UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE

CONCURSO PÚBLICO

Edital nº 016/2019

Analista de Tecnologia da Informação

Leia estas instruções:

1	Confira se os dados contidos na parte inferior desta capa estão corretos e, em seguida, assine no espaço reservado.
2	Este Caderno contém, respectivamente, **uma** prova discursiva (Estudo de caso) e **50 questões** de múltipla escolha, assim distribuídas: **01 a 10** › Língua Portuguesa; **11 a 20** › Legislação; **21 a 50** › Conhecimentos Específicos.
3	Quando o Fiscal autorizar, verifique se o Caderno está completo e sem imperfeições gráficas que impeçam a leitura. Detectado algum problema, comunique-o, imediatamente, ao Fiscal.
4	A prova discursiva (Estudo de caso) será avaliada considerando-se apenas o que estiver escrito no Espaço destinado na Folha de Respostas da Prova Discursiva.
5	Escreva de modo legível, pois dúvida gerada por grafia ou rasura implicará redução de pontos.
6	Cada questão de múltipla escolha apresenta quatro opções de resposta, das quais apenas uma é correta.
7	Interpretar as questões faz parte da avaliação; portanto, não peça esclarecimentos aos fiscais.
8	A Comperve recomenda o uso de caneta esferográfica de tinta preta, fabricada em material transparente.
9	Utilize qualquer espaço em branco deste Caderno para rascunhos e não destaque nenhuma folha.
10	Os rascunhos e as marcações que você fizer neste Caderno não serão considerados para efeito de avaliação.
11	Você dispõe de, no máximo, quatro horas e 30 minutos para responder ao Estudo de Caso na Folha de Resposta da Prova Discursiva, responder às questões de múltipla escolha e preencher a Folha de Respostas das Provas Objetivas.
12	O preenchimento da Folha de Respostas das Provas Objetivas e da Folha de Resposta da Prova Discursiva é de sua inteira responsabilidade.
13	Ao retirar-se definitivamente da sala, entregue ao Fiscal este Caderno, a Folha de Resposta das Provas Objetivas e a Folha de Resposta da Prova Discursiva.

Assinatura do Candidato: _____

É sábio quem tem em si tudo que leva à felicidade.

(Sócrates)

COMPERVE UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE

Prova Discursiva (Estudo de Caso) — 01 questão

Uma tendência mundial nas empresas é o BYOD (*bring your own device*), que permite aos funcionários levarem e utilizarem seus dispositivos pessoais (*smartphones*, *tablets* e *notebooks*) para tarefas no trabalho. Essa prática foi adotada por grandes empresas mundiais, mas ainda é incipiente no Brasil. Entre os adeptos e interessados no BYOD, é consenso que a sua adoção permite reduzir gastos com investimentos em TI, principalmente na aquisição de *hardware*. Já muito longe de consenso, estão as considerações sobre a segurança computacional. A discussão principal está na possibilidade de que esses dispositivos levem consigo vulnerabilidades que possam ser exploradas para ataques cibernéticos. Caso isso aconteça, deve-se proceder com a perícia do dispositivo, garantindo-se a cadeia de custódia.

Considerando essas informações,

A) explique a função e importância da cadeia de custódia na perícia de dispositivos informáticos.

B) descreva a sequência de passos a serem seguidos para a perícia de dispositivos informáticos, desde a obtenção destes até o resultado final do trabalho pericial.

INSTRUÇÕES

- Sua resposta deverá atender às seguintes normas:
  - ser redigida no espaço destinado à versão definitiva na Folha de Resposta da Prova Discursiva;
  - ser redigida na modalidade escrita padrão da língua portuguesa.
  - não ser assinada (nem mesmo com pseudônimo).

ATENÇÃO

- Será atribuída **NOTA ZERO** em qualquer um dos seguintes casos:
  - estiver em branco;
  - for redigida fora do espaço destinado ao texto definitivo na Folha de Resposta;
  - for redigida de forma ilegível;
  - for redigida com lápis grafite ou lapiseira;
  - for redigida em versos;
  - fugir ao tema ou à proposta da redação ou estudo de caso;
  - contiver identificação do candidato fora do espaço reservado para esse fim.
  - letra ilegível;
  - identificação do candidato (nome, assinatura ou pseudônimo);

ESPAÇO PARA RASCUNHO

(NÃO ASSINE)

Língua Portuguesa 01 a 10

As questões de 1 a 10 desta prova são baseadas no texto abaixo.

Um silêncio que MATA

Cláudia Maria França Pádua

A agressividade é a arma que o indivíduo utiliza para manifestar seu ódio. Existem vários tipos de violência, e os estudos desse tipo de comportamento são constantes com o intuito de descobrir as causas que levam o ser humano a cometer tal infração e que causam indignação aos olhos atentos da sociedade.

Inúmeras pesquisas mostram, há anos, a vergonhosa prevalência da violência contra as mulheres. Em 2013, 13 mulheres morreram, todos os dias, vítimas de feminicídio, isto é, assassinato em função de seu gênero. Cerca de 30% foram mortas pelo parceiro ou ex-companheiro (Mapa da Violência 2015). Outra pesquisa do Instituto Locomotiva, dessa vez de 2016, aferiu que 2% dos homens admitem espontaneamente ter cometido violência sexual contra uma mulher, mas, diante de uma lista de situações, 18% reconhecem terem sido violentos. Quase um quinto dos 100 milhões de homens brasileiros. E, curiosamente, um estudo recente revelou que 90% concorda que quem presencia ou toma conhecimento de um estupro e fica calado também é culpado. Um percentual relevante, mas por que ainda há tanto silêncio?

