PGE
Mato Grosso do Sul

Procuradoria-Geral
do Estado

PLANO

de Resposta a Incidentes de Segurança com Dados Pessoais

UPD - PGE/MS - Unidade de Proteção de Dados Pessoais 1ª Edição | 2025

PGE
Mato Grosso do Sul
Procuradoria-Geral do Estado

Administração Superior

Ana Carolina Ali Garcia
Procuradora-Geral do Estado

Márcio André Batista de Arruda
Procurador-Geral Adjunto do Estado do Contencioso

Ivanildo Silva da Costa
Procurador-Geral Adjunto do Estado do Consultivo

Elaboração – conteúdo

Cristiane Müller Dantas
Procuradora do Estado e Encarregada pelo Tratamento de Dados Pessoais

Revisão

Elcia Tatiane Pazeto Puks Campos

Diagramação

Elcia Tatiane Pazeto Puks Campos

Capa

Guido Brey Jr.

2025

PGE
Mato Grosso do Sul
Procuradoria-Geral do Estado

Procuradoria-Geral do Estado de Mato Grosso do Sul (PGE/MS)

Unidade de Proteção de Dados Pessoais (UPD)

Plano de Resposta a Incidentes de Segurança com Dados Pessoais. Procuradoria-Geral do Estado de Mato Grosso do Sul. Campo Grande-MS: PGE/MS, 2025.

1. Procuradoria-Geral do Estado. 2. Mato Grosso do Sul. 3. LGPD. 4. Plano de Resposta. 5. Incidentes de Segurança com Dados Pessoais.

Siglas

ANPD	Autoridade Nacional de Proteção de Dados
Ascom	Assessoria de Comunicação
ASTEC	Assessoria Técnica da COPGE
CETI	Comitê Estratégico de Tecnologia da Informação
CGF	Coordenação-Geral de Fiscalização
CIGE	Coordenadoria de Inteligência e Gestão Estratégica
CIRT	*Cyber Incident Response Team* (Equipe de Resposta a Incidentes Cibernéticos)
COPGE	Coordenadoria da Procuradoria-Geral do Estado
CGPGE	Corregedoria-Geral da Procuradoria-Geral do Estado
CPDP	Comitê de Proteção de Dados Pessoais
DOE	Diário Oficial Eletrônico do Estado
DoS	*Denial of Service* (Negação de Serviço)
DSG	Diretoria de Serviços Gerais
DSISTI	Diretoria de Suporte, Infraestrutura e Segurança em Tecnologia da Informação
LGPD	Lei Geral de Proteção de Dados Pessoais
PGE/MS	Procuradoria-Geral do Estado de Mato Grosso do Sul
SMS	*Short Message Service* (Serviço de Mensagens Curtas)
UPD	Unidade de Proteção de Dados Pessoais

Sumário

Apresentação

Desde 2018 o Brasil possui a Lei nº 13.709, de 14 de agosto de 2018, que regula a proteção aos dados pessoais das pessoas físicas, a chamada Lei Geral de Proteção de Dados Pessoais, a LGPD.

A norma prescreve a obrigatoriedade de os agentes de tratamento garantirem a segurança dos dados pessoais tratados, mesmo encerrado o procedimento. Também, determina a adoção de diligências para a proteção dos dados pessoais contra acessos não autorizados, situações acidentais e/ou tratamento inapropriado (arts. 17 e 46 da Lei nº 13.709/2018).

Proteger dados pessoais contempla o rol de direitos e garantias fundamentais, incluído pela Emenda Constitucional nº 115, de 10 de fevereiro de 2022. Por isso, a Autoridade Nacional de Proteção de Dados (ANPD) preocupa-se em zelar pela proteção dos dados pessoais contra ameaças e define ações para mitigar os riscos, assegurando a responsabilização em relação à segurança da informação por meio dos procedimentos específicos previstos na Resolução CD/ANPD n° 15, de 24 de abril de 2024.

Para a ANPD, Incidente de Segurança caracteriza qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais, como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou, ainda, qualquer forma de tratamento inadequada ou ilícita que possa ocasionar risco aos direitos e às liberdades do titular dos dados pessoais.

Mobilizar medidas de segurança para os possíveis eventos de risco não se resume a mero emprego de soluções tecnológicas e padrões de segurança, e sim exige elaboração, manutenção e revisão de documentos para melhoria dos processos internos, como ações de fortalecimento da governança de dados e da proteção do ente público, dos seus servidores e colaboradores, dos titulares dos dados e da sociedade em geral.

Nesse contexto regulamentar e procedimental de potencialidades cada vez mais digitais das práticas sociais contemporâneas é indispensável elaborar e publicizar um Plano de Resposta a Incidentes de Segurança de Dados Pessoais “na” e “para” a Procuradoria-Geral do Estado de Mato Grosso do Sul (PGE/MS).

O expressivo volume de dados tratados pela Procuradoria é real e pode gerar riscos significativos para os titulares. Sua atuação abrangente, como assessoramento jurídico, consultoria jurídica de todos os órgãos estaduais e representação judicial do Estado de Mato Grosso do Sul em todos os processos judiciais que seja parte, dívida ativa e solução consensual de conflitos, possibilita insegurança e gera ocorrência de incidentes com dados.

Por isso, a necessidade de uma ferramenta comunicacional formal, clara, intuitiva e eficaz de respostas de como agir nos casos de ataques cibernéticos e vazamentos de dados físico ou digital.

Logo, um Plano bem estruturado é crucial para mitigar riscos e garantir que a Instituição responda de forma eficaz e eficiente quaisquer incidentes de segurança com dados pessoais.

Afinal, proteger dados pessoais é uma responsabilidade social compartilhada e colaborativa.

Cristiane Müller Dantas
Procuradora do Estado
Encarregada pelo Tratamento de Dados Pessoais da PGE/MS

Vamos ao Plano!

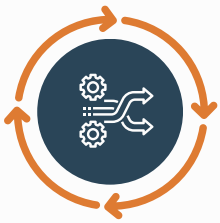
Conhecendo o Plano

Como está estruturado o Plano?

Por eixos temáticos

Definição e identificação

Comunicação e resposta



Ações imediatas

Mitigação e aprendizado

O Plano recepcionou as diretrizes de Linguagem Simples para facilitar a compreensão dos Procuradores do Estado, servidores e colaboradores em exercício na Instituição. O uso de recursos como estrutura de frases diretas, diminuição de termos técnicos, o uso de tópicos, perguntas e respostas e design proporcionam clareza, agilidade e acessibilidade para todos que, em momentos de urgências, necessitam localizar a informaçãao facilmente.

O que é um Plano de Resposta a Incidentes de Segurança?

É um manual de instruções para o caso de algo dar errado com os dados pessoais sob a guarda da Instituição. Ele ajudará e possibilitará o agir rápido e correto frente a situações-problema, como um vazamento de informações, por exemplo.
O Plano de Resposta a incidentes de segurança com dados pessoais delineia o processo de proteção a dados pessoais na Procuradoria-Geral do Estado de Mato Grosso do Sul.

Por que é importante ter um Plano assim?

Para estar preparado e munido de informações e instruções para proteger dados das pessoas e evitar problemas legais.
Nele estarão descritas as funções e as responsabilidades individuais e coletivas, bem como as medidas a serem implementadas para a proteção dos dados pessoais tratados pela PGE/MS.
A LGPD é bem clara: quem trabalha com dados pessoais precisa estar preparado para lidar com situações de risco.

Como serão observadas as informações, os arquivos e os dados sob a responsabilidade da PGE/MS descritas no Plano?

