A segurança da informação dentro de uma empresa não é apenas uma questão técnica, mas também de conformidade com normas e padrões reconhecidos. Essas normas servem como guias para garantir que os dados, processos e sistemas sejam protegidos de forma consistente, seguindo melhores práticas aceitas internacionalmente.

O objetivo deste módulo é apresentar as principais normas e padrões de segurança que empresas utilizam, explicando como elas se aplicam no dia a dia de um funcionário.

**1. Importância das normas e padrões**

Normas e padrões não são criados apenas para “cumprir exigências”, mas para estabelecer uma base sólida de segurança. Elas ajudam a padronizar processos, garantir qualidade, prevenir incidentes e facilitar auditorias.

**Exemplo prático:** Se todos os funcionários seguem um mesmo procedimento para criar senhas, o risco de falhas de segurança por senhas fracas é muito menor.

**2. Principais normas e padrões relevantes**

**2.1 ISO/IEC 27001 – Sistema de Gestão de Segurança da Informação**

* Define requisitos para implementar, manter e melhorar continuamente um sistema de gestão de segurança.
* Aplica-se a empresas de qualquer porte.
* Foco na proteção de dados e gestão de riscos.

**2.2 ISO/IEC 27002 – Boas práticas**

* Complementa a ISO 27001 com diretrizes práticas.
* Orienta sobre controle de acesso, uso de criptografia, segurança física, etc.

**2.3 NIST Cybersecurity Framework**

* Desenvolvido pelo Instituto Nacional de Padrões e Tecnologia dos EUA.
* Organiza a segurança em 5 funções: Identificar, Proteger, Detectar, Responder e Recuperar.

**2.4 LGPD e integração com normas**

* A LGPD também se alinha a normas como a ISO 27701 (focada em privacidade).
* Reforça a importância da proteção de dados pessoais.

**3. Como isso impacta o dia a dia do funcionário**

Mesmo que você não atue diretamente na área de TI, seguir normas e padrões influencia sua rotina.

**Exemplos:**

* Seguir protocolos para descarte de documentos físicos.
* Usar canais seguros para compartilhar informações internas.
* Participar de treinamentos obrigatórios.

**4. Boas práticas alinhadas a normas**

* Criar senhas fortes e renová-las periodicamente.
* Trancar a estação de trabalho ao se ausentar.
* Não compartilhar credenciais com colegas.
* Manter sistemas sempre atualizados.

As normas e padrões de segurança não são burocracia, mas ferramentas para criar um ambiente mais seguro e confiável. Funcionários que entendem e aplicam esses princípios contribuem diretamente para a proteção de dados e para a reputação da empresa.