Controladoria-Geral do Estado
de Mato Grosso do Sul

DESIGN: THAÍS FIRMINO | IMAGEM: 89STOCKER

PLANO DE RESPOSTA

A INCIDENTE DE SEGURANÇA **COM DADOS PESSOAIS**

EXPEDIENTE

Carlos Eduardo Girão de Arruda

Controlador-Geral do Estado

Marina Hiraoka Gaidarji

Controladora-Geral Adjunta do Estado

Juris Jankauskis Junior

Assessor de Governança e Comunicação

Elaboração:

Rosely Pereira Maia

Encarregada pelo Tratamento de Dados Pessoais – CGE/MS

Colaboração:

Leandro Silveira dos Santos

Assessor de Tecnologia da Informação – CGE/MS

Revisão de texto:

Thaiane Firmino da Silva

Assessora de Marketing – CGE/MS

Capa | Identidade visual | Ilustrações | Diagramação:

Maria Thaís Firmino da Silva

Assessora de Comunicação – CGE/MS

CONTROLADORIA-GERAL DO ESTADO DE MATO GROSSO DO SUL (CGE-MS)

Unidade de Tratamento de Dados – LGPD

Plano de Resposta a Incidente de Segurança com Dados Pessoais. Controladoria-Geral do Estado de Mato Grosso do Sul. Campo Grande, MS: CGE, 2024.

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

SUMÁRIO

01. APRESENTAÇÃO

A Lei nº 13.709/2018, Lei Geral de Proteção de Dados – LGPD, destaca a obrigatoriedade de garantia da Segurança da Informação pelos agentes de tratamento em relação aos dados pessoais, mesmo após o término do tratamento, conforme estabelecido no artigo 47. A não implementação de medidas de segurança técnicas e administrativas necessárias para a proteção dos dados pessoais sob custódia do controlador dos dados pode ser considerada tão ou mais grave que sofrer um ataque ou enfrentar um vazamento de dados.

Neste contexto, o artigo 46 reforça o dever de adoção de diligências tendentes a proteger dados pessoais de acessos não autorizados e situações acidentais ou tratamento inapropriado, que não se resumem ao emprego de medidas tecnológicas e padrões de segurança, mas também abrangem a elaboração, manutenção e revisão de documentos, com a finalidade de propiciar maior otimização dos processos internos, protegendo o órgão/entidade e sua reputação, além de seus servidores, prestadores de serviços e colaboradores.

Na Era da Tecnologia Digital, a popularização dos computadores e facilidade de acesso à internet trouxeram riscos de segurança que não devem ser negligenciados, pois qualquer sistema, a princípio, pode ser comprometido.

Assim, é essencial a criação de procedimentos e estratégias para o controle de potenciais danos, razão que justifica a elaboração de um Plano de Resposta a Incidente de Segurança, uma vez que ataques cibernéticos e episódios de vazamentos de dados estão se tornando até comuns e se apresentam cada vez mais sofisticados.

A Autoridade Nacional de Proteção de Dados – ANPD, responsável por legislar e fiscalizar sobre a aplicação da LGPD no Brasil, definiu **incidente de segurança** como "qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na 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".

Considerando o volume de dados que a **Controladoria-Geral do Estado de Mato Grosso do Sul – CGE/MS** trata e a relevância de seu papel institucional como Órgão central do Sistema de Controle Interno do Poder Executivo Estadual, é importante ter consciência de que **incidentes de segurança** são factíveis de ocorrer, sendo importante que esteja preparada para agir em caso de violações de segurança, como o acesso não autorizado, a divulgação indevida ou qualquer outra forma de comprometimento da confidencialidade, integridade ou disponibilidade dos dados pessoais.

O Plano de Resposta a Incidente de Segurança refere-se a um conjunto de diretrizes e procedimentos organizados para lidar com eventos de Segurança da Informação que possam afetar a privacidade e a proteção de dados pessoais de cidadãos.

A CGE/MS utiliza hipóteses de tratamento que se baseiam, preponderantemente, no cumprimento de suas obrigações legais ou regulatórias (art. 7°, II, LGPD), abrangendo, também, parte relativa ao controle social, no que tange ao uso compartilhado de dados para execução de política pública prevista em Regulamento (art.7°, III, LGPD) e dispõe de quantidade razoável de dados pessoais, tanto em arquivos físicos quanto digitais.

O Plano dispõe sobre as medidas que devem ser adotadas em "acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito" que envolvam dados pessoais triviais e/ou dados pessoais sensíveis sob a guarda da Controladoria-Geral do Estado de Mato Grosso do Sul, em meio físico ou digital.

Neste sentido, o presente **Plano de Resposta a Incidente de Segurança com Dados Pessoais, em conformidade com o que dispõe a Resolução CD/ANPD n. 15, de 24 de abril de 2024,** é apresentado para **conhecimento de todos os servidores, prestadores de serviços e colaboradores da CGE/MS,** objetivando, também, viabilizar a comunicação oportuna e tempestiva à ANPD, quando e se for o caso.

Rosely Pereira Maia

Encarregada pelo Tratamento de Dados Pessoais – CGE/MS

02. OBJETIVOS

Este Plano de Resposta a Incidente de Segurança tem o seguinte objetivo geral: Orientar a CGE/MS na resolução das questões pertinentes às situações de emergência e exceção, por meio de procedimento documentado, formalizado, célere e confiável, preservando as evidências que possam auxiliar a prevenir o acontecimento de novos incidentes e cumprir as exigências legais de comunicação e transparência.

Além disso, busca-se atingir os seguintes objetivos específicos:

1. Facilitar resposta coordenada e eficaz entre as áreas internas da CGE/MS, em caso de incidente de segurança;

2. Priorizar a proteção de ativos críticos do Órgão, como dados sigilosos e sistemas essenciais para a operação das atividades.

