ABGF
Agência Brasileira Gestora de Fundos Garantidores e Garantias

Colégio	Sala	Ordem
M0001	0001	0001

Setembro/2026

I Concurso Público para Provimento de Cargos de

Analistas (TI): Análise de Dados; Análise e Segurança de Dados; *Front-End* / *Back-End* / DevOps; Infraestrutura e Redes

Nome do Candidato: Caderno de Prova 'E05', Tipo 001

Nº de Inscrição: MODELO

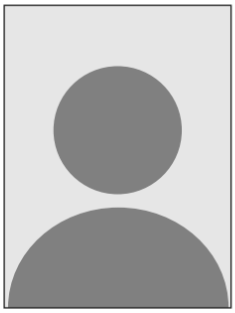
Nº do Caderno: TIPO-001

Nº do Documento: 0000000000000000

ASSINATURA DO CANDIDATO

PROVA

Conhecimentos Gerais
Conhecimentos Específicos
Discursiva-Redação



INSTRUÇÕES

Quando autorizado pelo fiscal de sala, transcreva a frase abaixo, com sua caligrafia usual, no espaço apropriado na Folha de Respostas.

Alberto Santos Dumont projetou, construiu e voou os primeiros balões dirigíveis com motor a gasolina.

- Verifique se este caderno corresponde a sua opção de cargo, contém 60 questões, numeradas de 1 a 60 e se contém a proposta e o espaço para o rascunho da Prova Discursiva-Redação.
  Caso contrário, solicite imediatamente ao fiscal da sala a substituição do caderno.
  Não serão aceitas reclamações posteriores.
- Para cada questão existe apenas UMA resposta certa.
- Leia cuidadosamente cada uma das questões e escolha a resposta certa.
- Essa resposta deve ser marcada na FOLHA DE RESPOSTAS que você recebeu.

VOCÊ DEVE

- Procurar, na FOLHA DE RESPOSTAS, o número da questão que você está respondendo.
- Verificar no caderno de prova qual a letra (A,B,C,D,E) da resposta que você escolheu.
- Marcar essa letra na FOLHA DE RESPOSTAS, conforme o exemplo: Ⓐ ● Ⓒ Ⓓ Ⓔ
- Ler o que se pede na Prova Discursiva-Redação e utilizar, se necessário, o espaço para rascunho.

ATENÇÃO

- Marque as respostas com caneta esferográfica de material transparente e tinta preta ou azul. Não será permitida a utilização de lápis, lapiseira, marca-textos, régua ou borracha durante a realização da prova.
- Marque apenas uma letra para cada questão. Será anulada a questão em que mais de uma letra estiver assinalada.
- Responda a todas as questões.
- Não será permitida nenhuma espécie de consulta ou comunicação entre os candidatos, nem a utilização de livros, anotações, códigos, manuais, notas ou impressos não permitidos, máquina calculadora ou similar, nem qualquer espécie de aparelho eletrônico.
- Em hipótese alguma o rascunho da Prova Discursiva-Redação será corrigido.
- Você deverá transcrever sua Prova Discursiva-Redação, a tinta, na folha apropriada.
- A duração da prova é de 5 horas para responder a todas as questões objetivas, preencher a Folha de Respostas e fazer a Prova Discursiva-Redação (rascunho e transcrição) na folha correspondente.
- Ao término da prova, chame o fiscal da sala e devolva todo o material recebido.
- É proibida a divulgação ou impressão parcial ou total da presente prova. Direitos Reservados.

CONHECIMENTOS GERAIS

Língua Portuguesa

Atenção: Leia o texto a seguir para responder às questões de números 1 a 4.

Quando a tecnologia serve para concentrar controle, ela amplia desigualdades; quando é desenhada para distribuir oportunidades, ela promove bem-estar e crescimento. O progresso não é linear nem neutro: é produto de decisões humanas e institucionais.

A IA generativa redefine tarefas e papéis, mas também desafia o significado do trabalho. Ao automatizar o que antes expressava o talento humano, pode corroer o senso de competência. Ao impor processos padronizados, reduz a autonomia. E ao substituir interações humanas por algoritmos fragiliza o pertencimento.

São três dimensões que, segundo a psicologia do trabalho, sustentam o bem-estar e a produtividade. A IA pode encurtar o árduo percurso do aprendizado, aquele que desenvolve instinto, julgamento e experiência. A eficiência não deve substituir o amadurecimento.

As evidências são eloquentes. Pesquisas de Puntoni e outros autores mostram que trabalhadores avaliados por algoritmos demonstram menos empatia. Segundo testes estatísticos, consumidores, por sua vez, valorizam mais produtos quando percebem participação humana em sua criação.

Mas a IA também pode abrir um novo ciclo de oportunidades. Como nos mostrou o prof. Christian Terwiesch, a IA generativa pode transformar o próprio processo de inovação. Em vez de restringir decisões a poucos, ela permite que mais pessoas criem, testem e proponham soluções apoiadas por IA; o que ele chama de "torneios de inovação". O papel humano, nesse contexto, seria o de curador, não de executor.

A GenAI ajuda a criar mais e melhores ideias, e mais rápido, mas continua precisando de gente para dar direção, propósito e juízo de valor. Empresas que souberem equilibrar as forças entre a velocidade da máquina e o discernimento humano abrirão novos horizontes de vantagem competitiva.

O futuro da inovação, portanto, não pertence apenas à tecnologia, mas à cultura que a cerca.

Mas, em última instância, essas escolhas não se farão no vácuo. Elas serão moldadas pelos incentivos econômicos, pelas políticas públicas e pela forma como os mercados valorizam – ou não – o investimento em pessoas.

Se o sistema recompensar apenas ganhos de produtividade de curto prazo, o uso da IA tenderá à substituição e à concentração. Se, ao contrário, premiar a criação de valor humano e a difusão do conhecimento, o avanço tecnológico poderá se tornar um novo motor de prosperidade compartilhada. O equilíbrio econômico dessa nova era estará em unir produtividade com desenvolvimento humano; eficiência com aprendizado.

O desafio, portanto, não é apenas das empresas, mas também da regulação: fazer com que o progresso técnico caminhe ao lado do progresso econômico e social. A inteligência artificial pode gerar abundância ou desigualdade. O que determinará o resultado não é o algoritmo, mas o conjunto de escolhas, incentivos e valores construídos em torno dele.

(VESCOVI, Ana Paula. Disponível em: **https://www1.folha.uol.com.br/colunas/ana-paula-vescovi/2025/10/o-poder-e-o-progresso-na-era-da-inteligencia-artificial.shtml**. Adaptado)

1. A autora elabora uma hipótese seguida de um possível desdobramento em:

(A) *Pesquisas de Puntoni e outros autores mostram que trabalhadores avaliados por algoritmos demonstram menos empatia.*

(B) *O desafio, portanto, não é apenas das empresas, mas também da regulação.*

(C) *A IA generativa redefine tarefas e papéis, mas também desafia o significado do trabalho.*

(D) *Se o sistema recompensar apenas ganhos de produtividade de curto prazo, o uso da IA tenderá à substituição e à concentração.*

(E) *Segundo testes estatísticos, consumidores, por sua vez, valorizam mais produtos quando percebem participação humana em sua criação.*

2. Respeitando as normas de concordância verbal, uma redação alternativa para um trecho do texto está em:

(A) Nem linear, nem neutro: cabem às decisões humanas e institucionais a redefinição do progresso.

(B) Caberá à união entre a produtividade e o desenvolvimento humano o equilíbrio econômico dessa nova era.

(C) São cada vez mais difíceis considerar como tangíveis as fronteiras entre a cultura de uma nação e o uso que fará do desenvolvimento tecnológico.

(D) Repousam nas empresas e também nas normas de regulação a expectativa de que o progresso técnico caminhe ao lado do econômico e social.

(E) Não apenas as políticas públicas, mas também a forma como se valorizam o investimento em pessoas determinará o futuro da inovação.

3. *Empresas que souberem equilibrar as forças entre a velocidade da máquina e o discernimento humano abrirão novos horizontes de vantagem competitiva.*

Ao se transpor a frase acima para a voz passiva, o verbo “abrir” deverá assumir a seguinte forma:

(A) serão abertos.

(B) se abrirá.

(C) haverá de abrir.

(D) têm-se aberto.

(E) foram abertos.

4. O termo empregado para retomar uma palavra anteriormente usada no texto está sublinhado em:

(A) *E ao substituir interações humanas por algoritmos fragiliza o pertencimento.*

(B) *O que determinará o resultado não é o algoritmo, mas o conjunto de escolhas, incentivos e valores construídos em torno dele.*

(C) *Em vez de restringir decisões a poucos, ela permite que mais pessoas criem, testem e proponham soluções apoiadas por IA.*

(D) *O futuro da inovação, portanto, não pertence apenas à tecnologia, mas à cultura que a cerca.*

(E) *Pesquisas de Puntoni e outros autores mostram que trabalhadores avaliados por algoritmos demonstram menos empatia.*

Língua Inglesa

5. *China’s domestic economy has faltered and is being sustained largely by a record trade surplus and strong exports from the technology and clean energy sectors.*
Consumer spending remains weak, while much of the housing market is still in crisis. A five-year nationwide decline in apartment prices has wiped out much of the middle class’s savings in a country where households typically hold about three-quarters of their assets in real estate.

(Disponível em: **https://www.nytimes.com/2026/07/30/business/china-economy-politburo.html**)

Without change in meaning, the word that could replace “wiped out” (underlined in the second paragraph) is:

(A) *dismissed.*

(B) *discharged.*

(C) *derailed.*

(D) *distorted.*

(E) *drained.*

6. A five-year nationwide decline in apartment prices has wiped out much of the middle class’s savings in a country where households typically hold about three-quarters of their assets in real estate.

The pronoun “their”, underlined in the excerpt, refers to

(A) *assets.*

(B) *savings.*

(C) *households.*

(D) *country.*

(E) *real estate.*

Raciocínio Lógico, Matemático e Analítico

7. Em uma empresa pública federal, formam-se duplas entre programadores e assistentes. Há, no máximo, 50 pessoas nessa empresa. Em certo momento, $\frac{3}{4}$ dos programadores trabalham em parceria com $\frac{4}{5}$ dos assistentes. O número total de pessoas nessa empresa é:

(A) 30

(B) 29

(C) 16

(D) 31

(E) 37

8. Ana, Bruno, Célia, Dario e Ênio são colegas de trabalho. Um deles quebrou a impressora. Ao questioná-los, o gerente teve as seguintes respostas:

Ana: "Eu não quebrei a impressora."
Bruno: "Eu quebrei a impressora."
Célia: "Ênio não quebrou a impressora."
Dario: "Eu não quebrei a impressora."
Ênio: "Ana quebrou a impressora."

Se apenas um dos colegas não está falando a verdade, quem quebrou a impressora foi

(A) Ana.
(B) Bruno.
(C) Célia.
(D) Dario.
(E) Ênio.

