PREFEITURA RIO | Rio-Águas

Plano de Resposta aos Incidentes de Proteção de Dados Pessoais PRIPDP

Fundação Instituto das Águas do Município do Rio de Janeiro - (Rio-Águas)

Outubro/2025

Introdução

Um incidente de segurança com dados pessoais ocorre quando há comprometimento da **confidencialidade, integridade ou disponibilidade** dessas informações, resultante de eventos adversos como uso não autorizado, destruição, perda, alteração, exposição, vazamento ou ataque a sistemas e bases de dados. Tais situações podem decorrer tanto de falhas acidentais — como envio de informações ao destinatário incorreto, publicação não intencional de dados de titulares ou perda de mídias de armazenamento — quanto de atos intencionais, a exemplo de invasões, sequestro de dados (*ransomware*) ou furto de dispositivos.

É importante destacar que a mera existência de uma vulnerabilidade não configura, por si só, um incidente de segurança; somente sua exploração ou materialização gera riscos concretos. A gravidade desses riscos dependerá de fatores como a natureza dos dados comprometidos, o contexto do tratamento, o volume envolvido, a presença de dados sensíveis e a existência (ou não) de mecanismos de proteção, como a criptografia. Incidentes que possam expor titulares a danos materiais ou morais, discriminação, roubo de identidade ou outros impactos relevantes — especialmente quando afetam dados em larga escala ou de grupos vulneráveis como crianças, adolescentes e idosos — exigem resposta imediata e estruturada.

Entre os exemplos mais comuns de incidentes de segurança da informação estão:

- **Acesso não autorizado** a redes ou sistemas, seja por agentes externos ou internos;
- **Infecção por vírus ou códigos maliciosos**, detectáveis por ferramentas especializadas;
- **Uso indevido de recursos tecnológicos**, como instalação de softwares não autorizados, transporte de dados em dispositivos externos sem permissão ou compartilhamento inadequado de informações sigilosas.

Considerando o volume de dados tratados pelo Órgão e sua responsabilidade institucional na prestação de serviços públicos, é fundamental reconhecer que incidentes de segurança são uma possibilidade concreta e que a prevenção deve ser acompanhada da capacidade de resposta eficiente.

Neste contexto, em conformidade com a **Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD)**, o presente **Plano de Resposta aos Incidentes de Proteção de Dados Pessoais (PRIPDP)** estabelece diretrizes e procedimentos para a identificação, tratamento e comunicação de incidentes, inclusive à **Autoridade Nacional de Proteção de Dados (ANPD)**, sempre que houver risco ou dano relevante aos titulares. O objetivo é garantir a adoção de medidas técnicas, administrativas e organizacionais que possibilitem a mitigação dos efeitos adversos, a preservação dos direitos fundamentais e a continuidade das atividades institucionais.

Objetivos

Geral

Estabelecer uma estratégia estruturada de **prevenção, resposta e comunicação** a incidentes de segurança envolvendo dados pessoais, de forma **documentada, rápida, confiável e transparente**, assegurando a preservação de evidências, o cumprimento das exigências legais e regulatórias e a adoção de medidas que reduzam riscos de recorrência.

Específicos

- **Proteger a reputação institucional** e a credibilidade das atividades desempenhadas pela Fundação Rio-Águas, evitando custos adicionais, impactos legais e danos à imagem pública.
- **Garantir confiança e segurança** aos titulares de dados, usuários internos e externos, por meio de práticas de tratamento adequadas e responsáveis.
- **Definir fluxos claros de procedimentos** e responsabilidades para o tratamento de incidentes, assegurando respostas rápidas, efetivas e coordenadas.
- **Aprimorar continuamente o processo de gestão de incidentes**, incorporando as lições aprendidas e fortalecendo as medidas de prevenção e mitigação.

A proteção de dados pessoais é dever da Administração Pública e pressupõe o alinhamento às normas da LGPD, ao Decreto Rio nº 54.984/2024 e às orientações da ANPD. A aplicação desses conceitos fundamenta o PRISDP e orienta a atuação institucional em resposta a incidentes.

