**UC Sistemas Computacionais e Segurança – 2025.1**

**Exercícios de Revisão**

**Prof. Calvetti**

# Fontes de estudo principais

* Material curado da UC Sistemas Computacionais e Segurança no U-Life
* Curso Cisco Fundamentos de Segurança Cibernética
* Material das aulas

# Questões

1. O que é um *pentest*? Quais são as etapas de um *pentest*?

Pentest é um teste de invasão, onde especialistas simulam ataques a sistemas pra encontrar falhas de segurança.  
As etapas são:

* **Planejamento e escopo**: definir o que será testado.
* **Coleta de informações**: buscar dados sobre o sistema alvo.
* **Análise de vulnerabilidades**: identificar possíveis falhas.
* **Exploração**: tentar invadir o sistema.
* **Relatório**: documentar tudo o que foi encontrado.

1. Explique o funcionamento de 3 ataques de segurança cibernética que podem comprometer diretamente a DISPONIBILIDADE de sistemas.

* **Ataque DDoS**: é quando vários dispositivos atacam um servidor ao mesmo tempo, sobrecarregando-o até cair e ninguém mais conseguir acessar.
* **Malware (ransomware):** é um tipo de vírus que entra no sistema e bloqueia o acesso aos dados, geralmente pedindo resgate pra liberar**.**
* **Spyware**: é um tipo de vírus espião que se instala no sistema e fica coletando dados sem o usuário perceber. Além de ser uma ameaça à privacidade, ele pode deixar o sistema mais lento ou instável, afetando a disponibilidade com o tempo.

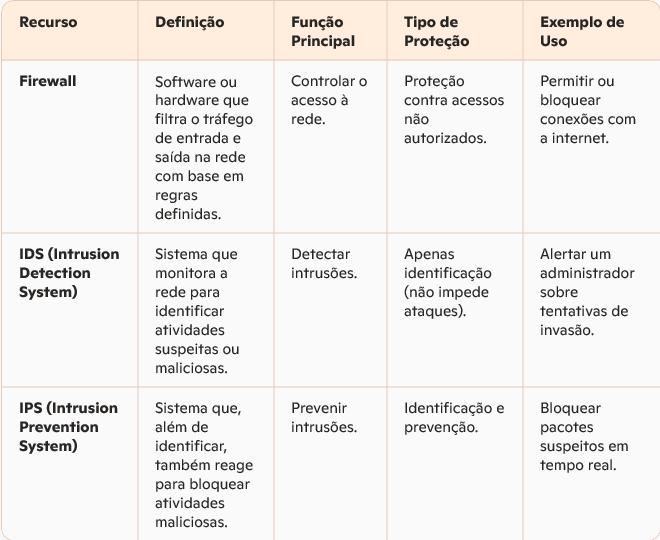
1. Leia o fragmento de texto a seguir.

Todas as empresas devem observar a legislação local, os seus regulamentos internos e as obrigações contratuais, além dos acordos internacionais. Os requisitos de segurança que uma empresa deve cumprir estão fortemente relacionados a isso. (HINTZBERGEN, 2018)

O texto acima se refere a um conceito que pode ser considerado importante quando se trata de segurança da informação. De qual conceito estamos falando (em uma palavra)?

**Resposta:** **Normas**

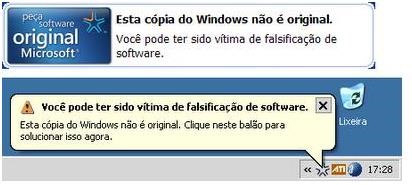
1. Existem vários recursos de software e hardware para estabelecer diversos níveis de segurança em uma rede de computadores. Entre outros, podemos citar os *firewalls* e os sensores (IDS e IPS). Faça um quadro comparativo resumindo as características de cada um dos três recursos.



1. Uma pessoa lhe procura e pede ajuda sobre formas de proteger as suas senhas. Cite pelo menos três conselhos que você daria a essa pessoa.

* **Use senhas fortes**: misture letras maiúsculas, minúsculas, números e símbolos. Evite datas de aniversário ou nomes óbvios.
* **Não use a mesma senha em tudo**: se uma for descoberta, as outras contas ficam em risco também.
* **Ative a verificação em duas etapas (2FA)**: assim, mesmo que alguém descubra sua senha, vai precisar de um código extra pra acessar.

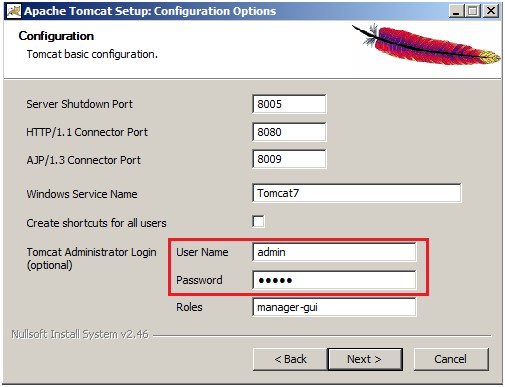
1. Observe a imagem a seguir.



Do ponto de vista da segurança da informação, identifique:

1. **A vulnerabilidade**: uso de software pirata ou não licenciado.
2. **A ameaça:** risco de malwares, falta de atualizações e falhas de segurança no sistema.
3. **Uma ação defensiva para mitigar a ameaça:** regularizar o sistema operacional com uma cópia original e manter ele sempre atualizado.