Cinco tipos de violência enquadram todos esses estudos: *1 - violência psicológica:* causa danos à autoestima da vítima, podendo ocorrer em casa, na escola, no trabalho, proporcionando humilhação, desvalorização, ofensa, chantagem, manipulação, constrangimento e outros; 2- *violência física:* causa danos ao corpo da vítima, podendo ocorrer sob a forma de socos, pontapés, chutes, amarrações e mordidas, impossibilitando defesa; 3 - *violência moral:* qualquer conduta que proporcione calúnia, difamação ou injúria; *4 - violência sexual:* esta não se limita somente ao estupro propriamente dito, mas a atos de violência proibitivos, como, por exemplo, não uso de contraceptivos, obrigação de práticas sexuais, "encoxada" nos transportes públicos, exploração do corpo de adolescentes e pedofilia; 5 - *violência simbólica:* utilização feminina como "objeto de desejo" (propagandas, *outdoors* etc.), traçando uma imagem negativa da mulher. O alerta que ecoa é que a violência é silenciosa. Ela ocorre nas residências, nos espaços públicos e em qualquer lugar onde a mulher é assediada.

O assédio é um comportamento criminoso e deve ser severamente tratado como tal. Seu desenvolvimento relaciona-se com a carência emocional ou com a separação, na infância, do elo materno. A partir desse momento, criam-se, no indivíduo, condutas antissociais, um desajuste afetivo, que podem levá-lo ao cometimento de crimes para sentir prazer no sofrimento dos outros e gerar uma excitação cortical, causando-lhe grande satisfação da libido e de seu ego malformado por uma personalidade psicopática e doentia, na qual os impulsos do mal ganham lugar e ímpeto para cometer tais absurdos. Nesse exato momento, instaura-se o grau de periculosidade do agressor. Portanto, muitas vezes, senão na maioria delas, o agressor sabe que está cometendo um delito e sente, inclusive, prazer nesse comportamento.

É necessário que as autoridades realizem emergencialmente políticas que inviabilizem esse avanço, para que esse crime não faça parte das principais estatísticas, em que 22 milhões das brasileiras com 16 anos ou mais relatam ter sofrido algum tipo de assédio em 2018. Vítimas com ensino médio e superior relatam, em seus depoimentos, terem sofrido algum tipo de assédio em maior número do que aquelas com ensino fundamental. O caso mais comum citado pela maioria das mulheres entrevistadas é o de comentários desrespeitosos na rua.

Sabemos que, desde a Idade Média, a violência psicológica e moral contra as mulheres era muito comum, e a violência física se valia até mesmo dos mais diferentes instrumentos de tortura utilizados nas mulheres de forma cruel e sem condenação aos torturadores. O "estripador de seios", por exemplo, costumava ser utilizado para punir mulheres acusadas de realizar bruxaria, aborto ou adultério. As garras aquecidas por brasas eram usadas para arrancar-lhes os seios. E existiram tantos outros instrumentos cruéis que marcaram a história mundial e registraram como a mulher foi e ainda é tratada.

No Brasil, a tortura se divide em duas fases: a primeira se estende do Brasil Império até a nossa Constituição Federal de 1988. A produção de prova se fazia, até aquela época, de forma brutal, e a escravatura, legalizada, tornava o ambiente adequado à violação da dignidade humana. O Código Criminal de 1830 previu o aumento da dor física, como agravante, e o termo

"tortura", que aparece na Lei Penal Brasileira em 1940, quando é arrolada entre os meios cruéis que agravam o delito.

A segunda fase se inicia com a Constituição de 1988, sob o desrespeito sistemático às liberdades fundamentais do homem, ocorrido nas décadas anteriores. Tipificada finalmente a tortura como crime em nossa legislação, espera-se que as formas mais silenciosas, como as violências psicológica, moral e simbólica, recebam um olhar atento para sua erradicação. Infelizmente, nosso país ainda caminha a passos lentos na recrudescência de leis mais efetivas, em que o respeito deveria permanecer como palavra-chave.

As mulheres têm, sim, exercido sua voz, mas mergulham, por vezes, em um conformismo de cultura social que não deverá mais ser aceito e precisa urgentemente ser resolvido com políticas públicas adequadas e conscientização. Afinal, não se pode ficar inerte diante da violência que assola o país e gera incredulidade. Sabemos que as palavras têm a força da razão, enquanto a crueldade emana do poder do ódio e da anomia.

PÁDUA, Cláudia Maria França. Um silencia que mata. **Psique, ciência e vida**. São Paulo: Editora Escala, Ed. 158, abr. 2019. p. 18-19. [Adaptado].

01. Prioritariamente, o texto objetiva

A) defender a criação de políticas públicas para combater o avanço da violência contra a mulher.

B) apresentar os cinco principais tipos de violência enfrentados pelas mulheres na atualidade.

C) descrever os mecanismos empregados para a prática da violência contra a mulher na história.

D) historicizar as fases da tortura contra as mulheres no Brasil, desde o Império até a atualidade.

02. A linguagem empregada no título tende à

A) conotação, o que prejudica o entendimento do texto.

B) conotação, o que contribui para despertar a curiosidade do leitor.

C) denotação, o que contribui para despertar a curiosidade do leitor.

D) denotação, o que prejudica o entendimento do texto.

03. Com base na leitura do texto, depreende-se que

A) o disciplinamento explícito da tortura na legislação brasileira promoveu um recrudescimento da violência no país.

B) a violência contra as mulheres circunscreve-se aos âmbitos psicológico, físico, moral, sexual e simbólico.

C) o comportamento antissocial decorrente de episódios de violência torna indivíduos criminosos em potencial.

D) a inércia da sociedade contribui para a manutenção do atual quadro de violência em razão do gênero.

04. No segundo parágrafo do texto, entrecruzam-se

A) cinco vozes, todas elas sob a forma direta.

B) cinco vozes, sendo as alheias sob a forma indireta.

C) quatro vozes, sendo as alheias sob a forma indireta.

D) quatro vozes, todas elas sob a forma direta.

05. No terceiro parágrafo do texto, predomina a sequência

A) argumentativa.

B) descritiva.

C) explicativa.

D) narrativa.

Para responder às questões 06, 07 e 08, considere o parágrafo transcrito abaixo.

