



Política de Segurança da Informação

Kicol Tecnologia e Serviços LTDA

Documento:	Política 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

Sumário

1. Objetivo
2. Escopo
3. Definições e Princípios
4. Diretrizes de Segurança da Informação
5. Controle de Acessos
6. Proteção de Dados
7. Segurança em Desenvolvimento de Software
8. Gestão de Incidentes de Segurança
9. Backup e Recuperação
10. Uso de Recursos Tecnológicos
11. Relacionamento com Terceiros e Clientes
12. Sanções e Medidas Disciplinares
13. Revisão e Atualização
14. Aprovação

1. Objetivo

Esta Política de Segurança da Informação (PSI) tem como objetivo estabelecer as diretrizes, responsabilidades e práticas adotadas pela Kicol Tecnologia e Serviços LTDA para proteger as informações sob sua responsabilidade, garantindo a confidencialidade, integridade e disponibilidade dos dados de clientes, parceiros e da própria organização.

A política visa assegurar que todos os envolvidos nas operações da empresa compreendam suas responsabilidades quanto à proteção das informações e adotem práticas adequadas de segurança no dia a dia.

2. Escopo

Esta política se aplica a todos os colaboradores, prestadores de serviço e parceiros que tenham acesso a sistemas, dados ou infraestrutura da Kicol Tecnologia, incluindo:

- Sistemas e aplicações desenvolvidos e mantidos pela empresa;
- Infraestrutura de hospedagem e servidores;
- Repositórios de código-fonte;
- Bancos de dados com informações de clientes;
- Equipamentos de trabalho (estações, dispositivos móveis);
- Serviços e plataformas de terceiros utilizados na operação.

Por se tratar de uma empresa com estrutura enxuta e especializada, os controles descritos nesta política são proporcionais ao porte da organização e ao nível de risco das operações realizadas, sem prejuízo à sua efetividade.

3. Definições e Princípios

A segurança da informação na Kicol Tecnologia é orientada por três princípios fundamentais:

Confidencialidade: garantir que as informações sejam acessadas apenas por pessoas autorizadas.

Integridade: assegurar que as informações não sejam alteradas de forma indevida ou não autorizada.

Disponibilidade: garantir que as informações e os sistemas estejam acessíveis quando necessário.

4. Diretrizes de Segurança da Informação

4.1 Autenticação e credenciais

Todas as credenciais de acesso a sistemas, servidores e plataformas devem ser armazenadas exclusivamente em gerenciador de senhas criptografado. É proibido o armazenamento de senhas em arquivos de texto, planilhas, e-mails ou qualquer meio não criptografado.

Senhas devem ter no mínimo 12 caracteres e combinar letras maiúsculas, minúsculas, números e caracteres especiais. A reutilização de senhas entre serviços diferentes é proibida.

O duplo fator de autenticação (2FA) deve ser habilitado em todos os serviços que ofereçam essa funcionalidade, incluindo painéis de hospedagem, repositórios de código e serviços em nuvem.

4.2 Criptografia

Todas as estações de trabalho utilizadas na operação devem possuir criptografia de disco ativada (FileVault no macOS, BitLocker no Windows ou equivalente em Linux).

A comunicação entre sistemas e APIs deve ser realizada exclusivamente por meio de protocolos criptografados (HTTPS/TLS). Conexões não criptografadas são proibidas em ambiente de produção.

Bancos de dados em produção devem utilizar conexões criptografadas (SSL/TLS) e, quando aplicável, criptografia de dados em repouso.

4.3 Infraestrutura e hospedagem

Os servidores de produção são hospedados em provedor de infraestrutura que possui certificações de segurança reconhecidas internacionalmente. O acesso aos servidores é realizado exclusivamente por meio de chaves SSH, sendo proibido o acesso por senha.

O painel de administração do provedor de hospedagem é protegido por duplo fator de autenticação (2FA).

Acessos root ou administrativos aos servidores são restritos ao responsável técnico da empresa.

5. Controle de Acessos

O acesso a sistemas, servidores, repositórios de código e bancos de dados segue o princípio do menor privilégio: cada pessoa recebe apenas o nível de acesso estritamente necessário para desempenhar sua função.

Atualmente, o acesso à infraestrutura de produção (servidores, bancos de dados e repositórios de código) é restrito exclusivamente ao responsável técnico e diretor da empresa. Em caso de ampliação da equipe, os acessos serão concedidos individualmente, registrados e revisados trimestralmente.

Todos os repositórios de código-fonte são mantidos como privados na plataforma GitHub. O acesso é controlado por permissões individuais vinculadas a contas autenticadas com 2FA.

Ao término de qualquer vínculo profissional (colaborador, prestador de serviço ou parceiro), todos os acessos são revogados imediatamente.

6. Proteção de Dados

A Kicol Tecnologia reconhece sua responsabilidade na proteção dos dados pessoais e corporativos que processa em nome de seus clientes, em conformidade com a Lei Geral de Proteção de Dados (LGPD — Lei nº 13.709/2018).

