dias úteis, a serem contados a partir do momento em que o controlador toma conhecimento do incidente de segurança, como razoável para que sejam realizadas tais comunicações.

2.9.3. Consoante explicitado no relatório de AIR, a fixação deste prazo harmoniza-se com a experiência internacional de outras autoridades, aproximando-se daquele adotado no Regulamento Geral de Proteção de Dados Europeu (RGPD), que é de 72h. Além disso, adotou-se cômputo do prazo em dias úteis, ao invés de horas, a fim de que houvesse a compatibilização da contagem de prazos neste regulamento com aquele ora previsto 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.

2.9.4. Vale mencionar que na fixação de prazo considerado razoável atentou-se para a necessidade de que fossem conjugadas tanto a celeridade na comunicação e viabilidade para análise prévia por parte do controlador, quanto à classificação do incidente em relação ao risco ou dano relevante que possa ocasionar.

2.9.5. Assim, não só foi adotado o prazo de até 3 (três) dias úteis, como também foi incluída uma previsão no §1º do presente artigo quanto à excepcional possibilidade de complementação das informações requeridas na comunicação no prazo de 20 (vinte) dias úteis, prorrogável uma vez, por igual período, mediante justificativa.

2.9.6. Tal medida justifica-se considerando o fato de que incidentes de segurança podem ser caracterizados a partir de diferentes níveis de complexidade, de modo que não se revela razoável a fixação de um prazo único para todo e qualquer incidente de segurança, de forma indistinta, o que, eventualmente, caso não observado, poderia refletir em um grande volume de incidentes comunicados de forma errônea, ou eventualmente inviabilizar a comunicação no prazo ora estipulado, tendo em vista a impossibilidade fática de que o controlador detenha as informações requeridas em tal prazo. Destaca-se que essa medida já era comumente adotada pela Coordenação-Geral de Fiscalização (CGF) antes mesmo da regulamentação do art. 48 da LGPD, todavia considerado o prazo de 30 (trinta) dias para complemento.

2.9.7. Insta salientar que 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 da ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, exceto quando 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.

2.9.8. Ademais, o art. 11 prevê as informações mínimas que deverão constar na comunicação de incidente à ANPD.

2.9.9. Quanto a esse ponto, vale observar que o art. 48, §1º da LGPD elenca as seis informações mínimas que deveriam estar contidas na comunicação à autoridade nacional e ao titular de dados, quais sejam: 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.

2.9.10. Assim, considerando a previsão de rol exemplificativo na referida Lei, buscou-se o acréscimo de outras informações, as quais foram julgadas como pertinentes pela equipe de projetos, para que houvesse maior detalhamento do incidente e que permitissem uma análise mais exaustiva para fins fiscalizatórios.

2.9.11. Nesse sentido, para além daquelas informações já exigíveis pela LGPD, a proposta de regulamento solicita os seguintes dados: VII - data e hora do conhecimento do incidente de segurança; VIII - dados do encarregado, quando aplicável, ou do notificante, acompanhado, nesta hipótese, de procuração com poderes para representar o controlador junto à ANPD; IX - dados de identificação do controlador e, se cabível, declaração de tratar-se de agente de tratamento de pequeno porte; X - informações sobre o operador, quando aplicável; XI - no caso de comunicação aos titulares, apresentar o conteúdo e o número de titulares comunicados; XII - descrição do incidente, incluindo a causa raiz, caso seja possível identificá-la e XIII - total de titulares cujos dados são tratados pela organização e na atividade de tratamento afetada pelo incidente.

2.9.12. Assim, de forma análoga à Lei, adotou-se um rol exemplificativo para determinação das informações necessárias na comunicação de incidentes e previu-se, no art. 13, que a ANPD poderá, a qualquer tempo, solicitar informações adicionais ou pedidos de esclarecimentos ao controlador referentes ao incidente de segurança, inclusive o registro das operações de tratamento de dados pessoais afetados pelo incidente ou o relatório de tratamento do incidente, estabelecendo prazo razoável para envio das

informações.

2.9.13. No tocante ao meio pelo qual deverá ser realizada a comunicação de incidente à ANPD, previu-se que ela deverá ocorrer por meio de formulário eletrônico, o qual será disponibilizado pela Autoridade.

