



Política de Segurança da Informação

CONTROLE DO DOCUMENTO

Campo	Descrição
Título	Política de Segurança da Informação
Código do Documento	ZDT-PSI-001
Versão	1.0
Data de Criação	25/04/2026
Última Revisão	25/04/2026
Próxima Revisão	25/04/2027
Responsável	Diretoria
Classificação	Interno
Aprovado por	Diretoria ZanderTek

HISTÓRICO DE REVISÕES

Versão	Data	Descrição	Responsável
1.0	25/04/2026	Criação inicial da política	Diretoria

Tabela de Conteúdo

1.	OBJETIVO	4
2.	ESCOPO.....	4
3.	CONTEXTO ORGANIZACIONAL.....	4
4.	PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO.....	5
5.	GOVERNANÇA E RESPONSABILIDADE	6
6.	GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO	7
7.	GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO	8
8.	CONTROLE DE ACESSO	10
9.	USO DE RECURSOS TECNOLÓGICOS.....	11
10.	SEGURANÇA NO USO DE INTELIGÊNCIA ARTIFICIAL	12
11.	GESTÃO DE INCIDENTES DE SEGURANÇA DE INFROMAÇÃO	13
12.	CONTINUIDADE DE NEGÓCIOS.....	14
13.	MONITORAMENTO E MELHORIA CONTÍNUA	15
14.	CONFORMIDADE	15
15.	SANÇÕES E NÃO CONFORMIDADE	16
16.	REVISÃO E ATUALIZAÇÃO	17

1. OBJETIVO

A Política de Segurança da Informação da ZanderTek tem como objetivo estabelecer as diretrizes, princípios e responsabilidades para a proteção dos ativos de informação da organização, assegurando sua confidencialidade, integridade, disponibilidade e uso adequado.

Esta política visa suportar a continuidade das operações da ZanderTek, reduzir a exposição a riscos relacionados à segurança da informação e garantir o atendimento a requisitos legais, regulatórios e contratuais aplicáveis, especialmente no contexto de relacionamento com clientes corporativos e parceiros estratégicos.

Adicionalmente, a política tem como objetivo orientar a adoção de práticas seguras no uso de tecnologias emergentes, incluindo Inteligência Artificial, promovendo inovação com responsabilidade e alinhamento às melhores práticas de mercado.

2. ESCOPO

Esta política aplica-se a todos os ativos de informação, processos e ambientes tecnológicos sob responsabilidade da ZanderTek, incluindo, mas não se limitando a:

- Sistemas, aplicações e plataformas utilizadas pela organização
- Infraestrutura tecnológica, incluindo dispositivos e redes
- Dados corporativos, operacionais e de clientes
- Informações em formato digital ou físico

Aplica-se também a:

- Todos os colaboradores, sócios e diretores da ZanderTek
- Terceiros, prestadores de serviço e fornecedores que tenham acesso a informações ou sistemas da empresa
- Parceiros de negócios, incluindo revendedores, no que se refere ao acesso ou tratamento de informações compartilhadas

A utilização de recursos e o acesso a informações devem respeitar os limites estabelecidos nesta política e em contratos firmados com clientes, parceiros e fornecedores.

Nos casos em que houver requisitos específicos de clientes ou regulamentações aplicáveis, prevalecerão as condições mais restritivas em relação à proteção da informação.

Esta política é complementada por normas e políticas específicas que detalham os controles e práticas de segurança da informação em áreas como controle de acesso, proteção de dados e gestão de terceiros.

3. CONTEXTO ORGANIZACIONAL

A ZanderTek é uma empresa especializada na curadoria, distribuição e suporte a soluções inovadoras de tecnologia da informação, com foco em Cybersecurity, Inteligência Artificial e Analytics, atuando junto a clientes corporativos de médio e grande porte na América Latina.

Seu modelo de atuação envolve a integração entre fabricantes internacionais de tecnologia, parceiros de negócios (revendedores) e clientes finais, o que implica na gestão e no trânsito de informações sensíveis em diferentes níveis, incluindo dados técnicos, comerciais e operacionais.

