

# Respostas – Estudos de Caso e Exercícios de Revisão

## Estudo de Caso 1

1. 1. Sim, o firewall e o servidor Web da Linen Planet oferecem serviços de criptografia. Isso é indicado.
2. 2. O acesso poderia ser mais seguro utilizando autenticação multifator (MFA), evitando o compartilhamento de credenciais.

## Estudo de Caso 2

1. 1. A política da ATI pode parecer rígida, mas é justificável do ponto de vista da segurança da informação.
2. 2. Embora compreensível o desejo de Ron de navegar em sites recreativos após o expediente, ele violou a política.
3. 3. Andy deve considerar o histórico confiável de Ron e usar a situação como uma oportunidade educacional.

## Exercícios de Revisão – Aula 07

1. 1) Um pentest (teste de penetração) é uma simulação controlada de ataque a sistemas para identificar vulnerabilidades.
2. 2) Três ataques que afetam a disponibilidade:
  - DDoS (negação de serviço): sobrecarrega servidores com tráfego.
  - Ransomware: criptografa dados e impede o acesso.
  - Sabotagem interna: funcionário desativa sistemas críticos.
3. 3) O conceito é 'Conformidade'.
4. 4) Comparativo:
  - Firewall: controla o tráfego de rede com base em regras.
  - IDS: detecta atividades suspeitas, sem agir diretamente.
  - IPS: detecta e impede atividades maliciosas automaticamente.
5. 5) Três conselhos para proteger senhas:
  - Usar senhas fortes e únicas.
  - Ativar autenticação multifator.
  - Não compartilhar senhas e evitar escrevê-las em locais inseguros.
6. 6) a) Vulnerabilidade: porta USB exposta.  
b) Ameaça: malware via pen drive.  
c) Ação defensiva: desabilitar portas USB ou restringir uso por políticas.
7. 7) a) Vulnerabilidade: uso de software desatualizado.  
b) Ameaça: exploração de falhas conhecidas.  
c) Ação defensiva: manter atualizações e patches em dia.
8. 8) a) Ana deve cifrar a mensagem de Bob com a chave pública de Bob.  
b) Bob deve decifrar com sua chave privada.  
c) Para Carlos, Ana deve assinar a mensagem com sua chave privada.  
d) Carlos verifica com a chave pública de Ana.
9. 9.a) O certificado garante a identidade do site. O cliente usa a chave pública do banco para estabelecer uma conexão segura.
10. 9.b) Benefícios: confidencialidade e autenticação do site.
11. 10) Três registros importantes:
  - Logins e logouts.
  - Alterações de configurações.
  - Tentativas de acesso não autorizado.