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

A Política de Segurança da Informação (PSI) é um documento estratégico que define as regras, diretrizes e responsabilidades relacionadas à proteção da informação dentro de uma organização. Ela é essencial para garantir que todos os envolvidos saibam como lidar com dados e sistemas de forma segura e adequada.

Sem uma política formal, a segurança da informação fica restrita a boas intenções. A PSI é o instrumento que transforma essas intenções em ações claras e organizadas, orientando o comportamento dos colaboradores e padronizando procedimentos.

De forma prática, a PSI funciona como uma “lei interna” que estabelece como a informação deve ser tratada para garantir três princípios fundamentais da segurança da informação: confidencialidade, integridade e disponibilidade.

Esse documento deve estar alinhado com os objetivos estratégicos da empresa, com as legislações e normas aplicáveis (como a LGPD e a ISO/IEC 27001), além de considerar os riscos específicos do ambiente organizacional.

Entre os principais temas abordados pela PSI, destacam-se:

* **Uso aceitável de recursos tecnológicos**: define como os colaboradores podem utilizar a internet, os sistemas, os dispositivos e demais recursos de TI da organização, evitando usos indevidos ou que coloquem a empresa em risco.
* **Gestão de credenciais e senhas**: orienta como criar, armazenar e utilizar senhas com segurança. Também pode incluir o uso de autenticação multifator e recomendações para troca periódica de senhas.
* **Controle de acesso e confidencialidade**: estabelece quem pode acessar quais informações e em quais condições, com base em critérios como o princípio do menor privilégio. Também orienta sobre como compartilhar informações com segurança.
* **Armazenamento e descarte seguro de informações**: define como os dados devem ser armazenados durante seu uso e como devem ser descartados ao final de seu ciclo de vida, de forma a evitar vazamentos ou acessos indevidos.

É importante entender que a PSI não é um documento apenas formal ou burocrático. Ela deve ser vista como uma ferramenta prática e essencial para a gestão da segurança da informação. Sua aplicação correta ajuda a:

* Reduzir riscos operacionais e tecnológicos;
* Promover uma cultura organizacional voltada à segurança;
* Estabelecer responsabilidades claras;
* Atender às exigências legais e normativas de proteção de dados.

Além disso, em um cenário regulatório cada vez mais rigoroso — com leis como a **LGPD no Brasil** —, a PSI também tem papel central na **conformidade legal**, ajudando a evitar penalidades e a proteger a reputação da empresa.

**Em resumo:**

A Política de Segurança da Informação é a base que sustenta todas as ações de proteção de dados dentro da organização. Ela organiza as práticas, define limites e orienta comportamentos. Mais do que um documento, é uma ferramenta de governança e gestão de riscos que garante que a informação seja tratada com responsabilidade e segurança em todas as áreas da empresa.

**Atividades**

1. Qual dos princípios abaixo NÃO faz parte dos fundamentos da segurança da informação mencionados na PSI?

1. Confidencialidade
2. Integridade
3. Disponibilidade
4. Rentabilidade

2. A PSI deve estar alinhada com os seguintes elementos, EXCETO:

1. Objetivos estratégicos da empresa
2. Legislações e normas aplicáveis
3. Preferências pessoais dos colaboradores
4. Riscos específicos do ambiente organizacional

3. Sobre o uso aceitável de recursos tecnológicos, a PSI orienta que:

1. Os colaboradores podem usar os sistemas livremente, sem restrições
2. O uso da internet deve ser limitado apenas ao horário de almoço
3. Os recursos de TI devem ser utilizados de forma segura e responsável
4. O uso de dispositivos pessoais é obrigatório

4. Explique com suas palavras por que a PSI é considerada uma “lei interna” dentro da organização. Dê exemplos de como ela pode impactar o dia a dia dos colaboradores.

5. Em sua opinião, qual é a importância da PSI para garantir a conformidade legal em relação à proteção de dados? Relacione com a LGPD ou outras normas que você conheça.