3. Minimizar o impacto na reputação do Órgão, comunicando-se de maneira eficaz com os titulares dos dados pessoais.

4. Melhorar as práticas de segurança, através de lições aprendidas com incidentes anteriores.

Neste Plano de Resposta a Incidente de Segurança serão estabelecidas funções e responsabilidades individuais e de equipes, bem como as medidas a serem implementadas para que a CGE/MS responda, adequadamente, a um incidente envolvendo dados pessoais e dados pessoais sensíveis, e deverá ser observado em conjunto com a Política de Segurança da Informação (Deliberação CETI n. 02, de 24/02/2022, no DOE n. 10.767, de 25 de fevereiro de 2022), por todas as áreas, servidores, prestadores de serviços e colaboradores, que possam vir a ter acesso às informações, arquivos e dados sob a responsabilidade da Controladoria-Geral do Estado de Mato Grosso do Sul.

Constam no Plano, também, dispositivos estabelecidos no "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.

"NESTE PLANO DE RESPOSTA A INCIDENTE DE SEGURANÇA SERÃO ESTABELECIDAS FUNÇÕES E RESPONSABILIDADES INDIVIDUAIS E DE EQUIPES, BEM COMO AS MEDIDAS A SEREM IMPLEMENTADAS".

03. DEFINIÇÕES

Para os efeitos deste Plano, são adotadas as seguintes definições:

I. LGPD: Lei Geral de Proteção de Dados Pessoais: diploma normativo (Lei Federal nº 13.709/2018), que dispõe sobre o tratamento de dados pessoais, em meios digitais ou físicos, realizado por pessoa natural ou jurídica de direito público ou privado, tendo como objetivo proteger os dados pessoais de titulares;

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

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

IV. 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;

V. Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, que impossibilitem que um dado seja associado, direta ou indiretamente, a um indivíduo;

VI. Pseudonimização: o 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 controlador em ambiente controlado e seguro;

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

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

IX. Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. O servidor não é operador;

X. Agentes de tratamento: o controlador e o operador;

XI. Encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares de dados e a ANPD;

XII. 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;

XIII. Incidente: ato, ameaça ou circunstância que comprometa a confidencialidade, integridade ou a disponibilidade de dados pessoais e dados pessoais sensíveis que estão sob custódia da CGE/MS;

XIV. 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;

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

XVI. 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 login, tokens e senhas;*

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

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

XIX. Dado protegido por sigilo legal, judicial ou profissional: dado pessoal cujo sigilo decorra de norma jurídica ou decisão judicial;*

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

XXI. 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;

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

XXIII. Vazamento de dados: quebra de sigilo, bem como divulgação de dados, intencional ou não, que resulte na perda, alteração, compartilhamento, acesso, transmissão, armazenamento ou processamento de dados, de forma não autorizada;

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

XXV. 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 uma rede, sistema de computador ou dispositivo digital;

XXVI. Acesso indevido a dados pessoais: acesso indevido a ambiente físico ou lógico;**

XXVII. Roubo de dados pessoais: dados pessoais roubados nas dependências do controlador, falhas nos controles de segurança dos sistemas;**

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

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

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

XXXI. 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.

Definições extraídas da Resolução CD/ANPD n. 15, de 24 de abril de 2024.

****Definições extraídas do Guia de Avaliação de Riscos de Segurança e Privacidade da Controladoria-Geral da União (2021).***

04. ELEMENTOS-CHAVE DO PLANO DE RESPOSTA A INCIDENTE DE SEGURANÇA

04.1 Contextualização

Incidente é toda e qualquer violação de segurança que, de forma acidental ou dolosa, ocasione destruição, perda, alteração, divulgação, uso ou acesso não autorizados a dados pessoais e dados pessoais sensíveis tratados pelo Órgão.

Incidentes podem ser causados por ações maliciosas, como ataques cibernéticos, furto de dispositivo de armazenamento de dados, ou por eventos não intencionais, como erros humanos ou falhas de sistema.

A diversidade de incidentes de segurança pode variar de acordo com a natureza e a complexidade das atividades e pode abranger uma ampla gama de eventos e situações que comprometem a segurança das informações ou recursos de um órgão, lembrando que a ANPD informa que "cabe ao controlador dos dados identificar, tratar e avaliar o risco dos incidentes de segurança que afetem suas operações de tratamento de dados pessoais".

Alguns exemplos de incidentes de segurança:

1. **Violações de dados:** acesso não autorizado a informações confidenciais (a exemplo de processos disciplinares, relatórios de auditoria, questões de Estado) que contenham dados pessoais ou dados pessoais sensíveis;
2. **Vazamento de dados pessoais:** divulgação não autorizada, por meios físicos ou digitais, de dados pessoais ou dados pessoais sensíveis;
3. **Erros humanos:** ações não intencionais que resultam em violações de segurança, como envio de documentos com dados pessoais/sensíveis para destinatários errados, publicação não proposital de dados pessoais de titulares;
4. **Ataques cibernéticos:** incluindo

malware, ransomware (sequestro de dados), ataques de phishing e engenharia social;

5. **Negação de serviço:** é uma tentativa maliciosa de sobrecarregar um servidor, rede ou serviço online com um volume excessivo de tráfego, impedindo que usuários legítimos acessem esses recursos; os ataques são realizados por meio de uma rede de computadores comprometidos chamados de "bots" ou "zumbis", que são controlados remotamente por um invasor, objetivando tornar o serviço inacessível, causando prejuízos financeiros e de reputação para a vítima;
6. **Acesso físico ou lógico prejudicado ou impossibilitado:** com relação à sistema que armazene dados pessoais, comprometendo a integridade dos mesmos permanentemente;
7. **Intrusões de rede:** acesso não autorizado a sistemas ou redes internas por meio de exploração de vulnerabilidades ou falhas de segurança;
8. **Acesso não autorizado:** tentativas de acesso físico ou lógico a sistemas que possuam dados pessoais ou dados pessoais sensíveis, sem permissão adequada;
9. **Uso inapropriado:** violação das Políticas de uso de dados, incluindo a Política de Segurança da Informação e a de Privacidade;
10. **Exploração de vulnerabilidades:** aproveitamento de falhas de segurança em software, sistemas ou infraestrutura para obter acesso não autorizado a dados pessoais ou dados pessoais sensíveis.

