POLÍTICA DE GESTÃO DE INCIDENTES

(31) 3658-7000 Rua Bélgica, 360, Bairro Glória - Contagem/MG - 32340-030
www.staterati.com.br

Histórico de revisões

Data	Versão	Descrição	Autor
11/05/2022	1.0	Criação da Política de Gestão de Incidentes	Deysiane C. S. Santos
30/05/2023	Rev. 2.0	Realizado a revisão da política, sem nenhuma alteração.	Giovanni M. Patrício
01/04/2024	Rev. 3.0	Revisão realizada.	Deysiane C. S. Santos
01/04/2024	Rev. 3.0	Revisão realizada.	Giovanni M. Patrício
07/02/2025	Rev. 4.0	Revisão realizada.	Giovanni M. Patrício
24/02/2026	2.0	Alterado o prazo para comunicação de incidentes à ANPD conforme Resolução CD/ANPD Nº 15, Seção II	Deysiane C. S. Santos
27/02/2026	Rev. 5.0	Revisão realizada.	Giovanni M. Patrício

Responsável	Deysiane C. S. Santos
Revisão:	Giovanni M. Patrício
Aprovado por:	Eric V. R. Cândido
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 TokReal Promotora e no servidor em Nuvem da Statera Tecnologia da Informação.
Data da aprovação	11/05/2022
Data de revisão	27/02/2026
Versão	V.2

Sumário

Introdução

O processo de gestão de incidentes consiste na implementação de procedimentos bem definidos que conduzirão a equipe para a resolução de um incidente.

Esta política descreve um processo para responder às emergências, ou evento de risco que venham ocasionar em algum impacto a estrutura e infraestrutura da empresa, atendendo as exigências legais de comunicação e transparência para a segurança da informação e privacidade.

Objetivo

O objetivo desta política é fornecer uma visão sobre o processo de gestão de incidentes, apresentando o escopo do processo, diretrizes, seus benefícios, papéis e responsabilidades, orientando o funcionamento do processo de forma que seja tratado adequadamente, reduzindo ao máximo os impactos para o negócio.

Esta política é baseada nas melhores práticas da ITIL (Information Tecnhnology Infraestructure Library).

Abrangência

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

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 TokReal 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:

