CÂMARA MUNICIPAL DE BELO HORIZONTE/MG

CONCURSO PÚBLICO
EDITAL Nº 1/2023

ANALISTA DE TECNOLOGIA DA INFORMAÇÃO – ÁREA DE DESENVOLVIMENTO DE SISTEMA

Manhã

Tipo 1 - BRANCA

Organizadora:

INSTITUTO CONSULPLAN

LÍNGUA PORTUGUESA

A importância da educação e conscientização no combate à violência feminina

No contexto atual, é alarmante constatar que muitas mulheres ainda desconheçam os diferentes tipos de violência feminina perpetrados contra elas. Essa falta de conhecimento não apenas contribui para a perpetuação do ciclo de abuso, mas também as impede de buscar ajuda e se proteger adequadamente. Dentro dessa realidade preocupante, destacam-se diversos tipos de violência feminina, cada um com suas características e impactos específicos.

A violência física, por exemplo, manifesta-se através de agressões diretas como socos, chutes e empurrões, deixando marcas visíveis e emocionais profundas. Já a violência psicológica, talvez menos evidente, é igualmente devastadora, minando a autoestima e o bem-estar emocional da vítima por meio de humilhações, xingamentos e ameaças constantes.

A violência sexual é outra forma de agressão que merece atenção especial. Ela engloba qualquer tipo de abuso, coerção ou intimidação sexual não consentida, deixando cicatrizes emocionais que muitas vezes perduram por toda a vida. Enquanto isso, a violência patrimonial é uma realidade cruel na qual a vítima é submetida ao controle abusivo de seus bens e recursos financeiros, limitando sua independência e liberdade.

Por fim, a violência moral, muitas vezes subestimada, também causa danos significativos ao expor a intimidade da mulher, difamando-a publicamente e comprometendo sua dignidade e reputação.

Para combater essa falta de conhecimento e conscientizar as mulheres sobre seus direitos e formas de se protegerem, é fundamental implementar programas educacionais desde cedo, principalmente nas escolas. Educar crianças e adolescentes sobre respeito, igualdade de gênero e prevenção da violência é essencial para criar uma sociedade mais justa e igualitária.

As escolas desempenham um papel fundamental nesse processo, pois são espaços privilegiados para a disseminação de conhecimento e valores. Ao incluir em suas grades curriculares conteúdos relacionados à violência de gênero, as escolas contribuem para a formação de cidadãos mais conscientes e engajados na luta contra a violência feminina. Além disso, é importante que as instituições de ensino ofereçam espaços seguros e acolhedores onde os alunos possam discutir abertamente questões relacionadas à violência de gênero, esclarecer dúvidas e buscar apoio em casos de violência.

Além disso, é crucial que o papel da mulher como mãe seja valorizado e discutido dentro das famílias. Conversas abertas sobre questões relacionadas à violência de gênero e o ensino aos filhos sobre o respeito e a valorização das mulheres desde cedo são eficazes na promoção de mudanças culturais e comportamentais.

Outra medida importante é a adoção de políticas mais rigorosas pelas plataformas digitais, que devem coibir publicações agressivas ou que promovam a violência contra as mulheres. A fiscalização rigorosa nessas plataformas pode ajudar a prevenir a disseminação de discursos de ódio e a proteger as mulheres do assédio *online*.

As plataformas digitais têm uma visibilidade ampla e a capacidade de disseminar informações rapidamente. Portanto, é essencial que utilizemos essas ferramentas de forma responsável e ética, promovendo a conscientização e o combate à violência feminina em todas as esferas da sociedade.

É essencial que a sociedade se una para garantir que essas leis sejam implementadas efetivamente e que as mulheres tenham acesso à informação, justiça e proteção necessárias para viverem livres de violência.

(Advogado Paulo Meira Passos, Diretor-Chefe da Meira Passos Advogados e Advogado da Comissão da OAB-MG. Disponível em: <https://www.hojeemdia.com.br/opiniao/. Acesso em: fevereiro de 2024.)

Questão 01

Acerca do emprego do acento indicativo de crase no título do texto, pode-se afirmar que:

A) É facultativo, considerando que o termo regente pertence ao gênero masculino.
B) É facultativo, já que o termo regente trata-se de uma expressão composta por um substantivo e adjetivo.
C) É obrigatório, reconhecendo-se a exigência da regência nominal estabelecida e o gênero do termo regido.
D) É obrigatório, reconhecendo-se a exigência da regência verbal estabelecida e a classificação morfológica do termo regido.

Questão 02

Considerando-se que o texto apresenta recursos e processos argumentativos para a construção de posicionamentos do enunciador acerca do tema tratado assim como de subtemas a ele relacionados, a seguir os trechos destacados apresentam expressão subjetiva na construção de tais posicionamentos, tendo direta relação com os processos citados, com EXCEÇÃO de:

A) "*A violência sexual é outra forma de agressão que merece atenção especial.*" (3º§)
B) "*A violência física, por exemplo, manifesta-se através de agressões diretas como socos, chutes e empurrões,* [...]" (2º§)
C) "*No contexto atual, é alarmante constatar que muitas mulheres ainda desconheçam os diferentes tipos de violência feminina* [...]" (1º§)
D) "*Dentro dessa realidade preocupante, destacam-se diversos tipos de violência feminina, cada um com suas características e impactos específicos.*" (1º§)

Questão 03

Em relação ao título do texto e às relações morfossintátitcas e semânticas estabelecidas em sua construção pode-se afirmar que:

A) O termo "violência" atua como determinante de "feminina".
B) O termo "feminina" atua como determinante de "violência".
C) O termo "combate" está determinado pela expressão "violência feminina".
D) A ausência do artigo definido diante do termo "educação" torna o seu sentido genérico.

Questão 04

O título "A importância da educação e conscientização no combate à violência feminina" atribuído ao texto refere-se diretamente às ideias trazidas ao texto nos parágrafos indicados a seguir:

A) 3º e 4º parágrafos.
B) 5º e 6º parágrafos.
C) 1º ao 5º parágrafo.
D) 5º ao 10º parágrafo.

Questão 05

"*Essa falta de conhecimento não apenas contribui para a perpetuação do ciclo de abuso, mas também as impede de buscar ajuda e se proteger adequadamente.*" (1º§) A locução conjuntiva "mas também", nesse contexto:

A) Estabelece uma ideia de acréscimo em relação à oração posterior.
B) Estabelece uma relação de oposição, pois opõe "a falta de conhecimento" ao referido impedimento.
C) Estabelece relação de acréscimo, adição, desempenhando a mesma função de uma conjunção aditiva.
D) Não estabelece relação de oposição entre as duas orações, mas entre o período destacado e ideia expressa no período seguinte.

Questão 06

Acerca do conectivo sublinhado em *"Educar crianças e adolescentes sobre respeito, igualdade de gênero e prevenção da violência é essencial <u>para</u> criar uma sociedade mais justa e igualitária."* (5º§), pode-se afirmar que há a indicação de uma ideia de:

A) Retificação.
B) Efeito visado.
C) Efeito contingente.
D) Consequência desejada.

