Políticas de Segurança da Informação

O que é a Política de Segurança da Informação (PSI)

A Política de Segurança da Informação (PSI) é um documento formal, aprovado pela alta administração, que define regras, responsabilidades e diretrizes para a proteção dos ativos de informação da organização.

Segundo Ferreira & Araujo (2008), ela deve ser vista como um marco regulatório interno, funcionando como “a constituição da segurança da informação” dentro da empresa.

> Em outras palavras: é o conjunto de normas e boas práticas que todos na organização precisam seguir para que a informação seja preservada e utilizada corretamente.

1.2 Objetivos Principais da PSI

1. Confidencialidade
   - Garantir que a informação só seja acessada por pessoas autorizadas.
   - Exemplo: relatórios financeiros disponíveis apenas para a diretoria.

2. Integridade
   - Assegurar que a informação não seja alterada ou corrompida de forma indevida.
   - Exemplo: banco de dados com logs que registram alterações em tempo real.

3. Disponibilidade
   - Garantir que a informação esteja acessível quando necessária.
   - Exemplo: sistema de atendimento online com plano de contingência para quedas de servidor.

1.2 Objetivos Principais da PSI

4. Redução de Riscos
   - Minimizar ameaças internas e externas que podem comprometer dados.
   - Exemplo: bloqueio de sites maliciosos e antivírus corporativo atualizado.

5. Definição de Responsabilidades
   - Estabelecer claramente quem faz o quê em termos de segurança.
   - Exemplo: área de TI responsável por backups; usuários responsáveis por não compartilhar senhas.

6. Promoção da Cultura de Segurança
   - Conscientizar colaboradores sobre boas práticas.
   - Exemplo: campanhas internas contra phishing e treinamentos anuais.

1.3 Importância Estratégica da PSI

Alinhamento ao Negócio: a informação é um ativo estratégico, assim como máquinas, prédios ou capital financeiro.

Redução de Prejuízos: falhas de segurança podem gerar perdas financeiras, danos à imagem e sanções legais.

Conformidade Legal e Normativa: ajuda a cumprir normas como LGPD, ISO 27001 e legislações setoriais.

Proteção contra Engenharia Social: políticas reduzem riscos de ataques baseados em manipulação de pessoas (Peixoto, 2006).

Prevenção em vez de Correção: uma política bem estruturada antecipa problemas, em vez de agir apenas após incidentes.

1.4 Exemplos Práticos de Relevância

Caso 1: Uma empresa sem PSI sofre um vazamento de dados de clientes. Além do dano à reputação, pode ser multada pela LGPD.

Caso 2: Uma instituição financeira com PSI bem definida consegue recuperar dados rapidamente após falha de servidor, mantendo a confiança do cliente.

Caso 3: Um colaborador tenta instalar software pirata; a PSI proíbe e responsabiliza, evitando riscos legais e técnicos.

A PSI não é apenas um documento burocrático, mas sim uma ferramenta estratégica de proteção organizacional.

Ela dá clareza, disciplina e direção às práticas de segurança, ajudando a transformar a cultura da organização em torno da informação como ativo crítico.

2. Estrutura de um Documento de Política de Segurança

Uma Política de Segurança da Informação (PSI) deve ser organizada em seções claras, de modo a orientar tanto a alta gestão quanto os usuários finais. Componentes:

1. **Introdução e Objetivos**
2. **Escopo e Abrangência**
3. **Princípios de Segurança**
4. **Responsabilidades**
5. **Regras e Diretrizes**
6. **Gestão de Incidentes**
7. **Treinamento e Conscientização**
8. **Revisão e Atualização da Política**

2.1. Introdução e Objetivos

Finalidade: explicar por que o documento existe e qual a sua função estratégica.

Exemplo: “Este documento estabelece as diretrizes para proteger as informações críticas da organização, garantindo a continuidade dos negócios e o cumprimento das normas legais.”