7) Observe a imagem a seguir.



Do ponto de vista da segurança da informação, identifique:

1. **A vulnerabilidade:** uso de credenciais padrão (usuário: admin) durante a configuração do Apache Tomcat.
2. **A ameaça:** invasores podem explorar essas credenciais conhecidas para obter acesso administrativo ao servidor.
3. **Uma ação defensiva para mitigar a ameaça:** alterar imediatamente o nome de usuário e senha padrão por credenciais fortes e únicas, além de limitar o acesso à interface administrativa.

8) Ana tem duas mensagens para enviar de forma criptografada para dois amigos: Bob e Carlos. Bob deseja receber a mensagem de maneira que apenas ele possa decifrá-la. Carlos não está preocupado com o sigilo da mensagem, mas deseja ter certeza de que foi mesmo Ana que a enviou. Assume que todos têm seu par de chaves pública e privada, que todas as chaves públicas são acessíveis. Visando a atender os requisitos de Bob e Carlos, descreva, **em termos de uso das chaves:**

1. como Ana deverá cifrar a mensagem antes de enviar para Bob;

Ela deve usar a **chave pública de Bob** para cifrar a mensagem. Assim, só ele poderá abrir.

1. como Bob deverá decifrar a mensagem de Ana corretamente;

Ele usa a **sua própria chave privada** para decifrar a mensagem que Ana mandou.

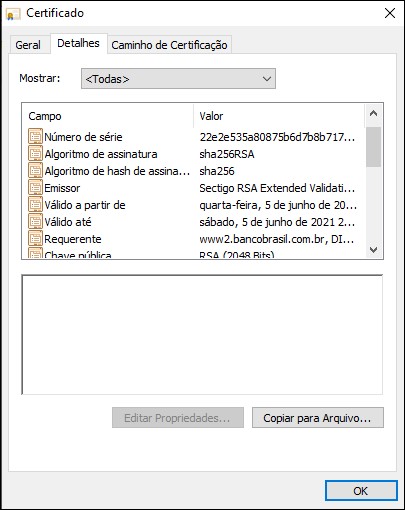
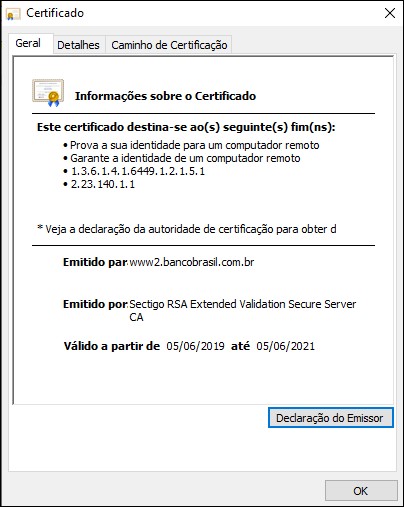
1. como Ana deverá cifrar a mensagem antes de enviar para Carlos;

Ela deve cifrar a mensagem usando **sua própria chave privada**. Isso mostra que foi ela mesma quem escreveu.

1. como Carlos deverá decifrar a mensagem de Ana corretamente.

Carlos usa a **chave pública de Ana** para abrir a mensagem e verificar que veio dela.

1. Observe as imagens a seguir:



As imagens apresentam informações do certificado digital do site [www.bb.com.br.](http://www.bb.com.br/) Com base nelas, responda:

* 1. Como se dá a utilização do certificado na origem e no destino? Identifique como são utilizadas as chaves criptográficas do Banco do Brasil.

Quando o cliente (você, no navegador) acessa o site do Banco do Brasil, o servidor envia o certificado digital para comprovar sua identidade. Esse certificado tem a chave pública do banco, que será usada para criar uma conexão segura (criptografada). A chave privada fica guardada com segurança no servidor do banco e é usada para decifrar dados enviados pelo cliente.

**Chave pública**: usada pelo cliente para cifrar os dados.

**Chave privada**: usada pelo banco para decifrar os dados.

* 1. Cite dois benefícios de segurança que uma transação eletrônica recebe com a utilização do certificado digital do Banco.

**Autenticidade** – Garante que você está realmente acessando o site oficial do Banco do Brasil, e não um falso (phishing).

**Criptografia dos dados** – Protege as informações trocadas (como senhas e dados bancários) contra interceptações.

1. Observe a imagem a seguir:



De acordo com a norma ISO 27002: 2013, “convém que registros (log) de eventos das atividades do usuário, exceções, falhas e eventos de segurança da informação sejam produzidos, mantidos e analisados criticamente, a intervalos regulares”. ABNT (2013).

Cite 3 registros importantes da atividade dos usuários que podem registrados para posterior auditoria de segurança.

t**entativas de login (bem-sucedidas e falhas)**  
– Ajuda a identificar acessos não autorizados ou possíveis ataques de força bruta.

**Acessos a arquivos e sistemas sensíveis**  
– Registra quem acessou quais dados e quando, garantindo rastreabilidade.

**Alterações em permissões ou configurações**  
– Mostra mudanças de privilégios, instalação de software ou alterações críticas no sistema.

# Referências

* ABNT (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS). **NBR ISO/IEC 27002:2013**: Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação. Rio de Janeiro, 2013.

* HINTZGBERGEN, Jule. **Fundamentos de Segurança da Informação**: com base na ISO 27001 e na ISO 27002. 3. ed. Brasport, Rio de Janeiro, 2018.