GUIA

PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA

ORIENTAÇÕES E PROCEDIMENTOS

CGE
CONTROLADORIA GERAL
DO ESTADO DO PARANÁ

GOVERNO DO ESTADO DO PARANÁ

Governador do Estado do Paraná
Carlos Massa Ratinho Junior

Controladora-Geral do Estado do Paraná
Luciana Carla da Silva Azevedo

Elaboração
Assessora Técnica
Mineia Lückfett de Oliveira

Contato:
lgpd@cge.pr.gov.br | mineial@cge.pr.gov.br
(41) 3883-40 47

SUMÁRIO

1 APRESENTAÇÃO

Este guia visa auxiliar os profissionais designados ao tratamento de dados pessoais e demais servidores que atuam subordinados ao controlador, incentivando a utilização de boas práticas de segurança e proteção de dados nos assuntos relacionados a respostas de incidentes.

As informações contidas neste guia serão atualizadas de forma contínua, buscando incorporar melhorias, conforme a publicação de novas normas e edificação dos processos de proteção de dados existentes.

2 DEFINIÇÕES

No contexto deste guia e com base na Lei Geral de Proteção de Dados – LGPD, são adotadas as seguintes definições:

agentes de tratamento

são aqueles que podem ter alguma ação no tratamento de um incidente que coloque em risco a segurança dos dados pessoais, tais como:

▷ **Controlador:** pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais. Na administração pública estadual, o Controlador é o Estado e os órgãos e entidades exercem as funções típicas do controlador.

▷ **Operador:** pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. No âmbito do Poder Executivo Estadual, podemos mencionar como exemplo, a Companhia de Tecnologia da Informação e Comunicação do Paraná - CELEPAR.

encarregado

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

autoridade nacional de proteção de dados

é entidade responsável por zelar, implementar e fiscalizar o cumprimento da 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 (arts. 55-A e seguintes da LGPD).

dado pessoal

é toda informação relacionada a pessoa natural identificada ou identificável.

inventário de dados pessoais (IDP)

instrumento utilizado para documentar o tratamento de dados pessoais realizados pelo órgão ou entidade em alinhamento ao previsto pelo art. 37 da LGPD.

incidente de segurança com dados pessoais

de acordo com a Autoridade Nacional de Proteção de Dados (ANPD), incidente de segurança à proteção de dados pessoais é qualquer evento adverso, confirmado ou sob suspeita, relacionado à violação de dados pessoais, sendo **acesso não autorizado, acidental ou ilícito que resulte em destruição, perda, alteração vazamento ou qualquer forma de tratamento de dados ilícita ou inadequada, que tem a capacidade de pôr em risco os direitos e as liberdades dos titulares dos dados pessoais.**

relatório final

relatório que contenha todas as evidências e ações realizadas para tratamento do incidente e que deve ser emitido ao final das tratativas.

relatório de impacto a proteção de dados pessoais (RIPD)

conforme a LGPD, o RIPD é uma documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que tem o potencial de gerar riscos às liberdades civis e aos direitos fundamentais dos titulares, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

3 INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS

Conforme supramencionado no item VI do tópico 2 deste guia, um incidente de segurança com dados pessoais é qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte em destruição, perda, alteração, vazamento ou, ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais.

De acordo com o art. 46 da LGPD, 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, e que tais medidas de segurança deverão ser observadas desde a concepção do produto ou serviço até a sua execução.

Neste contexto, os agentes de tratamento de dados pessoais, poderão sofrer sanções administrativas ou civis caso não cumpram com suas obrigações legais previstas na LGPD. A gestão de incidentes de forma incorreta ou inadequada pode acarretar tais penalidades.

3.1 INCIDENTES QUE PODEM ACARRETAR RISCO OU DANO AOS TITULARES

Um incidente pode acarretar risco ou dano relevante aos titulares quando o incidente envolver dados sensíveis ou de indivíduos em situação de vulnerabilidade, incluindo crianças e adolescentes, ou tiver o potencial de ocasionar danos materiais ou morais, tais como discriminação, violação do direito à imagem e à reputação, fraudes financeiras e roubo de identidade.