Questão 07

Considerando o emprego dos mecanismos de coesão textual no texto assim como sua relevância para que a mensagem tenha a devida compreensão, pode-se afirmar que no primeiro parágrafo do texto, a manutenção do elemento introduzido "muitas mulheres" pode ser identificada em:

A) Uma ocorrência apenas.
B) Duas ocorrências apenas.
C) Três ocorrências no total.
D) Seis ocorrências no total.

Questão 08

"*Ela engloba qualquer tipo de abuso, coerção ou intimidação sexual não consentida, deixando cicatrizes emocionais <u>que</u> muitas vezes perduram por toda a vida.*" (3º§) O pronome relativo destacado foi empregado como recurso coesivo que estabelece, no enunciado, relação de referência com:

A) Os tipos de abuso sofridos pelas mulheres.
B) A marcação temporal indicada: toda a vida.
C) Os abusos específicos: coerção e intimidação sexual.
D) Consequências mencionadas tais como cicatrizes emocionais.

Questão 09

"*Dentro dessa realidade preocupante, destacam-se diversos tipos de violência feminina, cada um com suas características e impactos específicos.*" (1º§) A flexão no plural da forma verbal empregada no período anterior justifica-se, pois:

A) A forma verbal deve concordar com o sujeito composto apresentado.
B) A forma verbal deve concordar com o sujeito que também está no plural.
C) O verbo impessoal não apresenta variação, apenas uma única forma: terceira pessoa do plural.
D) A forma na terceira pessoa do plural é característica do sujeito indeterminado conforme é visto no período.

Questão 10

No último parágrafo do texto, é possível reconhecer a retomada de um posicionamento do enunciador e uma referência a ideias propositivas em relação à situação-problema apresentada, que é um dos recursos textuais característicos

A) do texto injuntivo.
B) do texto prescritivo.
C) do discurso indireto.
D) do discurso dissertativo.

Questão 11

Segundo as informações e ideias trazidas ao texto, é correto afirmar que:

A) O autor estabelece uma afirmativa hipotética acerca da violência psicológica, apresentando também algumas de suas consequências.
B) Ao dizer que a violência sexual "merece atenção especial", a autora explicita que tal tipo de violência pressupõe um melhor atendimento às vítimas que os demais.
C) O controle dos bens está diretamente relacionado à violência contra o indivíduo nos mais diversos segmentos sociais; sem distinção de classe, idade ou situação econômica.
D) Em oposição ao que é possível constatar em situações históricas passadas, a maioria das mulheres pode constatar e reconhecer-se como participante de um grupo que não mais está silenciado.

Questão 12

Em "*Enquanto isso, a violência patrimonial é uma realidade cruel na qual a vítima é submetida ao controle abusivo de seus bens e recursos financeiros, limitando sua independência e liberdade.*" (3º§), a expressão introdutória do período destacado indica:

A) Temporalidade concomitante.
B) A consumação de um processo.
C) Ocasião referente ao momento exclusivo da enunciação.
D) Frequência de um fato independentemente de eixo referencial.

Questão 13

No trecho "*As escolas desempenham um papel fundamental nesse processo, pois são espaços privilegiados para a disseminação de conhecimento e valores.*" (6º§), a argumentação do articulista mostra:

A) Uma afirmativa seguida de uma oração explicativa relacionada ao tema textual.
B) A apresentação de um fato hipotético apontado como uma afirmativa indiscutível.
C) Um tangenciamento do tema, indicando um desvio aceitável em relação ao citado.
D) O emprego do argumento de autoridade, considerando a qualificação informada acerca do autor.

Questão 14

Considerando o contexto, pode-se afirmar que, dentre os termos destacados a seguir, tem seu significado expresso de forma correta o indicado em:

A) *"é alarmante constatar"* / contundente
B) *"constatar que muitas mulheres"* / averiguar
C) *"tipos de violência feminina perpetrados contra elas."* / imergidos
D) *"desconheçam os diferentes tipos de violência feminina"* / experienciam

Questão 15

A repetição indevida de palavras e/ou expressões pode comprometer o texto em relação ao nível de linguagem e clareza na transmissão da mensagem produzida. Assim, pode-se observar a seguir o emprego de termos que funcionam como elementos de coesão que mantêm o referente textual já introduzido e que impedem tal inadequação, com EXCEÇÃO de:

A) "*As escolas desempenham um papel fundamental nesse processo*, [...]" (6º§)
B) "*Conversas abertas sobre questões relacionadas à violência de gênero* [...]" (7º§)
C) "*Ao incluir em suas grades curriculares conteúdos relacionados à violência de gênero*, [...]" (6º§)
D) "*Além disso, é crucial que o papel da mulher como mãe seja valorizado e discutido dentro das famílias.*" (7º§)

Questão 16

Dentre os fragmentos destacados e as formas verbais grifadas, difere-se quanto ao emprego do modo verbal, apenas:

A) "*É essencial que a sociedade se una* [...]" (10º§)
B) "*As plataformas digitais têm uma visibilidade ampla* [...]" (9º§)
C) "*As escolas desempenham um papel fundamental nesse processo* [...]" (6º§)
D) "*Além disso, é importante que as instituições de ensino ofereçam espaços seguros e acolhedores* [...]" (6º§)

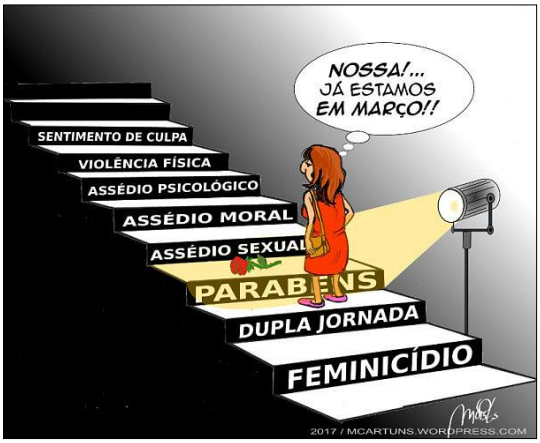
Questão 17

Considerando-se que o último parágrafo do texto apresenta uma conclusão, indique a alternativa cuja reescrita atende à adequação de acordo com a norma padrão da língua.

A) É essencial que a sociedade se una para garantir que essas leis; sejam, pois, implementadas efetivamente e que as mulheres tenham acesso à informação, justiça e proteção necessárias para viverem livres de violência.
B) É essencial, pois que a sociedade se una para garantir que essas leis sejam implementadas efetivamente e que as mulheres tenham acesso à informação, justiça e proteção necessárias para viverem livres de violência.
C) É essencial, pois, que a sociedade se una para garantir que essas leis sejam implementadas efetivamente e que as mulheres tenham acesso à informação, justiça e proteção necessárias para viverem livres de violência.
D) É essencial que a sociedade, se una para garantir que: essas leis sejam implementadas efetivamente e que as mulheres tenham acesso à informação, justiça e proteção necessárias para viverem livres de violência.

Questão 18

De acordo com as características do gênero textual apresentado a seguir, pode-se afirmar que:



(Charge do Moises Cartuns. Disponível em: https://blogs.correiobraziliense.com.br/aricunha/laranjal-e-feminicidio-mostram-um-brasil-que-nao-respeita-suas-mulheres/.)

