# Relatório de avaliação de risco de segurança

|  |
| --- |
| **Parte 1: Selecione até três ferramentas de proteção e métodos para implementar** |
| A seguir são sugeridos três métodos para endurecimento da segurança baseados no contexto atual da empresa.   * Política de controle de senhas mais rigorosas * Autenticação multifatorial (MFA) * Ferramenta SIEM para análise de log de rede |
|

|  |
| --- |
| **Parte 2: Explique suas recomendações** |
| Políticas de senhas mais rigorosas exigem que os usuários não utilizem sequências obvias de números e/ou letras, senhas que estejam nos dicionários mais utilizados, podem limitar a quantidade de tentativas de login, determinam padrões mínimos para cada senha, como quantidades mínima total de caracteres e mínimo de cada tipo (capitalizado, alfanumérico, caractere especial), podem exigir também uma frequência maior de alteração das senhas (ex. a cada 6 meses), estas medidas podem evitar que a maioria dos ataques de força bruta obtenham êxito.  A autenticação multifatorial exige que o usuário utilize ao menos um método extra para confirmar o acesso à uma conta, ou seja, além do login e senha, pode pedir um dado biométrico ou uma senha de uso único que pode ser enviada por email ou telefone, com isso, ainda que um usuário tenha o vazamento das suas credenciais o atacante não terá sucesso em utilizar sua conta, além disso, desencoraja o compartilhamento de senhas que sempre deveria ser individual.  Através dos logs de rede ferramentas SIEM podem analisar e monitoram a rede em tempo real, com isso, identifica qualquer atividade anormal envia alertas para a equipe de segurança cibernética que responde investigando e identificando e suprimindo potenciais ameaças. |