2.9.14. Por sua vez, em que pese o processo de comunicação de incidentes ser classificável como público, o art. 12 da minuta previu que as informações referentes a segredo comercial e industrial serão protegidas, mediante solicitação do controlador.

2.9.15. Ao final do capítulo, determinam-se os requisitos mínimos para o registro de incidente de segurança, e, ainda, fixa-se o prazo de no mínimo 5 (cinco) anos para que ele seja mantido pelo controlador, salvo se constatadas obrigações adicionais que demandem maior prazo de manutenção.

2.9.16. Assim sendo, a redação do Capítulo V dispõe o seguinte:

CAPÍTULO V

DA COMUNICAÇÃO DO INCIDENTE À ANPD

Art. 11. A comunicação do incidente de segurança deverá ser realizada pelo controlador à ANPD no prazo de até 3 (três) dias úteis, e deverá conter, no mínimo, as seguintes informações:

I - descrição da natureza e da categoria de dados pessoais afetados;

II - informações sobre o número de titulares afetados, discriminando, quando aplicável, o número de crianças, de adolescentes ou de idosos;

III - indicação das medidas de segurança utilizadas para a proteção dos dados pessoais, previamente ao incidente e medidas de segurança adicionais, adotadas após o incidente;

IV - riscos relacionados ao incidente com identificação dos possíveis impactos aos titulares;

V - motivos da comunicação do incidente não ter sido imediata, se for o caso;

VI - medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente sobre os titulares;

VII - data e hora do conhecimento do incidente de segurança;

VIII - dados do encarregado, quando aplicável, ou do notificante, acompanhado, nesta hipótese, de procuração com poderes para representar o controlador junto à ANPD;

IX - dados de identificação do controlador e, se cabível, declaração de tratar-se de agente de tratamento de pequeno porte;

X - informações sobre o operador, quando aplicável;

XI - no caso de comunicação aos titulares, apresentar o conteúdo e o número de titulares comunicados;

XII - descrição do incidente, incluindo a causa raiz, caso seja possível identificá-la;

XIII - total de titulares cujos dados são tratados pela organização e na atividade de tratamento afetada pelo incidente.

§ 1º Excepcionalmente, as informações poderão ser complementadas, no prazo de 20 (vinte) dias úteis, prorrogável uma vez, por igual período, mediante justificativa.

§ 2º A contagem dos prazos previstos neste artigo inicia-se a partir do momento em que o controlador tomou conhecimento do incidente de segurança.

§ 3º A comunicação do incidente de segurança deverá ocorrer por meio de formulário eletrônico, disponibilizado pela ANPD.

Art. 12. No âmbito do processo de comunicação de incidentes, as informações com sigredo comercial e industrial serão protegidas.

Parágrafo único. Cabe ao controlador solicitar à ANPD o sigilo de informações relativas à sua atividade empresarial, como dados e informações técnicas, econômico-financeiras, contábeis e operacionais, cuja divulgação possa representar violação a sigredo comercial ou a industrial, nos termos do art. 48, § 1º, III da LGPD.

Art. 13. A ANPD poderá, a qualquer tempo, solicitar informações adicionais ou pedidos de esclarecimentos ao controlador, referentes ao incidente de segurança, inclusive o registro das operações de tratamento dos dados pessoais afetados pelo incidente ou o relatório de tratamento do incidente, estabelecendo prazo razoável para envio das informações.

Art. 14. O controlador deverá manter o registro de incidentes de segurança com dados pessoais, inclusive daquele que não possa acarretar risco ou dano relevante aos titulares, pelo prazo mínimo de 5 (cinco) anos, contados a partir da data do registro, exceto se constatadas obrigações adicionais que demandem maior prazo de manutenção.

Parágrafo único. O registro do incidente deve conter, no mínimo:

I - data de conhecimento do incidente;

II - descrição geral das circunstâncias em que o incidente ocorreu;

III - natureza e categoria de dados afetados;

IV – número de titulares afetados;

V – avaliação do risco e possíveis danos aos titulares;

VI – medidas de correção e mitigação dos efeitos do incidente, quando aplicável; e

VII - se o incidente foi notificado à ANPD e aos titulares, a forma de comunicação e os motivos da ausência de notificação, quando for o caso.