A) Apresenta como principal característica o discurso claro e objetivo.
B) Trata-se de um texto híbrido considerando-se a linguagem empregada.
C) Mostra-se relacionado ao tipo textual narrativo, tendo presente em sua construção os mesmos elementos.
D) Tem como principal finalidade persuadir o leitor acerca de um tema de relevância social por meio de argumento e contra-argumento.

Questão 19

Algumas palavras podem apresentar dúvida em relação ao registro de acordo com a ortografia oficial. Em "*Já a violência psicológica, talvez menos evidente, é igualmente devastadora, minando a autoestima e o bem-estar emocional da vítima por meio de humilhações, xingamentos e ameaças constantes.*" (2º§), observa-se o emprego e registro correto de vocábulo em que o uso do hífen é evidenciado. Indique, a seguir, a alternativa que apresenta INCORREÇÃO de acordo com a norma padrão da língua.

A) micro-ondas; sem-terra; contra-ataque.
B) além-túmulo; aquém-mar; bem-nascido.
C) inter-racial; sub-bibliotecário; sub-região.
D) auto-conhecimento; anti-derrapante; semi-reta.

Questão 20

Considerando-se a produção de sentido da palavra introdutória do parágrafo destacado a seguir: "*Portanto, é essencial que utilizemos essas ferramentas de forma responsável e ética, promovendo a conscientização e o combate à violência feminina em todas as esferas da sociedade.*" (9º§), pode-se afirmar que o mesmo sentido é produzido pelo destacado em:

A) Em meio ao caos diário, entretanto, sobrevivemos.
B) A chuva parou um pouco; logo, podemos prosseguir.
C) A luta pode prosseguir, mas a vitória já está determinada.
D) O empreendimento começou a fracassar, pois alguns já começaram a desanimar.

CONHECIMENTOS ESPECÍFICOS DO CARGO

Questão 21

O MD5 – *Message Digest Algorithm 5*, é um algoritmo de função *hash* utilizado na criptografia de dados capaz de gerar um valor *hash* único e fixo para um conjunto de dados, independentemente do tamanho original dos dados. Sobre as características do MD5, assinale a alternativa que corresponde ao tamanho, em *bits*, do *hash* gerado pelo algoritmo MD5.

A) 64 *bits*.
B) 128 *bits*.
C) 256 *bits*.
D) 512 *bits*.

Questão 22

Algoritmos de criptografia são fundamentais para proteger informações confidenciais durante armazenamento e transmissão, garantindo a segurança e a privacidade dos dados. Sobre as características dos algoritmos de criptografia existentes, assinale a alternativa que corresponde ao algoritmo de criptografia mais seguro e resistente a uma ampla variedade de ataques.

A) DES.
B) AES.
C) RSA.
D) MD5.

Questão 23

A assinatura digital é utilizada para garantir autenticidade, integridade e não repúdio de documentos eletrônicos. Considerando as características de assinatura digital, marque V para as afirmativas verdadeiras e F para as falsas.

( ) Utiliza a criptografia assimétrica, onde o signatário usa sua chave privada para assinar digitalmente o documento.
( ) A validade de uma assinatura digital depende da integridade do certificado digital associado ao signatário.
( ) Garante que o documento não tenha sido alterado desde que foi assinado.

A sequência está correta em

A) F, F, F.
B) F, V, F.
C) V, F, V.
D) V, V, V.

Questão 24

Certificado digital é um documento eletrônico que contém informações sobre a identidade de uma entidade, como uma pessoa, organização ou dispositivo, juntamente com sua chave pública. Considere os conceitos fundamentais de certificado digital e assinale a afirmativa correta em relação ao que acontece quando um certificado digital expira.

A) É automaticamente renovado por mais um ano.
B) Torna-se inválido e não pode mais ser usado para autenticação.
C) É marcado como suspenso e pode ser reativado mediante solicitação.
D) Ele é excluído permanentemente do repositório da autoridade certificadora.

Questão 25

Segurança física e lógica são dois aspectos fundamentais da segurança da informação que visam proteger ativos e recursos valiosos de uma organização contra ameaças internas e externas. Ambos os aspectos desempenham papéis complementares na garantia da integridade, confidencialidade e disponibilidade dos dados e sistemas. Sobre as características da segurança física e lógica, assinale a alternativa que se refere à uma medida considerada como uma prática de segurança física.

A) Criptografar dados sensíveis.
B) Implementar câmeras de segurança.
C) Utilizar *firewalls* para proteger a rede.
D) Atualizar regularmente o sistema operacional.

Questão 26

O tempo médio para remediar um incidente é uma métrica importante na segurança da informação, sendo utilizada para avaliar a eficácia da resposta a incidentes de uma organização e sua capacidade de mitigar os danos causados por ameaças cibernéticas. Sobre a métrica do tempo médio para remediar um incidente, analise as alternativas, e assinale a afirmativa INCORRETA.

A) É o tempo necessário para identificar uma ameaça.
B) É o tempo médio para atualizar o sistema operacional.
C) É o tempo necessário para corrigir uma vulnerabilidade.
D) É o tempo médio entre a detecção e correção de um incidente de segurança.

Questão 27

Ataques são ações maliciosas ou tentativas deliberadas de comprometer a segurança de sistemas de computador, redes, dados ou usuários. Essas atividades são realizadas por indivíduos ou grupos com o objetivo de acessar informações confidenciais, interromper serviços, causar danos ou obter ganhos financeiros ilícitos. Sobre os tipos de ataques existentes, assinale a alternativa que se refere a um ataque de *phishing*.

A) Ataque que explora vulnerabilidades de *software*.
B) Ataque que envia *spam* para várias contas de *e-mail*.
C) Ataque que interrompe o funcionamento de um sistema.
D) Ataque que utiliza engenharia social para enganar as vítimas.

Questão 28

Métricas e indicadores desempenham papel crucial na avaliação e gestão da segurança da informação em organizações. Métricas são medidas quantitativas que ajudam a monitorar o desempenho e a eficácia das estratégias de segurança, enquanto os indicadores são dados específicos que fornecem direcionamentos sobre o estado da segurança da informação. Em relação às características da métrica de tempo médio para detectar ameaças no contexto de segurança, assinale a afirmativa INCORRETA.

A) Mede a rapidez com que uma ameaça é identificada.
B) Avalia a eficácia das políticas de segurança da informação.
C) Avalia a satisfação dos funcionários em relação à segurança da informação.
D) Determina o número de ameaças detectadas em determinado período de tempo.

Questão 29

***Tokens* e *smartcards* são dispositivos utilizados em sistemas de segurança da informação para fornecer autenticação e autorização de usuários. Sobre as características desses dispositivos, analise as afirmativas e assinale a INCORRETA.**

A) *Tokens* são mais seguros do que *smartcards* devido à sua natureza física.
B) *Tokens* são dispositivos de autenticação que geram senhas únicas e dinâmicas para cada *login*.
C) *Smartcards* armazenam dados sensíveis, como chaves de criptografia, em um *microchip* embutido.
D) *Smartcards* exigem um leitor de cartão para serem utilizados, enquanto *tokens* geralmente possuem um pequeno *display* para exibir senhas dinâmicas.