> O assédio é um comportamento criminoso e deve ser severamente tratado como tal. Seu desenvolvimento relaciona-se com a carência emocional ou com a separação, na infância, do elo materno. A partir desse momento, criam-se no indivíduo condutas antissociais, um desajuste afetivo, **que[1]** podem levá-lo ao cometimento de crimes, para sentir prazer no sofrimento dos outros, e gerar uma excitação cortical, causando-lhe grande satisfação da libido e de seu ego malformado por uma personalidade psicopática e doentia, na qual os impulsos do mal ganham lugar e ímpeto para cometer tais absurdos. Nesse exato momento, instaura-se o grau de periculosidade do agressor. Portanto, muitas vezes, senão na maioria delas, o agressor sabe que está cometendo um delito e sente, inclusive, prazer nesse comportamento.

06. No parágrafo, emprega-se, prioritariamente, uma estratégia baseada em

A) confronto de ideias, tendente a encaminhar o leitor para a refutação de uma opinião.

B) oposição de ideias, tendente a encaminhar o leitor para a refutação de uma opinião.

C) comparação, tendente a encaminhar o leitor para a adesão a uma ideia.

D) causa e efeito, tendente a encaminhar o leitor para a adesão a uma ideia.

07. A linguagem empregada no parágrafo revela um enunciador, predominantemente,

A) implicado com o tema, o que se evidencia pelo uso de adjetivos e advérbios.

B) distanciado do tema, o que se evidencia pelo uso da primeira pessoa nas construções frasais.

C) implicado com o tema, o que se evidencia pelo uso de verbos pouco valorados.

D) distanciado do tema, o que se evidencia pelo uso de substantivos pouco valorados.

08. No contexto em que surge, o elemento linguístico **[1]** é

A) um pronome e retoma “um desajuste afetivo”.

B) um pronome e retoma “condutas antissociais”.

C) uma conjunção e introduz uma oração substantiva.

D) uma conjunção e introduz uma oração adjetiva.

Para responder às questões 09 e 10, considere o excerto transcrito abaixo.

> As mulheres têm, sim, exercido sua voz, mas mergulham, por vezes, em um conformismo de cultura social que não **deverá[1]** mais ser aceito e **precisa[2]** urgentemente ser resolvido com políticas públicas adequadas e conscientização.

09. Sem alteração do sentido e com respeito à norma-padrão, o excerto está corretamente reescrito em:

A) As mulheres têm sim exercido sua voz, visto que mergulham, por vezes, em um conformismo de cultura social, que não deverá mais ser aceito e precisa urgentemente, ser resolvido com políticas públicas adequadas e conscientização.

B) As mulheres têm sim exercido sua voz, pois mergulham, por vezes, em um conformismo de cultura social, que não deverá mais ser aceito e precisa urgentemente ser resolvido com políticas públicas adequadas e conscientização.

C) As mulheres têm, sim, exercido sua voz; porém, mergulham por vezes em um conformismo de cultura social que não deverá mais ser aceito e precisa, urgentemente ser resolvido com políticas públicas adequadas e conscientização.

D) As mulheres têm, sim, exercido sua voz; no entanto, mergulham, por vezes, em um conformismo de cultura social que não deverá mais ser aceito e precisa, urgentemente, ser resolvido com políticas públicas adequadas e conscientização.

10. As formas verbais **[1]** e **[2]**

A) apresentam o mesmo sujeito: “cultura social”.

B) apresentam o mesmo sujeito: “que”.

C) apresentam sujeitos distintos: “que” e “cultura social”, respectivamente.

D) apresentam sujeitos distintos: “cultura social” e “que”, respectivamente.

Legislação 11 a 20

11. O Regime Jurídico dos Servidores Públicos Civis da União (Lei nº 8.112/90) estabelece expressamente as formas de provimento de cargo público. Dentre elas, estão:

A) nomeação, recondução e demissão.
B) recondução, readaptação e falecimento.
C) reintegração, reversão e nomeação.
D) reversão, aposentadoria e reintegração.

12. A Lei nº 8.112/90 prevê que as reposições e indenizações ao erário podem ser parceladas, a pedido do interessado. Nos expressos termos da sobredita lei, o valor de cada parcela não pode ser inferior ao correspondente a

A) vinte por cento da remuneração, provento ou pensão.
B) treze por cento da remuneração, provento ou pensão.
C) dez por cento da remuneração, provento ou pensão.
D) doze por cento da remuneração, provento ou pensão.

13. De acordo com as disposições do Regime Jurídico dos Servidores Públicos Civis da União (Lei nº 8.112/90), constituem indenizações ao servidor:

A) ajuda de custo, transporte, diárias e auxílio-moradia.
B) diárias, gratificações, auxílio-moradia e transporte.
C) transporte, ajuda de custo, auxílio-moradia e adicionais.
D) gratificações, adicionais, diárias e ajuda de custo.

14. À luz do que estabelece a Lei nº 8.112/90, "a gratificação natalina corresponde a 1/12 (um doze avos) da remuneração a que o servidor fizer jus no mês de dezembro, por mês de exercício no respectivo ano". Segundo as normas da referida lei, a gratificação natalina será paga até o dia

A) 25 do mês de dezembro de cada ano.
B) 22 do mês de dezembro de cada ano.
C) 20 do mês de dezembro de cada ano.
D) 30 do mês de dezembro de cada ano.

15. Considerando as normas previstas no Regime Jurídico dos Servidores Públicos Civis da União (Lei nº 8.112/90), analise as afirmativas abaixo.

I	Somente será permitido serviço extraordinário para atender a situações excepcionais e temporárias, respeitado o limite máximo de duas horas por jornada.
II	O serviço noturno, prestado em horário compreendido entre vinte e duas horas de um dia e cinco horas do dia seguinte, terá o valor-hora acrescido de vinte por cento, computando-se cada hora como cinquenta minutos e trinta segundos.
III	As férias poderão ser parceladas em até quatro etapas, desde que assim requeridas pelo servidor, e no interesse da administração pública.
IV	O servidor fará jus a trinta dias de férias, que podem ser acumuladas, até o máximo de dois períodos, no caso de necessidade do serviço, ressalvadas as hipóteses em que haja legislação específica.