2.10. Da comunicação do incidente ao titular de dados pessoais

2.10.1. O capítulo VI da presente minuta disciplina sobre a comunicação do incidente de segurança que possa acarretar risco ou dano relevante ao titular de dados pessoais, perante a este.

2.10.2. Relativamente ao prazo para comunicação, definiu-se, igualmente ao que foi estipulado para comunicação a ser feita à Autoridade, o prazo de até 3 (três) dias úteis para que o controlador o faça ao titular de dados pessoais. Todavia, diferentemente da comunicação à ANPD, não foi previsto prazo para eventual complementação das informações solicitadas. Tal opção justifica-se em razão do menor número de informações solicitadas e complexidade destas em comparação às requeridas para comunicação à Autoridade, assim como a necessidade de que o titular seja informado o mais rápido possível, a fim de que possa adotar medidas para mitigar os efeitos do incidente e evitar o agravamento dos danos sofridos. Quanto às medidas para mitigação dos efeitos do incidente, vale observar que a inclusão na comunicação ao titular de recomendações para reduzir os efeitos do incidente será considerada boa prática para fins do disposto no art. 52, §1º, IX da LGPD, consoante o §5º do art. 15.

2.10.3. Quanto aos requisitos para tal comunicação, determina-se que essa deverá empregar o uso de linguagem simples e de fácil entendimento, e que caso seja possível identificar os titulares afetados, que isso ocorra de forma direta e individualizada. Especificamente em relação à comunicação direta e individualizada, o §6º do art. 15 previu que poderão ser assim consideradas aquelas realizadas pelos meios usualmente utilizados pelo controlador para contatar o titular, tais como telefone, e-mail, mensagem eletrônica ou carta.

2.10.4. Ainda que não se tenha previsto prazo para complementação das informações, previu-se que em caso inviabilidade ou impossibilidade de determinação, parcial ou integral, dos titulares afetados no prazo de 3 (três) dias, que a comunicação do incidente seja realizada pelo controlador nos meios de divulgação disponíveis, com direta e fácil visualização pelo período de, no mínimo, seis meses.

2.10.5. Observa-se, ainda, que o presente capítulo previu a possibilidade de que a ANPD determine a comunicação de incidente de segurança ao titular, caso o controlador não tenha o feito, ou que refaça a comunicação a este, se verificado que não foram contempladas todas as informações exigidas para tanto, ou se porventura o controlador utilizou-se de meios inadequados para fazê-la.

2.10.6. Destaca-se, por fim, que foi incluída previsão no sentido de que o titular pode, a qualquer momento, solicitar esclarecimentos ao controlador sobre o incidente de segurança, os quais deverão ser respondidos em até 5 (cinco) dias úteis.

2.10.7. O prazo previsto de 5 (cinco) dias úteis buscou alinhamento ao prazo previsto no art. 13 do Decreto nº 11.034, de 05 de abril de 2022, que dispõe que as demandas do consumidor serão respondidas no prazo de sete dias corridos, contado da data de seu registro.

2.10.8. Assim sendo, a redação do Capítulo VI dispõe o seguinte:

CAPÍTULO VI

DA COMUNICAÇÃO DO INCIDENTE AO TITULAR DE DADOS PESSOAIS

Art. 15. A comunicação do incidente de segurança com dados pessoais ao titular deverá ser realizada pelo controlador, no prazo de 3 (três) dias úteis a partir do conhecimento do incidente de segurança, sempre que o incidente possa acarretar risco ou dano relevante aos titulares afetados e deve conter as seguintes informações:

I - descrição da natureza e da categoria de dados pessoais afetados;

II - riscos ou impactos ao titular;

III - indicação das medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente, quando cabíveis;

IV - data do conhecimento do incidente de segurança; e

V - informações de contato para obtenção de informações e dados do encarregado, quando aplicável.

§ 1º A comunicação do incidente aos titulares de dados deverá atender aos seguintes critérios:

I - fazer uso de linguagem simples e de fácil entendimento; e

II - ocorrer de forma direta e individualizada, caso seja possível identificá-los.