Objetivos típicos:

- Proteger os ativos de informação.
- Garantir conformidade com legislações e normas (ex.: LGPD, ISO 27001).
- Reforçar a responsabilidade individual de cada colaborador.

2.2. Escopo e Abrangência

Define o que está coberto pela política.

Inclui áreas, sistemas, pessoas, processos e informações.

Exemplo:

- “Abrange todos os colaboradores, prestadores de serviços e parceiros que tenham acesso a dados da organização.”
- “Inclui sistemas corporativos, dispositivos móveis, redes internas e informações em papel.”

2.3. Princípios de Segurança

Base para todas as normas descritas na política:

- Confidencialidade: apenas pessoas autorizadas podem acessar a informação.
- Integridade: a informação deve permanecer correta, íntegra e confiável.
- Disponibilidade: sistemas e dados devem estar acessíveis sempre que necessário.
- Autenticidade: garantia de que a identidade de usuários e sistemas é válida.
- Responsabilidade: cada colaborador responde por suas ações no uso da informação.
- Auditoria: todas as ações devem poder ser verificadas e rastreadas.

2.4. Responsabilidades

Define claramente os papéis dentro da organização:

Alta direção:

- Aprovar a política.
- Garantir recursos para a sua execução.
- Dar exemplo de conformidade.

Comitê de Segurança da Informação:

- Criar e revisar normas específicas.
- Avaliar incidentes e propor melhorias.

2.4. Responsabilidades

Usuários:

- Seguir as regras estabelecidas.
- Utilizar senhas fortes.
- Reportar comportamentos suspeitos.

Administradores e equipe de TI:

- Implementar controles técnicos (firewalls, backups, criptografia).
- Monitorar a rede e os sistemas.
- Apoiar usuários em dúvidas de segurança.

2.5. Regras e Diretrizes

São as normas práticas que todos devem seguir:

Uso aceitável:

- Proibição de instalar softwares não autorizados.
- Uso corporativo da internet e e-mail, evitando fins pessoais abusivos.

Controle de senhas:

- Mínimo de 8 caracteres, incluindo números e símbolos.
- Alteração periódica (ex.: a cada 90 dias).

2.5. Regras e Diretrizes

Backups e recuperação de desastres:

- Backup diário de servidores críticos.
- Testes regulares de restauração.

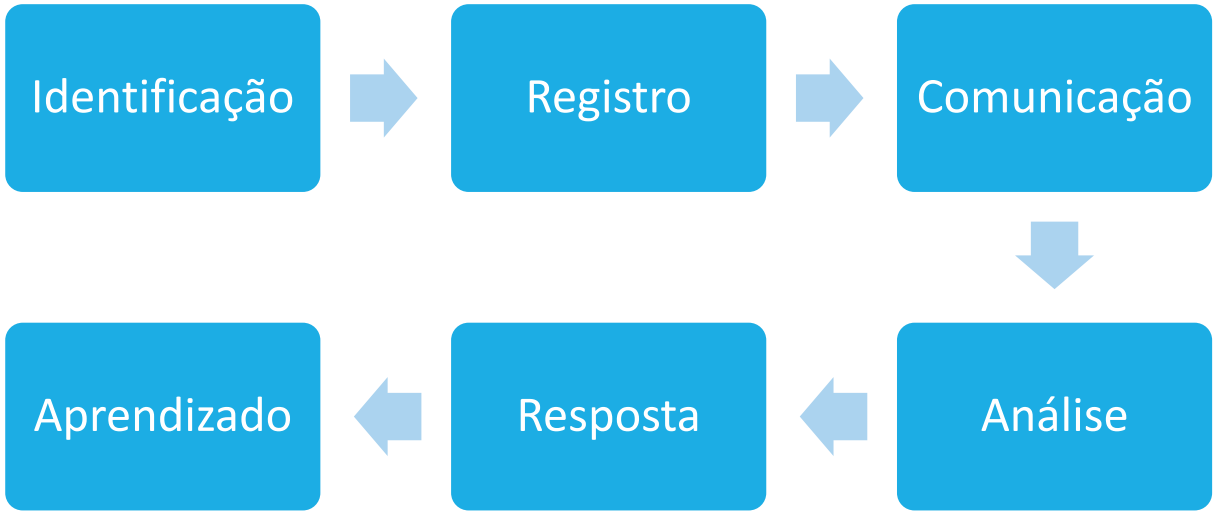
Classificação da informação:

- Confidencial, Interna, Pública.
- Cada nível deve ter regras específicas de uso e compartilhamento.

