PROCURADORIA GERAL DO ESTADO
RONDÔNIA

PGE·RO

GUIA DE RESPOSTAS A INCIDENTES DE SEGURANÇA.

EQUIPE TÉCNICA

PROCURADOR GERAL DO ESTADO
Maxwel Mota de Andrade

SECRETÁRIO GERAL
Fábio de Sousa Santos

ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS
Rod Daniel Gomes

DIAGRAMAÇÃO
Coordenação de Relações Públicas

SUMÁRIO

1. DEFINIÇÕES GERAIS

Para auxílio na leitura deste guia, serão adotadas as seguintes definições no que se refere a incidentes ocorridos no âmbito da Procuradoria-Geral do Estado de Rondônia.

AGENTE DE TRATAMENTO	De acordo com a LGPD, são agentes de tratamento aqueles que podem ter alguma ação no tratamento de um incidente que coloque em risco a segurança dos dados pessoais. Tais agentes abrangem
CONTROLADOR	Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; na administração pública federal, os órgãos 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.
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:	Os arts. 55-A e seguintes da LGPD definem a Autoridade Nacional de Proteção de Dados (ANPD), 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.
DADO PESSOAL	É toda informação relacionada a pessoa natural identificada ou identificável.
INCIDENTE	Evento, ação ou omissão que tenha permitido ou possa vir a permitir acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou, ainda, apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação.
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.
RIPD	Conforme a LGPD, o Relatório de Impacto a Proteção de Dados (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

2. INCIDENTES DE SEGURANÇA COM DADOS PESSOAIS

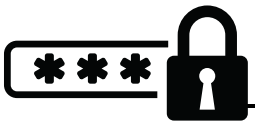
Um incidente de segurança com dados pessoais é qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte em destruição, perda, alteração, vazamento ou, ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais.

Evitar esses eventos, passa pela necessidade de 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, de acordo com as regras de boas práticas de governança para o tratamento de dados pessoais.

Em caso de suspeita de incidente que coloque em risco a segurança de dados pessoais, devem ser realizados alguns procedimentos específicos. A figura abaixo detalha de maneira simplificada este processo:

2.1. COMUNICAR AO ENCARREGADO DA ENTIDADE

A notificação de eventual vazamento de dados pessoais pelos colaboradores internos (Procuradores, servidores, estagiários, residentes e terceirizados) deverá em regra ser realizada via SEI à setorial PGE-EPD ou pelo e-mail epd@pge.ro.gov.br, o mais rápido possível, para as providências previstas na LGPD e no portal da ANPD sobre comunicação de incidentes de segurança.



2.2. AVALIAÇÃO DO INCIDENTE

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

a. **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.

b**. 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.

c. **Categoria de dados pessoais:** por exemplo, se se tratam de dados sensíveis, dados pessoais de crianças e adolescentes.

d. **Extensão do vazamento:** quantificar os titulares e os dados pessoais que tiveram a sua segurança violada neste evento.

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

f. **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:

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

b. Interações do time envolvido e todas as medidas adotadas;

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

d. Atas das reuniões relevantes.

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

2.2.1. RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

Diante de todas as evidências, é importante que a entidade avalie a necessidade de elaborar o Relatório de Impacto à Proteção de Dados Pessoais (RIPD), pois o RIPD poderá ou deverá ser solicitado em casos específicos previstos na LGPD. São eles:

- 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. 4°, 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).

O órgão deverá implementar o processo de elaboração e manutenção do Inventário de Dados Pessoais (IDP). Esse documento mostra detalhes da utilização dos dados pessoais por diversos programas, sistemas de informação ou processos existentes. Além dos casos específicos previstos pela LGPD relativos à elaboração do RIPD, é indicada a elaboração ou atualização do Relatório de Impacto sempre que existir a possibilidade de ocorrer impacto na privacidade dos dados pessoais.

2.3. COMUNICAR À ANPD E AO TITULAR DE DADOS PESSOAIS

O Encarregado tendo ciência do incidente, avaliará 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.

A autoridade nacional de proteção de dados disponibiliza, em seu sítio eletrônico, um formulário modelo para notificação de incidentes de segurança com proteção de dados. O formulário pode ser acessado no site da ANPD ou através do seguinte link:

https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca

Conforme a LGPD, cabe ao controlador (PGE) comunicar ao titular dos dados pessoais a ocorrência de incidente de segurança que tenha potencial de lhe gerar riscos ou danos relevantes.

O que e como comunicar aos titulares de dados?