04.2 Critérios

Pela inteligência do artigo 48 da LGPD, a obrigação de comunicar os incidentes de segurança à ANPD cabe somente aos controladores, que deverão informar ocorrência que possa acarretar risco ou dano relevante aos titulares dos dados pessoais, afetando interesses e direitos fundamentais.

Em adição ao dano/risco significativo acima mencionado, se houver atendimento cumulativo de, pelo menos, um dos parâmetros abaixo mencionados, o incidente deverá ser comunicado:

- Envolver dados pessoais sensíveis;
- Abranger dados de crianças, de adolescentes ou de idosos;
- Atingir dados financeiros;
- Comprometer dados de autenticação em sistemas;
- Compreender dados protegidos por sigilo legal, judicial ou profissional;
- Incluir dados em larga escala.

A ANPD estabelece que “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, adolescentes ou idosos.”

O incidente de segurança que pode atingir interesses e direitos fundamentais se consubstancia nas 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, conforme leciona § 2° do art. 5° da Resolução ANPD n. 15, de 24 de abril de 2024.

São considerados incidentes com larga escala os que envolverem número significativo de titulares, abrangendo, ainda, o volume de dados envolvidos, e também a duração, frequência e extensão geográfica de localização dos titulares.

Incidentes de segurança que abranjam somente dados anonimizados ou que não sejam alusivos a pessoas naturais identificáveis não precisam ser comunicados à ANPD.

A análise do impacto, constante no Item 07 deste Plano, propicia saber sobre o nível de gravidade e de sensibilidade dos dados pessoais expostos, classificados em grau alto, médio ou baixo, e permitindo conhecer da necessidade da comunicação.

04.3 Avaliação do risco de incidente

Aspectos que devem ser considerados na avaliação do risco de incidente de segurança com dados pessoais:

- Categorias e quantidades de titulares de dados pessoais afetados;
- Tipos e quantidades de dados pessoais violados;
- Possíveis e relevantes danos materiais, morais e reputacionais causados aos titulares dos dados pessoais;
- Se os dados vazados continham proteção de forma a impossibilitar a identificação de titulares;
- Medidas de mitigação diligenciadas pelo controlador após a ocorrência do incidente.

A simples existência de uma vulnerabilidade em um sistema de informação não se caracteriza como incidente de segurança, considerando-se, porém, que a utilização dessa vulnerabilidade pode resultar em um incidente.

05. PARTICIPANTES

Cada área da CGE/MS tem responsabilidades quando tomar conhecimento da ocorrência ou suspeita de Incidente de Segurança, devendo, imediatamente, comunicar o fato ao Time de Resposta a Incidente de Segurança com Dados Pessoais ou ao representante do Comitê Permanente de Proteção de Dados Pessoais da CGE/MS.

É importante registrar a necessidade de haver trabalho preliminar de conscientização de servidores e colaboradores, de forma que, proativamente, possam identificar e informar eventual ocorrência de vazamento de dados.

COMPONENTES

Descrição da função	Área participante
TIME DE RESPOSTA A INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS*	
Áreas da CGE/MS responsáveis por receber, analisar e responder as notificações e atividades relacionadas a incidentes de segurança envolvendo dados pessoais.	Titular da Assessoria de Tecnologia da Informação – ASTI
	Encarregado pelo Tratamento de Dados Pessoais – CGE/MS
	Titular da Assessoria de Gabinete – ASGAB/MS
	Titular da Corregedoria-Geral do Estado – CRG/MS
	Titular da Ouvidoria-Geral do Estado – OGE/MS
	Titular da Diretoria-Geral de Governança e Compliance – DGC/MS
	Titular do Centro de Informações Estratégicas – CIE/MS
	Titular do Centro de Estudos e Orientações Técnicas – CEOT/MS
	Titular da Superintendência Administrativa – SUAD/MS
	Titular da Assessoria de Governança e Comunicação – AGC/MS
COMITÊ PERMANENTE DE PROTEÇÃO DE DADOS PESSOAIS DA CGE/MS	
Comitê responsável pela proposição de ações voltadas ao aperfeiçoamento dos mecanismos de tratamento e proteção dos dados pessoais existentes.	Presidente do Comitê Permanente de Proteção de Dados Pessoais – CGE/MS
	Suplente do Presidente do Comitê Permanente de Proteção de Dados Pessoais – CGE/MS (Titular da Auditoria-Geral do Estado)

*O Time de Resposta a Incidente de Segurança com Dados Pessoais deve ser composto pelo encarregado de dados e por servidores de outras áreas que detenham expertise para a abordagem do tema ou cujos processos possam ser afetados pelo incidente de segurança.

