PROJETO DE ADEQUAÇÃO À LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

FICHA TÉCNICA

GOVERNO DO ESTADO DE MINAS GERAIS

Governador do Estado de Minas Gerais
Gerais Romeu Zema

Vice-governador do Estado de Minas Gerais
Mateus Simões

Secretária de Estado de Planejamento e Gestão
Luisa Barreto

Controlador-Geral do Estado de Minas Gerais
Rodrigo Fontenelle de Araújo Miranda

Secretário de Estado de Fazenda
Gustavo de Oliveira Barbosa

Advogado-Geral do Estado de Minas Gerais
Sérgio Pessoa de Paula Castro

Diretor-Presidente da Companhia de Tecnologia da Informação de MG
Roberto Tostes Reis

Elaboração
Comitê Estadual de Proteção de Dados Pessoais

Contato:
cepdmg@prodemge.gov.br
https://www.mg.gov.br/lgpd

COMITÊ ESTADUAL DE PROTEÇÃO DE DADOS PESSOAIS

Secretaria de Estado de Planejamento e Gestão
Rodrigo Diniz Lara
Fábrício de Barros Salum
Daniel Machado Maia

Controladoria-Geral do Estado
Beatriz Faria de Almeida Loureiro
Reginaldo Vieira Neres
Soraia Ferreira Quirino Dias

Secretaria de Estado de Fazenda
Rogério Zupo Braga
Anderson Aparecido Félix
Daniel de Oliveira Rezende

Advocacia-Geral do Estado
Marina Moretzsohn Trajano
Flávia Caldeira Brant
Maria Cristina Castro Diniz

Prodemge
Alander Antônio Faustino
Bruno Moreira Camargos Belo
Filipe Rodrigues Costa

FASE 5

SUMÁRIO

CONTEXTUALIZAÇÃO

1.1. Diagnóstico diferencial

Em complemento às análises realizadas na Fase 4, na qual foi enfatizada a gestão de riscos e seus impactos, sugere-se a execução do Diagnóstico de Maturidade em Segurança da Informação.

O propósito do diagnóstico é identificar problemas, investigar causas e buscar soluções estratégicas oportunas ao desenvolvimento da organização.

Para buscar um grau mais avançado de maturidade em segurança da informação em relação às obrigações definidas pela Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD) –, os órgãos e entidades públicas devem realizar amplas adaptações institucionais nos níveis estratégico, tático e operacional. Tais transformações abrangem:

- estruturar e aplicar medidas de segurança da informação, inclusive levantamento sobre necessidades específicas, e

- promover ações de conscientização de lideranças, servidores, terceirizados, estagiários e demais colaboradores do órgão ou entidade, a fim de promover a segurança no cotidiano do trabalho.

Para acelerar positivamente a transformação interna do órgão ou da entidade, recomendam-se a consulta e o acesso aos guias e modelos e às medidas de treinamento e desenvolvimento disponíveis no site da Autoridade Nacional de Proteção de Dados (ANPD).