Questão 30

SHA-1 (*Secure Hash Algorithm 1*) é um algoritmo de função de *hash* desenvolvido pela NSA (Agência de Segurança Nacional dos Estados Unidos) utilizado em protocolos de segurança e em sistemas de autenticação. Sobre as características do algoritmo SHA-1, assinale a afirmativa INCORRETA.

A) Produz uma saída de *hash* de 128 *bits*.
B) Não é possível recuperar a mensagem original a partir do *hash*.
C) Não pertence à família SHA-3, que inclui algoritmos como SHA-256 e SHA-512.
D) Não é seguro usar este algoritmo na criptografia de senhas devido às suas vulnerabilidades.

Questão 31

O controle de acesso em sistemas de informação é um componente essencial da segurança da informação, projetado para proteger os dados e recursos contra acesso não autorizado. Sobre o controle de acesso baseado em função (RBAC), assinale a afirmativa correta.

A) Concede acesso com base na experiência técnica do usuário.
B) Concede acesso com base na localização geográfica do usuário.
C) Concede acesso com base em funções ou cargos dentro da organização.
D) Concede acesso com base na posição hierárquica do usuário na organização.

Questão 32

Protocolos criptográficos são conjuntos de regras e procedimentos que permitem comunicação segura e protegida entre sistemas de computador por meio do uso de técnicas de criptografia. Tendo em vista os conceitos fundamentais desses protocolos, marque V para as afirmativas verdadeiras e F para as falsas.

( ) O protocolo IPsec é utilizado para estabelecer conexões VPN (*Virtual Private Network*) para comunicações seguras pela *internet*.
( ) O protocolo SSH é usado exclusivamente para criptografia de *e-mails*.
( ) O protocolo PGP é utilizado para criptografia de *e-mails* e arquivos, assinatura digital e autenticação de identidade.

A sequência está correta em

A) F, F, F.
B) F, V, F.
C) V, F, V.
D) V, V, V.

Questão 33

Segurança de banco de dados consiste em proteger os dados armazenados em um Sistema de Gerenciamento de Banco de Dados (SGBD) contra acesso não autorizado, alterações não autorizadas e perda de integridade. Considerando os conceitos fundamentais de segurança de banco de dados, marque V para as afirmativas verdadeiras e F para as falsas.

( ) As senhas de acesso aos bancos de dados devem ser armazenadas em texto simples para facilitar a autenticação.
( ) O *backup* regular dos bancos de dados é uma prática importante para garantir a recuperação de dados em caso de falhas ou ataques.
( ) Auditorias de banco de dados são úteis apenas para fins de conformidade regulatória e não contribuem para a segurança geral do banco de dados.

A sequência está correta em

A) F, F, F.
B) F, V, F.
C) V, F, V.
D) V, V, V.

Questão 34

Protocolos criptográficos desempenham papel fundamental na segurança da informação, garantindo confidencialidade, integridade e autenticidade dos dados transmitidos pela *internet*. Sobre os protocolos SSL/TLS, qual opção é considerada o protocolo de segurança da *internet* mais seguro?

A) SSL 2.0.
B) SSL 3.0.
C) TLS 1.0.
D) TLS 1.3.

Questão 35

A criptografia é uma técnica de segurança fundamental na proteção de dados e comunicações. Ela envolve a transformação de informações em um formato ilegível, chamado de texto cifrado, usando algoritmos matemáticos e chaves de criptografia. Levando-se em consideração as características fundamentais da criptografia, marque V para as afirmativas verdadeiras e F para as falsas.

( ) A criptografia de chave pública é geralmente mais lenta do que a criptografia de chave simétrica.
( ) Um exemplo de algoritmo de criptografia assimétrica é o RSA.
( ) Em sistemas criptográficos simétricos, a segurança depende principalmente do segredo da chave compartilhada entre as partes.

A sequência está correta em

A) F, F, F.
B) F, V, F.
C) V, F, V.
D) V, V, V.

Questão 36

As organizações realizam diversas transações eletrônicas durante a execução das suas atividades operacionais, com aplicações de uso interno e externo, desenvolvidas em diferentes linguagens de programação, que persistem os dados coletados em um Sistema de Gerenciamento de Banco de Dados. O armazenamento desses dados deve ser revestido de uma boa camada de segurança, bem como as aplicações que consomem e alimentam esse banco, pois as consultas dinâmicas desenvolvidas nessas aplicações, se não protegidas adequadamente, produzem vulnerabilidades que podem causar danos de magnitude catastrófica em uma base de dados, permitindo acessos indevidos através de ataques conhecidos como *SQL Injection*. Sobre esse tipo de ataque, analise as afirmativas a seguir.

I. Consiste basicamente em digitar comandos *SQL*, exclusivamente do tipo *DML*, nos *inputs* de formulários da aplicação.
II. Um teste de *SQL Injection* pode ser em uma tela de *login* de um sistema *WEB* qualquer, digitar o comando *' or 1=1 or 'a' = 'a* no campo de *login*, preencher o campo senha com qualquer valor e clicar no botão que efetua o *login* para verificar se o sistema realizará a autenticação.
III. Uma forma de proteger a aplicação do *SQL Injection* é realizar a validação/tratamento das informações manualmente ou utilizar *frameworks* de persistência/ORM que possuam mecanismos para evitar esse tipo de ataque.

Está correto o que se afirma apenas em

A) I.
B) II.
C) III.
D) II e III.

Questão 37

O LDAP (*Lightweight Directory Access Protocol*) é um protocolo para serviços de diretório que possibilita a organização dos dados de forma hierárquica, possibilitando que usuários de uma rede local ou pública possam localizar dados sobre organizações, indivíduos e outros recursos, como dispositivos, arquivos e aplicações; devido à sua configuração otimizada o protocolo é considerado leve se comparado a outros protocolos existentes no mercado. Comercialmente, o protocolo pode ser utilizado para disponibilizar um local centralizado para autenticação de usuários em um ambiente de rede, permitindo uma conexão única onde um usuário autorizado possa validar o acesso para múltiplas aplicações e serviços sem a necessidade um novo *logon* para cada operação. Por se tratar geralmente de um serviço baseado na *web*, o recurso está sujeito a um tipo de ataque conhecido como *LDAP Injection* que consiste em explorar as entradas de autenticação para obter informações confidenciais do recurso. Sobre o ataque, assinale a afirmativa INCORRETA.

A) É comum devido à falta de interfaces de consulta LDAP parametrizadas e mais seguras.
B) Uma forma de defesa ao ataque é tratar o escape de todas as variáveis usando a função de codificação LDAP correta.
C) Como medida preventiva ao ataque, os filtros LDAP com os caracteres especiais ** [ ] \ 0 NULL* devem possuir tratamento de escape.
D) Outra forma de defesa ao ataque é utilizar estruturas que protegem automaticamente contra a injeção de LDAP como, por exemplo, o *LINQ to Active Directory*.