Definições e Conceitos Fundamentais da LGPD

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 - LGPD) estabelece diretrizes e princípios para o tratamento de dados pessoais no Brasil. A seguir, apresentam-se os principais termos, conceitos e princípios que orientam este Plano:

Dados

- **Dado Pessoal**: Qualquer informação relacionada a pessoa natural identificada ou identificável, como nome, CPF, RG, endereço, telefone ou combinação de dados que possibilite a identificação do titular.
- **Dado Pessoal Sensível**: Informações que exigem maior proteção, como origem racial ou étnica, convicção religiosa, opinião política, filiação sindical, dados referentes à saúde, vida sexual, dados genéticos ou biométricos, quando vinculados a uma pessoa natural.

- **Dado Anonimizado**: Informação que passou por processo técnico que retira a possibilidade de associação, direta ou indireta, a um indivíduo de forma **irreversível**.
- **Anonimização**: Procedimento técnico que torna os dados pessoais impossíveis de identificar, de forma irreversível.
- **Pseudonimização**: Substituição de informações identificáveis por identificadores artificiais (como códigos), sendo possível reverter a anonimização por meio do acesso a uma base separada mantida pelo controlador.
- **Banco de Dados**: Conjunto estruturado de dados pessoais, em suporte físico ou eletrônico.
- **Bloqueio**: Suspensão temporária de qualquer operação de tratamento.
- **Eliminação**: Exclusão de dado ou conjunto de dados armazenados.

Agentes de Tratamento

- **Titular**: Pessoa natural a quem se referem os dados pessoais.
- **Agentes de Tratamento**: Incluem o **Controlador** e o **Operador**.
    - **Controlador**: Pessoa física ou jurídica, de direito público ou privado, responsável pelas decisões referentes ao tratamento de dados pessoais.
    - **Operador**: Pessoa física ou jurídica que realiza o tratamento em nome do Controlador, seguindo suas instruções.
    - **Controladoria Conjunta**: Situação em que dois ou mais Controladores compartilham responsabilidades sobre finalidades e meios do tratamento.
- **Encarregado de Dados (DPO)**: Pessoa indicada pelo Controlador para atuar como canal de comunicação entre titulares, Controlador e a Autoridade Nacional de Proteção de Dados (ANPD), além de orientar boas práticas e monitorar o tratamento.

Tratamento de Dados

- **Tratamento**: Toda operação realizada com dados pessoais, como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, modificação, comunicação, transferência ou difusão.
- **Consentimento**: Manifestação **livre, informada e inequívoca** pela qual o titular concorda com o tratamento de seus dados para uma finalidade específica.
- **Transferência Internacional de Dados**: Envio de dados pessoais para país estrangeiro ou organismo internacional.
- **Uso Compartilhado de Dados**: Comunicação, difusão ou tratamento compartilhado de dados entre órgãos públicos ou entre estes e entidades privadas, quando permitido pela LGPD.
- **Bases Legais**: Hipóteses que autorizam o tratamento de dados pessoais (art. 7º da LGPD) e de dados sensíveis (art. 11 da LGPD), incluindo consentimento e outras finalidades legítimas previstas em lei.

Governança e Fiscalização

- **Autoridade Nacional de Proteção de Dados (ANPD)**: Órgão da Administração Pública responsável por zelar, implementar, regular e fiscalizar a aplicação da LGPD, podendo aplicar sanções.
- **Relatório de Impacto à Proteção de Dados (RIPD)**: Documento elaborado pelo Controlador que descreve processos de tratamento e avalia riscos, salvaguardas e medidas de mitigação.
- ***Privacy by Design* (Privacidade desde a Concepção)**: Integração de requisitos de privacidade no desenvolvimento de produtos, serviços e processos desde a sua criação.
- ***Privacy by Default* (Privacidade por Padrão)**: Garantia de que, por padrão, apenas os dados estritamente necessários sejam coletados e tratados.
- **Princípios da LGPD**: As atividades de tratamento devem observar a boa-fé e os seguintes princípios:
  - Finalidade
  - Adequação
  - Necessidade
  - Livre Acesso
  - Qualidade dos Dados
  - Transparência
  - Segurança
  - Prevenção
  - Não Discriminação
  - Responsabilização e Prestação de Contas

