MATERIAL ESPECIAL

AULÃO DA MADRUGADA

12 ANOS

QUESTÕES DE INFORMÁTICA E TECNOLOGIA

CARREIRAS POLICIAIS | 7 QUESTÕES DE ALTO NÍVEL

ASSUNTOS TRABALHADOS

- GOOGLE DRIVE | PERMISSÕES E COMPARTILHAMENTO
- IPSEC | VPN | MODOS TÚNEL E TRANSPORTE
- METADADOS | CLASSIFICAÇÃO E SEGURANÇA
- ENGENHARIA SOCIAL | PRINCIPAIS TÉCNICAS
- CADEIA DE CUSTÓDIA | EVIDÊNCIAS DIGITAIS
- DEEP WEB | INDEXAÇÃO E ACESSO
- DARK WEB | TOR | ROTEAMENTO ONION

AULA AO VIVO | ACESSE PELO QR CODE FINAL

PROFESSOR DEODATO NETO

Informática para concursos públicos | 09 de setembro de 2026

QUESTÃO 01

GOOGLE DRIVE | PERMISSÕES E COMPARTILHAMENTO

Um administrador de TI de uma repartição pública, responsável pela gestão do ambiente Google Workspace institucional, foi consultado por servidores sobre os diferentes níveis de permissão de compartilhamento de arquivos e pastas no Google Drive. Sobre o tema, analise as afirmativas a seguir.

I. No compartilhamento de arquivos do Google Workspace, o nível de permissão “Leitor” permite a visualização do conteúdo, mas não a inserção de comentários nem a edição do arquivo.

II. O nível de permissão “Comentador” permite a inserção de comentários e sugestões no documento, sem conferir, todavia, permissão para alterar diretamente o conteúdo original do arquivo.

III. Quando um arquivo é compartilhado como “Qualquer pessoa com o link” na função de Editor, qualquer usuário que obtenha o link poderá editá-lo, independentemente de outras restrições de domínio eventualmente configuradas pelo administrador da organização.

IV. As permissões concedidas a uma pasta no Google Drive são, por padrão, herdadas pelos arquivos nela armazenados, de modo que um usuário com permissão de Editor sobre a pasta poderá, em regra, editar os arquivos nela contidos, salvo se as permissões desses arquivos tiverem sido configuradas individualmente.

V. O proprietário (owner) de um arquivo no Google Drive é sempre e exclusivamente o usuário que o criou originalmente, não sendo possível, em nenhuma hipótese, transferir essa titularidade para outra conta dentro da mesma organização.

VI. A permissão de “Editor” concedida a um usuário permite, por padrão e sem exceção, que esse usuário altere as configurações de compartilhamento do arquivo e adicione novos colaboradores.

A I, II, VI.

B II, IV, V.

C I, II, IV.

D III, IV, VI.

E I, III, V.

QUESTÃO 02

IPSEC | VPN | MODOS TÚNEL E TRANSPORTE

Sobre o protocolo IPsec e seus modos de operação, no contexto de redes privadas virtuais (VPN), analise as afirmativas a seguir.

I. No modo túnel do IPsec, todo o pacote IP original, cabeçalho e dados, é encapsulado dentro de um novo pacote IP, sendo esse o modo tipicamente empregado em VPNs site a site entre gateways de rede.

II. No modo transporte do IPsec, apenas a carga útil (payload) do pacote é protegida, permanecendo o cabeçalho IP original inalterado, sendo esse modo mais comumente utilizado em comunicações diretas entre dois hosts finais.

III. O cabeçalho AH (Authentication Header) do IPsec tem por finalidade primária garantir a confidencialidade dos dados transmitidos, mediante cifragem do conteúdo do pacote, não oferecendo, todavia, qualquer garantia quanto à integridade das informações.

IV. O protocolo ESP (Encapsulating Security Payload) pode ser configurado para oferecer tanto confidencialidade, mediante cifragem dos dados, quanto integridade e autenticação, sendo, por isso, mais frequentemente utilizado que o AH isoladamente em implementações práticas de VPN.

V. O modo túnel do IPsec é adequado à interligação de redes inteiras, como duas filiais de uma organização, ao passo que o modo transporte, por preservar o cabeçalho IP original, é mais adequado a cenários em que ambos os pontos da comunicação já atuam como as próprias extremidades finais do tráfego protegido.

VI. Independentemente do modo empregado (túnel ou transporte), o IPsec estabelece obrigatoriamente uma camada adicional de criptografia sobre o protocolo HTTPS já existente na comunicação, não sendo capaz de operar em conexões que não utilizem originalmente esse protocolo de aplicação.

A I, II, IV, V.

B I, III, VI.

C II, IV, VI.