Das afirmativas, estão corretas

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

16. Nos termos das disposições expressas na Lei nº 8.112/90, o "processo disciplinar é o instrumento destinado a apurar responsabilidade de servidor por infração praticada no exercício de suas atribuições, ou que tenha relação com as atribuições do cargo em que se encontre investido". No que concerne ao processo administrativo disciplinar submetido ao **rito sumário**, a citada lei estabelece que o prazo para a conclusão **NÃO** excederá

A) sessenta dias, contados da data da publicação do ato que constituir a comissão, admitida a sua prorrogação por até quinze dias, quando as circunstâncias o exigirem.

B) sessenta dias, contados da data da publicação do ato que constituir a comissão, admitida a sua prorrogação por até trinta dias, quando as circunstâncias o exigirem.

C) trinta dias, contados da data da publicação do ato que constituir a comissão, admitida a sua prorrogação por até trinta dias, quando as circunstâncias o exigirem.

D) trinta dias, contados da data da publicação do ato que constituir a comissão, admitida a sua prorrogação por até quinze dias, quando as circunstâncias o exigirem.

17. O Regime Jurídico dos Servidores Públicos Civis da União (Lei nº 8.112/90) prevê a possibilidade de afastamento preventivo do cargo no decorrer do processo disciplinar, como medida cautelar e a fim de que o servidor não venha a influir na apuração da irregularidade. À luz do que estabelece a sobredita lei, o servidor poderá ser afastado do exercício do cargo pelo prazo de até sessenta dias,

A) com prejuízo da remuneração e com possibilidade de prorrogação por igual prazo.

B) com prejuízo da remuneração e sem possibilidade de prorrogação por igual prazo.

C) sem prejuízo da remuneração e sem possibilidade de prorrogação por igual prazo.

D) sem prejuízo da remuneração e com possibilidade de prorrogação por igual prazo.

18. Considerando as normas da Lei nº 9.784, de 29 de janeiro de 1999, a qual regula o processo administrativo no âmbito da Administração Pública Federal, analise as afirmativas abaixo.

I	Entidade é a unidade de atuação integrante da estrutura da Administração direta e da estrutura da Administração indireta.
II	O administrado tem o direito de ter ciência da tramitação dos processos administrativos em que tenha a condição de interessado, sendo vedada a obtenção de cópias de documentos neles contidos.
III	Um dos critérios observados nos processos administrativos é o da atuação segundo padrões éticos de probidade, decoro e boa-fé.
IV	Finalidade, interesse público, eficiência e segurança jurídica são alguns dos princípios a serem obedecidos pela Administração Pública nos processos administrativos.

Das afirmativas, estão corretas

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

19. A lei que regula o processo administrativo no âmbito da Administração Pública Federal (Lei nº 9.784/99) estabelece os deveres do administrado perante a Administração, sem prejuízo de outros previstos em ato normativo. Nos termos das normas expressas na referida lei, o administrado deve

A) prestar informações que lhe forem solicitadas e colaborar para os esclarecimentos dos fatos.

B) fazer-se assistir por advogado, salvo quando a lei facultar tal dever.

C) formular alegações e apresentar documentos antes da decisão bem como ter vista dos autos.

D) proceder com lealdade, sendo prescindíveis a urbanidade e a boa-fé.

20. Tendo como base as disposições expressas na Lei nº 9.784, de 29 de janeiro de 1999, a qual regula o processo administrativo no âmbito da Administração Pública Federal, analise as afirmativas abaixo.

I	Concluída a instrução de processo administrativo, a Administração tem o prazo de até trinta dias para decidir, salvo prorrogação por igual período expressamente motivada.
II	Salvo disposição legal específica, é de cinco dias o prazo para interposição de recurso administrativo, contado a partir da ciência ou divulgação oficial da decisão recorrida.
III	Os resultados da consulta e audiência pública e de outros meios de participação de administrados deverão ser apresentados com a indicação do procedimento adotado.
IV	O recurso será dirigido à autoridade que proferiu a decisão, a qual, se não a reconsiderar no prazo de dez dias, o encaminhará à autoridade superior.

Das afirmativas, estão corretas

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

Conhecimentos Específicos 21 a 50

21. A empresa denominada Security10 acaba de implementar um conjunto de mecanismos para garantir que ações de uma entidade válida sejam atribuídas exclusivamente a ela, impedindo, por exemplo, que emissor ou receptor neguem uma mensagem transmitida. Diante disso, o objetivo de segurança que a Security10 quer alcançar com esses mecanismos é a

A) integridade.
B) confidencialidade.
C) irretratabilidade.
D) privacidade.

22. A organização tida como referência para o estabelecimento de boas práticas na área da segurança computacional, sendo inclusive mantenedora de um *framework* para cibersegurança que inclui padrões, diretrizes e melhores práticas para gerenciar o risco relacionado a esse tema é a

A) ITU-T (*Telecommunication Standardization Sector*).
B) ISO (*International Organization for Standardization*).
C) TCP/IP (*Transmission Control Protocol/Internet Protocol*).
D) NIST (*National Institute of Standards and Technology*).

23. Em segurança computacional, o termo AAA (a sigla derivada do inglês), ou triplo A, é recorrente na literatura e na prática. Esse termo faz referência direta a três serviços básicos. O primeiro "A" diz respeito ao serviço que verifica a identidade digital do usuário de um sistema; o segundo "A" faz referência ao serviço que garante que um usuário, que passou na verificação de sua identidade digital, somente tenha acesso aos recursos liberados a ele; e, por fim, o terceiro "A" refere-se ao serviço de coleta de informações sobre o uso dos recursos de um sistema pelos seus diferentes usuários. Em relação ao exposto, o termo AAA faz referência à

A) Armazenagem, Autorização e Contabilização.
B) Autenticação, Autorização e Contabilização.
C) Autenticação, Autorização e Armazenagem.
D) Autorização, Armazenagem e Privacidade.

