Políticas e Normas
Resposta a Incidentes

ASSUNTO: GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS PESSOAIS		
VERSÃO: 5.0	**DATA DE PUBLICAÇÃO:** 16 DE JULHO DE 2026	**REVISÃO:** ANUAL
AUTOR: EMBRASI GOVERNANCA E C. TECNOLOGICA		
INSTITUIÇÃO: SGM CONSULTORES ASSOCIADOS LTDA		**CNPJ:** 00.306.499/0001-60

Política de Resposta a Incidentes de Segurança da Informação

Sumário

Políticas e Normas
Resposta a Incidentes

ASSUNTO: GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS PESSOAIS		
VERSÃO: 5.0	**DATA DE PUBLICAÇÃO:** 16 DE JULHO DE 2026	**REVISÃO:** ANUAL
AUTOR: EMBRASI GOVERNANCA E C. TECNOLOGICA		
INSTITUIÇÃO: SGM CONSULTORES ASSOCIADOS LTDA		**CNPJ:** 00.306.499/0001-60

Resposta a Incidentes de Segurança da Informação

1. Objetivo

Esta Política estabelece as diretrizes, responsabilidades e procedimentos institucionais para identificação, análise, contenção, tratamento, comunicação e registro de incidentes de segurança da informação no âmbito da SGM. Este documento deve ser interpretado de forma integrada à Política de Segurança da Informação, à Política de Privacidade e Proteção de Dados Pessoais, às Diretrizes Complementares de Privacidade, à Política de Terceirização e à Política de Auditoria Interna, constituindo elemento central do sistema de governança de riscos e de continuidade operacional.

2. Escopo e Abrangência

Esta Política aplica-se a todos os colaboradores, administradores, estagiários, prestadores de serviços, fornecedores e terceiros autorizados que utilizem, acessem ou administrem recursos tecnológicos, sistemas, informações ou dados pessoais sob responsabilidade da SGM. Você é responsável por observar integralmente as disposições aqui estabelecidas e por cooperar com as ações de resposta sempre que houver suspeita ou confirmação de incidente.

3. Conceito de Incidente de Segurança da Informação

Considera-se incidente de segurança da informação qualquer evento confirmado ou sob suspeita que comprometa, ou tenha o potencial de comprometer, a confidencialidade, a integridade, a disponibilidade ou a rastreabilidade de informações, sistemas, redes ou dados pessoais. Eventos que não resultem em impacto imediato podem configurar incidentes caso revelem fragilidade de controle ou risco relevante ao ambiente institucional.

4. Princípios Orientadores da Resposta a Incidentes

A resposta a incidentes deve ser conduzida de forma estruturada, proporcional ao impacto, tempestiva e coordenada, priorizando a contenção de danos, a preservação de evidências, a continuidade das operações essenciais e a proteção dos direitos dos titulares de dados pessoais.

ASSUNTO: GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS PESSOAIS		
VERSÃO: 5.0	**DATA DE PUBLICAÇÃO:** 16 DE JULHO DE 2026	**REVISÃO:** ANUAL
AUTOR: EMBRASI GOVERNANCA E C. TECNOLOGICA		
INSTITUIÇÃO: SGM CONSULTORES ASSOCIADOS LTDA		**CNPJ:** 00.306.499/0001-60

Todas as decisões críticas devem ser tomadas por pessoas formalmente designadas, ainda que apoiadas por ferramentas tecnológicas.

5. Identificação e Comunicação de Incidentes

Você deve comunicar imediatamente qualquer evento suspeito ou confirmado que possa caracterizar incidente de segurança da informação, utilizando os canais institucionais definidos. A omissão, o atraso injustificado ou a tentativa de tratamento informal de incidentes configura descumprimento desta Política. Ferramentas automatizadas podem apoiar a detecção de eventos, porém a validação e classificação inicial do incidente dependem de análise humana.

6. Análise, Classificação e Contenção

Os incidentes devem ser analisados quanto à natureza, causa, extensão, impacto e criticidade, considerando os ativos afetados e a presença de dados pessoais ou informações sensíveis. As medidas de contenção devem ser adotadas de forma proporcional, buscando interromper a progressão do incidente sem ampliar riscos ou prejuízos operacionais. A definição da severidade e das ações prioritárias é atribuição humana, devidamente registrada.

7. Tratamento, Erradicação e Recuperação

O tratamento do incidente deve abranger a eliminação da causa raiz, a correção de vulnerabilidades identificadas e a restauração segura dos sistemas e informações afetados. A recuperação deve observar critérios de integridade, confiabilidade e validação, conforme diretrizes de backup, continuidade e segurança da informação. Nenhum sistema deve retornar à operação sem validação humana quanto à segurança e estabilidade.

8. Incidentes Envolvendo Dados Pessoais

Quando o incidente envolver dados pessoais, deve-se avaliar o risco aos direitos e liberdades dos titulares, em consonância com a Política de Privacidade e Proteção de Dados Pessoais. A decisão sobre comunicação a titulares, autoridades ou terceiros deve ser tomada por instâncias competentes, com base em análise técnica e jurídica, e devidamente documentada.

ASSUNTO: GOVERNANÇA DE SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS PESSOAIS		
VERSÃO: 5.0	**DATA DE PUBLICAÇÃO:** 16 DE JULHO DE 2026	**REVISÃO:** ANUAL
AUTOR: EMBRASI GOVERNANCA E C. TECNOLOGICA		
INSTITUIÇÃO: SGM CONSULTORES ASSOCIADOS LTDA		**CNPJ:** 00.306.499/0001-60

9. Comunicação e Gestão de Crise

A comunicação interna e externa relacionada a incidentes deve ser centralizada, controlada e alinhada à estratégia institucional, sendo vedada qualquer divulgação não autorizada. A gestão de crises decorrentes de incidentes de segurança deve priorizar a transparência responsável, a mitigação de impactos reputacionais e a preservação da confiança de clientes e parceiros.

10. Registro, Evidências e Auditoria

Todos os incidentes de segurança devem ser registrados de forma completa, precisa e rastreável, incluindo eventos, decisões, ações adotadas e evidências coletadas. Os registros devem ser preservados conforme critérios de retenção e estar disponíveis para auditorias internas, investigações e melhorias contínuas. Ferramentas de registro e correlação atuam como suporte, cabendo a análise conclusiva à avaliação humana.

11. Responsabilidades

O descumprimento desta Política ou a atuação negligente, imprudente ou dolosa na gestão de incidentes poderá resultar na aplicação de medidas disciplinares, contratuais e legais cabíveis. Cada agente é responsável por suas ações ou omissões, inclusive quando apoiadas por sistemas ou soluções tecnológicas.