Medidas de Prevenção

1. **Implementação de um Firewall:** Utilize firewalls para filtrar tráfego de rede, bloqueando acessos não autorizados e impedindo ataques externos.
2. **Sistemas de Detecção e Prevenção de Intrusões (IDS/IPS):** IDS monitorar atividades suspeitas, enquanto IPS toma medidas automáticas para bloquear ataques em tempo real.
3. **Autenticação Multifator (MFA):** Reforce a segurança de acesso exigindo múltiplas formas de autenticação, como senhas e tokens ou biometria.
4. **Política de Atualização e Patch Management:** Mantenha sistemas, aplicativos e dispositivos atualizados com os patches mais recentes para corrigir vulnerabilidades.
5. **Segmentação de Rede:** Divida a rede em segmentos menores para limitar o acesso e conter ameaças caso uma área seja comprometida.
6. **Controle de Acesso Baseado em Privilégios:** Adote o princípio do menor privilégio, permitindo que usuários acessem apenas os recursos necessários para suas funções.
7. **Treinamento de Conscientização de Segurança:** Treine funcionários para identificar e evitar ameaças, como phishing e engenharia social.
8. **Criptografia de Dados:** Proteja dados sensíveis em trânsito e em repouso com métodos robustos de criptografia.
9. **Políticas de Senhas Fortes:** Exija senhas complexas, com combinações de letras, números e caracteres especiais, além de mudanças periódicas.
10. **Backup Regular e Seguro:** Realize backups frequentes e guarde-os em locais seguros e isolados da rede principal.