# POLÍTICA DE GESTÃO DE INCIDENTES



Rua Rio de Janeiro, 600 - Sala 401 | 30160-911 | Centro | Belo Horizonte - MG

## Histórico de revisões

| Histórico de Versões Data | Versão | Descrição | Autor |
|---|---|---|---|
| 25/05/2023 | 1.0 | Criação da Política de Gestão de Incidentes | Deysiane C. S. Santos |
| 27/05/2023 | Rev. 1.0 | Revisão desta política | Giovanni M. Patrício |
| 09/04/2023 | Rev. 2.0 | Política Revisada | Deysiane C. S. Santos |
| 09/04/2024 | Rev. 2.0 | Política Revisada | Giovanni M. Patrício |
| 27/02/2025 | Rev. 3.0 | Política Revisada | Giovanni M. Patrício |



Rua Rio de Janeiro, 600 - Sala 401 | 30160-911 | Centro | Belo Horizonte - MG

| | |
|---|---|
| **Responsável:** | Deysiane C. S. Santos |
| **Revisado por:** | Giovanni M. Patrício |
| **Aprovação TI:** | Eric V. R. Cândido |
| **Aprovação Diretoria:** | Karla J. Teodoro |
| **Políticas relacionadas** | Política Geral de Segurança da Informação; Política de Gerenciamento de Vulnerabilidades. |
| **Localização de armazenamento** | Está política está armazenada no servidor de arquivos da Única Promotora; no servidor em Nuvem da Statera Tecnologia da Informação e no Sistema de gestão de crédito consignado, **STORM**. |
| **Data da aprovação** | 25/05/2023 |
| **Data de revisão** | 27/02/2025 |
| **Versão** | V.1 |



Rua Rio de Janeiro, 600 - Sala 401 | 30160-911 | Centro | Belo Horizonte - MG

# Sumário





Rua Rio de Janeiro, 600 - Sala 401 | 30160-911 | Centro | Belo Horizonte - MG

## Introdução

A gestão de incidentes envolve a aplicação de procedimentos claramente estabelecidos, que guiam a equipe na resolução de incidentes. Esta política detalha um processo para responder a emergências ou eventos de risco que possam afetar a estrutura e a infraestrutura da *Única Promotora*. Ela assegura a conformidade com as exigências legais de comunicação e transparência, visando à segurança da informação e à privacidade

## Objetivo

O objetivo desta política é oferecer uma visão abrangente do processo de gestão de incidentes, delineando seu escopo, diretrizes, benefícios, papéis e responsabilidades. Ela orienta a execução do processo de maneira adequada, minimizando os impactos sobre o negócio. Esta política se baseia nas melhores práticas da ITIL (Information Technology Infrastructure Library).

## Abrangência

Esta política se aplica a todo o corpo de colaboradores da *Única Promotora*, seja: funcionários, parceiros, substabelecidos, terceirizados ou pessoas que direta ou indiretamente utilizam os sistemas, infraestrutura ou informações da empresa.

## Compliance

1. Manter esta Política atualizada, submetendo sugestões de modificações em decorrência de alterações legais, normativas e de condutas;
2. Disseminar métodos para identificação, avaliação, monitoramento, controle e mitigação de riscos;
3. Disseminar a cultura de Riscos, Compliance e controles internos, promovendo a conscientização e enfatizando o comprometimento, engajamento de cada colaborador na implantação do Programa de Compliance para garanti de sucesso do mesmo.

## Lei Geral de Proteção de Dados (LGPD)

Esta Política está em conformidade com a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), respeitando os princípios definidos por ela, assim como disseminando a cultura de proteção e privacidade a toda organização.

## Confidencialidade

Está política deverá ser amplamente divulgada dentro da *Única Promotora* e disponibilizada a todos os colaboradores, parceiros e Substabelecidos, assim como as partes interessadas do processo.

Cabe a diretoria da *Única Promotora*, juntamente com seus gestores de área, e a equipe de tecnologia definir o nível de acesso as informações contidas neste documento, garantindo assim a confidencialidade e disponibilidade das informações somente as pessoas necessárias.



