A segurança no ambiente de trabalho vai muito além do uso de antivírus ou bloqueio de tela. Ela envolve um conjunto de atitudes e cuidados diários que reduzem os riscos de incidentes, vazamento de informações e até ameaças físicas. Funcionários são a primeira linha de defesa contra ataques — e, ao mesmo tempo, podem ser o elo mais fraco se não adotarem práticas corretas.

O objetivo deste módulo é apresentar boas práticas que todo colaborador deve seguir para contribuir com a proteção dos ativos da empresa.

**1. Segurança física**

A segurança física protege equipamentos, documentos e o acesso às áreas da empresa.

**Práticas importantes:**

* Mantenha portas e gavetas trancadas quando não estiver no ambiente.
* Use crachá de identificação e reporte imediatamente se ele for perdido.
* Não permita a entrada de pessoas não autorizadas.
* Posicione monitores de forma que informações confidenciais não sejam visíveis para terceiros.

**Exemplo prático:** Um visitante na empresa não deve ter acesso a áreas restritas sem acompanhamento.

**2. Segurança digital**

A segurança digital envolve o uso consciente e seguro de dispositivos e redes.

**Práticas importantes:**

* Utilize senhas fortes e únicas para cada sistema.
* Habilite autenticação de dois fatores sempre que possível.
* Nunca clique em links suspeitos ou baixe arquivos de fontes não confiáveis.
* Mantenha softwares e sistemas operacionais sempre atualizados.

**Exemplo prático:** Um simples clique em um link malicioso pode comprometer toda a rede corporativa.

**3. Proteção de informações**

Informações sensíveis exigem cuidado extra, tanto no meio digital quanto físico.

**Práticas importantes:**

* Classifique documentos de acordo com seu nível de confidencialidade.
* Não envie informações sigilosas por e-mail sem criptografia.
* Use pastas seguras ou sistemas autorizados para armazenamento.
* Descarte documentos impressos de forma segura (trituradores de papel, coleta seletiva segura).

**4. Postura em relação a e-mails e mensagens**

O phishing é uma das ameaças mais comuns. Treinar o olhar crítico para identificar fraudes é essencial.

**Práticas importantes:**

* Verifique o endereço de e-mail do remetente.
* Desconfie de mensagens urgentes pedindo dados pessoais.
* Não abra anexos suspeitos.
* Confirme solicitações sensíveis por outros canais antes de responder.

**5. Uso de dispositivos móveis**

Dispositivos móveis também representam riscos se não forem usados corretamente.

**Práticas importantes:**

* Configure bloqueio de tela automático.
* Evite conexões a redes Wi-Fi públicas sem VPN.
* Não armazene senhas ou dados sigilosos sem proteção.
* Mantenha aplicativos atualizados.

**6. Comportamento e conscientização**

O fator humano é determinante para a segurança.

**Práticas importantes:**

* Participe de treinamentos regularmente.
* Reporte incidentes imediatamente ao setor de TI.
* Não compartilhe informações corporativas em redes sociais.
* Siga sempre os procedimentos internos, mesmo que pareçam burocráticos.

**Exemplo prático:** Informar rapidamente sobre um e-mail suspeito pode evitar que outros colegas caiam no golpe.

**7. Conclusão**

Segurança no ambiente de trabalho é um esforço coletivo. Cada funcionário desempenha um papel crucial na prevenção de incidentes. Adotar boas práticas de forma consistente cria uma cultura organizacional forte e resiliente contra ameaças.