Em conjunto com:

- a Política de Segurança da Informação do Estado de Mato Grosso do Sul (Deliberação CETI n° 02, de 24/02/2022, no DOE n° 10.767, de 25 de fevereiro de 2022);
- o “Regulamento de Comunicação de Incidente de Segurança”, publicado pela ANPD, por meio da Resolução CD/ANPD n° 15, de 24/04/2024, no Diário Oficial da União, de 26 de abril de 2024.

E se dúvidas surgirem acerca das informações técnicas e regulamentares, mesmo com os recursos de Linguagem Simples aplicados ao Plano?

Foi elaborado um Glossário para auxiliar a compreensão e a abrangência conceitual de termos técnicos e explicações como:

- O que é um incidente de segurança?
- Quem faz parte do time de resposta?
- Como identificar um incidente de segurança?
- O que fazer quando identificar um incidente de segurança?
- Como avaliar o incidente de segurança?
- Como comunicar o incidente de segurança?

Definição e identificação

Histórico da LGPD

2010
Início das consultas e anteprojeto de Lei de Proteção de Dados

2011
Sancionada a Lei de Acesso à Informação - LAI

2012
Sancionada a Lei Carolina Dieckmann - tipificação de crimes cibernéticos, como compartilhar dados pessoais sem autorização

2014
Marco Civil da Internet - primeira lei responsável por regular o uso da internet no País

2018
Promulgação da Lei 13.709, que estabelece a LGPD

2020
Entra em vigor a Lei Geral de Proteção de Dados no Brasil (LGPD)

2022
Aprovação do Regulamento de aplicação da LGPD para agentes de pequeno porte

2022
Promulgação da Emenda Constitucional 115/22, que inclui o direito à proteção de dados na Constituição Federal

2022
A ANPD se torna uma autarquia de natureza especial

Objetivos

Orientar Procuradores do Estado, servidores, colaboradores de todas as áreas de atuação da Procuradoria-Geral do Estado, contratados e parceiros, a lidarem com situações excepcionais relativas a incidentes de segurança com dados pessoais.

Estabelecer um procedimento formal, célere e efetivo.

Preservar evidências que possam contribuir na governança institucional.

Melhorar processos internos para prevenção de outros incidentes.

Cumprir normativos legais e de transparência.

Formatar o processo de apuração de incidente de segurança com dados pessoais.

Priorizar a proteção de dados pessoais, dados sigilosos e sistemas operacionais da Instituição.

Minimizar eventuais impactos à reputação da Instituição, estabelecendo procedimentos e mecanismos de comunicação simples e efetiva com os titulares dos dados pessoais.

Ampliar a governança, valendo-se de lições aprendidas com incidentes anteriores.

O que é um incidente de segurança?

Definição: qualquer situação que coloque em risco a segurança dos dados pessoais.

Ex.: vazamento, acesso não autorizado ou perda de informações, etc.

Entenda: segundo a ANPD, cabe ao(à) Controlador(a) dos dados identificar, tratar e avaliar o risco dos incidentes de segurança que afetem suas operações de tratamento de dados pessoais.

Fique atento!

Há uma grande gama de incidentes de segurança que varia de acordo com a natureza e a complexidade das atividades desempenhadas na Instituição. E, nesse rumo, abrange uma considerável quantidade de eventos e situações que comprometem a segurança das informações ou dos recursos dela.

Por isso, é fundamental que o corpo técnico da Instituição esteja apto a identificar e a informar potenciais incidentes, e as equipes de resposta e técnicas específicas a conterem, documentarem e gerirem o incidente, os danos e a implementação de soluções mitigadoras e protetivas.

Exemplos de incidente de segurança

Acesso físico ou lógico prejudicado ou impossibilitado

Refere-se à situação em que a capacidade de acessar um sistema, rede ou informação é comprometida ou totalmente bloqueada.

Acesso não autorizado

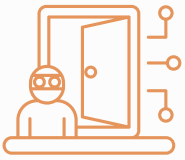
Ocorre quando uma pessoa ou um programa ganha acesso a sistemas, redes ou dados sem ter a permissão para isso. É como se alguém entrasse na sua casa sem bater à porta e começasse a mexer em suas coisas.

Ataques cibernéticos

Ações em ambiente digital como *malware, ransomware, phishing* e Engenharia Social.

Erros humanos

Ações não intencionais que resultam em violações de segurança, como envio de documentos com dados pessoais gerais ou sensíveis para destinatários errados, publicação não proposital de dados pessoais de titulares.



Exploração de vulnerabilidades

Processo pelo qual um indivíduo ou grupo de *hackers* busca identificar e aproveitar falhas de segurança em sistemas, redes ou aplicativos (prática comum no mundo da segurança da informação).

Intrusões de rede

São atividades não autorizadas que visam acessar, modificar ou danificar sistemas e dados em uma rede de computadores. Podem ser realizadas por *hackers, malware* ou por *insiders* mal-intencionados.

Negação de serviço

Também chamado *DoS* (*Denial of Service*), é um ataque cibernético que visa impedir o acesso de usuários legítimos a uma determinada rede ou servidor. Para isso, o atacante sobrecarrega o alvo com tráfego malicioso, tornando os recursos indisponíveis.

Uso inapropriado

É a utilização de sistemas e redes em desacordo com as regras e os processos internos estabelecidos.

Alguns exemplos de uso inapropriado são: usar o e-mail corporativo para *spam* ou promoção de negócios pessoais; instalar *softwares* não autorizados; usar um *pen drive* de forma não autorizada; e imprimir documentos sem autorização.

Vazamento de dados pessoais

Divulgação não autorizada de dados pessoais ou dados pessoais sensíveis por meios físicos ou digitais.

Violação de dados

Acesso não autorizado a informações confidenciais que contenham dados pessoais ou dados pessoais sensíveis.

Consulte o Guia de prevenção a incidentes de segurança para mais informações.

Como isso ocorre?

Um *hacker* invade a rede de computadores do Estado ou da PGE/MS e realiza cópia não autorizada de uma base de dados contendo dados pessoais e os expõem a risco de fraudes, danos morais e materiais.

Um servidor perde um *pen drive* contendo arquivos com dados pessoais.

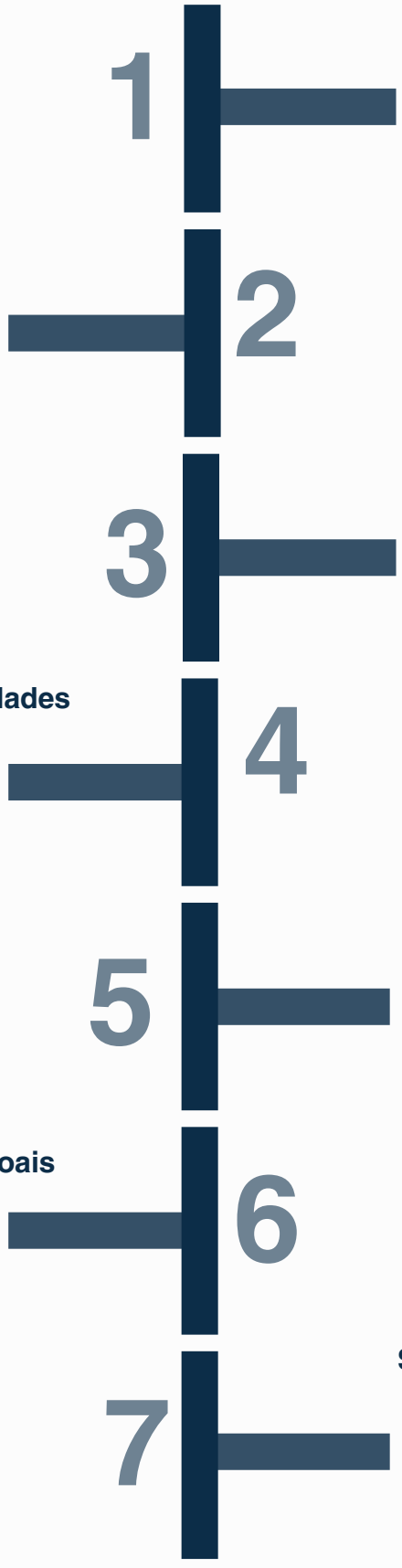
Um e-mail com informações confidenciais é enviado para a pessoa errada.