24. Em criptografia, a Cifra de César é considerada como uma das mais simples e conhecidas técnicas de cifragem. Relatos históricos apontam que Júlio César utilizava essa cifra nas mensagens enviadas a seus generais, no qual cada letra da mensagem original era trocada pela letra situada três posições à sua frente no alfabeto. A Cifra de César é classificada como uma cifra de

A) transposição e monoalfabética.
B) substituição e polialfabética.
C) substituição e monoalfabética.
D) transposição e polialfabética.

25. Atualmente, sistemas criptográficos assimétricos são largamente utilizados por geralmente serem mais robustos e, portanto, seguros, além de serem considerados um excelente método para garantir segurança num canal público e inseguro, como a Internet. Em comparação com a criptografia simétrica, a criptografia assimétrica tende a ser mais lenta e necessita de um maior poder computacional por parte das máquinas. Em relação ao uso de chaves criptográficas, um sistema criptográfico assimétrico é caracterizado pelo uso de

A) UMA chave de sessão que deve ser utilizada para encriptar a mensagem na origem e decriptar no destino.
B) DUAS chaves relacionadas, sendo uma pública usada para encriptar a mensagem na origem e outra secreta para decriptar a mensagem no destino.
C) DUAS chaves secretas, sendo uma usada para encriptar a mensagem na origem e outra para decriptar a mensagem no destino.
D) TRÊS chaves secretas. Um exemplo deste tipo de sistema é o DES Triplo (do inglês, *Triple-DES*).

26. A fim de testar o uso de funções de *hash*, João, funcionário recém contratado da empresa Security10, aplicou uma função *hash h(x)* sobre uma mensagem *M* e obteve como resultado o valor *F23AB5* em hexadecimal. Curioso sobre o funcionamento da função *hash*, João aplicou novamente a mesma função *hash* sobre a mensagem original. Assim, João obteve o valor de

A) C11004. **B)** F23AB6. **C)** F23AB5. **D)** B333FF.

27. Uma função *hash* é um algoritmo que mapeia dados de comprimento variável para dados de comprimento fixo. O valor retornado por uma função *hash* é chamado código *hash*, ou simplesmente *hash*. Essas funções são consideradas unidirecionais, garantindo que a partir do código *hash* seja impossível voltar aos dados que foram usados para gerá-lo.

As funções *hash* conhecidas e ainda utilizadas são

A) MD5, AES e RSA.

B) MD5, SHA-1 e SHA-512.

C) AES, RSA e SHA-512.

D) MD5, DES e SHA-1.

28. Um protocolo de autenticação de mensagem geralmente faz uso de algum mecanismo capaz de produzir um autenticador, ou seja, um valor que possa ser verificável e certifique que a mensagem é autêntica. Diferentes mecanismos podem ser usados para gerar um autenticador. Entre esses, os mais utilizados são *hash* e MAC (*Message Authentication Code*). Outro método que também pode ser utilizado para autenticar mensagens é a

A) encriptação simétrica utilizando a chave pública.

B) encriptação assimétrica com assinatura, utilizando a chave pública.

C) encriptação assimétrica utilizando a chave de sessão.

D) encriptação assimétrica com assinatura, utilizando a chave privada.

29. Em segurança de redes, é possível a utilização de diferentes métodos para a imposição de acesso à rede, permitindo liberar o acesso apenas aos elementos devidamente autorizados. Nessa perspectiva, muitos fornecedores de equipamentos de rede oferecem suporte a múltiplos métodos, permitindo combiná-los de acordo com a necessidade. Firewall e Redes locais virtuais (VLANs) são exemplos desses métodos. Nesse sentido, outro método bastante comum, utilizado inclusive em redes sem fios, é o

A) IEEE 802.11ac.

B) IDS (*Intrusion Detection System*).

C) IPS (*Intrusion Prevention System*).

D) IEEE 802.1X .

30. Atualmente, é muito comum a utilização de uma conta de usuário já criada em grandes provedores (como Facebook, Google e outros) para efetuar a autenticação em sistemas de terceiros. Para isso, as entidades envolvidas formam uma estrutura de confiança mútua. O conceito central utilizado é o de autenticação única ou SSO (do inglês, *Single Sign-On*). Com isso, o usuário não precisa realizar o cadastro em diferentes sites ou lembrar de múltiplas senhas. De acordo com a terminologia da área de segurança de redes, essa é uma autenticação do tipo

A) mútua. **B)** federada. **C)** externa. **D)** facilitada.

31. A Segurança Computacional possui uma terminologia própria. Uma padronização na utilização dessa terminologia garante o correto entendimento entre os diferentes agentes envolvidos. Em relação a isso, considere as seguintes afirmações sobre a Segurança Computacional.

I	A segurança física visa providenciar mecanismos para restringir o acesso às áreas críticas da organização a fim de garantir a integridade e autenticidade dos dados.
II	Uma ameaça pode ser definida como algum evento que pode ocorrer e acarretar algum perigo a algum ativo da rede. As ameaças podem ser intencionais ou não-intencionais.
III	São ameaças mais comuns às redes de computadores: o acesso não-autorizado, o reconhecimento (ex: PortScan) e a negação de serviço (ex: DoS ou DDoS).
IV	O “Tripé da Segurança” é formado de Pessoas, Processos e Políticas de Segurança. De nada adianta uma Política de Segurança se Pessoas e Processos não forem considerados.