§ 2º Caso a comunicação direta e individualizada se mostre inviável ou não seja possível determinar, parcial ou integralmente, os titulares afetados, no prazo de 3 (três) dias úteis, o controlador deverá comunicar a ocorrência do incidente de segurança, com as informações definidas no caput, imediatamente, nos meios de divulgação disponíveis, tais como na sua página na Internet, em aplicativos, em suas mídias sociais e em canais de atendimento ao titular, de modo que permita o conhecimento amplo, com direta e fácil visualização pelo período de, no mínimo, seis meses.

§ 3º A ANPD poderá determinar que o controlador comunique o incidente de segurança ao titular, caso não tenha sido realizado, ou que faça nova comunicação, caso a primeira não contenha todas as informações necessárias ou tenha utilizado meios inadequados.

§ 4º Os titulares dos dados poderão solicitar ao controlador, a qualquer momento, esclarecimentos sobre o incidente de segurança, tais como, dados afetados, riscos e medidas de segurança adotadas, que deverão ser respondidos em até 5 (cinco) dias úteis.

§ 5º Será considerada boa prática para fins do disposto no art. 52, §1º, IX da LGPD, a inclusão na comunicação ao titular de recomendações para reduzir os efeitos do incidente.

§ 6º Considera-se comunicação de forma individualizada e direta aquela realizada pelos meios usualmente utilizados pelo controlador para contatar o titular, tais como, telefone, e-mail, mensagem eletrônica ou carta.

2.11. Do processo de comunicação do incidente de segurança

2.11.1. O Capítulo VII da proposta de regulamento trata do processo de comunicação de incidente de segurança, inclusive da apuração daqueles que a Autoridade tomar conhecimento sem a devida comunicação pelo controlador.

2.11.2. Nos termos da competência fiscalizadora da Autoridade, o referido Capítulo prevê que poderão ser realizadas auditorias ou inspeções junto aos agentes de tratamento de forma a se obter subsídios para o processo de comunicação do incidente de segurança.

2.11.3. Por fim, o Capítulo traz procedimentos administrativos necessários para o melhor cumprimento da norma, tanto pela Administração quanto pelos administrados, tais como hipóteses de arquivamento e previsão de monitoramento e fiscalização.

2.11.4. Importa esclarecer que, mesmo no caso de arquivamento do processo de comunicação do incidente, resta preservada a competência fiscalizadora da Autoridade e o indício de eventuais descumprimentos de obrigações poderá ensejar a abertura de processo administrativo sancionador.

2.11.5. Assim, o Capítulo VII traz a seguinte proposta:

CAPÍTULO VII

DO PROCESSO DE COMUNICAÇÃO DO INCIDENTE DE SEGURANÇA

Art. 16. A ANPD poderá apurar a ocorrência de incidentes de segurança com dados pessoais de que venha a tomar conhecimento por meio do procedimento de apuração de incidente.

Art. 17. Caso a ANPD identifique a ocorrência de incidente de segurança que possa ocasionar risco ou dano relevante aos titulares, que não lhe tenha sido comunicado, poderá instaurar processo administrativo sancionador para apurar o descumprimento do previsto no art. 11 deste regulamento.

Art. 18. O procedimento de apuração de incidente poderá ser arquivado nas seguintes hipóteses:

I - o controlador apresentar o comunicado de incidente de segurança e não serem necessárias ações complementares;

II - o incidente não envolver dados pessoais;

III - a ANPD considerar que o incidente não acarreta risco ou dano relevante aos titulares de dados; ou

IV - não sejam identificadas pela ANPD evidências suficientes da ocorrência do incidente, ressalvada a possibilidade de desarquivamento caso surjam fatos novos.

Parágrafo único. Nas hipóteses dos incisos III e IV, mesmo com a decisão do arquivamento do procedimento de apuração do

incidente, a ANPD poderá determinar a adoção de medidas de segurança, técnicas e administrativas, no intuito de salvaguardar os direitos dos titulares.

Art. 19. A ANPD poderá, a qualquer momento, realizar auditorias ou inspeções junto aos agentes de tratamento para coletar informações complementares ou validar as informações recebidas, com o objetivo de subsidiar as decisões no âmbito do processo de comunicação do incidente de segurança.

