Plano de Resposta a Incidentes de Segurança

Kicol Tecnologia e Serviços LTDA

Documento:	Plano de Resposta a Incidentes de Segurança
Versão:	1.0
Data de aprovação:	03 de março de 2026
Próxima revisão:	Março de 2027
Aprovado por:	Eduardo Macedo — Diretor / Responsável Técnico
Classificação:	Uso interno

CNPJ: 64.973.433/0001-06

Rua Alcindo Guanabara, 17, Sala 1313, Centro, Rio de Janeiro - RJ, 20031-130

1. Objetivo

Definir os procedimentos para identificação, contenção, erradicação, recuperação e comunicação de incidentes de segurança da informação na Kicol Tecnologia e Serviços LTDA, minimizando o impacto sobre as operações e os dados de clientes.

2. Escopo

Este plano se aplica a qualquer evento que comprometa ou possa comprometer a confidencialidade, integridade ou disponibilidade dos sistemas e dados gerenciados pela empresa, incluindo mas não se limitando a:

- Acesso não autorizado a servidores, bancos de dados ou repositórios;
- Vazamento ou exposição de dados de clientes;
- Infecção por malware ou ransomware;
- Indisponibilidade de serviços por ataque (DDoS ou outros);
- Comprometimento de credenciais;
- Exploração de vulnerabilidades em aplicações.

3. Classificação de Incidentes

Severidade	Descrição	Tempo de resposta
Crítica	Vazamento de dados de clientes, acesso não autorizado a produção, ransomware	Imediato (até 1 hora)
Alta	Vulnerabilidade explorada, indisponibilidade de serviço, comprometimento de credenciais	Até 4 horas
Média	Tentativa de acesso não autorizado bloqueada, comportamento anômalo detectado	Até 24 horas
Baixa	Alertas informativos, tentativas de phishing bloqueadas	Até 72 horas

4. Etapas de Resposta

4.1 Identificação

Monitoramento contínuo dos sistemas por meio de logs do servidor, alertas do provedor de hospedagem e monitoramento de aplicações. Qualquer comportamento anômalo identificado é tratado como potencial incidente e investigado.

4.2 Contenção

- Isolamento imediato do recurso comprometido (servidor, conta, aplicação);
- Revogação de credenciais potencialmente comprometidas;
- Bloqueio de IPs ou acessos suspeitos;
- Preservação de logs e evidências para análise posterior.

4.3 Erradicação

- Identificação e remoção da causa raiz do incidente;
- Correção da vulnerabilidade explorada;
- Atualização de sistemas e dependências, se necessário;
- Verificação de que não há outros pontos comprometidos.

4.4 Recuperação

- Restauração dos sistemas a partir de backups íntegros, quando necessário;
- Verificação da integridade dos dados restaurados;
- Reativação gradual dos serviços com monitoramento intensificado;
- Geração de novas credenciais e chaves quando aplicável.

4.5 Notificação

Em caso de incidentes que envolvam dados de clientes, o cliente será notificado em até 48 horas após a confirmação do incidente, com as seguintes informações:

- Descrição do incidente e dados potencialmente afetados;
- Medidas de contenção e correção adotadas;
- Recomendações para o cliente (ex: alteração de senhas);
- Ponto de contato para acompanhamento.

Para incidentes que envolvam dados pessoais, a notificação à Autoridade Nacional de Proteção de Dados (ANPD) será realizada conforme previsto na LGPD, quando aplicável.

4.6 Lições aprendidas

Após a resolução de cada incidente, é realizada uma análise para identificar as causas, avaliar a eficácia da resposta e definir ações preventivas para evitar recorrência. O registro do incidente é mantido com data, descrição, impacto, ações tomadas e melhorias implementadas.

5. Canal de Comunicação

Incidentes de segurança podem ser reportados diretamente ao responsável técnico da empresa pelo e-mail de contato oficial ou por telefone. Todas as comunicações sobre incidentes são tratadas

com confidencialidade.

6. Revisão

Este plano será revisado anualmente ou após a ocorrência de qualquer incidente significativo de segurança.

Versão	Data	Descrição	Responsável
1.0	03/03/2026	Versão inicial do documento	Eduardo Macedo

7. Aprovação

_____

Eduardo Macedo
Diretor / Responsável Técnico
Kicol Tecnologia e Serviços LTDA
03 de março de 2026