412334

PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA MILITAR DO ESTADO DE SÃO PAULO

CONCURSO PÚBLICO

003. PROVA OBJETIVA

ANALISTA DE SEGURANÇA DA INFORMAÇÃO JUDICIÁRIO

- Você recebeu sua folha de respostas, este caderno, contendo 50 questões objetivas, e o caderno de prova dissertativa.
- Confira seus dados impressos na capa deste caderno e na folha de respostas.
- Quando for permitido abrir o caderno, verifique se está completo ou se apresenta imperfeições. Caso haja algum problema, informe ao fiscal da sala para a devida substituição desse caderno.
- Leia cuidadosamente todas as questões e escolha a resposta que você considera correta.
- Marque, na folha de respostas, com caneta de tinta preta, a letra correspondente à alternativa que você escolheu.
- A duração das provas objetiva e dissertativa é de 4 horas, já incluído o tempo para o preenchimento da folha de respostas e para a transcrição da resposta definitiva.
- Só será permitida a saída definitiva da sala e do prédio após transcorridas 3 horas do início das provas.
- Deverão permanecer em cada uma das salas de prova os 3 últimos candidatos, até que o último deles entregue sua prova, assinando termo respectivo.
- Ao sair, você entregará ao fiscal o caderno de prova dissertativa, a folha de respostas e este caderno.
- Até que você saia do prédio, todas as proibições e orientações continuam válidas.

AGUARDE A ORDEM DO FISCAL PARA ABRIR ESTE CADERNO DE QUESTÕES.

Nome do candidato

RG | Inscrição | Prédio | Sala | Carteira

FUNDAÇÃO vunesp

Confidencial até o momento da aplicação.

CONHECIMENTOS GERAIS

Língua Portuguesa

Leia o texto a seguir para responder às questões de **01** a **04**:

Nos anos 1970, um professor do curso de Psicologia de Harvard tinha um estranho aluno em sua classe. Depois das primeiras aulas, ele se aproximou do professor para explicar por que se matriculara naquele curso. Ele disse que precisava de ajuda, porque coisas estranhas estavam acontecendo com ele, como o fato de sua mulher falar as palavras em que ele estava pensando logo antes que ele pudesse dizê-las. Além disso, perdera o emprego dois dias depois de um colega fazer um comentário casual sobre cortes de pessoal no trabalho.

Com o tempo, afirmou, passara por dezenas de situações de má sorte, que considerava serem coincidências perturbadoras. A princípio, ficou confuso com a situação. Depois, assim como a maioria de nós faria, criou um modelo mental para reconciliar os fatos com suas crenças sobre o comportamento do mundo. A teoria que engendrou, no entanto, era muito diferente do que ditaria o senso comum: ele estava sendo usado como cobaia de um experimento científico complexo e secreto. Acreditava que o experimento era executado por um grande grupo de conspiradores, liderados pelo famoso psicólogo Skinner. Também acreditava que, quando o experimento estivesse concluído, ele ficaria famoso e talvez fosse eleito para um alto cargo público. Assim, matriculara-se no curso para aprender a testar sua hipótese, tendo em vista a quantidade de indícios que já acumulara.

(Leonard Mlodinow, *O andar do bêbado*. Adaptado)

01. É possível deduzir que o aluno matriculou-se no curso de Psicologia para encontrar explicações que

(A) pudessem ajudá-lo a abandonar a prática de acumular indícios de sua má sorte.

(B) corroborassem suas convicções acerca da lógica que preside os acontecimentos.

(C) permitissem defender as falas e as atitudes daqueles que o cercavam.

(D) determinassem as razões pelas quais as pessoas são demitidas de seus empregos.

(E) traduzissem o raciocínio que embasa as conclusões a que chega o senso comum.

02. Nos trechos transcritos, há comparação e hipótese, respectivamente, em:

(A) “Depois, assim como a maioria de nós faria, criou um modelo mental...” (2º parágrafo) e “... ele ficaria famoso e talvez fosse eleito para um alto cargo público.” (2º parágrafo)

(B) “... o experimento era executado por um grande grupo de conspiradores...” (2º parágrafo) e “Ele disse que precisava de ajuda, porque coisas estranhas estavam acontecendo com ele...” (1º parágrafo)

(C) “... um professor do curso de Psicologia de Harvard tinha um estranho aluno em sua classe.” (1º parágrafo) e “... depois de um colega fazer um comentário casual sobre cortes de pessoal no trabalho.” (1º parágrafo)

(D) “... ele se aproximou do professor para explicar por que se matriculara naquele curso.” (1º parágrafo) e “A princípio, ficou confuso com a situação.” (2º parágrafo)

(E) “Com o tempo, afirmou, passara por dezenas de situações de má sorte...” (2º parágrafo) e “... tendo em vista a quantidade de indícios que já acumulara.” (2º parágrafo)

03. Considere as passagens a seguir:

- “... depois de um colega fazer um comentário **casual**...” (1º parágrafo)
- “A teoria que **engendrou**, no entanto, era muito diferente...” (2º parágrafo)
- “... tendo em vista a quantidade de **indícios** que já acumulara.” (2º parágrafo)

No contexto em que foram empregadas, as palavras destacadas são, correta e respectivamente, sinônimas de

(A) “eventual”, “desvendou” e “deduções”.