Art. 20 O processo de comunicação de incidente poderá ser arquivado sumariamente nas seguintes hipóteses:

I – se a ANPD considerar que o incidente não acarreta risco ou dano relevante aos titulares de dados; ou

II - se não existir legitimidade do notificante.

§ 1º Na hipótese de arquivamento do processo de comunicação do incidente, poderá ser aberto processo administrativo sancionador para apurar eventuais descumprimentos de obrigações.

§ 2º As comunicações de incidente integrarão o cálculo dos indicadores do ciclo de monitoramento vigente na data de seu registro nos sistemas da ANPD.

§ 3º Caso o notificante não tenha legitimidade para realizar a comunicação poderá ser aberto procedimento de apuração de incidente.

2.12. Da determinação de providências para a salvaguarda dos direitos dos titulares

2.12.1. Propõe-se, na Seção I do Capítulo VII, que avaliada a gravidade, a ANPD poderá determinar ao controlador a adoção das providências indicadas no art. 48, §2º, da LGPD, quais sejam: i) ampla divulgação do incidente em meios de comunicação; ou ii) medidas para reverter ou mitigar os efeitos do incidente. Mostra-se necessário, contudo, em vista das particularidades de cada incidente, prever que outras determinações para a salvaguarda dos direitos dos titulares poderão ser adotadas pela ANPD na avaliação do caso concreto, desde que diretamente relacionadas ao incidente.

2.12.2. Ainda com vistas a resguardar os titulares de dados pessoais afetados pelo incidente, o Capítulo prevê que a ANPD poderá divulgar em sua página na Internet informações relativas a incidentes de segurança com dados pessoais, com o objetivo de trazer maior transparência, segurança e orientações aos titulares afetados, observados os segredos comercial e industrial.

2.12.3. Para melhor delinear as determinações previstas em lei, propõe-se que a ampla divulgação em meios de comunicação será determinada quando a comunicação realizada pelo controlador se mostrar insuficiente para

alcançar parcela significativa dos titulares afetados pelo incidente. Ademais, descreveu-se alguns exemplos de meio de comunicação, como mídia escrita impressa, radiodifusão de sons e imagens e transmissão de informações pela Internet, para facilitar a compreensão e cumprimento do dispositivo regulamentar.

2.12.4. Do mesmo modo, no que concerne as medidas para reverter ou mitigar os efeitos do incidente, propõe-se que serão consideradas aquelas que possam garantir a confidencialidade, integridade e disponibilidade dos dados pessoais afetados.

2.12.5. Cabe destacar que o art. 22 esclarece que as providências contidas nesta seção não são sanções, mas são equiparadas às medidas preventivas do processo de fiscalização e sanção.

2.12.6. A Seção I também propõe, no art. 27 da minuta, a possibilidade de a Coordenação-Geral de Fiscalização poder determinar ao controlador a adoção imediata de medidas necessárias para salvaguardar direitos dos titulares ou para reverter ou mitigar os efeitos do incidente sem prévia manifestação do controlador, nos termos do art. 45 da Lei nº 9.784, de 29 de janeiro de 1999, que regula o processo administrativo no âmbito da Administração Pública Federal.

2.12.7. Tal dispositivo é necessário devido à necessidade de tutela da urgência em alguns casos de comunicação de incidentes, como por exemplo, casos em que vazamentos de dados pessoais podem causar graves danos morais ou materiais aos titulares de dados, inclusive em grupos de vulneráveis, tais como, crianças, adolescentes e idosos.

2.12.8. Assim, o texto proposto para a Seção é o seguinte:

Seção I

Da Determinação de Providências para a Salvaguarda dos Direitos dos Titulares

Art. 21. Avaliada a gravidade do incidente, a ANPD poderá determinar ao controlador a adoção das seguintes providências para a salvaguarda dos direitos dos titulares, dentre outras:

I - ampla divulgação do incidente em meios de comunicação; ou

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

§ 1º As providências citadas no caput devem estar diretamente relacionadas ao incidente de segurança.