Diante desse contexto, a segurança da informação é considerada um elemento estratégico para a operação da ZanderTek, sendo fundamental para:

- Garantir a proteção de informações próprias e de terceiros
- Assegurar a confiança de clientes e parceiros de negócios
- Viabilizar a operação em ambientes corporativos altamente regulados, como instituições financeiras
- Sustentar a continuidade e a resiliência das operações

A natureza das soluções distribuídas pela ZanderTek, especialmente aquelas relacionadas à Cybersecurity e ao uso de Inteligência Artificial, amplia a responsabilidade da organização na adoção de práticas robustas de segurança, tanto em sua operação interna quanto na interação com clientes e parceiros.

Além disso, a empresa reconhece que o uso crescente de tecnologias emergentes, como modelos de Inteligência Artificial e plataformas baseadas em dados, introduz novos vetores de risco, incluindo:

- Exposição indevida de informações sensíveis
- Uso não controlado de ferramentas externas (Shadow IT e Shadow AI)
- Dependência de serviços e infraestruturas de terceiros
- Riscos associados à cadeia de fornecimento de tecnologia

Dessa forma, a ZanderTek adota uma abordagem de segurança da informação baseada em risco, alinhada às melhores práticas de mercado e proporcional ao seu porte e modelo operacional, buscando equilibrar proteção, eficiência operacional e capacidade de inovação.

A arquitetura tecnológica da ZanderTek pode incluir soluções comerciais e de código aberto, sendo as práticas de segurança da informação aplicadas de forma compatível com os ambientes adotados.

4. PRINCÍPIOS DE SEGURANÇA DA INFORMAÇÃO

A ZanderTek adota um conjunto de princípios que orientam a proteção de seus ativos de informação e a condução de suas atividades, servindo como base para a definição de controles, processos e decisões relacionadas à segurança da informação.

4.1 Confidencialidade

As informações devem ser acessadas apenas por pessoas autorizadas, sendo protegidas contra divulgação indevida ou não autorizada, especialmente no contexto de dados de clientes, parceiros e informações estratégicas da organização.

4.2 Integridade

As informações devem ser mantidas íntegras, completas e consistentes ao longo de todo o seu ciclo de vida, garantindo que não sejam alteradas de forma indevida, acidental ou maliciosa.

4.3 Disponibilidade

As informações e os sistemas devem estar disponíveis para uso sempre que necessário, dentro dos níveis acordados com clientes e definidos internamente, assegurando a continuidade das operações.

4.4 Responsabilidade

Todos os colaboradores, parceiros e terceiros que tenham acesso às informações da ZanderTek são responsáveis por sua proteção e uso adequado, de acordo com as diretrizes estabelecidas nesta política e em normas complementares.

4.5 Rastreabilidade

As ações realizadas sobre sistemas e informações devem ser registradas e passíveis de auditoria, permitindo a identificação de usuários, atividades e eventos relevantes para a segurança da informação.

4.6 Princípio do Menor Privilégio

O acesso a sistemas e informações deve ser concedido com base na necessidade de negócio, limitando-se ao mínimo necessário para a execução das atividades de cada usuário.

4.7 Segurança por Design e por Padrão

A segurança da informação deve ser considerada desde a concepção de processos, sistemas e integrações, sendo aplicada de forma preventiva e não apenas reativa, com configurações seguras definidas como padrão.

4.8 Gestão Baseada em Risco

As decisões relacionadas à segurança da informação devem considerar a identificação, análise e priorização de riscos, garantindo que os esforços de proteção sejam proporcionais ao impacto potencial para o negócio.

4.9 Segurança em Ecossistemas e Terceiros

Considerando o modelo de atuação da ZanderTek, a segurança deve abranger não apenas o ambiente interno, mas também as interações com parceiros, fornecedores e clientes, assegurando que o compartilhamento de informações ocorra de forma controlada e segura. As relações com terceiros devem observar diretrizes específicas de segurança da informação, conforme definido em política dedicada.