Noções de Direito Constitucional e Administrativo

9. Considere:

I. Proteger o meio ambiente e combater a poluição em qualquer de suas formas.
II. Legislar sobre trânsito e transporte.
III. Legislar sobre seguridade social.

Com base na Constituição Federal de 1988, é competência comum da União, dos Estados, do Distrito Federal e dos Municípios o constante APENAS em

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

10. De acordo com a Lei nº 13.303/2016,

(A) a empresa pública poderá lançar debêntures ou outros títulos ou valores mobiliários, conversíveis em ações, e emitir partes beneficiárias, devendo divulgar toda e qualquer forma de remuneração dos administradores.
(B) empresa pública é a entidade dotada de personalidade jurídica de direito público, com criação autorizada por lei e com patrimônio próprio, cujo capital social é integralmente detido pela União, pelos Estados, pelo Distrito Federal ou pelos Municípios.
(C) a exploração de atividade econômica pelo Estado será exercida exclusivamente por meio de empresa pública, dependendo, sua constituição, de prévia autorização legal que indique, de forma clara, relevante interesse coletivo ou imperativo de segurança nacional.
(D) independe de autorização legislativa a criação de subsidiárias de empresa pública e de sociedade de economia mista, assim como a participação de qualquer delas em empresa privada, cujo objeto social deve estar relacionado ao da investidora, nos termos da Constituição Federal.
(E) sociedade de economia mista é a entidade dotada de personalidade jurídica de direito privado, com criação autorizada por lei, sob a forma de sociedade anônima, cujas ações com direito a voto pertençam em sua maioria à União, aos Estados, ao Distrito Federal, aos Municípios ou a entidade da administração indireta.

Ética, Integridade, Governança, *Compliance* e Controles Internos

11. Uma empresa pública na forma de sociedade de economia mista federal contratou determinado fornecedor para a prestação de serviços de manutenção predial. Posteriormente, apurou-se que um preposto desse fornecedor ofereceu vantagem indevida a empregado público para obter tratamento favorecido em processo de licenciamento de interesse da contratante. À luz da Lei nº 12.846/2013 (Lei Anticorrupção), é correto afirmar que a empresa

(A) poderá ser responsabilizada administrativa e civilmente apenas mediante comprovação de que sua diretoria tinha conhecimento prévio do ato lesivo praticado pelo preposto do fornecedor.
(B) poderá ser responsabilizada objetivamente, nos âmbitos administrativo e civil, independentemente da comprovação de culpa ou dolo de seus dirigentes.
(C) poderá ser responsabilizada apenas na esfera penal, uma vez que a lei não prevê sanções administrativas para pessoas jurídicas.
(D) estará isenta de responsabilização caso o preposto do fornecedor venha a ser processado e condenado individualmente pelo ato de corrupção.
(E) poderá firmar acordo de leniência que a exima integralmente de qualquer sanção, bastando para tanto cooperar com as investigações.

12. O modelo das três linhas de defesa é amplamente adotado por organizações, inclusive empresas estatais, para estruturar a governança de riscos e dos controles internos. Considerando esse modelo, é correto afirmar que, ao promover avaliação independente e objetiva sobre a eficácia da governança, da gestão de riscos e dos controles internos, a auditoria interna posiciona-se na

(A) primeira linha, pois atua diretamente na execução e no controle cotidiano dos processos operacionais da organização.

(B) segunda linha, uma vez que estabelece as políticas de gestão de riscos e conformidade a serem observadas pelas áreas operacionais.

(C) terceira linha, por fornecer avaliação independente sobre a eficácia da governança, da gestão de riscos e dos controles internos.

(D) primeira e segunda linhas simultaneamente, por acumular funções de execução operacional e de supervisão de riscos.

(E) terceira linha, e sua função deve necessariamente ser exercida por empresa de auditoria independente contratada externamente.

Proteção de Dados, Segurança da Informação e Uso Responsável de Dados

13. Uma Agência Brasileira Gestora de Fundos Garantidores mantém dados pessoais de representantes e beneficiários relacionados às operações dos fundos e contrata uma empresa especializada em tecnologia para hospedar e processar parte dessas informações. Durante a execução dos serviços, a agência identifica um incidente de segurança que possibilitou acesso não autorizado a dados pessoais armazenados pela empresa contratada. Considerando as disposições da LGPD, a

(A) empresa de tecnologia, por administrar o ambiente em que os dados são armazenados, assume a condição de controladora e passa a definir as providências relacionadas aos titulares afetados pelo incidente identificado.

(B) agência gestora, na condição de controladora, deve avaliar o incidente e adotar as providências cabíveis, inclusive comunicar a ANPD e os titulares quando houver risco ou dano relevante, enquanto a empresa contratada atua como operadora.

(C) agência gestora deixa de responder pelas decisões relacionadas aos dados pessoais quando contrata uma empresa especializada, pois a execução técnica do tratamento passa a ser realizada pelo operador contratado.

(D) empresa contratada responde integralmente pelo incidente perante os titulares, pois a manutenção da infraestrutura tecnológica lhe atribui responsabilidade direta pelas decisões sobre o tratamento dos dados pessoais.

(E) existência de contrato entre a agência gestora e a empresa de tecnologia implica que a agência gestora deve avaliar o incidente em conjunto com a empresa contratada, considerando a natureza dos dados, as medidas de segurança e os possíveis impactos aos titulares, e ambos devem tomar as providências cabíveis, incluindo a comunicação à ANPD.

14. Uma Agência Brasileira Gestora de Fundos Garantidores identificou duas ocorrências durante suas atividades. Na primeira, alguns colaboradores receberam uma mensagem personalizada, encaminhada por uma instituição parceira, informando sobre uma suposta atualização cadastral, que direcionava a pessoa para uma página visualmente semelhante ao portal institucional, onde eram solicitados usuário e senha. Na segunda, um sistema utilizado para consulta de informações permaneceu inacessível durante determinado período após receber requisições provenientes de grande quantidade de dispositivos conectados à Internet. Considerando as características específicas dos ataques descritos, a primeira ocorrência corresponde

(A) à engenharia social, pois a personalização da mensagem constitui o elemento central do ataque, enquanto a segunda corresponde ao *ransomware*, devido ao comprometimento da disponibilidade do sistema afetado.

(B) ao *ransomware*, pois a obtenção das credenciais pode permitir o bloqueio posterior de sistemas, enquanto a segunda corresponde ao *phishing*, devido à utilização de uma infraestrutura distribuída para atingir o serviço.

(C) à engenharia social, pois obriga o usuário a fornecer credenciais em ambiente fraudulento, enquanto a segunda corresponde a um ataque DDoS, caracterizado pela tentativa de explorar vulnerabilidades do sistema por meio de requisições *backdoor.*

(D) ao *phishing*, pois emprega uma comunicação fraudulenta para capturar credenciais, enquanto a segunda corresponde à engenharia social, pois utiliza diferentes dispositivos para induzir o sistema a processar requisições.

(E) ao *phishing*, pois combina uma mensagem fraudulenta com uma página destinada à captura de credenciais, enquanto a segunda corresponde a um ataque DDoS, no qual múltiplos dispositivos contribuem para sobrecarregar o serviço e afetar sua disponibilidade.

Noções de Economia, Finanças Públicas, Sistema Financeiro, Garantias e Crédito à Exportação

15. O Fundo de Garantia à Exportação (FGE), instituído pela Lei nº 9.818/1999, constitui um dos principais instrumentos de apoio oficial às exportações brasileiras. A respeito da natureza e do funcionamento desse fundo, é correto afirmar que o FGE

(A) é fundo contábil de natureza pública, vinculado ao Tesouro Nacional, cuja gestão compete à Agência Brasileira Gestora de Fundos Garantidores e Garantias (ABGF), destinado a cobrir riscos comerciais, políticos e extraordinários nas operações de exportação com apoio oficial.

(B) constitui pessoa jurídica de direito privado, organizada sob a forma de associação civil sem fins lucrativos, com patrimônio próprio segregado do Tesouro Nacional.

(C) tem por finalidade exclusiva assegurar a estabilidade cambial das operações de exportação, não alcançando riscos de natureza comercial ou política.

(D) é administrado diretamente pelo Banco Nacional de Desenvolvimento Econômico e Social (BNDES), na qualidade de agente financeiro responsável pela concessão de crédito à exportação.

(E) tem sua atuação estendida à cobertura de operações de importação realizadas por empresas brasileiras de pequeno porte.

16. Considere a seguinte situação hipotética: uma seguradora, ao ceder parte de seus riscos a um ressegurador, estabelece contratualmente que reterá, para cada sinistro individualmente considerado, um valor fixo de até R$ 2 milhões, ficando o ressegurador responsável pelo montante excedente a esse limite, até o teto contratado, independentemente da proporção que o risco cedido representa em relação ao risco total assumido pela seguradora. Essa modalidade de resseguro é denominada

(A) resseguro proporcional, na modalidade de quota-parte (*quota-share*).

(B) resseguro proporcional, na modalidade de excedente de responsabilidade (*surplus*).

(C) resseguro não proporcional, na modalidade de excesso de danos (*excess of loss*).

(D) resseguro não proporcional, na modalidade de *stop loss*.

(E) retrocessão, uma vez que o ressegurador transfere parte do risco assumido a outro ressegurador.

Sustentabilidade, Aspectos Ambientais, Sociais e de Governança (ASG), Diversidade e Inclusão

17. For institutions subject to the Brazilian PRSAC regulatory *framework*, it correctly describes the Social, Environmental and Climate Responsibility Policy (PRSAC) and the actions aimed at its effectiveness:

(A) They should be coordinated with the risk management framework, but the institution may assess social, environmental and climate-related risks in isolation, without addressing their interactions with other risks incurred by the institution.

(B) They must appoint a director who will approve and review the policy and assume the board of directors' responsibilities for adherence, integration and timely correction, irrespective of whether a board has been constituted at the institution.

(C) They should primarily provide a framework for public communication and philanthropic initiatives, while social, environmental and climate-related considerations affecting business, activities, processes and stakeholder relationships remain within other institutional policies.

(D) They should be proportionate to the institution's business model, the nature of its operations and the complexity of its products, services, activities and processes; adequate to the magnitude and materiality of its exposures to social, environmental and climate-related risks; and consider corresponding impacts and business opportunities.

(E) They should follow a uniform design across the financial system to ensure comparability, while differences in business models, operations, product and service complexity and risk exposures are addressed through separate internal instruments.

18. A financial institution is developing a methodology to classify investments and financing linked to economic activities within the scope of the Brazilian Sustainable Taxonomy (TSB). The operations may involve green bonds, sovereign green bonds, carbon credits or blended finance.

The basis of assessment that the institution use to determine whether the underlying economic activity is aligned with the TSB is:

(A) Base the classification on the relevant TSB technical criteria applied to the underlying economic activity, verifying substantial contribution to its defined objectives, do no significant harm and compliance with the applicable minimum safeguards.

