TRÊS RIOS
PREFEITURA
EDIÇÃO EXTRAORDINÁRIA

BIO Boletim Informativo Oficial do Município de Três Rios

*Formato Eletrônico regulamentado pela Lei nº 4.498, de 18 de maio de 2018.*

www.tresrios.rj.gov.br - Ano LVI - 11 de Setembro de 2025 - Edição OnLine - Nº 2.185



ERRATA

Fica retificada a publicação do extrato de Termo de Homologação, Processo nº 10502/2025, Pregão Eletrônico nº 90074/2025, referente a Prestação do serviço de locação, montagem e desmontagem de estruturas físicas para a execução da Semana da Pátria da Secretaria de Educação, no que segue: Centro, Vila Isabel e Bemposta, publicada no Boletim Informativo Oficial nº 2.184, página 11, de 10/09/2025, onde se lê: “OBJETO: Aquisição de equipamentos de dados, equipamentos médicos, mobiliários e eletrodomésticos e veículos, destinados à reestruturação das Unidades Básicas de Saúde.”, leia-se: “OBJETO: Prestação do serviço de locação, montagem e desmontagem de estruturas físicas para a execução da Semana da Pátria da Secretaria de Educação, no que segue: Centro, Vila Isabel e Bemposta”.

Mantem-se inalteradas as demais condições do Extrato de Termo de Homologação.

**PREFEITURA DO MUNICÍPIO**
**DE TRÊS RIOS/RJ**

# DECRETO Nº 7.473, DE 9 DE SETEMBRO DE 2025.

**Aprova o Plano de Resposta a Incidentes de Segurança com Dados Pessoais, e dá outras providências.**

O **PREFEITO DO MUNICÍPIO DE TRÊS RIOS**, no uso de suas atribuições legais, especialmente das que lhe são conferidas pelo inciso I, do art. 43, e inciso II, do art. 135, da Lei Orgânica do Município e;

**CONSIDERANDO** o disposto no Processo Administrativo nº 3.205/2025;

**CONSIDERANDO** o Acórdão nº 003931/2025-PLENV constante do Processo TCE/RJ nº 217899-0/2024

**DECRETA:**

**Art. 1º** Fica aprovado, na forma do Anexo Único que passa a fazer parte integrante deste Decreto, o Plano de Resposta a Incidentes de Segurança com Dados Pessoais.

**Art. 2º** Este Decreto entra em vigor na data de sua publicação, revogando-se todas as disposições em contrário.

Três Rios, 9 de setembro de 2025.

***Jonas Mascarenhas Macedo***
Prefeito


Praça São Sebastião, 81, Centro, Três Rios/RJ – Telefone: +55 24 2252-0266
www.tresrios.rj.gov.br – gabinete@tresrios.rj.gov.br

# PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA COM DADOS PESSOAIS

Secretaria de
TECNOLOGIA DA INFORMAÇÃO
E PROTEÇÃO DE DADOS

TRÊS RIOS
PREFEITURA

EQUIPE TÉCNICA

# COMISSÃO GESTORA E DE REGULAMENTAÇÃO, MONITORAMENTO E ACOMPANHAMENTO PARA IMPLEMENTAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS

**Guilherme Medeiros da Silva**
Presidente

**Oscar Ferreira Salgueiro de Castro**
Vice-Presidente

**Euler dos Santos Souza**
Secretário e DPO

**Membros:**
Edimilson Guimarães de Oliveira Filho
Handerson Luiz Saggioro Ferreira
Fernando Rodrigues Barbosa
Márcio Luís dos Santos Pereira
Márcio Mesquita Malafaia
Pedro Henrique Brasil
Jaider dos Santos Costa

**SUB DPO**
Maílson dos Santos Francisco

EDIÇÃO - JULHO 2025

2

Secretaria de TECNOLOGIA DA INFORMAÇÃO E PROTEÇÃO DE DADOS
TRÊS RIOS PREFEITURA

# SUMÁRIO

# INTRODUÇÃO

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, estabeleceu um novo marco regulatório para o tratamento de dados pessoais no Brasil, impondo a todos os agentes de tratamento, incluindo o Poder Público, o dever de adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais.

