



Política de Backup e Recuperação

Controle do Documento

Campo	Descrição
Título	Política de Backup e Recuperação
Código do Documento	ZDT-PBR-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 BACKUP E RECUPERAÇÃO	4
4.	REALIZAÇÃO DE BACKUPS	4
5.	ARMAZENAMENTO DE BACKUPS	4
6.	RECUPERAÇÃO DE DADOS	5
7.	TESTES DE RECUPERAÇÃO.....	5
8.	RETENÇÃO DE BACKUPS.....	5
9.	INTEGRAÇÃO COM GESTÃO DE INCIDENTES	5
10.	MONITORAMENTO E REVISÃO.....	5
11.	RESPONSABILIDADES	6

1. OBJETIVO

Estabelecer diretrizes para a proteção, backup e recuperação de dados da ZanderTek, garantindo a disponibilidade das informações e a continuidade das operações em caso de falhas, incidentes ou perda de dados.

2. ESCOPO

Esta política aplica-se a:

- Dados corporativos, operacionais e de clientes sob responsabilidade da ZanderTek
 - Sistemas e ambientes utilizados para armazenamento de dados
 - Colaboradores e terceiros envolvidos no tratamento de informações
-

3. PRINCÍPIOS DE BACKUP E RECUPERAÇÃO

As práticas de backup devem observar os seguintes princípios:

- Proteção dos dados conforme sua criticidade
 - Garantia de recuperação em caso de necessidade
 - Adoção de mecanismos compatíveis com o ambiente tecnológico
 - Simplicidade e efetividade na implementação
-

4. REALIZAÇÃO DE BACKUPS

Os dados considerados relevantes para a operação devem ser protegidos por mecanismos de backup, considerando:

- A criticidade dos dados
- A necessidade de recuperação
- A frequência adequada ao contexto de uso

Os backups devem ser realizados de forma a reduzir o risco de perda de informações. A definição dos dados a serem protegidos por backup deve considerar sua classificação e criticidade, conforme estabelecido na Política de Proteção de Dados da ZanderTek. A criticidade dos dados deve ser avaliada com base na classificação da informação definida na Política de Segurança da Informação.

5. ARMAZENAMENTO DE BACKUPS

Os backups devem ser armazenados de forma segura, considerando:

- Proteção contra acesso não autorizado
- Redução de risco de perda ou corrupção
- Uso de soluções compatíveis com o ambiente tecnológico adotado, incluindo soluções comerciais ou de código aberto

6. RECUPERAÇÃO DE DADOS

A ZanderTek deve ser capaz de recuperar dados relevantes em caso de incidentes ou falhas, priorizando:

- Dados classificados como críticos ou sensíveis
- Sistemas essenciais para o negócio
- Continuidade das operações

A recuperação deve considerar a ordem de prioridade definida com base no impacto para o negócio.

7. TESTES DE RECUPERAÇÃO

Sempre que aplicável, devem ser realizados testes de recuperação de dados, com o objetivo de:

- Validar a efetividade dos backups
- Identificar possíveis falhas
- Garantir a capacidade de recuperação

Os testes devem ser realizados de forma proporcional à criticidade dos sistemas e dados. A realização de testes pode variar conforme a criticidade dos dados e sistemas, sendo priorizados os ambientes mais relevantes para o negócio.

8. RETENÇÃO DE BACKUPS

Os backups devem ser mantidos por período compatível com:

- Necessidades operacionais
- Requisitos legais ou contratuais
- Criticidade dos dados

Após o período de retenção, os dados devem ser descartados de forma segura.

9. INTEGRAÇÃO COM GESTÃO DE INCIDENTES

Em caso de incidentes que envolvam perda ou indisponibilidade de dados, os mecanismos de backup e recuperação devem ser utilizados como parte do processo de resposta, conforme definido na Política de Gestão de Incidentes da ZanderTek.

A recuperação de dados deve ser conduzida de forma coordenada com as ações de tratamento de incidentes.

10. MONITORAMENTO E REVISÃO

As práticas de backup e recuperação devem ser revisadas periodicamente, considerando mudanças no ambiente tecnológico, criticidade dos dados e necessidades do negócio.

11. RESPONSABILIDADES

Diretoria

- Definir diretrizes de backup e recuperação
- Priorizar a recuperação de sistemas e dados

Colaboradores

- Garantir o uso adequado dos sistemas e dados
- Reportar falhas ou incidentes relacionados a dados

Terceiros

- Cumprir requisitos de proteção e recuperação de dados quando aplicável