Rua Rio de Janeiro, 600 - Sala 401 | 30160-911 | Centro | Belo Horizonte - MG

# Incidentes de Segurança da Informação

São considerados exemplos de incidentes de Segurança da Informação ou Fragilidades em Sistemas ou serviços que devem ser notificados:

I. Código malicioso;
II. Negação de serviço (DDoS);
III. Erros resultantes de dados incompletos ou inconsistentes;
IV. Violações de confidencialidade e integridade das informações;
V. Indisponibilidade das informações;
VI. Uso impróprio de sistemas de informação;
VII. Perda de serviço, equipamento ou recursos;
VIII. Erros humanos;
IX. Violações da Política Geral de Segurança da Informação da ÚNICA PROMOTORA;
X. Violações de procedimentos de segurança física;
XI. Mudanças não controladas ou não previstas de sistemas;
XII. Mau funcionamento de softwares e hardwares;
XIII. Violações de acesso;
XIV. Tentativas de fraude;
XV. Tentativas de invasão física ou lógica;
XVI. Sinistros envolvendo ativos de informação;
XVII. Vulnerabilidades em software ou aplicativos.

# Incidentes envolvendo o tratamento de dados pessoais

São considerados exemplos de incidentes envolvendo o tratamento de dados pessoais e corporativos que devem ser notificados:

I. O vazamento de dados pessoais;
II. A suspeita de vazamento de dados pessoais;
III. A invasão ou tentativa de invasão do banco de dados;
IV. O compartilhamento ou cópia indevidos de dados pessoais;
V. Violações da Política Geral de Segurança da Informação envolvendo dados pessoais e corporativos.

# Plano de Resposta

## Atores

- Notificador - pessoa ou sistema de monitoração que notifica incidente.
- TRI - Time de Resposta a Incidentes, definido na preparação prévia.
- Acionadores do TRI - grupo que receberá notificações de incidentes em primeira mão para triagem, estruturado em níveis distintos para viabilizar a importante cobertura 24 horas.



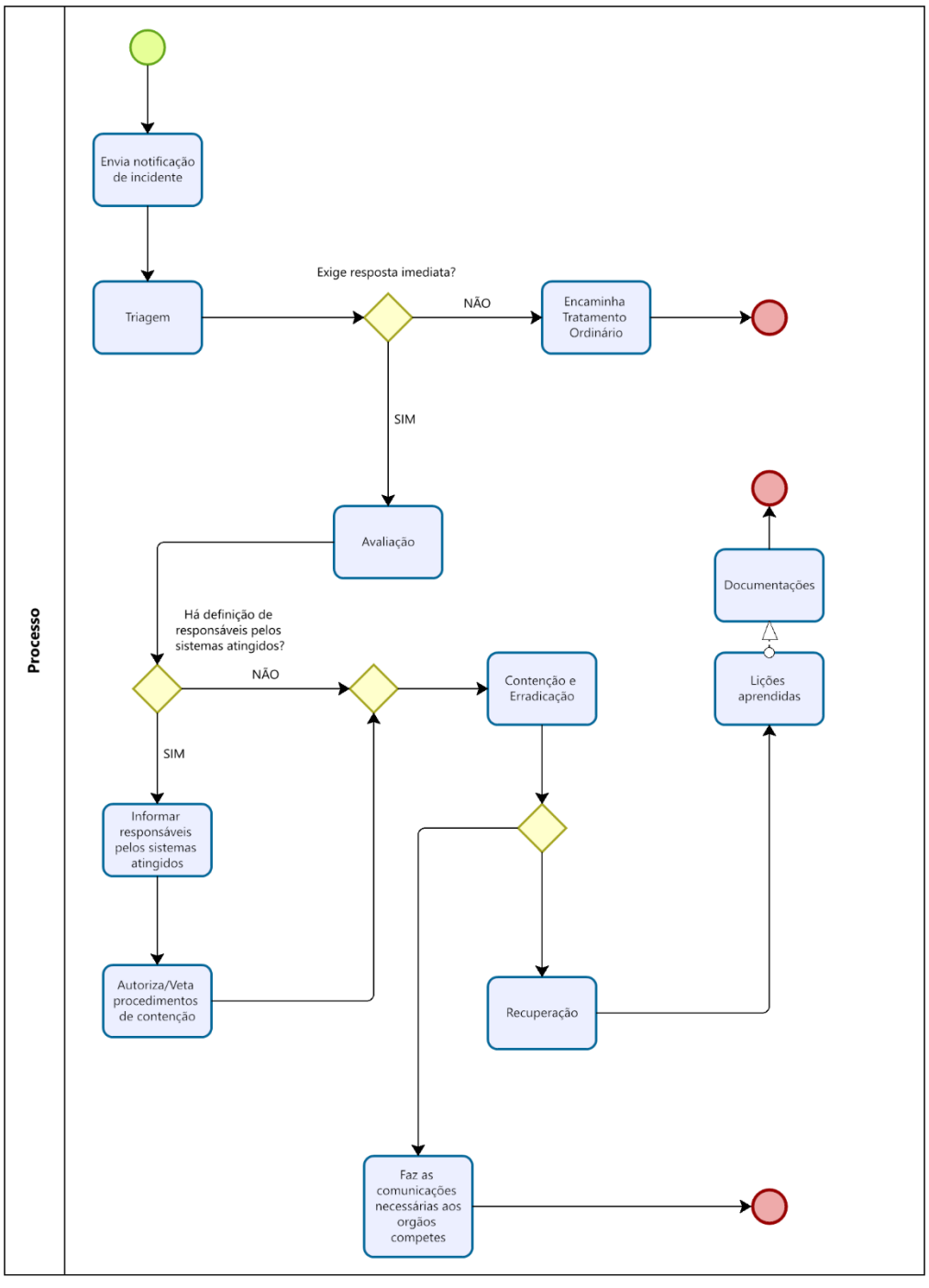
Rua Rio de Janeiro, 600 - Sala 401 | 30160-911 | Centro | Belo Horizonte - MG