2. FINALIDADE DO DIAGNÓSTICO

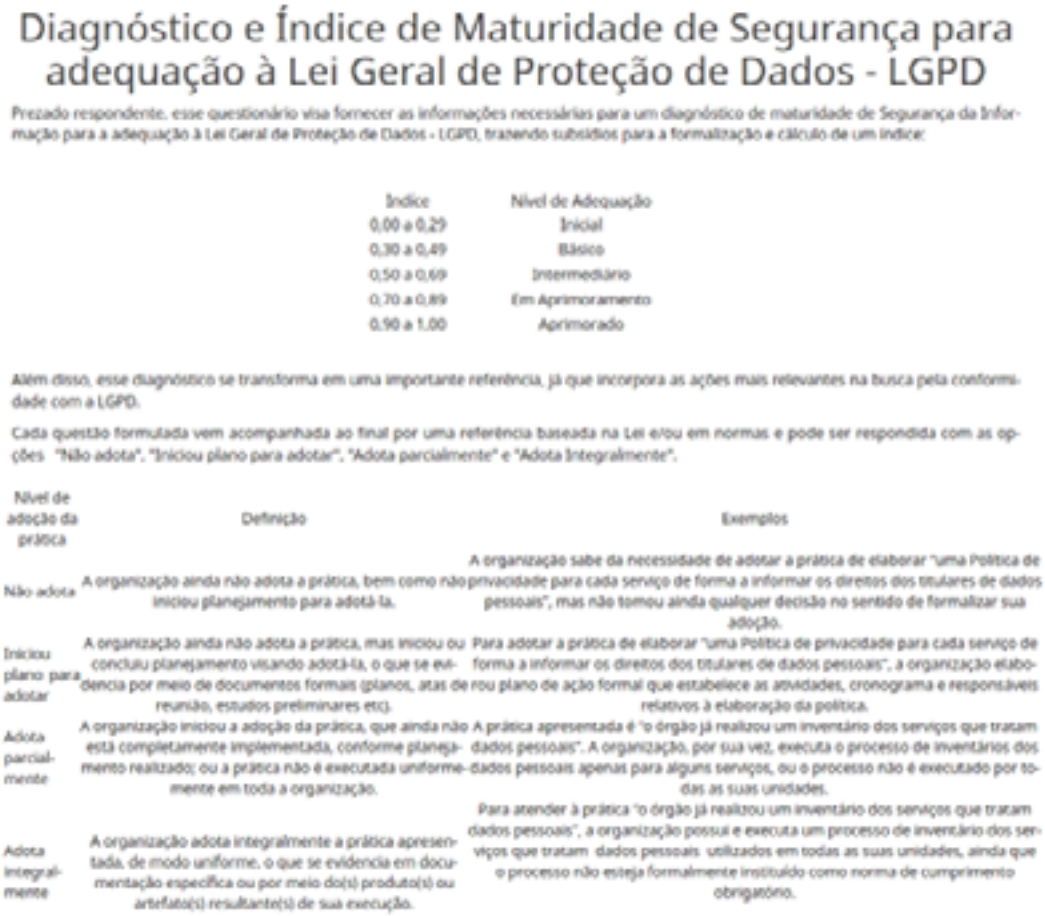
Está disponível no link abaixo o questionário que tem como objetivo fornecer ao órgão respondente as informações necessárias para um diagnóstico de maturidade de segurança para adequação à LGPD.

O resultado e as respostas apresentarão um índice de maturidade que possibilitará aos órgãos e às entidades o direcionamento de esforços e a priorização das ações necessárias para aumentar a conformidade à LGPD.

Os resultados do diagnóstico têm caráter meramente informativo. Competirá ao órgão ou à entidade interessada adotar as medidas organizacionais internas para que sua instituição aumente a conformidade à referida lei.

3. ACESSO AO QUESTIONÁRIO

Para efetuar o diagnóstico, clique no link e preencha o questionário para obter o resultado.



Diagnóstico e Índice de Maturidade de Segurança para adequação à Lei Geral de Proteção de Dados - LGPD

Prezado respondente, esse questionário visa fornecer as informações necessárias para um diagnóstico de maturidade de Segurança da Informação para a adequação à Lei Geral de Proteção de Dados - LGPD, trazendo subsídios para a formalização e cálculo de um índice.

Índice	Nível de Adequação
0,00 a 0,29	Inicial
0,30 a 0,49	Básico
0,50 a 0,69	Intermediário
0,70 a 0,89	Em Aprimoramento
0,90 a 1,00	Aprimorado

Além disso, esse diagnóstico se transforma em uma importante referência, já que incorpora as ações mais relevantes na busca pela conformidade com a LGPD.

Cada questão formulada vem acompanhada ao final por uma referência baseada na Lei e/ou em normas e pode ser respondida com as opções "Não adota", "Iniciou plano para adotar", "Adota parcialmente" e "Adota Integralmente".