DESIGN: THAÍS FIRMINO

06. MACROETAPAS DO PROCESSO

Este Plano de Resposta a Incidente está estruturado conforme as macroetapas apresentadas a seguir:

MACROETAPA		DESCRIÇÃO
01	Identificação do incidente	Dispor de medidas de detecção e identificação de incidentes, como ferramentas de monitoramento, eventos de log, mensagens de erro firewalls, entre outros, para detecção precoce, geralmente notificados pela Secretaria-Executiva de Transformação Digital – SETDIG/SEGOV/MS ou pelos recursos computacionais da CGE/MS.
02	Avaliação interna do incidente pelo Time de Resposta a Incidente de Segurança com Dados Pessoais e Comitê Permanente de Proteção de Dados Pessoais da CGE/MS	Obter informações iniciais sobre o impacto do evento, quais sejam: categoria e quantidade de titulares e de dados pessoais afetados; consequências do incidente para os titulares e para o Órgão; necessidade de preservação das evidências existentes.
03	Procedimentos de notificação	Comunicar a existência do incidente ao encarregado pelo Tratamento de Dados Pessoais, caso envolva dados pessoais. Comunicar a existência do incidente ao controlador dos dados, caso envolva dados pessoais. Comunicar a existência do incidente à Autoridade Nacional de Proteção de Dados Pessoais – ANPD, caso haja acúmulo dos critérios do subitem 4.2 deste Plano. Comunicar a existência do incidente ao Titular dos dados pessoais, caso haja acúmulo dos critérios do subitem 4.2 deste Plano. Desenvolver Plano de comunicação para lidar com a divulgação pública e informação ao titular.
04	Contenção e erradicação do incidente; recuperação dos sistemas/processos	Conter ou isolar o incidente, de forma a não afetar outros sistemas/processos, evitando maiores danos. Inclusão da contenção de curto prazo, backup do sistema, contenção a longo prazo. Simultaneamente, adotar medidas para registrar e documentar a ocorrência do incidente, descrevendo as ações para isolar o incidente, conter danos e mitigar riscos. Após a contenção, partir para a remoção da ameaça e restauração dos sistemas ou processos afetados, com a realização de testes e validações, objetivando o retorno ao estado original anteriormente ao incidente.
05	Elaboração da documentação	Registrar todas as informações e ações realizadas para o tratamento do incidente, para fins do princípio da responsabilização e prestação de contas (art. 6º, X, LGPD), se necessário.
06	Revisão do procedimento	Realizar revisão pós-incidente a eficácia da resposta e providenciar a atualização do Plano, com base em lições aprendidas.

07. DESCRIÇÃO DO PROCESSO

Um Plano de Resposta a Incidente de Segurança é essencial para que haja continuidade das operações da Controladoria-Geral do Estado de Mato Grosso do Sul relacionadas à proteção dos dados pessoais e dados pessoais sensíveis que estão sob guarda do Órgão.

Obviamente, o encarregado de dados deve ser comunicado, e este deve cientificar o controlador dos dados, sendo que o artigo 48 da LGPD estabelece a obrigação deste comunicar à ANPD e ao titular dos dados pessoais a ocorrência de incidente que gere dano relevante aos titulares de dados pessoais.

Lembrando que, pela inteligência do inciso 5º do §1º do art 48 da Lei, é necessário justificar os motivos da demora, caso a comunicação não seja imediata.

A seguir, o detalhamento dos procedimentos que devem ser adotados, em caso de possível incidente de segurança:

1. IDENTIFICAÇÃO DO INCIDENTE

Um incidente de segurança pode chegar

ao conhecimento da CGE/MS por meio de quaisquer fontes, tais como e-mails, telefones, canais de ouvidoria ou similar, sistemas internos (como a notificação do titular diretamente ao encarregado), área de Tecnologia da Informação do Órgão ou pela Secretaria-Executiva de Transformação Digital – SETDIG/SEGOV/MS.

O incidente também pode ser identificado por meio de interrupção de um serviço de TI; recebimento de e-mails com links suspeitos ou código malicioso; vírus; ataques cibernéticos; entre outros.

Nesta fase, pode haver a classificação sobre o incidente, nos moldes do que dispõe o subitem 4.3 deste Relatório, às fls. 22.

2. AVALIAÇÃO INTERNA DO INCIDENTE

Na identificação de possível incidente na Controladoria-Geral do Estado de Mato Grosso do Sul, é necessário avaliar internamente o episódio. Nesta fase, é indispensável, também, que sejam preservadas todas as evidências existentes e sejam obtidas as seguintes informações:

2.a – Tipo de vulnerabilidade ocorrida, envolvendo situações como:

2.b – Fonte dos dados pessoais: meio pelo qual foram obtidos os dados pessoais.*

- Próprio titular dos dados pessoais (incluídos crianças e adolescentes), por meio de preenchimento de formulário eletrônico ou sistema.
- Documentos digitalizados, oriundos de webmail, processos administrativos, requerimentos, mandados de segurança, vídeos de oitivas, entre outros.
- Órgãos externos (MP/CGU/TCU/TCE) ou Terceiros (denunciantes/-testemunhas/defensores, professores, entre outros).
- Unidades Setoriais e Seccionais de Controle Interno.
- Órgãos e entidades do Poder Executivo Estadual.
- Protocolo ou outras áreas internas da CGE/MS.
- Sistemas e Bancos de Dados institucionais, quando acessados por servidores/colaboradores da CGE/MS.
- Dados oriundos de serviços de nuvem (cloud) de softwares de terceiros.
- Coletado diretamente do servidor.

*Informação extraída do Inventário de Dados Pessoais da CGE/MS.

2.c – Categoria de dados pessoais, cuja segurança foi violada:

Dados pessoais triviais	Informação relacionada a pessoa natural identificada ou identificável.
Dados pessoais sensíveis	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.
Dados pessoais de crianças e adolescentes	Crianças (até 12 anos incompletos); adolescentes (12 a 18 anos).
Dados pessoais de idosos	Grupo vulnerável (igual ou superior a 60 anos).
Dados pessoais tornados manifestamente públicos pelo próprio titular	Iniciativa do titular de tornar o dado de conhecimento público.
Dados pessoais pseudonimizados (P); Dados anonimizados (A)	(P) Dados que não oferecem possibilidade de associação direta ou indireta a uma pessoa, senão pelo uso de informação adicional mantida separadamente pelo controlador dos dados; (A) Dados que não são passíveis de associação a uma pessoa, direta ou indiretamente, e não são considerados como dados pessoais.