(B) Base the classification on must the Green Bond Principles, utilizing using eligible use of proceeds, project evaluation and selection, management of proceeds and reporting.

(C) Base the classification on eligibility under a sovereign green bond framework, using the public nature of the issuer and the environmental allocation of proceeds.

(D) Base the classification on verified carbon-credit methodologies, using quantified reductions or removals.

(E) Base the classification on blended-finance principles, using the strategic mobilization of additional commercial finance for sustainable development.

Noções de Análise de Dados, Informações e Indicadores

19. Tanto Ishikawa como Cinco Porquês são metodologias que podem ser utilizadas na análise e identificação de causas-raiz, mas não têm exatamente a mesma função nem operam da mesma forma. Uma distinção relevante é:

(A) Ishikawa é quantitativo, baseado fundamentalmente na análise de dados coletados e tratados; Cinco Porquês é eminentemente qualitativo e fortemente randômico.

(B) Ishikawa identifica, no momento da elaboração do Diagrama, somente causas comprovadas; Cinco Porquês trabalha somente com dados estatísticos.

(C) Ishikawa busca estruturar e explorar múltiplas categorias de possíveis causas; Cinco Porquês aprofunda uma cadeia causal por questionamentos sucessivos.

(D) ambos trabalham com coleta e análise de dados para identificação da causa-raiz, porém Ishikawa apresenta uma única causa, enquanto Cinco Porquês apresenta as cinco principais em ordem de prevalência.

(E) Cinco Porquês trabalha com dimensões diferentes de um problema ou falha sistêmica; Ishikawa investiga e avalia apenas a dimensão econômico-financeira.

20. No que concerne aos diferentes tipos indicadores de desempenho, tem-se que um *leading indicator* distingue-se de um *lagging indicator* na medida em que

(A) não se presta à medição de performance, pois o indicador apenas captura situações exógenas à organização, como variações de mercado.

(B) é utilizado para avaliar os resultados alcançados e analisar o desempenho após a ocorrência dos eventos.

(C) mede exclusivamente resultados financeiros, conectando-se com os índices de performance da instituição.

(D) somente pode ser utilizado no nível operacional, fornecendo métricas para ações corretivas de forma pontual.

(E) procura acompanhar fatores antecedentes ou direcionadores que podem influenciar resultados futuros.

CONHECIMENTOS ESPECÍFICOS

Fundamentos de Sistemas e Redes

21. Em um *cluster* Kubernetes destinado à execução de código não confiável, foi configurado um *runtime* que emprega máquinas virtuais leves para ampliar o isolamento proporcionado pelos mecanismos convencionais de contêineres. Ao processar a criação de um novo *sandbox*, o fluxo que caracteriza adequadamente essa arquitetura é o *runtime* que

(A) inicia o monitor de máquina virtual, inicializa um *kernel* convidado no ambiente isolado e utiliza um agente no sistema convidado para gerenciar os processos do *workload*.

(B) inicia o monitor de máquina virtual, conserva os processos do *workload* no sistema hospedeiro e utiliza o *kernel* convidado principalmente para mediar o acesso aos *namespaces* do *host*.

(C) mantém uma máquina virtual persistente no nó, executa os *sandboxes* como processos isolados nesse mesmo sistema convidado e utiliza *cgroups* para estabelecer a principal fronteira entre *tenants*.

(D) inicia um processo de *sandbox* no sistema hospedeiro, encaminha suas chamadas de sistema para um agente privilegiado e utiliza uma máquina virtual para armazenar os sistemas de arquivos dos *workloads*.

(E) inicializa um *kernel* convidado compartilhado pelos *sandboxes* do nó, executa cada *workload* em *namespaces* próprios dentro desse ambiente e mantém a máquina virtual independente da criação dos *sandboxes*.

---

22. Durante a análise de uma captura sanitizada de uma LAN IPv6, um servidor possui o endereço `2001:db8:8a2e:370:7334:1b9c:a2d7:6f3a`. Um roteador precisa resolver o endereço de enlace desse servidor por *Neighbor Discovery*. Considerando o *Neighbor Solicitation Multicast* usado para essa resolução, o endereço IPv6 de destino exato é

(A) `FF02::1:FFA2:D76F`

(B) `FF05::1:FFD7:6F3A`

(C) `FF02::1:FF34:1B9C`

(D) `FF02::1:FFD7:6F3A`

(E) `FF02::1:FF6F:3A00`

---

23. Uma Agência Brasileira Gestora de Fundos Garantidores e Garantias migrou a rede de acesso para IPv6-*only*. Os *endpoints* executam aplicações IPv6-*capable*, consultam os destinos por DNS e o desenho não inclui CLAT ou B4 nos clientes. Sistemas externos legados publicam registros A e as conexões são iniciadas pelos *endpoints*, com compartilhamento de endereços IPv4 públicos na borda. A arquitetura que implementa exatamente esse requisito é:

(A) 464XLAT com CLAT nos clientes e PLAT *stateful* na borda do domínio IPv6.

(B) DNS64 com NAT64 *stateful* na borda do domínio IPv6.

(C) *Dual-stack* com endereços IPv4 e IPv6 atribuídos aos clientes do domínio.

(D) DS-Lite com função B4 nos clientes e AFTR *stateful* na borda do domínio.

(E) MAP-T com regras de mapeamento *stateless* entre CE e BR na borda do domínio.

---

24. Uma Agência Brasileira Gestora de Fundos Garantidores e Garantias utiliza um único SSID corporativo em vários prédios e autentica usuários por credenciais individuais. Funcionários, terceiros e administradores devem ingressar em VLANs distintas conforme a identidade autenticada, mantendo o mesmo SSID durante a mobilidade. O controlador possui integração com um servidor AAA/RADIUS. Considerando essas condições, a implementação que realiza essa associação é:

(A) Q-in-Q IEEE 802.1ad, adicionando uma S-VLAN externa distinta ao tráfego de cada grupo autenticado no acesso.

(B) *private* VLAN com portas *isolated* e *community*, separando grupos de estações dentro de uma mesma VLAN de acesso.

(C) 802.1X com RADIUS, usando *Tunnel-Type*, *Tunnel-Medium-Type e Tunnel-Private-Group-ID* para atribuição dinâmica da VLAN.

(D) LLDP-MED com *voice* VLAN, utilizando RADIUS para autenticação do *endpoint* e associando a VLAN de voz anunciada pelo *switch* ao perfil identificado na porta.

(E) mapeamento estático de VLAN por SSID, vinculando cada perfil corporativo a uma WLAN e VLAN previamente configuradas.

---

25. Uma WLAN anteriormente configurada com WPA2-Personal passa a operar exclusivamente em WPA3-Personal, sem modo de transição. O requisito de segurança determina que a captura passiva das mensagens de autenticação não forneça um verificador que permita testar sucessivas hipóteses da senha sem nova interação com o ponto de acesso. Nesse contexto, o mecanismo que deve realizar a autenticação baseada em senha utilizada na formação do material inicial de chave é o

(A) OWE, que negocia criptografia oportunista entre estações de redes abertas sem utilizar uma credencial de autenticação previamente compartilhada.

(B) EAP-TLS, que executa autenticação IEEE 802.1X baseada em certificados digitais previamente provisionados nas partes participantes da comunicação.

(C) FT-PSK, que reduz o tempo de transição entre pontos de acesso utilizando material criptográfico previamente derivado durante a autenticação.

(D) WPA2-PSK, que obtém a chave mestra mediante PBKDF2 aplicado à senha compartilhada e ao identificador utilizado pela rede.

(E) SAE, que executa uma troca autenticada por senha e estabelece novo material criptográfico entre as partes participantes.

Banco de Dados

26. Após cada fechamento mensal, uma instituição deve preservar os valores de garantia e exposição por mês, fundo, beneficiário e modalidade, sem que alterações posteriores no sistema operacional modifiquem as posições já encerradas. As consultas históricas devem ser processadas fora do ambiente transacional e acessar os atributos de cada eixo analítico sem percorrer cadeias de tabelas dimensionais. A arquitetura que atende integralmente a esses requisitos é composta por um *data*

(A) *warehouse* independente, com fato de *snapshot* periódico mensal na granularidade definida e dimensões desnormalizadas vinculadas diretamente ao fato por chaves substitutas.

(B) *warehouse* independente, com fato transacional no nível de cada movimentação e apuração dos valores mensais durante as consultas, utilizando dimensões normalizadas vinculadas por chaves naturais.

(C) *mart* independente, com cópias das tabelas normalizadas do sistema operacional e recomposição das posições mensais durante as consultas por meio de relacionamentos entre entidades replicadas.

(D) *warehouse* independente, com fato de *snapshot* acumulativo atualizado em cada fechamento e dimensões normalizadas distribuídas em tabelas hierárquicas vinculadas por chaves substitutas.

(E) *mart* integrado ao ambiente operacional, com posições mensais armazenadas em tabela própria e atributos analíticos obtidos das mesmas tabelas normalizadas utilizadas nas transações.

---

27. Uma Agência Gestora de Fundos Garantidores e Garantias avalia modelos de bancos de dados NoSQL para quatro cargas de trabalho independentes:

I. Dossiês recuperados como agregados, contendo campos opcionais, listas e subestruturas que podem variar entre registros.

II. Valores de sessão acessados por chave exata e descartados após um tempo de vida configurado.

III. Consultas de beneficiário final que percorrem cadeias de controle societário com profundidade variável.

IV. Eventos de telemetria gravados continuamente em grande volume, organizados em partições definidas pela origem do evento, com o *timestamp* como chave de ordenação dentro de cada partição, permitindo consultas eficientes por chave de partição e por intervalos da chave de ordenação.

Considerando o modelo de dados que favorece cada padrão de acesso, a sequência correta correspondente a I, II, III e IV é:

(A) Documentos; chave-valor; *wide-column*; grafos.

(B) *Wide-column*; documentos; grafos; chave-valor.

(C) Chave-valor; grafos; documentos; *wide-column.*

(D) Documentos; chave-valor; grafos; *wide-column.*

(E) Grafos; *wide-column*; chave-valor; documentos.

---

28. Em um modelo de dados de uma Agência Gestora de Fundos Garantidores e Garantias, a entidade `CertificadoGarantia` possui chave primária (`id_fundo, nr_certificado`), sendo possível que um mesmo `nr_certificado` ocorra em fundos distintos. Cada certificado pode possuir diversas ocorrências de `CoberturaParcela`. O atributo `nr_parcela` diferencia as parcelas de um mesmo certificado, embora possa assumir o mesmo valor em certificados distintos. O atributo `data_vencimento` também pode apresentar valores repetidos entre parcelas do mesmo certificado. Considerando a transformação para o modelo relacional, a definição correta da chave primária mínima de `CoberturaParcela` e da respectiva chave estrangeira que referencia `CertificadoGarantia` é:

(A) PK `(nr_certificado, nr_parcela)` e FK `(id_fundo, nr_certificado)`.