Questão 38

Para elaborar um *software* bem estruturado é fundamental que a equipe técnica dedique um tempo para estudo, análise e aplicação de uma estrutura de dados compatível com o projeto, para que as informações geradas pela aplicação possam ser acessadas, processadas e persistidas com agilidade e eficiência. A aplicação dessas estruturas permite que os programadores representem e manipulem os dados de forma eficaz dentro da aplicação desenvolvida. Considere que dentro de determinado *software* foi desenvolvido o seguinte código em *Python* (versão 3):

```
1   class Nx:
2       def __init__(self, ch=None, lef=None, rig=None):
3           self.ch = ch
4           self.lef = lef
5           self.rig = rig
6
7       def __repr__(self):
8           return '%s <- %s -> %s' % (self.lef and self.lef.ch,
9                                      self.ch,
10                                     self.rig and self.rig.ch)
11
12  rl = Nx(3)
13  rl.lef = Nx(5)
14  rl.rig  = Nx(1)
```

O algoritmo apresenta uma estrutura de dados do tipo:

A) Fila.
B) Grafo.
C) *Hash table*.
D) Árvore binária.

Questão 39

Determinado usuário com conhecimentos avançados em tecnologia da informação estava navegando em um portal de notícias da sua cidade, quando observou que era possível inserir trechos em HTML nos campos de comentários das reportagens. Esse comportamento chamou a atenção do usuário, que resolveu testar se também era possível adicionar códigos *JavaScript;* logo, foi verificado que o teste foi bem-sucedido, pois nenhum bloqueio foi detectado ao adicionar esse tipo de código. A vulnerabilidade observada pelo usuário na situação hipotética torna possível um ataque conhecido como *Cross-Site Scripting* (XSS), que explora a falta de tratamento adequado das informações digitadas pelos usuários. Analise as afirmativas a seguir sobre o tipo de ataque em questão.

I. O objetivo é enviar comandos *JavaScript* e *css* que serão executados pelo servidor com comportamentos prejudiciais ao usuário.
II. Uma forma de burlar algoritmos de tratamento de XSS é utilizar os códigos *JavaScript* mascarados como, por exemplo, em notação hexadecimal.
III. Um exemplo de ataque pode ser: adicionar um código *JavaScript* para coletar os dados de autenticação digitados pelo usuário e, em seguida, realizar uma requisição *ajax* para outra aplicação enviando-os.

Está correto o que se afirma apenas em

A) I.
B) II.
C) III.
D) II e III.

Questão 40

No desenvolvimento de uma aplicação, uma etapa fundamental e primordial durante todo o processo é a construção de algoritmos. O algoritmo é uma sequência de raciocínios, instruções e operações que trabalham conjuntamente para alcançar um objetivo. Um sistema é constituído de diversos algoritmos que recebem múltiplas entradas de dados, manipulando-as através de processamento, para que sejam geradas saídas com informações úteis e relevantes para os usuários. Sobre essas estruturas, marque V para as afirmativas verdadeiras e F para as falsas.

( ) A propriedade finitude afirma que um algoritmo deve ter um número finito de instruções, garantindo que ele termine sua execução em algum momento.
( ) A propriedade do determinismo afirma que um algoritmo deve produzir o mesmo resultado sempre que for executado com determinados dados de entrada, produzindo sempre um resultado correto.
( ) Um algoritmo de ordenação pode ser utilizado para organizar uma lista de elementos em ordem crescente ou decrescente.
( ) Um algoritmo guloso pode ser utilizado para resolver um problema dividindo-o em problemas menores para resolvê-los recursivamente.

A sequência está correta em

A) V, V, F, F.
B) V, F, V, F.
C) F, V, F, V.
D) F, F, V, V.

Questão 41

Certa empresa atua na construção de soluções tecnológicas para o ramo contábil. A empresa trabalha com um modelo de desenvolvimento ágil que busca uma entrega efetiva de valor para os seus clientes a cada *sprint*. O time principal dessa equipe é composto de diversos programadores, QA's e outros atores necessários para o funcionamento adequado da metodologia utilizada. Um determinado desenvolvedor desse time recebeu uma demanda de construção de uma rotina simples de cálculo que será adicionada no sistema como um utilitário; o recurso simplesmente recebe um valor bruto e um percentual de desconto a ser aplicado como entrada de dados do usuário e, após o processamento, deverá ser exibido o valor líquido. Para auxiliar o desenvolvedor na construção dessa demanda, foi anexado um modelo de código na linguagem *Python* (versão 3) com a seguinte estrutura:

```
1  lValorBruto = float(input("Informe o valor bruto: "))
2  lPercentualDesconto = float(input("Informe o percentual de desconto: "))
3  lValorLiquido = lValorBruto - (lValorBruto * (lPercentualDesconto / 100))
4  print("Valor líquido: " + str(lValorLiquido))
```

Considerando o exemplo recebido, o desenvolvedor deve registrar na sua documentação técnica que o mesmo estava em uma estrutura de controle básica do tipo:

A) Contínua.
B) Repetição.
C) Sequencial.
D) Condicional.

Questão 42

A tecnologia da informação é composta de múltiplas áreas que atuam em conjunto para a construção e manutenção de ferramentas e soluções tecnológicas para diversos grupos de usuários distintos. Uma área relevante nesse contexto é a ciência da computação, que trata da análise de complexidade de algoritmos e outras diversas atribuições. Essa análise consiste em estudar o desempenho de algoritmos em termos de tempo e espaço, determinando o crescimento da quantidade de recursos computacionais necessários para executar um algoritmo à medida que o tamanho da entrada de dados escala, colaborando ativamente para o desenvolvimento de *softwares* eficientes e cada vez mais adequados para as tarefas que foram projetados. Sobre esse conceito, analise as afirmativas a seguir.

I. O tempo de execução de um algoritmo é a quantidade de tempo necessária para executar o algoritmo completamente.
II. Uma complexidade $O(n^2)$ indica que o tempo de execução do algoritmo cresce quadraticamente ao tamanho da entrada.
III. Uma complexidade $O(1)$ indica que o tempo de execução do algoritmo cresce proporcionalmente ao tamanho da entrada.

Está correto o que se afirma em

A) I, II e III.
B) I e II, apenas.
C) I e III, apenas.
D) II e III, apenas.

Questão 43

Determinado usuário utilizou o seu computador pessoal com um *browser* de sua preferência, para realizar *login* no *site* de uma instituição financeira que ele utiliza. Após realizar corretamente a autenticação com o seu usuário/senha, ele recebeu um *e-mail* em nome dessa mesma instituição que possuía um *link* para acesso à conta; sem desconfiar da procedência da mensagem, o usuário clicou no *link* e prosseguiu com o preenchimento dos dados para uma transferência bancária. O sistema da instituição financeira em questão não apresentava um mecanismo eficiente de proteção para a utilização de *cookies* e, com isso, um *hacker* explorou essa vulnerabilidade capturando o *cookie* original da autenticação que foi realizada, para promover um ataque conhecido como *Cross-Site Request Forgery* (CSRF), forjando uma requisição *cross-site* de um *site* para o outro. Sobre o ataque sofrido pelo usuário, assinale a afirmativa INCORRETA.

