POLÍTICA DE GESTÃO DE INCIDENTES

Histórico de Versões Data	Versão	Descrição	Autor
14/04/2026	1.0	Criação da Política de Gestão de Incidentes	Henrique Nogueira Reys

Sumário

1. INTRODUÇÃO

A Zeni Digital reconhece a importância da segurança da informação e da proteção de dados pessoais no desenvolvimento de suas atividades. Nesse contexto, a empresa adota medidas destinadas à prevenção, identificação e tratamento adequado de incidentes de segurança que possam comprometer a integridade, confidencialidade ou disponibilidade de informações.

A presente Política de Gestão de Incidentes estabelece diretrizes para a identificação, registro, tratamento e comunicação de incidentes relacionados à segurança da informação e à proteção de dados pessoais no âmbito das atividades desenvolvidas pela plataforma Zeni Digital.

Esta política integra o conjunto de instrumentos de governança voltados à proteção de dados pessoais e à segurança da informação, sendo parte do compromisso institucional da organização com a transparência, a conformidade regulatória e a adoção de boas práticas de gestão de riscos.

2. OBJETIVO

Esta Política tem como objetivo estabelecer diretrizes e procedimentos para a identificação, registro, análise, tratamento e comunicação de incidentes de segurança da informação que possam impactar os sistemas, as informações ou os dados pessoais tratados pela Zeni Digital.

Busca-se, por meio desta política, reduzir riscos operacionais, proteger os dados pessoais tratados pela plataforma e assegurar que eventuais incidentes sejam tratados de maneira estruturada, transparente e proporcional ao risco envolvido.

3. CONCEITO DE INCIDENTE DE SEGURANÇA

Para fins desta Política, considera-se incidente de segurança qualquer evento que possa comprometer a confidencialidade, integridade ou disponibilidade de informações ou dados pessoais tratados pela Zeni Digital.

Podem ser considerados incidentes de segurança, entre outras situações:

1) acesso não autorizado a sistemas ou bases de dados
2) vazamento ou exposição indevida de informações
3) falhas de segurança em sistemas tecnológicos
4) perda ou indisponibilidade de dados
5) falhas operacionais que resultem em risco à proteção de dados pessoais

A caracterização do incidente será realizada a partir da análise do evento e de seu potencial impacto sobre os sistemas e informações da organização.

4. IDENTIFICAÇÃO, REGISTRO E CLASSIFICAÇÃO DE INCIDENTES

Sempre que identificado um possível incidente de segurança, o evento deverá ser registrado internamente para análise e tratamento adequado.

O registro do incidente deverá conter, sempre que possível:

a) data e horário da ocorrência ou identificação do evento
b) descrição do incidente identificado
c) sistemas ou dados potencialmente afetados
d) medidas iniciais adotadas
e) responsáveis pela análise e tratamento do caso

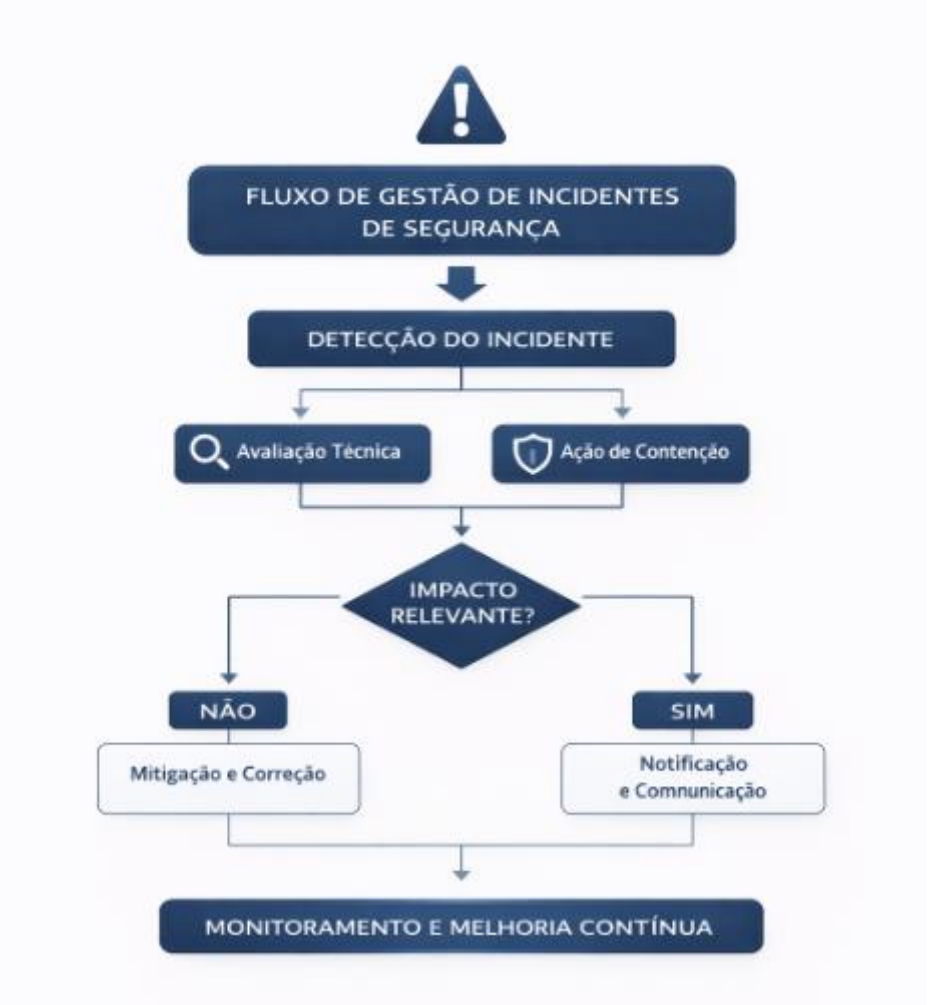
A Zeni Digital manterá registro interno das ocorrências identificadas, permitindo a manutenção de histórico de incidentes e a melhoria contínua de seus mecanismos de prevenção e resposta.