(B) PK `(id_fundo, nr_parcela)` e FK `(id_fundo, nr_certificado)`.

(C) PK `(id_fundo, nr_certificado, nr_parcela)` e FK `(id_fundo, nr_certificado)`.

(D) PK `(id_fundo, nr_certificado, data_vencimento)` e FK `(id_fundo, nr_parcela)`.

(E) PK `(nr_certificado, nr_parcela, data_vencimento)` e FK `(id_fundo, nr_certificado)`.

---

29. Em um SGBD relacional, um painel consulta frequentemente registros de garantias aplicando condições de igualdade sobre `id_fundo` e `status` e uma condição de intervalo sobre `data_referencia`. Deseja-se implementar uma solução que deve disponibilizar a consulta como uma relação virtual reutilizável, obter os dados das tabelas-base no momento de sua execução e utilizar um índice B-tree composto com as colunas submetidas a igualdade antes da coluna submetida a intervalo. A implementação que satisfaz simultaneamente esses requisitos consiste em criar uma

(A) *view* materializada atualizada por agendamento e manter, na estrutura armazenada, um índice B-tree composto por (`id_fundo, status, data_referencia`).

(B) *view* não materializada e manter, na tabela-base, um índice B-tree composto por (`id_fundo, status, data_referencia`).

(C) tabela derivada atualizada por processo incremental e manter, na tabela-base, índices B-tree independentes sobre `id_fundo`, `status` e `data_referencia`.

(D) *procedure* parametrizada que execute a seleção e manter, na tabela-base, um índice B-tree composto por (`data_referencia, id_fundo, status`).

(E) CTE incorporada aos comandos do painel e manter, na tabela-base, índices B-tree independentes sobre `id_fundo`, `status` e `data_referencia`.

30. Em uma aplicação de *stream processing*, um sistema de processamento contínuo agrupa registros em janelas de *event time*. Em determinado instante, o maior *timestamp* recebido pela aplicação é `14:08:20`. A configuração admite desordenação de até 90 segundos e utiliza essa tolerância para determinar o avanço do progresso lógico do *event time*. Nessa situação, o mecanismo utilizado para sinalizar aproximadamente `14:06:50` como progresso do *event time* é um

(A) *checkpoint* distribuído, que registra uma imagem consistente dos estados dos operadores e permite restaurar o processamento após falhas sem utilizar a ordem temporal dos registros como referência de progresso.

(B) mecanismo de *backpressure*, que propaga aos operadores anteriores a redução da capacidade de consumo e controla a vazão do fluxo quando componentes posteriores processam registros em velocidade inferior.

(C) indicador de *consumer lag*, que compara a posição alcançada pelo consumidor com a posição disponível no *log* e permite avaliar o volume ainda pendente de processamento nas partições.

(D) registro de *offset* confirmado, que mantém a posição a partir da qual um consumidor pode retomar a leitura e auxilia a recuperação do processamento depois de reinicializações ou rebalanceamentos.

(E) *watermark*, que comunica aos operadores uma estimativa do avanço do tempo associado aos eventos e permite avaliar condições temporais de disparo das janelas.

Segurança da Informação e Cibersegurança

31. Uma Agência Gestora de Fundos Garantidores e Garantias publica serviços utilizando endereços IP próprios por meio de um enlace de internet com capacidade de 2 Gbit/s. Durante ataques volumétricos, aproximadamente 8 Gbit/s de tráfego UDP são direcionados a esses endereços. Os servidores permanecem com recursos computacionais disponíveis, mas o enlace de acesso torna-se saturado. A agência precisa conservar os endereços IP publicados e permitir que conexões legítimas continuem alcançando os serviços, sem aumentar a capacidade do enlace contratado. Considerando que a mitigação deve impedir que o tráfego identificado como malicioso atravesse o enlace de acesso da organização, a solução tecnicamente adequada consiste em

(A) instalar um dispositivo de filtragem no lado interno do enlace de acesso, dimensionado para identificar os datagramas maliciosos e descartar o tráfego depois de sua chegada à rede corporativa.

(B) configurar no provedor um policiamento agregado de 2 Gbit/s para o prefixo anunciado, mantendo dentro dessa taxa tanto os fluxos legítimos quanto os classificados como potencialmente maliciosos.

(C) acionar no provedor um mecanismo de *blackhole* baseado no prefixo de destino, descartando a montante o tráfego destinado aos endereços atacados enquanto permanecer ativa a condição de mitigação.

(D) desviar a montante o tráfego destinado aos endereços protegidos para uma infraestrutura de *scrubbing*, que filtre o ataque e encaminhe à organização o tráfego legítimo resultante.

(E) distribuir os serviços entre servidores internos e aplicar controles de taxa individualmente em cada instância, de forma que os fluxos recebidos sejam repartidos antes do processamento pelas aplicações.

32. Uma arquitetura publica APIs REST por meio de um API *gateway* que realiza autenticação OAuth 2.0 e validação estrutural das requisições com base nos contratos OpenAPI. A equipe de segurança pretende acrescentar um controle *inline* no caminho das requisições externas. O novo controle deverá examinar o conteúdo HTTP presente em diferentes partes das mensagens, aplicar regras de detecção atualizáveis e impedir que requisições classificadas como maliciosas alcancem os serviços de *backend*. O componente mais adequado para desempenhar essa função é um

(A) *Web Application Firewall* operando em modo preventivo, com regras de inspeção HTTP atualizáveis para identificar e bloquear padrões de ataque na entrada.

(B) validador de contratos OpenAPI operando no *gateway*, com políticas para rejeitar mensagens incompatíveis com tipos, formatos, limites e esquemas definidos para cada operação.

(C) *service mesh* com autenticação mútua e políticas de autorização entre *workloads*, destinado a controlar identidades de serviço e comunicações internas entre componentes da aplicação.

(D) sistema de detecção de intrusão de rede em modo passivo, destinado a analisar cópias do tráfego e emitir alertas relacionados a eventos considerados suspeitos.

(E) agente de proteção de *runtime* implantado nos *workloads*, destinado a observar processos, chamadas ao sistema e comportamentos apresentados pelos componentes durante sua execução.

33. Dois NGFW formam um *cluster* de alta disponibilidade ativo/passivo. As configurações de segurança estão sincronizadas e, após um *failover* planejado, o *peer* anteriormente passivo assume os endereços virtuais e passa a aceitar imediatamente novas conexões. Entretanto, sessões TCP estabelecidas antes da mudança precisam ser reiniciadas pelos clientes. As capturas de pacotes não indicam assimetria de roteamento nem tradução de endereços no tráfego avaliado. Nesse cenário, o mecanismo de alta disponibilidade que deve ser habilitado ou corretamente configurado para permitir a continuidade das conexões já estabelecidas após a troca do nó ativo é a

(A) replicação das configurações de políticas de segurança entre os membros do *cluster* a cada mudança do equipamento que exerce a função ativa.

(B) replicação da tabela de vizinhança de camada 2 entre os membros do *cluster* durante cada alteração de nó ativo.

(C) sincronização das rotas aprendidas dinamicamente entre os membros do *cluster* antes da transferência dos endereços virtuais compartilhados.

(D) preservação das decisões de balanceamento de caminhos entre os membros do *cluster* durante a alteração do equipamento responsável pelo encaminhamento.

(E) replicação do estado dinâmico das sessões entre os membros do *cluster*.

34. Uma aplicação corporativa atua como *Relying Party* OIDC e utiliza *Authorization Code Flow*. Durante uma auditoria, exigiu-se associar a sessão iniciada pelo cliente ao ID *Token* recebido e detectar a reutilização de um ID *Token* pertencente a outra transação. Considerando que o valor deve ser enviado na *Authentication Request* e posteriormente conferido no ID *Token*, o parâmetro/*claim* que atende exatamente ao requisito é

(A) `jti`

(B) `state`

(C) `code_verifier`

(D) `nonce`

(E) `acr`

---

35. Uma Agência Gestora de Fundos Garantidores classificada como Grupo de Implementação 2 do CIS Controls gerencia *laptops* corporativos, *tablets* e *smartphones* e está configurando o bloqueio automático após tentativas locais de autenticação malsucedidas. Considerando o Safeguard 4.10 do CIS Controls v8.1.2, que trata do bloqueio automático de dispositivos portáteis após falhas locais de autenticação, os limites máximos definidos para *laptops* e para *tablets* e *smartphones*, respectivamente, são:

(A) 15 e 10.

(B) 20 e 10.

(C) 20 e 15.

(D) 10 e 20.

(E) 15 e 5.

Engenharia de *Software*

36. Uma Agência Brasileira Gestora de Fundos Garantidores utiliza PHP para validar as regras de negócio relacionadas ao cálculo de coberturas. Considere que o trecho de código abaixo será executado em condições ideais, com o ambiente PHP e o PHPUnit devidamente configurados.

```
class Cobertura{
    public function calcular(float $valor, float $limite): float  {
        return min($valor, $limite);
    }
}


public function testCalculaCobertura(){


    __I__
    $resultado = $cobertura->calcular(80000, 100000);
    __II__
}
```

O método `calcular()` retorna o menor valor entre o valor da operação e o limite de cobertura estabelecido. Para verificar esse comportamento usando teste unitário, as lacunas **`I`** e **`II`** devem ser preenchidas, correta e respectivamente, com:

(A)
```
$cobertura = new Cobertura();
$this->assertEquals(80000, $resultado);
```

(B)
```
$cobertura = Cobertura();
$this->assertSame(80000.00, $resultado);
```

(C)
```
$Cobertura = new Cobertura;
$this->assertTrue($resultado === 80000);
```

(D)
```
$cobertura = new cobertura();
$this->assertEquals($resultado = 80000);
```

(E)
```
$cobertura = new Cobertura();
$this->assertTrue($resultado == 100000);
```

37. O sistema de uma Agência Brasileira Gestora de Fundos Garantidores possui um módulo responsável por calcular o valor de cobertura de operações garantidas. Para permitir a substituição da regra de cálculo sem alterar a classe responsável pelo processamento das operações, foi adotada uma arquitetura baseada em herança, polimorfismo, encapsulamento e injeção de dependências. Considere o código Java a seguir, que será executado em condições ideais.

```
interface RegraCobertura {
    double calcular(double saldo);
}

class RegraPadrao __I__ {
    public double calcular(double saldo) {
        return saldo * 0.80;
    }
}

class RegraEspecial __II__ {
    @Override
    public double calcular(double saldo) {
        return super.calcular(saldo) + 500.00;
    }
}

class OperacaoGarantida {
    private final RegraCobertura regra;

    public OperacaoGarantida(RegraCobertura regra) {
        __III__
    }

    public double cobertura(double saldo) {
        return regra.calcular(saldo);
    }
}

public class Main {
    public static void main(String[] args) {
        RegraCobertura regra = new RegraEspecial();
        OperacaoGarantida operacao = new OperacaoGarantida(regra);

        System.out.println("Valor da operação R$" + operacao.cobertura(10000.00));
    }
}
```