Governança Municipal (Decreto Rio nº 54.984/2024)

- **Encarregado de Dados (DPO)**: Responsável pela coordenação da proteção de dados na Fundação Rio-Águas, comunicação com a ANPD e orientação de boas práticas.
- **Comitê de Privacidade e Proteção de Dados Pessoais**: Grupo de apoio ao DPO, encarregado de avaliar processos, apoiar a implantação do Programa de Governança e analisar incidentes.

Compartilhamento e Direitos dos Titulares

- **Compartilhamento de Dados**: Deve ser formalizado por contrato, convênio ou ato normativo, observando finalidade, necessidade, transparência e medidas de segurança. É vedada a transferência a entidades privadas, salvo exceções legais.
- **Direito de Petição dos Titulares**: Os titulares podem exercer seus direitos de forma gratuita mediante requerimento expresso, atendido no prazo de até 15 dias, prorrogável mediante justificativa.

Incidente de Segurança e Vazamento de Dados Pessoais

Definição

Um **Incidente de Segurança** é qualquer evento indesejado ou inesperado que comprometa a segurança de dados pessoais, podendo resultar em:

- Acesso não autorizado;
- Destruição, perda ou alteração (acidental ou ilícita);
- Comunicação ou outro tratamento inadequado ou ilícito.

O **Vazamento de Dados** é um tipo específico de incidente em que informações privadas e sigilosas são expostas publicamente ou a terceiros sem autorização. Esse cenário pode permitir que dados sejam acessados, comercializados, utilizados em golpes, extorsões ou causem danos à imagem institucional.

Causas e Fatores de Vazamento de Dados

Causas mais comuns

1. **Ataques maliciosos** - como *malwares* e *ransomwares*, que sequestram dados e exigem resgate.
2. **Falhas técnicas ou de sistema** - decorrentes de indisponibilidade, bugs ou falta de manutenção.
3. **Erro humano** - ações acidentais de servidores, colaboradores ou terceiros.

Fatores que facilitam ataques

- Uso de credenciais comprometidas;
- Falhas de configuração em ambientes de nuvem;
- Vulnerabilidades em softwares de terceiros;
- Práticas de *phishing* e engenharia social.

Medidas Preventivas e Estrutura de Governança

A **LGPD** determina que os Agentes de Tratamento (Controlador e Operador) adotem medidas de segurança técnicas e administrativas para proteger os dados pessoais.

Medidas Preventivas

Área	Medidas Preventivas
Tecnologia	Implementar soluções de proteção contra códigos maliciosos homologadas, com atualizações automáticas de antivírus e firewall corporativo. Utilizar criptografia de disco (BitLocker) em estações de trabalho.