Um servidor acessa informações contendo dados pessoais (gerais ou sensíveis) indevidamente.

Perda ou roubo de documentos ou dispositivos de armazenamento de dados, que contenham dados pessoais protegidos por sigilo profissional, cópias de documentos de identificação oficial e dados de contato dos titulares podem expô-los a riscos reputacionais e a fraudes financeiras.

Um Operador sofre a invasão de sua rede e o furto de dados relativos a atividades da Procuradoria-Geral do Estado, etc.

Incidentes de segurança e consequências



Acesso não autorizado

Acesso não autorizado refere-se ao ingresso de indivíduos ou programas em sistemas ou dados sem permissão. Este tipo de incidente é comparado a uma invasão doméstica, destacando a grave violação de privacidade e segurança.

Ataques cibernéticos

Englobam várias formas de violação digital, como *malware, ransomware e phishing*. Esses ataques podem comprometer gravemente a segurança das informações, levando à perda de dados e a impactos financeiros significativos.

Erros humanos

Erros não intencionais, como o envio de dados pessoais a destinatários errados, representam uma fraqueza significativa na segurança. A falta de atenção ou de treinamento adequado pode resultar em exposições de dados pessoais gerais e sensíveis.

Exploração de vulnerabilidades

Hackers frequentemente buscam explorar falhas de segurança em sistemas, redes e aplicativos. Esse processo pode resultar em invasões, roubo de dados ou desconfiguração de sistemas essenciais.

Negação de serviço (*DoS*)

Os ataques de negação de serviço visam impedir o acesso a serviços e dados legítimos ao sobrecarregar um sistema com tráfego malicioso. Isso pode ter um impacto severo na operação da instituição.

Vazamento de dados pessoais

Referem-se à divulgação não autorizada de dados pessoais gerais e/ou sensíveis, o que pode resultar em graves repercussões legais e perda de confiança dos administrados.

Soluções para mitigação

Implementar ferramentas de proteção é crucial para gerenciar acessos de forma segura e eficiente, ajudando prevenir ou minimizar os efeitos de incidentes de segurança.

Procedimentos da PGE/MS para incidentes de segurança

Informação do Incidente

Qualquer membro da PGE/MS que tomar conhecimento de um incidente de segurança deve informar imediatamente ao chefe da unidade para iniciar o processo de resposta.

Verificação e Resposta ao Incidente

A Unidade de Proteção de Dados Pessoais (UPD) coordena a verificação do incidente, categorizando-o como físico ou digital, e aciona as unidades correspondentes para uma resposta em até 24 horas.

Relatório Circunstanciado e Deliberação do Comitê

Dentro de 48 horas, a equipe deve elaborar um relatório sobre o incidente, sugerindo medidas mitigadoras. O Comitê de Proteção de Dados avalia a situação, define comunicações necessárias, propõe melhorias nos processos internos e remete o processo ao(à) Controlador(a) para decisão e encaminhamentos.

Comunicação e resposta

Quem faz parte do time de resposta?

Equipe de resposta

Deve ser formada por profissionais multidisciplinares e, sobretudo, por servidores especializados em segurança da informação, com atuação predominantemente vinculada à Diretoria de Suporte, Infraestrutura e Segurança em Tecnologia da Informação (DSIST/COPGE) da PGE/MS. Os servidores são responsáveis por gerenciar todos os aspectos técnicos relacionados aos incidentes, assegurando a identificação precisa, a contenção eficaz, a erradicação completa dos problemas e a implementação de medidas preventivas para evitar futuros eventos de segurança.

Entenda: imagine que a PGE/MS seja um grande prédio e os dados dela e os dos processos que atua sejam documentos e informações importantes guardados lá dentro.

A Equipe de Resposta é o grupo responsável por proteger os dados de "*hackers*" e de outros perigos digitais.

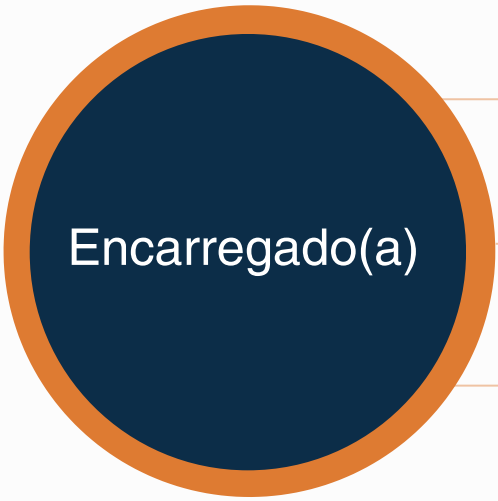
Fique atento!

Deve ser designada equipe responsável para lidar com o incidente de segurança, físico ou lógico, composta por:

1 (um) Encarregado(a) pelo Tratamento de Dados Pessoais da PGE/MS (titular ou suplente);
2 (dois) servidores da Diretoria de Suporte, Infraestrutura e Segurança em Tecnologia da Informação (DSISTI/COPGE);
1 (um) servidor da Diretoria de Serviços Gerais (DSG/COPGE);
1 (um) servidor da Assessoria de Manifestação de Ouvidoria e Acesso à Informação da Corregedoria-Geral (ASOUV/CGPGE);
1 (um) assessor jurídico da Coordenadoria de Inteligência e Gestão Estratégica (CIGE);
1 (um) servidor da Assessoria de Comunicação (Ascom).

Em caso de empate nas deliberações, incumbe ao(à) Encarregado(a) o desempate.

Atribuições do Encarregado(a)



Ser o elo entre a equipe técnica e as chefias: imagine um incêndio e que a equipe técnica seja os bombeiros apagando o fogo (o problema com os dados) e os gestores sejam os chefes dos bombeiros. O (A) Encarregado(a) seria a pessoa que fica no meio, garantindo que os bombeiros tenham os recursos necessários para apagar o fogo e que os chefes estejam informados a cada momento. Além disso, ele(a) precisa garantir que tudo seja feito conforme as regras da LGPD (a lei que protege os dados pessoais).

Avisar a ANPD e a imprensa: quando acontece um problema muito sério com os dados, ele(a) precisa, segundo o comando do(a) Controlador(a), avisar a ANPD e mantê-la informada acerca dos procedimentos mobilizados para resolver o problema. Além disso, precisa trabalhar com a equipe de comunicação para informar as pessoas que tiveram seus dados afetados, de uma forma clara e fácil de entender.

Informar as pessoas afetadas: se os dados de alguém forem roubados ou vazados, a pessoa afetada deve ser informada o mais rápido possível. É importante uma comunicação clara para o entendimento do ocorrido, sobretudo para compreender as ações mobilizadas para resolver o problema.

Principais atribuições da Equipe de Resposta

Detetives digitais

Quando acontece algum problema com os dados, eles investigam “como e por que” isso aconteceu, visando identificar a origem e o alcance do problema.