§ 2º A depender da complexidade das providências para a salvaguarda dos direitos dos titulares a serem exigidas ao controlador, as determinações poderão ser feitas, em processo administrativo apartado, por meio de solicitação de regularização ou plano de conformidade, nos termos do art. 32, III e IV, do Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de

Proteção de Dados, aprovado pela Resolução nº CD/ANPD nº 1, de 28 de outubro de 2021.

§ 3º A ANPD poderá divulgar em sua página na Internet informações relativas a incidentes de segurança com dados pessoais, com o objetivo de trazer maior transparência, segurança e orientações aos titulares afetados, observados os segredos comercial e industrial.

Art. 22. As providências descritas nesta Seção não constituem sanções ao agente regulado, sendo equiparadas às medidas preventivas dispostas no Capítulo IV, Título II do Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados, aprovado pela Resolução CD/ANPD nº 1, de 28 de outubro de 2021.

Art. 23. A ANPD poderá determinar ampla divulgação do incidente em meios de comunicação para a salvaguarda dos direitos dos titulares, nos termos do art. 48, § 2º, I da LGPD, quando a comunicação realizada pelo controlador se mostrar insuficiente para alcançar parcela significativa dos titulares afetados pelo incidente.

§ 1º O meio de ampla divulgação do incidente em meios de comunicação deverá ser compatível com a abrangência de atuação do agente de tratamento de dados e a localização dos titulares dos dados pessoais afetados no incidente.

§ 2º A ampla divulgação do incidente poderá ser viabilizada em meio físico ou digital, considerada sempre a necessidade de se atingir o maior número possível de titulares afetados, admitidos os seguintes meios de veiculação, dentre outros:

I – mídia escrita impressa;

II – radiodifusão de sons e de sons e imagens; ou

III – transmissão de informações pela Internet.

Art. 24. Para a determinação das medidas serão consideradas aquelas que possam garantir a confidencialidade, integridade e disponibilidade dos dados pessoais afetados, bem como as medidas para minimizar os efeitos decorrentes do incidente.

Art. 25. A ANPD realizará o monitoramento do cumprimento das determinações e da implantação das medidas, com base em critérios de priorização.

Art. 26. A ANPD poderá instaurar processo administrativo sancionador caso o controlador não adote as medidas para reverter ou mitigar os efeitos do incidente no prazo determinado pela Autoridade.

Parágrafo único. O não atendimento, ou o atendimento fora do prazo ou incompleto das medidas determinadas pela ANPD será considerado agravante caso seja instaurado o processo administrativo sancionador.

Art. 27. Excepcionalmente, a Coordenação-Geral de Fiscalização poderá determinar ao controlador a adoção imediata de medidas necessárias para salvaguardar direitos dos titulares ou para reverter ou mitigar os efeitos do incidente sem prévia manifestação do controlador, nos termos do art. 45 da Lei nº 9.784, de 29 de janeiro

de 1999, que regula o processo administrativo no âmbito da Administração Pública Federal.

Parágrafo único. As medidas referidas no caput devem estar diretamente relacionadas ao incidente de segurança e à salvaguarda dos direitos dos titulares.

Do encerramento do processo de comunicação de incidente de segurança

2.13. Do encerramento do processo de comunicação de incidente de segurança

2.13.1. A minuta prevê, na Seção II do Capítulo VII, que tendo sido adotadas as determinações cabíveis e não havendo medidas adicionais a serem prescritas, o processo de comunicação de incidente de segurança poderá ser encerrado. O objetivo da proposição é trazer transparência e segurança jurídica aos agentes públicos e administrados.

2.13.2. O texto proposto traz o que segue:

Seção II

Do Encerramento do Processo de Comunicação de Incidente de Segurança

Art. 28. O processo de comunicação de incidente de segurança será encerrado após a análise, considerando que foi constatado a devida comunicação à autoridade e aos titulares e não são necessárias medidas adicionais para mitigação de seus efeitos.

2.14. Das disposições finais

2.15. No que tange às disposições finais, o art. 29 da presente minuta, em harmonia com o preceituado pelo art. 14 da Lei nº 13.105, de 16 de março de 2015, determina que as disposições desta proposta de regulamento se aplicarão desde logo aos processos de comunicação de incidentes de segurança em curso, respeitados os atos já praticados.