Para que o comportamento esperado seja preservado e a saída do programa mostre o valor da operação como R$ 8500.00 (oito mil e quinhentos reais), as lacunas **I**, **II** e **III** devem ser preenchidas, correta e respectivamente, com:

(A)
```
extends RegraCobertura
implements RegraPadrao
this.regra = regra;
```

(B)
```
implements RegraEspecial
extends RegraCobertura
this.regra = new RegraPadrao();
```

(C)
```
extends RegraCobertura
implements RegraCobertura
this.regra = new RegraPadrao();
```

(D)
```
implements RegraCobertura
extends RegraPadrao
this.regra = regra;
```

(E)
```
implements RegraCobertura
extends RegraPadrao
this.regra = new RegraPadrao();
```

38. Uma analista implementou um mecanismo para armazenar credenciais de usuários responsáveis pela análise de solicitações de garantia. O objetivo seria reduzir os riscos associados ao vazamento de senhas, seguindo boas práticas de desenvolvimento seguro. Considere o código Python a seguir que será executado em condições ideais.

```
import hashlib
import secrets


def cadastrar_usuario(usuario, senha):
    salt = secrets.token_hex(16)
    senha_hash = hashlib.sha256((salt + senha).encode()).hexdigest()


    return {
        "usuario": usuario,
        "salt": salt,
        "senha_hash": senha_hash
    }


def autenticar(registro, senha_informada):
    novo_hash = hashlib.sha256(
        (registro["salt"] + senha_informada).encode()
    ).hexdigest()


    return  __I__


registro = cadastrar_usuario("analista01", "SenhaForte2026!")


print(autenticar(registro, "SenhaForte2026!"))
print(autenticar(registro, "SenhaIncorreta"))
```

Considerando os princípios de desenvolvimento seguro e o funcionamento do processo de autenticação, a lacuna **I** do código deve ser preenchida com

(A) `novo_hash in registro["senha_hash"]`

O uso do `salt` é um mecanismo de proteção contra tentativas repetidas de autenticação previstas pela OWASP.

(B) `hashlib.sha256(senha_informada.encode()).hexdigest() == registro["senha_hash"]`

O `salt` armazenado no cadastro não influencia o SHA-256, pois este produz sempre resultados diferentes para uma senha.

(C) `novo_hash == registro["senha_hash"]`

O `salt` aleatório faz com que senhas iguais produzam *hashes* diferentes entre usuários distintos, dificultando ataques com tabelas pré-computadas.

(D) `registro["senha_hash"] == senha_informada`

Armazenar o *hash* permite comparar diretamente a senha em texto informado pelo usuário sem necessidade de novo processamento.

(E) `registro["salt"] == novo_hash`

A autenticação é realizada verificando se o valor aleatório gerado durante o cadastro corresponde ao *hash* calculado da senha informada.

39. Em uma Agência Brasileira Gestora de Fundos Garantidores, um microsserviço em JavaScript recebe eventos de solicitação de garantia. O objetivo é desacoplar o processamento do registro da operação, permitindo que outros componentes (auditoria, notificações e conformidade) reajam ao mesmo evento futuramente. O trecho de código a seguir será executado em condições ideais.

```
class EventBus {
  constructor() {
    this.handlers = {};
  }

  subscribe(event, handler) {
    this.handlers[event] ??= [];
    this.handlers[event].push(handler);
  }

  publish(event, payload) {
    (this.handlers[event] || []).forEach(h => h(payload));
  }
}

const bus = new EventBus();
const auditoria = [];

bus.subscribe("garantia.solicitada", dados => {
  auditoria.push(`AUD:${dados.id}`);
});

function registrarGarantia(id, valor) {
  const garantia = { id, valor };

  __I__

  return garantia;
}

registrarGarantia("FG-901", 800000);
console.log("Registros de auditoria processados:", auditoria);
```

Considerando o código JavaScript, a lacuna **I** deve ser preenchida, de forma a preservar o desacoplamento entre a regra de negócio e os consumidores do evento, com:

(A)
```
bus.publish("garantia.solicitada", {
  identificador: garantia.id,
  valor: garantia.valor
  });
```

(B)
```
bus.publish("garantia.solicitada", garantia.id);
```

(C)
```
bus.publish("garantia.solicitada", garantia);
```

(D)
```
bus.subscribe("garantia.solicitada", dados => {
   auditoria.push(`AUD:${dados.id}`);
  });
```

(E)
```
bus.publish("garantia.emitida", garantia);
```

40. A equipe de analistas de uma Agência Brasileira Gestora de Fundos Garantidores definiu que todas as chamadas externas deverão passar por um API Gateway. Determinadas operações, como consulta de saldo garantido, exigem resposta imediata, enquanto eventos como auditoria e atualização de indicadores podem ser processados posteriormente. Considere o seguinte trecho de código em Python (que será executado em condições ideais), responsável por encaminhar uma requisição recebida pelo *gateway* para um microsserviço interno.

```
import requests


def consultar_fundo(token, id_fundo):
    headers = {
        "Authorization": f"Bearer {token}"
    }


    resposta = requests.get(
        f"https://api-interna/fundos/{id_fundo}",
        headers=headers,
        timeout=3
    )


    return resposta.json()
```

Analisando a situação, o trecho de código e considerando a utilização de APIs REST, API Gateway, integração síncrona e assíncrona e segurança de APIs, um analista conclui corretamente que

(A) a consulta deve ser convertida para processamento assíncrono em fila, pois operações REST apresentam maior disponibilidade quando todas as respostas são desacopladas do fluxo de requisição e eliminam dependências temporais entre consumidores e provedores.

(B) a consulta pode permanecer síncrona por depender de resposta imediata ao consumidor, enquanto eventos secundários, como auditoria e atualização de métricas, podem ser publicados de forma assíncrona; o API Gateway continua responsável pela autenticação, pelas políticas de segurança e pelo controle do tráfego.

(C) o API Gateway deve encaminhar o *token* recebido diretamente para todos os microsserviços sem validação, preservando o princípio *end to end* da autenticação e reduzindo a sobrecarga de processamento em ambientes distribuídos de alta disponibilidade.

(D) a utilização de HTTPS torna desnecessários mecanismos adicionais de autenticação entre *gateway* e microsserviços, pois a confidencialidade do canal garante que chamadas REST sejam aceitas apenas por aplicações previamente autorizadas.

(E) a configuração de *timeout* na chamada HTTP engloba políticas de resiliência, como repetição controlada, *circuit breaker* e observabilidade, uma vez que o encerramento da conexão impede impactos em serviços dependentes.

Computação em Nuvem e Infraestrutura

41. Para modernizar o ecossistema de análise de dados e mitigar riscos operacionais no processamento de fundos garantidores, uma organização pretende implantar uma nova solução analítica em nuvem pública. A estratégia exige que a equipe de engenharia mantenha o controle sobre as aplicações e os dados analíticos, sem a necessidade de administrar o *hardware* físico, a camada de virtualização, o sistema operacional ou o ambiente de execução (*runtime*). Considerando o modelo de responsabilidade compartilhada e os modelos de serviço em computação em nuvem, o analista deve

(A) adotar o modelo IaaS, delegando ao provedor o gerenciamento do *hardware* físico, da virtualização e do sistema operacional, enquanto a equipe permanece responsável pelo ambiente de execução (*runtime*), pelas aplicações e pelos dados analíticos.

(B) contratar a solução no modelo PaaS, delegando ao provedor o gerenciamento do *hardware* físico, da virtualização, do sistema operacional e do ambiente de execução (*runtime*), enquanto a equipe permanece responsável pelas aplicações e pelos dados analíticos.

(C) contratar a solução no modelo PaaS, delegando ao provedor o gerenciamento do *hardware* físico, da virtualização e do sistema operacional, enquanto a equipe permanece responsável pelo ambiente de execução (*runtime*), pelas aplicações e pelos dados analíticos.

(D) adotar o modelo IaaS, mantendo sob responsabilidade da equipe o gerenciamento do sistema operacional, das aplicações e dos dados analíticos, enquanto o provedor gerencia o *hardware* físico, a virtualização e o ambiente de execução (*runtime*).

(E) contratar a solução no modelo PaaS, delegando ao provedor o gerenciamento do *hardware* físico, da virtualização, do sistema operacional, do ambiente de execução (*runtime*) e das aplicações, permanecendo com a equipe apenas a gestão dos dados analíticos.

42. Uma organização pretende contratar serviços de computação em nuvem para diferentes necessidades. Na primeira delas, deseja utilizar máquinas virtuais, sistemas operacionais e recursos de armazenamento e rede, mantendo sob sua responsabilidade a instalação e a administração dos sistemas operacionais e das aplicações. Na segunda, deseja concentrar-se no desenvolvimento e na execução de aplicações, deixando ao provedor a administração da infraestrutura subjacente. Na terceira, para usuários finais, pretende disponibilizar uma aplicação pronta para uso, sem que esses usuários precisem administrar a infraestrutura ou a plataforma que a sustenta.

A correta correspondência entre essas necessidades e os modelos de serviço de computação em nuvem é:

(A) SaaS para a primeira necessidade, IaaS para a segunda e PaaS para a terceira.

(B) PaaS para a primeira necessidade, SaaS para a segunda e IaaS para a terceira.

(C) IaaS para a primeira necessidade, SaaS para a segunda e PaaS para a terceira.

(D) PaaS para a primeira necessidade, IaaS para a segunda e SaaS para a terceira.

(E) IaaS para a primeira necessidade, PaaS para a segunda e SaaS para a terceira.

---

43. Para garantir resiliência e rápido restabelecimento na execução de microsserviços críticos de análise de risco, a infraestrutura deve combinar isolamento em nível do sistema operacional por meio de contêineres com alta disponibilidade sobre máquinas virtuais. A arquitetura exige:

I. Empacotamento em contêineres.

II. Orquestração automatizada para replicação e recuperação de falhas.

III. Segmentação lógica da comunicação entre os microsserviços.

Nesse contexto, o profissional de infraestrutura deve

(A) empacotar os microsserviços com Docker e implantá-los em máquinas virtuais independentes, mantendo a alta disponibilidade por meio de reinicialização automática do sistema operacional.

(B) empacotar os microsserviços com Docker e orquestrá-los por Kubernetes sobre máquinas virtuais em alta disponibilidade, utilizando a rede padrão do *host*, com a especificação SIN para comunicação entre os *pods*.

(C) empacotar os microsserviços com Docker, orquestrá-los por meio de *pods* gerenciados pelo Kubernetes sobre máquinas virtuais organizadas em *cluster* de alta disponibilidade e utilizar uma solução compatível com a especificação Container Network Interface (CNI) para prover a comunicação entre os *pods* e os serviços do *cluster*.