DESIGN: THAÍS FIRMINO

2.d – Dimensão do vazamento: quantificação dos titulares e dos dados pessoais que sofreram vazamento.

A identificação do tipo de dado pessoal vazado e da quantidade de dados e titulares atingidos propicia o conhecimento da extensão do ocorrido.

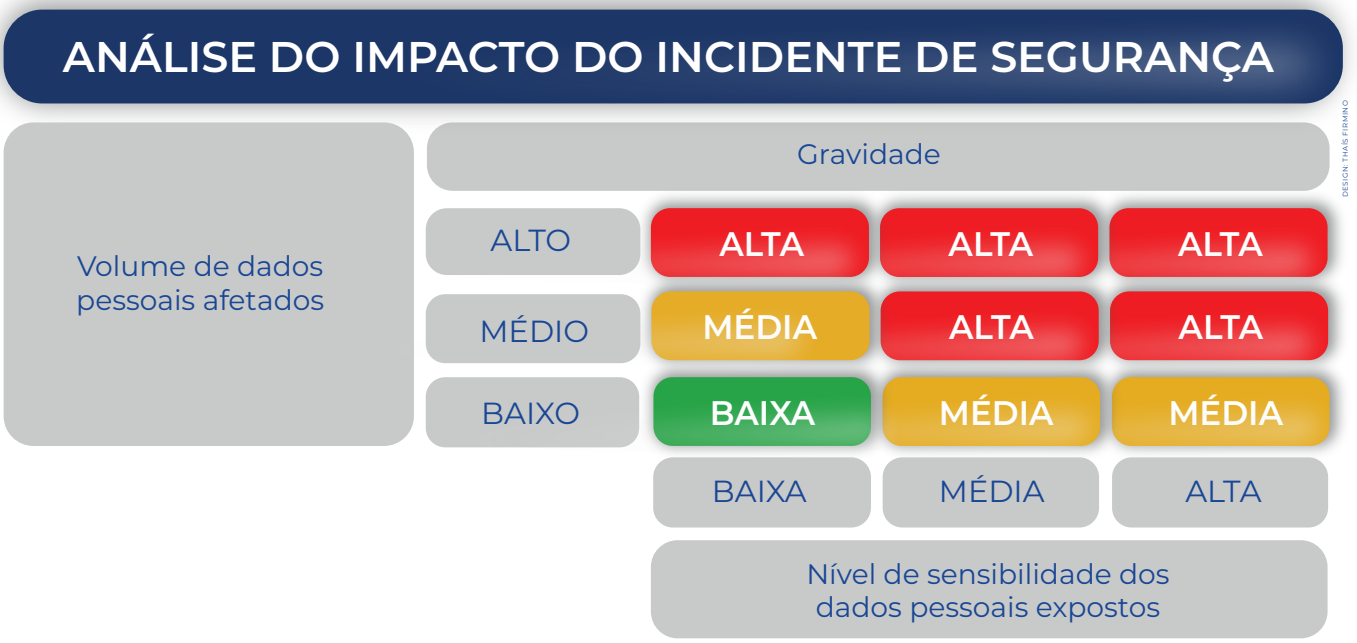
2.e – Análise do impacto do incidente: avaliar os efeitos, resultados ou prejuízos que o incidente pode causar, tanto para o titular, quanto para o Órgão ou parte interessada.

Devem ser avaliadas várias vertentes, quais sejam:

- Quais sistemas e serviços foram afetados?
- Quais categorias e quantidades de titulares foram afetados?
- Quais tipos e quantidades de dados foram expostos?

- Em decorrência disso, o titular pode ter algum tipo de prejuízo (dano material, moral, reputacional)?
- Como resultado, o titular pode ser vítima de fraude ou discriminação?
- Os dados expostos estavam protegidos, impossibilitando a identificação dos titulares?
- Quais atitudes foram adotadas pelo controlador para minimizar os danos?
- O fato concorre para prejuízo na imagem do Órgão?

A seguir, alguns indicadores para auxiliar na avaliação do risco:



Fonte: Junta Comercial do Estado de Minas Gerais.