2.16. Isso se justifica em razão dos casos comunicados atualmente em análise pela ANPD.

2.17. Nesse sentido, a redação do Capítulo XII proposta é a seguinte:

CAPÍTULO XII

DAS DISPOSIÇÕES FINAIS

Art. 29. Ao entrar em vigor este regulamento, suas disposições se aplicarão desde logo aos processos de comunicação de incidentes de segurança em curso, respeitados os atos já praticados.

3. ANEXO

- 3.1. Relatório de Análise de Impacto Regulatório de comunicação de incidentes de segurança (SEI nº 3632102)
- 3.2. Fluxograma do processo de comunicação de incidentes de segurança (SEI nº 3627707)
- 3.3. Minuta do Regulamento de Comunicação de Incidentes de Segurança (SEI nº 3633083)

4. CONCLUSÃO

4.1. A presente Nota Técnica apresenta a proposta de Resolução que dispõe sobre Regulamento de Comunicação de Incidente de Segurança com Dados Pessoais (SEI nº 3633088), com a definição de quais incidentes acarretam risco ou dano relevante, com a fixação de prazo para comunicação à ANPD e aos titulares e o estabelecimento do tratamento dos incidentes comunicados à Autoridade.

4.2. Espera-se que o regulamento facilite a identificação dos incidentes de segurança que necessariamente deverão ser comunicados à Autoridade e possa 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.

4.3. Diante do exposto, encaminha-se a minuta de proposta de ato normativo anexa (SEI nº 3633083) e o Relatório de AIR (SEI nº 3632342) à Procuradoria da ANPD para análise.

À consideração superior.

Brasília, 16 de setembro de 2022.

ANDRESSA GIROTTO VARGAS

Especialista na Coordenação-Geral de Normatização

SABRINA FERNANDES MACIEL FAVERO

Especialista em Políticas Públicas e Gestão Governamental

De acordo. Encaminha-se o presente processo à Procuradoria da ANPD para análise.

Brasília, 16 de setembro de 2022.

RODRIGO SANTANA DOS SANTOS

Coordenador-Geral de Normatização Substituto

[1] Contribuíram na qualidade de representantes do Setor Privado: Ajinomoto; ANAHP; ANBC; Associação Nacional dos Fabricantes de Veículos Automotores (ANFAVEA); ASBZ Advogados; Federação das Associações das Empresas Brasileiras de Tecnologia da Informação (ASSESPRO); AUDITSAFE Auditoria e Consultoria em Riscos Corporativos Ltda; Banco Rabobank International Brasil S/A; Baptista Luz Advogados; Barral Parente e Pinheiro Advogados; Associação Brasileira das Empresas de Tecnologia da Informação e Comunicação (BRASSCOM); Brotto e Campelo Advogados; BSA – The Software Alliance; Centre for Information Policy Leadership (CIPL); Comissão de Mediação e Métodos Consensuais da OAB/RJ; Confederação Nacional das Instituições Financeiras (CNF); Confederação Nacional das Seguradoras (CNSeg); Confederação Nacional de Saúde (CNSaúde); Confederação Nacional do Transporte (CNT); COTS Advogados; Datablock Proteção de Dados Ltda; DaVita Brasil Participações e Serviços de Nefrologia Ltda; Davita Healthcare Brasil Serviços Médicos Ltda; Dr. Oetker Brasil Ltda; Elo Participações Ltda; Federação das Indústrias do Estado de São Paulo (FIESP); FIRJAN; FSFX; FUNEF; Gardemann & Vidotti Advogados Associados; Grupo Financeiro BMG; Hughes Telecomunicações Do Brasil Ltda; IAB Brasil (AMI - Associação de Mídia Interativa); Information Technology Industry (ITI); KPMG Auditores Independentes; Lima ≡ Feigelson Sociedade de Advogados; Loeser e Hadad Advogados; Moraes Andrade, Leandrin, Molina Sociedade de Advogados; NBFA Advogados; Ouriques Cruz Advocacia Empresarial; PDK Advogados; Pimentel, Vega, Souza Advogados; Pricewaterhousecoopers Tecnologia da Informação Ltda; Rodoil Distribuidora de Combustíveis S.A; Sindicato Nacional das Empresas de telefonia e de Serviço Móvel celular e Pessoal - Conexis Brasil Digital; Sindicato da Indústria de Produtos Farmacêuticos (SINDUSFARMA); Soluções Inteligentes Em Telecomunicações Ltda (SOLINTEL); Tiago Neves Furtado - Opice Blum Advocacia (Clientes do setor de óleo e combustíveis, GLP, armazenagem de grânéis líquidos, Indústria de especialidades químicas, plataforma de pagamentos digitais e varejo farmacêutica); TozziniFreire, Teixeira e Silva, Freire Advogados; Tramontina Central de Administração Ltda;