Área	Medidas Preventivas
Tecnologia	Utilizar criptografia SMB em servidores físicos. Aplicar controle inteligente de aplicativos para bloquear execuções não autorizadas. Ativar proteção baseada em reputação e mitigação contra *exploits*. Assegurar o isolamento do núcleo habilitado para integridade do sistema. Auditar periodicamente as configurações e chaves de criptografia. Utilizar autenticação multifator (MFA) para sistemas críticos e serviços em nuvem. Aplicar de patches de segurança e firmware conforme recomendações dos fabricantes. Adotar mecanismos de auditoria e monitoramento contínuo de acessos, incidentes e registros de rede. Coagir a instalação de softwares não homologados e o uso de mídias externas sem verificação de antivírus. Utilizar protocolos WPA3 ou superior em redes sem fio e a configuração segura de ambientes de nuvem com criptografia em repouso e em trânsito. Realizar backups completos e incrementais, com verificação de integridade e testes periódicos de restauração.
Infraestrutura	Atualizar continuamente sistemas, softwares e hardwares. Armazenar documentos físicos em armários trancados, com controle de chaves e acesso restrito e eliminar os mesmos com segurança conforme temporalidade. Assegurar o controle físico de acesso a salas de servidores, com registro de entrada e saída de pessoas autorizadas. Instalar equipamentos de rede em locais protegidos contra acesso indevido. Reprimir a instalação de *access points* ou roteadores sem coordenação do Suporte de TI. Implementar redundância de energia e conectividade, garantindo continuidade dos serviços essenciais. Analisar vulnerabilidade e efetuar testes de recuperação periodicamente. Restaurar ao estado de fábrica os equipamentos antes do descarte. Manter cópias de segurança armazenadas de forma segura, com definição de ciclos de retenção e cronogramas de verificação.
Acesso e Controle	Manter autenticação individual e intransferível para cada usuário. Excluir contas inativas e atualizar imediatamente credenciais comprometidas. Estabelecer regras de criação e renovação de senhas (mínimo 10 caracteres, letras, números e símbolos). Bloquear contas inativas e forçar a troca de senhas a cada 60 dias. Orientar que senhas não sejam armazenadas em navegadores ou transmitidas por e-mail. Adotar controle de tentativas de autenticação (máximo de 3 antes do bloqueio).

Área	Medidas Preventivas
Acesso e Controle	Implementar registro e rastreabilidade de acessos a sistemas e bancos de dados. Controlar concessão de acessos privilegiados e revisar perfis de usuários periodicamente.
Tecnologia	Implementar soluções de proteção contra códigos maliciosos homologadas, com atualizações automáticas de antivírus e firewall corporativo. Utilizar criptografia de disco (BitLocker) em estações de trabalho. Utilizar criptografia SMB em servidores físicos. Aplicar controle inteligente de aplicativos para bloquear execuções não autorizadas. Ativar proteção baseada em reputação e mitigação contra *exploits*. Assegurar o isolamento do núcleo habilitado para integridade do sistema. Auditar periodicamente as configurações e chaves de criptografia. Utilizar autenticação multifator (MFA) para sistemas críticos e serviços em nuvem. Aplicar de patches de segurança e firmware conforme recomendações dos fabricantes. Adotar mecanismos de auditoria e monitoramento contínuo de acessos, incidentes e registros de rede. Coagir a instalação de softwares não homologados e o uso de mídias externas sem verificação de antivírus. Utilizar protocolos WPA3 ou superior em redes sem fio e a configuração segura de ambientes de nuvem com criptografia em repouso e em trânsito. Realizar backups completos e incrementais, com verificação de integridade e testes periódicos de restauração.
Pessoas e Cultura	Promover treinamentos e fomentar a capacitação em LGPD e em relação aos riscos em segurança da informação entre os colaboradores. Vedar o uso de e-mails pessoais para tratar de assuntos institucionais. Reforçar o uso ético e seguro de dados pessoais e dos ativos tecnológicos na cultura organizacional. Orientar que os usuários internos deverão reportar imediatamente problemas e situações de possível risco ao Comitê de Privacidade e/ou Suporte de TI Promover condições para o Comitê de Privacidade planejar e acompanhar a execução das políticas internas e avaliar incidentes.
Governança	Estabelecer e atualizar periodicamente os instrumentos de gestão da LGPD. Formalizar matriz de responsabilidades entre titulares das pastas, fiscais de contrato, operadores, agentes de monitoramento de riscos e encarregados. Registrar e avaliar todos os incidentes em fluxo institucional. Fiscalizar as cláusulas dos Contratos Administrativos e congêneres referentes à LGPD. Emitir Orientações do Controlador aos Operadores. Celebrar Termos de Compartilhamento de Dados Pessoais. Aplicar anonimização em relatórios e bases de dados que contenham informações pessoais sensíveis para fins de ampla divulgação e compartilhamento com pessoas jurídicas de direito privado, bem como em respostas à requerimentos LAI.