4.10 Segurança no Uso de Tecnologias Emergentes

O uso de tecnologias emergentes, incluindo Inteligência Artificial, deve ser conduzido com responsabilidade, considerando riscos associados à exposição de dados, tomada de decisão automatizada e uso de serviços externos. A ZanderTek é uma empresa especializada na curadoria, distribuição e suporte a soluções inovadoras de tecnologia da informação, com foco em Cybersecurity, Inteligência Artificial e Analytics, atuando junto a clientes corporativos de médio e grande porte na América Latina.

5. GOVERNANÇA E RESPONSABILIDADE

A governança de segurança da informação na ZanderTek é estruturada de forma proporcional ao porte da organização e alinhada às suas necessidades operacionais e estratégicas, sendo conduzida pela Diretoria.

A Diretoria é responsável por estabelecer as diretrizes de segurança da informação, assegurar a implementação desta política e promover a proteção dos ativos de informação da organização.

5.1 Responsabilidades da Diretoria

Compete à Diretoria da ZanderTek:

- Definir e aprovar a Política de Segurança da Informação e suas atualizações
- Garantir que práticas de segurança estejam integradas às operações da empresa
- Avaliar e priorizar riscos relacionados à segurança da informação
- Assegurar que existam recursos adequados para a proteção das informações
- Deliberar sobre incidentes relevantes e suas tratativas
- Promover a cultura de segurança da informação na organização

5.2 Responsabilidades dos Colaboradores

Todos os colaboradores da ZanderTek são responsáveis por:

- Cumprir esta política e demais normas relacionadas à segurança da informação
- Proteger as informações sob sua responsabilidade
- Utilizar os recursos tecnológicos de forma adequada e segura
- Reportar incidentes, falhas ou suspeitas de segurança
- Preservar a confidencialidade das informações, inclusive após eventual desligamento

5.3 Responsabilidades de Terceiros e Parceiros

Terceiros, fornecedores e parceiros de negócios que tenham acesso a informações ou sistemas da ZanderTek devem:

- Cumprir os requisitos de segurança definidos pela organização
- Utilizar as informações exclusivamente para os fins acordados
- Adotar práticas adequadas de proteção de dados e informações
- Reportar incidentes de segurança que possam impactar a ZanderTek ou seus clientes

O acesso de terceiros às informações e sistemas deve ser formalizado e controlado por meio de contratos ou acordos específicos.

5.4 Responsável pela Segurança da Informação

A responsabilidade pela coordenação das atividades de segurança da informação é atribuída à Diretoria da ZanderTek, podendo ser delegada, total ou parcialmente, a colaboradores ou terceiros conforme a evolução da estrutura organizacional.

5.5 Segregação de Funções

Sempre que aplicável, a ZanderTek buscará adotar práticas de segregação de funções, de forma a reduzir riscos associados a conflitos de interesse, erros ou atividades não autorizadas. adota um conjunto de princípios que orientam a proteção de seus ativos de

6. GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

A ZanderTek adota uma abordagem de gestão de riscos de segurança da informação baseada na identificação, análise e tratamento de riscos que possam impactar seus ativos de informação, suas operações e seus compromissos com clientes e parceiros.

A gestão de riscos é conduzida de forma proporcional ao porte da organização e alinhada às suas necessidades operacionais, buscando equilibrar proteção, eficiência e capacidade de inovação.

6.1 Identificação de Riscos

A ZanderTek busca identificar riscos relacionados à segurança da informação considerando, entre outros fatores:

- A natureza de suas operações e modelo de negócios
- O uso de tecnologias e sistemas utilizados
- O acesso e tratamento de informações sensíveis
- A interação com terceiros, parceiros e fornecedores
- A adoção de tecnologias emergentes, incluindo Inteligência Artificial

6.2 Análise e Avaliação de Riscos

Os riscos identificados são avaliados com base em critérios qualitativos, considerando:

- Potencial impacto para o negócio
- Probabilidade de ocorrência
- Consequências para clientes, parceiros e operações

A priorização dos riscos visa direcionar os esforços de proteção para os cenários de maior criticidade.

