

Processo de Gestão de Vulnerabilidades

Identificação, classificação e correção de vulnerabilidades em aplicações e infraestrutura, com varreduras periódicas, patching e metas de prazo orientativas.

Versão 1.0

Status Aprovada e publicada

Revisão Anual ou sob mudança

1. Objetivo e escopo

Definir como a Bix Tecnologia identifica, prioriza e corrige vulnerabilidades em código, dependências e infraestrutura, reduzindo a exposição a riscos de forma proporcional à criticidade.

2. Identificação (varreduras)

- **Dependências:** análise de bibliotecas e SCA no pipeline (ex.: alertas de dependências, scanners de vulnerabilidade).
- **Aplicação:** revisões de código e testes de segurança quando aplicável.
- **Infraestrutura:** recursos do **GCP** (Cloud Run, Cloud SQL) e **Cloudflare** acompanhados por recursos de segurança nativos da plataforma.
- Varreduras executadas periodicamente e a cada mudança relevante.

3. Classificação de severidade

Severidade avaliada tomando o **CVSS** como referência, considerando o contexto de exposição:

SEVERIDADE	META DE CORREÇÃO (ORIENTATIVA)
Crítica	Tratamento prioritário, o quanto antes
Alta	Em poucos dias úteis
Média	Dentro do ciclo de manutenção
Baixa	Conforme planejamento / aceitação de risco

As metas acima são **orientativas** e podem ser ajustadas conforme o risco real, a disponibilidade de correção e o impacto operacional.

4. Correção e patching

- Atualizações de segurança priorizadas conforme a severidade.

- Preferência por correções automatizadas e deploys controlados (CI/CD).
- Quando não houver correção imediata, aplicam-se mitigações compensatórias.

5. Reavaliação e registro

- Itens corrigidos são reverificados; itens aceitos têm a decisão registrada.
- Acompanhamento via repositório (issues/PRs) e ferramentas das plataformas.

6. Papéis

- **Engenharia:** corrige e valida.
- **Segurança da Informação:** orienta prioridades e acompanha pendências.

Aprovação

DOCUMENTO

Processo de Gestão de Vulnerabilidades

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; detalhes operacionais constam em normas internas complementares.