



Política de Criptografia

Controle do Documento

Campo	Descrição
Título	Política de Criptografia
Código do Documento	ZDT-PCR-001
Versão	1.0
Data de Criação	26/04/2026
Última Revisão	26/04/2026
Próxima Revisão	26/04/2027
Responsável	Diretoria
Classificação	Interno
Aprovado por	Diretoria ZanderTek

Histórico de Revisões

Versão	Data	Descrição	Responsável
1.0	26/04/2026	Criação inicial da política	Diretoria

Sumário

1. OBJETIVO.....	4
2. ESCOPO.....	4
3. PRINCÍPIOS DE CRIPTOGRAFIA.....	4
4. CRIPTOGRAFIA DE DADOS EM TRÂNSITO	4
5. CRIPTOGRAFIA DE DADOS EM ARMAZENAMENTO	4
6. GESTÃO DE CREDENCIAIS E CHAVES.....	4
7. USO DE CRIPTOGRAFIA EM FERRAMENTAS E SERVIÇOS	5
8. INTEGRAÇÃO COM OUTRAS POLÍTICAS	5
9. RESPONSABILIDADES	5

1. OBJETIVO

Estabelecer diretrizes para o uso de criptografia na proteção de dados da ZanderTek, garantindo a confidencialidade e integridade das informações durante seu armazenamento e transmissão.

2. ESCOPO

Esta política aplica-se a:

- Dados armazenados e transmitidos pela ZanderTek
 - Sistemas e aplicações utilizados pela empresa
 - Colaboradores, sócios, diretores e terceiros que tratem informações
-

3. PRINCÍPIOS DE CRIPTOGRAFIA

O uso de criptografia deve observar:

- Proteção de dados conforme sua criticidade
- Uso de mecanismos de criptografia reconhecidos e adequados
- Aplicação proporcional ao risco e ao contexto
- Compatibilidade com o ambiente tecnológico adotado

A adoção de criptografia deve ser realizada de forma compatível com a realidade operacional da organização, priorizando soluções já disponíveis nos sistemas utilizados.

4. CRIPTOGRAFIA DE DADOS EM TRÂNSITO

Sempre que possível, os dados devem ser protegidos durante sua transmissão por meio de mecanismos seguros, incluindo:

- Uso de protocolos seguros de comunicação
 - Evitar transmissão de dados sensíveis por canais não protegidos
 - Verificação de segurança em conexões externas
-

5. CRIPTOGRAFIA DE DADOS EM ARMAZENAMENTO

A proteção de dados armazenados deve considerar:

- Uso de mecanismos de proteção compatíveis com a criticidade dos dados
 - Proteção adicional para dados classificados como confidenciais ou restritos
 - Avaliação do ambiente onde os dados estão armazenados
-

6. GESTÃO DE CREDENCIAIS E CHAVES

O acesso a dados protegidos deve considerar:

- Proteção de credenciais utilizadas para acesso
- Uso adequado de mecanismos de autenticação
- Restrição de acesso a informações sensíveis

Quando aplicável, mecanismos de proteção de chaves devem ser adotados de forma compatível com o ambiente tecnológico.

7. USO DE CRIPTOGRAFIA EM FERRAMENTAS E SERVIÇOS

A utilização de ferramentas e serviços deve considerar:

- A adoção de mecanismos de proteção de dados disponíveis
- Avaliação de riscos associados ao uso de serviços externos
- Compatibilidade com os requisitos de segurança da organização

8. INTEGRAÇÃO COM OUTRAS POLÍTICAS

Esta política deve ser aplicada em conjunto com:

- Política de Controle de Acesso (ZDT-PCA-001)
- Política de Proteção de Dados (ZDT-PPD-001)
- Política de Segurança de Endpoints (ZDT-PSE-001)

9. RESPONSABILIDADES

Diretoria

- Definir diretrizes de uso de criptografia
- Avaliar riscos associados

Colaboradores

- Utilizar mecanismos seguros de proteção de dados
- Evitar exposição de informações sensíveis

Terceiros

- Adotar práticas adequadas de proteção de dados
- Cumprir requisitos de segurança estabelecidos