6.3 Tratamento de Riscos

A ZanderTek define ações para tratamento dos riscos identificados, que podem incluir:

- Implementação de controles de segurança
- Ajustes em processos ou práticas operacionais
- Restrição ou limitação de determinadas atividades
- Aceitação consciente do risco, quando aplicável

As decisões relacionadas ao tratamento de riscos são conduzidas pela Diretoria.

6.4 Monitoramento e Revisão

Os riscos devem ser revisados periodicamente ou sempre que houver mudanças relevantes, tais como:

- Adoção de novas tecnologias
- Início de novos projetos ou parcerias
- Alterações no ambiente operacional
- Ocorrência de incidentes de segurança

6.5 Integração com Clientes e Terceiros

Sempre que aplicável, a gestão de riscos deve considerar requisitos específicos de clientes e parceiros, especialmente em ambientes regulados, podendo demandar a adoção de controles adicionais ou alinhamento a políticas externas. A governança de segurança da informação na ZanderTek é estruturada de forma proporcional ao porte da organização e alinhada às suas necessidades operacionais e estratégicas, sendo conduzida pela

7. CLASSIFICAÇÃO DA INFORMAÇÃO

A ZanderTek estabelece um modelo de classificação da informação com o objetivo de garantir que os dados sejam protegidos de forma adequada ao seu nível de sensibilidade, criticidade e impacto para o negócio.

A classificação da informação deve orientar seu armazenamento, acesso, compartilhamento e descarte, sendo aplicada a todas as informações sob responsabilidade da organização, independentemente de seu formato.

7.1 Níveis de Classificação

As informações devem ser classificadas nos seguintes níveis:

Pública

Informações que podem ser divulgadas sem restrições, não causando impacto à organização, clientes ou parceiros.

Exemplos:

- Conteúdos institucionais públicos
- Materiais de marketing aprovados

Interna

Informações destinadas ao uso interno da ZanderTek, cujo acesso deve ser restrito a colaboradores e pessoas autorizadas.

Exemplos:

- Documentos operacionais
- Comunicações internas
- Processos e rotinas

Confidencial

Informações sensíveis que devem ser acessadas apenas por pessoas autorizadas, podendo causar impacto relevante em caso de divulgação indevida.

Exemplos:

- Dados de clientes
- Informações comerciais e estratégicas
- Contratos
- Propostas comerciais

Restrita

Informações altamente sensíveis e críticas, cujo acesso deve ser rigorosamente controlado, podendo causar impacto significativo para a organização ou terceiros em caso de exposição.

Exemplos:

- Informações financeiras sensíveis
- Credenciais de acesso e segredos técnicos
- Dados protegidos por requisitos regulatórios específicos

7.2 Responsabilidade pela Classificação

A classificação da informação deve ser realizada pelos responsáveis pela sua criação ou gestão, com base nos critérios definidos nesta política.

A Diretoria pode estabelecer orientações adicionais sempre que necessário.

7.3 Regras Gerais de Tratamento

De acordo com sua classificação, as informações devem seguir diretrizes gerais, incluindo:

- Restrição de acesso conforme necessidade de negócio
- Proteção contra acesso não autorizado
- Uso adequado de mecanismos de armazenamento e compartilhamento
- Adoção de medidas adicionais de proteção para informações confidenciais e restritas

7.4 Compartilhamento de Informações

O compartilhamento de informações deve respeitar:

- O nível de classificação atribuído
- A necessidade de negócio
- Os acordos contratuais com clientes, parceiros e fornecedores

Informações classificadas como confidenciais ou restritas não devem ser compartilhadas sem autorização adequada.

