[1.Introdução 2](#_Toc1731461062)

[1.1. Objetivo: 2](#_Toc561121675)

[1.2. Escopo: 2](#_Toc897514220)

[2. Princípios de Segurança 3](#_Toc155904238)

[2.1. Confidencialidade: 3](#_Toc577478291)

[2.2. Integridade: 3](#_Toc558829156)

[2.3. Disponibilidade: 4](#_Toc1647196548)

[3. Gerenciamento de Acesso 4](#_Toc116853929)

[3.1. Controle de Acesso: 4](#_Toc1155584134)

[3.2. Autenticação: 5](#_Toc911433969)

[3.3. Autorização: 5](#_Toc1017623094)

[4.Segurança Física e Ambiental 6](#_Toc690250917)

[4.1. Proteção de instalações: 6](#_Toc466146413)

[4.2. Controle de acesso físico: 6](#_Toc764430313)

[4.3. Segurança ambiental: 7](#_Toc338496807)

[5.Segurança de Redes e Comunicações 8](#_Toc1070218515)

[5.1. Proteção de redes: 8](#_Toc1146895102)

[5.2. Monitoramento e detecção de intrusões: 8](#_Toc338723593)

[6.Gestão de Incidentes de Segurança 8](#_Toc1118451014)

[6.1. Resposta a incidentes: 8](#_Toc1768271222)

[6.2. Relatórios de incidentes: 8](#_Toc1861168745)

[7.Conscientização e Treinamento em Segurança 9](#_Toc1224835064)

[7.1. Programa de conscientização: 9](#_Toc962451648)

[7.2. Treinamento em segurança: 9](#_Toc770701089)

[8.1. Auditorias de segurança: 9](#_Toc1761904346)

[8.2. Revisão de políticas e procedimentos: 9](#_Toc1651088183)

[8.3. Análise de riscos: 9](#_Toc2120184603)

[8.4. Medição de desempenho: 9](#_Toc1054111817)

[9.Conformidade Legal e Regulatória 10](#_Toc1792004686)

[9.1. Conformidade com leis e regulamentações: 10](#_Toc820163630)

[9.2. Gerenciamento de vulnerabilidades e patches: 10](#_Toc1013459909)

[10.Responsabilidades 10](#_Toc647640014)

[10.1. Direção: 10](#_Toc1191865309)

[10.2. Equipe de segurança da informação: 10](#_Toc1171483448)

[10.3. Funcionários: 11](#_Toc14208129)

[Referências: 11](#_Toc1884137789)

# **1.** **Introdução**

## **1.1. Objetivo:**

Este documento tem como objetivo proteger os dados, sistemas e os ativos da informação da Onyx Tech, assegurando sua confidencialidade, integridade e disponibilidade, garantindo a conformidade com as legislações vigentes (como a LGPD), normas internas e a continuidade das operações da empresa.

## **1.2. Escopo:**

Este documento se aplica a todos os colaboradores, estagiários, terceirizados, prestadores de serviço, parceiros que utilize ou tenha acesso aos ativos de informação da Onyx Tech, tanto nas unidades físicas (Contagem e Belo Horizonte) quanto em atividades remotas.

## **2. Princípios de Segurança**

## **2.1. Confidencialidade:**

A confidencialidade garante que a informação seja acessada apenas por pessoas autorizadas. Isso significa proteger dados sensíveis de acessos não autorizados, evitando vazamentos ou exposição de indivíduos ou organizações que não tem permissão para visualizar essas informações.

Classificação de Informação: Configuração de prioridades de acessos como internos ou externos.

Uso de Criptografia: Aplicação de criptografia em ativos de armazenamento de dados como HD, em notebooks e celulares com dados sensíveis, banco de dados e e-mails.  
   
 Restrição de acesso: Restringir o acesso a dados de clientes, financeiro e garantias somente a usuários autorizados.

Criação de senhas: Utilizar senhas fortes em todos os sistemas.

**2.2. Integridade:**

A integridade assegura que a informação permaneça precisa e inalterada ao longo de seu ciclo de vida. Isso envolve a proteção contra alterações não autorizadas, acidentais ou maliciosas, assegurando que os dados sejam consistentes.

Backup e verificação: Configuração de backups periódicos e verificação constante de da integridade dos dados.  
 Armazenamento de dados: Armazenar planilhas e arquivos em ambientes corporativos (ex: pastas da empresa e não Google Drive pessoal).

Assinatura digital: Prevenção para que os dados não sejam alterados durante o armazenamento e envio.

Validação e verificação de dados: Certificar que os dados não sejam modificados sem autorização e verificar alterações em documentos críticos periodicamente.

**2.3. Disponibilidade:**

A disponibilidade assegura que a informação e os sistemas estejam acessíveis quando necessário. Isso envolve garantir que os dados possam ser acessados e utilizados por usuários autorizados, sem interrupções indesejadas, e que existam formas de restaurar o acesso em caso de falha.