Nesse contexto, a Prefeitura Municipal de Três Rios, ciente de sua responsabilidade na proteção das informações dos cidadãos e de seus servidores, reconhece que incidentes de segurança são uma realidade possível e que a preparação para responder a eles de forma ágil e eficaz é fundamental para mitigar riscos e danos.

Este Plano de Resposta a Incidentes de Segurança com Dados Pessoais (PRI) foi elaborado com o propósito de estabelecer uma visão clara e objetiva sobre as ações a serem tomadas em caso de uma situação de emergência ou evento que possa comprometer a segurança dos dados pessoais tratados pela Prefeitura.

O documento dispõe sobre as medidas que devem ser adotadas para identificar, analisar, conter e responder a incidentes como vazamentos, acessos não autorizados ou ataques cibernéticos. Seu objetivo é viabilizar uma comunicação apropriada e tempestiva à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares dos dados, quando necessário, em estrita conformidade com o Art. 48 da LGPD.

Este plano serve como um guia para todos os setores da Prefeitura, garantindo que a resposta a incidentes seja documentada, formalizada e coordenada, preservando a confiança da sociedade nos serviços públicos prestados e fortalecendo a cultura de segurança da informação e privacidade no âmbito municipal.

# OBJETIVOS

## OBJETIVO GERAL

Orientar os setores da Prefeitura de Três Rios bem como responder às situações de emergência com incidentes de segurança da informação, de forma documentada, formalizada, rápida e confiável, ao passo em que resguarde as evidências que possam ajudar a prevenir novos incidentes e a atender às exigências legais de comunicação e transparência.

## OBJETIVOS ESPECÍFICOS

- Conferir clareza sobre o fluxo de procedimentos adequados e responsáveis no caso de incidentes;
- Adequar as condutas internas às diretrizes estabelecidas pela LGPD;
- Preservar a reputação e imagem da Prefeitura de Três Rios;
- Assegurar respostas rápidas, efetivas e coordenadas para evitar maiores danos ao titular de dados e a Prefeitura;
- Quantificar e monitorar desempenho;
- Evoluir continuamente com as lições aprendidas;
- Tornar a Prefeitura de Três Rios referência em proteção de dados pessoais e segurança da informação.

# TERMOS E DEFINIÇÕES

Para auxílio na leitura deste plano, serão adotadas as seguintes definições:

**Agente de tratamento:** aqueles que podem ter alguma ação no tratamento de um incidente que coloque em risco a segurança dos dados pessoais.

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

**Operador:** pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

**Encarregado pelo Tratamento de Dados Pessoais:** é a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

**Autoridade Nacional de Proteção de Dados (ANPD):** entidade responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional, conforme as atribuições descritas no art. 55-J da LGPD e no Decreto nº 10.474 de 26 de agosto de 2020.

**Dado pessoal:** é toda informação relacionada à pessoa natural identificada ou identificável.

**Inventário de Dados Pessoais (IDP):** representa um artefato primordial para documentar o tratamento de dados pessoais realizados pela instituição.

**Incidente:** evento, ação ou omissão que tenha permitido ou possa vir a permitir acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou, ainda, apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação.

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

**Incidente de segurança:** qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores.

**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.

**Lei Geral de Proteção de Dados Pessoais (LGPD):** Lei no 13.709, de 14 de agosto de 2018, cujo objetivo é proteger os direitos fundamentais de privacidade e de liberdade de cada indivíduo.

**Relatório final:** documento que contém todas as evidências e ações realizadas para tratamento do incidente e que deve ser emitido ao final das tratativas.

