



Política de Segurança de Terceiros

Controle do Documento

Campo	Descrição
Título	Política de Segurança de Terceiros
Código do Documento	ZDT-PST-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. DEFINIÇÃO DE TERCEIROS.....	4
4. PRINCÍPIOS DE SEGURANÇA PARA TERCEIROS.....	4
5. AVALIAÇÃO DE TERCEIROS.....	4
6. REQUISITOS DE SEGURANÇA	5
7. GESTÃO DE ACESSO DE TERCEIROS.....	5
8. COMPARTILHAMENTO DE INFORMAÇÕES.....	6
9. MONITORAMENTO E REVISÃO	6
10. ENCERRAMENTO DE RELACIONAMENTO	6
11. CONFORMIDADE E OBRIGAÇÕES CONTRATUAIS	6
12. RESPONSABILIDADES.....	6

1. OBJETIVO

Estabelecer diretrizes para a gestão de riscos associados a terceiros que tenham acesso a informações, sistemas ou recursos da ZanderTek, garantindo que tais relações ocorram de forma segura, controlada e alinhada às melhores práticas de segurança da informação.

2. ESCOPO

Esta política aplica-se a todos os terceiros que, de alguma forma, interajam com a ZanderTek, e tenham acesso a informações ou sistemas, incluindo:

- Fornecedores de tecnologia
- Prestadores de serviço
- Parceiros comerciais e operacionais
- Revendedores (canais)
- Fabricantes e provedores de soluções

Aplica-se também a colaboradores envolvidos na contratação, gestão e relacionamento com terceiros.

3. DEFINIÇÃO DE TERCEIROS

Para fins desta política, consideram-se terceiros todas as entidades externas à ZanderTek que possuam algum nível de interação com a organização, especialmente quando envolvem:

- Acesso a sistemas
 - Tratamento de informações
 - Integração tecnológica
 - Atuação conjunta em projetos
-

4. PRINCÍPIOS DE SEGURANÇA PARA TERCEIROS

A gestão de terceiros deve observar os seguintes princípios:

- Acesso limitado ao mínimo necessário
 - Proteção das informações compartilhadas
 - Responsabilidade compartilhada na segurança
 - Conformidade com requisitos legais e contratuais
 - Avaliação proporcional ao risco envolvido
-

5. AVALIAÇÃO DE TERCEIROS

A ZanderTek realiza avaliação de terceiros de forma proporcional ao nível de risco envolvido, considerando fatores como:

- Tipo de acesso a sistemas ou informações
- Sensibilidade dos dados envolvidos

- Criticidade do serviço prestado
- Dependência operacional da ZanderTek em relação ao terceiro

Sempre que aplicável, a avaliação poderá considerar:

- A existência de práticas mínimas de segurança da informação
- O nível de maturidade do terceiro em relação à proteção de dados
- Reputação e histórico do terceiro no mercado
- A aderência a requisitos contratuais e regulatórios aplicáveis

Para terceiros com maior nível de risco, a ZanderTek poderá adotar medidas adicionais, tais como:

- Solicitação de informações sobre práticas de segurança
- Formalização de requisitos específicos em contrato
- Limitação do escopo de acesso a sistemas e informações

A avaliação de terceiros deve ser conduzida de forma pragmática, priorizando os riscos mais relevantes e evitando a adoção de processos excessivamente burocráticos.

6. REQUISITOS DE SEGURANÇA

Os terceiros devem cumprir requisitos mínimos de segurança da informação, compatíveis com o nível de acesso concedido e com a criticidade das atividades desempenhadas.

De forma geral, espera-se que os terceiros:

- Protejam adequadamente as informações acessadas, evitando divulgação ou uso indevido
- Utilizem as informações exclusivamente para os fins acordados
- Adotem práticas seguras no acesso a sistemas, incluindo proteção de credenciais
- Respeitem os níveis de classificação da informação definidos pela ZanderTek
- Cumpram obrigações contratuais relacionadas à confidencialidade e segurança

Quando aplicável, a ZanderTek poderá exigir requisitos adicionais, tais como:

- Uso de mecanismos de autenticação segura
- Restrição de acesso a ambientes específicos
- Adoção de medidas de proteção para dados sensíveis
- Reporte de incidentes de segurança que possam impactar a organização ou seus clientes

Os requisitos de segurança devem ser definidos de forma proporcional ao risco e ao contexto de uso, evitando a imposição de controles desnecessários ou incompatíveis com a realidade operacional.

7. GESTÃO DE ACESSO DE TERCEIROS

O acesso concedido a terceiros deve:

- Ser previamente autorizado
- Ser limitado ao necessário para execução das atividades
- Ser individual e controlado sempre que aplicável
- Ser revogado quando não houver mais necessidade

8. COMPARTILHAMENTO DE INFORMAÇÕES

O compartilhamento de informações com terceiros deve:

- Respeitar a classificação da informação definida pela ZanderTek
- Ser limitado ao necessário para execução das atividades
- Garantir que as informações sejam protegidas de forma adequada
- Observar requisitos contratuais e regulatórios aplicáveis

9. MONITORAMENTO E REVISÃO

A ZanderTek poderá realizar revisões periódicas das relações com terceiros, considerando:

- Continuidade da necessidade de acesso
- Nível de risco associado
- Adequação das práticas de segurança

10. ENCERRAMENTO DE RELACIONAMENTO

Ao término do relacionamento com terceiros, devem ser adotadas medidas para:

- Revogação de acessos concedidos
- Interrupção do compartilhamento de informações
- Garantia de descarte ou devolução de dados, quando aplicável

11. CONFORMIDADE E OBRIGAÇÕES CONTRATUAIS

As relações com terceiros devem observar:

- Cláusulas contratuais de confidencialidade
- Requisitos de segurança estabelecidos por clientes
- Obrigações legais e regulatórias aplicáveis

Quando necessário, poderão ser adotados requisitos adicionais para atendimento a demandas específicas.

12. RESPONSABILIDADES

Diretoria

- Definir diretrizes e aprovar relações relevantes
- Avaliar riscos associados a terceiros

Colaboradores

- Seguir as diretrizes desta política
- Garantir uso adequado das informações
- Reportar riscos ou incidentes relacionados a terceiros

Terceiros

- Cumprir requisitos de segurança estabelecidos
- Proteger as informações acessadas
- Reportar incidentes ou falhas de segurança