(B) “ocasional”, “acompanhou” e “conclusões”.

(C) “pretensioso”, “criou” e “marcas”.

(D) “fortuito”, “idealizou” e “vestígios”.

(E) “essencial”, “elaborou” e “sinais”.

04. Considere as seguintes passagens do 2º parágrafo:

- “**A princípio**, ficou confuso com a situação...”
- “A teoria que engendrou, **no entanto**, era muito diferente do que ditaria o senso comum...”
- “**Assim**, matriculara-se no curso para aprender a testar sua hipótese, **tendo em vista** a quantidade de indícios que já acumulara.”

As expressões destacadas podem ser substituídas, respectivamente, sem prejuízo ao sentido original e de acordo com a norma-padrão, por:

(A) Inicialmente ... todavia ... Portanto ... considerando

(B) De modo geral ... portanto ... Logo ... visando

(C) Em tese ... porém ... Desse modo ... observando

(D) De pronto ... pois ... Com isso ... vislumbrando

(E) No começo ... ademais ... Então ... verificando

Leia o texto a seguir para responder às questões **05** e **06** :

Por que no Brasil a maioria da população tem rejeitado o parlamentarismo? A resposta aponta para a índole do nosso povo. Aqui a semente presidencialista viceja em todos os espaços.

O sociólogo francês Maurice Duverger defende a tese de que o gosto latino-americano pelo sistema presidencialista tem a ver com o aparato monárquico na região. O Império Inca, com seus grandes caciques, e depois o poderio espanhol, com seus reis, vice-reis e corregedores, plasmaram a inclinação por regimes de caráter autocrático.

O presidencialismo por estas plagas agregaria, assim, uma boa dose de autocracia. Já o parlamentarismo que vicejou na Europa teria se inspirado na ideologia liberal da Revolução Francesa, cujo alvo era a derrubada do soberano. Isso explicaria a distância da Europa ante o modelo presidencialista.

Portanto, o presidencialismo está fincado no altar mais alto da cultura política. O poder que dele emana impregna a figura do mandatário. A imagem do Estado e a imagem do governante imbricam-se. Sob essa configuração, imaginar que o parlamentarismo tenha chance por aqui é apostar que a fada madrinha decidiu deixar o reino da fantasia para nos visitar. Temos de conviver mesmo com o fardão presidencialista.

(Gaudêncio Torquato, Jornal da USP,
"Parlamentarismo, uma sombra no horizonte".
Disponível em: https://jornal.usp.br/articulistas/gaudencio-torquato/parlamentarismo-uma-sombra-no-horizonte/. Adaptado)

05. Assinale a alternativa em que todas as palavras foram empregadas em sentido próprio.

(A) "A resposta aponta para a índole do nosso povo." (1º parágrafo)

(B) "Por que no Brasil a maioria da população tem rejeitado o parlamentarismo?" (1º parágrafo)

(C) "Aqui a semente presidencialista viceja em todos os espaços." (1º parágrafo)

(D) "O presidencialismo por estas plagas agregaria, assim, uma boa dose de autocracia." (3º parágrafo)

(E) "A imagem do Estado e a imagem do governante imbricam-se." (4º parágrafo)

06. Considerando o contexto em que as expressões destacadas se apresentam, assinale a alternativa em que o comentário sobre elas é correto.

(A) "... ideologia liberal da Revolução Francesa, **cujo** alvo era a derrubada do soberano." (3º parágrafo) – corresponde a "que o".

(B) "Isso **explicaria** a distância da Europa ante o modelo presidencialista." (3º parágrafo) – o tempo do verbo expressa certeza.

(C) "... a fada madrinha decidiu deixar o reino da fantasia **para** nos visitar." (4º parágrafo) – estabelece relação de causa.

(D) "Temos de conviver **mesmo** com o fardão presidencialista." (4º parágrafo) – corresponde à palavra "ainda".

(E) "**Já** o parlamentarismo que vicejou na Europa..." (3º parágrafo) – introduz ideia que contrasta com a anterior.

07. Assinale a alternativa em que a norma-padrão de regência e concordância verbais foi plenamente respeitada.

(A) Existe, na história da América Latina, fatores importantes que embasam a opção das pessoas pelo presidencialismo.

