Configuração de sistemas de detecção de intrusão e prevenção de ataques:

Sistema de Detecção de Intrusão (IDS):

Configuração de Alertas: Configurar alertas em caso de atividades suspeitas na rede, como tentativas de acesso não autorizado ou varreduras de porta.

Sistema de Prevenção de Intrusão (IPS):

Bloqueio Automático: Implementar um IPS que bloqueie automaticamente tráfego malicioso identificado, prevenindo ataques antes que eles possam causar danos.

Análise de Tráfego em Tempo Real: Monitorar o tráfego de rede em tempo real para identificar padrões de comportamento anômalo que possam indicar um ataque.

Regras de Firewall: Configurar regras de firewall para bloquear tráfego não autorizado e permitir apenas comunicações essenciais e seguras.

Divisão de Rede: Dividir a rede em segmentos menores para limitar a propagação de ataques e isolar sistemas críticos de acesso geral.

Permissões Restritas: Implementar controle de acesso baseado em funções para garantir que usuários tenham apenas as permissões necessárias para suas funções.

Revisão Regular: Analisar logs de sistemas e redes regularmente para identificar e responder rapidamente a atividades suspeitas.

Verificação Adicional: Implementar autenticação multifator para adicionar uma camada extra de segurança no acesso a sistemas críticos.

Manutenção Regular: Garantir que todos os sistemas e softwares estejam atualizados com os patches de segurança mais recentes para proteger contra vulnerabilidades conhecidas.

Testes Periódicos: Realizar testes de penetração e avaliações de vulnerabilidade regularmente para identificar e corrigir pontos fracos na segurança.