(D) implantar os microsserviços diretamente em máquinas virtuais dedicadas, utilizando o Kubernetes para administrar a infraestrutura e empregar contêineres NFS na execução das aplicações.

(E) empacotar os microsserviços com Docker e orquestrá-los por Kubernetes sobre máquinas virtuais em alta disponibilidade, atribuindo ao Docker a responsabilidade pelo balanceamento de carga e pela recuperação automática de falhas do *cluster*.

---

44. Com a finalidade de padronizar a infraestrutura de servidores e garantir alta disponibilidade na sustentação de ambientes analíticos e de arquivos corporativos, uma organização precisa integrar ambientes Windows e Linux. A solução deve atender simultaneamente aos seguintes requisitos:

I. Autenticação centralizada para usuários de estações Windows e servidores Linux.

II. Compartilhamento corporativo de arquivos de forma distribuída.

III. Alta disponibilidade dos serviços de armazenamento por meio de *clustering*.

Nesse contexto, o analista de infraestrutura deve

(A) implementar um domínio Active Directory para autenticação unificada, integrar os servidores Linux ao domínio por meio de SSSD/Samba e disponibilizar os compartilhamentos corporativos via SMB/CIFS integrados ao DFS, mantendo os servidores de arquivos independentes e mecanismo de *clustering* ADFS.

(B) implementar um domínio Active Directory para autenticação unificada, integrar os servidores Linux ao domínio por meio de SSSD/Samba, disponibilizar os compartilhamentos corporativos via SMB/CIFS integrados ao DFS e estruturar um *cluster* Linux com Pacemaker/Corosync, utilizando NFSv2 como protocolo de armazenamento compartilhado.

(C) implementar um domínio Active Directory para autenticação das estações Windows, manter um serviço OpenLDAP independente para autenticação dos servidores Linux, disponibilizar compartilhamentos corporativos via SMB/CIFS integrados ao DFS e estruturar um *cluster* Linux com Pacemaker/Corosync para garantir alta disponibilidade dos serviços de armazenamento.

(D) implementar um domínio Active Directory para autenticação unificada, integrar os servidores Linux ao domínio por meio de SSSD/Samba, disponibilizar compartilhamentos corporativos via SMB/CIFS integrados ao DFS e estruturar um *cluster* Linux com Pacemaker/Corosync para garantir alta disponibilidade dos serviços de armazenamento compartilhado, utilizando o protocolo NFSv4.

(E) implementar um domínio Active Directory para autenticação unificada, integrar os servidores Linux ao domínio por meio de SSSD/Samba, disponibilizar compartilhamentos corporativos via NFSv4 e estruturar *clusters* Linux com Pacemaker/Corosync, usando SMB/CIFS e DFS/*LINK* para o acesso aos compartilhamentos corporativos.

45. Um analista de infraestrutura precisa estruturar a sustentação de um ambiente analítico que exige elevado desempenho de operações de entrada e saída (I/O), elevada disponibilidade diante de falhas de discos e uma estratégia de *backup* que reduza a janela diária de cópia, permitindo rápida recuperação dos dados sem a necessidade de restaurar toda a cadeia de *backups*. Para atender a esses requisitos, a solução técnica deve utilizar armazenamento

(A) em rede SAN com arranjo RAID 10 para o ambiente analítico, executando *backup* completo semanal e *backups* diferenciais diários, com utilização complementar de *snapshots* para recuperação operacional rápida.

(B) em rede NAS com arranjo RAID 5 para o ambiente analítico, executando *backup* completo semanal e *backups* diferenciais diários, complementados por *snapshots* para recuperação operacional rápida.

(C) DAS com arranjo RAID 10 para o ambiente analítico, executando *backup* completo semanal e *backups* diferenciais diários, complementados por *snapshots* para recuperação operacional rápida.

(D) em rede SAN com arranjo RAID 10 para o ambiente analítico, executando *backups* incrementais diários, com a realização periódica de RECOVERY/NAS.

(E) em rede NAS com arranjo RAID 10 para o ambiente analítico, executando *backup* completo semanal e *backups* diferenciais diários, com utilização complementar de snapshots para recuperação operacional rápida.

DevOps, CI/CD e Automação

46. Para automatizar a construção, validação e disponibilização de uma aplicação analítica distribuída executada em um ambiente baseado em contêineres orquestrados por Kubernetes, a equipe técnica deve estruturar uma esteira de CI/CD que contemple:

I. Compilação automática do código;

II. Execução de testes automatizados a cada integração;

III. Análise estática de código e segurança;

IV. Publicação versionada dos artefatos em um *registry*;

V. Implantação automatizada em ambiente de homologação;

VI. Coleta de *logs* e métricas da execução da *pipeline*.

Nesse contexto, o analista deve estruturar o

(A) versionamento em Git, executar automaticamente *build*, testes e análise estática de código, publicar os artefatos em um *registry* corporativo e realizar a implantação manual em Kubernetes por meio de comandos kubectl.

(B) versionamento em Git, executar automaticamente *build* e testes, publicar os artefatos em *registry* corporativo, implantar automaticamente em Kubernetes por meio de Helm e registrar os *logs* da *pipeline*, mantendo a análise estática de segurança como atividade controlada pelo gestor operacional.

(C) versionamento em Git, executar automaticamente *build*, testes e análise estática, implantar automaticamente em Kubernetes por meio de Helm e armazenar os artefatos diretamente no sistema de arquivos dos nós do *cluster*, com a utilização de um *registry*/GLAB na esteira regressiva.

(D) controle de versão em Git, integrar o GitLab CI/CD com *runners* para *build*, testes automatizados e análise estática, publicar as imagens OCI em um *registry* corporativo, automatizar a implantação em Kubernetes por meio do Helm e monitorar a *pipeline* por *logs* e métricas.

(E) controle de versão em Git, integrar o GitLab CI/CD com *runners* para *build*, testes automatizados e análise estática, publicar os artefatos em um *registry* corporativo e automatizar a implantação diretamente por SSH nos nós do *cluste*r Kubernetes.

---

47. Na sustentação das plataformas de análise de risco e concessão de garantias operadas por uma agência de fundos garantidores, uma equipe de DevSecOps precisa incorporar controles de segurança diretamente à esteira de CI/CD para reduzir vulnerabilidades sem comprometer a frequência das entregas. A solução deve identificar vulnerabilidades no código-fonte, dependências de terceiros, Dockerfiles, imagens de contêiner e infraestrutura como código (IaC), executando verificações automatizadas ao longo da *pipeline* antes da implantação em produção. Nesse contexto, o analista deve executar, automaticamente, a análise estática de segurança (SAST), a análise de dependências (SCA), a validação de Dockerfiles, o escaneamento de imagens de contêiner

(A) e a verificação de arquivos IaC em *pipelines* disparadas por *push* ou *merge request*, realizando testes dinâmicos (DAST) em ambiente temporário antes da implantação em produção.

(B) com Hadolint e a verificação de arquivos IaC em *pipelines* disparadas por *push* ou *merge request*, realizando testes dinâmicos (DAST) em ambiente temporário antes da implantação em produção.

(C) e a verificação de arquivos IaC, realizando os testes dinâmicos (DAST) diretamente sobre as imagens de contêiner antes de sua execução.

(D) e a verificação de arquivos IaC via *push,* após a implantação em produção, executando os testes dinâmicos (DAST) em ambiente temporário antes da publicação da aplicação.

(E) e a verificação de arquivos IaC em *pipelines* disparadas por *push* ou *merge request*, realizando testes dinâmicos (DAST) posteriores à entrada da aplicação em produção.

48. Uma equipe de infraestrutura precisa padronizar automaticamente a configuração de servidores já provisionados que compõem um ambiente analítico de dados. A solução deve utilizar Infraestrutura como Código (IaC), permitindo versionamento, parametrização e execução automatizada das configurações sem necessidade de acesso manual aos servidores.

A arquitetura deve atender simultaneamente aos seguintes requisitos:

I. Versionar as definições de infraestrutura em plataforma colaborativa.

II. Parametrizar a configuração por meio de inventários, variáveis e *templates*.

III. Aplicar as configurações utilizando módulos orientados ao estado desejado.

IV. Executar automaticamente as configurações por meio de *pipelines* a partir de um nó de controle.

Nesse contexto, o analista deve versionar os *playbooks* em um repositório Git, utilizar inventários, variáveis e *templates* do Ansible,

(A) parametrizar os servidores, empregando módulos orientados ao estado desejado, e executar automaticamente as configurações por meio de *pipelines*, utilizando agentes residentes instalados em todos os servidores de destino.

(B) substituir os módulos orientados ao estado desejado por *scripts Bash* executados sequencialmente, mantendo a execução automatizada por meio de *pipelines* a partir de um nó de controle.

(C) empregar módulos orientados ao estado desejado, executar automaticamente as configurações por meio de *pipelines* a partir de um nó de controle e realizar a configuração dos servidores sem necessidade de agentes residentes.

(D) empregar módulos orientados ao estado desejado e executar automaticamente as configurações por meio de *pipelines*, utilizando *soft commands ad hoc* do Ansible para o gerenciamento contínuo da configuração dos servidores.

(E) empregar módulos orientados ao estado desejado, executar automaticamente as configurações por meio de *pipelines* e forçar a alteração de todos os recursos em cada execução, independentemente do estado atual dos servidores.

---

49. Considere um ambiente que disponha de Bash e PowerShell 7 (PowerShell Core). Um sistema parceiro disponibiliza diariamente arquivos em formato JSON contendo, entre outros, os atributos `fundo_id`, `codigo`, `valor` e `vigente`.

Um analista precisa implementar uma rotina automatizada para:

I. Realizar o *parsing* do arquivo JSON;

II. Extrair os atributos `fundo_id`, `codigo` e `valor`;

III. Selecionar apenas as garantias vigentes;

IV. Exportar o resultado para um arquivo CSV utilizando exclusivamente os recursos disponíveis no ambiente de execução escolhido, sem recorrer a linguagens adicionais.

Nessas condições, a implementação correta consiste em

(A) desenvolver a rotina em Bash, utilizando `jq` para realizar o *parsing* do arquivo, `cut` para projetar os atributos desejados e gerar o arquivo CSV.

(B) desenvolver a rotina em Bash, utilizando `jq` para realizar o *parsing* do arquivo, `grep` para filtrar os registros vigentes e `awk` para converter os objetos JSON em CSV.

(C) implementar a rotina em PowerShell 7, utilizando `ConvertFrom-Json`, `Where-Object`, `Select-Object` e `Export-Csv` para processar os registros vigentes e gerar o arquivo CSV.

(D) implementar a rotina em PowerShell 7, utilizando `Import-Csv` para carregar o arquivo JSON, `Select-String` para localizar os atributos desejados e `Export-Csv` para gerar o arquivo de saída.