Bombeiros digitais

Se algum dado estiver em perigo, eles agem rápido para proteger as informações importantes, como se estivessem apagando um incêndio para conter o incidente e mitigar seus efeitos, como isolar sistemas comprometidos, restringir acessos e interromper atividades prejudiciais.

Consertadores

Depois de resolver o problema, eles consertam tudo para os dados ficarem seguros novamente, removem as vulnerabilidades ou as ameaças causadas pelo incidente e restauram os sistemas afetados, para garantir o retorno da operação de maneira segura e normal.

Preventores

Procuram por possíveis problemas antes que aconteçam; mobilizam medidas para evitar novos ataques aos dados; e registram os detalhes das ações realizadas, dos erros identificados e das soluções aplicadas durante o processo de resposta para preservação da informação sobre a ocorrência.

Responsabilidade do Comitê de Proteção de Dados Pessoais

O Comitê de Proteção de Dados Pessoais (CPDP) da PGE/MS é responsável por definir estratégias e formular diretrizes para a gestão e a proteção de dados pessoais na Instituição.

Propõe a devida regulamentação, quando necessário; conduz o Plano de Adequação da PGE/MS à LGPD; avalia os mecanismos de tratamento e proteção dos dados pessoais existentes para conformidade da Procuradoria-Geral do Estado com as disposições da Lei Federal n° 13.709, de 2018; e promove o intercâmbio de informações entre a proteção de dados pessoais e outros órgãos.

Por isso, exerce importante papel no caso de incidente de segurança com dados pessoais. Fornece apoio às ações da Equipe de Resposta e do(a) Encarregado(a), apreciando o relatório para o Plano ser seguido adequadamente e que as ações estejam alinhadas à LGPD.

Responsabilidade da Assessoria de Comunicação na composição da equipe

O membro da Equipe de Resposta oriundo da Assessoria de Comunicação é responsável por coordenar, em conjunto com o(a) Encarregado(a) de Dados, a comunicação com o público e as outras partes interessadas, durante e após a ocorrência de um incidente, com o objetivo de conferir clareza, transparência e alinhamento das informações divulgadas.

Atua para proteger a reputação da PGE/MS e gerenciar eventuais crises de imagem decorrentes do incidente.

Responsabilidade da Administração Superior e das chefias de Especializadas, Coordenadorias Jurídicas e órgãos de apoio

Recebem, analisam e respondem as notificações da Equipe de Resposta relacionadas a incidentes de segurança envolvendo dados pessoais com prioridade máxima para minimizar impactos negativos e preservar a continuidade das atividades. Também, permitem ações de reparação demandadas pela Equipe de Resposta relacionadas à contenção, à mitigação e à recuperação dos sistemas e dos processos internos atingidos.

Reponsabilidade do(a) Controlador(a)

A ele(a) compete as decisões relacionadas ao tratamento de dados pessoais. E, em matéria de incidente de segurança envolvendo dados pessoais, é responsável por:

(i) notificar a ANPD e os titulares dos dados sobre incidentes com possíveis riscos ou danos relevantes (deve indicar a natureza dos dados afetados, os titulares envolvidos, as medidas técnicas e de segurança adotadas e possíveis impactos);
(ii) acompanhar toda a apuração do incidente e das medidas previstas no Plano;
(iii) decidir sobre ações e procedimentos sugeridos pela Equipe de Resposta e pelo Comitê de Proteção de Dados Pessoais da PGE/MS, no tocante a ajustes em processos internos e sistemas para mitigar os riscos de novos incidentes.

Composição e funções de uma Equipe de Resposta a incidentes

Diversidade de especializações na equipe

Uma equipe de *CIRT* deve incluir diversas especializações, como gerentes, analistas de segurança, profissionais técnicos e especialistas em privacidade, cada um contribuindo com sua experiência para lidar com incidentes de segurança de forma eficaz.

Papel do Gerente de resposta a incidentes

O gerente de resposta a incidentes é responsável pela supervisão de todas as etapas do processo de resposta, mantendo a comunicação clara com as partes interessadas internas e assegurando que as estratégias sejam implementadas corretamente.

Importância dos Profissionais jurídicos

Os advogados desempenham um papel fundamental, ajudando a equipe a entender as implicações legais do incidente e a formular respostas adequadas, minimizando riscos legais e estabelecendo uma abordagem de defesa.

Coordenação para resposta eficaz

A integração de vários profissionais, como representantes da áreas finalística e técnica, assegura uma resposta coordenada que não só aborda a questão de segurança, mas também garante a continuidade das atividades após o incidente.

Como identificar um incidente de segurança com dados pessoais?

Sinais

A detecção precoce de incidentes de segurança é um fator importante para minimizar os danos causados. E, para isso, sistemas de monitoramento e análise de eventos são fundamentais para identificar atividades suspeitas. Por isso, a necessidade de investimento em soluções de segurança robustas, como *firewalls* e sistemas de detecção de intrusões.

Atividades suspeitas

Atividades suspeitas caracterizam acessos não autorizados, tráfego incomum, comportamentos suspeitos, mensagens de erro, atividades duvidosas no sistema ou nos relatos de usuários, etc.

Apurar tipos de incidentes

Apurar os tipos de incidentes é fundamental para avaliar se houve potencial violação de segurança a dados pessoais.

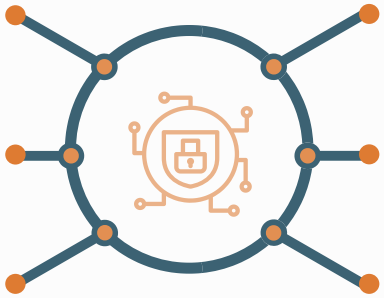
Quais incidentes de segurança precisam ser comunicados aos titulares e à ANPD?

Aqueles que...

Envolvem dados pessoais sensíveis.

Abrangem dados de crianças, de adolescentes ou de idosos.

Atingem dados financeiros.



Comprometem dados de autenticação em sistemas.

Compreendem dados protegidos por sigilo legal, judicial ou profissional.

Incluem dados em larga escala.[1]

Entenda: o incidente deve ser obrigatoriamente comunicado se, além do dano/risco significativo, houver atendimento cumulativo de, pelo menos, um dos parâmetros acima descritos.

O incidente que envolver apenas **dados anonimizados** ou que **não** sejam **alusivos a pessoas naturais identificáveis não precisam ser comunicados** à ANPD.

Fique atento!

O art. 48 da LGPD estabelece que os Controladores têm obrigação de comunicar os incidentes de segurança à ANPD **toda vez que a ocorrência envolva dados pessoais sujeitos à LGPD e possa acarretar risco ou dano relevante aos titulares[2] dos dados pessoais, afetando interesses e direitos fundamentais**[3].

Somente os Controladores sujeitos à LGPD têm obrigação de comunicar os incidentes à ANPD. E, no caso da Procuradoria-Geral do Estado, há sujeição às regras de proteção de dados.

1 São os que envolverem número significativo de titulares, volume de dados envolvidos, duração, frequência e extensão geográfica de localização dos titulares.

2 São considerados incidentes capazes de causar risco ou dano relevante aqueles que possam causar aos titulares danos materiais ou morais, expô-los a situações de discriminação ou de roubo de identidade, especialmente se envolverem dados em larga escala, sensíveis e de grupos vulneráveis como crianças e adolescentes ou idosos. Disponível em: https://lgpd.sfiec.org.br/noticia/152988/comunicacao-de-incidente-de-seguranca. Acesso em: 21 fev. 2025.