Em relação à Segurança Computacional, estão corretas as afirmativas

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

32. O *iptables* é conhecido como o aplicativo de firewall Linux padrão. Na verdade, o *iptables* é apenas uma ferramenta que controla o módulo *netfilter* do Linux, permitindo a filtragem de pacotes. A operação do *iptables* é baseada em regras que são expressas em um conjunto de comandos. No departamento de TI da Security10, João terá que revisar o conjunto de regas do script atual de firewall *iptables* utilizado na empresa. Analisando as 2.954 linhas do arquivo de script, João se deparou com a seguinte REGRA-Y, definida a partir da sequência de comandos abaixo.

```
echo "0" > /proc/sys/net/ipv4/tcp_syncookies
$IPTABLES -N REGRA-Y
$IPTABLES -A INPUT -i $WAN -p tcp --syn -j REGRA-Y
$IPTABLES -A REGRA-Y -m limit --limit 1/s --limit-burst 4 -j RETURN
$IPTABLES -A REGRA-Y -j DROP
```

A REGRA-Y definida permite impedir o ataque de

A) SYN flood.

B) Ping da morte (do inglês, *ping of death*).

C) SYS flood

D) portscan

33. Considere que o departamento de TI da empresa Security10 está analisando a possibilidade de utilizar o IPSec para aumentar a segurança da rede. No entanto, sua equipe ainda tem algumas dúvidas sobre o funcionamento do IPSec, no que diz respeito aos dois tipos de serviços oferecidos. Eles leram que um dos serviços protege e verifica a integridade dos dados, permitindo certificar que o dado não foi alterado durante o seu transporte. Neste tipo de serviço, o campo protocolo IP do datagrama é definido com o valor 50. Já o outro serviço encripta os dados e garante a confidencialidade destes durante o seu transporte, tendo o campo protocolo IP do datagrama definido com o valor 51.

Os tipos de serviço do IPSec retratados na circunstância acima são

A) *Authentication Service (AH)* e *Encapsulating Security Payload (ESP).*

B) *Secure Header (SH)* e IV - *Extended Protocol (EXP).*

C) *Authentication Service (AH)* e *Extended Protocol (EXP).*

D) *Integrity Service (IS)* e *Encapsulating Security Payload (ESP).*

34. Um dos ataques comuns aos mecanismos de segurança das redes sem fios é a utilização de dicionários por força bruta. Nesse caso, o atacante submete diferentes senhas, baseado em um dicionário de senhas, na expectativa de que alguma senha seja validada. Para evitar este tipo de ataque nativamente, deve ser utilizado o mecanismo de

A) WEP (*Wired Equivalent Privacy*).

B) WPS (*Wi-Fi Protected Setup*).

C) WPA2 (*Wi-Fi Protected Access version 2*).

D) WPA3 (*Wi-Fi Protected Access version 3*).

35. Recentemente, foi divulgada uma grave vulnerabilidade no protocolo de comunicação WPA2, e na sua versão mais antiga, a WPA1. A vulnerabilidade foi descoberta por Mathy Vanhoef, pesquisador da Universidade de Leuven, na Bélgica, com pós-doutorado em segurança da informação. Segundo Vanhoef, sistemas que utilizam a ferramenta "*wpa_supplicant*" para negociação das chaves de criptografia em redes WPA e WPA2 estão mais vulneráveis, por exemplo Android (versão 6.0+) e Linux. A essa vulnerabilidade foi dado o nome de

A) KRACK (*Key Reinstallation Attacks*).

B) WCrack (*WPA Crack*).

C) WBFA (*WPA Brute Force Attack*).

D) WSF (*WPA Supplicant Fail*).

36. O chefe do departamento de TI da Security10 enviou para João, por e-mail, o programa simples em linguagem C, mostrado abaixo, com intuito de aferir os conhecimentos do novo contratado sobre segurança de software.

```
L1. void LerParametros (char *arg);
L2. void main (int argc, char *argv[]) {
L3.     if (arg > 1){
L4.             printf ("Parametros informados: %s\n", argv[1]);
L5.             LerParametros (argv[1]);
L6.     }
L7. }
L8. void LerParametros (char *arg) {
L9.       char buffer[10];
L10.      strcpy (buffer, arg);
L11.      printf (buffer);
L12. }
```

Junto ao código, estava a mensagem: “João, por favor, verifique esse código. Sei que estamos fazendo algo errado e, com isso, expondo uma vulnerabilidade de segurança comum em programação, mas não consigo perceber qual. Falamos mais sobre isso na segunda”.

João, ao analisar o código enviado, concluiu que esse apresenta como vulnerabilidade

A) uma Falha de Segmentação (do inglês, *Segmentation Fault*) na linha L5.

B) uma Falha de Segmentação (do inglês, *Segmentation Fault*) na linha L4.

C) um Estouro de buffer (do inglês, *Buffer Overflow*) na linha L9.

D) um Estouro de buffer (do inglês, *Buffer Overflow*) na linha L10.

37. Em Segurança Web, é bastante comum confundir o ataque de XSS (*Cross-site Scripting*) com o ataque de CSRF (*Cross-site Request Forgery*).

A diferença entre esses ataques está na

A) forma como os navegadores reconhecem o *payload*: no XSS o *payload* é reconhecido como código JavaScript puro, enquanto no CSRF, o navegador o reconhece como uma imagem codificada em Base64.

B) linguagem utilizada: o XSS utiliza um JavaScript, enquanto o CSRF utiliza Java puro.

C) maneira de executar o *payload*: o XSS utiliza um *script* no navegador web, enquanto o CSRF utiliza qualquer solicitação que execute um verbo HTTP GET ou POST para completar alguma ação válida na aplicação web.

D) origem do ataque: no XSS, o ataque tem sua origem na rede interna, enquanto no CSRF, o ataque tem origem na rede externa.

38. O departamento de TI da Security10 está envolvido no desenvolvimento de uma aplicação Web, mas está com receio de lançá-la em produção sem antes efetuar alguns testes de segurança. Como João acabou de ser admitido para a vaga em segurança, coube a ele realizar essa tarefa. Seu chefe de equipe sabe que, para a realização deste tipo de teste, é comum a utilização de plataformas que incluem recursos como *proxy*, *scanner* de vulnerabilidades e rastreamento de mensagens e conteúdo e, portanto, disponibilizou o seu próprio computador para que João realize os testes.

