



Política de Proteção de Dados

Controle do Documento

Campo	Descrição
Título	Política de Proteção de Dados
Código do Documento	ZDT-PPD-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 PROTEÇÃO DE DADOS.....	4
4.	CLASSIFICAÇÃO DOS DADOS	4
5.	TRATAMENTO DE DADOS.....	4
6.	ARMAZENAMENTO DE DADOS.....	5
7.	COMPARTILHAMENTO DE DADOS	5
8.	RETENÇÃO E DESCARTE DE DADOS	5
9.	PROTEÇÃO DE DADOS EM AMBIENTES DE TERCEIROS	5
10.	USO DE DADOS EM TECNOLOGIAS EMERGENTES.....	6
11.	INCIDENTES RELACIONADOS A DADOS	6
12.	CONFORMIDADE LEGAL	6
13.	RESPONSABILIDADES	6

1. OBJETIVO

Estabelecer diretrizes para o tratamento, proteção e uso adequado de dados sob responsabilidade da ZanderTek, garantindo sua segurança ao longo de todo o ciclo de vida e o atendimento a requisitos legais, regulatórios e contratuais aplicáveis.

2. ESCOPO

Esta política aplica-se a:

- Todos os dados tratados pela ZanderTek, incluindo dados próprios, de clientes e de parceiros
 - Todos os colaboradores, sócios e diretores
 - Terceiros que tenham acesso ou realizem tratamento de dados em nome da ZanderTek
 - Todos os sistemas, aplicações e ambientes utilizados para armazenamento ou processamento de dados
-

3. PRINCÍPIOS DE PROTEÇÃO DE DADOS

A proteção de dados deve observar os seguintes princípios:

- Uso de dados conforme finalidade definida
 - Acesso restrito conforme necessidade de negócio
 - Proteção adequada de acordo com a sensibilidade dos dados
 - Responsabilidade no tratamento de informações
 - Conformidade com requisitos legais e contratuais
-

4. CLASSIFICAÇÃO DOS DADOS

Os dados devem ser classificados de acordo com os níveis definidos na Política de Segurança da Informação da ZanderTek, considerando seu grau de sensibilidade e impacto para o negócio.

A classificação deve ser realizada no momento da criação ou recebimento dos dados, sendo responsabilidade de quem os gera ou gerencia.

A classificação orienta o tratamento dos dados ao longo de todo o seu ciclo de vida, incluindo:

- Controle de acesso
- Armazenamento
- Compartilhamento
- Retenção e descarte

Quando houver dúvida quanto à classificação adequada, deve-se adotar o nível mais restritivo até que a classificação seja definida de forma apropriada.

5. TRATAMENTO DE DADOS

O tratamento de dados deve:

- Ser realizado apenas para finalidades legítimas e relacionadas às atividades da organização

- Limitar-se ao mínimo necessário para execução das atividades
 - Ser conduzido de forma a garantir a proteção contra acesso não autorizado, perda ou alteração indevida
-

6. ARMAZENAMENTO DE DADOS

Os dados devem ser armazenados de forma segura, considerando:

- A proteção contra acesso não autorizado
- A integridade das informações
- A disponibilidade quando necessário

Os mecanismos de armazenamento devem ser compatíveis com a criticidade dos dados e com o ambiente tecnológico adotado pela organização. Podem ainda incluir soluções comerciais ou de código aberto, desde que atendam aos requisitos de segurança compatíveis com a criticidade dos dados tratados.

Sempre que aplicável, devem ser adotadas medidas de segregação lógica de dados, de forma a reduzir riscos de acesso indevido.

7. COMPARTILHAMENTO DE DADOS

O compartilhamento de dados deve:

- Ser realizado apenas quando necessário para o negócio
- Respeitar a classificação da informação
- Garantir que terceiros adotem práticas adequadas de proteção
- Observar requisitos contratuais e regulatórios aplicáveis

Dados sensíveis ou confidenciais não devem ser compartilhados sem avaliação adequada e autorização quando aplicável. O compartilhamento de dados pode ocorrer por meio de diferentes plataformas tecnológicas, desde que sejam adotadas práticas adequadas de proteção da informação.

8. RETENÇÃO E DESCARTE DE DADOS

Os dados devem ser mantidos apenas pelo período necessário para atendimento de suas finalidades, requisitos legais ou obrigações contratuais.

Após esse período, devem ser descartados de forma segura, evitando acesso indevido ou recuperação não autorizada.

9. PROTEÇÃO DE DADOS EM AMBIENTES DE TERCEIROS

O tratamento de dados por terceiros deve:

- Seguir as diretrizes estabelecidas pela ZanderTek
- Ser limitado ao necessário para execução das atividades
- Garantir a proteção adequada das informações

A ZanderTek deve assegurar que terceiros que tratem dados em seu nome estejam sujeitos a obrigações contratuais compatíveis com esta política.

10. USO DE DADOS EM TECNOLOGIAS EMERGENTES

O uso de dados em tecnologias emergentes, incluindo Inteligência Artificial, deve:

- Respeitar a classificação e sensibilidade dos dados
 - Evitar o uso de dados confidenciais em ambientes não autorizados
 - Considerar riscos associados ao processamento externo de informações
-

11. INCIDENTES RELACIONADOS A DADOS

Incidentes que envolvam dados, incluindo perda, acesso não autorizado, alteração indevida ou exposição não autorizada, devem ser tratados de forma adequada e tempestiva.

Tais incidentes devem ser reportados e tratados conforme as diretrizes estabelecidas na Política de Gestão de Incidentes da ZanderTek.

Quando aplicável, devem ser adotadas medidas para:

- Conter o incidente e minimizar impactos
 - Avaliar os riscos associados
 - Comunicar as partes envolvidas, conforme requisitos legais ou contratuais
 - Implementar ações corretivas para evitar recorrência
-

12. CONFORMIDADE LEGAL

A ZanderTek compromete-se a observar as legislações aplicáveis relacionadas à proteção de dados, incluindo a Lei Geral de Proteção de Dados (LGPD), quando aplicável.

13. RESPONSABILIDADES

Diretoria

- Definir diretrizes de proteção de dados
- Avaliar riscos associados ao tratamento de dados

Colaboradores

- Tratar dados de forma adequada
- Respeitar classificação e restrições de uso
- Reportar incidentes ou riscos

Terceiros

- Cumprir requisitos de proteção de dados
- Utilizar dados conforme autorizados
- Garantir segurança das informações