Tudo sobre IOT; Unimed Belo Horizonte Cooperativa De Trabalho Médico; Usina Termelétrica Norte Fluminense SA; Vezzi Lapolla e Mesquita Advogados e Vilarinho Scarel Sociedade De Advogados.

[2] Contribuíram na qualidade de representantes da Sociedade Civil: Associação Nacional Dos Peritos Em Computação Forense, Associação Parque Tecnológico São José Dos Campos, Coreit-Data Center, Serviços Gerenciados e Infraestrutura em Ti Ltda., Coresec Segurança Da Informação Ltda., Energy Telecom Comércio e Serviços Ltda., Energy Telecom Sul Segurança Da Informação Ltda, Instituto Ctem+; CAC OAB SP Pinheiros e CWC LGPD; Câmara Brasileira da Economia Digital (CAMARA-E.NET); Centro de Estudos em Políticae Economia Do Setor Público | EESP e EASP | Fundação Getulio Vargas; Data Privacy; Federação Brasileira de Bancos – (FEBRABAN); Federação das Associações Comerciais e Empresariais do Estado Do Paraná; Federação das indústrias do Estado de Minas Gerais (FIEMG); Federação do Comércio de Bens, Serviços e Turismo do Estado de São Paulo (FECOMERCIO/SP); Grupo de Estudos Estratégicos em Segurança da Informação e Proteção de Dados Pessoais; Iagor Augusto; Instituto Brasileiro de Defesa do Consumidor (Idec); Instituto Paranaense De Compliance – Grupo de Trabalho da Lei Geral de Proteção de Dados (GT-LGPD); Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec); Instituto de Referência em Internet e Sociedade (IRIS); Instituto de Tecnologia e Sociedade (ITS Rio); Jairo William Pereira; José Antonio Maurilio Milagre de Oliveira; Kely Cristina Genebra; Laboratório de Políticas Públicas e Internet (LAPIN); LGPD Acadêmico; Luciane Joana Quipers; Núcleo de Informação e Coordenação do Ponto BR – NIC.br, Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil – CERT.br; Sociedade Beneficente Israelita Brasileira Hospital Albert Einstein – SBIBHAE e ZETTA.

[3] Contribuíram na qualidade de pessoas naturais: Ana Liz Vieira Soares e Armando Baltazar Palla de Medeiros.

[4] Contribuíram na qualidade de representantes do setor público: Agência Nacional de Aviação Civil (ANAC) e Financiadora de Estudos e Projetos (FINEP).

[5] Contribuíram na qualidade de membros da academia: Instituto Brasileiro de Defesa da Concorrência, Consumo e Comércio Internacional (IBRAC) e Universidade de São Paulo USP/Faculdade de Direito/Departamento de Direito Civil/Grupo de Pesquisa Direito Civil na Sociedade em Rede.



Documento assinado eletronicamente por **Rodrigo Santana dos Santos**, **Coordenador(a)-Geral substituto(a)**, em 16/09/2022, às 16:07, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Andressa Giroto Vargas, ANPD - Autoridade Nacional de Proteção de Dados**, em 16/09/2022, às 16:13, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



Documento assinado eletronicamente por **Sabrina Fernandes Maciel Favero, ANPD - Autoridade Nacional de Proteção de Dados**, em 16/09/2022, às 16:15, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade do documento pode ser conferida informando o código verificador **3632102** e o código CRC **447DC437** no site: https://super.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0