- Responsável por Sistema ou Controlador de Sistema, indicado que deve ser contatado e pode autorizar ou vetar procedimentos de emergência. Deve estar documentado na CMDB, inclusive forma de contato para emergências
- Equipe de Segurança da Informação
- Encarregado pelo Tratamento de Dados Pessoais (DPO) - membro especial do TRI, responsável por encaminhar comunicações formais em incidentes envolvendo vazamentos de dados pessoais.
- Desenvolvedores/Operadores/Fornecedores dos sistemas - atuam no desenvolvimento de solução e instalação destes.



Rua Rio de Janeiro, 600 - Sala 401 | 30160-911 | Centro | Belo Horizonte - MG

# Processo






Rua Rio de Janeiro, 600 - Sala 401 | 30160-911 | Centro | Belo Horizonte - MG

# Descrição do Processo

## Início

Um novo incidente pode ser relatado por uma pessoa externa ou interna à *Única Promotora*, ou por meio de um alarme de monitoramento, utilizando um dos mecanismos de comunicação estabelecidos. A notificação é então recebida pelo Acionador do TRI.

## Triagem

O Acionador do TRI deve realizar uma avaliação preliminar do incidente ou contatar imediatamente outro Acionador qualificado para fazer essa avaliação. Notificações nulas ou claramente improcedentes devem ser descartadas com os devidos cuidados.

Na avaliação preliminar, é necessário coletar informações sobre os sistemas supostamente afetados, avaliar sua criticidade, identificar danos aparentes e considerar o risco de agravamento da situação se não houver uma resposta imediata.

Conforme a avaliação preliminar, incidentes que não envolvam sistemas online e que claramente não apresentam riscos aumentados pela falta de ação imediata podem ser redirecionados para os trâmites regulares da Companhia. A Equipe de Segurança da Informação e o Encarregado pelo Tratamento de Dados Pessoais devem gerenciar esses casos, especialmente se envolverem dados pessoais.

Para incidentes que exigem resposta imediata ou uma avaliação mais detalhada, o TRI deve ser acionado para avançar para as próximas fases.

## Avaliação

Nesta fase deve ser iniciada uma avaliação mais detalhada do incidente. Deve-se procurar identificar a causa do incidente, endereços IP e credenciais envolvidas, transações e transferências de dados irregulares, métodos e vulnerabilidades exploradas, visando determinar ações para as demais fases.