2.6. Gestão de Incidentes

Define como lidar com falhas ou ataques de segurança.

Fluxo básico:



Exemplo: Caso de phishing reportado deve ser imediatamente comunicado ao time de segurança para análise.

2.7. Treinamento e Conscientização

A política só é eficaz se as pessoas a conhecerem e aplicarem.

Deve haver campanhas periódicas, workshops e treinamentos sobre:

- Boas práticas de senha.
- Reconhecimento de e-mails fraudulentos.
- Uso correto de mídias removíveis e dispositivos móveis.

2.8. Revisão e Atualização da Política

Uma PSI não é estática: deve acompanhar mudanças tecnológicas, legais e de negócio.

Periodicidade: revisão anual (ou semestral, em ambientes críticos).

Responsáveis: geralmente o Comitê de Segurança e a alta direção.

Exemplo prático: atualização para atender às exigências da LGPD no Brasil.

3. Responsabilidades

A Política de Segurança da Informação (PSI) só é efetiva quando todos compreendem e cumprem suas responsabilidades. A segurança não é apenas tarefa da equipe técnica, mas sim de toda a organização.

3.1. Alta Administração

Papel:

- Definir a visão estratégica da segurança da informação.
- Aprovar a política formalmente.
- Garantir orçamento, equipe e ferramentas necessárias.

Exemplo prático: investir em sistemas de backup redundantes mesmo que o custo seja elevado, pois garante continuidade dos negócios.

Boa prática: demonstrar comprometimento visível (patrocínio ativo, participação em comitês e auditorias).

3.2. Gestores

Papel:

- Integrar a política de segurança nos processos sob sua responsabilidade.
- Monitorar se suas equipes seguem os procedimentos.
- Servir de elo entre a alta direção e os usuários.

Exemplo prático: gerente de RH garantir que apenas profissionais autorizados acessem a folha de pagamento.

Boa prática: incluir metas de conformidade em segurança nos indicadores de desempenho da equipe.

3.3. Equipe de TI/Segurança

Papel:

- Implementar e manter controles técnicos (firewalls, antivírus, criptografia).
- Gerenciar permissões de acesso e autenticação.
- Monitorar logs e detectar incidentes de segurança.
- Apoiar usuários com orientações técnicas.

Exemplo prático: configurar regras de firewall para bloquear acessos suspeitos e monitorar tentativas de login não autorizadas.

Boa prática: documentar procedimentos e adotar ferramentas de automação para respostas a incidentes.

3.4. Usuários Finais

Papel:

- Cumprir as regras estabelecidas pela PSI.
- Utilizar os recursos de forma ética, responsável e profissional.
- Reportar comportamentos suspeitos ou incidentes (ex.: e-mails de phishing).

Exemplo prático: não compartilhar senha de e-mail corporativo com colegas de trabalho.

Boa prática: participar ativamente dos treinamentos de conscientização.

3.5. Auditores Internos/Externos

Papel:

- Avaliar periodicamente se a organização cumpre as políticas e normas de segurança.
- Emitir relatórios com recomendações de melhorias.
- Garantir que controles estejam alinhados a padrões como ISO 27001, LGPD, SOX, entre outros.

Exemplo prático: auditor externo validar se os backups são realizados conforme a política (diariamente e com testes de restauração).

Boa prática: manter independência e imparcialidade, assegurando credibilidade às análises.