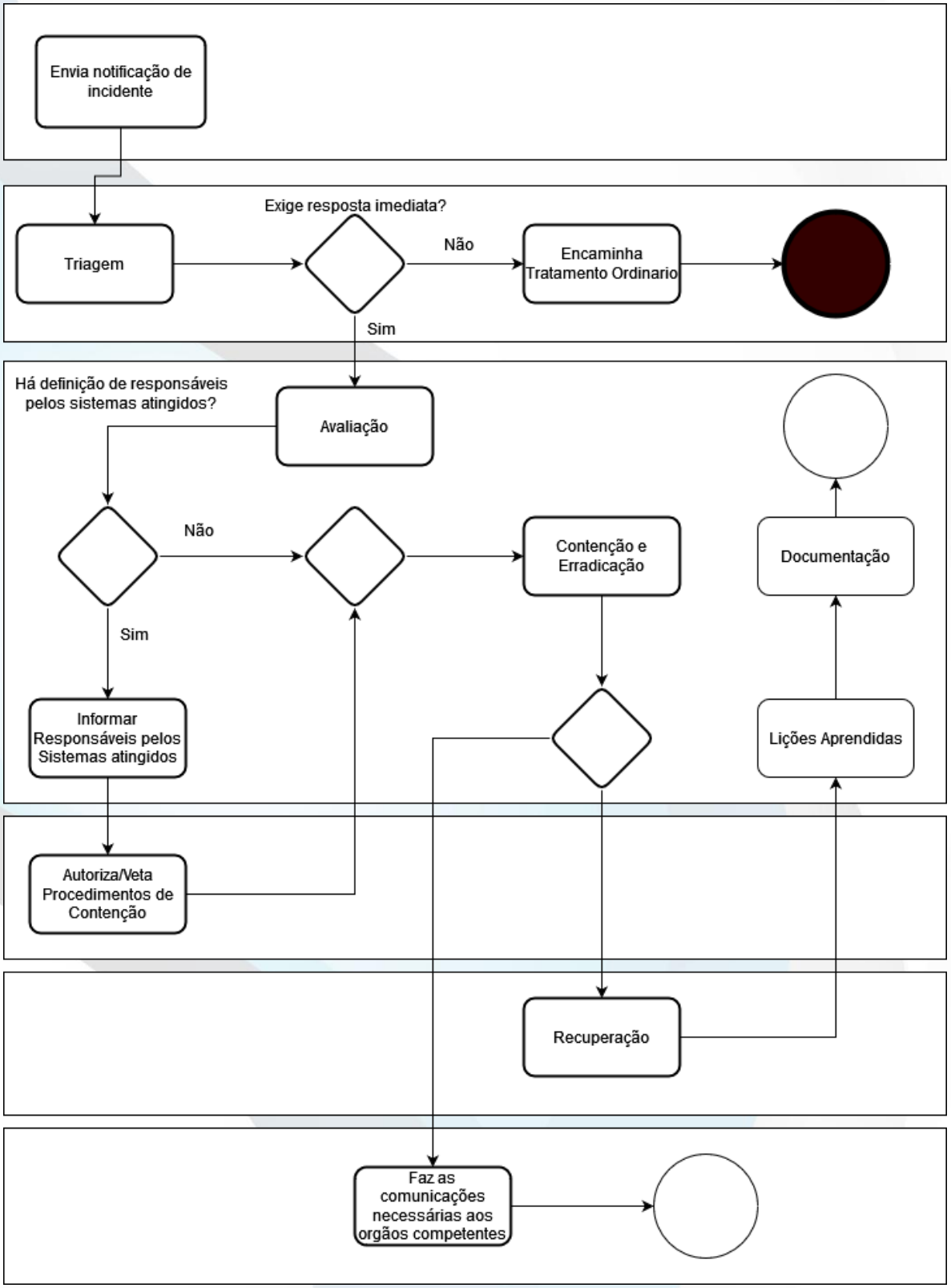
I. O vazamento de dados pessoais;
II. A suspeita de vazamento de dados pessoais;
III. A invasão ou tentativa de invasão do banco de dados;
IV. O compartilhamento ou cópia indevidos de dados pessoais;
V. Violações da Política Geral de Segurança da Informação envolvendo dados pessoais e corporativos.

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.
- 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.

Processo



Descrição do Processo

Início

Um novo incidente é notificado, por pessoa externa ou não a TokReal ou por alarme da monitoração, usando um dos mecanismos de comunicação definidos. Notificação é recebida pelo Acionador do TRI.

Triagem

O Acionador do TRI deve fazer a avaliação preliminar ou contatar imediatamente outro Acionador em condições de realizar a referida avaliação, descartando as notificações nulas ou claramente improcedentes, tomando os devidos cuidados.

Na avaliação preliminar, devem ser buscadas informações sobre os sistemas que foram alegadamente impactados, sua criticidade, quais os danos aparentes e o risco da situação se agravarem caso não haja resposta imediata.

Conforme a avaliação preliminar, incidentes que não envolvem sistemas online e que seguramente não apresentam riscos aumentados pela falta de ação imediata, podem ser reencaminhados para tramites regulares da Companhia pela Equipe de Segurança da Informação e Encarregado pelo Tratamento de Dados Pessoais, caso o incidente envolva dados pessoais.

Em caso de incidentes que exigem resposta imediata ou melhor avaliação, o TRI deve ser acionado e passamos às fases seguintes.

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 identificados na CMDB, devem ser acionados os responsáveis pelos sistemas impactados, conforme indicado na documentação, que irão orientar e se manifestar sobre os procedimentos de contenção e erradicação.

O objetivo das medidas de contenção e erradicação é limitar o dano e isolar os sistemas afetados para evitar mais danos. Aqui, conforme a necessidade e a autorização obtida será realizado o desligamento dos sistemas inteiros ou de funcionalidades especificas, colocação de avisos de indisponibilidade para manutenção, sempre que possível tomando cuidados para não impactar evidências que poderiam ser usadas para identificar autoria, origem e método usado para quebrar a segurança.

Em caso de incidente envolvendo máquinas virtuais, deve ser feito snapshots delas para posterior análise.

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 Tok Real 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.

A Comunicação deve ser feita no prazo de 3 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.