Os dados de clientes são tratados exclusivamente para a finalidade contratada. Não é permitido o uso de dados de produção em ambientes de desenvolvimento ou testes. Para fins de teste, devem ser utilizados dados fictícios ou anonimizados.

Dados sensíveis como credenciais de API, tokens de autenticação e chaves de acesso são armazenados em variáveis de ambiente protegidas no servidor, nunca em código-fonte ou repositórios.

Em caso de incidente envolvendo dados pessoais, o cliente será notificado em até 48 horas após a identificação do incidente, conforme previsto na LGPD.

7. Segurança em Desenvolvimento de Software

O processo de desenvolvimento de software da Kicol Tecnologia segue práticas de desenvolvimento seguro, incluindo:

- Validação e sanitização de todas as entradas de dados do usuário;
- Proteção contra vulnerabilidades comuns (OWASP Top 10): SQL Injection, XSS, CSRF, entre outras;
- Utilização de consultas parametrizadas para acesso a banco de dados;
- Separação de ambientes de desenvolvimento, homologação e produção;
- Revisão de código antes de qualquer deploy em produção;
- Credenciais e chaves armazenadas exclusivamente em variáveis de ambiente, nunca em código-fonte;
- Dependências e bibliotecas de terceiros são mantidas atualizadas e verificadas quanto a vulnerabilidades conhecidas.

O deploy em produção é realizado manualmente via SSH com autenticação por chave, garantindo que apenas o responsável técnico autorizado possa publicar alterações no ambiente de produção.

8. Gestão de Incidentes de Segurança

A Kicol Tecnologia mantém um procedimento de resposta a incidentes de segurança da informação que compreende as seguintes etapas:

- **Identificação:** monitoramento contínuo dos sistemas e análise de alertas do provedor de hospedagem;
- **Contenção:** isolamento imediato do recurso comprometido para evitar propagação;

- **Erradicação:** remoção da causa raiz do incidente e correção da vulnerabilidade explorada;
- **Recuperação:** restauração dos sistemas a partir de backups e verificação de integridade;
- **Notificação:** comunicação ao cliente em até 48 horas, com detalhes do ocorrido, impacto e medidas tomadas;
- **Lições aprendidas:** registro do incidente e revisão dos controles para evitar recorrência.

9. Backup e Recuperação

A Kicol Tecnologia realiza backups diários de todos os sistemas e bancos de dados de produção. Os procedimentos de backup incluem:

- Backup diário automatizado dos bancos de dados e arquivos de aplicação;
- Armazenamento dos backups em ambiente separado do servidor de produção;
- Retenção mínima de 30 dias de histórico de backups;
- Testes periódicos de restauração para validar a integridade dos backups;
- Criptografia dos arquivos de backup em trânsito e em repouso.

10. Uso de Recursos Tecnológicos

Os recursos tecnológicos da empresa (equipamentos, servidores, licenças de software e serviços em nuvem) devem ser utilizados exclusivamente para fins profissionais relacionados às atividades da empresa.

É proibido instalar softwares não autorizados ou de procedência desconhecida em equipamentos que acessem a infraestrutura da empresa ou de seus clientes.

Os sistemas operacionais e softwares utilizados devem ser mantidos atualizados com as últimas correções de segurança disponibilizadas pelos fabricantes.

11. Relacionamento com Terceiros e Clientes

Todos os contratos com clientes incluem cláusulas de confidencialidade e proteção de dados, estabelecendo as responsabilidades de cada parte quanto à segurança da informação.

Ao trabalhar com dados ou sistemas de clientes, a Kicol Tecnologia se compromete a seguir as políticas de segurança do cliente, quando aplicáveis, além das suas próprias.

Plataformas e serviços de terceiros utilizados na operação (hospedagem, repositórios, ferramentas de desenvolvimento) são avaliados quanto às suas práticas de segurança e certificações antes da adoção.

12. Sanções e Medidas Disciplinares

O descumprimento desta política por qualquer colaborador, prestador de serviço ou parceiro poderá acarretar medidas disciplinares proporcionais à gravidade da infração, incluindo:

- Advertência formal por escrito;
- Suspensão imediata dos acessos a sistemas e infraestrutura;
- Rescisão do vínculo contratual;
- Responsabilização civil e criminal, quando cabível, nos termos da legislação vigente.

Todos os incidentes de segurança causados por descumprimento desta política serão registrados e investigados.

13. Revisão e Atualização

Esta política será revisada anualmente ou sempre que houver mudança significativa na estrutura da empresa, nos serviços prestados, na infraestrutura tecnológica ou na legislação aplicável.

O responsável pela revisão é o diretor e responsável técnico da empresa. Cada revisão gera uma nova versão do documento, com registro da data e das alterações realizadas.

Versão	Data	Descrição	Responsável
1.0	03/03/2026	Versão inicial da política	Eduardo Macedo

14. Aprovação

Este documento foi aprovado pela direção da Kicol Tecnologia e Serviços LTDA e entra em vigor na data de sua publicação.

Eduardo Macedo

Diretor / Responsável Técnico

Kicol Tecnologia e Serviços LTDA

03 de março de 2026