Equipe de TI: Garantir a implementação e a disponibilidade dos dados, realizar backups automáticos diariamente.

Equipe de Gestão: Apoiar na implementação aplicação da política e assegurar os recursos.

Recuperação de dados: Ter plano de recuperação de desastres e testes de restauração de dados.

## **3. Gerenciamento de Acesso**

## **3.1. Controle de Acesso:**

O objetivo de gerenciamento de acesso, é certificar que somente usuários que são autorizados, possam ter acesso a dados de informação e a determinados sistemas.

Definir perfis de usuários por função (Role- Based Access Control): Estabelecer o perfil do usuário baseado em sua função, para garantir que este tenha acesso somente o que lhe for atribuído.

Controles de acesso físico a servidores, datacenter, Firewall, Switch e outros: Implementar fechaduras, registro de entradas em áreas críticas. Controlar acessos a dispositivos corporativos (notebooks, tablets e celulares).

Rastreamento de acessos: Criar logins individuais para cada colaborador. Ativar logs de acessos em todos os sistemas críticos e retenção de dados de log para análises.

**3.2. Autenticação:**  
   
 O objetivo da autenticação é validar a identidade do usuário no sistema antes de fornecer permissões de acesso as informações, serviços e recursos protegidos.

Autenticação multifator (MFA): Habilitar o MFA para os usuários em sistemas que contém informações sensíveis e críticas.

Senha Fortes e política de expiração: Exigir que os usuários usem senhas com maior complexidade, (Mínimo de 8 caracteres, uso de símbolos e números), renovação periódica.

Sessões com tempo de expiração automática: Configurar encerramento automático de sessões inativas para evitar riscos de acessos indevidos.

**3.3. Autorização:**  
   
 O objetivo da autorização, é certificar que somente os usuários autenticados possa acessar os dados, recursos e funcionalidades que possuem permissão para utilizar.

Matriz de permissões: Registrar quem pode acessar quais pastas, sistemas e dispositivos.

Validação de permissões: Verificação periódica de quem tem acesso a quais tipos de sistemas e recursos.

Logs de autorização: Armazenar histórico de registros de todas as atividades permitidas ou negadas.

## **4.** **Segurança Física e Ambiental**

## **4.1. Proteção de instalações:**

Implementar medidas para proteger as instalações físicas onde os sistemas de informação e recursos de TI estão localizados.

Sistema de CFTV: Monitoramento de câmeras 24 horas como armazenamento de dados em nuvem.

Contingência: Procedimentos a serem executados em situações de furtos, desastres

naturais e dano físico. Portas trancadas com biometria nas salas de estoque e laboratório.

Segurança: Alarmes de presença e sensores de fumaça instalados.

As medidas para proteção de instalações podem ser divididas da seguinte forma:

Controles de acesso (citado no item 4.2)

Monitoramento através de câmeras e sensores de movimento

Proteção física: grades,portões,cercas,muros e reforços como portas e janelas resistentes a arrombamento

Proteção contra roubo e furto: armazenamento seguro de ativos valiosos em armários, cofres e salas com fechadura eletrônica, câmeras e sistemas de alarme, elaboração de inventário de equipamentos e auditoria

**4.2. Controle de acesso físico:**  
   
 Algumas formas de proteção para controlar acesso a áreas físicas sensíveis:

Acesso restrito com senha, biometria e crachá nas áreas sensíveis.

Controle de acesso rígido em áreas mais críticas.

Registros de entrada e saída de pessoas autorizadas.

**4.3. Segurança ambiental**:  
   
 Proteção contra riscos e ameaças ambientais que possam afetar as instalações, ativos físicos e ativos lógicos da empresa.  
   
  **4.3.1 Proteção contra desastres naturais:**

Avaliação de riscos ambientais, baseando na localização de suas filiais, identificando e documentando os tipos de desastres naturais comuns as regiões que podem afetar a segurança dos dados e operação da empresa.

Plano de contingência, elaborar e implementar planos de contingência que incluam medidas especificas para proteção de ativos de dados da empresa em caso de desastres naturais.

**4.3.2 Proteção contra incêndios:**

Adotar sistemas de prevenção e combate a incêndios, como por exemplo: sprinklers automáticos, alarmes de incêndio e extintores de fácil acesso.  
 Inspeção regular dos sistemas de controle e prevenção de incêndios.  
 Conscientização e instrução dos funcionários com treinamentos sobre procedimentos de segurança em caso de incêndio.  
 Minimizar fontes de risco dentro de todas as instalações da empresa, como materiais inflamáveis e tomadas velhas, que tem a chance de causar incêndios

## **5.** **Segurança de Redes e Comunicações**

## **5.1. Proteção de redes:**

Proteção de redes A Onyx Tech manterá a segmentação das redes Wi-Fi entre clientes e colaboradores para evitar interceptação de dados. A rede interna será restrita e protegida por firewall. Todo o tráfego será monitorado por ferramentas de inspeção e controle de conteúdo, bloqueando o acesso a sites maliciosos ou impróprios. Os dispositivos da empresa devem ser conectados apenas à rede segura e corporativa.