A) Alguns *Frameworks* como *Joomla*, *Spring*, *Struts*, *Ruby on Rails* e *.NET* possuem suporte CSRF integrado.
B) As transações realizadas em várias etapas e a utilização de HTPS são consideradas medidas de prevenção efetivas.
C) A construção de URL ou *script* de exploração aliada às práticas de engenharia social são consideradas estratégias para promover o ataque.
D) A proteção com *tokens* CSRF às solicitações de mudança de estado e a validação dessas no *backend* são consideradas formas de prevenção.

Questão 44

As aplicações *WEB* facilitam consideravelmente o cotidiano dos usuários, automatizando cadastros, promovendo ambientes eletrônicos para compras e digitalizando diversos procedimentos que demandavam um tempo considerável para serem operacionalizados. Em um sistema eletrônico de vendas, uma medida protetiva e necessária para a aplicação é que o armazenamento de dados sensíveis como, por exemplo, o número de cartão de crédito, seja armazenado de forma criptografada, aumentando a segurança do dado sensível dentro da aplicação. Para minimizar os riscos de vulnerabilidades causadas pelo armazenamento inseguro de dados criptografados, são medidas que podem ser aplicadas de forma preventiva, EXCETO:

A) Desativar o armazenamento em *cache* para respostas que contenham dados confidenciais.
B) Gerar chaves de forma criptograficamente aleatória e armazenadas na memória como um *array* de *bytes*.
C) Armazenar senhas usando fortes funções de *hash* adaptáveis e saltadas com um fator de trabalho como *Argon2*, SHA1, *bcrypt* ou PBKDF2.
D) Classificar os dados processados, armazenados ou transmitidos por um aplicativo, identificando os dados confidenciais, conforme legislação de privacidade, requisitos regulamentares ou necessidades de negócios.

Questão 45

Em aplicações, *WEB* é uma prática comum a utilização de sessões para realizar o armazenamento do estado de uma aplicação; porém, geralmente, esse recurso realiza o procedimento no *servidor web* da aplicação e não no próprio navegador do usuário, como ocorre quando se utilizam os *cookies*. Um exemplo prático da utilização desse recurso em uma aplicação dessa natureza pode ser o armazenamento de dados sensíveis como usuário e *e-mail* em uma rotina de autenticação. Apesar das sessões utilizarem o servidor para a sua operacionalização, existem vulnerabilidades no mecanismo que podem ser exploradas pelos *hackers* para promover a quebra do gerenciamento da sessão de uma aplicação. Analise as afirmativas a seguir sobre práticas seguras para o gerenciamento de sessões.

I. Gerar um novo identificador de sessão quando houver uma nova autenticação.
II. Configurar o atributo "*secure*" para *cookies* transmitidos através de uma conexão TLS.
III. Configurar os *cookies* com o atributo *"HttpOnly"*, a menos que seja explicitamente necessário ler ou definir os valores dos mesmos através de *scripts* do lado cliente da aplicação.

Está correto o que se afirma em

A) I, II e III.
B) I e II, apenas.
C) I e III, apenas.
D) II e III, apenas.

Questão 46

Analise as afirmativas a seguir.

I. As métricas de segurança são estabelecidas a partir de análises qualitativas realizadas sobre os dados relacionados à segurança da informação coletados em diversos departamentos da organização.
II. Métricas de segurança são utilizadas para justificar os investimentos em segurança da informação; podem contribuir para reduzir os riscos ou aprimorar a postura de segurança de uma organização.
III. O processo de cálculo e análise de métricas de segurança deve ser executado de maneira contínua.
IV. Porcentagem de pontos de acesso IEEE 802.11 que utilizam o protocolo WPA2 e porcentagem do tempo em que o servidor está disponível são exemplos de métricas que podem ser utilizadas para avaliar a infraestrutura e serviços.

Está correto o que se afirma apenas em

A) I e II.
B) III e IV.
C) I, II e III.
D) II, III e IV.

Questão 47

Qual das seguintes afirmações descreve corretamente a classificação de informações em segurança da informação?

A) Engloba apenas a proteção de dados contra ameaças externas.
B) É uma prática opcional e não é necessária para a proteção dos ativos de informação.
C) Refere-se apenas à categorização de dados em diferentes níveis de confidencialidade.
D) Abrange a identificação, rotulagem e proteção de dados sensíveis ou críticos em conformidade com as políticas de segurança da organização.

Questão 48

Qual é o objetivo principal da auditoria de posição no contexto do ambiente de tecnologia da informação?

A) Realizar testes de segurança nos sistemas de informação.
B) Implementar novos controles de segurança da informação.
C) Avaliar o desempenho dos usuários de tecnologia da informação.
D) Revisar e avaliar as recomendações e verificar a aplicação dos controles.

Questão 49

A segurança da informação é um aspecto crucial para proteger os sistemas contra ameaças externas e garantir integridade, confidencialidade e disponibilidade dos dados. Diversas medidas e tecnologias são empregadas para fortalecer a segurança dos sistemas e minimizar os riscos de ataques cibernéticos. Como os sistemas de segurança podem aumentar a disponibilidade dos sistemas?

A) Criptografando os dados armazenados.
B) Restringindo o acesso apenas a usuários autorizados.
C) Implementando *firewalls* para bloquear o tráfego malicioso.
D) Utilizando equipamentos, aplicativos e servidores redundantes.

Questão 50

Os sistemas de autenticação foram concebidos para confirmar se o usuário é autêntico, realizar a autorização e, principalmente, a auditoria. Essas soluções ficaram conhecidas como AAA. Qual protocolo é amplamente utilizado para comunicação entre dispositivos de rede e servidores – uma solução padrão para AAA?

A) LDAP.
B) SNMP.
C) TCP/IP.
D) RADIUS.

Questão 51

***Firewall* é um exemplo de segurança lógica, uma medida essencial para proteger redes de computadores contra ameaças cibernéticas. Essa ferramenta é responsável por monitorar e controlar o tráfego de dados, permitindo ou bloqueando o acesso com base em regras predefinidas. O que um *firewall* de inspeção de estado (*stateful firewall*) faz para aumentar a segurança?**

A) Bloqueia todas as conexões de entrada e saída da rede.
B) Filtra o tráfego com base apenas nos endereços IP de origem.
C) Analisa o conteúdo dos pacotes de dados em busca de ameaças conhecidas.
D) Mantém um registro do estado das conexões de rede e permite apenas o tráfego autorizado.

Questão 52

Em um sistema criptográfico simétrico, a principal preocupação em termos de segurança refere-se à segurança

A) na autenticação dos usuários.
B) durante a transmissão das chaves.
C) na geração de chaves públicas e privadas.
D) na proteção da única chave compartilhada.

Questão 53

Sobre a distinção fundamental entre os sistemas criptográficos simétricos e assimétricos de chave pública, considerando as implicações para a segurança e a complexidade computacional, assinale a afirmativa correta.

A) Sistemas simétricos e assimétricos são conceitos equivalentes, referindo-se ao mesmo princípio subjacente na criptografia.
B) Sistemas simétricos usam uma única chave para criptografia e descriptografia, enquanto sistemas assimétricos utilizam chaves distintas.
C) Ambos os sistemas utilizam a mesma chave para criptografia, mas sistemas assimétricos requerem senhas adicionais para descriptografia.
D) Sistemas simétricos são intrinsecamente mais seguros devido ao uso de chaves públicas, enquanto sistemas assimétricos dependem de chaves privadas.