3 São situações em que a atividade de tratamento impedir o exercício de direitos ou a utilização de um serviço, bem como causar danos materiais ou morais aos titulares, incluídas a discriminação, violação à integridade física e/ou ao direito à imagem, fraudes financeiras ou roubo de identidade (art. 5º, § 2º, da Resolução ANPD nº 15, de 24 de abril de 2024).

Ações imediatas

Canal para denúncia

Suspeitas internas: as suspeitas de incidente de segurança internas devem ser comunicadas à Unidade de Proteção de Dados Pessoais, via:

e-MS

Comunicação Interna

e-mail

encarregadolgpd@pge.ms.gov.br

Suspeitas externas: as suspeitas de incidente de segurança externas devem ser informadas à Ouvidoria, via:

Ouvidoria

fala.BR: https://falabr.cgu.gov.br/web/home

Conforme item 4 deste Plano.

O que fazer quando identificar um incidente de segurança com dados pessoais?

Informar o superior imediato

Todos aqueles em exercício na Procuradoria-Geral do Estado que identificarem a ocorrência ou suspeitarem de incidente de segurança com dados pessoais devem comunicar, imediatamente, o(a) chefe da unidade onde ocorreu o incidente.

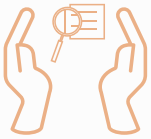
Acionar a equipe

O(A) chefe da unidade deve comunicar, imediatamente, a UPD, por meio de Comunicação Interna ou e-mail (encarregadolgpd@pge.ms.gov.br).

Isolar a área

Se possível, isole a área afetada para evitar que o problema se espalhe.

Preservar as evidências



Colete todas as informações relevantes para a investigação, como *logs* de acesso, imagens, cópias de arquivos, depoimentos de testemunhas, etc. O material deve ser entregue à UPD para a instrução do processo.

Quais as etapas do processo?

Notificador

O Chefe de Procuradoria Especializada, Coordenadoria Jurídica da PGE/MS, órgãos de apoio ou qualquer um dos integrantes da administração superior da PGE/MS atuará como notificador e encaminhará comunicação interna, urgente e instruída com o máximo de informações, à Unidade de Proteção de Dados Pessoais da PGE/MS como representante da Equipe de Resposta. Na sequência, convocará equipe para identificação do incidente de segurança, comunicação das partes, verificação e classificação do incidente e definição de medidas mitigadoras de urgência.

Fique atento!

Qualquer Procurador do Estado, servidor público ou colaborador em exercício na Procuradoria-Geral do Estado, ciente de incidente de segurança, deve noticiar o fato ao chefe de sua unidade.

Encarregado(a)

Avalia se o incidente tem impacto em dados pessoais. Se não tiver impacto, encaminha para a Administração Superior (Gabinete e Corregedoria) da PGE/MS para providências de governança e integridade na COPGE, encerrando o procedimento de incidentes de segurança com dados pessoais. Se tiver impacto, convoca a Equipe de Resposta.

Equipe de Resposta

Havendo incidente com dados pessoais, a equipe deverá identificar o incidente; comunicar as partes interessadas internas; classificar o incidente; encaminhar ao Encarregado(a) as informação para serem preparadas comunicações e notificações com apoio da Comunicação; analisar as medidas de contenção e submetê-las à autorização da administração superior e chefias; conter incidente; extinguir violações; recuperar dados e problemas; revisar processos pós-incidente; e elaborar relatório do incidente.

Relatório Circunstanciado

Em 48h do início do processo, a Equipe de Resposta deve preparar relatório circunstanciado do fato, dos eventuais danos, dos impactos institucional e pessoal do titular dos dados, bem como apresentar as medidas mitigadoras de urgência adotadas e as sugestões de eventuais outras medidas mitigadoras necessárias para o Comitê de Proteção de Dados Pessoais da PGE/MS.

Incidente físico ou digital

Físico: o chefe da Diretoria de Serviços Gerais (DSG/COPGE) e a unidade envolvida deverão ser, imediatamente, comunicados pela Equipe de Resposta a incidentes para atuarem, no prazo de 24 horas, na verificação e na apuração do ocorrido, bem como encaminharem informações formais e detalhadas à Equipe de Resposta.
Digital: o chefe da Diretoria de Suporte, Infraestrutura e Segurança em Tecnologia da Informação (DSISTI/COPGE) e a unidade envolvida deverão ser, imediatamente, comunicados pela Equipe de Resposta a incidentes para atuarem, no prazo de 24 horas, na verificação e na apuração do ocorrido, bem como encaminharem informações formais e detalhadas à equipe.
Físico e digital ao mesmo tempo: o prazo é comum a ambas diretorias e unidades envolvidas.

Administração Superior e Chefias

Devem adotar providências de governança e integridade, se o incidente de segurança não envolver dados pessoais, e comunicar as unidades da COPGE responsáveis e outras eventuais. Se houver impacto em dados pessoais, devem autorizar as medidas de contenção e disponibilizar o suporte eventualmente necessário para o devido cumprimento.

Controlador(a)

Deve notificar a ANPD e os titulares dos dados. A comunicação é encaminhada pelo(a) Encarregado(a).

Comitê de Proteção de Dados Pessoais

Deverá convocar reunião imediata para análise e deliberação acerca do relatório. A deliberação do Comitê deve apreciar o relatório e, se não aprovar por falta de informações efetivas ou por outro motivo, devolverá à Equipe de Resposta para revisão e submissão ao Comitê em 6 horas. Se aprovado o relatório, a deliberação deve ser encaminhada, imediatamente, ao(à) Encarregado(a) para preparar o material com relatório e medidas adotadas para a Unidade Central de Proteção de Dados para registro do incidente e das medidas adotadas.