**5.2. Monitoramento e detecção de intrusões:**  
   
 Monitoramento e detecção de intrusões A equipe de TI realizará o monitoramento contínuo das redes e dispositivos. Logs de acesso serão armazenados e analisados regularmente para identificar atividades suspeitas. Alertas de comportamento anômalo devem ser configurados para disparar notificações em tempo real.

## **6.** **Gestão de Incidentes de Segurança**

## **6.1. Resposta a incidentes**:

Será mantido um plano de resposta a incidentes, com procedimentos claros para isolamento, comunicação, contenção e recuperação. A equipe de TI deve ser imediatamente notificada sobre qualquer anormalidade, como acessos indevidos, perda de dispositivos ou vazamentos de informação.

**6.2. Relatórios de incidentes:**

Todos os incidentes deverão ser documentados com detalhes como data, hora, envolvidos, sistemas afetados e medidas corretivas adotadas. Os relatórios serão avaliados para identificação de falhas e definição de melhorias.

## **7.** **Conscientização e Treinamento em Segurança**

## **7.1. Programa de conscientização:**

Programa de conscientização A Onyx Tech promoverá campanhas internas de conscientização sobre boas práticas em segurança da informação, com foco em ameaças como phishing, engenharia social, uso seguro de WhatsApp Business e tratamento de dados pessoais.

**7.2. Treinamento em segurança:**

Treinamentos serão realizados semestralmente, com simulações de ataques cibernéticos e estudos de caso reais ocorridos na empresa. Novos colaboradores devem receber esse conteúdo na integração.

**8.** **Avaliação e Melhoria Contínua**

## **8.1. Auditorias de segurança:**

Auditorias internas serão conduzidas semestralmente para verificar o cumprimento da PSI, uso adequado dos sistemas e dispositivos, e existência de vulnerabilidades nos processos.

## **8.2. Revisão de políticas e procedimentos:**

A PSI será revisada anualmente ou sempre que houver mudanças significativas na estrutura da empresa, legislação ou ocorrências de incidentes relevantes.

## **8.3. Análise de riscos:**

O processo de vendas será reavaliado com frequência, utilizando a matriz de risco adotada, com foco em dispositivos móveis, comunicação externa e armazenamento de dados.

## **8.4. Medição de desempenho:**

Indicadores como número de incidentes, tempo de resposta, dispositivos sem proteção e participação nos treinamentos serão acompanhados mensalmente.

**9.** **Conformidade Legal e Regulatória**

## **9.1. Conformidade com leis e regulamentações:**

A Onyx Tech atuará conforme as determinações da LGPD, do Marco Civil da Internet, do Código de Defesa do Consumidor e demais normas pertinentes à proteção de dados e direitos do cliente.

## **9.2. Gerenciamento de vulnerabilidades e patches:**

A equipe de TI será responsável por manter os sistemas atualizados, aplicando correções de segurança (patches) assim que forem disponibilizados pelos fornecedores. Também serão monitoradas as vulnerabilidades mais críticas divulgadas pelo CERT.br.

**10.** **Responsabilidades**

## **10.1. Direção:**

A alta direção deverá aprovar, apoiar e promover a PSI, além de fornecer os recursos necessários para sua aplicação e evolução.

## **10.2. Equipe de segurança da informação**:

Equipe de segurança da informação / TI Responsável pela implementação e manutenção da PSI, suporte a usuários, gerenciamento de incidentes, controle de acesso, backup e atualização dos sistemas e dispositivos.

## **10.3. Funcionários:**

Todos os colaboradores devem seguir as orientações da política, utilizar os recursos da empresa com responsabilidade, proteger senhas, relatar comportamentos suspeitos e participar dos treinamentos de segurança obrigatórios.

Esta política de segurança de modelo abrange todos os aspectos importantes para garantir a integridade, confidencialidade e disponibilidade dos recursos e informações da organização.

## **Referências:**

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <https://www.planalto.gov.br>.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet. Disponível em: <https://www.planalto.gov.br>.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Código de Defesa do Consumidor (CDC).

CERT.br – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Disponível em: <https://www.cert.br>.

ABNT NBR ISO/IEC 27001:2013. Tecnologia da informação — Técnicas de segurança — Sistemas de gestão de segurança da informação — Requisitos.

BRASILIANO, R. J. Gestão de Riscos Corporativos – Enterprise Risk Management. 5ª ed. São Paulo: Atlas, 2018.