Política de Gestão de Riscos de Segurança da Informação

Kicol Tecnologia e Serviços LTDA

Documento:	Política de Gestão de Riscos de Segurança da Informação
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 as diretrizes para identificação, análise, tratamento e monitoramento dos riscos de segurança da informação na Kicol Tecnologia e Serviços LTDA, de forma a proteger os ativos de informação da empresa e de seus clientes.

2. Escopo

Esta política se aplica a todos os processos, sistemas, infraestrutura e informações gerenciadas pela Kicol Tecnologia, incluindo projetos desenvolvidos para clientes, ambientes de produção e ferramentas de trabalho.

3. Processo de Gestão de Riscos

3.1 Identificação de riscos

A identificação de riscos é realizada de forma contínua, considerando:

- Ameaças e vulnerabilidades conhecidas nos sistemas e infraestrutura utilizados;
- Mudanças no ambiente tecnológico (novos projetos, novas integrações, novos fornecedores);
- Requisitos de segurança de clientes;
- Alertas de segurança de fornecedores (Hostinger, GitHub, NuvemShop, Bling);
- Incidentes de segurança anteriores, próprios ou do mercado.

3.2 Análise e avaliação

Cada risco identificado é avaliado quanto à probabilidade de ocorrência e ao impacto potencial sobre a confidencialidade, integridade ou disponibilidade das informações. A combinação desses fatores determina a criticidade do risco:

	Impacto Baixo	Impacto Médio	Impacto Alto
Probabilidade Alta	Médio	Alto	Crítico
Probabilidade Média	Baixo	Médio	Alto
Probabilidade Baixa	Baixo	Baixo	Médio

3.3 Tratamento de riscos

Para cada risco avaliado, uma das seguintes estratégias de tratamento é adotada:

- **Mitigar:** implementar controles que reduzam a probabilidade ou o impacto do risco;

• **Aceitar:** aceitar o risco quando o custo do controle supera o impacto potencial, com registro formal;

• **Transferir:** transferir o risco a terceiros (ex: utilização de provedor de hospedagem com SLA e certificações);

• **Evitar:** eliminar a atividade ou condição que gera o risco.

3.4 Monitoramento

Os riscos identificados e seus tratamentos são revisados semestralmente ou sempre que houver mudança relevante no ambiente (novo projeto, novo cliente, mudança de infraestrutura, incidente de segurança).

4. Gestão de Riscos em Fornecedores

A Kicol Tecnologia avalia os riscos de segurança dos fornecedores e plataformas de terceiros utilizados em sua operação. Os critérios de avaliação incluem:

• Certificações de segurança (ISO 27001, SOC 2 ou equivalentes);

• Práticas de criptografia e proteção de dados;

• Histórico de incidentes de segurança;

• Políticas de backup e disponibilidade;

• Conformidade com a LGPD.

Atualmente, os principais fornecedores utilizados são a Hostinger (hospedagem), o GitHub (repositórios de código) e a Vercel (hospedagem de aplicações frontend), todos avaliados quanto às suas práticas de segurança.

5. Responsabilidades

O responsável técnico e diretor da empresa é responsável pela condução do processo de gestão de riscos, incluindo identificação, avaliação, definição de tratamento e monitoramento contínuo.

6. Revisão

Esta política será revisada anualmente ou sempre que houver mudança significativa no ambiente de riscos da empresa.

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