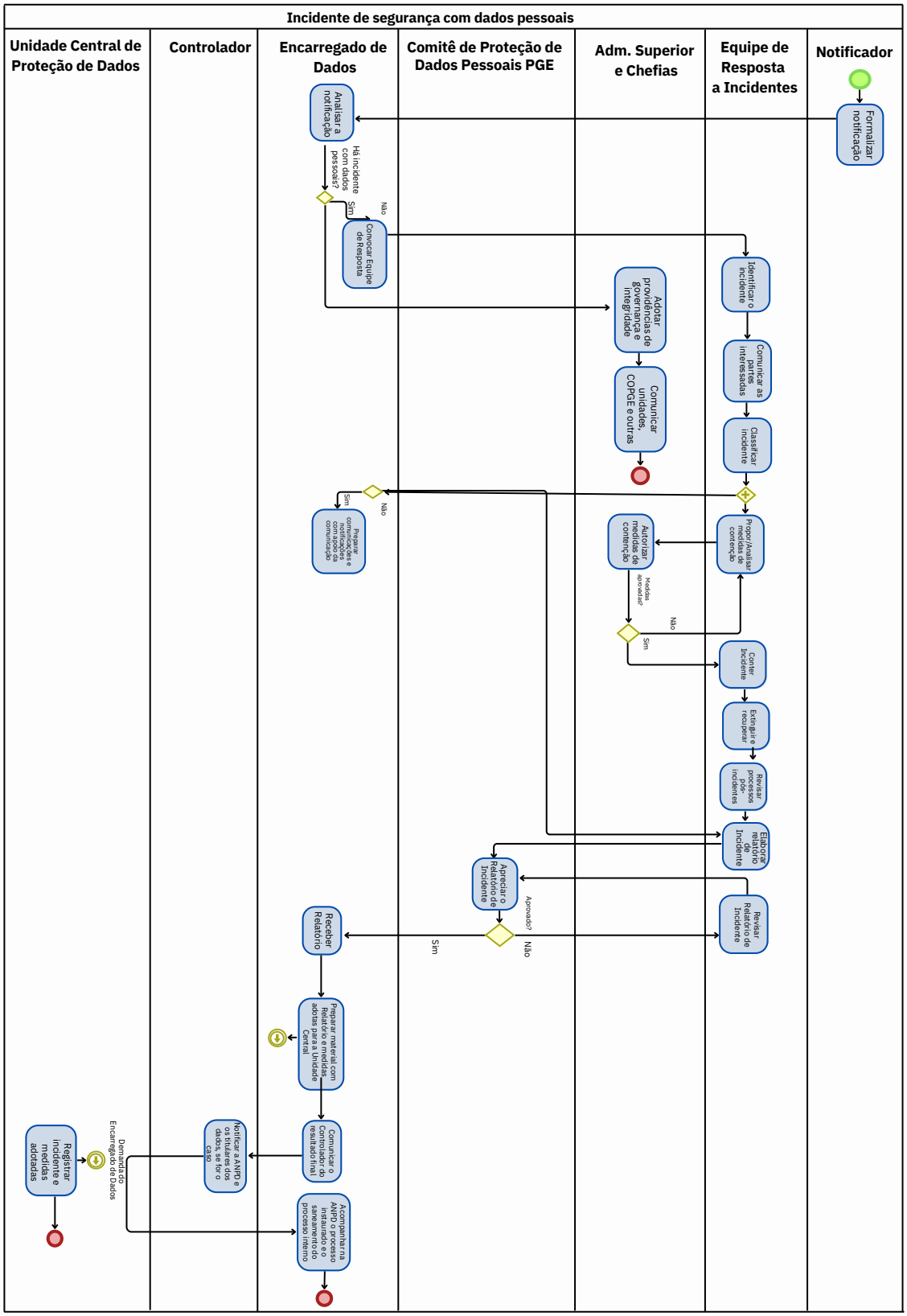
Controlador(a) dos Dados

Deverá notificar a ANPD e os titulares dos dados, conforme o caso. Encaminhará as notificações para o(a) Encarregado(a) realizar a comunicação externa (ANPD, titulares e canais de comunicação) e acompanhar o processo eventualmente instaurado na ANPD, conforme o caso, e o saneamento do processo interno. O(À) Controlador(a) pode, ainda:

(i) fazer a comunicação oficial do incidente nos canais oficiais, conforme o caso;
(ii) definir e determinar as medidas mitigadoras para o caso;
(iii) fixar melhorias de processos internos, se for o caso;
(iv) revisar o Plano de Resposta a Incidentes de Segurança com Dados Pessoais, se for o caso;
(v) determinar a instauração de processo administrativo de apuração de responsabilidade, se for o caso.

Fluxo do processo de incidente de segurança com dados pessoais da PGE/MS

Imagem: Fluxo Incidente de Segurança PGE/MS



Modelo: *Bizagi Modeler*

Mitigação e aprendizado

Como avaliar o risco do incidente de segurança com dados pessoais?

Análise da extensão ou da gravidade do incidente, como:

(i) contexto da atividade de tratamento de dados;
(ii) categorias e quantidades de titulares de dados pessoais afetados;
(iii) natureza, tipos e quantidades de dados pessoais violados;
(iv) possíveis e relevantes danos materiais, morais e reputacionais causados aos titulares dos dados pessoais;
(v) observar se os dados vazados continham proteção de forma a impossibilitar a identificação de titulares;
(vi) medidas de mitigação diligenciadas pelo(a) Controlador(a) após a ocorrência do incidente.

Identificar as causas

Investigue as causas do incidente para evitar que ocorra novamente.

Não é incidente de segurança

A simples existência de uma vulnerabilidade em um sistema de informação não caracteriza como incidente de segurança. Mas, a utilização dessa vulnerabilidade pode resultar em um incidente.

Manutenção corretiva

Detectada a vulnerabilidade em qualquer sistema, deve ser providenciada a devida correção o mais breve possível.

Fique atento!

Um mesmo tipo de incidente pode, ou não, ser considerado capaz de causar risco ou dano relevante em função da combinação desses critérios.

Ex.: um incidente de roubo de um dispositivo eletrônico pode, ou não, ser capaz de causar um risco relevante aos titulares de dados. A avaliação vai depender do tipo de dado armazenado, do contexto da atividade de tratamento e do fato de os dados estarem, ou não, protegidos por criptografia.[4]

4 Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis. Acesso em: 27 dez. 2024.

Como comunicar o incidente de segurança com dados pessoais?

Encarregado(a)

Apresenta ao(à) Controlador(a) dos Dados a documentação preparada pelo Comitê de Proteção de Dados Pessoais da PGE/MS.

Controlador(a) dos Dados

Realiza a comunicação voluntária do incidente como demonstração de transparência, cooperação e boa-fé do agente. Nesse caso, será positivamente considerada em eventual ação fiscalizadora da ANPD.

Demora injustificada

Se houver, na comunicação de incidente de segurança que possa causar risco ou dano relevante aos titulares, poderá ocorrer a sujeição dos agentes às sanções administrativas previstas na LGPD.

Notificar as autoridades

O(A) Controlador(a) dos Dados deve informar, se necessário, a ANPD e outros órgãos competentes, por meio do(a) Encarregado(a) pelo Tratamento de Dados Pessoais.

Prazo para comunicação à ANPD e aos titulares

O(A) Controlador(a) deverá realizar a comunicação no prazo de três **(3) dias úteis**, ressalvada a existência de prazo diverso previsto em legislação específica[5]

5 Arts. 6º e 9º da Resolução CD/ANPD nº 15, de 24 de abril de 2024, que Aprova o Regulamento de Comunicação de Incidente de Segurança.

Indisponibilidade das informações no prazo

Excepcionalmente, na hipótese de o(a) Controlador(a) não dispor de informações completas a respeito do incidente ou não conseguir notificar os titulares no prazo recomendado, a comunicação à ANPD poderá ser realizada em etapas: **preliminar e complementar**. A comunicação complementar deve ser protocolada no mesmo processo que a preliminar, por meio de petição intercorrente.[6]

Indisponibilidade completa das informações

Se a indisponibilidade for completa, deve ser devidamente justificada pelo(a) Controlador(a).[7]

Operador

É obrigação do(a) Controlador(a), por meio do(a) Encarregado(a) pelo Tratamento de Dados Pessoais,[8] comunicar o incidente de segurança aos titulares e à ANPD. Quando um incidente de segurança ocorrer, o Operador deverá informar o fato, sem demora injustificada, **ao(à) Controlador(a) dos Dados** que demandará internamente, conforme item 4 deste Plano. Todas as informações necessárias à comunicação do incidente de segurança, à ANPD e aos titulares deverão ser fornecidas pelo Operador ao(à) Controlador(a).

Comunicar aos titulares

Se o(a) Controlador(a) constatar que o incidente pode causar risco ou dano relevante aos titulares, o(a) Encarregado(a) entrará em contato com as pessoas cujos dados foram afetados, o mais rápido possível, explicando o ocorrido e as medidas que estão sendo tomadas.

6 A comunicação preliminar é insuficiente para o cumprimento da obrigação estabelecida pelo art. 48 da LGPD e deve ser complementada pelo controlador no prazo estabelecido.
7 Conforme o § 3º do Regulamento de Comunicação de Incidente de Segurança, as informações poderão ser complementadas, de maneira fundamentada, no prazo de vinte dias úteis, a contar da data da comunicação.
8 Art. 48 da LGPD.