7.5 Armazenamento e Descarte

As informações devem ser armazenadas e descartadas de forma segura, considerando sua classificação e criticidade, evitando acesso indevido, perda ou exposição não autorizada.

8. CONTROLE DE ACESSO

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

O acesso deve ser baseado no princípio do menor privilégio, sendo concedido apenas na medida necessária para o desempenho das atividades de cada usuário. O acesso a sistemas e informações deve ser controlado com base na necessidade de negócio, com uso de mecanismos de autenticação seguros e, sempre que possível, autenticação multifator, conforme detalhado em política específica.

8.1 Concessão de Acesso

O acesso a sistemas e informações deve:

- Ser concedido com base na função e necessidade de negócio
- Ser previamente autorizado pela Diretoria ou responsável designado
- Ser individual e intransferível
- Ser concedido de forma controlada e passível de verificação

8.2 Autenticação

A ZanderTek adota práticas de autenticação seguras, incluindo:

- Uso de credenciais individuais
- Utilização de autenticação multifator (MFA) sempre que disponível
- Proibição de compartilhamento de credenciais
- Utilização de mecanismos de autenticação considerados seguros

8.3 Revisão de Acessos

Os acessos concedidos devem ser revisados periodicamente, ou sempre que houver:

- Mudança de função
- Encerramento de vínculo com colaboradores ou terceiros
- Alterações relevantes em sistemas ou processos

8.4 Revogação de Acesso

O acesso deve ser revogado imediatamente quando:

- Houver desligamento de colaboradores ou término de contrato com terceiros
- O acesso não for mais necessário para as atividades desempenhadas
- Houver identificação de uso indevido ou risco associado

8.5 Acesso de Terceiros

O acesso concedido a terceiros, parceiros ou fornecedores deve:

- Ser limitado ao necessário para execução das atividades contratadas
- Ser formalmente autorizado
- Ser monitorado e revogado ao término da necessidade

8.6 Uso de Dispositivos e Acessos Remotos

O acesso a sistemas e informações deve ser realizado de forma segura, considerando:

- Proteção das credenciais
- Uso adequado de dispositivos
- Adoção de práticas mínimas de segurança no acesso remoto

9. USO DE RECURSOS TECNOLÓGICOS

Os recursos tecnológicos da ZanderTek devem ser utilizados de forma responsável, segura e alinhada aos objetivos do negócio, respeitando as diretrizes desta política e demais normas aplicáveis.

O uso inadequado de sistemas, dispositivos e serviços pode expor a organização a riscos de segurança, operacionais e legais.

9.1 Uso Aceitável

Os usuários devem utilizar os recursos tecnológicos da ZanderTek exclusivamente para fins profissionais e de forma ética, sendo proibido:

- Utilizar sistemas corporativos para atividades ilícitas ou não autorizadas
- Compartilhar informações sem autorização adequada
- Utilizar recursos da empresa de forma que comprometa a segurança da informação

9.2 Uso de E-mail Corporativo

O e-mail corporativo deve ser utilizado de forma segura e responsável, incluindo:

- Evitar o envio de informações sensíveis sem proteção adequada
- Não abrir anexos ou links suspeitos
- Não utilizar o e-mail corporativo para fins não relacionados ao negócio

9.3 Uso de Internet e Sistemas

O acesso à internet e aos sistemas corporativos deve:

- Ser utilizado de forma alinhada às atividades profissionais
- Evitar acesso a conteúdos que representem risco à segurança
- Respeitar as diretrizes de segurança da organização

9.4 Uso de Aplicações e Serviços Externos

A utilização de aplicações externas (SaaS, ferramentas online, plataformas digitais) deve considerar:

- Avaliação prévia quanto ao uso de informações corporativas
- Restrição ao uso de ferramentas não autorizadas para tratamento de dados sensíveis
- Adoção de práticas seguras no compartilhamento de informações

9.5 Uso de Dispositivos

Os dispositivos utilizados para acesso a sistemas e informações da ZanderTek devem:

- Ser utilizados de forma segura e responsável
- Estar protegidos contra acesso não autorizado
- Não ser compartilhados sem controle adequado

10. SEGURANÇA NO USO DE INTELIGÊNCIA ARTIFICIAL

A ZanderTek reconhece o papel crescente das tecnologias de Inteligência Artificial (IA) em suas operações e nos ambientes de seus clientes, adotando diretrizes para garantir seu uso seguro, responsável e alinhado às melhores práticas de mercado.