PARÂMETROS PARA ANÁLISE DO IMPACTO DO INCIDENTE DE SEGURANÇA

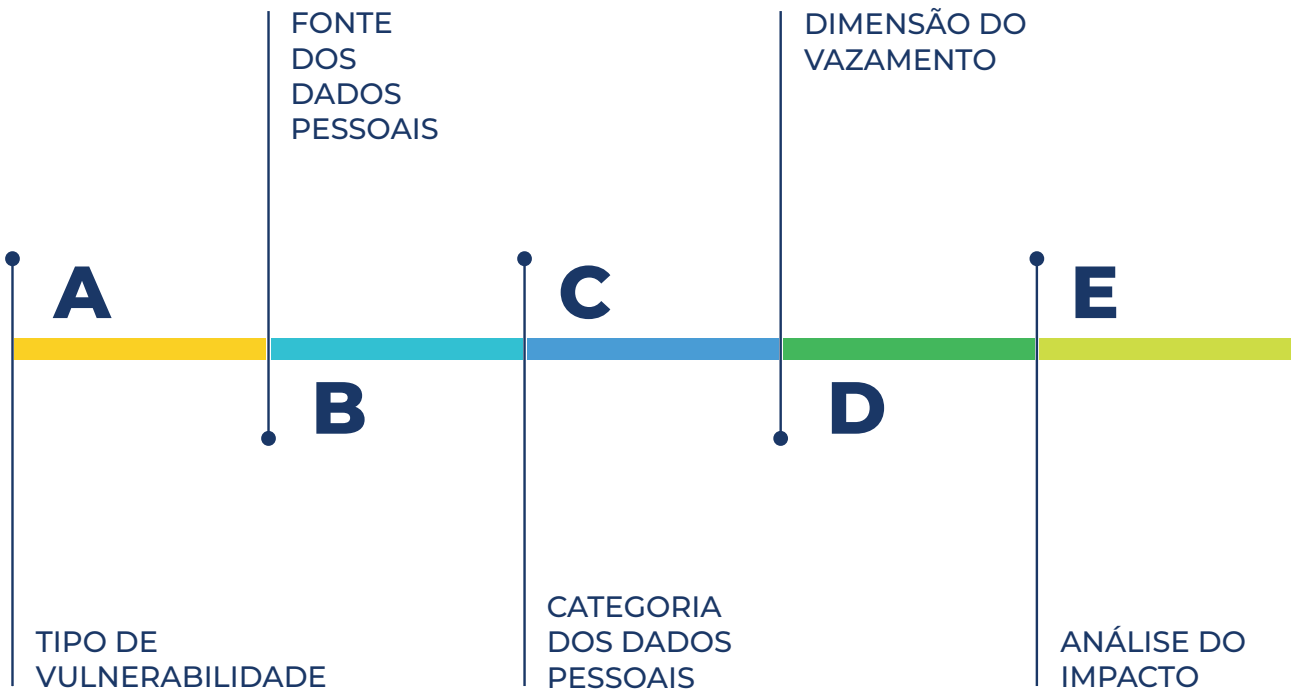
DESIGN: THAÍS FIRMINO

VOLUME DE DADOS PESSOAIS AFETADOS		NÍVEL DE SENSIBILIDADE DOS DADOS PESSOAIS EXPOSTOS	
ALTO	Volume de dados pessoais afetados superior a 10% da base de dados da Controladoria-Geral do Estado de MS.	ALTO	Dados pessoais sensíveis; Dados pessoais de crianças, adolescentes, idosos ou grupo vulnerável.
MÉDIO	Volume de dados pessoais afetados inferior a 10% e superior a 2% da base de dados da Controladoria-Geral do Estado de MS.	MÉDIO	Dados pessoais diretamente identificáveis, aliados ou não com informações comportamentais.
BAIXO	Volume de dados pessoais afetados inferior a 2% da base de dados da Controladoria-Geral do Estado de MS.	BAIXO	Dados anonimizados; dados pessoais pseudonimizados; dados pessoais de difícil identificação.

Fonte: Junta Comercial do Estado de Minas Gerais.

AVALIAÇÃO INTERNA DO INCIDENTE

DESIGN: THAÍS FIRMINO



3. PROCEDIMENTOS DE NOTIFICAÇÃO

3.a – O conhecimento da ocorrência de incidente de segurança deve motivar uma comunicação ao ***encarregado pelo tratamento de dados pessoais****, o mais breve possível, a fim de que sejam adotadas as providências cabíveis.*

3.b - Na sequência, o encarregado de dados cientifica o ***controlador dos dados****, visto que este detém o* ***poder de decisão*** *sobre o tratamento de dados pessoais do órgão sob sua titularidade.*

Caso o Time de Resposta a Incidente de Segurança com Dados Pessoais e o Comitê Permanente de Proteção de Dados Pessoais da CGE/MS **concluam que o incidente acarretou risco ou dano relevante** aos

titulares de dados pessoais, deverão ser realizadas as comunicações obrigatórias por Lei.

A responsabilidade de comunicar o fato à ANPD é do controlador dos dados, conforme estabelecido pelo art. 48 da LGPD.

O processo de comunicação do incidente de segurança pode ser iniciado de ofício ou com o recebimento da comunicação formalizada, por meio de formulário eletrônico disponibilizado no sítio eletrônico da ANPD.

Importante observar que o **operador** é um terceiro (Pessoa Jurídica) que realiza o tratamento de dados pessoais **em nome do controlador** e, em caso de incidente, **deve**, imediatamente, relatar o fato ao controlador, a fim de que este informe à ANPD.

***3.c- Evidentemente, se houver* acúmulo de critérios** *contidos no subitem* **4.2** *deste Plano, a* **ANPD** *deve ser comunicada, sendo importante observar que a lei determina que a "comunicação será feita em prazo razoável", considerando o* **prazo de 3 dias** *úteis para essa informação a partir do conhecimento pelo controlador de*

que o incidente afetou dados pessoais, conforme estabelecido no "Regulamento de Comunicação de Incidente de Segurança com Dados Pessoais", publicado pela ANPD no Diário Oficial da União, em 24 de abril de 2024.

A comunicação da ocorrência de incidente à ANPD deve conter, no mínimo:

IDENTIFICAÇÃO
Nome do órgão
Nome do controlador dos dados
Nome do encarregado de dados
Nome do operador, quando for o caso
Informação sobre ser comunicação preliminar ou completa – sendo possível o complemento da comunicação de ocorrência em até 20 dias úteis a partir de seu registro
INFORMAÇÕES SOBRE O INCIDENTE
Data e hora da descoberta do incidente
Data, hora e duração do incidente
Tipo de vulnerabilidade ocorrida (Subitem 2.a)
Descrição do incidente, incluindo a causa principal
Categoria de dados pessoais afetados (Subitem 2.c)
Quantidade de titulares atingidos
Resumo do incidente de segurança
Consequências (efeitos negativos) para os titulares
Medidas técnicas e de segurança adotadas antes e após o incidente
Riscos relacionados à ocorrência
Medidas de mitigação de riscos adotadas pelo controlador
Informações sobre medidas úteis que os titulares afetados podem tomar
Motivos da demora da comunicação, caso não seja no prazo de 3 dias úteis

DESIGN: THAÍS FIRMINO

A ANPD disponibiliza em seu sítio eletrônico um **formulário** para notificação de incidentes de segurança com dados pessoais.