É recomendável ainda analisar o volume de dados envolvido, o número de indivíduos afetados, a boa-fé e as intenções dos terceiros que tiveram acesso aos dados após o incidente e a facilidade de identificação dos titulares por terceiros não autorizados.

Quando houver dúvida sobre a relevância dos riscos e danos envolvidos, recomenda-se que seja feita a comunicação.
Cabe à ANPD a regulamentação das situações de risco ou dano relevante ao titular. Até o momento da publicação deste guia, a ANPD ainda não havia regulamentado o tema.

Na hipótese de incidente que coloque em risco a segurança de dados pessoais, devem ser realizados **alguns procedimentos específicos, quais são:**

Avaliar internamente o incidente com o objetivo de
(i) obter informações iniciais sobre impacto do evento;
(ii) natureza, categoria e quantidade de titulares de dados pessoais afetados;
(iii) categoria e quantidade de dados afetados, consequências do incidente para os titulares e a entidade, criticidade e probabilidade;
(iv) além disso, é necessário preservar todas as evidências do incidente.

Comunicar ao encarregado do órgão ou entidade.

Comunicar a autoridade máxima do órgão ou entidade.

Comunicar ao Núcleo de Informática e Informações - NII.

Comunicar à ANPD e ao titular de dados pessoais a existência do incidente de segurança que venha a gerar risco ou dano considerado relevante aos titulares (art. 48 da LGPD).

Emitir o relatório final com todas as informações coletadas, as ações realizadas para o tratamento efetivo do evento e as considerações necessárias para promover a melhoria no atendimento de incidentes.

3.2 AVALIAR INTERNAMENTE O INCIDENTE

Quando a entidade tem conhecimento do incidente de segurança, deve ser realizada uma avaliação interna para que sejam obtidas informações como:

- **Qual vulnerabilidade** foi explorada no evento, abrangendo situações como: acesso indevido aos dados pessoais; roubo de dados; ataques cibernéticos; erros de programação de aplicativos e sistemas internos; engenharia social; descartes indevidos; repasse de dados pessoais; roubo, venda e utilização de dados tutelados pela entidade; comprometimento de senhas de acesso; e outras.

- **Fonte dos dados pessoais:** meio pelo qual foram obtidos os dados pessoais, tais como preenchimento de formulário eletrônico ou não eletrônico por parte do titular, API, uso compartilhado de dados, XML e cookies.

- **Categoria de dados pessoais:** dados sensíveis, dados pessoais, de crianças e adolescentes.Extensão do vazamento: quantificar os titulares e os dados pessoais que tiveram a sua segurança violada neste evento.

- **Avaliação do impacto ao titular:** avaliar quais são os impactos que o incidente pode gerar aos titulares.

- **Avaliação do impacto no serviço:** avaliar os impactos que o incidente pode gerar a entidade como perda de confiabilidade do cidadão, ações judiciais, dano à imagem da instituição em âmbito nacional e internacional, prejuízo à entidade em contratos com fornecedores e clientes, e impacto total ou parcial nas atividades desenvolvidas pela entidade.

Devem ser preservados o máximo de evidências do incidente e de todas as medidas adotadas a partir da sua ciência, a fim de que se demonstre, para eventuais autoridades que posteriormente vierem a apurar os fatos, toda a cadeia de diligências realizadas para entendimento do evento e mitigação dos seus efeitos.

Nesse cenário, todos os passos devem ser devidamente documentados, desde o momento inicial de atuação até a contenção e os efeitos. Isso inclui, mas não se limita a:

▷ Todos os logs dos sistemas internos e externos envolvidos no incidente;

▷ Interações do time envolvido e todas as medidas adotadas;

▷ Eventuais contratações de ferramentas e equipes de especialistas e auditores para atuação pontual no incidente a ser tratado.

▷ Atas das reuniões relevantes.

À medida que o tratamento do incidente avançar, as informações de tal avaliação preliminar podem ser atualizadas.