A ferramenta adequada para a realização dos testes requisitados é

A) Wireshark.

B) Burp Suite.

C) Netstat.

D) Packet Tracer.

39. Considere o trecho abaixo

> A Cartilha de Segurança para Internet da CERT.br é uma renomada fonte de informação sobre segurança da informação. Em uma de suas versões, entre outros conceitos, traz as definições de diferentes tipos de códigos maliciosos. Segundo a cartilha, há um tipo de código malicioso que torna inacessível os dados armazenados, geralmente usando criptografia, e exige pagamento de resgate para restabelecer o acesso ao usuário. O pagamento do resgate geralmente é feito via *bitcoins*. SimpleLocker e WannaCry são exemplos conhecidos desse tipo de código malicioso.

O trecho define claramente um

A) Adware.
B) Spyware.
C) Ransomware.
D) Backdoor.

40. Maria, do setor de Contabilidade da Security10, relatou que recentemente recebeu uma mensagem eletrônica sobre um seguro de vida que ela não solicitou, mas a mensagem provém do banco no qual ela tem conta. O conteúdo da mensagem trazia um link para o contrato do seguro com as informações gerais da apólice e um outro link para a geração do boleto a ser pago. Ao clicar em qualquer um dos links, era exibida uma página do banco requisitando os dados da conta, incluindo a senha para operações *online*. Tudo parecia legítimo, mas ao tentar prosseguir, sempre dava uma mensagem para tentar novamente. Nesse caso, Maria foi vítima de um ataque de

A) Phishing.
B) SPAM.
C) Malware.
D) Adware.

41. A Security10 resolveu implementar um *proxy* transparente com a utilização do *iptables* e *Squid*. Foi determinado que o serviço *Squid* será configurado na porta 3300. No entanto, o analista de TI, João, ainda está inseguro no uso do *iptables* e não sabe bem como realizar esta tarefa. Nesse contexto, o comando *iptables* necessário para permitir que requisições http padrão oriundas da rede interna, através da interface eth1, para acesso internet sejam automaticamente redirecionadas para a porta usada pelo Squid é

A) iptables -t nat -A PREROUTING -o eth1 -p tcp --dport 80 -j REDIRECT --to-port 3300.

B) iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 80 -j REDIRECT --to-port 3300.

C) iptables -i eth1 -p tcp --dport 80 -j REDIRECT --to-port 3300.

D) iptables -t nat -A PREROUTING -i eth1 -p tcp --dport 3300 -j REDIRECT .

42. O protocolo SSL (*Secure Sockets Layer*) é muito útil na proteção do canal de comunicação, sendo bastante utilizado para fornecer uma camada adicional de segurança às aplicações web. Sobre as características do SSL, analise as afirmativas abaixo.

I	O SSL opera entre as camadas de Transporte e Aplicação, segundo o modelo TCP/IP.
II	TLS (*Transport Layer Security*) é uma especificação de outro padrão para suportar o SSL em redes TCP/IP e é definido na RFC 5246.
III	O protocolo SSL fornece serviços básicos de confidencialidade e integridade a entidades de aplicação. É o caso do HTTP (*Hypertext Transfer Protocol*) que utiliza o SSL para fornecer navegação segura na Web, sendo então referenciado como HTTPS.
IV	Por padrão, para o HTTPS é utilizada a porta 8080.

Em relação ao SSL, estão corretas as afirmativas

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

43. O servidor Web da Security10 sofreu um ataque distribuído de negação de serviço, também conhecido como DDoS (*Distributed Denial of Service*), onde um computador mestre denominado *master* pode ter sob seu comando até milhares de computadores escravos ou *zombies*.

A rede formada pelo *master* e seus *zombies*, criada a fim de organizar o ataque de DDoS, é denominada

A) Botnet.
B) Rootnet.
C) Rootkit.
D) Intranet.

44. Uma boa política de segurança deve cobrir diferentes aspectos da organização, orientando sobre a necessidade de implementação de diferentes níveis de controle. Sobre alguns desses controles, analise as afirmativas abaixo.

I	Controles físicos referem-se à restrição de acesso indevido de pessoas a áreas críticas da empresa (ex: sala de servidores) e restrições de uso de equipamentos ou sistemas por funcionários mal treinados.
II	Controles lógicos referem-se a qualquer tipo de aplicação ou equipamento que usa da tecnologia para impedir que pessoas acessem documentos, dados ou qualquer tipo de informação sem a devida autorização.
III	Controles pessoais referem-se ao monitoramento de atividade digital dos funcionários e à cobrança de assiduidade na avaliação do funcionário.
IV	Controles organizacionais referem-se ao acompanhamento dos fatores de risco de TI identificados na organização.

Em relação aos controles que devem fazer parte da política de segurança, estão corretas as afirmativas

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

45. Os logs do Linux fornecem uma linha de tempo dos eventos para o *kernel* Linux, aplicativos e sistema, e são uma valiosa ferramenta de solução de problemas de segurança. Na maioria das distribuições Linux, os arquivos são armazenados em texto simples e podem ser encontrados no diretório /var/log e subdiretórios. Após suspeitar de uma invasão no servidor Linux da empresa Security10, o analista de TI precisa verificar todos os logs de autenticação, incluindo *logins* e métodos de autenticação bem-sucedidos e com falhas. Essas informações estarão gravadas provavelmente nos arquivos,

A) /var/log/boot.log e /var/log/dmesg.
B) /var/log/syslog e /var/log/messages.
C) /var/log/httpd/error_log e /var/log/httpd/access_log.
D) /var/log/auth.log ou /var/log/secure.

