

Política de Segurança da Informação

Versão 1.0

CÓDIGO	VERSÃO	APROVAÇÃO	REVISÃO
3K-POL-005	1.0	Diretoria	Anual

1. Objetivo

Esta Política estabelece as diretrizes da **3K BUSINESS LTDA** ("**3K Business**") para proteger as informações próprias e as de seus clientes quanto à **confidencialidade**, à **integridade** e à **disponibilidade**, abrangendo o desenvolvimento, a operação e a sustentação das soluções que desenvolve e mantém.

2. Abrangência

Aplica-se a sócios, administradores, colaboradores, estagiários e prestadores de serviços, e a todas as informações, sistemas, ambientes de nuvem, repositórios de código, dispositivos e serviços utilizados pela 3K Business ou mantidos por ela para seus clientes.

3. Referências

- ABNT NBR ISO/IEC 27001:2022 e 27002:2022 — sistemas de gestão e controles de segurança da informação;
- Lei nº 13.709/2018 (LGPD) e regulamentos da Autoridade Nacional de Proteção de Dados (ANPD);
- Lei nº 12.965/2014 (Marco Civil da Internet);
- OWASP Top 10 e OWASP ASVS, para desenvolvimento seguro.

4. Princípios

- Confidencialidade:** a informação é acessível apenas a quem está autorizado;
- Integridade:** a informação é exata, completa e protegida contra alterações indevidas;
- Disponibilidade:** a informação e os sistemas estão acessíveis quando necessário;
- Menor privilégio e necessidade de saber:** cada pessoa ou sistema recebe apenas os acessos indispensáveis à sua função;
- Segurança desde a concepção:** requisitos de segurança e privacidade são considerados desde o início de cada projeto.

5. Classificação da informação

Classe	Exemplos	Tratamento
Pública	Conteúdo do site, materiais de divulgação, políticas publicadas.	Livre divulgação.
Interna	Procedimentos, documentação interna, planejamento.	Restrita a colaboradores e prestadores autorizados.
Confidencial	Contratos, propostas, código-fonte, dados cadastrais e documentos de clientes.	Acesso pela necessidade de saber; armazenamento em ambientes controlados.
Restrita	Credenciais, chaves de API, certificados digitais, bancos de dados de produção, dados pessoais de usuários finais.	Acesso mínimo e nominal, criptografia, autenticação multifator e registro de acesso.

6. Controle de acesso

- Todo acesso é individual e nominal; contas compartilhadas são vedadas, salvo exceção técnica documentada;
- A autenticação multifator (MFA) é obrigatória em e-mail corporativo, repositórios de código, provedores de nuvem, painéis de infraestrutura e sistemas administrativos;
- Senhas têm no mínimo 12 caracteres, são únicas por serviço e armazenadas em gerenciador de senhas;
- Acessos a ambientes de produção são concedidos apenas a quem deles necessita e revisados ao menos semestralmente;
- Acessos de colaboradores e prestadores desligados são revogados em até 24 horas, e as credenciais que eles conheciam são rotacionadas.

7. Gestão de segredos e credenciais

- Senhas, tokens, chaves de API e certificados **nunca** são gravados em código-fonte, repositórios, tickets, documentação ou mensagens;
- Segredos são armazenados em variáveis de ambiente de plataformas de implantação ou em cofres de segredos, com acesso restrito;
- Chaves e tokens têm o menor escopo possível e são rotacionados periodicamente e imediatamente em caso de suspeita de exposição;
- Certificados digitais são mantidos em repositório protegido, com senha armazenada separadamente do arquivo.

8. Desenvolvimento seguro

- O código-fonte é mantido em repositórios privados, com controle de versão e acesso por autenticação multifator;

- Alterações passam por revisão de código antes de chegar ao ambiente de produção;
 - Os ambientes de desenvolvimento, homologação e produção são segregados;
 - Dados reais de produção não são utilizados em desenvolvimento ou homologação sem anonimização;
 - As aplicações seguem as recomendações do OWASP Top 10, incluindo validação de entradas, proteção contra injeção, controle de autorização em todas as rotas e armazenamento de senhas com algoritmos de hash adequados;
 - Dependências de terceiros são mantidas atualizadas e verificadas quanto a vulnerabilidades conhecidas;
 - Alterações de estrutura em bancos de dados de produção são planejadas, versionadas e executadas de forma controlada.
-