D I, III, IV, V.

E II, III, V.

QUESTÃO 03

METADADOS | CLASSIFICAÇÃO E SEGURANÇA

Sobre metadados e sua classificação, analise as afirmativas a seguir.

I. Metadados descritivos são aqueles voltados à identificação e à localização de um recurso, incluindo elementos como título, autor e palavras-chave, sendo tipicamente empregados em catálogos e mecanismos de busca.

II. Metadados estruturais descrevem como as partes de um objeto digital composto se relacionam entre si, como a ordem das páginas de um documento digitalizado ou dos capítulos de uma obra, distinguindo-se, nesse aspecto, dos metadados descritivos.

III. Metadados administrativos compreendem informações voltadas à gestão de um recurso digital, podendo abranger, entre outros aspectos, dados técnicos de criação do arquivo, informações sobre direitos de uso e dados relacionados à preservação digital do recurso.

IV. Um arquivo de imagem digital, por sua própria natureza binária, não é capaz de conter metadados embutidos referentes à data de captura ou às coordenadas geográficas de sua criação, sendo tais informações necessariamente armazenadas em arquivo apartado.

V. A remoção de metadados de um arquivo, antes de seu compartilhamento público, pode constituir boa prática de segurança da informação e de proteção de dados pessoais, na medida em que tais metadados podem conter informações sensíveis não destinadas à divulgação.

VI. Metadados técnicos e metadados de direitos (rights management) são, na literatura especializada, tratados como categorias inteiramente apartadas dos metadados administrativos, não guardando qualquer relação de subordinação ou de pertencimento a essa categoria mais ampla.

A I, II, III, V.

B I, IV, VI.

C II, III, VI.

D I, III, IV, V.

E II, IV, V, VI.

QUESTÃO 04

ENGENHARIA SOCIAL | PRINCIPAIS TÉCNICAS

Sobre engenharia social e suas principais técnicas, analise as afirmativas a seguir.

I. Phishing e spear phishing distinguem-se, essencialmente, pelo grau de direcionamento do ataque: enquanto o phishing tradicional costuma ser disparado de forma massiva e genérica, o spear phishing é direcionado a um indivíduo ou grupo específico, com informações previamente coletadas sobre a vítima.

II. Vishing e smishing são variações de engenharia social que utilizam, respectivamente, chamadas de voz e mensagens de texto (SMS) como vetor do ataque, em vez do correio eletrônico tipicamente associado ao phishing.

III. Pretexting caracteriza-se pela criação de um cenário ou de uma identidade falsa, previamente elaborada pelo atacante, para obter a confiança da vítima e induzi-la a fornecer informações ou a realizar determinada ação.

IV. Tailgating (ou piggybacking) é técnica de engenharia social restrita ao ambiente puramente digital, não guardando qualquer relação com o acesso físico não autorizado a instalações ou a ambientes restritos de uma organização.

V. Baiting caracteriza-se pela oferta de algo atrativo à vítima, como um dispositivo de armazenamento aparentemente esquecido em local público, usado como isca para induzi-la a executar uma ação que comprometa a segurança, como conectar o dispositivo a um computador.

VI. Por depender fundamentalmente da persuasão e da manipulação psicológica da vítima, e não da exploração de falhas técnicas de sistemas, a engenharia social é, em regra, mitigada exclusivamente por meio de controles técnicos de segurança, sendo dispensável, nesse contexto, qualquer investimento em capacitação e conscientização dos usuários.

A I, II, III, V.

B I, IV, VI.

C II, III, IV.

D III, IV, V, VI.

E I, II, V, VI.

QUESTÃO 05

CADEIA DE CUSTÓDIA | EVIDÊNCIAS DIGITAIS

Sobre a cadeia de custódia de evidências digitais e suas etapas, analise as afirmativas a seguir.

I. A cadeia de custódia de evidências digitais tem início desde o momento em que o vestígio é identificado e reconhecido como potencialmente relevante para a investigação, e não apenas a partir de sua efetiva coleta física ou lógica.

II. A etapa de acondicionamento da evidência digital volta-se à sua preservação adequada, por meio, por exemplo, de embalagens antiestáticas, lacres invioláveis e cópias forenses (imagens bit a bit), de modo a impedir alterações no conteúdo original.

III. Uma vez concluída a etapa de coleta da evidência digital, encerra-se, por completo, a necessidade de documentação da cadeia de custódia, sendo o registro de toda movimentação subsequente do vestígio (transporte, armazenamento, acesso) providência dispensável para fins de validade probatória.

IV. A etapa de transporte da evidência digital deve ser documentada de modo a registrar quem a transportou, por qual meio e em que condições, preservando-se a rastreabilidade do vestígio até sua chegada ao local de armazenamento ou de análise.