Questão 54

Trata-se de uma medida fundamental para fortalecer a segurança na implementação dos dispositivos de *tokens* e *smartcards* utilizados em sistemas criptográficos para autenticação e proteção de informações sensíveis, considerando a complexidade das ameaças digitais contemporâneas:

A) Compartilhamento público das chaves privadas.
B) Implementação de autenticação de dois fatores.
C) Utilização de algoritmos de criptografia desatualizados.
D) Armazenamento das chaves criptográficas em servidores externos.

Questão 55

Sobre as características distintivas entre os algoritmos de criptografia RSA, DES e AES, marque V para as afirmativas verdadeiras e F para as falsas.

( ) RSA é um algoritmo de chave simétrica; DES e AES são algoritmos de chave assimétrica.
( ) DES utiliza um tamanho de chave fixo de 128 *bits*; tanto RSA quanto AES permitem ajustar dinamicamente o comprimento das chaves.
( ) RSA é amplamente utilizado para criptografia de dados em trânsito; DES e AES são mais adequados para armazenamento seguro de informações.
( ) AES é uma evolução do DES, mantendo as mesmas características de segurança, mas com maior eficiência.

A sequência está correta em

A) F, V, V, F
B) V, F, V, V.
C) F, V, F, F.
D) V, F, F, V

Questão 56

Considerando os desafios complexos relacionados à segurança em Banco de Dados e Desenvolvimento Seguro de *Software*, qual das seguintes estratégias representa uma abordagem avançada para mitigar riscos de segurança e proteger efetivamente dados sensíveis?

A) Uso de ferramentas de monitoramento de integridade e auditoria contínua.
B) Utilização de senhas complexas e atualização regular de chaves criptográficas.
C) Implementação de *firewalls* de aplicação e monitoramento de tráfego de rede.
D) Adoção de técnicas de ofuscação de código e estabelecimento de controle de acesso granular.

Questão 57

Diante das práticas avançadas empregadas em testes de invasão em aplicativos *WEB*, qual das seguintes opções representa uma estratégia avançada para contornar sistemas de detecção de intrusões durante um ataque?

A) Utilização de *payloads* genéricos para evitar detecção por meio de assinaturas.
B) Foco exclusivo em vulnerabilidades amplamente documentadas, negligenciando possíveis ameaças emergentes.
C) Implementação de ataques de força bruta para explorar possíveis vulnerabilidades nas camadas de autenticação.
D) Emprego de técnicas de evasão avançadas, como manipulação de *tokens* de sessão, com o intuito de evitar a detecção eficiente.

Questão 58

Considere o impacto significativo que a *Open Web Application Security Project* (OWASP) teve no campo da segurança de aplicações *WEB*. Dentre as seguintes alternativas, qual melhor descreve o papel central da Metodologia OWASP no cenário da segurança de aplicações *WEB*?

A) Desenvolver aplicações *web* que são resistentes a ameaças cibernéticas.
B) Promover e propagar as melhores práticas de segurança para aplicações *WEB*.
C) Oferecer serviços avançados de hospedagem, focados em ambientes altamente seguros.
D) Estabelecer diretrizes específicas para codificação em diversas linguagens de programação.

Questão 59

Considerando a complexidade da segurança em aplicações *WEB*, qual das afirmativas a seguir oferece a justificativa mais precisa para a vitalidade da gestão de *patches* e atualizações no contexto da segurança de aplicações *WEB*?

A) Orquestração eficiente da infraestrutura para otimizar a resiliência operacional e a capacidade de resposta.
B) Implementação proativa de contramedidas contra ameaças persistentes avançadas, como ataques DDoS distribuídos.
C) Sincronização meticulosa de sistemas com arquiteturas legadas para preservar a interoperabilidade e minimizar descontinuidades.
D) Correção diligente de vulnerabilidades previamente identificadas, promovendo uma postura defensiva e aprimoramento constante da segurança em conformidade com as melhores práticas.

Questão 60

Diante da crescente sofisticação dos ataques cibernéticos, especialmente no contexto de ataques de dicionário e força bruta em aplicações *WEB*, assinale a alternativa que melhor exemplifica uma estratégia avançada para enfrentar com eficácia ataques de dicionário e força bruta em aplicações *WEB:*

A) Adoção de senhas complexas e alteração frequente de políticas.
B) Utilização de autenticação multifatorial com fatores biométricos.
C) Utilização de *honeypots* para atrair e detectar potenciais invasores.
D) Implementação de bloqueio de IP após um número fixo de tentativas de *login*.

ATENÇÃO

NÃO É PERMITIDA a anotação das respostas da prova em NENHUM MEIO.
O candidato flagrado nesta conduta poderá ser ELIMINADO do processo.

PROVA DISCURSIVA

ORIENTAÇÕES GERAIS

- A Prova Discursiva terá caráter eliminatório e classificatório; é constituída de 2 (duas) dissertações sobre temas específicos da área respectiva do cargo. Será avaliada em 100 (cem) pontos, sendo 50 (cinquenta) pontos para cada dissertação.
- A resposta deverá ser manuscrita em letra legível, com caneta esferográfica de corpo transparente e de tinta azul ou preta, não sendo permitida a interferência e/ou a participação de outras pessoas. A Prova Discursiva terá extensão mínima de 20 (vinte) linhas e máxima de 30 (trinta) linhas para cada resposta. Será atribuída nota 0 (zero) ao texto que contiver número de linhas inferior aos limites mínimos estabelecidos.
- O candidato receberá nota zero na Prova Discursiva em casos de não atendimento ao conteúdo avaliado, de não haver texto, de manuscrever em letra ilegível ou de grafar por outro meio que não o determinado em edital, bem como no caso de identificação em local indevido, sendo vedado qualquer tipo de rasura e/ou adulteração na identificação das páginas, sob pena de eliminação.
- Serão considerados os seguintes elementos de avaliação para cada questão discursiva:

CRITÉRIOS	PONTUAÇÃO
(A) ASPECTOS MACROESTRUTURAIS	**38 pontos**
ABORDAGEM DO TEMA E DESENVOLVIMENTO DO CONTEÚDO	
Neste critério serão avaliados: Pertinência de exposição relativa ao problema, à ordem de desenvolvimento proposto e ao padrão de resposta, conforme detalhamento a ser oportunamente publicado.	
(B) ASPECTOS MICROESTRUTURAIS	**12 pontos**
Indicação de um erro para cada ocorrência dos tipos a seguir:	
1. Conectores (sequência do texto). 2. Correlação entre tempos verbais. 3. Precisão vocabular. 4. Pontuação. 5. Concordância nominal e verbal. 6. Regência nominal e verbal. 7. Colocação pronominal. 8. Vocabulário adequado ao texto escrito. 9. Ortografia. 10. Acentuação.	
OBSERVAÇÕES QUANTO AOS CRITÉRIOS DE CORREÇÃO:	
1. A cada erro textual referente aos aspectos microestruturais ocorrerá o decréscimo de 0,4 ponto, até o limite de 12 pontos. 2. Por linha efetivamente escrita, entende-se a linha com no mínimo duas palavras completas, excetuando-se preposições, conjunções e artigos. 3. O padrão de resposta será divulgado com o resultado preliminar da Prova Discursiva.	