9. Infraestrutura e operações

- Toda comunicação com as aplicações ocorre por canais criptografados (HTTPS/TLS);
 - Servidores são acessados por SSH com chaves ou por painéis com autenticação forte, e expõem à internet apenas os serviços necessários;
 - Sistemas operacionais, imagens de contêineres e componentes são atualizados periodicamente, com prioridade para correções de segurança;
 - As aplicações contam com registro de eventos (logs) e ferramentas de monitoramento e observabilidade, com alertas de indisponibilidade e erros;
 - Registros de acesso a aplicações são mantidos pelo prazo mínimo exigido pelo Marco Civil da Internet, quando aplicável;
 - Bancos de dados de produção têm **backup ao menos diário**, com cópia armazenada em local distinto do ambiente principal e **teste de restauração ao menos semestral**.
-

10. Dispositivos e trabalho remoto

- Dispositivos utilizados no trabalho devem ter sistema operacional atualizado, criptografia de disco, bloqueio de tela automático e proteção contra códigos maliciosos;
 - Informações confidenciais e restritas não são armazenadas em dispositivos pessoais não autorizados nem em mídias removíveis;
 - Redes Wi-Fi públicas devem ser evitadas para acesso a ambientes administrativos ou de produção;
 - A perda ou o furto de dispositivo deve ser comunicada imediatamente, para revogação de sessões e rotação de credenciais.
-

11. Uso aceitável

- Os recursos da empresa são utilizados para fins profissionais e de forma ética e legal;
- É vedado inserir dados pessoais, dados de clientes, credenciais ou código confidencial em ferramentas externas, incluindo ferramentas de inteligência artificial, que não tenham sido aprovadas pela empresa para esse uso;
- É vedado instalar softwares não licenciados ou de origem desconhecida.

12. Fornecedores e serviços em nuvem

Fornecedores que armazenem ou tratem informações da 3K Business ou de seus clientes são avaliados quanto a controles de segurança, localização dos dados e aderência à LGPD. Os contratos preveem obrigações de confidencialidade, segurança e comunicação de incidentes.

13. Gestão de incidentes

Qualquer suspeita de incidente de segurança deve ser comunicada imediatamente ao Responsável por Segurança da Informação. O tratamento segue as etapas:

1. **Detecção e registro** do incidente;
 2. **Contenção:** isolamento de sistemas, revogação de acessos e rotação de credenciais;
 3. **Erradicação e recuperação:** correção da causa e restauração segura dos serviços;
 4. **Comunicação:** aos clientes afetados, sem demora injustificada. Quando o incidente envolver dados pessoais e puder acarretar risco ou dano relevante: se a 3K Business for a controladora, comunica a ANPD e os titulares em até 3 (três) dias úteis, conforme a Resolução CD/ANPD nº 15/2024; se atuar como operadora, comunica imediatamente o controlador, para que ele cumpra esse prazo;
 5. **Lições aprendidas:** análise de causa-raiz e atualização de controles e do Registro de Riscos.
-

14. Proteção de dados pessoais

O tratamento de dados pessoais observa a LGPD e a [Política de Privacidade](#). Quando atua como operadora de dados de seus clientes, a 3K Business trata os dados exclusivamente conforme as instruções do controlador e para as finalidades contratadas.

15. Conscientização e treinamento

Colaboradores e prestadores recebem orientação sobre esta Política no ingresso e treinamento de conscientização em segurança da informação ao menos uma vez por ano, e assinam termo de confidencialidade.

16. Responsabilidades

- **Diretoria:** aprova esta Política, designa o Responsável por Segurança da Informação e provê os recursos necessários;
- **Responsável por Segurança da Informação:** coordena a implementação dos controles, a gestão de incidentes, as revisões de acesso e os treinamentos;
- **Líderes técnicos:** garantem a aplicação das práticas de desenvolvimento seguro e de operação nos projetos;
- **Todos:** cumprem esta Política e comunicam imediatamente incidentes e vulnerabilidades.

As funções de Responsável por Compliance e PLD/FT, por Riscos e por Segurança da Informação podem ser exercidas pela mesma pessoa, conforme designação formal da Diretoria, de modo compatível com o

porte da empresa.

17. Descumprimento

Violações desta Política sujeitam o infrator às medidas disciplinares e contratuais cabíveis, sem prejuízo das responsabilidades civis e penais.

18. Vigência e revisão

Esta Política entra em vigor na data de sua aprovação pela Diretoria e é revisada ao menos anualmente, ou antes, sempre que houver mudança relevante no ambiente tecnológico, no negócio ou na legislação.