Política de Segurança da Informação

Kicol Tecnologia e Serviços LTDA

Documento:	Política de Segurança da Informação
Versão:	1.0
Data de aprovação:	3 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

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 a 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 as suas responsabilidades quanto à proteção das informações e adotem práticas adequadas de segurança no quotidiano.

2. Âmbito de Aplicação

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

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

Por se tratar de uma empresa com estrutura reduzida e especializada, os controlos descritos nesta política são proporcionais à dimensão da organização e ao nível de risco das operações realizadas, sem prejuízo da 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 acedidas 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 gestor de palavras-passe encriptado. É proibido o armazenamento de palavras-passe em ficheiros de texto, folhas de cálculo, e-mails ou qualquer meio não encriptado.

As palavras-passe devem ter no mínimo 12 caracteres e combinar letras maiúsculas, minúsculas, números e caracteres especiais. A reutilização de palavras-passe entre serviços diferentes é proibida.

A autenticação de dois fatores (2FA) deve ser ativada em todos os serviços que disponibilizem esta funcionalidade, incluindo painéis de alojamento, repositórios de código e serviços na nuvem.

4.2 Encriptação

Todas as estações de trabalho utilizadas na operação devem possuir encriptação 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 encriptados (HTTPS/TLS). Ligações não encriptadas são proibidas em ambiente de produção.

As bases de dados em produção devem utilizar ligações encriptadas (SSL/TLS) e, quando aplicável, encriptação de dados em repouso.

4.3 Infraestrutura e alojamento

Os servidores de produção são alojados num fornecedor 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 palavra-passe.

O painel de administração do fornecedor de alojamento é protegido por autenticação de dois fatores (2FA).

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

5. Controlo de Acessos

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

Atualmente, o acesso à infraestrutura de produção (servidores, bases de dados e repositórios de código) é restrito exclusivamente ao responsável técnico e diretor da empresa. Em caso de alargamento da equipa, os acessos serão concedidos individualmente, registados e revistos 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.

Aquando do 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 a sua responsabilidade na proteção dos dados pessoais e corporativos que processa em nome dos seus clientes, em conformidade com a Lei Geral de Proteção de Dados (LGPD — Lei n.º 13.709/2018) do Brasil.

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.

7. Desenvolvimento Seguro 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 utilizador;
- Proteção contra vulnerabilidades comuns (OWASP Top 10): SQL Injection, XSS, CSRF, entre outras;
- Utilização de consultas parametrizadas para acesso à base de dados;
- Separação de ambientes de desenvolvimento, homologação e produção;
- Revisão de código antes de qualquer implementação 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.

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:** monitorização contínua dos sistemas e análise de alertas do fornecedor de alojamento;
- **Contenção:** isolamento imediato do recurso comprometido para evitar propagação;
- **Erradicação:** remoção da causa raiz do incidente e correção da vulnerabilidade explorada;
- **Recuperação:** restauro dos sistemas a partir de cópias de segurança e verificação de integridade;

- **Notificação:** comunicação ao cliente em até 48 horas, com detalhes do ocorrido, impacto e medidas tomadas;
- **Lições aprendidas:** registo do incidente e revisão dos controlos para evitar recorrência.

9. Cópias de Segurança e Recuperação

A Kicol Tecnologia realiza cópias de segurança diárias de todos os sistemas e bases de dados de produção, incluindo:

- Cópia de segurança diária automatizada das bases de dados e ficheiros de aplicação;
- Armazenamento das cópias em ambiente separado do servidor de produção;
- Retenção mínima de 30 dias de histórico;
- Testes periódicos de restauro para validar a integridade;
- Encriptação dos ficheiros de cópia de segurança em trânsito e em repouso.

10. Utilização de Recursos Tecnológicos

Os recursos tecnológicos da empresa devem ser utilizados exclusivamente para fins profissionais. É proibido instalar software não autorizado ou de procedência desconhecida em equipamentos que acedam à infraestrutura da empresa ou dos seus clientes.

11. Relacionamento com Terceiros e Clientes

Todos os contratos com clientes incluem cláusulas de confidencialidade e proteção de dados. As plataformas e serviços de terceiros utilizados na operação são avaliados quanto às suas práticas de segurança antes da adoção.

12. Sanções e Medidas Disciplinares

O incumprimento desta política poderá resultar em 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 aplicável.

13. Revisão e Atualização

Esta política será revista anualmente ou sempre que ocorra uma alteração significativa na estrutura da empresa, nos serviços prestados, na infraestrutura tecnológica ou na legislação aplicável.

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

14. Aprovação

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

_____

Eduardo Macedo
Diretor / Responsável Técnico
Kicol Tecnologia e Serviços LTDA
3 de março de 2026