(B) Na Europa, os ideais da Revolução Francesa acarretaram na preferência dos cidadãos pelo parlamentarismo.

(C) É comum que se estudem na escola os elementos que configuram os diferentes sistemas e formas de governo.

(D) Segundo alguns estudiosos, os países europeus tendem naturalmente em adotar o parlamentarismo como sistema de governo.

(E) Em muitas obras da ciência política, falam-se de questões que concernem aos sistemas de governo parlamentarista e presidencialista.

08. Considere a passagem a seguir:

Com meu pai, aprendi a não ter vaidade em relação _____ que parece honroso. A ser industrioso e pronto para ouvir os que _____ algo a contribuir para o bem comum. A estar sempre disposto a dar _____ cada um _____ que lhe cabe segundo o seu valor.

(Marco Aurélio, *Meditações*. Adaptado)

As lacunas devem ser preenchidas, correta e respectivamente, com:

(A) aquilo ... têm ... a ... aquilo

(B) aquilo ... tem ... à ... aquilo

(C) àquilo ... têm ... a ... àquilo

(D) àquilo ... têm ... a ... aquilo

(E) àquilo ... tem ... à ... àquilo

09. De acordo com um estudo que avalia os registros de crimes em certa região, o número total de registros durante o ano de 2023, quando comparado com o número total de registros durante o ano de 2022, correspondeu a um aumento de 50%. Verificou-se também que o número total de registros durante o ano de 2024, quando comparado com o número total de registros durante o ano de 2022, correspondeu a um aumento de 80%.

Se forem comparados, então, os números totais de registros durante os anos de 2023 e 2024, será possível verificar que este último, em comparação com o total de registros em 2023, correspondeu a um aumento de

(A) 30%.

(B) 25%.

(C) 42,5%.

(D) 20%.

(E) 62,5%.

10. Em certa comarca judicial, há no total 2.640 processos em tramitação, dos quais alguns são cíveis e outros são criminais. Alguns desses processos estão em fase recursal: dentre os cíveis, a quinta parte; dentre os criminais, a quarta parte. Desses processos da comarca em fase recursal, a diferença entre os números de processos cíveis e criminais é igual a 132.

Com base nessas informações, é correto afirmar que a diferença entre os números totais de processos cíveis e de processos criminais dessa comarca é igual a

(A) 920.

(B) 880.

(C) 960.

(D) 900.

(E) 940.

11. Dois submarinos militares, A e B, transmitem sinais de segurança para a central de comando em intervalos de tempo regulares: o submarino A, a cada 5 minutos; o submarino B, a cada 8 minutos. Às 12 horas de certo dia, esses dois submarinos transmitiram seus sinais de segurança à central.

Quantas vezes a central de comando recebeu sinal de segurança de um, e apenas um, submarino, considerando o intervalo entre as 12 horas e as 13 horas e 42 minutos desse dia?

(A) 34

(B) 32

(C) 30

(D) 26

(E) 28

12. Uma empresa possui uma política de incentivo à assiduidade por meio da disponibilização de verbas semestrais, que são repassadas a cada gestor de equipe. Uma vez recebida pelo gestor, a verba é dividida entre os seus funcionários de modo que o valor a ser recebido por cada um seja inversamente proporcional ao número de faltas injustificadas que o funcionário teve naquele semestre. O gestor da equipe de Amanda, Bruno e Cecília recebeu R$ 2.200,00 e vai dividir esse valor entre os 3 funcionários de acordo com o critério da empresa.

Se, naquele semestre, os números de faltas injustificadas de Amanda, Bruno e Cecília foram iguais a 2, 3 e 1, respectivamente, então quantos reais Amanda receberá de bonificação?

(A) 600,00

(B) 520,00

(C) 730,00

(D) 400,00

(E) 1.100,00

13. Um sistema de localização opera através de coordenadas para determinar a posição de um evento ou objeto no espaço.

Para determinar as coordenadas de certo evento de interesse militar, esse programa precisou solucionar o sistema de equações do primeiro grau formado pelas seguintes 3 equações:

I. $2x + y - z = -1$

II. $x + y + z = 6$

III. $2y - z = 5$

Uma vez determinados os valores que solucionam esse sistema, é correto afirmar que $x^2 + y^2 + z^2$ é igual a

(A) 6.

(B) 24.

(C) 41.

(D) 26.

(E) 12.

14. Cícero vai comprar azulejos para colocar em uma parede retangular com 2,5 m de altura e 4,0 m de comprimento. Ele comprará peças de forma quadrada, com lado medindo 25 cm. Dessas peças, 96 serão azuis, e as demais, brancas. Para facilitar o cálculo, desprezou-se qualquer espaço que possa haver entre as peças em sua colocação.

