



Política de Segurança de Endpoints

Controle do Documento

Campo	Descrição
Título	Política de Segurança de Endpoints
Código do Documento	ZDT-PSE-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 SEGURANÇA DE ENDPOINTS	4
4.	CONTROLE DE ACESSO AOS DISPOSTIVOS.....	4
5.	PROTEÇÃO DOS DISPOSITIVOS	4
6.	USO DOS DISPOSITIVOS PESSOAIS (BYOD)	4
7.	ARMAZENAMENTO DE INFORMAÇÕES EM DISPOSITIVOS	5
8.	PERDA OU ROUBO DE DISPOSITIVOS.....	5
9.	ACESSO REMOTO	5
10.	INTEGRAÇÃO COM OUTRAS POLÍTICAS	5
11.	RESPONSABILIDADES	5

1. OBJETIVO

Estabelecer diretrizes para a proteção de dispositivos utilizados para acesso a sistemas e informações da ZanderTek, reduzindo riscos relacionados a acesso não autorizado, perda de dados e comprometimento de ativos.

2. ESCOPO

Esta política aplica-se a:

- Dispositivos corporativos e pessoais utilizados para acesso a sistemas da ZanderTek
 - Computadores, notebooks, dispositivos móveis e similares
 - Colaboradores, sócios, diretores e terceiros que utilizem tais dispositivos
-

3. PRINCÍPIOS DE SEGURANÇA DE ENDPOINTS

A proteção de endpoints deve observar:

- Uso responsável dos dispositivos
 - Proteção contra acesso não autorizado
 - Atualização e manutenção adequadas
 - Compatibilidade com o ambiente tecnológico adotado
-

4. CONTROLE DE ACESSO AOS DISPOSITIVOS

Os dispositivos devem:

- Estar protegidos por autenticação (senha, biometria ou equivalente)
 - Ser utilizados apenas por pessoas autorizadas
 - Ter bloqueio automático após período de inatividade, quando possível
-

5. PROTEÇÃO DOS DISPOSITIVOS

Os dispositivos devem adotar práticas mínimas de segurança, incluindo:

- Uso de mecanismos de proteção contra software malicioso
 - Atualização regular de sistemas e aplicações
 - Proteção contra instalação de softwares não confiáveis
-

6. USO DOS DISPOSITIVOS PESSOAIS (BYOD)

O uso de dispositivos pessoais é permitido, desde que:

- Sejam adotadas práticas adequadas de segurança
- Não haja armazenamento indevido de informações sensíveis
- O acesso a sistemas ocorra de forma segura

7. ARMAZENAMENTO DE INFORMAÇÕES EM DISPOSITIVOS

O armazenamento de dados em dispositivos deve:

- Respeitar a classificação da informação
- Evitar armazenamento desnecessário de dados sensíveis
- Adotar medidas de proteção compatíveis com a criticidade dos dados

8. PERDA OU ROUBO DE DISPOSITIVOS

Em caso de perda, roubo ou comprometimento de dispositivos:

- O incidente deve ser reportado imediatamente
- Devem ser adotadas medidas para proteção das informações
- O acesso aos sistemas deve ser revogado ou protegido, quando aplicável

9. ACESSO REMOTO

O acesso remoto a sistemas da ZanderTek deve:

- Ser realizado de forma segura
- Utilizar credenciais protegidas
- Considerar riscos associados ao ambiente de acesso

10. 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 Gestão de Incidentes (ZDT-PGI-001)

11. RESPONSABILIDADES

Diretoria

- Definir diretrizes de segurança de endpoints
- Avaliar riscos associados

Colaboradores

- Utilizar dispositivos de forma segura
- Proteger informações e acessos
- Reportar incidentes ou riscos

Terceiros

- Seguir requisitos de segurança aplicáveis
- Proteger dispositivos utilizados