



INFORMAÇÃO INSTITUCIONAL

Segurança da Informação

Versão 1.0 · Em vigor desde 1 de outubro de 2026

VERSÃO PARA REVISÃO JURÍDICA — NÃO VINCULATIVA

Índice

1. Compromisso
2. Proteção de dados
3. Autenticação e sessões
4. Controlo de acessos
5. Proteção da aplicação
6. Monitorização e resposta
7. Continuidade do serviço
8. Certificações
9. Divulgação responsável de vulnerabilidades

VERSÃO PARA REVISÃO JURÍDICA

Nota: Este documento é a versão pública das práticas de segurança da TROKA. Por razões de segurança, não descreve a infraestrutura, as tecnologias utilizadas nem os procedimentos internos. A informação detalhada é partilhada com instituições parceiras e reguladores ao abrigo de acordos de confidencialidade.

1. Compromisso

A TROKA trata a segurança da informação e a proteção dos dados dos clientes como condição essencial do serviço. Os controlos descritos neste documento estão em produção e são acompanhados por um programa de melhoria contínua, revisto periodicamente.

2. Proteção de dados

- Toda a comunicação entre as aplicações da TROKA e os seus servidores é cifrada em trânsito.
- As palavras-passe nunca são guardadas em texto simples: apenas um resumo criptográfico irreversível.
- Segredos de sistema e credenciais de integração são guardados cifrados.
- Os registos técnicos ocultam automaticamente informação sensível, como palavras-passe e dados de autenticação.
- São recolhidos apenas os dados estritamente necessários ao serviço.

3. Autenticação e sessões

- Autenticação multifator disponível para clientes e para os colaboradores com acesso à plataforma de gestão.
- Bloqueio automático após múltiplas tentativas de autenticação falhadas.
- Sessões de curta duração, com renovação segura e possibilidade de revogação individual.

4. Controlo de acessos

- Acesso interno baseado em funções, com segregação entre perfis operacionais (por exemplo, suporte, compliance e administração).
- O acesso a documentação de identificação e a dados financeiros está restrito a perfis com permissão explícita.

- As ações sensíveis ficam registadas numa trilha de auditoria, com autor, data e conteúdo da alteração.

5. Proteção da aplicação

- Validação estruturada de todos os dados recebidos pela plataforma.
- Limitação do número de pedidos, reforçada nas operações de autenticação.
- Cabeçalhos de segurança e políticas de origem aplicados e verificados em produção.
- Proteção contra ataques de negação de serviço ao nível da rede.

6. Monitorização e resposta

A TROKA regista e acompanha eventos de segurança, o que permite detetar e investigar incidentes. Em caso de incidente com impacto nos dados pessoais, a TROKA atua nos termos do RGPD, incluindo a notificação à autoridade de controlo e aos titulares, quando aplicável.

7. Continuidade do serviço

A TROKA mantém cópias de segurança dos dados de produção e procedimentos de recuperação, integrados no programa de melhoria contínua. **A validar: confirmar que a estratégia de cópias de segurança e o teste periódico de recuperação estão em produção à data de publicação**

8. Certificações

A TROKA não detém, à data deste documento, certificação ISO/IEC 27001 nem certificação PCI DSS. A contratação de um teste de intrusão externo e independente integra o programa de melhoria contínua.

9. Divulgação responsável de vulnerabilidades

Se identificar uma vulnerabilidade na plataforma TROKA, comunique-a de forma responsável.

A validar: canal de reporte de vulnerabilidades (ex.: endereço dedicado e ficheiro security.txt)