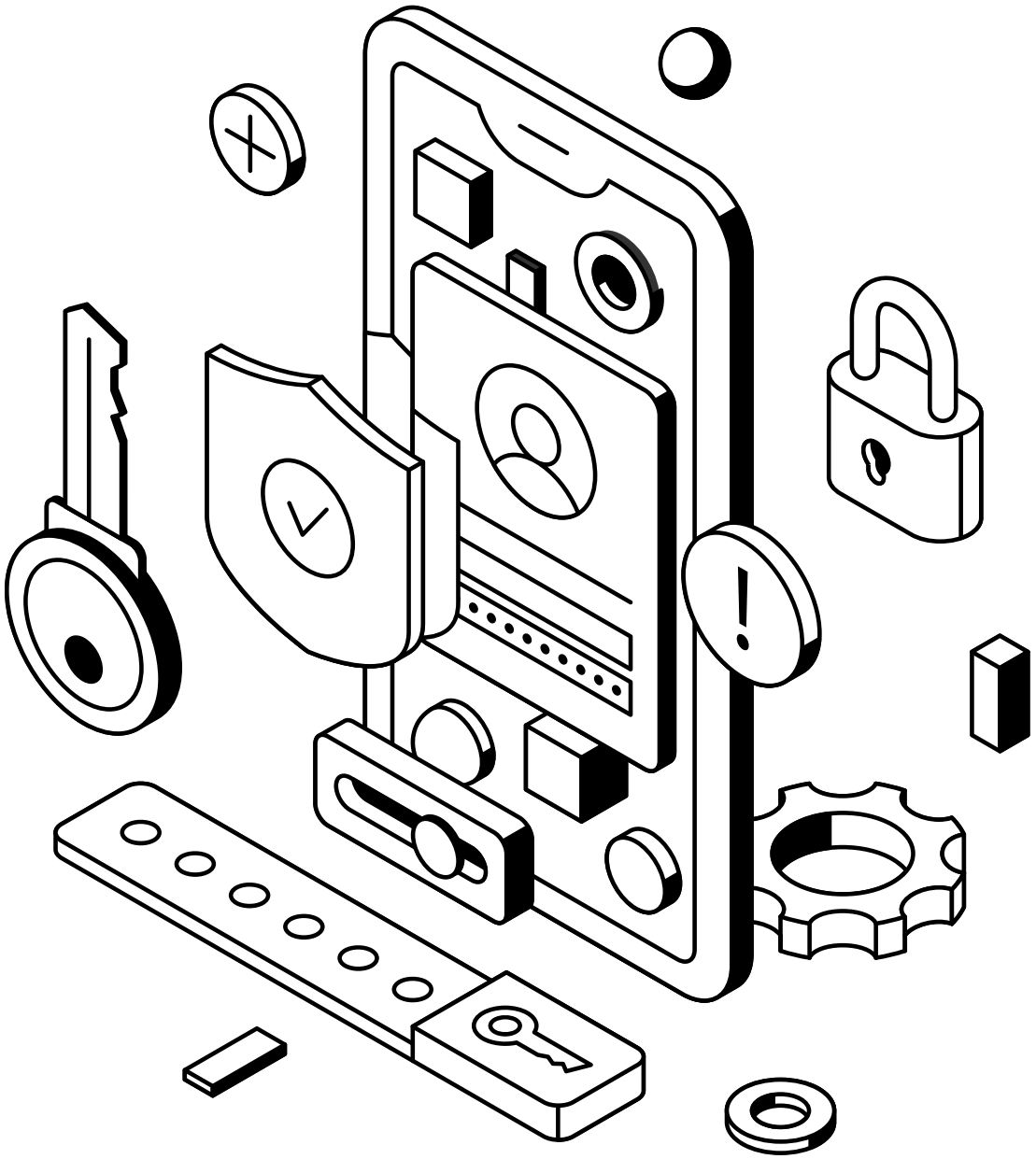
Como proceder em casos de INCIDENTES DE SEGURANÇA:

