



Política de Desenvolvimento Seguro

Kicol Tecnologia e Serviços LTDA

Documento:	Política de Desenvolvimento Seguro
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

Estabelecer as práticas e diretrizes de segurança adotadas durante o ciclo de desenvolvimento de software na Kicol Tecnologia e Serviços LTDA, garantindo que as aplicações sejam projetadas, desenvolvidas e mantidas com proteção contra vulnerabilidades e ameaças conhecidas.

2. Escopo

Esta política se aplica a todos os projetos de desenvolvimento de software conduzidos pela empresa, incluindo aplicações web, APIs, integrações com plataformas de terceiros e scripts de automação.

3. Princípios de Desenvolvimento Seguro

3.1 Proteção contra vulnerabilidades comuns (OWASP Top 10)

Todas as aplicações desenvolvidas pela Kicol Tecnologia devem implementar proteções contra as vulnerabilidades mais comuns, conforme o OWASP Top 10:

- **Injeção (SQL, NoSQL, OS):** uso obrigatório de consultas parametrizadas e ORMs; proibido concatenar dados do usuário em queries;
- **Autenticação quebrada:** implementação de autenticação robusta com hash seguro de senhas (bcrypt/argon2), proteção contra força bruta e suporte a 2FA;
- **Exposição de dados sensíveis:** criptografia em trânsito (HTTPS/TLS obrigatório) e em repouso quando aplicável;
- **XSS (Cross-Site Scripting):** sanitização e escape de todas as saídas renderizadas no navegador;
- **CSRF (Cross-Site Request Forgery):** uso de tokens anti-CSRF em todas as operações que alteram estado;
- **Configurações inseguras:** remoção de credenciais padrão, desativação de debug em produção, cabeçalhos de segurança HTTP configurados;
- **Componentes vulneráveis:** dependências e bibliotecas mantidas atualizadas e verificadas quanto a CVEs conhecidas.

3.2 Gestão de credenciais e segredos

- Credenciais, tokens de API, chaves de criptografia e segredos nunca são incluídos no código-fonte;
- Todos os segredos são armazenados em variáveis de ambiente no servidor;
- O arquivo .env é incluído no .gitignore de todos os projetos;
- Credenciais de produção são diferentes das de desenvolvimento e homologação.

3.3 Separação de ambientes

Os ambientes de desenvolvimento, homologação e produção são separados. Dados de produção não são utilizados em ambientes de desenvolvimento ou testes. Para fins de teste, são utilizados dados fictícios ou anonimizados.

3.4 Revisão de código

Todo código é revisado antes de ser integrado à branch principal do repositório. A revisão verifica aspectos funcionais, de segurança e de qualidade, incluindo validações de entrada, tratamento de erros e proteções contra vulnerabilidades.

4. Testes de Segurança

- Testes de segurança são realizados antes de cada deploy em produção;
- Verificações incluem validação de entradas, testes de autenticação e autorização, e verificação de cabeçalhos de segurança;
- Após atualizações significativas, testes de vulnerabilidade são conduzidos para validar a integridade da aplicação;
- Vulnerabilidades identificadas são corrigidas antes da publicação em produção.

5. Dependências e Bibliotecas

Todas as dependências e bibliotecas de terceiros utilizadas nos projetos devem ser:

- Provenientes de fontes confiáveis (npm, pip, packagist ou repositórios oficiais);
- Mantidas atualizadas com as últimas versões estáveis;
- Verificadas quanto a vulnerabilidades conhecidas antes da adoção;
- Monitoradas continuamente por meio de alertas de segurança do GitHub (Dependabot).

6. Deploy em Produção

O deploy em produção segue o procedimento definido na Política de Gestão de Mudanças. O acesso ao ambiente de produção para deploy é realizado exclusivamente via SSH com autenticação por chave, restrito ao responsável técnico.

7. Revisão

Esta política será revisada anualmente ou quando houver mudança significativa nas tecnologias ou práticas de desenvolvimento adotadas pela empresa.

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

8. Aprovação

Eduardo Macedo

Diretor / Responsável Técnico

Kicol Tecnologia e Serviços LTDA

03 de março de 2026