3.d - Por fim, cumprindo-se cumulativamente os critérios do subitem 4.2, o* titular *dos dados pessoais deverá ser notificado, sendo importante a participação da* área de Comunicação *para esta função.

A ANPD recomenda que a informação seja feita de forma individual e direta ao titular, podendo ser utilizado e-mail, SMS, carta ou mensagem telefônica, ou por meio do canal de atendimento. Se o titular não foi individualizado, poderão ser notificados todos os constantes na base de dados violada. A comunicação indireta, por publicação em meios de comunicação, pode ser efetuada, em caráter excepcional, devendo ser dado destaque à informação.

O comunicado deve ser apresentado em linguagem clara, contendo, no mínimo:

Resumo e data da ocorrência do incidente
Data do conhecimento da ocorrência
Descrição da natureza e da categoria dos dados pessoais afetados
Informação sobre a comunicação do incidente à ANPD
Motivos da demora da comunicação, se ultrapassar 3 dias úteis
Medidas técnicas e de segurança utilizadas para a proteção dos dados
Riscos e consequências para o titular
Medidas de mitigação adotadas pelo controlador dos dados
Medidas que o titular pode adotar em benefício de sua proteção
Contato do encarregado de dados para informações suplementares

DESIGN: THAÍS FIRMINO

A Assessoria de Governança e Comunicação da CGE/MS pode colaborar, por intermédio da elaboração de informações, **tanto para os titulares**

de dados quanto para a Imprensa e a própria ANPD, se for necessário. A Assessoria poderá, também, auxiliar o encarregado de dados nas notificações obrigatórias por lei, mencionadas no Item 3 deste Plano.

4. CONTENÇÃO E ERRADICAÇÃO DO INCIDENTE; RECUPERAÇÃO DOS SISTEMAS/PROCESSOS

Na fase da contenção, é importante que os responsáveis pelos processos ou sistemas atingidos se manifestem. O incidente deve ser reprimido, de forma a atenuar os danos e impedir o comprometimento dos demais recursos.

Conforme a necessidade e autorização obtida, podem ser adotadas medidas no sentido de isolar a rede afetada ou, até mesmo, desconectar o sistema comprometido, principalmente no caso de perda ou roubo de informações durante o ataque. Também podem ser alteradas as políticas de roteamento de equipamentos de rede para interromper o fluxo malicioso ou, ainda, desabilitar serviços vulneráveis de modo a obstar o comprometimento de outros sistemas.

A fase de erradicação trata da eliminação das causas do acidente, objetivando que haja remoção dos métodos de acesso utilizados pelo atacante, seja por implementação de novas contas de acesso, backdoors e acesso físico ao sistema prejudicado, se cabível.

A recuperação visa recompor o sistema ao seu estado original e pode ser feita de forma gradual. Objetiva-se restaurar a integridade do sistema, com o propósito de que este seja recuperado e as funcionalidades estejam operantes. É conveniente que novos comprometimentos sejam reprimidos, por meio da implementação de medidas de segurança.

No caso de incidentes relacionados à atividade humana, os fatos poderão, caso envolvam atuação de servidor público no exercício do cargo ou função, ensejar a instauração de procedimentos disciplinares; ou ainda, ser objeto de comunicação às autoridades policiais, sem prejuízo da adoção de outras medidas dispostas na legislação.

Nesta fase, é necessário considerar a viabilidade de implementação das seguintes ações, conforme as características e gravidade da invasão:

CONTENÇÃO
Desconectar o sistema comprometido ou isolar a área atingida
Desativar o sistema para evitar roubo de informações durante o ataque
Alterar políticas de roteamento de equipamentos
Desabilitar serviços vulneráveis para obstar comprometimento de mais sistemas
ERRADICAÇÃO
Remover as causas do incidente
Promover a remoção dos métodos de acesso do atacante
RECUPERAÇÃO
Recompor o sistema afetado ao estado original
Verificar recuperação do sistema e das funcionalidades
Implementar medidas de segurança

DESIGN: THAÍS FIRMINO

Por fim, pode ser que haja necessidade de instalar atualizações de aplicação no Sistema Operacional ou elaborar novas rotinas.

5. ELABORAÇÃO DA DOCUMENTAÇÃO

Nesta etapa, devem ser preservadas todas as evidências que se apresentaram, com a finalidade de que, se mencionado o princípio da responsabilização, possa ser demonstrada, pelo agente, a "adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas" (art. 6º, X, LGPD).

O incidente deve ser documentado, com detalhamento das informações obtidas e a construção de uma linha do tempo contendo a especificação dos envolvidos, tipos e quantidades de dados pessoais afetados, enfim, todas as evidências coletadas, ações adotadas, danos causados, mitigação dos efeitos e neutralização da ameaça, também com vistas à prevenção futura. Esse registro deve ser mantido pelo prazo mínimo de 5 anos, a contar da comunicação do

incidente ao controlador dos dados. Além disso, deve ser preservada uma cópia dos dados vazados, para fins de registro/comprovação do ocorrido.

É necessário registrar também:

Origem do incidente (Qual área?)
Contato da origem (Qual dado de contato do informante?)
Registro da data e local do incidente (Qual a data da ocorrência e a do conhecimento? Qual endereço IP?)
Titulares afetados (Qual a quantidade?)
Recursos utilizados pela origem do incidente (Qual protocolo, portas, procedimentos adotados na ação do incidente?)
Categoria de dados atingidos (Qual natureza e categoria?)
Serviços afetados (Quais serviços envolvidos?)
Descrição do incidente (Qual tipo de ataque ou motivo?)
Logs ou evidências (Quais logs, imagens, códigos de erro ou registro?)
Usuários e métodos de acesso utilizados na intrusão
Medidas de mitigação dos efeitos (Quais as adotadas?)