Nível de adoção da prática	Definição	Exemplos
Não adota	A organização ainda não adota a prática, bem como não iniciou planejamento para adotá-la.	A organização sabe da necessidade de adotar a prática de elaborar "uma Política de privacidade para cada serviço de forma a informar os direitos dos titulares de dados pessoais", mas não tomou ainda qualquer decisão no sentido de formalizar sua adoção.
Iniciou plano para adotar	A organização ainda não adota a prática, mas iniciou ou concluiu planejamento visando adotá-la, o que se evidencia por meio de documentos formais (planos, atas de reunião, estudos preliminares etc).	Para adotar a prática de elaborar "uma Política de privacidade para cada serviço de forma a informar os direitos dos titulares de dados pessoais", a organização elaborou plano de ação formal que estabelece as atividades, cronograma e responsáveis relativos à elaboração da política.
Adota parcialmente	A organização iniciou a adoção da prática, que ainda não está completamente implementada, conforme planejamento realizado; ou a prática não é executada uniformemente em toda a organização.	A prática apresentada é "o órgão já realizou um inventário dos serviços que tratam dados pessoais". A organização, por sua vez, executa o processo de inventários dos dados pessoais apenas para alguns serviços, ou o processo não é executado por todas as suas unidades.
Adota integralmente	A organização adota integralmente a prática apresentada, de modo uniforme, o que se evidencia em documentação específica ou por meio do(s) produto(s) ou artefato(s) resultante(s) de sua execução.	Para atender à prática "o órgão já realizou um inventário dos serviços que tratam dados pessoais", a organização possui e executa um processo de inventário dos serviços que tratam dados pessoais utilizados em todas as suas unidades, ainda que o processo não esteja formalmente instituído como norma de cumprimento obrigatório.

4. CONCLUSÃO

Ao final da execução do diagnósto previsto na fase 4 e do diagnóstico descrito nesta fase, os órgãos e entidades serão capazes de identificar as causas e priorizar os riscos a serem mitigados, consequentemente, aumentando a conformidade à LGPD.

Sugere-se a elaboração de planilha contendo as informações relativas às causas, riscos, definição de prioridades, responsáveis e cronograma de atividades, contendo prazos para adoção das medidas corretivas diante dos riscos identificados.

Este documento foi elaborado no intuito de apresentar um padrão mínimo a ser realizado por cada órgão/entidade, não tendo a intenção de esgotar o tema nem engessar possíveis propostas dos órgãos, as quais podem ser superiores à presente.

O desenvolvimento conjunto e o aprimoramento das atividades institucionais visa à eficiência e ao aperfeiçoamento de todos na prestação do serviço público.

PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA COM DADOS PESSOAIS

Fluxo de comunicação

O presente documento faz parte de uma estratégia de resposta a incidentes de segurança com dados pessoais, e visa apresentar boas práticas e medidas a serem adotadas pelos órgãos e entidades da Administração Pública estadual diante de eventuais incidentes de segurança envolvendo dados pessoais tratados no âmbito institucional.

Trata-se de medidas a serem observadas como referência, sendo que cada órgão/entidade deverá zelar pela proteção e pelo tratamento adequado dos dados.

Este fluxo foi elaborado pelo Comitê Estadual de Proteção de Dados Pessoais (CEPD), e é fundamentado em diversas publicações, dentre as quais: Comunicação de incidente de segurança[1](ANPD), Guia do Framework de Privacidade e Segurança da Informação[2], Guia de Resposta a Incidentes de Segurança[3].

O documento não pretende esgotar o tema, podendo ser revisado e complementado por atualizações e boas práticas que venham a se apresentar como adequadas oportunamente.

[1] Disponível em: <https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis>. Acesso em: 24/11/2023.

[2] Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_framework_psi.pdf>. Acesso em: 24/11/2023.

[3] Disponível em: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_resposta_incidentes.pdf>. Acesso em: 24/11/2023.

Introdução

Em observância ao disposto na Lei nº 13.709, de 14 de agosto de 2018 (LGPD), especialmente no capítulo VII "Da Segurança e Das Boas Práticas", que prevê que "os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito", cabe à Administração Pública zelar pelo tratamento adequado dos dados pessoais sob sua gestão.

O Poder Público é responsável ainda por adotar medidas de proteção, segurança e gestão de eventuais incidentes de segurança relacionados aos dados pessoais sob sua custódia, diante de potenciais riscos ou danos relevantes aos titulares de dados pessoais.

Neste contexto, o presente fluxo apresenta propostas e medidas de segurança a serem observadas, diante de eventuais incidentes de segurança envolvendo dados pessoais tratados no âmbito da Administração Pública estadual.

Conceitos e definições

Neste documento, foram adotados os seguintes termos e respectivos conceitos[4]:

Agentes de tratamento: o controlador e o operador

Autoridade Nacional de Proteção de Dados: Autarquia de Natureza Especial responsável por zelar, implementar e fiscalizar o cumprimento da Lei nº 13.709, de 14 de agosto de 2018 (LGPD) em todo o território nacional, conforme as atribuições descritas no art. 55-J da LGPD e no Decreto nº 10.474, de 26 de agosto de 2020.