Os incidentes poderão ser classificados conforme sua natureza e impacto potencial, podendo envolver falhas técnicas, acessos indevidos, exposição de dados, indisponibilidade de sistemas ou qualquer evento que represente risco relevante à segurança da informação.

5. FLUXO DE TRATAMENTO DE INCIDENTES

O tratamento de incidentes seguirá fluxo estruturado de identificação, análise, contenção, comunicação e monitoramento.

Esse fluxo tem como objetivo garantir que os eventos identificados sejam avaliados de forma organizada e que as medidas adequadas sejam adotadas conforme a natureza e o impacto do incidente.



6. RESPOSTA E CONTENÇÃO DE INCIDENTES

Uma vez identificado um incidente de segurança, deverão ser adotadas medidas proporcionais à natureza do evento, com o objetivo de interromper ou mitigar seus efeitos e evitar a ampliação dos danos.

As ações de resposta poderão envolver análise técnica do incidente, isolamento de sistemas potencialmente comprometidos, correção de vulnerabilidades identificadas, restauração de serviços e adoção de medidas preventivas destinadas a evitar recorrência do evento.

A organização buscará atuar de forma diligente e tempestiva para restabelecer a normalidade de suas operações e preservar a segurança das informações tratadas.

7. COMUNICAÇÃO DE INCIDENTES

Quando um incidente envolver risco relevante aos titulares de dados pessoais, poderão ser adotadas medidas de comunicação adequadas, observando-se as disposições da legislação aplicável.

Nessas situações, poderá ser realizada comunicação aos titulares potencialmente afetados e, quando necessário, à Autoridade Nacional de Proteção de Dados – ANPD.

A comunicação será realizada de forma transparente e com informações suficientes para permitir a compreensão do incidente e das medidas adotadas pela organização.

8. GOVERNANÇA E RESPONSABILIDADES

A gestão de incidentes de segurança da informação envolve a atuação coordenada das áreas responsáveis pela tecnologia da informação, gestão operacional e jurídico/compliance.

Essas áreas são responsáveis por avaliar os eventos identificados, definir medidas de resposta e assegurar que os incidentes sejam tratados de forma adequada e em conformidade com a legislação aplicável.

Embora a organização ainda não possua Encarregado de Proteção de Dados formalmente designado, compromete-se a estruturar mecanismos adequados de governança relacionados à proteção de dados pessoais e, conforme a evolução de suas atividades, poderá designar responsável específico para essa função.

9. CANAL DE REPORTE DE INCIDENTES

A Zeni Digital incentiva que eventuais incidentes de segurança da informação ou situações que possam representar risco à proteção de dados pessoais sejam comunicados de forma imediata, a fim de permitir a rápida avaliação e adoção das medidas necessárias para mitigação de riscos.

Colaboradores, prestadores de serviço, parceiros ou quaisquer pessoas que identifiquem eventos que possam caracterizar incidente de segurança, falha operacional relevante ou possível exposição de informações deverão comunicar o fato por meio dos canais institucionais da organização.

Para esse fim, a Zeni Digital disponibiliza canal específico para comunicação de ocorrências relacionadas à segurança da informação e proteção de dados pessoais, podendo as comunicações serem encaminhadas para o seguinte endereço eletrônico: **privacidade@zeni.com.br**

As comunicações recebidas por meio desse canal serão analisadas pelas áreas responsáveis, que adotarão as providências necessárias para avaliação do evento, registro do incidente e eventual implementação das medidas de contenção, mitigação ou correção aplicáveis.

A utilização desse canal contribui para o fortalecimento dos mecanismos internos de segurança da informação e para a melhoria contínua das práticas de proteção de dados adotadas pela organização.

10. APRIMORAMENTO CONTÍNUO

Após o tratamento de incidentes de segurança, poderão ser avaliadas medidas adicionais destinadas ao aprimoramento contínuo dos controles de segurança, dos processos internos e das práticas de proteção de dados pessoais adotadas pela organização.

Essa avaliação busca reduzir a probabilidade de ocorrência de eventos semelhantes e fortalecer continuamente os mecanismos de governança relacionados à segurança da informação.

11. DISPOSIÇÕES FINAIS

Esta Política integra o conjunto de documentos institucionais relacionados à proteção de dados pessoais e à segurança da informação adotados pela Zeni Digital.

O documento poderá ser revisado e atualizado periodicamente, a fim de refletir mudanças nas práticas operacionais da organização, avanços tecnológicos ou alterações na legislação aplicável.

A revisão periódica desta política tem como finalidade assegurar a melhoria contínua das práticas de segurança da informação e da governança relacionada à proteção de dados pessoais.