DESIGN: THAÍS FIRMINO

De posse de todas as informações, posteriormente, **o encarregado pelo tratamento dos dados pessoais da CGE/MS deve elaborar relatório circunstanciado** expondo o ocorrido, apresentando os fatos: momento da identificação do incidente, natureza, extensão, consequências, adoção de providências, preservação das evidências, processo de contenção do vazamento, medidas técnicas implementadas, além de outras questões que se mostrem relevantes.

É importante que todas as informações sejam registradas, visto que a ANPD poderá:

- Avaliar as ações adotadas pelo controlador;
- Aplicar o princípio da responsabilização (art. 6º, LGPD);
- Utilizar o Relatório como referência para questionamentos.

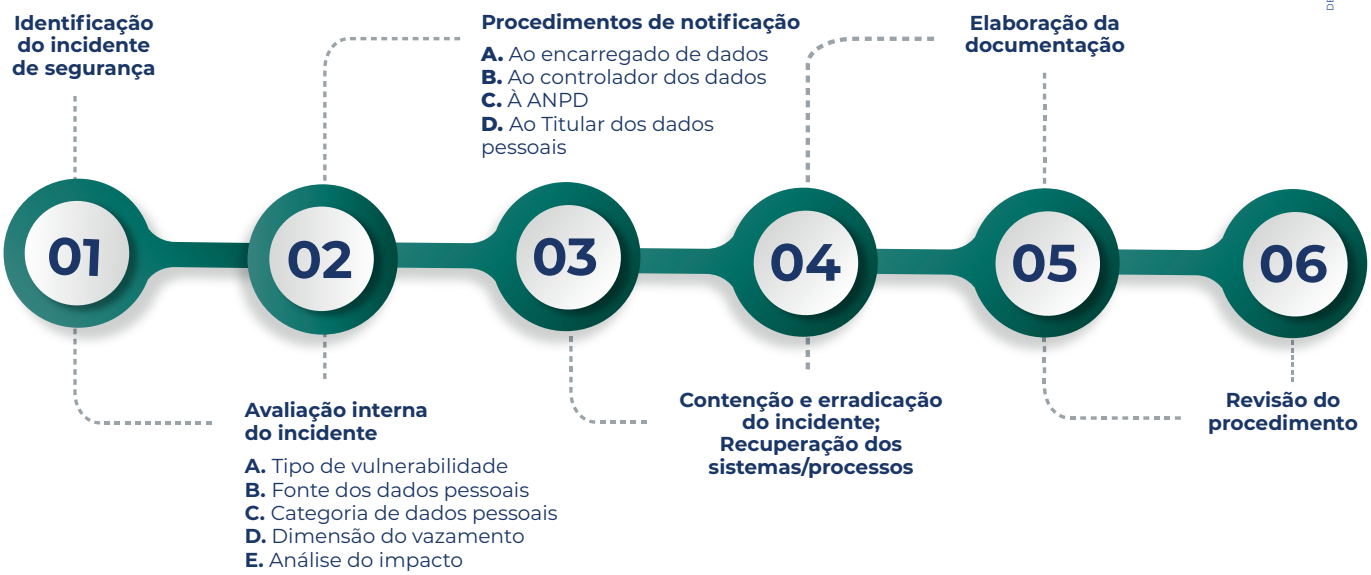
6. REVISÃO DO PROCEDIMENTO

Após os trâmites de contenção, erradicação e recuperação, deve ser **avaliada a eficácia** das soluções que foram empregadas. É apropriado o agendamento de evento com o Time de Resposta a Incidente de Segurança com Dados Pessoais e o Comitê Permanente de Proteção de Dados Pessoais para reunião de "**lições aprendidas**", que até pode contar com a participação de pessoas que não pertencem às equipes nominadas, caso necessário.

Objetiva-se o debate sobre os eventuais erros e dificuldades encontradas, com a finalidade de propor melhorias tanto nos

recursos computacionais quanto nos sistemas e processos, bem como para adequação/atualização do Plano de Resposta a Incidente de Segurança com Dados Pessoais da CGE/MS, cientificando a área afetada sobre as decisões empregadas para prevenção de incidentes da mesma natureza.

DESCRIÇÃO DO PROCESSO



08. DISPOSIÇÕES FINAIS

Os objetivos da resposta a incidentes de segurança são mitigar danos, investigar a causa raiz e implementar medidas preventivas para evitar futuros incidentes semelhantes. Essas finalidades visam propiciar que a CGE/MS possa lidar com incidentes de segurança de forma eficaz, minimizando o impacto e protegendo os ativos de informação e sua reputação.

É importante mencionar que a diversidade de incidentes de segurança pode variar de acordo com a natureza e a complexidade das operações do Órgão, razão pela qual qualquer evento que comprometa a confidencialidade, integridade ou disponibilidade de informações ou recursos deve ser comunicado a um dos titulares do Time de Resposta a Incidente de Segurança com Dados Pessoais ou do Comitê Permanente de Proteção de Dados Pessoais.

Ao seguir essas diretrizes, a Controladoria-Geral do Estado de Mato Grosso do Sul estará preparada para responder de maneira eficaz a incidentes de segurança que possam impactar a privacidade dos dados pessoais.

Este Plano de Resposta a Incidente de Segurança com Dados Pessoais entrará em vigor na data de sua publicação, por tempo indeterminado, podendo ser revisto e alterado sempre que identificada a necessidade.


CGE
Controladoria-Geral do Estado
de Mato Grosso do Sul
GOVERNO DE
Mato
Grosso
do Sul