Controlador: é a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. É responsável pelas principais decisões sobre o tratamento de dados pessoais e por definir a finalidade desse tratamento.

Dado pessoal: toda informação relacionada a pessoa natural identificada ou identificável.

Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Incidente de segurança com dados pessoais: evento adverso confirmado que comprometa a confidencialidade, integridade ou disponibilidade de dados pessoais. Pode decorrer de ações voluntárias ou acidentais que resultem em divulgação, alteração, perda ou acesso não autorizado a dados pessoais, independentemente do meio em que estão armazenados.

[4] Conceitos extraídos da Lei Federal nº 13.709/2018; LGPD: quem é quem?; Comunicação de incidente de segurança (ANPD) Art. 6º, inc. VIII da Lei nº 13.709/2018

LGPD: Lei Federal nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais.

Operador: é o agente responsável por realizar o tratamento de dados em nome do controlador e conforme a finalidade por este delimitada. Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

Titular de dados pessoais: é a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento. São as pessoas, os cidadãos, sejam adultos ou crianças, servidores públicos ou não.

ORIENTAÇÕES RELATIVAS A INCIDENTES DE SEGURANÇA COM DADOS PESSOAIS

A LGPD dispõe que as atividades de tratamento de dados pessoais devem observar a boa-fé e, dentre outros, o princípio da prevenção. Tal princípio consiste na adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais[5].

Para este fluxo de comunicação, considera-se a definição de incidente de segurança com dados pessoais apresentada pela ANPD: evento adverso confirmado que comprometa a confidencialidade, integridade ou disponibilidade de dados pessoais. Pode decorrer de ações voluntárias ou acidentais que resultem em divulgação, alteração, perda ou acesso não autorizado a dados pessoais, independentemente do meio em que estão armazenados.

Se mesmo com a adoção das medidas de proteção vier a ocorrer um incidente de segurança com dados pessoais, algumas medidas visando mitigar os danos devem ser tomadas:

[5] Art. 6º, inc. VIII da Lei nº 13.709/2018

1. Análise interna do incidente para reunir informações sobre o evento:

a) identificar a quantidade e a categoria de dados afetados;
b) identificar a quantidade e a categoria de titulares potencialmente afetados;
c) analisar as possíveis consequências do incidente para os titulares e para a instituição;
d) realizar análise de risco relativa ao incidente;
e) registrar as evidências do incidente.

2. Comunicação ao encarregado sobre o incidente.

3. Comunicação ao controlador sobre o incidente.

4. Comunicação à ANPD, ao titular de dados pessoais e ao Comitê Estadual de Proteção de Dados (CEPD) sobre o incidente.

5. Emissão de relatório em que constem as informações registradas sobre o incidente, assim como outras informações pertinentes, tais como: as ações adotadas para tratamento, medidas para melhorias relativas às ações de gestão e contingenciamento de incidentes, lições aprendidas.
O fluxo a seguir demonstra o processo acima descrito, de modo sucinto:

Fluxograma da comunicação de incidentes de segurança com dados pessoais

Fonte: elaboração própria, baseada em figura do Guia de Resposta a Incidentes

MEDIDAS E PROCEDIMENTOS DE COMUNICAÇÃO

A seguir, estão descritas de forma simplificada as medidas a serem adotadas diante da ocorrência de incidentes de segurança com dados pessoais.

1. Análise do incidente

Mediante a suspeita de incidente de segurança, deve-se realizar análise interna a fim de confirmar o evento.

Incidentes de segurança podem decorrer de atos acidentais ou intencionais

Note que tanto o efeito de atos acidentais ou de atos intencionais podem configurar incidentes de segurança com dados pessoais. Como exemplo de eventos acidentais, cita-se o envio de informações para destinatário incorreto. Já os casos como a invasão de um sistema de informação ou o furto de um dispositivo de armazenamento de dados, configurariam atos intencionais.

Incidentes de segurança não são somente aqueles que expõem os dados indevidamente

Não se consideram somente as violações de confidencialidade ou a divulgação indevida de dados pessoais como incidentes de segurança. A perda, ou indisponibilidade de dados pessoais, o sequestro de dados (ransomware) e o acesso não autorizado a dados armazenados em sistemas de informação são exemplos de incidentes de segurança.