Comunicação Institucional

Caso não seja possível individualizar os titulares afetados, pode ser necessário comunicar todos cujos dados estejam presentes na base de dados violada. Para isso, a Ascom será acionada.

Comunicação indireta

A comunicação por meio de publicação em meios de comunicação pode ser feita de forma excepcional e justificada, mas o meio precisa ter alcance do maior número possível de titulares e deve ser dado o devido destaque à divulgação.

Forma e meio

A comunicação deve ser feita de forma simples, individual e direta aos titulares[9], sempre que possível. Pode ser realizada por quaisquer meios, como e-mail, SMS, carta ou mensagem eletrônica e, preferencialmente, através do canal habitualmente utilizado pelo agente para comunicar com o titular.

Comprovação

A ANPD poderá solicitar ao(à) Controlador(a), a qualquer tempo, a apresentação de cópia do comunicado aos titulares para fins de fiscalização, não sendo necessário encaminhar à Autoridade Nacional a lista de titulares afetados, ou seus dados de contato para comprovação da comunicação.

9 Conforme art. 9º do Regulamento de Comunicação de Incidente de Segurança, a comunicação de incidente de segurança ao titular deverá fazer o uso de linguagem simples e de fácil entendimento, ocorrer de forma direta e individualizada, caso seja possível a identificação do titular e conter, ao menos, as seguintes informações:
I - a descrição da natureza e da categoria de dados pessoais afetados;
II - as medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
III - os riscos relacionados ao incidente com identificação dos possíveis impactos aos titulares;
IV - os motivos da demora, no caso de a comunicação não ter sido feita no prazo do caput deste artigo;
V - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente, quando cabíveis;
VI - a data do conhecimento do incidente de segurança; e
VII - o contato para obtenção de informações e, quando aplicável, os dados de contato do encarregado (grifos nossos).

Procedimento ANPD

As comunicações de incidente de segurança são recebidas e tratadas pela Coordenação-Geral de Fiscalização (CGF) da ANPD. A gravidade do incidente será considerada na priorização da análise dos comunicados recebidos.

Arquivamento

Caso o(a) Controlador(a) tenha comunicado a ocorrência do incidente aos titulares de dados e, após análise, a CGF não identificar infração à LGPD, nem a necessidade de adoção de medidas adicionais, o processo será arquivado.

Complementações

Se a comunicação aos titulares não for realizada ou considerada inadequada, pode ser determinada a realização ou a correção em sua forma ou conteúdo. Poderá, se necessário, ser determinado ao(à) Controlador(a) a adoção de medidas adicionais para mitigar os efeitos do incidente, como sua ampla divulgação.

Processo administrativo

Além disso, a CGF avaliará a possível ocorrência de infrações à LGPD e aplicará, se cabível, as sanções administrativas previstas no art. 52 da LGPD, em procedimento administrativo que possibilite às partes a ampla defesa e o contraditório.

Medidas preventivas e sanções

Poderão ser aplicadas nos casos em que o(a) Controlador(a) não comunicar o incidente à ANPD e aos titulares em tempo razoável; não comunicar o incidente aos titulares de dados pessoais afetados; e não adotar medidas de segurança técnicas e administrativas compatíveis aos riscos de suas atividades de tratamento de dados.

Comunicar internamente

O público interno deve ser informado sobre o incidente e as ações em andamento para melhoria dos processos e da capacitação do corpo técnico e administrativo.

Como mitigar os danos?

Restaurar os dados

Restaure os dados perdidos ou danificados, se possível.

Oferecer suporte aos titulares

Ofereça suporte aos titulares afetados, como auxílio para alterar senhas e monitorar suas contas.

Bloquear acessos

Bloqueie os acessos não autorizados e corrija as vulnerabilidades do sistema.

Treinamento

Se houver falha de processos internos, promova nova rodada de capacitações para evitar/mitigar a ocorrência de outros incidentes.

Operador

Se houver falha de processo ou de sistema, o(a) Controlador(a) deve solicitar adequação e fixar prazo para realização e comprovação e determinar a observância das regras contratuais e da LGPD.

Como aprender com o incidente?

Revisar o Plano

Revise o Plano de resposta periodicamente para garantir que ele esteja atualizado e seja eficaz. Um Plano de resposta à LGPD é um documento vivo, que deve ser atualizado regularmente para acompanhar as mudanças na legislação, no seu órgão ou na sua Instituição. Se você tiver sugestões, encaminhe-as à Unidade de Proteção de Dados Pessoais da PGE/MS, por comunicação interna ou e-mail (encarregadolgpd@pge.ms.gov.br).

Analisar as lições

Analise o que deu certo e o que pode ser melhorado, após a resolução do incidente.

Implementar melhorias

Implemente as melhorias necessárias para evitar a repetição do incidente.

Glossário[10]

Acesso indevido a dados pessoais: entrada irregular em ambiente físico ou lógico.

Agentes de tratamento: o(a) Controlador(a) e o Operador.

Ampla divulgação do incidente em meios de comunicação: providência que pode ser determinada pela ANPD ao(à) Controlador(a), nos termos do art. 48, § 2º, I, da LGPD, no processo de comunicação de incidente de segurança, como a publicação no sítio eletrônico, nas redes sociais do(a) Controlador(a) ou em outros meios de comunicação.

Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, que impossibilitem associar, direta ou indiretamente, a um indivíduo.

ANPD: Autoridade Nacional de Proteção de Dados, uma autarquia de natureza especial, responsável por zelar, implementar e fiscalizar o cumprimento da legislação de proteção de dados pessoais em território nacional.

Ataque cibernético: esforço intencional para tirar proveito das vulnerabilidades, com execução de ações maliciosas, visando roubar, expor, alterar ou destruir dados, por meio de acesso não autorizado a redes, sistemas de computador ou dispositivos digitais.

Autenticidade: propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade.

***Bot*:** um *bot* ou *botnet*, no contexto *hacker*, é um programa de computador utilizado para automatizar atividades maliciosas, como ataques cibernéticos, disseminação de *spam*, propagação de *malware*, ataques de negação de serviço distribuído (*DDoS*) ou roubo de dados.

Categoria de dados pessoais: classificação dos dados pessoais de acordo com o contexto e a utilização, como dados de identificação pessoal, dados de autenticação em sistemas, dados financeiros.

Comprometimento de senha: credenciais de acesso (*login* e senha de acesso pessoal) expostas a terceiros.

Comunicação de incidente de segurança: ato do(a) Controlador(a) que comunica à ANPD e ao titular de dados a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

10 Definições extraídas da Resolução CD/ANPD n° 15, de 24 de abril de 2024, e do Guia de Avaliação de Riscos de Segurança e Privacidade da Controladoria-Geral da União (2021).

Confidencialidade: propriedade pela qual se assegura que o dado pessoal não esteja disponível ou não seja revelado a pessoas, empresas, sistemas, órgãos ou entidades não autorizados.

Controlador(a): pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

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, como contas de l*ogin, tokens* e senhas.

Dado financeiro: dado pessoal relacionado às transações financeiras do titular, inclusive para contratação de serviços e aquisição de produtos.

Dado pessoal: qualquer informação relativa à pessoa natural identificada ou identificável que permita identificar, direta ou indiretamente, um indivíduo, como: nome completo, números de documentos pessoais e profissionais, assinaturas, telefone, endereço, e-mail, dentre outros.

Dado pessoal afetado: dado pessoal cuja confidencialidade, integridade, disponibilidade ou autenticidade tenha sido comprometida em um incidente de segurança.

