BIX TECNOLOGIA · DOCUMENTO CORPORATIVO

Política de Gestão de Riscos de Segurança da Informação

Diretrizes para identificar, avaliar e tratar riscos de segurança da informação de forma proporcional ao contexto e ao apetite de risco da Bix Tecnologia.

Versão 1.0 **Status** Aprovada e publicada **Revisão** Anual ou sob mudança

1. Objetivo

Estabelecer diretrizes gerais para a gestão de riscos de segurança da informação, orientando a identificação, a análise, o tratamento e o monitoramento de riscos de maneira contínua e proporcional à criticidade dos ativos e ao apetite de risco da empresa.

2. Escopo

- Aplica-se a colaboradores, prestadores e terceiros que tratem informações ou sistemas da Bix Tecnologia.
- Abrange riscos sobre confidencialidade, integridade e disponibilidade das informações.
- A profundidade dos controles é **proporcional ao risco** e ao valor do ativo.

3. Princípios

- **Proporcionalidade:** o esforço de tratamento acompanha o nível de risco.
- **Decisão informada:** riscos relevantes são comunicados a quem decide.
- **Melhoria contínua:** os riscos são reavaliados ao longo do tempo.

4. Processo de gestão de riscos

O processo segue, de forma flexível, as etapas a seguir:

- **Identificação:** levantamento de ameaças, vulnerabilidades e ativos envolvidos.
- **Análise e avaliação:** estimativa qualitativa de probabilidade e impacto.
- **Tratamento:** definição da resposta mais adequada ao contexto.
- **Monitoramento:** acompanhamento dos riscos e da eficácia das ações.

5. Níveis de risco

Classificação qualitativa orientativa (ajustável ao contexto):

NÍVEL	INTERPRETAÇÃO	POSTURA ESPERADA
Baixo	Impacto/probabilidade reduzidos	Aceitar ou monitorar
Médio	Impacto moderado	Tratar conforme custo-benefício
Alto	Impacto relevante ao negócio ou a clientes	Tratamento prioritário

6. Opções de tratamento

- **Mitigar:** aplicar controles para reduzir o risco.
- **Aceitar:** assumir o risco residual, com registro da decisão.
- **Transferir:** compartilhar o risco (ex.: contratos, terceiros).
- **Evitar:** descontinuar a atividade que gera o risco.

7. Papéis e responsabilidades

- **Direção:** define o apetite de risco e aprova esta política.
- **Segurança da Informação:** conduz e apoia o processo de gestão de riscos.
- **Gestores e donos de ativos:** identificam riscos e decidem tratamentos sob sua alçada.

8. Revisão

- Os riscos relevantes são reavaliados periodicamente — em regra anualmente — ou sob mudança significativa.
- Esta política é revisada na mesma cadência.

Aprovação

DOCUMENTO
Política de Gestão de Riscos de Segurança da Informação

VERSÃO
1.0

APROVADO POR
Direção — Bix Tecnologia

DATA DE REVISÃO
Junho de 2026

PRÓXIMA REVISÃO
Junho de 2027 (ou sob mudança relevante)

CONTATO
info@bixtecnologia.com.br

Documento oficial publicado pela Bix Tecnologia. Diretrizes de caráter geral e orientador; detalhamentos operacionais constam em normas internas complementares.