V. A etapa de análise da evidência digital, realizada preferencialmente sobre uma cópia forense e não sobre o dispositivo original, tem por finalidade extrair e interpretar as informações relevantes à investigação, subsidiando a etapa final de apresentação dos resultados, inclusive em juízo.

VI. A eventual quebra da cadeia de custódia em qualquer de suas etapas é circunstância irrelevante para a valoração da prova digital em juízo, não sendo, em nenhuma hipótese, motivo apto a suscitar questionamento sobre a integridade ou a autenticidade do vestígio apresentado.

A I, II, IV, V.

B I, III, VI.

C II, IV, VI.

D III, IV, V, VI.

E I, II, III, V.

QUESTÃO 06

DEEP WEB | INDEXAÇÃO E ACESSO

Sobre a deep web, analise as afirmativas a seguir.

I. A deep web compreende todo o conteúdo da internet não indexado pelos mecanismos de busca convencionais, categoria que abrange, predominantemente, conteúdo lícito, como bancos de dados acadêmicos, sistemas internos de organizações e caixas de correio eletrônico.

II. O acesso a conteúdos hospedados na deep web pressupõe, em todos os casos, a utilização de navegadores ou de softwares específicos de anonimização, não sendo possível o acesso a esse tipo de conteúdo por meio de um navegador convencional.

III. Um extrato bancário disponibilizado a um correntista mediante autenticação em um sistema de internet banking é exemplo de conteúdo tipicamente classificado como pertencente à deep web, por não ser indexado nem acessível a mecanismos de busca convencionais.

IV. A extensão da deep web, em termos de volume de dados, é, segundo estimativas amplamente aceitas na literatura especializada, significativamente inferior à da chamada surface web (internet indexada e de acesso público), invertendo-se essa proporção apenas no caso específico da dark web.

V. A existência da deep web decorre, em essência, de uma característica técnica de indexação, a ausência de rastreamento do conteúdo por robôs de busca (crawlers), e não necessariamente da natureza lícita ou ilícita do conteúdo nela hospedado.

A I, III, V.

B I, II, IV.

C II, III, V.

D III, IV, V.

E I, II, III.

QUESTÃO 07

DARK WEB | TOR | ROTEAMENTO ONION

Sobre a dark web e a tecnologia de roteamento onion, analise as afirmativas a seguir.

I. A dark web utiliza, como uma de suas tecnologias características, o roteamento onion (onion routing), no qual o tráfego é encapsulado em múltiplas camadas sucessivas de criptografia, removidas progressivamente por cada nó intermediário até alcançar o destino.

II. Na rede Tor, cada nó intermediário do circuito de roteamento onion tem acesso simultâneo tanto ao endereço de origem quanto ao endereço de destino final da comunicação, o que constitui, precisamente, o fundamento técnico de seu anonimato.

III. Domínios com a extensão “.onion” são acessíveis exclusivamente por meio de navegadores ou softwares configurados para operar na rede Tor, não sendo resolvidos por servidores DNS convencionais utilizados na navegação comum da internet.

IV. O circuito estabelecido pela rede Tor costuma envolver, tipicamente, ao menos três nós: um nó de entrada (guarda), um ou mais nós intermediários e um nó de saída, sendo o nó de saída aquele por meio do qual o tráfego, ao deixar a rede Tor, pode tornar-se visível ao destino final.

V. A utilização da rede Tor, por si só, confere anonimato absoluto ao usuário, tornando tecnicamente inviável, em qualquer circunstância, a identificação de sua origem, ainda que associada a outras técnicas de investigação ou a falhas de configuração do próprio usuário.

VI. A dark web constitui subconjunto da deep web, caracterizado por exigir softwares ou configurações específicas de acesso, como a rede Tor, não se confundindo, portanto, com a totalidade do conteúdo não indexado que compõe a deep web.

A I, III, IV, VI.

B I, II, V.

C II, IV, VI.

D III, IV, V.

E I, II, III, VI.

AULÃO DA MADRUGADA 12 ANOS

A AULA É AO VIVO.
A APROVAÇÃO É O FOCO.

AULA AO VIVO | ENTRE PELO QR CODE

ESTUDE COM O PROFESSOR DEODATO NETO

09 de setembro de 2026

Questões estratégicas, explicação direta e foco na sua aprovação

TRANSFORMANDO SONHOS EM APROVAÇÕES

INSTAGRAM

@profdeodatoneto

WHATSAPP

67 99217-6565

SITE

Acesse o portal

AULA AO VIVO

Acesse a aula ao vivo

APONTE A CÂMERA E ENTRE NA AULA.

Professor Deodato Neto | Informática para concursos públicos