RT – CEISC

1) 2025. Em relação às ferramentas e técnicas utilizadas na proteção de sistemas e informações, assinale a alternativa correta.

a) Antivírus tem como função principal controlar o tráfego de rede entre diferentes ambientes.
b) Firewall atua como mecanismo de filtragem de tráfego, aplicando regras para permitir ou bloquear comunicações.
c) Anti-spyware é utilizado para criptografar dados sensíveis armazenados no sistema.
d) Autenticação multifatorial baseia-se exclusivamente no uso de senhas fortes.
e) Firewall substitui integralmente a necessidade de antivírus em um sistema seguro.

2) 2025. Em investigações digitais e na preservação da cadeia de custódia, funções hash são utilizadas para verificar a integridade de arquivos. Considerando os algoritmos MD5, SHA-1 e SHA-256, assinale a alternativa correta.

a) MD5 gera hash de 128 bits, SHA-1 de 160 bits e SHA-256 de 256 bits, sendo este último mais seguro.
b) SHA-1 é mais seguro que SHA-256 por utilizar maior complexidade matemática.
c) MD5, SHA-1 e SHA-256 produzem resumos criptográficos de mesmo tamanho e mesma resistência a colisões.
d) A aplicação de função hash impede qualquer modificação do arquivo original.
e) Funções hash são técnicas de criptografia reversível utilizadas para proteger o conteúdo do arquivo.

3) 2025. No âmbito da investigação criminal que envolve evidências digitais, o correto cumprimento do ciclo da prova digital é essencial para a validade da prova. Considerando as etapas do ciclo da prova digital e a análise de metadados, assinale a alternativa correta.

a) A análise de metadados ocorre exclusivamente na fase de apresentação da prova, quando o juiz avalia sua validade.
b) A etapa de preservação visa impedir qualquer acesso ao dispositivo, inclusive por peritos autorizados, até o trânsito em julgado.
c) Metadados podem fornecer informações relevantes como data, horário, dispositivo de origem e local aproximado de criação de arquivos.
d) A coleta da prova digital dispensa cuidados com integridade, desde que a análise seja realizada por perito oficial.
e) A apresentação da prova digital prescinde da demonstração da cadeia de custódia.

4) 2025. Durante uma investigação criminal, autoridades analisam conteúdos obtidos em redes sociais, aplicativos de mensagens instantâneas e plataformas de vídeo. Sobre a utilização dessas fontes como evidências digitais, assinale a alternativa correta.

a) Mensagens obtidas em aplicativos de mensageria instantânea são inválidas como prova, por não possuírem valor jurídico.
b) Conteúdos publicados em redes sociais dispensam qualquer tipo de verificação de autenticidade, por serem de acesso público.
c) Vídeos hospedados em plataformas digitais não contêm metadados úteis à investigação criminal.
d) Evidências digitais provenientes de redes sociais e mensageria devem ser coletadas e preservadas de forma a garantir autenticidade e integridade.
e) Prints de tela substituem integralmente a necessidade de técnicas periciais na coleta de provas digitais.

5) 2025. Em investigação de crimes praticados por meio de dispositivos móveis, foi detectado o uso de criptografia em diferentes camadas: armazenamento do aparelho, backups e aplicativos de mensageria. Sobre as implicações práticas da criptografia simétrica e assimétrica na investigação digital, assinale a alternativa correta.

a) Se um arquivo estiver criptografado com AES-256, é sempre possível descriptografá-lo apenas com a chave pública do usuário.

b) Em geral, a quebra de criptografia simétrica moderna (como AES-256) por força bruta é inviável na prática, tornando a obtenção de chaves ou desbloqueio legalmente assistido uma estratégia mais relevante.

c) A criptografia assimétrica elimina a necessidade de qualquer segredo, pois a chave privada pode ser divulgada sem prejuízo da segurança.

d) Em mensageria com criptografia ponta a ponta, a interceptação de tráfego na rede permite obter o texto em claro, pois a cifra só ocorre no servidor.

a) Incorreta.

AES é simétrico. Para descriptografar, é necessária a chave secreta correspondente. Chave pública é conceito de criptografia assimétrica.

06) 2025. Durante a perícia em um notebook apreendido, a equipe identificou que certos arquivos estavam protegidos por criptografia e que o investigado utilizava um aplicativo de comunicação com criptografia ponta a ponta. Considerando os conceitos de criptografia simétrica e assimétrica, seus algoritmos e propriedades, assinale a alternativa correta.

a) Criptografia simétrica utiliza um par de chaves (pública e privada), sendo o RSA um exemplo clássico desse tipo de criptografia.

b) Criptografia assimétrica emprega a mesma chave para cifrar e decifrar dados, sendo o AES um exemplo típico desse modelo.

c) Algoritmos de hash, como SHA-256 e MD5, são técnicas de criptografia reversível utilizadas para garantir confidencialidade de arquivos apreendidos.

d) Em aplicações práticas, a criptografia simétrica é utilizada para cifrar grandes volumes de dados com algoritmos como AES ou ChaCha20, enquanto a criptografia assimétrica é empregada para troca segura de chaves, autenticação ou assinatura digital, com algoritmos como RSA e ECC.

e) A criptografia ponta a ponta dispensa qualquer mecanismo de autenticação, pois o sigilo do conteúdo é suficiente para garantir a identidade dos interlocutores.