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.

Dado protegido por sigilo legal ou judicial: dado pessoal cujo sigilo decorra de norma jurídica ou decisão judicial.

Dado protegido por sigilo profissional: dado pessoal cujo sigilo decorra do exercício de função, ministério, ofício ou profissão, cuja revelação possa produzir dano a outrem.

Disponibilidade: propriedade pela qual se assegura que o dado pessoal esteja acessível e utilizável, sob demanda, por uma pessoa natural ou por determinado sistema, órgão ou entidade devidamente autorizados.

Encarregado(a): pessoa indicada pelo(a) Controlador(a) e pelo Operador para atuar como canal de comunicação entre o(a) Controlador(a), os titulares de dados e a ANPD.

Engenharia Social: técnica utilizada por golpistas para manipular usuários, explorando erros humanos para obter dados pessoais sigilosos, além de induzir o acesso a *links* infectados e/ou espalhar infecções por *malware*.

Falha ou erro de processamento: dados de entrada que não são corretamente validados e/ou operações de tratamento automatizadas de sistema que alteram de maneira indevida a composição do dado armazenado.

Incidente: é um dispositivo de segurança que monitora o tráfego de rede de entrada e saída e decide permitir ou bloquear tráfegos específicos de acordo com um conjunto definido de regras de segurança.

***Firewall*:** ato, ameaça ou circunstância que comprometa a confidencialidade, a integridade ou a disponibilidade de dados pessoais e dados pessoais sensíveis, sob custódia da PGE/MS.

Incidente de segurança com dados pessoais: evento inadequado, relacionado à violação de dados pessoais, sendo acesso não autorizado, acidental ou não, resultando na perda, alteração, vazamento ou qualquer forma ilícita de tratamento de dados.

Integridade: propriedade pela qual se assegura que o dado pessoal não foi modificado ou destruído de maneira não autorizada ou acidental.

LGPD: Lei Geral de Proteção de Dados Pessoais nº 13.709, de 14 de agosto de 2018, que dispõe sobre o tratamento de dados pessoais, em meios físicos e digitais, realizado por pessoa natural ou jurídica de direito público ou privado, com o objetivo de proteger os dados pessoais dos titulares.

Log: processo de registro de eventos relevantes em sistema computacional.

Malware: *software* malicioso concebido para se infiltrar em dispositivos eletrônicos à revelia do usuário.

Medidas de segurança: medidas técnicas e/ou administrativas adotadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

Natureza dos dados pessoais: classificação de dados pessoais em gerais ou sensíveis.

Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do(a) Controlador(a). O servidor não é Operador.

Phishing: ataque cibernético por meio de tentativas de fraude para obter ilegalmente informações como número da identidade, senhas bancárias, número de cartão de crédito, entre outras, por meio de e-mail com conteúdo duvidoso.

Procedimento de apuração de incidente de segurança: procedimento instaurado pela ANPD para apurar a ocorrência de incidente de segurança não comunicado pelo(a) Controlador(a).

Procedimento de comunicação de incidente de segurança: procedimento instaurado pela ANPD após o recebimento de comunicação de incidente de segurança.

Processo de comunicação de incidente de segurança: processo administrativo instaurado pela ANPD do procedimento de apuração incidente de segurança e do procedimento de comunicação de incidente de segurança.

Pseudonimização: tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo(a) Controlador(a) em ambiente controlado e seguro.

Ransomware: é um tipo de *malware* que sequestra dados confidenciais ou dispositivos da vítima e ameaça mantê-los bloqueados – ou até pior – a menos que a vítima pague um resgate ao invasor.

Relatório de tratamento de incidente: documento fornecido pelo(a) Controlador(a) que contém cópias, em meio físico ou digital, de dados e informações relevantes para descrever o incidente e as providências adotadas para reverter ou mitigar os seus efeitos.

Repasse indevido de dados pessoais: instituição não atende sua finalidade legal e compartilha os dados sem consentimento do titular dos dados pessoais.

Roubo de dados pessoais: dados pessoais apropriados irregularmente nas dependências do(a) Controlador(a), falhas nos controles de segurança dos sistemas.

Sistemas: *hardware, software*, armazenador de mídias e demais recursos computacionais utilizados, desenvolvidos, adquiridos, acessados ou operados pela PGE/MS para apoio na execução de suas atividades.

Titular: pessoa natural a quem se referem os dados pessoais que são objeto do tratamento.

Tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Vazamento de dados: quebra de sigilo e/ou divulgação de dados, intencional ou não, que resulte em perda, alteração, compartilhamento, acesso, transmissão, armazenamento ou processamento de dados não autorizados.

Violação (privacidade/segurança): conduta e evento que resulte em destruição, perda, roubo, alteração, divulgação dos dados pessoais ou acesso não autorizado, danos ou desvio de finalidade em seu tratamento.

Bibliografia

ANPD, Autoridade Nacional de Proteção de Dados. **Meus dados vazaram, e agora?**. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/meus-dados-vazaram-e-agora. Acesso em: 23 dez. 2024.

_____, Autoridade Nacional de Proteção de Dados. **Guia Segurança da Informação para agentes de tratamento de pequeno porte**. Disponível em: https://www.gov.br/anpd/pt-br/documentospublicacoes/guia_seguranca_da_informacao_para_atpps___defeso_eleitoral.pdf. Acesso em: 27 dez. 2024.

_____, Autoridade Nacional de Proteção de Dados. **Resolução da ANPD n° 15, de 24 de abril de 2024**. Aprova o Regulamento de Comunicação de Incidente de Segurança. Disponível em: https://www.abrapp.org.br/legislacao/resolucao-cd-anpd-no-15-de-24-de-abril-de-2024/. Acesso em: 7 jan. 2025.

_____, Autoridade Nacional de Proteção de Dados. **Guia Orientativo de Tratamento de Dados Pessoais pelo Poder Público**. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em: 2 jan. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 19 jan. 2025.

CERT. **Vazamento de dados**. Cartilha. Disponível em: https://cartilha.cert.br/fasciculos/vazamento-de-dados/fasciculo-vazamento-de-dados.pdf. Acesso em: 20 dez. 2024.

GOVBR. **Guia de Boas Práticas: Lei Geral de Proteção de Dados Pessoais (LGPD)**. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/guias/guia_lgpd.pdf. Acesso em: 23 dez. 2024.

ISO/IEC 27035:201. **Tecnologias da Informação – Segurança – Gestão de Incidentes de Segurança da Informação.** Disponível em: https://www.iso27001security.com/html/27035.html. Acesso em: 4 dez. 2024.

MATO GROSSO DO SUL. **Decreto Estadual n° 15.572, de 28 de dezembro de 2020**. Dispõe sobre a adoção de medidas destinadas à aplicação da Lei Federal n° 13.709, de 14 de agosto de 2018 - Lei de Proteção de Dados Pessoais (LGPD), no âmbito do Poder Executivo Estadual. Disponível em: https://www.lgpd.ms.gov.br/wp-content/uploads/2021/08/DECRETO-ESTADUAL-No-15-572-2020.pdf. Acesso em: 2 dez. 2024.

PGE
Mato Grosso do Sul

Procuradoria-Geral
do Estado

UPD - Unidade de Proteção de Dados Pessoais

(67) 3318-2607

encarregadolgpd@pge.ms.gov.br

Link: https://www.pge.ms.gov.br/lgpd-lei-geral-de-protecao-de-dados-pessoais/

Av. Des. José Nunes da Cunha S/N
Parque dos Poderes, Bloco IV
Campo Grande - MS
CEP: 79031-310