46. Backup é um mecanismo simples, mas de grande importância em qualquer esquema de segurança computacional. Na verdade, quando todos os outros mecanismos falham, o backup pode ser a solução. O recomendado é estabelecer uma agenda de backup, mesclando diferentes estratégias de backup, a fim de otimizar o tempo e os recursos gastos nesta tarefa. As estratégias de backup mais comuns são: backup completo ou *full*; incremental e diferencial. Na empresa Security10, o analista de TI, João, implementou a estratégia de backup *full* a cada semana, pois é preciso um final de semana para que a cópia de segurança seja gerada, devido à quantidade de dados. Insatisfeito e temendo o risco de uma falha no meio da semana, o que acarretaria em uma perda de alguns dias, João resolveu incrementar sua rotina de backup e incluir uma estratégia diária. Entretanto, a quantidade de dados computacionais da empresa inviabiliza um backup *full* diário. Assim, João optou por copiar somente os dados que não faziam parte do último backup completo.

Nesse caso, João realizará um backup do tipo

A) *full* semanal e um backup diferencial diário.
B) *full* semanal e um backup incremental diário.
C) completo quinzenal e um backup diferencial diário.
D) completo mensal e um backup incremental semanal.

47. Algumas situações de suspeita de cibercrimes exigem uma investigação forense computacional. Para esse fim, são necessárias ferramentas que permitam adquirir, preservar e recuperar as provas do suposto crime. Algumas ferramentas permitem, inclusive, a análise dos dados armazenados em mídias computadorizadas. No Brasil, a Operação Lava Jato deu notoriedade a este tipo de ferramenta, sendo fundamental para a investigação. Os sistemas IPED, EnCase, FTK e UFED Touch são exemplos conhecidos deste tipo de ferramenta. Infelizmente, a empresa Security10 não possui nenhuma dessas ferramentas que certamente seriam úteis para que o analista de TI, João, pudesse realizar a perícia que lhe foi atribuída. Na ausência dessas ferramentas, João resolveu enviar uma imagem assinada (através do uso de *hash*) do disco principal da máquina suspeita para um amigo da Polícia Federal que lhe prestará alguma ajuda. Nesse caso, considerando que João possui apenas o Linux à sua disposição, ele deve gerar a imagem através do seguinte comando:

A) dd if=/dev/hda bs=4K conv=sync,noerror | tee mycase.img

B) fsck -t ext4 /dev/hda > mycase.img

C) dd if=/dev/hda bs=4K conv=sync,noerror | tee mycase.img | md5sum > mycase.md5

D) fsck -M -y /dev/sda | tee mycase.img | md5sum > mycase.md5

48. Nos primeiros dias em que João iniciou suas atividades na empresa Security10, o chefe entregou um notebook para que João atribuísse um endereço IP ao equipamento. João ainda estava se adaptando ao seu setor e verificou as configurações de sua própria máquina, concluindo que estavam configurados o IP 192.168.33.111 e a máscara 255.255.255.0. Mesmo com pouca experiência, João sabia que não deveria atribuir um IP qualquer, pois este poderia já estar sendo utilizado em outro *host* e certamente iria acusar conflito de IP. Resolveu então procurar nas gavetas do seu setor uma lista dos IPs ativos, porém não a encontrou. Como alternativa, pensou em "pingar" cada endereço na faixa da rede local e anotar aqueles que respondessem, mas logo percebeu que era impraticável. Sem saber como proceder, acabou pedindo ajuda ao seu supervisor que recomendou a utilização do *nmap* para efetuar uma varredura na rede local para identificar os IPs ativos. Recomendou ainda evitar a varredura de porta, pois seria muito demorado. Levando-se em consideração as orientações do supervisor, João deve utilizar o *nmap* com os seguintes parâmetros

A) nmap -sF -n 192.168.33.0/24

B) nmap -sT -P0 -n -p25 192.168.33.0/24

C) nmap -sn 192.168.33.0/24

D) nmap -sT -F -p1-65535 192.168.33.0/24

49. O Regulamento Geral de Proteção de Dados ou GDPR (*General Data Protection Regulation*) recentemente adotado pela União Europeia (UE) é um rigoroso conjunto de regras sobre privacidade, válido para a UE, baseado em três pilares: governança de dados, gestão de dados e transparência de dados. No Brasil, existe a Lei Geral de Proteção de Dados (Lei nº 13.709) ou LGPD, sancionada em 14 de agosto de 2018 e que entrará em vigor a partir de agosto de 2020. O principal objetivo da LGPD é garantir transparência no uso dos dados das pessoas físicas em quaisquer meios. Esta lei altera a Lei nº 12.965, de 23 de abril de 2014, popularmente chamada de Marco Civil da Internet.

Considerando que a empresa Security10, criada e sediada apenas no Brasil, comercializa soluções de TI no mercado nacional e recentemente fechou contrato com uma empresa em Londres para a comercialização de seus produtos na UE, ela deve

A) apenas se ajustar ao LGPD e Marco Civil, por se tratar de uma empresa brasileira e, portanto, sujeita às leis do Brasil.

B) se ajustar não somente à LGPD e Marco Civil, mas também ao GDPR, sob o risco de ser penalizada na UE.

C) apenas se ajustar ao GDPR, pois esta é mais abrangente e se sobrepõe à LGPD e ao Marco Civil

D) se preocupar com privacidade dos dados apenas em 2020, quando a LGPD entrará em vigor.

50. De acordo com o Guia de Governança de TIC do SISP (Sistema de Administração dos Recursos de Tecnologia da Informação), a existência de práticas organizacionais de gestão da continuidade do negócio é uma das condicionantes para reduzir os riscos de TI e, consequentemente, aumentar a segurança da informação na organização. Baseado nesse guia, a Security10 planejou um conjunto de estratégias para garantir a continuidade do negócio. Em uma delas, a Security10 firmou um contrato com uma empresa da região a fim de espelhar seus centros de dados (*datacenters*), possibilitando o uso do centro de dados parceiro para a execução dos serviços de TI em caso de algum desastre ou falha severa em sua infraestrutura de TI, reduzindo o tempo de recuperação para algumas horas. Foi um contrato de muitos milhões de reais. Esse tipo de estratégia de Continuidade do Negócio é classificado como

A) *Fast site*.

B) *Cold site*.

C) *Hot site*.

D) *Warm site*.