Estrutura Municipal de Resposta a Incidentes

O **Programa Municipal de Proteção de Dados Pessoais** contempla a gestão de riscos e o tratamento de incidentes de segurança, conforme previsto na LGPD.

Fluxo de Comunicação em Caso de Incidente

1. Identificação de incidente que possa acarretar risco ou dano relevante aos titulares.
2. Comunicação imediata ao **Encarregado de Dados**.
3. Sob coordenação do **Encarregado Geral do Município**, comunicar a **ANPD** e o **titular dos dados**, nos termos da LGPD.
4. O **Controlador de Dados** do órgão também deve formalizar a comunicação.
5. O **Comitê de Privacidade e Proteção de Dados Pessoais** deve:
    - Avaliar a criticidade do incidente e acionar TI, quando necessário;
    - Documentar todas as etapas da resposta ao incidente.

Consequências e Responsabilidade Legal

- Sanções administrativas (inclusive multas).
- Perdas financeiras (contratuais, operacionais ou de imagem).
- Quebra de confiança com usuários e titulares de dados.
- Danos à reputação institucional.
- Ações judiciais individuais ou coletivas.

O **Controlador** ou **Operador** responde por danos patrimoniais ou morais decorrentes de incidentes, salvo se comprovar que:

- Não realizou o tratamento em questão;
- Houve tratamento, mas sem violação à legislação;
- O dano decorreu exclusivamente de culpa do titular ou de terceiros.

Compartilhamento de Dados Pessoais

Requisitos internos:

- **Formalização** por processo administrativo, contrato ou convênio;
- **Necessidade e finalidade** específicas e compatíveis com a coleta original;
- **Base legal e prazo** de utilização definidos;
- **Segurança e transparência** garantidas;
- **Publicidade** das hipóteses de compartilhamento no site institucional.

Compartilhamento com órgãos de controle:

Permitido com Judiciário, Legislativo, Tribunais de Contas, Ministério Público e outras autoridades, desde que:

- Não envolva reserva de jurisdição;
- Seja restrito às atribuições legais do órgão requisitante;
- Seja formalizado em processo auditável.

Vedação a entidades privadas:

É proibida a transferência de dados pessoais a entes privados, exceto quando:

- For para execução descentralizada de atividade pública;
- Envolver dados publicamente acessíveis;
- Estiver respaldada por previsão legal ou contratual;
- For exclusiva para prevenção de fraudes ou proteção do titular.

Direito de Petição dos Titulares e Tramitação

Petição:

- Direito pode ser exercido pelo titular ou representante legal;
- Encaminhamento ao **Encarregado**;
- Resposta gratuita em até 15 dias, prorrogável por igual período;
- Veda-se requerimentos anônimos ou de terceiros não autorizados.

Deverá ser empregado o formulário padronizado disponível no site:

https://fundacaorioaguas.prefeitura.rio/programa-de-governanca-em-privacidade-e-protecao-de-dados-pessoais/

Tramitação de documentos

- **Para outros poderes/entes públicos**: deve seguir os parâmetros de compartilhamento.
- **Entre órgãos municipais**: a tramitação física ou digital é atividade administrativa legítima e necessária para a execução de atribuições públicas.

Tratamento de Resposta a Incidentes

Identificação e análise inicial

Recebida a notificação de possível incidente de segurança, o Encarregado, deverá imediatamente identificar os dados vinculados ao episódio, analisando cautelosa e detalhadamente todas as informações disponíveis, a fim de:

1. Confirmar se os dados integram bases sob responsabilidade da Fundação Rio-Águas.
2. Verificar se os dados em questão se enquadram como **dados pessoais**, nos termos do art. 5º, I, da LGPD.