Resumo visual das responsabilidades

Ator	Responsabilidade-chave	Exemplo prático
Alta Administração	Patrocínio e recursos	Aprovar compra de solução de backup em nuvem
Gestores	Cumprimento nos processos	RH restringir acesso à folha de pagamento
Equipe de TI/Segurança	Controles técnicos e monitoramento	Configurar firewall e monitorar acessos
Usuários finais	Uso ético e seguro	Não compartilhar senhas
Auditores	Avaliação e conformidade	Validar rotinas de backup

4. Análise Crítica da Política

A análise crítica é o processo de avaliar continuamente a Política de Segurança da Informação (PSI), verificando se ela está atualizada, eficaz e realmente aplicada no dia a dia da organização. Uma PSI bem estruturada perde valor se não for revisada ou se não refletir a realidade do ambiente corporativo.

4.1 Requisitos de uma Análise Crítica

1. Realista e Aplicável
   - A política não pode conter regras impossíveis de cumprir.
   - Exemplo: exigir que usuários troquem senha todos os dias seria impraticável e levaria ao descumprimento.

2. Linguagem Clara e Acessível
   - Deve ser entendida por colaboradores de diferentes áreas, não apenas pelo setor de TI.
   - Exemplo: em vez de “uso de autenticação multifatorial via token RSA”, pode-se escrever “uso de mais de um método de verificação (senha + código enviado ao celular)”.

3. Dinamismo e Atualização Contínua
   - A política deve acompanhar mudanças em:
     - Tecnologias (ex.: uso de dispositivos móveis e nuvem).
     - Legislação (ex.: adequação à LGPD).
     - Modelos de negócio (ex.: trabalho remoto).

4.1 Requisitos de uma Análise Crítica

4. Exemplos Práticos
   - A inclusão de situações reais torna a política mais compreensível.
   - Exemplo: ao invés de “proibido o uso inadequado de e-mail”, detalhar: “é proibido usar o e-mail corporativo para encaminhar correntes, piadas ou conteúdos pessoais”.

5. Periodicidade de Revisão
   - Recomenda-se revisão anual, ou semestral em ambientes críticos.
   - A ausência de revisão pode tornar a política obsoleta e gerar vulnerabilidades.

4.2 Critérios de Avaliação da PSI

Durante a análise crítica, podem ser usados critérios como:

- Efetividade: A política realmente reduz incidentes?
- Aderência: Os colaboradores conhecem e seguem as regras?
- Clareza: O documento é compreendido por todos os níveis da organização?
- Atualização: Está alinhada às novas tecnologias e legislações?
- Medição: Há indicadores (KPIs) que comprovem sua aplicação?

4.3 Exemplos de Problemas Detectados em Análises Críticas

Política antiga que não menciona trabalho remoto nem uso de dispositivos pessoais (BYOD).

Documento excessivamente técnico, sem tradução prática para o dia a dia.

Colaboradores desconhecem a política, pois nunca foram treinados.

Revisão feita apenas no papel, sem validação prática dos controles.

4.4 Benefícios da Análise Crítica

Garante que a PSI continue eficaz e atualizada.

Reforça o comprometimento da alta direção.

Melhora a adesão dos colaboradores.

Evita falhas que poderiam gerar multas, perdas financeiras ou danos à reputação.

Exemplo 1 – Uso de Senhas

Senha deve ter no mínimo 8 caracteres, incluindo letras maiúsculas, minúsculas, números e símbolos.

Proibido compartilhar senhas.

Alteração obrigatória a cada 90 dias.

Exemplo 2 – Classificação da Informação

Confidencial: acesso restrito, exige criptografia.

Interna: uso apenas dentro da organização.

Pública: pode ser divulgada sem restrições.

Exemplo 3 – Resposta a Incidentes

Qualquer e-mail suspeito deve ser reportado ao time de segurança em até 24h.

Vazamento de dados deve ser comunicado imediatamente à gestão.