Relatório de Avaliação de Risco de Segurança

# Parte 1: Ferramentas e métodos de hardening de rede selecionados

* Implementar autenticação multifator (MFA)  
  A autenticação multifator exige que o usuário utilize dois ou mais métodos de verificação antes de acessar a rede ou sistemas da empresa. Pode incluir senha + código via aplicativo autenticador, biometria ou token.
* Aplicar política de senhas fortes e exclusivas  
  Criar regras claras para senhas: mínimo de 12 caracteres, uso de letras maiúsculas e minúsculas, números e símbolos. Proibir o uso de senhas padrão e o compartilhamento entre funcionários.
* Manutenção e atualização das regras de firewall  
  Verificar e ajustar regularmente as regras dos firewalls para permitir apenas o tráfego autorizado e bloquear IPs suspeitos. Isso ajuda a proteger a rede de acessos indevidos.

# Parte 2: Recomendação e justificativa

1. Recomendação 1: Implementar autenticação multifator (MFA)  
   A MFA é eficaz porque impede que uma única credencial (como uma senha) seja suficiente para acessar sistemas críticos. Mesmo que uma senha seja descoberta por ataque de força bruta ou compartilhamento, o segundo fator bloqueia o acesso não autorizado. Além disso, a MFA desencoraja o compartilhamento de senhas, pois o segundo fator é pessoal.
2. Recomendação 2: Criar política de senhas fortes e exclusivas  
   Senhas fracas ou padrão facilitam a entrada de atacantes na rede. Com uma política robusta, o risco de sucesso de ataques por força bruta ou engenharia social diminui drasticamente. A política pode incluir a obrigatoriedade de trocar senhas a cada 90 dias, bloqueio após 5 tentativas incorretas, e proibição de reutilização de senhas antigas.
3. Recomendação 3: Atualizar regras de firewall regularmente  
   Firewalls são a primeira linha de defesa contra tráfego não autorizado. A ausência de regras de filtragem foi uma das falhas detectadas. Ao manter regras atualizadas, a organização reduz o risco de ataques DoS, DDoS, spoofing e exploração de vulnerabilidades conhecidas. A revisão deve ser feita quinzenalmente ou após qualquer incidente de segurança.