



Política de Controle de Acesso

Controle do Documento

Campo	Descrição
Título	Política de Controle de Acesso
Código do Documento	ZDT-PCA-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 CONTROLE DE ACESSO	4
4.	TIPOS DE ACESSO	4
5.	CONCESSÃO DE ACESSOS.....	4
6.	AUTENTICAÇÃO	5
7.	GESTÃO DE ACESSOS PRIVILEGIADOS.....	5
8.	REVISÃO DE ACESSOS	5
9.	REVOGAÇÃO DE ACESSOS	5
10.	ACESSO DE TERCEIROS.....	5
11.	ACESSO REMOTO E DISPOSITIVOS	6
12.	RESPONSABILIDADES	6

1. OBJETIVO

Estabelecer diretrizes para o controle de acesso a sistemas, informações e recursos tecnológicos da ZanderTek, garantindo que o acesso seja concedido de forma segura, controlada e alinhada às necessidades do negócio.

2. ESCOPO

Esta política aplica-se a:

- Todos os colaboradores, sócios e diretores
 - Terceiros e parceiros com acesso a sistemas ou informações
 - Todos os sistemas, aplicações e ambientes utilizados pela ZanderTek
-

3. PRINCÍPIOS DE CONTROLE DE ACESSO

O controle de acesso deve observar os seguintes princípios:

- Concessão baseada na necessidade de negócio
- Aplicação do menor privilégio
- Identificação individual de usuários
- Rastreabilidade de acessos
- Revogação oportuna de acessos

As diretrizes desta política devem ser aplicadas de forma compatível com a arquitetura tecnológica adotada pela ZanderTek, incluindo ambientes baseados em soluções comerciais ou de código aberto.

4. TIPOS DE ACESSO

Os acessos devem ser concedidos de acordo com sua finalidade, podendo incluir:

- Acesso de usuário padrão
- Acesso administrativo ou privilegiado
- Acesso de terceiros ou parceiros

A concessão deve considerar o nível de risco associado a cada tipo de acesso.

5. CONCESSÃO DE ACESSOS

O acesso a sistemas e informações deve:

- Ser previamente autorizado pela Diretoria
- Ser concedido com base na função desempenhada
- Ser individual e intransferível
- Ser registrado de forma que permita verificação posterior

6. AUTENTICAÇÃO

A ZanderTek adota práticas seguras de autenticação, incluindo:

- Uso de credenciais individuais
- Adoção de autenticação multifator (MFA) sempre que disponível
- Proibição de compartilhamento de credenciais
- Utilização de mecanismos de autenticação considerados seguros e compatíveis com o ambiente tecnológico adotado

7. GESTÃO DE ACESSOS PRIVILEGIADOS

Os acessos privilegiados devem ser:

- Restritos a usuários autorizados
- Concedidos apenas quando necessário
- Utilizados de forma controlada
- Revistos com maior atenção devido ao seu nível de risco

8. REVISÃO DE ACESSOS

Os acessos devem ser revisados periodicamente ou sempre que houver:

- Mudança de função
- Encerramento de vínculo
- Alterações relevantes em sistemas

A revisão deve considerar a necessidade real de manutenção dos acessos.

9. REVOGAÇÃO DE ACESSOS

O acesso deve ser revogado de forma oportuna quando:

- Não houver mais necessidade de utilização
- Houver desligamento de colaboradores ou terceiros
- For identificado uso indevido ou risco associado

10. ACESSO DE TERCEIROS

O acesso concedido a terceiros deve:

- Ser limitado ao necessário
- Ser autorizado previamente
- Ser controlado e revisado
- Ser revogado ao término da necessidade

11. ACESSO REMOTO E DISPOSITIVOS

O acesso a sistemas da ZanderTek pode ocorrer remotamente, desde que:

- Seja realizado por meio de conexões seguras
- As credenciais sejam devidamente protegidas
- Sejam adotadas práticas mínimas de segurança nos dispositivos utilizados compatíveis com o ambiente tecnológico da organização

12. RESPONSABILIDADES

Diretoria

- Autorizar acessos relevantes
- Avaliar riscos relacionados ao controle de acessos

Colaboradores

- Utilizar os acessos de forma adequada
- Proteger suas credenciais
- Reportar qualquer uso indevido

Terceiros

- Utilizar os acessos conforme autorizado
- Proteger informações e credenciais
- Cumprir requisitos de segurança