Se os preços do metro quadrado das peças brancas e azuis são, respectivamente, R$ 50,00 e R$ 58,00, qual será o valor total dessa compra, em reais?

(A) 558,00

(B) 568,00

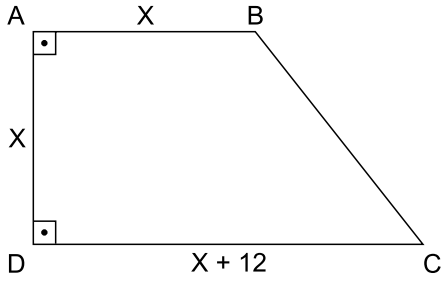
(C) 548,00

(D) 578,00

(E) 588,00

R A S C U N H O

15. Um depósito de munições possui a forma de um trapézio. Sua altura e sua base menor possuem a mesma medida X, e sua base maior supera sua base menor em 12 metros. A figura a seguir (fora de escala) representa esse depósito:



Foi solicitado a Mauro que calculasse a soma das medidas dos lados $\overline{AB}$, $\overline{AD}$ e $\overline{CD}$, para posterior avaliação do custo de reinstalação de cerca elétrica no topo desses muros. Além das informações apresentadas, Mauro sabe que a área desse depósito mede 315 m^2.

Com base nessas informações, Mauro concluiu corretamente que a soma das medidas dos lados $\overline{AB}$, $\overline{AD}$ e $\overline{CD}$ é igual a quantos metros?

(A) 60

(B) 48

(C) 57

(D) 54

(E) 51

R A S C U N H O

Raciocínio Lógico

16. Considere as seguintes proposições lógicas:

- Se Mauro não está endividado, então seu carro está na funilaria.
- Se Silvano foi de ônibus para o trabalho, então sua moto está na oficina mecânica.
- Se o carro de Mauro está na funilaria ou a moto de Silvano está na oficina mecânica, então haverá pelo menos uma vaga livre na empresa para que Janaína estacione seu carro.

Se não havia vagas livres na empresa para que Janaína estacionasse seu carro, é correto concluir, logicamente, que Mauro

(A) está endividado e Silvano foi de ônibus para o trabalho.

(B) está endividado e Silvano não foi de ônibus para o trabalho.

(C) não está endividado e Silvano não foi de ônibus para o trabalho.

(D) está endividado ou Silvano não foi de ônibus para o trabalho.

(E) não está endividado ou Silvano não foi de ônibus para o trabalho.

17. Filomena é uma pessoa que procura cuidar da própria casa. A esse respeito, considere a seguinte proposição lógica:

- Se a cozinha não está organizada, então Filomena estava doente ou ela ficou o dia todo fora.

Assinale a alternativa que apresenta corretamente uma proposição logicamente equivalente à apresentada.

(A) Se Filomena estava doente ou ficou o dia todo fora, então a cozinha não está organizada.

(B) Se a cozinha está organizada, então Filomena não estava doente ou ela não ficou o dia todo fora.

(C) Se Filomena não estava doente ou não ficou o dia todo fora, então a cozinha está organizada.

(D) Se a cozinha está organizada, então Filomena não estava doente e ela não ficou o dia todo fora.

(E) Se Filomena não estava doente e não ficou o dia todo fora, então a cozinha está organizada.

18. Considere as seguintes sequências numéricas, formadas a partir de padrões matemáticos:

S_1: (14; 11; 8; 5; …)

S_2: (–25; –18; –11; –4; …)

Foram somados os elementos de S_1 e de S_2 que ocupam a posição n em cada uma dessas sequências, e obteve-se, como resultado, 365.

Então, o valor de n é

(A) 95.

(B) 92.

(C) 91.

(D) 93.

(E) 94.

19. Em uma urna, há 9 bolas, numeradas de 1 a 9, das quais 3 são brancas, 3 são azuis e 3 são vermelhas, mas não necessariamente nessa ordem. Sobre essas bolas, sabe-se:

- todas as bolas vermelhas possuem números maiores ou iguais a 5;
- das bolas brancas, uma tem o número 1, e os números das outras duas não são números primos;
- a bola de número 8 é vermelha;
- a bola de número 9 não é branca;
- a soma dos números das bolas vermelhas é 22.

Com base nessas informações, é correto afirmar que a bola de número

(A) 2 é azul.

(B) 7 é vermelha.

(C) 6 é vermelha.

(D) 9 é branca.

(E) 4 é azul.

20. Em uma sala, todas as pessoas presentes falam pelo menos uma das três seguintes línguas estrangeiras: inglês, francês e espanhol.