O uso de IA deve equilibrar inovação e proteção da informação, considerando os riscos associados ao tratamento de dados, à tomada de decisão automatizada e à utilização de serviços externos.

10.1 Princípios para Uso de IA

A utilização de tecnologias de IA na ZanderTek deve observar:

- Proteção da confidencialidade das informações
- Uso responsável e ético das tecnologias
- Transparência no uso de ferramentas quando aplicável
- Avaliação de riscos associados ao uso de IA

10.2 Proteção de Informações

É vedada a inserção de informações classificadas como confidenciais ou restritas em ferramentas de IA que não sejam autorizadas ou que não ofereçam garantias adequadas de proteção de dados.

O uso de IA deve respeitar a classificação da informação e as diretrizes de proteção de dados da organização.

10.3 Uso de Ferramentas Externas

A utilização de plataformas externas de IA deve considerar:

- O tratamento e armazenamento das informações fornecidas
- Os termos de uso e políticas de privacidade dos provedores
- O risco de exposição de dados sensíveis

O uso de ferramentas não avaliadas para tratamento de informações sensíveis deve ser evitado.

10.4 Riscos Associados à IA

A ZanderTek reconhece que o uso de IA pode introduzir riscos, incluindo:

- Vazamento de informações sensíveis
- Uso indevido ou não autorizado de dados
- Geração de conteúdo impreciso ou inadequado
- Dependência de serviços externos

Esses riscos devem ser considerados no uso das tecnologias.

10.5 Uso em Ambiente de Clientes

Quando aplicável, o uso de IA em contextos relacionados a clientes deve:

- Respeitar requisitos contratuais e regulatórios
- Garantir a proteção das informações dos clientes
- Seguir diretrizes específicas estabelecidas para cada contexto

11. GESTÃO DE INCIDENTES DE SEGURANÇA DE INFORMAÇÃO

A ZanderTek estabelece diretrizes para identificação, reporte, tratamento e acompanhamento de incidentes de segurança da informação, com o objetivo de minimizar impactos ao negócio, proteger seus ativos e garantir a continuidade das operações.

Um incidente de segurança da informação é qualquer evento que possa comprometer a confidencialidade, integridade ou disponibilidade das informações ou dos sistemas da organização.

11.1 Identificação de Incidentes

Devem ser considerados incidentes de segurança, entre outros:

- Acesso não autorizado a sistemas ou informações
- Vazamento ou suspeita de exposição de dados
- Perda ou comprometimento de dispositivos
- Uso indevido de credenciais
- Comportamentos anômalos em sistemas

11.2 Reporte de Incidentes

Todos os colaboradores, parceiros e terceiros devem reportar imediatamente qualquer incidente ou suspeita de incidente de segurança da informação à Diretoria.

O reporte deve ser realizado de forma clara e tempestiva, permitindo a rápida avaliação da situação.

11.3 Tratamento de Incidentes

Os incidentes devem ser avaliados e tratados de forma proporcional ao seu impacto, incluindo, quando aplicável:

- Contenção do incidente
- Análise de causa
- Adoção de medidas corretivas
- Comunicação às partes envolvidas

A condução do tratamento é de responsabilidade da Diretoria.

11.4 Comunicação

Quando necessário, a ZanderTek poderá comunicar incidentes de segurança a:

- Clientes impactados
- Parceiros envolvidos
- Autoridades competentes, conforme exigido por legislação ou contrato

A comunicação deve ser realizada de forma responsável e alinhada aos requisitos aplicáveis.

