**ATIVIDADE 1 — Políticas de Segurança para Pequena Empresa Fictícia**

**Empresa Fictícia:** InfoPlus Solutions – Serviços de Suporte em TI  
 **Número de funcionários:** Aproximadamente 20  
 **Ativos principais:** Notebooks corporativos, rede Wi-Fi interna, sistema ERP em nuvem, dados de clientes

**1️ Política de Acesso e Controle de Usuários**

**Política:**

* Cada colaborador deve possuir credenciais únicas e intransferíveis.
* Permissões baseadas no **princípio do menor privilégio**.
* Senhas com validade de 90 dias, no mínimo 10 caracteres e MFA sempre que possível.
* Desativação imediata de contas de funcionários desligados.

**Justificativa:**  
Reduz riscos de uso indevido de contas e dificulta ataques por credenciais comprometidas.

**2️ Política de Uso de Dispositivos Móveis e Redes**

**Política:**

* Dispositivos móveis usados para trabalho devem ter criptografia de armazenamento, senha biométrica e app de gestão MDM.
* Acesso remoto somente via VPN com autenticação forte.
* Wi-Fi da empresa com SSID segregado para visitantes.
* É proibido instalar aplicativos não autorizados em dispositivos corporativos.

**Justificativa:**  
Protege dados contra perda, roubo e redes inseguras (BYOD apresenta riscos – Aula 06).

**3️ Diretrizes para Resposta a Incidentes de Segurança**

**Política:**

* Todo colaborador deve comunicar incidentes imediatamente ao responsável de segurança.
* Deve existir um fluxo de resposta com etapas: **identificação → contenção → erradicação → recuperação → lições aprendidas**.
* Registro obrigatório em um livro de incidentes para auditoria.

**Justificativa:**  
Reduz impacto e tempo de indisponibilidade, garantindo rastreabilidade e conformidade.

**4️ Política de Backup e Recuperação de Desastres**

**Política:**

* Backups diários automáticos para nuvem segura.
* Retenção de 30 dias e criptografia obrigatória dos backups.
* Testes trimestrais de restauração para validar integridade.
* Plano de continuidade documentado para eventos críticos.

**Justificativa:**  
Assegura **disponibilidade**, mesmo em caso de ataques de ransomware, falhas físicas ou humanas.