Sobre essas pessoas, sabe-se que o número das que falam

- apenas inglês e espanhol é 2 unidades maior do que o número das que falam as três línguas;
- apenas francês é 4 vezes o número das que falam as três línguas;
- apenas inglês é 6 unidades maior do que o número das que falam apenas inglês e francês;
- espanhol, mas não falam inglês, é 9 vezes o número das que falam apenas inglês e francês.

Sabendo que o total de pessoas que falam inglês é 16 e que o total de pessoas que falam espanhol é 31, é correto concluir que o número total de pessoas nessa sala é igual a

(A) 45.

(B) 46.

(C) 48.

(D) 47.

(E) 44.

R A S C U N H O

CONHECIMENTOS ESPECÍFICOS

21. A existência de uma política de segurança relacionada ao uso de mídias removíveis em uma organização

(A) mitiga ou controla o risco de infecção por *worms*.

(B) dispensa o uso de softwares antivírus nos computadores da organização, reduzindo custos.

(C) é considerada obsoleta, porque, mesmo quando utilizadas, as mídias removíveis não trazem mais riscos de segurança aos computadores modernos.

(D) impõe que todos os computadores da organização usem o mesmo sistema operacional, visando a compatibilidade do sistema de arquivos desses computadores.

(E) é considerada obsoleta, porque apenas computadores antigos possuem unidades de disco flexível (disquetes), que são as mídias removíveis.

22. Um dos pilares comumente adotados em iniciativas de segurança da informação tem como princípio básico que as informações permaneçam imutáveis quando estão em repouso ou durante sua transmissão.

Tal pilar é chamado de

(A) disponibilidade.

(B) acessibilidade.

(C) integridade.

(D) autenticidade.

(E) confidencialidade.

23. No contexto do framework *OAuth* 2.0, assinale a alternativa correta.

(A) *Access tokens* devem ser interpretados pelo cliente *OAuth*.

(B) *Access tokens* devem ser usados para efetuar requisições ao servidor de recursos (*resource server*).

(C) *Sender-constrained tokens* não requerem que o cliente *OAuth* prove a posse de uma chave privada.

(D) *Bearer tokens* incluem, de forma codificada, informações de identificação do usuário que efetua requisições ao servidor de recursos (*resource server*).

(E) *ID tokens* devem ser usados para efetuar requisições ao servidor de recursos (*resource server*).

24. Dentre as alternativas a seguir, assinale aquela que reflete o conceito de privacidade por padrão.

(A) Deve-se dar preferência ao uso de conexões discadas com a Internet em detrimento a conexões de banda larga, uma vez que as primeiras são imunes a ataques do tipo *man-in-the-middle*.

(B) Enquanto estiver em trânsito, um usuário deve manter seu *smartphone* em "modo avião" para não ter sua localização rastreada.

(C) Autenticação por fatores biométricos não devem ser utilizados em qualquer tipo de sistema, uma vez que sua coleta envolve dados de características físicas do usuário.

(D) Aplicativos e *websites* de redes sociais não devem ser usados, conferindo ao usuário menor exposição de dados pessoais na Internet.

(E) Quando um usuário utiliza um sistema ou serviço digital pela primeira vez, suas configurações de privacidade devem iniciar no modo que lhe confere maior grau de privacidade.

25. Conceitualmente, a principal diferença entre um ataque do tipo DoS e um DDoS é que o ataque do tipo DoS

(A) tem como alvo específico o sistema operacional Linux (bastante comum em servidores da Internet), enquanto o DDoS é capaz de atacar múltiplos sistemas operacionais.

(B) tem como alvo o protocolo de camada de transporte UDP, enquanto o DDoS tem como alvo o TCP, de modo que as aplicações que podem ser atacadas são distintas entre ambos.

(C) tem como alvo servidores de aplicações *web*, enquanto o DDoS tem como alvo o lado do cliente, principalmente os navegadores de Internet.

(D) é lançado, em geral, a partir de uma única origem, enquanto o DDoS é lançado a partir de múltiplas origens simultaneamente, ainda que possa ser disparado por um comando único.

(E) tem como alvo o protocolo de camada de rede IPv4, enquanto o DDoS tem como alvo o IPv6.

26. A validação de conteúdos de entrada recebidos em chamadas a *web services* baseados em XML (ex.: SOAP), antes que tais conteúdos sejam consumidos, é importante para evitar tipos de ataques conhecidos.

Um deles é o XML *Bomb*, que consiste em

(A) utilizar caracteres estrangeiros no conteúdo do documento XML de entrada, fora do alfabeto latino, provocando o mau funcionamento do *parser*.

(B) colocar um documento JSON dentro de uma *tag* XML, confundindo o *parser* e provocando seu mau funcionamento.

