



**SENAI**

A solid red vertical bar on the left side of the slide.

# POLÍTICA SEGURANÇA DA INFORMAÇÃO





# Introdução

**Política de segurança da Informação (PSI)** é um documento utilizado em organizações contendo um conjunto de normas e diretrizes que estabelecem princípios, valores, requisitos e orientações com o objetivo de mitigar risco para os dados armazenados da organização.

De forma mais simplificada, é um documento que contém normas do que se pode e não se pode fazer na empresa com o objetivo de evitar ciber ataques e vazamentos de dados.



# Introdução

Uma Política de Segurança da Informação deve atender a alguns requisitos, tais como:

**Introdução:** apresenta o objetivo, o escopo, o público-alvo e as referências da política;

**Definições:** esclarece os termos técnicos ou específicos utilizados na política;

**Princípios:** estabelece os valores e as diretrizes que norteiam a política;

**Objetivos:** define os resultados esperados com a implementação da política;

**Responsabilidades:** atribui as funções e as obrigações dos envolvidos na gestão da segurança da informação;

**Normas:** especifica as regras e os procedimentos que devem ser seguidos para garantir a segurança da informação;

**Sanções:** determina as penalidades aplicáveis em caso de descumprimento da política;

**Revisão:** indica a periodicidade e os critérios para a atualização da política.





# Introdução

As normas ISO da família 27000 possuem orientações e boas práticas para proteção de dados para empresas e órgãos públicos.

A ISO 27000 é dividida em 3 categorias principais:

**ISO/IEC 27001:** é uma normatização para sistemas de gestão da **Segurança da Informação**.

**ISO/IEC 27002:** é uma normatização para **controles** de sistemas de Segurança da Informação

**ISO/IEC 27003:** é uma normatização para **definição** do que deve ser protegido e monitorado

É uma boa prática e altamente recomendado, utilizar as normas ISO como referências para criar uma PSI.



## Escopo

Um dos pontos principais de uma PSI é a definição do escopo.

Definir o escopo da PSI é definir onde essa política será aplicada e para quem serão aplicados.

Exemplo de escopo da PSI da empresa SOLVIMM

## 5. Escopo

Esta política abrange todos os sistemas, equipamentos e informações da SOLVIMM, incluindo também seus colaboradores, estagiários, terceirizados, temporários e fornecedores em quaisquer das dependências da SOLVIMM, ou locais onde estes se façam presentes, por meio da utilização, do manuseio ou do processamento eletrônico das informações.

<https://solvimm.com/quem-somos/politicas/politica-de-seguranca-da-informacao/>





## Responsabilidade

Outro ponto importante na criação de uma PSI é definir as responsabilidades.

Aqui declaramos quem terá acesso a quais informações, sempre levando em consideração o risco e a gravidade daquela informação ser vazada.



Com o crescimento da internet, popularização dos dispositivos conectados e o uso cotidiano da internet, em 2014 foi criado o **Marco Civil da Internet**, também conhecido como **Lei 12.965/14**.

O objetivo do Marco Civil da Internet é estabelecer direitos, deveres e garantias no meio digital (uso da internet).







# Legislação



## Princípios do Marco Civil da Internet:

- Garantia da liberdade de expressão, comunicação e manifestação de pensamento;
- Proteção da privacidade;
- Proteção dos dados pessoais;
- Preservação e garantia da neutralidade de rede;
- Preservação da estabilidade, segurança e funcionalidade da rede;
- Responsabilização dos agentes de acordo com suas atividades;
- Preservação da natureza participativa da rede;
- Liberdade dos modelos de negócios promovidos na internet.





# Legislação

## Lei Geral de Proteção de Dados

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018, foi promulgada para proteger os direitos fundamentais de liberdade e de privacidade, e a livre formação da personalidade de cada indivíduo.

A LGPD veio para proteger as informações pessoais de cada indivíduo, obrigando as empresas a terem uma norma para tratar e utilizar dados pessoais



## Exemplos de PSI

SOLVIMM

<https://solvimm.com/quem-somos/politicas/politica-de-seguranca-da-informacao/>

TOTVS

[https://tic.fgv.br/sites/tic.fgv.br/files/arquivos/politica\\_de\\_seguranca\\_da\\_informacao.pdf](https://tic.fgv.br/sites/tic.fgv.br/files/arquivos/politica_de_seguranca_da_informacao.pdf)

B3

[https://s3.amazonaws.com/mz-filemanager/5fd7b7d8-54a1-472d-8426-eb896ad8a3c4/0b5bc320-709e-4f36-9526-f82630f66649\\_PoliticaSegurancaInformacao.pdf](https://s3.amazonaws.com/mz-filemanager/5fd7b7d8-54a1-472d-8426-eb896ad8a3c4/0b5bc320-709e-4f36-9526-f82630f66649_PoliticaSegurancaInformacao.pdf)

SENAC

[https://www.sp.senac.br/normasadministrativas/psi\\_normas\\_administrativas.pdf](https://www.sp.senac.br/normasadministrativas/psi_normas_administrativas.pdf)



# | Dúvidas



## Referências

Lei 12.965/14: Tire as suas dúvidas sobre o Marco Civil da Internet – **Acessado em 14/05/2024**

<https://www.aurum.com.br/blog/marco-civil-da-internet/>

ABNT NBR ISO/IEC 27001

Número de referência ABNT NBR ISO/IEC 27001:2006, 34 páginas

ABNT NBR ISO/IEC 27002

Número de referência ABNT NBR ISO/IEC 27002:2022

191 páginas



## Referências

Guia comentado da Lei Geral de Proteção de Dados – LGPD (13709/18) – **Acessado em 14/05/2024**

<https://www.aurum.com.br/blog/lgpd/>

Lei Geral de Proteção de Dados Pessoais (LGPD) – **Acessado em 14/05/2024**

<https://www.gov.br/esporte/pt-br/acesso-a-informacao/lgpd#:~:text=A%20Lei%20Gera%20de%20Prote%C3%A7%C3%A3o,da%20personalidade%20de%20cada%20indiv%C3%ADduo.>