11.5 Registro e Aprendizado

Os incidentes relevantes devem ser registrados e analisados, com o objetivo de:

- Identificar causas e vulnerabilidades
- Evitar recorrência
- Promover melhorias nos processos e controles de segurança

12. CONTINUIDADE DE NEGÓCIOS

A ZanderTek adota diretrizes para garantir a continuidade de suas operações em situações adversas, minimizando impactos ao negócio, aos clientes e aos parceiros.

A abordagem de continuidade de negócios considera a identificação de cenários que possam interromper as operações e a definição de medidas proporcionais para assegurar a recuperação dos serviços e das informações.

12.1 Objetivo da Continuidade

A continuidade de negócios tem como objetivo:

- Assegurar a disponibilidade dos serviços essenciais
- Minimizar impactos decorrentes de interrupções
- Garantir a recuperação de informações e sistemas críticos
- Preservar o relacionamento com clientes e parceiros

12.2 Cenários de Interrupção

A ZanderTek considera, entre outros, os seguintes cenários que podem impactar suas operações:

- Falhas em sistemas ou serviços tecnológicos
- Indisponibilidade de provedores externos
- Perda ou comprometimento de dados
- Incidentes de segurança da informação
- Eventos que afetem a operação dos colaboradores

12.3 Estratégias de Continuidade

A organização adota medidas proporcionais ao seu porte e modelo operacional para garantir a continuidade, incluindo:

- Uso de serviços tecnológicos com alta disponibilidade
- Proteção e recuperação de informações
- Redundância sempre que aplicável
- Adoção de práticas que reduzam a dependência de pontos únicos de falha

12.4 Recuperação de Operações

Em caso de interrupção, a ZanderTek buscará:

- Restabelecer o acesso aos sistemas e informações
- Priorizar a recuperação de serviços essenciais
- Adotar medidas corretivas para estabilizar a operação

12.5 Responsabilidades

A Diretoria é responsável por coordenar as ações relacionadas à continuidade de negócios, incluindo a avaliação de impactos, definição de prioridades e condução das ações necessárias para recuperação das operações.

12.6 Revisão e Evolução

As práticas de continuidade devem ser revisadas periodicamente, considerando:

- Mudanças na operação
- Adoção de novas tecnologias
- Ocorrência de incidentes ou interrupções

13. MONITORAMENTO E MELHORIA CONTÍNUA

A ZanderTek adota práticas de monitoramento e melhoria contínua da segurança da informação, com o objetivo de assegurar a efetividade dos controles adotados e a evolução constante de suas práticas, de forma proporcional ao seu porte e modelo operacional.

13.1 Monitoramento

A organização realiza o acompanhamento de seus controles de segurança da informação por meio de:

- Avaliação periódica das práticas adotadas
- Acompanhamento de eventos relevantes relacionados à segurança
- Análise de incidentes e situações de risco identificadas

O monitoramento é conduzido de forma compatível com a estrutura da empresa, priorizando simplicidade e efetividade.

13.2 Avaliação de Controles

Os controles de segurança da informação devem ser avaliados periodicamente, considerando:

- Sua adequação aos riscos identificados
- Sua efetividade na proteção das informações
- A necessidade de ajustes ou melhorias

13.3 Melhoria Contínua

A ZanderTek promove a melhoria contínua de suas práticas de segurança da informação por meio de:

- Aprendizado a partir de incidentes e eventos relevantes
- Revisão de processos e controles
- Adaptação a novas ameaças e tecnologias

13.4 Evolução Proporcional

A evolução das práticas de segurança da informação será conduzida de forma proporcional ao crescimento da organização, considerando:

- A expansão das operações
- O aumento da complexidade tecnológica
- As demandas de clientes e requisitos regulatórios

14. CONFORMIDADE

A ZanderTek compromete-se a conduzir suas atividades em conformidade com requisitos legais, regulatórios e contratuais aplicáveis, bem como alinhada às boas práticas de mercado em segurança da informação.