(C) inserir conteúdo XML em parâmetros GET dentro da URL da requisição HTTP, confundindo o servidor *web* e potencialmente provocando sua derrubada ou travamento.

(D) montar um XML com pelo menos um erro de má-formação, tais como *tags* abertas sem fechamento, provocando o mau funcionamento ou travamento do *parser*.

(E) definir entidades XML de tal modo que haja uma expansão de uma entidade em várias outras, e assim repetidas vezes, até formar um conteúdo muito grande que tem o potencial de provocar estouro de memória no *parser*.

27. A respeito do conceito conhecido como MFA, ou *multifactor authentication*, assinale a alternativa correta.

(A) Um exemplo de fator de conhecimento é a leitura de impressão digital.

(B) Requer o uso de um *token* físico ou aplicativo de celular que gera um número, que muda com o tempo, a ser digitado em complemento ao usuário e senha, durante um processo de *login*.

(C) Um exemplo de fator de inerência é o reconhecimento facial.

(D) Requer o uso de um fator do tipo “algo que você é” durante um processo de *login*, em complemento à digitação de um usuário e senha.

(E) É sinônimo de 2FA (*two-factor authentication*).

28. Uma prática recomendada para a implementação do SIEM (*Security Information and Event Management*) em uma empresa é que sejam estabelecidas políticas de BYOD. Essas políticas, independentemente de serem proibitivas ou permissivas, dizem respeito ao

(A) acesso físico a servidores *on premises* da empresa.

(B) uso de dispositivos de informática (computadores, *tablets*, etc.) pessoais de funcionários para fins de trabalho.

(C) uso de inteligência artificial generativa para fins de trabalho.

(D) tipo de cabeamento de rede que deve ser usado nas instalações físicas da empresa.

(E) processo de seleção de fornecedores para a compra de equipamentos de rede, considerando principalmente os aspectos de segurança.

29. No padrão *Syslog* de registro (*logging*) de mensagens, o código *facility* é usado para

(A) especificar o tipo de sistema que está logando uma mensagem.

(B) especificar o nível de dificuldade para tratar ou resolver o efeito ou erro reportado por uma mensagem.

(C) especificar o nível de severidade de uma mensagem.

(D) codificar o endereço IP do dispositivo que originou uma mensagem.

(E) especificar o identificador (*id*) do usuário responsável por verificar e tratar uma mensagem.

30. Um determinado arquivo ZIP está encriptado pelo algoritmo AES (que é suportado por algumas ferramentas de compactação) e requer uma senha para ter seu conteúdo extraído. Isso significa que

(A) a decriptação necessária para a extração do conteúdo precisa ser feita por um serviço na nuvem, o que possibilita manter o algoritmo em segredo.

(B) a senha consiste em uma chave privada.

(C) embora o conteúdo esteja encriptado, a senha precisa estar armazenada no próprio arquivo em uma área não encriptada, o que não é seguro.

(D) o arquivo está encriptado por criptografia simétrica.

(E) a senha consiste em uma chave pública.

31. No contexto de uma rede local (LAN) com DMZ em arquitetura *dual firewall*, de acordo com as práticas recomendadas, o *firewall* de perímetro

(A) deve ser configurado para aceitar conexões de entrada, provenientes da Internet, exclusivamente para a DMZ.

(B) deve rejeitar todas as conexões entrantes da Internet, para garantir máxima segurança, mesmo se a DMZ possuir servidores *web* com aplicações que devem ser acessadas por usuários externos.

(C) deve ser configurado para aceitar conexões de entrada, provenientes da Internet, exclusivamente para a LAN.

(D) é o *firewall* que fica entre a LAN e a DMZ.

(E) deve possuir, no mínimo, quatro interfaces de rede.

32. De acordo com os *Pods Security Standards* da documentação do Kubernetes, a política direcionada a desenvolvedores e operadores de aplicações não críticas é chamada de

(A) *Privileged*.

(B) *Baseline*.

(C) *Restricted*.

(D) *Regular*.

(E) *Basic*.

33. De acordo com a norma ABNT NBR ISO/IEC 27001:2022, a organização deve estabelecer os objetivos da segurança da informação para as funções e níveis relevantes.

Segundo a norma, dentre outras coisas, esses objetivos devem ser

(A) independentes da política de segurança da informação.

(B) imutáveis, evitando que atualizações indevidas comprometam os objetivos originais.

(C) votados por todos os funcionários da organização, garantindo participação ampla da equipe no processo.

(D) memorizados pela equipe de segurança cibernética, garantindo mais agilidade no planejamento.

(E) disponibilizados como informação documentada.

34. *Rootkits* do tipo *bootloader* são caracterizados por

(A) utilizar técnicas de *phishing* para infectar computadores.

(B) serem ativados antes mesmo do sistema operacional da máquina inicializar.