Respostas e Remediações



Cepdap | MPRJ

01

Apresentação

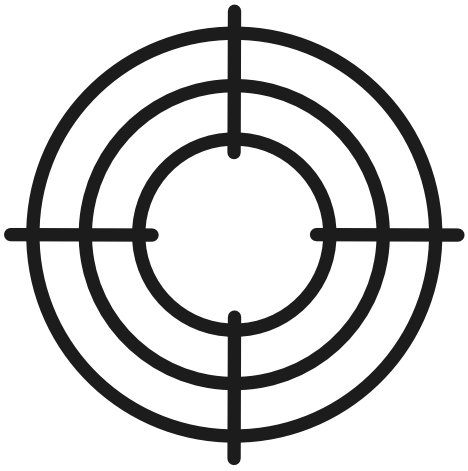
Esta cartilha é uma iniciativa do Ministério Público do Estado do Rio de Janeiro para fornecer informações claras sobre como lidar com incidentes de segurança de dados pessoais na Instituição. Em um mundo onde a segurança da informação e a proteção de dados são fundamentais, o Ministério Público do Estado do Rio de Janeiro reconhece sua responsabilidade em garantir a integridade e confidencialidade dos dados que possui.

A Resolução GPGJ n° 2.434/2021 destaca o compromisso do Ministério Público do Estado do Rio de Janeiro com a proteção de dados, e a Resolução GPGJ nº 2.548/2023 estabelece um plano para lidar com incidentes de segurança de dados.

02

Objetivos

Este documento tem o objetivo de explicar as regras da Resolução GPGJ nº 2.548/2023 sobre incidentes de segurança de dados pessoais de forma clara e acessível. Queremos que todos saibam como agir se algo der errado, como comunicar o que aconteceu e entender as consequências se não tomarmos medidas. Além disso, enfatizamos a importância de criar uma cultura de segurança e proteção de dados, que envolve tanto a prevenção quanto a correção de problemas. Com esta cartilha, esperamos que todos se sintam mais preparados para lidar com situações desafiadoras, demonstrando nosso compromisso com a privacidade e a segurança dos dados de todos que confiam em nossa Instituição.



03

Conceitos importantes

Nesta seção, vamos explicar conceitos-chave sobre segurança de dados e como agir em casos de problemas. Entender esses conceitos é fundamental para uma resposta eficaz que proteja dados pessoais e mantenha a confiança das pessoas envolvidas.

Princípio da segurança

O princípio da segurança na Lei n.º 13.709/2018 (Lei Geral de Proteção de Dados Pessoais) envolve medidas para proteger dados pessoais contra acessos não autorizados e é essencial para todos que lidam com dados pessoais.

Princípio do accountability

O princípio do accountability, junto com o da segurança, requer que quem lida com dados seja responsável e preste contas, demonstrando que está seguindo as normas de proteção de dados e comprovando sua eficácia, refletindo um compromisso com a transparência e segurança no tratamento de dados.

Incidente de segurança

Um incidente de segurança é qualquer evento que envolva acessos não autorizados, interrupções, mudanças, dano ou inadequação de informações protegidas, abrangendo desde eventos acidentais até acessos ilícitos que afetem os dados pessoais. A Autoridade Nacional de Proteção de Dados considera incidente de segurança qualquer evento adverso envolvendo violação de dados pessoais, seja por acesso não autorizado, acidental ou ilícito, com potencial para prejudicar os direitos dos titulares dos dados.

Violação de dados

Uma violação de dados acontece quando informações confidenciais são acessadas, usadas indevidamente, divulgadas ou perdidas de maneira inadequada, podendo envolver dados pessoais como nomes, números de identificação e informações financeiras. Isso pode ocorrer por falhas de segurança, ataques cibernéticos, negligência humana, entre outros fatores, representando riscos potenciais para a privacidade e os direitos das pessoas afetadas.

