**POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)**

[Nome da Empresa]

**Versão X.X**

Sumário

[1. INTRODUÇÃO 3](#_Toc190553027)

[2. PROPÓSITO 3](#_Toc190553028)

[3. ABRANGÊNCIA 3](#_Toc190553029)

[4. DIREITOS DE USO 3](#_Toc190553030)

[5. DEVERES 3](#_Toc190553031)

[6. PROIBIÇÕES 3](#_Toc190553032)

[7. COMPROMISSOS 4](#_Toc190553033)

[8. SOFTWARES E LICENÇAS 4](#_Toc190553034)

[9. ADIÇÃO E REMOÇÃO DE RECURSOS 4](#_Toc190553035)

[10. ADMINISTRAÇÃO DA REDE 4](#_Toc190553036)

[11. AUDITORIA E SINDICÂNCIA 4](#_Toc190553037)

[12. USO DE CREDENCIAIS 4](#_Toc190553038)

[13. TERMO DE POLÍTICA DE SEGURANÇA DA INFORMAÇÃO 5](#_Toc190553039)

# 1. INTRODUÇÃO

A **Política de Segurança da Informação (PSI)** estabelece diretrizes para garantir a proteção das informações corporativas, assegurando a confidencialidade, integridade e disponibilidade dos dados, alinhada às boas práticas do mercado, como a **ISO 27001**, **NIST CSF** e a **LGPD**.

# 2. PROPÓSITO

Definir regras e diretrizes para o **uso seguro dos ativos de informação**, prevenindo ameaças cibernéticas, acessos indevidos e vazamentos de dados.

# 3. ABRANGÊNCIA

Esta PSI se aplica a **todos os colaboradores, prestadores de serviço, fornecedores e terceiros** que tenham acesso aos ativos de TI da organização.

# 4. DIREITOS DE USO

Os usuários têm direito ao uso dos recursos de TI, respeitando:

* A **legislação vigente** (LGPD, Marco Civil da Internet);
* As **normas internas** da organização;
* Os **padrões de boas práticas de segurança da informação**.

# 5. DEVERES

Os usuários devem:

* Utilizar os sistemas de informação de forma **responsável e segura**;
* Proteger suas **credenciais de acesso**;
* Reportar **incidentes de segurança** imediatamente.

# 6. PROIBIÇÕES

* Compartilhamento de senhas;
* Instalação de softwares não autorizados;
* Uso dos recursos de TI para atividades ilegais ou não relacionadas ao trabalho.

# 7. COMPROMISSOS

A empresa se compromete a:

* **Monitorar continuamente** a infraestrutura de TI;
* **Implementar camadas de segurança**, como firewall, IDS/IPS e autenticação multifator (MFA);
* Realizar **auditorias periódicas** para garantir a conformidade.

# 8. SOFTWARES E LICENÇAS

Todos os softwares utilizados devem ser **licenciados e homologados** pela área de TI. O uso de softwares piratas é estritamente proibido.

# 9. ADIÇÃO E REMOÇÃO DE RECURSOS

* O acesso a sistemas e dados deve ser concedido **mediante autorização**;
* A remoção de acessos deve ocorrer imediatamente após o desligamento do colaborador ou mudança de função.

# 10. ADMINISTRAÇÃO DA REDE

A **Administração de Rede** deve:

* Garantir a **segurança e disponibilidade** dos serviços de TI;
* Implementar **políticas de segmentação de rede**;
* Adotar **VPNs seguras** para acesso remoto.

# 11. AUDITORIA E SINDICÂNCIA

* Monitoramento contínuo de logs e acessos;
* Auditorias periódicas para avaliação de riscos;
* Investigação de incidentes com medidas disciplinares quando necessário.

# 12. USO DE CREDENCIAIS

* É obrigatório o uso de **senhas fortes e MFA**;
* As credenciais são pessoais e intransferíveis;
* O bloqueio de conta ocorre após **múltiplas tentativas falhas**.

# 13. TERMO DE POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Todos os colaboradores e terceiros devem assinar um **Termo de Adesão à PSI**, concordando com as normas estabelecidas.

**TERMO DE COMPROMISSO COM A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO**

Eu, **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**, colaborador(a) da **[Nome da Empresa]**, declaro para os devidos fins que estou ciente e em pleno acordo com as diretrizes e normas estabelecidas na **Política de Segurança da Informação (PSI)** desta organização.

**1. DIRETRIZES GERAIS**

1. Todos os **equipamentos, sistemas, acessos à rede corporativa e e-mails institucionais** são de propriedade da **[Nome da Empresa]** e devem ser utilizados **exclusivamente para fins profissionais** dentro dos limites estabelecidos por normativas internas e legislação vigente.
2. O uso dos recursos de TI para fins pessoais, atividades ilegais ou que comprometam a integridade e confidencialidade das informações é **estritamente proibido**.

**2. MONITORAMENTO E CONFORMIDADE**

1. Reconheço a legitimidade da **[Nome da Empresa]** para **monitorar e auditar minhas atividades digitais** sempre que necessário para garantir a **segurança da informação, conformidade regulatória e integridade da infraestrutura tecnológica**.
2. Estou ciente de que todas as atividades realizadas em **dispositivos, redes e sistemas corporativos** podem ser registradas e analisadas para prevenção de ameaças, conformidade com a legislação (LGPD, ISO 27001, NIST) e proteção contra acessos indevidos.
3. O não cumprimento das normas de segurança pode resultar em **medidas disciplinares**, incluindo advertências, restrição de acessos e, em casos graves, rescisão contratual e responsabilização legal.

**3. DEVERES E RESPONSABILIDADES**

1. Comprometo-me a manter a **confidencialidade das informações corporativas** e a proteger **minhas credenciais de acesso** (senhas, tokens, autenticação multifator).
2. Estou ciente de que é minha responsabilidade reportar **incidentes de segurança** imediatamente ao setor de TI.
3. Declaro que **não compartilharei minhas credenciais de acesso**, não realizarei **instalações de softwares não autorizados** e não utilizarei os recursos da empresa para finalidades não permitidas.

**4. AUTORIZAÇÃO E CONSENTIMENTO**

Pelos motivos expostos, declaro ter **lido, compreendido e aceito** os termos desta política, autorizando a **[Nome da Empresa]** a monitorar e auditar minhas atividades computacionais no ambiente corporativo.

Boa Vista, \_\_\_\_\_\_\_ de \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ de \_\_\_\_\_\_\_.

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**  
Assinatura

CPF: **\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**