(C) roubar senhas e dados de pagamento armazenados em navegadores, carregando esses dados (*load*) em servidores remotos mantidos por criminosos digitais.

(D) hospedar o sistema operacional alvo como uma máquina virtual e, assim, interceptar chamadas de hardware.

(E) encriptar arquivos do usuário e exigir um resgate financeiro para decriptá-los, em geral solicitando uma carga (*load*) de valores em criptomoedas a um endereço específico.

35. Assinale a alternativa que corresponde a uma prática adequada para *hardening* de servidores Linux.

(A) Dar preferência ao uso do protocolo Telnet, considerado mais moderno, em substituição ao SSH.

(B) Habilitar todos os serviços que vêm por padrão na distribuição Linux instalada, mesmo que não utilizados, pois cada um adiciona um aspecto extra de segurança.

(C) Dar preferência por manter contas de usuário com senha vazia, pois estas não podem ser descobertas por ataques de força bruta (*brute force attacks*).

(D) Desabilitar o *login* do usuário `root`, dando preferência ao uso do comando `sudo`.

(E) Modificar o UID de contas de usuário que não são `root` para 0, garantindo que não tenham permissões máximas de acesso ao sistema.

36. Uma recomendação de segurança para o servidor de banco de dados MySQL no sistema operacional Linux consiste em

(A) fornecer o privilégio `FILE` para usuários não administrativos.

(B) fornecer o privilégio `PROCESS` para usuários não administrativos.

(C) não executar o processo `mysqld` como o usuário `root` do Linux.

(D) mover os *scripts* e arquivos binários do servidor, tais como o `mysqld`, para o diretório `/boot`.

(E) oferecer permissão de acesso somente-leitura à tabela `mysql.user` para todos os usuários do MySQL.

37. No contexto de gestão de riscos cibernéticos, uma fórmula comum para estimar financeiramente a perda anualizada é

ALE = ARO x SLE

em que ALE (*annualized loss expectancy*) representa a expectativa de perda anualizada, ARO (*annual rate of occurrence*) é a taxa anual de ocorrência e SLE (*single loss expectancy*) é a expectativa de perda única.

Por sua vez, SLE pode ser calculado por

SLE = AV x EF

em que AV (*asset value*) é o valor monetário do ativo e EF (*exposure factor*) é o fator de exposição.

Para um ativo que vale $ 5.000,00 com fator de exposição de 10%, para que a expectativa de perda anualizada seja inferior a $ 1.800,00, a taxa anual de ocorrência máxima (considerando-se somente números inteiros) deve ser igual a

(A) 3.

(B) 1.

(C) 2.

(D) 5.

(E) 4.

38. O normativo de segurança referente à Resolução CNJ nº 396/2021 (Estratégia Nacional de Segurança Cibernética do Poder Judiciário) institui o chamado Comitê Gestor da Informação do Poder Judiciário (CGSI-PJ), sendo correto afirmar que

(A) o CGSI-PJ se reunirá exclusivamente em caráter extraordinário.

(B) o CGSI-PJ tem, em sua composição, três especialistas representantes do Tribunal Superior do Trabalho.

(C) os integrantes do CGSI-PJ não necessitam ter conhecimento técnico na área de segurança da informação.

(D) as indicações dos representantes do CGSI-PJ serão feitas pela presidência do Supremo Tribunal Federal.

(E) o CGSI-PJ se reunirá, em caráter ordinário, semestralmente.

39. A Resolução CNJ nº 91/209 – Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Judiciário Brasileiro – MoReqJus, versão 1.0, em sua seção 5 – Preservação, descreve algumas técnicas que podem ser utilizadas para evitar situações que possam por em risco a preservação de documentos em virtude de obsolescência tecnológica, sendo, especificamente, duas dessas técnicas:

(A) captura e codificação.

(B) recolhimento e cognição.

(C) emulação e conversão de dados.

(D) manutenção e classificação.

(E) gestão e desmembramento.

40. Considerando o processo da Análise de Impacto de Negócio (BIA – *Business Impact Analysis*), é correto afirmar que ele

(A) representa um processo que examina os processos de negócios, identificando os processos críticos e as áreas de alto risco, visando estudar prováveis impactos de incidentes adversos naturais ou provocados pelo homem no bom andamento dos negócios.

(B) representa, específica e prioritariamente, um processo projetado para possibilitar que a contratação de colaboradores da empresa seja a mais adequada possível.

(C) representa, unicamente, as ações que o departamento jurídico de uma empresa deve tomar, frente a todo o conjunto de leis estabelecido pelo governo de um país.

(D) corresponde à definição e implementação das técnicas de compactação e encriptação de dados vitais para a continuidade dos negócios de uma empresa.