Pode ser importante engajar especialistas dos sistemas afetados para colaborar e isso deve ser feito a critério do TRI a qualquer momento que julgar adequado e viável.

## Contenção e Erradicação

Caso estejam listados na CMDB, os responsáveis pelos sistemas afetados devem ser acionados conforme indicado na documentação. Esses responsáveis irão orientar e se manifestar sobre os procedimentos de contenção e erradicação.

O objetivo das medidas de contenção e erradicação é limitar os danos e isolar os sistemas afetados para evitar mais prejuízos. Conforme a necessidade e a autorização obtida, pode ser realizado o desligamento completo dos sistemas ou de funcionalidades específicas, além da colocação de avisos de indisponibilidade para manutenção. Sempre que possível, devem ser tomados cuidados para não



Rua Rio de Janeiro, 600 - Sala 401 | 30160-911 | Centro | Belo Horizonte - MG

comprometer evidências que possam ser usadas para identificar a autoria, a origem e o método utilizado para a violação de segurança.

Em caso de incidentes envolvendo máquinas virtuais, devem ser feitos snapshots dessas máquinas para análise posterior.

### Recuperação

Caso exista Plano de Continuidade de Negócio dos sistemas impactados, eles devem ser iniciados, conforme especificado.

A recuperação é o conjunto de medidas para restaurar os serviços completamente, mas pode ser feita de forma gradual, conforme viabilidade e decisão do responsável pelo sistema.

O TRI tem a responsabilidade de passar as informações que obteve para o desenvolvimento da solução e sua instalação.

Para a recuperação devem ser tomadas medidas identificadas na Avaliação, tais como restauração de backups, clonagem de máquinas virtuais, reinstalação de sistemas.

Pode ser necessário o desenvolvimento e instalação de atualizações de aplicação ou do Sistema Operacional, por isso esta fase pode ser prolongada, de acordo com a priorização dada.

### Lições Aprendidas

Com o incidente contido e sua resolução encaminhada, o TRI deve agendar e conduzir uma reunião de Lições Aprendidas, com convidados a seu critério, com o objetivo de discutir erros e dificuldades encontradas, propor melhorias para os sistemas e processos - inclusive deste Plano de Resposta a Incidentes.

As melhorias sugeridas na reunião, com o devido consenso, devem ser encaminhadas aos responsáveis para definição sobre a adoção.

### Documentação

O TRI deve documentar o incidente em base de conhecimentos apropriada, detalhando as informações obtidas, linha de tempo, atores envolvidos, evidencias, conclusões, decisões, autorizações e ações tomadas, inclusive as da reunião de lições aprendidas.

## Comunicações

Assim que possível, no caso de incidente com vazamento de dados pessoais, o Encarregado de Tratamento de Dados (DPO) deve avaliar e fazer as comunicações obrigatórias por Lei, As Instituições Financeiras que a Única Promotora trabalha, bem como a Agência Nacional de Proteção de dados (ANPD) e informar e subsidiar os Encarregados de Tratamento de Dados dos controladores do sistema.



Rua Rio de Janeiro, 600 - Sala 401 | 30160-911 | Centro | Belo Horizonte - MG

A Comunicação deve ser feita no prazo de 2 dias úteis, conforme definido pela Autoridade Nacional, e deverá mencionar, no mínimo:

- A descrição da natureza dos dados pessoais afetados;
- As informações sobre os titulares envolvidos;
- A indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
- Os riscos relacionados ao incidente;
- Os motivos da demora, no caso de a comunicação não ter sido imediata; e
- As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

Caso não seja possível fornecer todas as informações no momento da comunicação preliminar, informações adicionais poderão ser fornecidas posteriormente.

Para notificar as Instituições Financeiras, é enviado através do e-mail do Encarregado de Dados (DPO) uma Carta de Notificação de Violação de Dados para o e-mail do Encarregado de Dados (DPO) de cada IF.

Essas comunicações podem incluir agradecimentos ao notificador, informações para os titulares de dados, relatórios formais para a ANPD entre outros que julgar necessário.



Rua Rio de Janeiro, 600 - Sala 401 | 30160-911 | Centro | Belo Horizonte - MG