No processo de análise interna, deve-se buscar identificar informações como:

a) Vulnerabilidade exposta no incidente, ou seja, qual foi a forma ou o meio que possibilitou a ocorrência do incidente. Dentre as situações possíveis estão: acesso indevido a dados pessoais; comprometimento de credenciais ou senhas de acesso; transmissão indevida de dados pessoais; roubo/sequestro de dados pessoais; ataques cibernéticos; erros de programação de aplicativos e sistemas; descartes indevidos; falhas/erros de sistemas e outras.

b) Fonte ou origem dos dados pessoais: a identificação da fonte a partir da qual os dados foram obtidos pode permitir, dentre outras ações, recuperar os dados. Deve-se verificar se os dados foram obtidos a partir de formulários preenchidos pelo titular, ou por compartilhamento, cookies e outros meios.

c) Categoria de dados pessoais: conforme a categorização já realizada na instituição, pode-se verificar os tipos de dados afetados, como: dados pessoais sensíveis e dados pessoais de crianças e adolescentes.

d) Extensão do incidente: identificar a quantidade de dados e de titulares potencialmente afetados.

e) Impacto ao titular: avaliar os potenciais riscos ou danos relevantes que o incidente pode causar para os titulares dos dados pessoais afetados.

f) Impacto institucional: avaliar os potenciais impactos que o incidente pode acarretar à instituição, como impactos no exercício das atividades institucionais, dano reputacional, perda de confiança dos titulares para com a instituição, impactos relativos a contratos com fornecedores, sanções administrativas, ações judiciais.

Todas as informações sobre o incidente devem ser registradas, de modo mais completo possível, o que inclui, não somente: registro de comunicações e reuniões realizadas, medidas adotadas e logs dos sistemas envolvidos no incidente.

Deve-se considerar, nesse momento, a elaboração do Relatório de Impacto à Proteção de Dados Pessoais, tendo em vista que tal documento poderá vir a ser solicitado pela ANPD.

2. Comunicação ao encarregado e controlador

Para viabilizar uma resposta rápida e eficaz a incidentes de segurança com dados pessoais, é fundamental que as organizações estabeleçam um fluxo de comunicação interna claro e eficiente. O objetivo é possibilitar que eventuais incidentes sejam identificados e reportados tempestivamente, permitindo uma ação oportuna. A rapidez na comunicação é essencial para minimizar possíveis danos.
O agente público, colaborador, fornecedor ou parte interessada deve reportar o incidente ao encarregado pela proteção de dados pessoais. Note-se que diante de suspeita ou confirmação de incidente, a comunicação poderá ser feita por qualquer parte, seja: agente público, titular de dados pessoais, operador, fornecedor, parceiro, cliente, prestador de serviço etc.

Quando aplicável, o operador deve prontamente comunicar incidentes ao controlador para permitir que este tome as ações necessárias.

3. Confirmação de potencial risco ou dano relevante

Na ausência de regulamentação que defina com precisão o que caracteriza risco ou dano relevante, a Autoridade Nacional de Proteção de Dados propõe recomendações a serem consideradas para avaliar se um incidente de segurança deve ser comunicado aos titulares e à ANPD.

Inicialmente, deve-se observar se o incidente engloba todos os critérios abaixo listados:

- ocorrência confirmada;
- contém dados pessoais sujeitos à proteção da LGPD;
- provoca risco ou dano relevante aos titulares dos dados.

Para auxiliar na avaliação sobre o incidente e sobre se ele pode acarretar risco ou dano relevante, a ANPD cita alguns exemplos, como[6]:

- A invasão de uma rede de computadores de uma instituição financeira por um agente malicioso que realize a cópia não autorizada de uma base de dados contendo dados pessoais dos correntistas, tais como extratos bancários, números de cartões de crédito e senhas viola o sigilo bancário dos titulares e os expõe a risco de fraudes e danos morais e materiais.
- A indisponibilidade prolongada de um sistema utilizado por uma rede hospitalar em razão de um incidente de sequestro de dados, impedindo o acesso aos dados dos pacientes ou a realização de procedimentos médicos, pode expor dados pessoais sensíveis dos titulares e causar-lhes riscos ou danos à saúde.
- A perda ou roubo de documentos ou dispositivos de armazenamento de dados que contenham dados pessoais protegidos por sigilo profissional, cópia de documentos de identificação oficial e dados de contato dos titulares pode expô-los a riscos reputacionais e de sofrer fraudes financeiras.