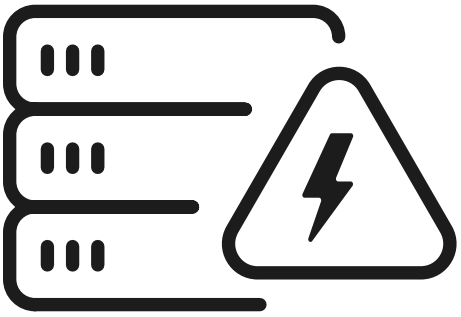
Vazamento de dados

Um vazamento de dados é uma forma específica de violação em que informações não acessíveis ao público são intencionalmente ou acidentalmente divulgadas para um público não autorizado. Isso pode ocorrer por compartilhamento sem consentimento adequado, violação de políticas de segurança ou ataques cibernéticos, causando danos potenciais à privacidade e à reputação das pessoas afetadas.

04

Exemplos de Incidente de Segurança

Entender e identificar incidentes de segurança é crucial para proteger ativos de informação e sistemas de computação em organizações. Aqui, fornecemos exemplos práticos, abordando várias facetas de ameaças cibernéticas e práticas inadequadas que podem comprometer dados e sistemas.



A seguir,

exemplos que ilustram problemas de segurança no Ministério Público do Estado do Rio de Janeiro, originados por ações inadequadas de colaboradores ou ataques externos. A avaliação da gravidade é feita pelo Encarregado de Dados, com apoio do Comitê Estratégico de Proteção de Dados Pessoais e da Secretaria de Tecnologia da Informação e de Comunicação.

Uso inadequado

a) Utilização inadequada do e-mail corporativo para o envio de spam ou para a promoção de interesses pessoais.

b) Instalação não autorizada de ferramentas na máquina do Ministério Público do Estado do Rio de Janeiro.

c) Utilização não autorizada de dispositivos de armazenamento removível como HDs externos.

d) Impressão de documentos sem a devida autorização.

Tentativas de acesso não autorizado a sistemas ou dados

a) Acesso ao sistemas do Ministério Público do Estado do Rio de Janeiro com credenciais roubadas.

b) Tentativa de acesso aos arquivos confidenciais de forma acidental.

c) Falha no sistema de autenticação do Ministério Público do Estado do Rio de Janeiro impedindo o acesso autorizado e interrompendo as operações.

Ataque de negação de serviço distribuído (DDoS)

a) Um ataque de negação de serviço distribuído (DDoS) contra o site público do Ministério Público do Estado do Rio de Janeiro sobrecarrega os servidores, tornando o site inacessível.

b) Ataque de negação de serviço distribuído (DDoS) a um servidor, que consome todos os recursos de rede, tornando a comunicação interna ineficaz.

Por fim, incidentes de segurança incluem ameaças de código malicioso

a) Envio de vírus como anexo de e-mail espalhando-o pela rede interna do Ministério Público do Estado do Rio de Janeiro.

b) Sistemas do Ministério Público do Estado do Rio de Janeiro são atacados por ransomware, que criptografa dados exigindo resgate.

c) Hackers alteram o site público do Ministério Público do Estado do Rio de Janeiro com mensagens políticas ou ofensivas.

d) Modificações não permitidas no firewall por um servidor do Ministério Público do Estado do Rio de Janeiro expõem a rede a riscos.

e) Instalação de software não licenciado por um funcionário do Ministério Público do Estado do Rio de Janeiro, expondo o computador do trabalho a vulnerabilidades, afetando os sitemas e a segurança internos.

05

Como proceder em caso de Incidentes com Dados Pessoais

O Ministério Público do Estado do Rio de Janeiro tem procedimentos rigorosos para lidar com incidentes que possam comprometer a segurança de dados pessoais, conforme estabelecido na Resolução GPGJ nº 2.548/2023, artigo 2º.