(E) implementar a rotina em PowerShell 7, utilizando `ConvertFrom-Json`, `Where-Object` e `Out-File` para filtrar os registros vigentes e gravar o resultado em formato CSV.

50. Considere que o arquivo CSV encontra-se previamente ordenado por `fundo_id` e `data_ref`, podendo registros de um mesmo fundo estar distribuídos entre diferentes lotes (*chunks*) de leitura. Um analista precisa calcular, para cada fundo, a média móvel das três últimas exposições, preservando a continuidade do cálculo entre os lotes e gravando os resultados em uma tabela SQLite. Para isso, é necessário utilizar leitura em *chunks*, manter entre os lotes apenas o histórico mínimo necessário para o cálculo da média móvel entre os lotes e persistir os resultados sem sobrescrever os registros já processados.

Analise o código a seguir:

```
import sqlite3
import pandas as pd

historico = {}

with sqlite3.connect("metricas_operacionais.db") as conn:

    chunks = pd.read_csv(
        "exposicao_operacoes.csv",
        chunksize=10000,
        parse_dates=["data_ref"]
    )

    for chunk in chunks:

        resultados = []

        for fundo_id, grupo in chunk.groupby("fundo_id", sort=False):

            grupo = grupo.sort_values("data_ref").copy()

            anteriores = historico.get(
                fundo_id,
                pd.Series(dtype="float64")
            )

            valores = pd.concat(
                [
                    anteriores,
                    grupo["valor_exposto"].reset_index(drop=True)
                ],
                ignore_index=True
            )

            medias = valores.rolling(
                window=3,
                min_periods=1
            ).mean()

            grupo["media_movel"] = (
                medias.iloc[len(anteriores):].to_numpy()
            )

            historico[fundo_id] = (
                valores.tail(2).reset_index(drop=True)
            )

            resultados.append(grupo)

        resultado = pd.concat(
            resultados,
            ignore_index=True
        )

        resultado.to_sql(
            "tb_metricas_consolidadas",
            con=conn,
            if_exists="append",
            index=False
        )
```

A implementação apresentada está correta porque

(A) preserva a continuidade da média móvel entre os *chunks* ao armazenar todas as observações previamente processadas de cada fundo, recalculando integralmente a série antes da gravação dos resultados na tabela SQLite.

(B) preserva a continuidade da média móvel ao manter, para cada fundo, apenas as duas últimas observações necessárias para a janela deslizante, calculando as médias considerando o histórico preservado e gravando os resultados incrementalmente por meio de `DataFrame.to_sql(..., if_exists="append")`

(C) utiliza corretamente a leitura em *chunks*, porém deveria substituir `DataFrame.to_sql()` por comandos SQL nativos da biblioteca sqlite3, pois o método do pandas não permite inserções incrementais em tabelas existentes.

(D) preserva corretamente a continuidade da média móvel entre os lotes, mas deveria substituir `if_exists="append"` por `if_exists="replace"` para evitar inconsistências decorrentes da gravação parcial dos resultados.

(E) garante a continuidade da média móvel por utilizar `groupby(sort=False)`, que preserva automaticamente a ordenação cronológica dos registros de cada fundo entre diferentes lotes de leitura.

Análise de Dados, Aprendizado de Máquina e Inteligência Artificial

51. Uma Agência Brasileira Gestora de Fundos Garantidores desenvolveu um modelo de aprendizado supervisionado para estimar o valor recuperado (em milhares de reais) de operações inadimplentes com base no número de garantias válidas apresentadas. Após o treinamento com dados históricos rotulados, o modelo resultou na equação de regressão linear `Y = 15X + 20`, em que `Y` representa o valor recuperado estimado, `X` representa o número de garantias válidas, `15` é o coeficiente angular e `20` é o intercepto. Em condições ideais, nesse caso,

(A) o intercepto indica que, para cada garantia válida adicional, o valor recuperado estimado aumenta 20 mil reais, enquanto o coeficiente angular representa 15 mil reais.

(B) como o modelo foi treinado com dados históricos, o valor previsto para uma operação com `X = 10` garantias válidas corresponde ao valor que será recuperado na operação analisada.

(C) o intercepto representa o valor previsto quando `X = 1`, enquanto o coeficiente angular determina o número mínimo de garantias para que a estimativa seja positiva.

(D) o treinamento da regressão linear consiste em ajustar o coeficiente angular, mantendo o intercepto constante para preservar a proporcionalidade entre as variáveis.

(E) para uma operação com `X = 8` garantias válidas, a estimativa do modelo é de recuperação de 140 mil reais, sendo os coeficientes ajustados durante o treinamento para minimizar a soma dos erros quadráticos entre os valores observados e os previstos.

---

52. Uma Agência Brasileira Gestora de Fundos Garantidores importou para o Power BI os dados consolidados por setor econômico apresentados no quadro a seguir:

Setor	Valor recuperado (R$ milhões)	Valor honrado (R$ milhões)
Comércio	18	45
Indústria	27	60
Serviços	15	24
Agronegócio	30	81

A equipe de analistas pretende criar um painel para comparar a taxa de recuperação de cada setor, definida como o quociente entre o valor recuperado e o valor honrado, além de identificar rapidamente o setor com melhor desempenho. Considerando esse cenário, o setor de

(A) Comércio apresenta a maior taxa de recuperação, igual a 40%, e um gráfico de pizza é o mais indicado para comparar esse indicador entre os setores.

(B) Serviços apresenta taxa de recuperação inferior a 60% e um gráfico de linhas é o mais apropriado para comparar as taxas entre os setores.

(C) Indústria apresenta taxa de recuperação de 45% e um gráfico de área facilita a identificação deste setor com maior desempenho.

(D) Agronegócio apresenta taxa de recuperação acima de 40% e um gráfico de dispersão é o mais indicado para comparar as taxas entre categorias.

(E) Serviços apresenta a maior taxa de recuperação, igual a 62,5%, e um gráfico de barras permite comparar de forma mais adequada esse indicador entre os setores.

53. Um *pipeline* de MLOps foi implementado em uma agência para apoiar a previsão da recuperação de operações de crédito inadimplentes utilizando uma árvore de decisão. Considere as etapas do *pipeline* que serão executadas em condições ideais.

I. Uma operação de R$ 1 milhão, pertencente ao setor de agronegócio e com 6 garantias válidas, é enviada para consulta. O sistema retorna a classificação “alto”, indicando recuperação esperada acima de R$ 350 mil.

II. O sistema identifica que, nos últimos meses, operações do setor de serviços passaram a apresentar valores recuperados superiores aos previstos pelo modelo, gerando um alerta para revisão do desempenho.

III. São incorporadas 5 mil operações inadimplentes contendo atributos como número de garantias válidas, valor da operação, setor econômico e histórico de pagamentos. Em seguida, os atributos são tratados para formar variáveis categóricas e numéricas adequadas ao treinamento.

IV. O algoritmo passa a entender que operações com quatro ou mais garantias no setor indústria tendem a apresentar recuperação elevada, enquanto operações com até duas garantias no setor de serviços tendem a apresentar recuperação baixa.

V. Uma operação com três garantias válidas, setor comércio e valor honrado de R$ 800 mil recebe a classificação “médio”, correspondente à faixa entre R$ 150 mil e R$ 250 mil. Posteriormente verifica-se que o valor efetivamente recuperado foi de R$ 200 mil.

Considerando as etapas do *pipeline* de MLOps e os valores apresentados, conclui-se que a etapa I corresponde

(A) à Implantação; a II ao Monitoramento; a III à Coleta e preparação dos dados; a IV ao Treinamento; a V à Validação. Os valores entre R$ 150 mil e R$ 250 mil representam a faixa prevista pelo modelo para a recuperação da operação, enquanto R$ 200 mil corresponde ao valor efetivamente recuperado, utilizado para verificar a aderência da previsão.

(B) à Validação; a II ao Retreinamento; a III ao Treinamento; a IV à Coleta e preparação dos dados; a V à Implantação. O valor de R$ 200 mil representa o limite superior da faixa prevista pelo modelo, enquanto os valores de R$ 150 mil e R$ 250 mil correspondem aos resultados observados após a implantação.

(C) ao Retreinamento; a II à Validação; a III ao Treinamento; a IV à Implantação; a V ao Monitoramento. Os valores entre R$ 150 mil e R$ 250 mil constituem os limites definidos durante o treinamento da árvore de decisão e o valor de R$ 200 mil representa o parâmetro utilizado para separar as classes de recuperação.

(D) ao Monitoramento; a II à Validação; a III à Coleta e preparação dos dados; a IV à Implantação; a V ao Treinamento. O valor acima de R$ 350 mil corresponde ao resultado efetivamente recuperado na operação consultada por uma API, enquanto a classificação “alto” expressa a confiança do modelo na previsão.

(E) ao Retreinamento; a II ao Monitoramento; a III à Implantação; a IV ao Treinamento; a V à Validação. O intervalo entre R$ 150 mil e R$ 250 mil corresponde aos valores efetivamente recuperados em operações semelhantes durante o treinamento, ao passo que R$ 200 mil representa a média histórica utilizada pela árvore de decisão para classificar novas operações.

---

54. Uma analista avaliou a relação entre o número de operações garantidas (X) e o valor das provisões constituídas (Y), obtendo uma correlação linear de 0,88 e ajustando um modelo de regressão linear. Em determinado período, o modelo estimou provisão de R$ 2,4 milhões para um conjunto de operações, enquanto o valor efetivamente observado foi de R$ 2,6 milhões. Considerando os conceitos de estatística descritiva, as distribuições de probabilidade, a correlação e a regressão, é correto afirmar:

(A) A diferença de R$ 0,2 milhão comprova que a correlação entre as variáveis é fraca e que o modelo de regressão deve ser descartado e substituído por outro mais robusto.

(B) Como a correlação é positiva, isso indica que valores altos de X estão sempre associados a valores altos de Y e o modelo produzirá estimativas semelhantes aos valores observados em todas as situações analisadas.

(C) Se o modelo for corrigido e a correlação linear resultar em zero, isso indicará uma correlação perfeita entre X e Y.

(D) A diferença entre o valor estimado e o observado corresponde a um resíduo da regressão, sendo compatível com um modelo que apresenta forte correlação entre as variáveis.

(E) O coeficiente de correlação de 0,88 representa a probabilidade de que a estimativa do modelo coincida com o valor observado em uma nova análise.

---

55. Uma Agência Brasileira Gestora de Fundos Garantidores monitora mensalmente a quantidade de garantias honradas por setor econômico. Após a validação dos dados e a análise exploratória de 48 meses de histórico, foram observados redução gradual da variabilidade, crescimento consistente da média mensal e picos recorrentes nos mesmos meses de cada ano. Os resultados indicam que

(A) houve redução da dispersão dos dados, permitindo concluir que os picos recorrentes não influenciam mais o comportamento da série ao longo do tempo.