6 https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis

Há fatores que, combinados, podem reduzir o potencial risco aos titulares, e isso deverá ser ponderado conforme o caso concreto. Em casos como os exemplificados a seguir, o uso de medidas de proteção e prevenção contribuem para mitigar riscos: a proteção de dados por criptografia, o uso de ferramentas de segurança robustas que dificultam o acesso a dados em dispositivos, ainda que tenham sido furtados/roubados, e outras. Tudo isso deve ser considerado e ponderado na análise sobre os potenciais riscos ou danos relevantes ao titular e à instituição.

4. Comunicação à ANPD e/ou ao titular e Comitê Estadual de Proteção de Dados (se aplicável)

Havendo a confirmação ou, ainda, a suspeita de potencial risco ou dano relevante ao titular dos dados pessoais, o encarregado ou representante legal designado pelo controlador deverá comunicar o incidente à ANPD, aos titulares e ao CEPD.

A Autoridade Nacional de Proteção de Dados disponibiliza um formulário a ser preenchido e protocolado eletronicamente em seu sítio eletrônico. A ANPD recomenda que tais comunicações sejam feitas no prazo mais breve possível, em até 2 (dois) dias úteis da ciência do incidente. Segundo a própria Autoridade Nacional, "a comunicação voluntária do incidente pelo controlador é demonstração de transparência, cooperação e boa-fé do agente e será considerada em eventual ação de fiscalização da ANPD" [7].

Alguns critérios são úteis para análise do incidente, a fim de avaliar se há potencial risco ou dano relevante para os titulares, como definido no Guia de Resposta a Incidentes de Segurança[8]. As questões a seguir, dentre outras, podem ser realizadas:

[7] Ahttps://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis

[8] https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/ppsi/guia_resposta_incidentes.pdf

a) Quais informações foram objeto do incidente?
b) O titular pode ser vítima de fraude em razão do incidente?
c) O incidente foi devidamente comunicado às autoridades?
d) O que o titular pode fazer em benefício da sua proteção?
e) Onde o titular pode obter mais informações sobre o incidente?

Tais questões devem ser tomadas pela instituição como uma referência para auxiliar na análise do incidente. Conforme as especificidades do caso concreto, as perguntas acima deverão ser adaptadas. A partir daí, o encarregado poderá calibrar a comunicação com a ANPD e com os titulares.

Se constatado que o incidente pode acarretar risco ou dano relevante aos titulares, a comunicação deverá ocorrer, direta e individualmente, aos titulares, preferencialmente, por meio do canal já utilizado por aquela instituição para contato com o titular. Poderão ser usados os canais: e-mail, mensagens SMS, mensagens eletrônicas, cartas e outros. Não sendo possível identificar individualmente os titulares impactados, todos os titulares cujos dados potencialmente tenham sido afetados, deverão ser incluídos na comunicação.

O comunicado deve ser realizado com linguagem simples e clara, apresentando ao titular, pelo menos[9]:

1) Resumo e data da ocorrência do incidente;
2) Descrição dos dados pessoais afetados;
3) Riscos e consequências aos titulares de dados;
4) Medidas tomadas pelo controlador e as recomendadas aos titulares para mitigar os efeitos do incidente, se cabíveis;
5) Dados de contato do encarregado do controlador para que os titulares possam solicitar informações adicionais a respeito do incidente.

A comunicação ao CEPD deverá ser feita por meio do e-mail: cepd@prodemge.gov.br. Deverá ser enviado a cópia do formulário encaminhado à ANPD.

[9] https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis

5. Relatório final

Todas as informações sobre o incidente, incluindo as medidas e ações tomadas, comunicações realizadas, evidências e outros dados coletados sejam registrados em um relatório final sobre o incidente. Além do histórico e do registro sobre o incidente, o relatório deve apresentar as lições aprendidas e propostas de melhoria para prevenção e tratamento de incidentes de segurança. Em caso de novos desdobramentos relevantes, relativos ao incidente ocorrido, o relatório deverá ser atualizado, conforme necessário. Esse documento poderá subsidiar a elaboração de relatório de impacto a proteção de dados (RIPD).


MINAS
GERAIS
GOVERNO
DIFERENTE.
ESTADO
EFICIENTE.