3. Identificar se houve algum tipo de tratamento de dados pessoais capaz de acarretar risco ou dano relevante aos titulares, como:
    - **Acesso não autorizado** a sistemas corporativos de gestão administrativa, financeira ou operacional;
    - **Indisponibilidade prolongada** de sistemas de cadastro ou gestão de serviços por incidente de sequestro de dados (*ransomware*), comprometendo a continuidade das atividades institucionais;
    - **Perda, furto ou extravio** de documentos físicos ou dispositivos de armazenamento contendo dados pessoais de servidores, fornecedores, usuários de serviços públicos ou cidadãos atendidos pela Fundação.

A simples existência de vulnerabilidade em sistemas não configura, por si só, incidente de segurança. Contudo, a exploração dessa vulnerabilidade pode resultar em evento de risco relevante.

Avaliação do incidente

Confirmada a ocorrência, o Comitê de Privacidade e Proteção de Dados Pessoais deve iniciar a avaliação de gravidade dos dados comprometidos.

Essa análise deve contemplar:

- O contexto da atividade de tratamento.
- A classificação do incidente, a exemplo de:
    - **Conteúdo abusivo** (spam, assédio);
    - **Código malicioso** (vírus, trojan, spyware);
    - **Tentativas de intrusão** ou exploração de vulnerabilidades;
    - **Intrusão confirmada** em sistemas ou contas;
    - **Indisponibilidade de serviço** (negação de serviço, sabotagem);
    - **Uso indevido de informação** (alteração ou acesso não autorizado);
    - **Fraudes** ou falsificação de identidade;
    - **Outros eventos categorizáveis**.
- As categorias e quantidades de titulares afetados.
- A natureza e volume dos dados pessoais comprometidos.
- Potenciais danos materiais, morais e reputacionais aos titulares.
- Grau de proteção existente (como criptografia ou pseudonimização).
- Medidas de contenção ou mitigação já aplicadas.

Com base nesses critérios, a classificação de criticidade do incidente seguirá os níveis:

- **Alta (impacto grave):** comprometimento de sistemas críticos ou de grande volume de dados pessoais, com impacto direto sobre as atividades institucionais e riscos elevados aos titulares.
- **Média (impacto significativo):** afeta sistemas ou dados pessoais sensíveis, mas sem paralisação total das atividades da Fundação.

- **Baixa (impacto mínimo):** incidentes pontuais, sem comprometimento crítico ou com alcance restrito.

Parecer técnico

A equipe responsável deverá elaborar um **Parecer técnico**, que:

- Documente as evidências técnicas do incidente;
- Aponte falhas de segurança que possibilitaram ou contribuíram para o evento;
- Recomende ações corretivas e de prevenção;
- Registre as providências adotadas.

Esse relatório é fundamental para aprimorar as práticas de governança em privacidade da Fundação Rio-Águas.

Comunicação do incidente

Conforme a LGPD e o Decreto Rio nº 54.984/2024:

- O **Encarregado da Fundação Rio-Águas** deverá notificar, quando necessário, o **Encarregado Geral do Município,** a **Autoridade Nacional de Proteção de Dados (ANPD)**, e os **titulares afetados**, em até **3 dias úteis** da ciência do fato.
- A **Assessoria de Comunicação da Prefeitura**, em conjunto com a Fundação, poderá ser acionada para elaboração de **plano de comunicação institucional**, que inclua:
    - Notas técnicas;
    - Comunicados oficiais a titulares;
    - Eventual divulgação à imprensa.

Relatório final e lições aprendidas

Encerrada a resposta ao incidente, será elaborado relatório circunstanciado contendo:

- A avaliação do processo de resposta;
- A eficácia das medidas adotadas;
- As falhas e recursos insuficientes identificados;
- As lições aprendidas e recomendações de melhoria;
- As ações a serem implementadas no **Programa de Governança em Privacidade e Proteção de Dados Pessoais da Fundação Rio-Águas**.

Fluxograma