Primeiro, deve ser feita uma avaliação interna detalhada do incidente, obtendo informações importantes, como: o impacto, a natureza, a quantidade e as possíveis consequências em relação aos dados afetados e aos titulares. Todas as evidências do incidente devem ser preservadas para análise posterior.

Comunicação Estratégica, via peticionamento no sistema SEI!

O procedimento determinado na Resolução GPGJ n. 2.548/2023 estabelece várias etapas de comunicação para diferentes agentes na cadeia de tratamento de dados pessoais:

a) Comunicar ao Encarregado de Dados do Ministério Público do Estado do Rio de Janeiro se houver um incidente com dados pessoais, por meio de peticionamento no sistema SEI!

b) Informar ao controlador Ministério Público do Estado do Rio de Janeiro, conforme exigido pela Lei Geral de Proteção de Dados Pessoais, se dados pessoais estiverem envolvidos no incidente.

c) Notificar a Autoridade Nacional de Proteção de Dados e os titulares de dados pessoais sobre a existência do incidente, conforme o artigo 48 da Lei Geral de Proteção de Dados Pessoais.

d) Para incidentes que afetem a infraestrutura de TI, comunicar à Secretaria de Tecnologia da Informação e de Comunicação.

Relatório Final e Melhoria Contínua

a) Gerar um relatório final abrangente:

Incluir informações da avaliação.

Detalhar ações tomadas.

Apresentar considerações para melhorias contínuas no tratamento de incidentes.

b) Uso Conclusivo do Relatório:

Atualizar o Relatório de Impacto à Proteção de Dados Pessoais.

Manter o Ministério Público do Estado do Rio de Janeiro alinhado com as melhores práticas de proteção de dados pessoais.

c) Compromisso e Demonstração:

Fortalecimento do compromisso do Ministério Público do Estado do Rio de Janeiro com a segurança de dados pessoais.

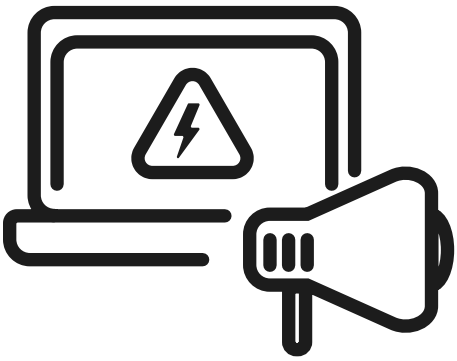
Demonstração de capacidade de resposta eficaz em incidentes.

Reforço de transparência, proteção da privacidade e confiança dos cidadãos na Instituição.

06

Comunicar Incidentes de Segurança é um Dever de Todos

Destaque para a Resolução GPGJ nº 2.548/2023:



Enfatiza deveres claros para membros, servidores, alunos-residentes, estagiários e terceirizados no Ministério Público do Estado do Rio de Janeiro.

Estabelece comunicação imediata ao Comitê Estratégico de Proteção de Dados Pessoais em casos de incidentes de segurança.

Procedimentos para Comunicar Incidentes ao Comitê Estratégico de Proteção de Dados Pessoais

A comunicação se dá por peticionamento externo no sistema SEI!

a) Identificação completa do comunicante.

b) Descrição resumida do evento suspeito.

c) Motivos que sugerem relação com a gestão de dados do Ministério Público do Estado do Rio de Janeiro.

d) Data precisa ou aproximada do evento.

e) Justificação para eventual demora na comunicação, se for o caso.

f) Indicação dos dados pessoais do comunicante.

g) Suspeita de afetação de seus dados.

h) Identificação dos dados pessoais de terceiros afetados (se possível).

i) Estimativa do número de titulares de dados pessoais possivelmente afetados.

j) Identificação da relação entre titulares afetados e o controlador (se possível).

Colaboração e Responsabilidades

a) Colaboração essencial de todos para manter a integridade e confidencialidade dos dados.

b) O Comitê Estratégico de Proteção de Dados Pessoais pode solicitar informações adicionais em até 24 horas, se necessário.