(B) há coexistência de tendência de crescimento e componente sazonal, devendo ambos ser considerados na interpretação dos padrões identificados na série histórica.

(C) a série apresenta tendência crescente, enquanto os picos recorrentes decorrem de oscilações aleatórias que tendem a desaparecer com a ampliação da amostra analisada.

(D) a repetição dos picos em determinados meses caracteriza estabilidade do processo, evidenciando a precisão das análises exploratórias sobre os dados coletados.

(E) há diminuição da variabilidade, sugerindo que o comportamento futuro da série deve seguir padrão semelhante ao histórico observado.

Gestão de TI

56. Considere hipoteticamente que, para reestruturar a governança de tecnologia e alinhar a prestação de serviços às metas institucionais da ABGF, um Analista de TI foi encarregado de implementar um modelo integrado que conecte objetivos institucionais, indicadores e mitigação de ameaças.

Diante do cenário, a conduta técnica adequada para garantir o alinhamento estratégico e a continuidade dos negócios é

(A) mapear os objetivos de TI no modelo COBIT 2019, definindo indicadores-chave de desempenho (KPIs) voltados à infraestrutura tecnológica, associados aos objetivos operacionais da organização, de modo a evitar interferências da gestão corporativa de riscos.

(B) desdobrar os objetivos de negócio em metas de TI conforme o COBIT 2019, vincular os indicadores-chave de desempenho (KPIs) aos objetivos estratégicos institucionais e integrar a gestão dos riscos de TI à gestão corporativa de riscos da organização.

(C) adotar o COBIT 2019 como estrutura de governança, mensurar o desempenho por meio de KPIs predominantemente estratégicas de infraestrutura e incluir a gestão dos riscos de TI no plano anual de auditoria interna da organização.

(D) estruturar o alinhamento estratégico com base no *framework* COBIT 2019, utilizar indicadores de desempenho voltados ao controle de riscos táticos, tratando a gestão dos riscos por meio de uma matriz de impacto vinculada ao processo de governança corporativa.

(E) alinhar a TI ao negócio utilizando indicadores financeiros relacionados aos custos de infraestrutura e licenciamento, delegando a gestão dos riscos de TI aos gestores dos sistemas, com integração ao processo operacional de governança.

57. Uma organização identificou recorrentes indisponibilidades em um serviço corporativo. Para restabelecer rapidamente os serviços, eliminar as causas das falhas e manter a qualidade operacional conforme o ITIL 4, o Analista de TI deve restaurar o serviço pelo gerenciamento de incidentes, bem como

(A) tratar as causas pelo gerenciamento de problemas, submeter alterações ao *Change Enablement*, manter atualizadas as informações de configuração, acompanhar os SLAs e promover a melhoria contínua.

(B) tratar os incidentes pelo gerenciamento dos SLAs, registrar as mudanças no gerenciamento de configuração e utilizar o registro dos problemas para propor alterações na infraestrutura orientadas pelo processo *Change Enablement*.

(C) encaminhar os incidentes diretamente ao *Change Enablement*, atualizar a configuração após as mudanças, identificar as causas das falhas na melhoria contínua e alterar os SLAs incompatíveis.

(D) centralizar o tratamento das indisponibilidades no gerenciamento de configuração, aplicar alterações corretivas durante a restauração do serviço, utilizar os SLAs para identificar as causas das falhas e promover a melhoria contínua.

(E) registrar os incidentes, atribuir a análise das causas ao gerenciamento de níveis de serviço, atualizar a configuração após as mudanças, validar a restauração por meio da melhoria contínua e propor mudanças na infraestrutura.

58. Uma organização pretende alinhar a governança de TI aos objetivos do negócio e aperfeiçoar a gestão dos serviços. A conduta técnica mais adequada é

(A) tratar incidentes usando a matriz RACI do COBIT 2019 e alinhar objetivos por indicadores operacionais e funcionalmente aderentes à ITIL v4.

(B) vincular mudanças ao gerenciamento de configuração e definir KPIs pela gestão de problemas, de acordo com as boas práticas de gestão de incidentes do COBIT 2019.

(C) centralizar a governança no ITIL v4 e tratar riscos pela gestão de incidentes do COBIT 2019.

(D) desdobrar objetivos pelo COBIT 2019, gerenciar serviços pelo ITIL v4 e acompanhar resultados por KPIs e melhoria contínua.

(E) definir KPIs pela gestão de configuração e alinhar objetivos após a resolução dos incidentes. As matrizes de incidentes do ITIL V4 e do COBIT 2010 devem ser equivalentes.

59. A equipe de analistas de uma organização estuda a aplicação do COBIT 2019 como solução para resolver problemas de tecnologia no âmbito corporativo, levantados em recente diagnóstico. De acordo com o referido *framework*, a solução mais adequada para fortalecer a governança em Ti é

(A) definir KPIs pelos domínios de governança e adequar os objetivos estratégicos a partir dos recursos de TI.

(B) alinhar os recursos de TI aos domínios de controle e governança e estabelecer os objetivos estratégicos considerando também a gestão dos riscos operacionais.

(C) desdobrar os objetivos corporativos em objetivos de governança e gestão, utilizar os recursos de TI para apoiá-los e monitorar os domínios de controle.

(D) desdobrar os domínios de controle a partir dos KPIs e definir os objetivos estratégicos conforme o modelo de governança estabelecido no Processo COBIT 2019 – EDM (Avaliar, Dirigir e Mensurar).

(E) priorizar os recursos de TI, estabelecer os domínios de controle e revisar os objetivos de governança conforme os indicadores operacionais do Processo COBIT 2019 (Avaliar, Planejar e Organizar).

60. Uma Agência Gestora de Fundos Garantidores pretende aprimorar a gestão de projetos de TI. Para integrar práticas do PMBOK, Scrum e Kanban, é mais adequado

(A) organizar o projeto pelos grupos de processos do PMBOK, distribuir os recursos de TI usando o Kanban e utilizar o Scrum para gerir a performance dos processos.

(B) planejar o projeto conforme as áreas de conhecimento do PMBOK, utilizar o Kanban para definir as atividades e empregar o Scrum para atender rapidamente as entregas.

(C) estruturar o cronograma pelo PMBOK, utilizar o Scrum para controlar o fluxo contínuo e aplicar o Kanban para realizar as reuniões de retrospectiva de melhoria contínua.

(D) integrar os grupos de processos do PMBOK ao Scrum, utilizar o Kanban para melhorar os papéis da equipe e acompanhar os riscos durante as *sprints* mensais.

(E) integrar os grupos de processos do PMBOK ao gerenciamento do projeto, utilizar o Scrum para o desenvolvimento iterativo e incremental e aplicar o Kanban para visualizar e otimizar o fluxo de trabalho.

DISCURSIVA-REDAÇÃO

Instruções Gerais: *Conforme o Edital de Abertura de Inscrições, Capítulo 12. Da Prova Discursiva-Redação, itens: 12.4 Na Prova Discursiva-Redação, o candidato deve produzir um texto dissertativo-argumentativo autoral, coeso e coerente, empregando a norma-padrão da língua portuguesa, a partir de proposta única sobre assunto de interesse geral não atrelado necessariamente ao Conteúdo Programático de Conhecimentos Específicos referido no presente Edital.* [...] *12.10 O candidato deverá atentar para a folha destinada ao rascunho e a folha destinada à resposta definitiva, a fim de que não seja prejudicado. A folha para a resposta definitiva será a única válida para a avaliação da Prova Discursiva-Redação. 12.11 Na Prova Discursiva-Redação, deverão ser rigorosamente observados o limite mínimo de 20 (vinte) e máximo de 30 (trinta) linhas sob pena de perda de pontos a serem atribuídos à Redação.* [...] *12.13 A Prova Discursiva-Redação terá caráter eliminatório e classificatório e será avaliada na escala de 0 (zero) a 100,00 (cem) pontos. 12.14 Para todos os candidatos, serão considerados habilitados os candidatos que obtiverem* ***nota igual ou superior a 60,00 (sessenta)****.*

TEXTO I

As boas práticas de governança corporativa são compostas por 4 princípios básicos, que buscam aumentar o valor econômico da empresa e promover uma gestão de qualidade:

- ***Transparência*** *– deve-se disponibilizar informações sobre a organização, não apenas relacionadas ao desempenho econômico-financeiro, como também dos demais fatores que fazem parte da sua gestão e que colaboram para um ganho de valor do negócio;*
- ***Equidade*** *– é o tratamento justo e isonômico de todos os sócios e demais partes interessadas, considerando seus direitos, deveres, necessidades, interesses e expectativas;*
- ***Prestação de contas (accountability)*** *– feita de forma clara, concisa, compreensível e tempestiva, assumindo suas responsabilidades e possíveis consequências de seus atos;*
- ***Responsabilidade corporativa*** *– zela pelo sistema e ambiente da empresa, levando em consideração o capital intelectual, financeiro, social, manufaturado, reputacional, humano, ambiental e social no curto, médio e longo prazos.*

(Disponível em: **https://www.insper.edu.br/pt/conteudos/gestao-e-negocios/entenda-o-conceito-de-governanca-corporativa-e-seus-beneficios**. Adaptado)

TEXTO II

A integração de sistemas de Inteligência Artificial na governança corporativa está emergindo como uma tendência transformadora no cenário empresarial contemporâneo. Com sua capacidade de analisar grandes volumes de dados e automatizar processos complexos, a IA oferece oportunidades sem precedentes para aprimorar a eficiência, a transparência e a tomada de decisões das organizações no âmbito da governança corporativa, reforçando o caráter de desenvolvimento exponencial da tecnologia, fomentado pelos desdobramentos da quarta revolução industrial.

Considerando sua potencialidade de ser empregada de múltiplas formas em uma corporação e seus benefícios à atividade da instituição, verifica-se também a necessidade de refletir acerca dos possíveis desdobramentos éticos e riscos quanto à aplicação de IA, de forma que sejam seguidas boas práticas de governança.

(Adaptado de: A integração Da Inteligência artificial na governança corporativa: Enfoque Ético E Regulatório. Brenda Dutra Franco; Caroline Da Rosa Pinheiro; Larissa Almeida Del Lhano. Disponível em: **Revista de Direito, Governança e Novas Tecnologias | e-ISSN: 2526-0049 | XXXI Congresso Nacional de Brasília | v. 10 | n. 2 | p. 22 – 44 | Jan/Jul. 2025**)

A partir do que se afirma em **I** e **II**, escreva um texto dissertativo-argumentativo sobre o tema:

Inteligência artificial na governança corporativa: eficiência e responsabilidade.

01	
02	
03	
04	
05	
06	
07	
08	
09	
10	
11	

RASCUNHO

12	
13	
14	
15	
16	
17	
18	
19	
20	
21	
22	
23	
24	
25	
26	
27	
28	
29	
30	

RASCUNHO

NÃO ESCREVA NESTE ESPAÇO