(E) tem como premissa básica reduzir significativamente o orçamento da empresa, notadamente no que diz respeito aos gastos com equipamentos de informática.

41. Assinale a alternativa que apresenta corretamente a camada do modelo OSI que é responsável pelo roteamento e pelo endereçamento lógico.

(A) Enlace de Dados.

(B) Transporte.

(C) Sessão.

(D) Rede.

(E) Apresentação.

42. O mecanismo NAT apresenta diversas características, por exemplo,

(A) converter nomes de redes para endereços IPv6.

(B) converter endereços IP privados em públicos.

(C) utilizar faixas de endereços reservadas, como a faixa de 192.168.0.0 a 192.172.255.255/16.

(D) incorporar mecanismos de proteção de redes, como o *firewall*.

(E) possibilitar o rastreamento do caminho do pacote transmitido, por meio de ferramentas como *traceroute*.

43. Deseja-se realizar a interligação de duas redes, sendo que elas utilizam protocolos distintos. Um equipamento que é utilizado para essa interconexão é o(a)

(A) *switch*.

(B) *gateway*.

(C) *bridge*.

(D) concentrador.

(E) ponto de acesso.

44. Os principais tipos de *backup* utilizados são: completo, incremental e diferencial. Assinale a alternativa que apresenta a ordem correta desses tipos de *backup*, do mais rápido ao mais lento, considerando a velocidade de recuperação dos dados.

(A) Completo > Incremental > Diferencial

(B) Diferencial > Completo > Incremental

(C) Completo > Diferencial > Incremental

(D) Diferencial > Incremental > Completo

(E) Incremental > Completo > Diferencial

45. A respeito do método de teste de segurança de aplicações conhecido como SAST, é correto afirmar que

(A) consiste em uma operação de escaneamento de portas de rede abertas (*port scan*).

(B) é realizado com a aplicação em execução, por meio de um agente de testes embutido na própria aplicação.

(C) requer acesso ao código-fonte.

(D) é um subtipo do método DAST.

(E) inclui o método DAST como seu subtipo.

46. Na metodologia de *pentest* PTES, dentre suas 7 seções principais, aquela que tem como foco estabelecer acesso a um sistema ou recurso, contornando (*bypassing*) as restrições de segurança, é conhecida como

(A) *Intelligence Gathering*.

(B) *Full Attack*.

(C) *Threat Modeling*.

(D) *Post Exploitation*.

(E) *Exploitation.*

47. Uma determinada aplicação *web* possui uma página de *login* onde o usuário deve preencher um nome de usuário e senha. É sabido que esses usuários e senhas são gerenciados pela própria aplicação, e não por um serviço externo. Um atacante efetuou o seguinte preenchimento, na tentativa de realizar um ataque do tipo *SQL Injection*.

Usuário: `" or ""="`

Senha: `" or ""="`

As aspas duplas indicadas fazem parte do preenchimento. O efeito exato dessa tentativa dependerá da construção interna da aplicação *web*, o que é desconhecido.

No entanto, pela análise do preenchimento, essa tentativa de ataque tem o potencial de

(A) excluir a tabela de usuários do sistema.

(B) inserir indevidamente um novo usuário na tabela de usuários do sistema, permitindo posterior *login* com a conta desse novo usuário.

(C) alterar a senha do usuário administrador da aplicação *web*.

(D) retornar todos os usuários do sistema.

(E) excluir por completo todo o banco de dados da aplicação.

48. De acordo com a classificação STRIDE, a ação de ameaça que visa alterar ou modificar maliciosamente dados persistentes, como registros em um banco de dados, ou alterar dados em trânsito entre dois computadores em uma rede aberta, como a Internet, é conhecida como

(A) *tampering*.

(B) *spoofing*.

(C) *repudiation*.

(D) *denial of service*.

(E) *elevation of privilege*.

49. Arquivos de *shell script* geralmente começam com uma linha que contém a sequência de caracteres chamada "*shebang*".

A função dessa linha é indicar

(A) o autor do *script*.

(B) o espaço de memória alocado para o *script*.

(C) o interpretador para executar o *script*.

(D) a quantidade de memória alocada pelo *script*.

(E) as permissões de execução do *script*.

50. Jenkins é uma plataforma de integração e entrega contínua. Nos arquivos `Jenkinsfile`, define-se um *pipeline* que segue uma hierarquia específica.

Considerando essa hierarquia, assinale a alternativa que apresenta a ordem correta, do nível mais alto ao mais baixo.

(A) Pipeline > agent > stage > step > stages.

(B) Pipeline > agent > steps > stage > stages.

(C) Pipeline > agent > steps > stages > stage.

(D) Pipeline > agent > stages > stage > steps.

(E) Pipeline > agent > stages > steps > stage.