Responsabilidades no Ministério Público do Estado do Rio de Janeiro

a) Obrigatoriedade de relatar rapidamente ao Comitê Estratégico de Proteção de Dados Pessoais qualquer evento sugerindo um incidente de segurança.

b) Descumprimento pode resultar em sanções, conforme regulamentos e leis, incluindo a Lei Geral de Proteção de Dados Pessoais.

c) Cumprimento vital para proteger dados e manter a integridade dos processos.

07

Deveres dos Operadores em Casos de Incidente de Segurança

Compromisso Destacado pelo Artigo 47 da Lei Geral de Proteção de Dados Pessoais:

Enfatiza o compromisso contínuo de todos no tratamento de dados pessoais para garantir a segurança da informação, mesmo após o término do processo.

Responsabilidades dos Operadores

A comunicação se dá por peticionamento externo no sistema SEI!

a) Devem comunicar imediatamente ao Ministério Público do Estado do Rio de Janeiro os incidentes identificados.

b) Prazo de 24 horas a partir da ciência do incidente.

c) Notificação via procedimento administrativo no SEI, preenchendo o formulário disponível.

d) Detalhes essenciais incluídos na comunicação: descrição completa do incidente, dados pessoais afetados, informações sobre os titulares dos dados impactados, medidas de segurança, contato do responsável pela proteção de dados do operador, avaliação de consequências e riscos, ações planejadas ou adotadas para resolver e mitigar perdas.

Penalidades para Operadores

a) Não seguir regras de proteção de dados pode resultar em multas de até 2% do faturamento pela Autoridade Nacional de Proteção de Dados, conforme artigo 52, II, da Lei Geral de Proteção de Dados Pessoais.

Colaboração e Relatório de Impacto à Proteção de Dados Pessoais

a) O Comitê Estratégico de Proteção de Dados Pessoais pode solicitar informações faltantes em 24 horas, se necessário.

b) Operadores podem colaborar na elaboração do Relatório de Impacto à Proteção de Dados Pessoais, especialmente em casos sensíveis e de alto risco nos serviços contratados.

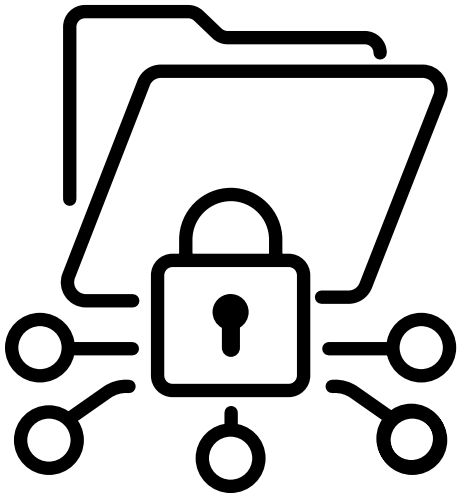
IMPORTANTE

Não seguir regras de proteção de dados pode resultar em multas de até 2% do faturamento pela Autoridade Nacional de Proteção de Dados, conforme artigo 52, inciso II, da Lei Geral de Proteção de Dados Pessoais, excluídos os tributos, limitadas, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração.

08

Fases da Atuação Institucional

O tratamento de incidentes de segurança de dados pessoais segue fases organizadas para garantir transparência, eficácia e conformidade legal. Órgãos específicos conduzem essas etapas para garantir uma resposta coordenada e robusta.



Avaliação Inicial e Encaminhamento

O Encarregado de Dados da Instituição avalia a comunicação recebida por meio do procedimento criado no SEI!, verificando a robustez, veracidade e relevância do incidente. Se houver indícios suficientes, encaminha o procedimento à Secretaria de Tecnologia da Informação e Comunicação.