A comunicação do incidente aos titulares deve ser feita em linguagem clara e simplificada e mencionar, no que couber, os elementos previstos no §1° do Art. 48 da LGPD, tais como:

- A descrição geral do incidente e a data da ocorrência;
- A natureza dos dados pessoais afetados e os riscos relacionados ao incidente;
- As medidas tomadas e recomendadas para mitigar os efeitos do incidente;
- O contato do encarregado ou o ponto de contato para que os titulares obtenham informações a respeito do incidente;
- Outras informações que possam auxiliar os titulares a prevenir possíveis danos.

A comunicação deve ser feita de forma individual e diretamente aos titulares, sempre que possível. Se, pela natureza do incidente, não for possível identificar individualmente os titulares afetados, devem ser comunicados todos os presentes na base de dados comprometida.

2.4. 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:

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

b. estar disponível para consulta em caso de 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.

2.5. CANAIS DE COMUNICAÇÃO DE INCIDENTES COM DADOS PESSOAIS

Os canais abaixo de contato poderão ser explorados no processo de comunicação de incidentes. Recorde-se, entretanto, que cada um dos órgãos listados a seguir possui atribuições legais e regimentais distintas, e que a ANPD é o ponto focal para LGPD e a autoridade administrativa fiscalizatória para recebimento de incidentes envolvendo dados pessoais:

- **Encarregado de Proteção de Dados:** O titular poderá entrar em contato por meio do e-mail **epd@pge.ro.gov.br** ou enviar diretamente pelo SEI pela unidade PGE-EPD para sanar quaisquer dúvidas sobre o tratamento dos dados realizados com fundamento na LGPD.

- **ANPD - Agência Nacional de Proteção de Dados:** Autoridade Nacional de Proteção de Dados) é o órgão federal responsável por fiscalizar e aplicar a LGPD, a Lei Geral da Proteção de Dados. A criação de uma autoridade independente é necessária para que empresas que têm acesso à informações pessoais cumpram a legislação e possam ser auditadas nos casos em que não observarem o devido tratamento destes dados.

- **Polícia Federal:** apenas quando houver indícios de crime, de acordo com a Lei nº 12.737, de 30 de novembro de 2012, ou outras normas presentes na legislação penal extravagante, a Polícia Federal deverá ser comunicada através de ofício diretamente enviado ao Diretor.

Embora a responsabilidade e a obrigação pela comunicação do incidente sejam do controlador, podem ocorrer casos excepcionais em que tal comunicação provenha do operador, caso em que tal comunicação será devidamente analisada pela autoridade de proteção de dados.

REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 31000:2018: Gestão de Riscos — Diretrizes. Rio de Janeiro, 2018.

BRASIL. Autoridade Nacional de Proteção de dados. Comunicação de incidentes de segurança. Disponível em: < https://www.gov.br/anpd/pt-br/assuntos/incidente-de- seguranca >. Acesso em: 03 de outubro de 2022.

BRASIL. Presidência da República. Decreto n° 10.748, de 16 de julho de 2021. Rede Federal de Gestão de Incidentes Cibernéticos. Disponível em: <https://www.in.gov.br/en/web/dou/-/decreto-n-10.748-de-16-de-julho-de-2021-332610022> Acesso em: 03 de outubro de 2022.

BRASIL. Presidência da República. Lei n° 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais. Disponível em:< http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 03 de outubro de 2022.

COMITÊ CENTRAL DE GOVERNANÇA DE DADOS – CCGD. Guia de Avaliação de Riscos de Segurança e Privacidade. Disponível em: <https://www.gov.br/governodigital/pt- br/seguranca-e-protecao-de-dados/guias/guia_avaliacao_riscos.pdf >. Acesso em: 04 de outubro de 2022.

COMITÊ CENTRAL DE GOVERNANÇA DE DADOS - CCGD. Guia de Boas Práticas LGPD. Disponível em: < https://www.gov.br/governodigital/pt-br/governanca-de- dados/guia-de-boas-praticas-lei-geral-de-protecao-de-dados-lgpd >. Acesso em: 20 de abril de 2021.

COMITÊ CENTRAL DE GOVERNANÇA DE DADOS - CCGD. Guia de Inventário de Dados Pessoais. Disponível em: < https://www.gov.br/governodigital/pt-br/seguranca-e-protecao- de-dados/guias/guia_inventario_dados_pessoais.pdf >. Acesso em: 04 de outubro de 2022.

COMITÊ CENTRAL DE GOVERNANÇA DE DADOS - CCGD. Guias Operacionais para adequação à LGPD. Disponível em: < https://www.gov.br/governodigital/pt-br/governanca- de-dados/guias-operacionais-para-adequacao-a-lgpd >. Acesso em: 04 de outubro de 2022.

PROCURADORIA GERAL DO ESTADO
RONDÔNIA

PGE·RO