A conformidade é considerada um elemento essencial para a proteção das informações, a confiança de clientes e parceiros e a sustentabilidade das operações da organização.

14.1 Requisitos Legais e Regulatórios

A ZanderTek observa as legislações aplicáveis relacionadas à proteção da informação e dados, incluindo, quando pertinente:

- Leis de proteção de dados pessoais aplicáveis às suas operações
- Requisitos regulatórios de setores atendidos, especialmente instituições financeiras
- Obrigações contratuais estabelecidas com clientes e parceiros

14.2 Conformidade Contratual

A organização compromete-se a atender aos requisitos de segurança da informação definidos em contratos com clientes, parceiros e fornecedores, incluindo:

- Cláusulas de confidencialidade
- Requisitos específicos de segurança
- Obrigações relacionadas à proteção de dados

Quando aplicável, a ZanderTek adotará controles adicionais para atender demandas específicas de clientes.

14.3 Alinhamento com Boas Práticas de Mercado

A ZanderTek busca alinhar suas práticas de segurança da informação a referenciais reconhecidos de mercado, incluindo:

- ISO/IEC 27001
- NIST

Esse alinhamento não implica necessariamente certificação formal, mas orienta a adoção de práticas consistentes e reconhecidas.

14.4 Atendimento a Auditorias e Avaliações

A ZanderTek poderá, quando aplicável:

- Participar de processos de avaliação de segurança conduzidos por clientes
- Fornecer evidências relacionadas às suas práticas de segurança da informação
- Apoiar auditorias conforme acordado contratualmente

14.5 Tratamento de Não Conformidades

Eventuais não conformidades identificadas em relação a requisitos legais, regulatórios ou contratuais devem ser avaliadas e tratadas de forma adequada, considerando:

- O impacto para o negócio
- Os riscos associados
- A necessidade de correção ou mitigação

15. SANÇÕES E NÃO CONFORMIDADE

O descumprimento das diretrizes estabelecidas nesta Política de Segurança da Informação poderá resultar em medidas apropriadas, proporcionais à gravidade da situação e ao impacto causado para a organização, seus clientes ou parceiros.

15.1 Aplicabilidade

Esta política é de cumprimento obrigatório para todos os colaboradores, sócios, diretores, terceiros e parceiros que tenham acesso a informações ou sistemas da ZanderTek.

15.2 Medidas em Caso de Descumprimento

Em caso de violação desta política, poderão ser adotadas medidas, incluindo:

- Orientação e reforço das diretrizes de segurança
- Revisão de acessos e privilégios
- Adoção de medidas disciplinares internas, quando aplicável
- Encerramento de contratos com terceiros ou parceiros
- Adoção de medidas legais cabíveis

15.3 Tratamento de Não Conformidades

Situações de não conformidade devem ser avaliadas pela Diretoria, considerando:

- A natureza e a gravidade da ocorrência
- O impacto para o negócio e para terceiros
- A necessidade de ações corretivas e preventivas

A organização buscará tratar não conformidades de forma estruturada, visando evitar recorrência e fortalecer seus controles de segurança.

16. REVISÃO E ATUALIZAÇÃO

A presente Política de Segurança da Informação será revisada periodicamente, ou sempre que necessário, com o objetivo de garantir sua adequação às necessidades da ZanderTek e ao contexto de segurança da informação.

16.1 Periodicidade de Revisão

A política deve ser revisada, no mínimo, anualmente, ou em prazo inferior quando houver:

- Mudanças relevantes na estrutura organizacional
- Adoção de novas tecnologias ou processos
- Alterações em requisitos legais, regulatórios ou contratuais
- Ocorrência de incidentes significativos de segurança

16.2 Responsabilidade pela Revisão

A responsabilidade pela revisão e atualização desta política é da Diretoria da ZanderTek.

16.3 Controle de Versão

Todas as revisões devem ser registradas no histórico de versões do documento, garantindo rastreabilidade e transparência das alterações realizadas.