3.2.1 RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS (RIPD)

O RIPD poderá ser solicitado nas seguintes hipóteses:

▷ Para tratamento de dados pessoais realizados para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (exceções previstas pelo inciso art. 4º, inciso III da LGPD);

▷ Quando houver infração da LGPD em decorrência do tratamento de dados pessoais por órgãos públicos (arts. 31 e 32 da LGPD, combinados); e

▷ A qualquer momento, sob determinação da ANPD (art. 38).

Em síntese, o RIPD é um documento que pode ser solicitado pela ANPD e servirá de subsídio para o processo de gestão de incidentes com dados pessoais.

3.3 COMUNICAR AO ENCARREGADO DE DADOS

A notificação ao Encarregado de Dados quanto a eventual incidente de segurança com dados pessoais deverá ser feita via e-mail institucional, o mais rápido possível, para as providências previstas na LGPD e no portal da ANPD sobre comunicação de incidentes de segurança.

Cabe ao Encarregado, diante das informações levantadas internamente e dos parâmetros estabelecidos pelo órgão, pela ANPD ou com base em boas práticas, avaliar a necessidade e a profundidade da comunicação com a ANPD e com os titulares de dados. Nessas tarefas, a LGPD e os demais normativos infralegais vigentes sobre proteção de dados pessoais deverão ser sempre consultados e utilizados como balizas.

3.4 COMUNICAR AO CONTROLADOR

O Encarregado de Dados Pessoais deve comunicar incidentes com dados pessoais ao Controlador o mais rápido possível, a fim de viabilizar que o Controlador possa comunicar a ANPD e ao titular de dados.

O controlador deverá ter cautela quanto ao julgamento acerca da relevância dos riscos e danos referentes ao incidente e, em caso de dúvida, a comunicação do incidente deverá ser realizada de forma breve.

3.5 COMUNICAR À ANPD E AO TITULAR DE DADOS PESSOAIS

O art. 48 da LGPD determina que é obrigação do controlador comunicar à Autoridade Nacional de Proteção de Dados (ANPD) e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

Excepcionalmente, podem ocorrer situações em que tal comunicação provenha do operador, caso em que será devidamente analisada pela autoridade de proteção de dados.

A ANPD estipula o prazo de 2 (dois) dias úteis para comunicação de incidente de segurança a proteção de dados.

Poderá ser acessado no site da ANPD ou por meio do link: https:/www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca, formulário modelo para notificação de incidentes de segurança com proteção de dados.

3.6 EMITIR O RELATÓRIO FINAL DO INCIDENTE

É importante que todas as informações e evidências coletadas e as ações do processo de tratamento de incidente de segurança à proteção de dados sejam documentadas, de modo a possibilitar a elaboração de um relatório final do incidente.

Este documento deve:

- conter as devidas considerações para a promoção da melhoria contínua dos processos de tratamento de incidentes; e

- estar disponível para consulta em caso de elaboração e atualização do relatório de impacto a proteção de dados (RIPD).

A ANPD pode solicitar o mencionado relatório para análise, com o propósito de:

▷ avaliar as ações tomadas durante um incidente em que dados pessoais tenham sido expostos ou comprometidos;

▷ publicar e atualizar normas referentes à proteção de dados;

▷ cumprir o princípio da responsabilização (art. 6º, inciso X da LGPD);

▷ utilizá-lo como subsídio para eventuais questionamentos, facilitando a comprovação de conformidade.

3.7 CANAIS DE COMUNICAÇÃO DE INCIDENTES COM DADOS PESSOAIS

Os canais abaixo de contato poderão ser explorados no processo de comunicação de incidentes:

ANPD
formulário de comunicação de incidentes disponível no link:
https:/www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca

Ecarregado de Dados
e-mail para: pedro.augusto@cge.pr.gov.br

Controlador de Dados
e-mail para: gabinetecge@gabinete.cge.gov.br; a comunicação deverá ser feita pelo encarregado de dados pessoais do órgão ou entidade;

FONTE:
Guia de Resposta a Incidentes de Segurança – Lei Geral de Proteção de Dados (LGPD) – Versão 1.0 – Brasília, setembro de 2021 – Acesso em: 14.03.2022

CGE

CONTROLADORIA GERAL
DO ESTADO DO PARANÁ