Questão 01

Segundo o autor *Willian Stallings*, "o protocolo SSL/TLS desempenha um papel fundamental na garantia da confidencialidade e integridade dos dados transmitidos pela *internet*".

(STALLINGS, William. Criptografia e Segurança de Redes: Princípios e Práticas. 6ª ed. São Paulo: Pearson, 2015.)

Descreva como o protocolo SSL/TLS garante uma comunicação segura entre um cliente e um servidor *web*, elucidando os principais conceitos envolvidos; disserte sobre a negociação de parâmetros de segurança, o estabelecimento de sessões seguras e a troca de chaves criptográficas, destacando a importância de cada etapa na proteção da integridade e confidencialidade dos dados transmitidos.

01	
02	
03	
04	
05	
06	
07	
08	
09	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	
22	
23	
24	
25	
26	
27	
28	
29	
30	

Questão 02

Considere o cenário em que certo Analista de Tecnologia da Informação foi contratado para avaliar a segurança de um aplicativo *web* crítico para uma instituição financeira. Nesse contexto, explique os principais conceitos relacionados à segurança de aplicativos *web* e destaque as vulnerabilidades mais comuns encontradas nesse tipo de sistema. Discorra sobre a importância da análise de vulnerabilidades em aplicações *web* e apresente algumas ferramentas e técnicas utilizadas para explorar essas vulnerabilidades. Por fim, discuta sobre a importância dos testes de invasão em aplicativos *web* e como eles podem contribuir para melhorar a segurança desses sistemas.

01	
02	
03	
04	
05	
06	
07	
08	
09	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	
22	
23	
24	
25	
26	
27	
28	
29	
30	


INSTITUTO
CONSULPLAN


INSTITUTO
CONSULPLAN

INSTRUÇÕES

1. Somente será permitida a utilização de caneta esferográfica de tinta azul ou preta, feita de material transparente e de ponta grossa.

2. É proibida, durante a realização das provas, a comunicação entre os candidatos e a utilização de máquinas calculadoras e/ou similares, livros, anotações, impressos ou qualquer outro material de consulta, protetor auricular, lápis, borracha ou corretivo. Especificamente, não será permitido ao candidato ingressar na sala de provas sem o devido recolhimento, com respectiva identificação, dos seguintes equipamentos: *bip*, telefone celular, *walkman*, agenda eletrônica, *notebook*, *palmtop*, *ipod*, *ipad*, *tablet*, *smartphone*, mp3, mp4, receptor, gravador, máquina de calcular, máquina fotográfica, controle de alarme de veículo, relógio de qualquer modelo, pulseiras magnéticas e similares etc., o que não acarreta em qualquer responsabilidade do Instituto Consulplan sobre tais equipamentos.

3. Com vistas à garantia da segurança e da integridade do certame, no dia da realização das provas escritas, os candidatos serão submetidos ao sistema de detecção de metais na entrada e na saída dos sanitários. Excepcionalmente, poderão ser realizados, a qualquer tempo durante a realização das provas, outros procedimentos de vistoria além do descrito.

4. O caderno de provas consta de 60 (sessenta) questões de múltipla escolha para todos os cargos; 2 (duas) questões discursivas para os cargos superiores, exceto, para os cargos de procurador e redator; 1 (uma) peça prático-profissional privativa de advogado (petição ou parecer) para o cargo de procurador; 1 (uma) proposição normativa, com justificativa para o cargo de redator; e, ainda, 1 (uma) redação para o cargo de Técnico Legislativo II.

5. Ao receber o material de realização das provas, o candidato deverá conferir atentamente se o caderno de provas contém o número de questões previsto, se corresponde ao cargo a que está concorrendo, bem como se os dados constantes no Cartão de Respostas (Gabarito) e na Folha de Textos Definitivos (Prova Discursiva) estão corretos. Caso os dados estejam incorretos, ou o material esteja incompleto ou, ainda, detenha qualquer imperfeição, o candidato deverá informar tal ocorrência ao Fiscal de Aplicação, não cabendo reclamações posteriores neste sentido.

6. A prova terá duração de 5 (cinco) horas para todos os cargos. Esse período abrange a assinatura, assim como a transcrição das respostas para o Cartão de Respostas (Gabarito) e a Folha de Textos Definitivos (Prova Discursiva).

7. As questões das provas objetivas são do tipo múltipla escolha, com 4 (quatro) opções (A a D) e uma única resposta correta. Ao terminar a prova, o candidato, obrigatoriamente, deverá devolver ao Fiscal de Aplicação o Cartão de Respostas (Gabarito) e a Folha de Textos Definitivos (Prova Discursiva) devidamente assinados em local indicado.

8. Os Fiscais de Aplicação não estão autorizados a emitir opinião nem prestar esclarecimentos sobre o conteúdo das provas. Cabe única e exclusivamente ao candidato interpretar e decidir.

9. Não é permitida a anotação de informações relativas às suas respostas (cópia de gabarito) no comprovante de inscrição ou em nenhum outro meio.

10. O candidato somente poderá se retirar do local de realização das provas escritas levando o caderno de provas no decurso dos últimos 60 (sessenta) minutos anteriores ao horário previsto para o seu término. O candidato poderá se retirar do local de realização das provas somente a partir dos 90 (noventa) minutos após o início de sua realização; contudo, não poderá levar o seu caderno de provas.

11. Os 3 (três) últimos candidatos de cada sala só poderão sair juntos. Caso algum candidato insista em sair do local de aplicação antes de autorizado pelo Fiscal de Aplicação, será lavrado Termo de Ocorrência, assinado pelo candidato e testemunhado pelos 2 (dois) outros candidatos, pelo Fiscal de Aplicação da sala e pelo Coordenador da Unidade de Provas, para posterior análise pela Comissão de Acompanhamento do Concurso.

RESULTADOS E RECURSOS

- Os gabaritos oficiais preliminares das provas objetivas serão divulgados na *Internet*, no endereço eletrônico www.institutoconsulplan.org.br, a partir das 16h00min da segunda-feira subsequente à realização das provas escritas objetivas de múltipla escolha.

- O candidato que desejar interpor recursos contra os gabaritos oficiais preliminares das provas objetivas disporá de 3 (três) dias úteis, a partir do dia subsequente ao da divulgação (terça-feira), em requerimento próprio disponibilizado no *link* correlato ao Concurso Público no endereço eletrônico www.institutoconsulplan.org.br.

- A interposição de recursos poderá ser feita via *Internet*, através do Sistema Eletrônico de Interposição de Recursos, com acesso pelo candidato ao fornecer dados referentes à sua inscrição apenas no prazo recursal, ao Instituto Consulplan, conforme disposições contidas no endereço eletrônico www.institutoconsulplan.org.br, no *link* correspondente ao Concurso Público. Será disponibilizado, ainda, um ponto de acesso à *Internet* para o candidato no endereço indicado no item 1.12 do Edital.