Triagem, Análise e Resposta

A Secretaria de Tecnologia da Informação e de Comunicação confirma a procedência da comunicação do incidente e elabora um relatório em 1 dia útil para o Comitê Estratégico de Proteção de Dados Pessoais, detalhando informações essenciais, como data e hora da detecção, natureza da vulnerabilidade, extensão do vazamento, impacto nos titulares e na Instituição, além de medidas técnicas adotadas.

Comunicação à Autoridade Nacional de Proteção de Dados e ao Conselho Nacional do Ministério Público

O Encarregado pela Proteção de Dados notifica a Autoridade Nacional de Proteção de Dados sobre o incidente em até 2 dias úteis. A comunicação inclui informações cruciais, como responsáveis, datas e circunstâncias do incidente, bem como medidas preventivas adotadas. Se necessário, informações adicionais podem ser fornecidas posteriormente. O Comitê Estratégico de Proteção de Dados Pessoais comunica ao Conselho Nacional do Ministério Público sobre incidentes significativos, registrando internamente avaliações, medidas e análises de riscos conforme a Lei Geral de Proteção de Dados Pessoais.

Comunicação aos Titulares Afetados

O Comitê informa diretamente aos titulares afetados sobre incidentes, destacando riscos e fornecendo detalhes do incidente, avaliação de fraude, confirmação de notificação às autoridades, medidas de proteção e orientações. Em casos de impossibilidade de identificação individual, todos na base de dados comprometida são notificados. Em situações graves, o Comitê Estratégico de Proteção de Dados Pessoais pode recomendar a divulgação nos canais oficiais do Ministério Público do Estado do Rio de Janeiro, em colaboração com a Ouvidoria para informar à sociedade.

Medidas Tomadas

O Comitê elabora documentação que inclui a avaliação interna do incidente, medidas adotadas e análise de risco completa, cumprindo o princípio de responsabilidade da Lei Geral de Proteção de Dados Pessoais (artigo 6º, X). O Encarregado pelo Tratamento das informações deve elaborar o Relatório de Impacto à Proteção de Dados Pessoais em situações específicas, como tratamento de dados relacionados aos temas segurança pública, defesa nacional, segurança do Estado, atividades de investigação, repressão de infrações penais, infração da Lei Geral de Proteção de Dados Pessoais por órgãos públicos ou quando há possibilidade de impacto na privacida de dos titulares.

09

Conclusão

A cartilha representa o compromisso sólido do Ministério Público do Estado do Rio de Janeiro com a segurança e proteção abrangente dos dados pessoais. Por meio de resoluções específicas, o Ministério Público do Estado do Rio de Janeiro reforça seu empenho em adotar as melhores práticas.

Os procedimentos detalhados revelam uma abordagem séria do Ministério Público do Estado do Rio de Janeiro para a segurança de dados, garantindo transparência e eficácia na gestão de incidentes. A ênfase na colaboração destaca a importância de todos no processo de proteção de dados.

O dever de comunicar incidentes, aplicável a membros, a colaboradores e a operadores, reflete a seriedade do Ministério Público do Estado do Rio de Janeiro na segurança dos dados pessoais. A documentação e análise de incidentes, junto com o Relatório de Impacto à Proteção de Dados Pessoais, demonstram o compromisso do Ministério Público do Estado do Rio de Janeiro com a prestação de contas e a responsabilização.

Cepdap | MPRJ

Luciano Oliveira Mattos de Souza

Procurador-Geral de Justiça

Guilherme Magalhães Martins

Procurador de Justiça Encarregado pelo Tratamento de Dados Pessoais

Comitê Estratégico de Proteção de Dados Pessoais (CEPDAP/MPRJ)

Revisão e validação

Gerência de Portal e Comunicação Visual (GPPV/MPRJ)

Projeto gráfico | Visual Law

Em caso de dúvidas

Entre em contato com o Comitê Estratégico de Proteção de Dados Pessoais.

E-mail: **cepdap@mprj.mp.br**

Tel.: **21-25501250**