**Relatório de Impacto a Proteção de Dados (RIPD):** documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que tem o potencial de gerar riscos às liberdades civis e aos direitos fundamentais dos titulares, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

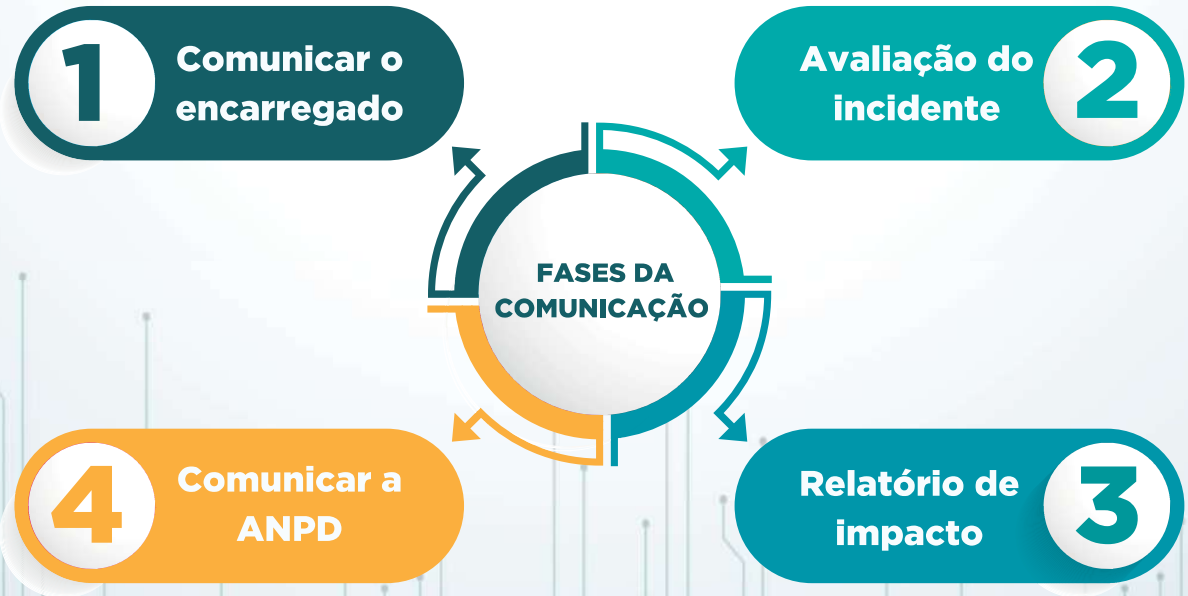
# INCIDENTES DE SEGURANÇA COM DADOS PESSOAIS

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

Evitar esses eventos, passa pela necessidade de adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito, de acordo com as regras de boas práticas de governança para o tratamento de dados pessoais.

Em caso de suspeita de incidente que coloque em risco a segurança de dados pessoais, devem ser realizados alguns procedimentos específicos.

A figura abaixo detalha de maneira simplificada este processo:



## 1 Comunicar o encarregado

A notificação de eventual vazamento de dados pessoais pelos colaboradores internos (servidores, comissionados, estagiários e terceirizados) deverá em regra ser realizada via e-mail para dpo@tresrios.rj.gov.br, o mais rápido possível, para as providências previstas na LGPD e no portal da ANPD sobre comunicação de incidentes de segurança.

## Avaliação do incidente 2

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

a. Qual vulnerabilidade foi explorada no evento, abrangendo situações como: acesso indevido aos dados pessoais; roubo de dados; ataques cibernéticos; erros de programação de aplicativos e sistemas internos; engenharia social; descartes indevidos; repasse de dados pessoais; roubo, venda e utilização de dados tutelados pela entidade; comprometimento de senhas de acesso; e outras.

b. Fonte dos dados pessoais: meio pelo qual foram obtidos os dados pessoais, tais como preenchimento de formulário eletrônico ou não eletrônico por parte do titular, API, uso compartilhado de dados, XML e cookies.