7) FUNDATEC - RS - Técnico em Informática

As assertivas a seguir tratam dos conceitos básicos das redes LAN, MAN e WAN:

I. LAN (*Local Area Networks*): abrange computadores interligados em uma área restrita de redes WANs. II. MAN (*Metropolitan Area*): quando uma rede WAN tem abrangência geográfica apenas dentro de uma cidade, é chamada de MAN. III. WAN (*Wide Area Networks*): é definida como uma rede de computadores distantes e interconectados.

Quais estão corretas?

a) Apenas I.

b) Apenas III.

c) Apenas I e II.

d) Apenas II e III.

e) I, II e III.

8) FUNDATEC - RS - Técnico em Informática

Relacione a Coluna 1 à Coluna 2, associando o tipo de rede de computador à área de abrangência.

Coluna 1

1. WAN.
2. MAN.
3. LAN.

Coluna 2

( ) Escola.
( ) Cidade.
( ) Residência.
( ) País.

A ordem correta de preenchimento dos parênteses, de cima para baixo, é:

Alternativas

a) 1 – 2 – 1 – 3.
b) 2 – 1 – 2 – 3.
c) 2 – 3 – 2 – 1.
d) 3 – 2 – 3 – 1.
e) 3 – 1 – 3 – 2.

9) 2025. A autenticação multifatorial é um mecanismo de segurança amplamente utilizado para reforçar o controle de acesso a sistemas computacionais e serviços digitais. Sobre esse tipo de autenticação, assinale a alternativa correta.

a) A autenticação multifatorial utiliza apenas um fator de autenticação, normalmente baseado em senha, desde que ela seja considerada forte.
b) A autenticação multifatorial exige a combinação de dois ou mais fatores distintos, como algo que o usuário sabe, algo que possui ou algo que é.
c) A autenticação multifatorial elimina totalmente a necessidade de senhas, baseando-se exclusivamente em fatores biométricos.
d) A autenticação multifatorial garante segurança absoluta contra invasões, tornando impossível o acesso não autorizado.
e) A autenticação multifatorial é restrita a ambientes governamentais, não sendo aplicada em sistemas corporativos ou comerciais.

10) 2025. O protocolo Ethernet é amplamente utilizado em redes locais cabeadas. Sobre suas características, assinale a alternativa correta.

a) Opera na camada de rede do modelo OSI e é responsável pelo endereçamento lógico.
b) Utiliza exclusivamente endereços IP para identificar dispositivos na rede local.
c) Define regras de acesso ao meio físico e utiliza endereços MAC para identificar os dispositivos.
d) É um protocolo orientado à conexão e garante entrega confiável dos dados.
e) Atua apenas em redes sem fio, sendo equivalente ao Wi-Fi.

11) 2025. O protocolo IP é essencial para o encaminhamento de pacotes na Internet. Sobre IPv4 e IPv6, assinale a alternativa correta.

a) O IPv4 e o IPv6 utilizam endereços de 32 bits, diferenciando-se apenas pela notação.
b) O IPv6 surgiu para substituir o TCP, oferecendo maior segurança e velocidade.
c) O IPv6 utiliza endereços de 128 bits, ampliando significativamente o espaço de endereçamento.
d) O IPv4 elimina a necessidade de NAT devido à grande quantidade de endereços disponíveis.
e) O IPv4 e o IPv6 são protocolos orientados à conexão.

12) 2025. O protocolo TCP é utilizado por aplicações que exigem confiabilidade na transmissão de dados. Sobre o TCP, assinale a alternativa correta.

a) É um protocolo não orientado à conexão e não realiza controle de erros.
b) Garante entrega confiável, ordenada e com controle de fluxo e congestionamento.
c) Não utiliza numeração de sequência para os dados transmitidos.
d) É utilizado exclusivamente por aplicações de tempo real, como streaming ao vivo.
e) Atua na camada de enlace do modelo OSI.

13) 2025. O protocolo UDP apresenta características distintas em relação ao TCP. Assinale a alternativa correta.

a) É orientado à conexão e garante entrega confiável dos dados.
b) Realiza retransmissão automática de pacotes perdidos.
c) Implementa controle de congestionamento e fluxo.
d) Prioriza velocidade, não garantindo entrega nem ordenação dos pacotes.
e) Atua na camada de aplicação do modelo OSI.

14) 2025. O protocolo DNS é fundamental para a navegação na Internet. Sobre sua função, assinale a alternativa correta.

a) Realiza a tradução de endereços IP em endereços MAC.
b) Associa nomes de domínio a endereços IP.
c) Distribui automaticamente endereços IP aos dispositivos da rede.
d) Atua exclusivamente na camada de enlace do modelo OSI.
e) Utiliza apenas o protocolo TCP para suas consultas.

15) O protocolo DHCP facilita a configuração de redes IP. Sobre esse protocolo, assinale a alternativa correta.

a) Exige que cada endereço IP seja configurado manualmente.
b) É responsável pela tradução de nomes de domínio.
c) Fornece automaticamente parâmetros como IP, máscara, gateway e DNS.
d) Opera exclusivamente sobre o protocolo TCP.
e) Substitui o protocolo IP em redes locais.

16) O protocolo SNMP é utilizado para gerenciamento de redes. Assinale a alternativa correta.

a) É utilizado para transferência segura de arquivos.
b) Permite o gerenciamento e monitoramento de dispositivos de rede.
c) Substitui protocolos de roteamento dinâmico.
d) Atua apenas em redes sem fio.
e) Opera exclusivamente sobre o protocolo TCP.