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

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

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

f. Avaliação do impacto no serviço: avaliar os impactos que o incidente pode gerar a entidade como perda de confiabilidade do cidadão, ações judiciais, dano à imagem

da instituição em âmbito nacional e internacional, prejuízo à entidade em contratos com fornecedores e clientes, e impacto total ou parcial nas atividades desenvolvidas pela entidade.

Devem ser preservados o máximo de evidências do incidente e de todas as medidas adotadas a partir da sua ciência, a fim de que se demonstre, para eventuais autoridades que posteriormente vierem a apurar os fatos, toda a cadeia de diligências realizadas para entendimento do evento e mitigação dos seus efeitos.

Nesse cenário, todos os passos devem ser devidamente documentados, desde o momento inicial de atuação até a contenção e os efeitos. Isso inclui, mas não se limita a:

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

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

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

d. Atas das reuniões relevantes.

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

## Relatório de impacto 3

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

- Para tratamento de dados pessoais realizados para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (exceções previstas pelo inciso art. 4º, inciso III da LGPD);
- Quando houver infração da LGPD em decorrência do tratamento de dados pessoais por órgãos públicos (arts. 31 e 32 da LGPD, combinados); e

A qualquer momento, sob determinação da ANPD (art. 38)

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

## 4 Comunicar a ANPD

Conforme o Art. 48 da LGPD, se o incidente puder acarretar risco ou dano relevante aos titulares, o Controlador (a Prefeitura) deve comunicar a Autoridade Nacional de Proteção de Dados (ANPD).

A comunicação à ANPD deve ser feita no prazo de 2 dias úteis a contar da data de ciência do incidente.

Nessas tarefas, a LGPD e os demais normativos infralegais vigentes sobre proteção de dados pessoais deverão ser sempre consultados e utilizados como balizas.

A autoridade nacional de proteção de dados disponibiliza, em seu site, um formulário modelo para notificação de incidentes de segurança com proteção de dados.

O formulário pode ser acessado no site da ANPD ou através do seguinte link:

**https://l1nk.dev/p7Jy9**

### O que e como comunicar aos titulares de dados?

A comunicação do incidente aos titulares deve ser feita em linguagem clara e simplificada e mencionar, no que couber, os elementos previstos no §1º do Art. 48 da LGPD, tais como: A descrição geral do incidente e a data da ocorrência; A natureza dos dados pessoais afetados e os riscos relacionados ao incidente; As medidas tomadas e recomendadas para mitigar os efeitos do incidente; O contato do encarregado ou o ponto de contato para que os titulares obtenham informações a respeito do incidente; Outras informações que possam auxiliar os titulares a prevenir possíveis danos.

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

# IMPORTANTE

importante que todas as informações e evidências coletadas e as ações do processo de tratamento de incidente de segurança à proteção de dados sejam documentadas, de modo a possibilitar a elaboração de um relatório final do incidente. Este documento deve:

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

**b** - estar disponível para consulta em caso de atualização do relatório de impacto a proteção de dados (RIPD).

A ANPD pode solicitar o mencionado relatório para análise, com o propósito de:

- Avaliar as ações tomadas durante um incidente em que dados pessoais tenham sido expostos ou comprometidos;
- Publicar e atualizar normas referentes à proteção de dados;
- Cumprir o princípio da responsabilização (art. 6º, inciso X da LGPD);
- Utilizá-lo como subsídio para eventuais questionamentos, facilitando a comprovação de conformidade.

# TRÊS RIOS
## PREFEITURA

## Secretaria de TECNOLOGIA DA INFORMAÇÃO E PROTEÇÃO DE DADOS

ASSINADO DIGITALMENTE
JONAS MASCARENHAS MACEDO
A conformidade com a assinatura pode ser verificada em:
http://serpro.gov.br/assinador-digital
SERPRO

## COMISSÃO GESTORA E DE REGULAMENTAÇÃO, MONITORAMENTO E ACOMPANHAMENTO PARA IMPLEMENTAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS