Controladoria Geral do Estado de São Paulo

TARDE

AUDITOR ESTADUAL DE CONTROLE

TECNOLOGIA DA INFORMAÇÃO

PROVA TIPO 4

SUA PROVA

- Além deste caderno de questões contendo **60 (sessenta)** questões objetivas e **1 (uma)** questão discursiva, você receberá do fiscal de sala o cartão de respostas e a folha de textos definitivos.
- As questões objetivas têm 5 (cinco) opções de resposta (A, B, C, D e E) e somente uma delas está correta.

TEMPO

- **4 (quatro) horas e 30 (trinta) minutos** é o tempo disponível para a realização da prova, já incluídos a marcação do cartão de respostas e o texto definitivo da questão discursiva.
- **2 (duas) horas** após o início da prova, é possível retirar-se da sala, sem levar o caderno de questões nem qualquer tipo de anotação de suas respostas.
- **30 (trinta) minutos** antes do término do período de prova, é possível retirar-se da sala **levando o caderno de questões**.

NÃO SERÁ PERMITIDO

- Qualquer tipo de comunicação entre os candidatos durante a aplicação da prova.
- Usar o sanitário ao término da prova, após deixar a sala.
- Anotar informações relativas às respostas em qualquer outro meio que não seja este caderno de questões.

INFORMAÇÕES GERAIS

- Verifique se este caderno de questões está completo e sem falhas de impressão. Caso contrário, **notifique imediatamente o fiscal da sala**, para que sejam tomadas as devidas providências.
- No cartão de respostas e na folha de textos definitivos, confira seus dados pessoais, especialmente nome, número de inscrição e documento de identidade, e leia atentamente as instruções de preenchimento.
- **Use somente caneta esferográfica, fabricada em material transparente, com tinta preta ou azul**.
- Assine seu nome apenas no espaço reservado no cartão de respostas e na folha de textos definitivos.
- Confira o programa, a cor e o tipo do seu caderno de questões. Caso tenha recebido caderno de questões com programa ou tipo diferente do impresso em seu cartão de respostas e em sua folha de textos definitivos, o fiscal deve ser **obrigatoriamente** informado para o devido registro na ata da sala.
- O preenchimento das respostas é de sua responsabilidade e não será permitida a substituição do cartão de respostas ou da folha de textos definitivos em caso de erro cometido por você.
- Para fins de avaliação, serão levadas em consideração apenas as marcações realizadas no cartão de respostas e o texto redigido na folha de textos definitivos.
- Os candidatos serão submetidos ao sistema de detecção de metais quando do ingresso e da saída de sanitários durante a realização das provas.

Boa prova!

FGV CONHECIMENTO

Conhecimentos Específicos
Segurança da Informação

1

Sobre as categorias de soluções de proteção, no contexto de segurança em ambientes *cloud-native*, avalie as afirmativas a seguir.

I. CWPP (*Cloud Workload Protection Platform*) é responsável pela análise de vulnerabilidades em imagens de contêineres armazenadas em registries e pelo escaneamento de código de infraestrutura (IaC) antes do *deployment*, não provendo proteção durante a execução (*runtime*) das *workloads*.

II. CSPM (*Cloud Security Posture Management*) identifica e corrige configurações inadequadas de recursos *cloud* através de avaliação contínua contra *benchmarks* de segurança e frameworks de *compliance*, focando em postura de segurança e *misconfigurations* como *buckets* públicos, criptografia desabilitada e *security groups* permissivos.

III. CNAPP (*Cloud Native Application Protection Platform*) unifica funcionalidades de CSPM e CWPP em uma plataforma única, adicionando capacidades como análise de IaC, segurança de APIs, CIEM (*Cloud Infrastructure Entitlement Management*) e correlação de eventos através do ciclo de vida completo de aplicações *cloud-native.*

Está correto o que se afirma em

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

2

Um *Security Operations Center (*SOC) está operando uma solução SIEM (*Security Information and Event Management*) que recebe logs de múltiplas fontes:

- *Firewall* de perímetro (5.000 eventos/segundo);
- *Proxies web* (8.000 eventos/segundo);
- Servidores Windows/Linux (3.000 eventos/segundo);
- EDR em *endpoints* (12.000 eventos/segundo);
- *Cloud AWS/Azure* (4.000 eventos/segundo).

O SOC configurou as seguintes regras de correlação:

Regra 1: "Múltiplas tentativas de *login* falhadas (>10) em diferentes sistemas pelo mesmo usuário em janela de 5 minutos" → Gera alerta de severidade MÉDIA.

Regra 2: "*Login* bem-sucedido após múltiplas falhas + acesso a arquivo sensível + exfiltração de dados (>100MB *upload* externo)" → Gera alerta de severidade ALTA.

Regra 3: "Criação de nova conta administrativa + modificação de GPO + execução de *PowerShell* codificado em *Base64*" → Gera alerta de severidade CRÍTICA.

Durante uma janela de 30 minutos, o SIEM detectou:

09:00h: Usuário "joao.silva" - 15 l*ogins* falhados em 3 aplicações diferentes (SIEM, ERP, Portal RH);

09:03h: Usuário "joao.silva" - *Login* bem-sucedido no ERP a partir de IP 177.192.20.71 (Brasil);

09:07h: Usuário "joao.silva" - Acesso ao diretório "*fileserver*\financeiro\confidencial";

09:15h: Mesmo IP 177.192.20.71 - *Upload* de 250MB para storage.xpto.com via HTTPS;

09:20h: *Login* bem-sucedido do usuário "*admin.ti*" (conta administrativa) a partir do mesmo IP 177.192.20.71.

Com base neste cenário, assinale a opção que apresenta a análise correta dos alertas disparados e a resposta adequada para este cenário.

(A) Apenas o alerta da Regra 1 foi disparado, indicando possível ataque de força bruta. A Regra 2 não foi acionada porque o *upload* ocorreu 12 minutos após o *login*, excedendo a janela de correlação típica. Ação recomendada: resetar senha de "joao.silva", implementar MFA na conta e monitorar por 24h.

(B) Os alertas das Regras 1 e 2 foram disparados, caracterizando provável comprometimento de credenciais seguido de exfiltração. Ação recomendada: revogar sessões ativas de "joao.silva", isolar o *endpoint* no IP 177.192.20.71, bloquear comunicação com *storage.xpto.com*, e iniciar investigação forense do *fileserver* e *logs* de acesso.

(C) Os alertas das Regras 1, 2 e 3 foram disparados em sequência. O *login* de "*admin.ti*" às 09:20h do mesmo IP indica elevação de privilégios após o comprometimento inicial. Ação recomendada: desabilitar ambas as contas ("joao.silva" e "*admin.ti"),* reverter alterações em GPOs, e acionar resposta a incidente nível crítico.

(D) Apenas o alerta da Regra 2 foi disparado. A Regra 1 não foi acionada porque os 15 *logins* falhados distribuídos em 3 sistemas diferentes não caracterizam "múltiplos sistemas" conforme *threshold* da regra. Ação recomendada: bloquear IP 177.192.20.71 no *firewall*, quarentenar arquivos acessados e notificar usuário "joao.silva" sobre possível comprometimento.

(E) Nenhum alerta foi disparado porque a sequência de eventos, embora suspeita, não atende simultaneamente a todos os critérios de nenhuma das três regras configuradas. Ação recomendada: criar nova regra de correlação que capture este padrão específico de comportamento e manter monitoramento manual do IP 177.192.20.71.

3

Considerando técnicas de testes de segurança em aplicações, analise as afirmativas a seguir.

I. SAST (*Static Application Security Testing*) pode identificar vulnerabilidades de lógica de negócio e falhas de autorização baseadas em contexto de execução, sendo mais efetivo que DAST para detectar quebras de controle de acesso horizontal (IDOR - *Insecure Direct Object Reference).*

II. IAST (*Interactive Application Security Testing*) utiliza instrumentação de código para correlacionar entrada de dados com fluxo de execução em *runtime*, reduzindo falsos positivos em comparação com SAST puro, mas introduzindo *overhead* de performance que pode inviabilizar uso em ambientes de produção.

III. Fuzzing (*Fuzz Testing*) é técnica eficaz para identificar vulnerabilidades de corrupção de memória (*buffer overflow, use-after-free*) em aplicações compiladas, mas tem limitação em detectar falhas de lógica de negócio que requerem sequências específicas de operações válidas.

IV. DAST (*Dynamic Application Security Testing*) consegue identificar todas as rotas e *endpoints* de uma API REST automaticamente por meio de *spidering,* sem necessidade de documentação *OpenAPI/Swagger*, sendo mais abrangente em cobertura de código que SAST.

Está correto o que se afirma em

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

4

Um analista de segurança está implementando soluções de monitoramento de comportamento para detectar ameaças avançadas que contornam controles tradicionais baseados em assinaturas.

Sobre as tecnologias e os conceitos de monitoramento comportamental, assinale a afirmativa correta.

(A) *Network Traffic Analysis* (NTA) pode empregar modelos estatísticos e de *machine learning* para estabelecer *baselines* de tráfego e identificar anomalias potencialmente maliciosas.
(B) *User and Entity Behavior Analytics* (UEBA) concentra-se principalmente em usuários humanos e, quando aplicado a outras fontes (como contas de serviço ou IoT), trata-as apenas como *logs* auxiliares, não como entidades comportamentais.
(C) A análise comportamental, quando bem implementada, torna dispensáveis as assinaturas na maior parte dos cenários operacionais.
(D) *Network Detection and Response* (NDR) foca a inspeção na camada de aplicação, não considerando as informações das camadas inferiores do modelo OSI.
(E) *Beaconing* com periodicidade regular costuma refletir rotinas legítimas de atualização e, por isso, tende a ter baixa prioridade de investigação.

5

Uma equipe de segurança realizou uma varredura em infraestrutura crítica de comércio eletrônico e identificou as seguintes vulnerabilidades:

X: PHP 8.1.0 - CVE-2024-4577 (*Argument Injection leading to RCE*) | CVSS 9.8 (Crítica) | *Exploit* público (PoC no GitHub) | Servidor web exposto à Internet processando pagamentos | *Patch* disponível (atualização para 8.3.8);

Y: nginx 1.18.0 - CVE-2023-44487 (HTTP/2 *Rapid Reset* - DDoS) | CVSS 7.5 (Alta) | *Exploit* público, ataques em massa documentados | Servidor usa HTTP/2 para CDN e APIs | Mitigação via *rate limiting* disponível, *patch* requer atualização para 1.25.3;

W: *Curl* 7.68.0 - CVE-2023-38545 (SOCKS5 *heap buffer overflow*) | CVSS 9.8 (Crítica) | RCE potencial | *Scripts* internos de integração usam *curl* para comunicação com parceiros via *proxy* SOCKS5 | Servidor não exposto diretamente à Internet | Atualização para 8.4.0 disponível;

Z: *Open*SSH 8.2p1 - CVE-2024-6387 (*regreSSHion - Signal Handler Race Condition*) | CVSS 8.1 (Alta) | RCE com *exploit* complexo (requer 6-8 horas) | SSH exposto apenas para equipe DevOps (10 IPs *whitelisted,* MFA habilitado) | *Patch* disponível (9.8p1).

Considerando as boas práticas de gestão de vulnerabilidades e a análise de risco contextual, assinale a opção que apresenta a priorização correta para remediação.

(A) X → W → Z → Y.
(B) X → Y → Z → W.
(C) W → X → Z → Y.
(D) Y → X → W → Z.
(E) X → Z → Y → W.

6

Um órgão público sofreu um ataque direcionado com a seguinte sequência de eventos:

- T0 (13:00): Funcionário do setor financeiro recebeu *e-mail* de *phishing* com documento Excel malicioso (.xlsm) que explorou macro habilitada.
- T1 (13:02): O Excel executou *PowerShell* ofuscado que baixou *payload* da segunda etapa de domínio legítimo comprometido (pastebin.com) via HTTPS.
- T2 (13:05): *Payload* injetou *shellcode* em processo legítimo (svchost.exe) por meio de *process hollowing*, estabelecendo persistência via registro do *Windows (Run key).*
- T3 (13:15): Atacante realizou *credential dumping* extraindo *hashes* NTLM da memória do LSASS usando técnica *living-off-the-land (Mimikatz reflective injection*).
- T4 (13:30): Movimentação lateral via PsExec para servidor de aplicação usando credenciais roubadas, sem exploração de vulnerabilidade.
- T5 (14:00): Exfiltração de 500MB de dados para servidor C2 externo via DNS *tunneling,* fragmentando dados em *queries* DNS aparentemente legítimas.

Com base nos eventos T0–T5, assinale a opção que indica a tecnologia adequada para identificar o padrão observado e sustentar a investigação e a contenção do incidente.

(A) Antivírus tradicional baseado em assinaturas detectaria o *hash* do arquivo Excel malicioso em T0 e bloquearia toda a cadeia de ataque subsequente.

(B) EDR com análise comportamental detectaria T1, T2 e T3 fornecendo telemetria detalhada da cadeia de execução, mas teria visibilidade limitada da movimentação lateral (T4) e exfiltração DNS (T5) por serem eventos de rede/servidor.

(C) XDR com telemetria unificada de *endpoints*, rede e *cloud* correlacionaria eventos de T0 até T5, detectando o padrão completo por meio de múltiplos vetores e fornecendo visão holística com resposta coordenada.

(D) Antivírus *next-generation* (NGAV) com *machine learning* identificaria comportamento anômalo do Excel executando *PowerShell* em T1 e bloquearia imediatamente, tornando irrelevantes as etapas posteriores.

(E) EDR avançado detectaria todas as etapas T0 a T5 através de análise comportamental de processos e telemetria de conexões de rede do *endpoint,* tornando XDR redundante para este cenário.

7

No contexto da segurança de redes e aplicações corporativas, diferentes tipos de ataques requerem medidas de proteção específicas e adequadas às suas características técnicas.

Relacione os tipos de ataque listados a seguir, às suas respectivas medidas de proteção primárias.

1. *Ransomware*
2. *Credential Stuffing*
3. *DNS Spoofing*
4. *Server-Side Request Forgery* (SSRF)

( ) Implementar segmentação de rede com micro-segmentação, *backup* imutável (*immutable backup*) com retenção *offline*, EDR com detecção comportamental, e *Application Control* para bloquear executáveis não autorizados.

( ) Implementar DNSSEC (*Domain Name System Security Extensions*) para autenticação de respostas DNS, configurar *resolvers* DNS confiáveis, e utilizar DoH (DNS *over* HTTPS) ou DoT (DNS *over* TLS) para criptografar consultas.

( ) Implementar validação rigorosa de URLs de entrada, utilizar *allowlist* de destinos permitidos, restringir acesso de servidores a recursos internos através de *firewalls* internos, e sanitizar/validar todos os parâmetros que constroem requisições HTTP.

( ) Implementar *rate limiting* por IP e por conta de usuário, CAPTCHA após tentativas falhadas, monitoramento de credenciais vazadas em bases públicas (*Have I Been Pwned*), autenticação multifator (MFA), e detecção de anomalias baseada em geolocalização e dispositivos.

Assinale a opção que indica a relação correta na ordem apresentada.

(A) 1 – 3 – 4 – 2.

(B) 1 – 4 – 2 – 3.

(C) 2 – 1 – 3 – 4.

(D) 3 – 4 – 1 – 2.

(E) 4 – 3 – 2 – 1.

8

No contexto da segurança de sistemas de Inteligência Artificial, diversas técnicas de ataque e defesa foram desenvolvidas para lidar com vulnerabilidades específicas de modelos de *Machine Learning.*

Relacione os tipos de ataques e técnicas de segurança em IA apresentados a seguir, às suas respectivas características.

1. *Adversarial Evasion Attack*
2. *Model Poisoning Attack*
3. *Model Extraction Attack*
4. *Adversarial Training*

( ) Técnica defensiva que consiste em treinar o modelo utilizando exemplos adversariais junto com dados legítimos para aumentar a robustez do sistema contra perturbações maliciosas.

( ) Ataque realizado durante a fase de inferência, no qual entradas são sutilmente modificadas para induzir o modelo a classificações incorretas, mantendo-se imperceptíveis ao usuário humano.

( ) Ataque executado na fase de treinamento, no qual dados maliciosos são injetados no conjunto de dados de treinamento para comprometer o comportamento do modelo resultante.

( ) Ataque que visa replicar a funcionalidade de um modelo proprietário através de consultas sistemáticas, permitindo ao atacante obter uma cópia funcional sem acesso direto aos parâmetros originais.

Assinale a opção que indica a relação correta, segundo a ordem apresentada.

(A) 1 – 3 – 2 – 4.
(B) 2 – 4 – 3 – 1.
(C) 3 – 2 – 4 – 1.
(D) 4 – 1 – 2 – 3.
(E) 4 – 3 – 1 – 2.

9

José, recentemente contratado como CISO pela *Banana Inc,* sociedade empresária de médio porte com 500 funcionários, ficou entusiasmado ao ler sobre *Arquitetura Zero Trust* em uma rede social.

Interpretando literalmente o termo *Zero Trust* (confiança zero), José concluiu que isso significava não confiar em absolutamente nada nem ninguém. Ele então:

- Bloqueou todas as comunicações entre sistemas internos por padrão, sem exceções;
- Removeu todos os usuários e grupos do *Active Directory* que tivesse qualquer tipo de permissão;
- Desativou a VPN e o acesso remoto completamente ("não podemos confiar em ninguém fora do escritório");
- Configurou o *firewall* para negar todo tráfego de entrada e saída;
- Desabilitou certificados digitais da sociedade empresária ("não podemos confiar nem em nós mesmos");
- Bloqueou o acesso administrativo a todos os servidores, incluindo para a própria equipe de TI.

Após essa implementação, a sociedade empresária ficou completamente paralisada: os sistemas não comunicavam entre si, os usuários não conseguiam acessar nenhum recurso, os *e-mails* não eram recebidos nem enviados, e a própria equipe de TI ficou impossibilitada de gerenciar a infraestrutura.

A diretoria exigiu correção imediata mantendo princípios de segurança modernos. Para implementar corretamente *Arquitetura Zero Trust* conforme a NIST SP 800-207, José deveria

(A) substituir a VPN tradicional por uma solução ZTNA (*Zero Trust Network Access*), pois *Zero Trust* consiste essencialmente em trocar VPN por acesso baseado em identidade, mantendo o restante da arquitetura de segurança inalterado.
(B) implementar micro-segmentação de rede por meio de VLANs e ACLs rigorosas em todos os *switches* e *firewalls* internos, isolando cada departamento em sua própria zona de confiança separada.
(C) implementar a autenticação multifator (MFA) obrigatória para todos os acessos de usuários e *service accounts*, pois *Zero Trust*, fundamentalmente, significa fortalecer a autenticação para eliminar confiança implícita.
(D) implementar um modelo em que a segurança não se baseia em confiança implícita na localização de rede, mas em verificação contínua de identidade, contexto do dispositivo e autorização granular por recurso, usando *Policy Engine e Policy Enforcement Points* automatizados.
(E) bloquear todo tráfego por padrão e criado um processo automatizado de *whitelist,* em que cada usuário solicita acesso a recursos específicos via sistema de *tickets*, com aprovação automática baseada em função do usuário no organograma.

10

Uma aplicação web corporativa está vulnerável aos ataques em que usuários maliciosos conseguem fazer a aplicação executar comandos arbitrários do sistema operacional por meio da manipulação de parâmetros que são passados diretamente para funções de execução de processos no servidor.

Este tipo de vulnerabilidade caracteriza-se como

(A) SQL Injection.
(B) Path Traversal.
(C) Command Injection.
(D) Cross-Site Scripting (XSS).
(E) XML External Entity (XXE).

11

Considerando a Gestão de Segurança da Informação e seus processos fundamentais, como a Gestão de Riscos e a Gestão de Identidade e Acesso, bem como sua relação com a Continuidade do Negócio, avalie as afirmativas a seguir e assinale (V) para a verdadeira e (F) para a falsa.

( ) Na Gestão de Segurança da Informação (ISO 27001), a definição do escopo do SGSI deve obrigatoriamente levar em conta o contexto da organização (questões internas e externas) e os requisitos das partes interessadas.
( ) Na Gestão de Continuidade do Negócio, o RPO (*Recovery Point Objective*) define a idade máxima dos dados que devem ser recuperados após um incidente, representando o volume de perda de dados aceitável.
( ) Na Gestão de Identidade e Acesso, o *OpenID Connect* (OIDC) funciona como uma camada de identidade construída sobre o protocolo OAuth 2.0, adicionando a capacidade de autenticação de usuários e a obtenção de informações básicas de perfil.

As afirmativas são, respectivamente,

(A) V – F – F.
(B) V – F – V.
(C) V – V – V.
(D) V – V – F.
(E) F – V – V.

12

Uma equipe identificou que um servidor *web* crítico foi comprometido por um atacante que explorou uma vulnerabilidade de aplicação. A análise inicial revelou que o atacante instalou uma *webshell* e está usando o servidor para movimentação lateral na rede. O servidor processa transações financeiras e está em produção atendendo clientes.

O analista de segurança precisa decidir a ação imediata mais adequada na fase de contenção do incidente, conforme boas práticas de resposta a incidentes (NIST SP 800-61 e ISO/IEC 27035).

Assinale a opção que apresenta a estratégia de contenção apropriada para esse cenário.

(A) Desligar imediatamente o servidor comprometido para prevenir danos adicionais, mesmo que cause indisponibilidade do serviço, pois a prioridade absoluta é impedir que o atacante continue acessando o sistema.
(B) Manter o servidor em operação normal sem alterações, enquanto realiza monitoramento detalhado das atividades do atacante por 48 horas, coletando evidências extensivas antes de qualquer ação de contenção.
(C) Implementar contenção segmentada isolando o servidor da rede por meio de regras de *firewall* que bloqueiem comunicação lateral mas mantenham o acesso de clientes externos, enquanto inicia investigação forense em memória e preserva evidências, consultando *stakeholders* sobre janela de manutenção para contenção completa.
(D) Executar imediatamente procedimento de reimagem do servidor com *backup* limpo anterior à data do comprometimento, restaurando o serviço rapidamente, e considerar o incidente resolvido sem necessidade de análise forense detalhada.
(E) Notificar imediatamente a ANPD (Autoridade Nacional de Proteção de Dados) e publicar comunicado público sobre o incidente, antes de realizar qualquer ação técnica de contenção, para cumprir requisitos de transparência da LGPD.

13

No âmbito da ICP-Brasil, certificados digitais podem ser revogados antes do término da validade quando há comprometimento da chave privada.

Nesse contexto, assinale a opção que apresenta o mecanismo usado para verificar o estado de revogação de certificados digitais em tempo real.

(A) LCR (Lista de Certificados Revogados)
(B) OCSP (*Online Certificate Status Protocol)*
(C) *Timestamp Authority.*
(D) CRL *Distribution Point.*
(E) *Certificate Pinning.*

14

Uma organização de médio porte está priorizando a implementação dos Controles de Segurança CIS v8 e possui os seguintes recursos:

- Orçamento limitado de segurança;
- Equipe técnica de 5 profissionais;
- Maturidade inicial em segurança (não possui inventário de ativos completo);
- Alta dependência de *e-mail* para comunicação de negócios.

O CISO está analisando as salvaguardas *(safeguards*) que deve implementar prioritariamente. Os Controles de Segurança CIS v8 classificam os controles em três grupos de implementação (*Implementation Groups* – IGs):

- IG1: Controles básicos e fundamentais (56 *safeguards).*
- IG2: Controles intermediários (74 *safeguards).*
- IG3: Controles avançados (23 *safeguards*).

Considerando o contexto organizacional e a metodologia do *CIS Controls v8*, assinale a opção que indica a estratégia de implementação adequada.

(A) Implementar todos os 153 *safeguards* dos três IGs simultaneamente para garantir proteção abrangente, utilizando ferramentas *open-source* para reduzir custos.

(B) Focar exclusivamente nos *6 CIS Controls* básicos (1- *Inventory of Assets;* 2- *Inventory of Software;* 3- *Data Protection*; 4- *Secure Configuration*; 5- *Account Management;* 6- *Access Control Management*), implementando todos os *safeguards* desses controles.

(C) Implementar prioritariamente os 56 *safeguards* do IG1, focando inicialmente nos controles 1 (Inventário de Ativos) e 2 (Inventário de Software) como fundação, depois 4 (Configuração Segura), 5 (Gestão de Contas) e 6 (Controle de Acesso), seguindo a ordem de prioridade recomendada.

(D) Começar pelos controles mais avançados do IG3, como *Penetration Testing* e *Red Team Exercises*, pois são os que oferecem maior retorno sobre investimento em detecção de vulnerabilidades.

(E) Implementar apenas controles relacionados a *e-mail* (*anti-spam, anti-phishing*, DMARC/SPF/DKIM) do IG2, pois *e-mail* é o maior vetor de ataque, segundo o contexto da organização.

15

Soluções DLP (*Data Loss Prevention*) utilizam diferentes métodos para identificar e classificar dados sensíveis que precisam ser protegidos.

Assinale a opção que descreve corretamente o método de classificação de dados por "*Exact Data Match"* (EDM) em soluções DLP.

(A) Utiliza expressões regulares para identificar padrões de dados sensíveis como números de cartão de crédito ou CPF.

(B) Aplica algoritmos de *machine learning* para classificar documentos baseado em conteúdo e contexto semântico.

(C) Analisa *metadados* de arquivos como autor, data de criação e *tags* para determinar sensibilidade dos dados.

(D) Identifica dados sensíveis através de palavras-chave e dicionários personalizados configurados pelo administrador.

(E) Cria *hashes* criptográficos de registros específicos de bancos de dados permitindo identificação sem expor os dados originais.

Banco de Dados

16

Em um banco de dados relacional (PostgreSQL), um administrador está projetando a tabela Vendas que armazena informações sobre transações. A integridade referencial com a tabela *Clientes* precisa ser garantida, e a combinação dos campos *ID_Venda* e *Data_Venda* deve garantir a unicidade de cada registro na tabela.

Assinale a opção que indica o tipo de chave que deve ser usada no campo que garante a integridade referencial com a tabela *Clientes*, e o tipo de chave que a combinação de *ID_Venda* e *Data_Venda* representa, garantindo a unicidade mínima e não-redundante do registro.

(A) Chave Primária para integridade referencial e Superchave para unicidade.

(B) Chave Estrangeira para integridade referencial e Chave Candidata para unicidade.

(C) Chave Candidata para integridade referencial e Chave Primária para unicidade.

(D) Chave Estrangeira para integridade referencial e Superchave para unicidade.

(E) Chave Alternativa para integridade referencial e Chave Estrangeira para unicidade.

17

Uma consulta SQL que realiza múltiplos JOINs e filtros sobre tabelas grandes está apresentando lentidão.

As opções a seguir apresentam estratégias recomendadas para otimização, ***<u>à exceção de uma</u>***. Assinale-a.

(A) Normalizar ainda mais as tabelas envolvidas.

(B) Utilizar EXPLAIN para verificar o plano de execução.

(C) Avaliar estatísticas e atualizá-las com ANALYZE.

(D) Criação de índices nos campos usados em JOIN e WHERE.

(E) Reescrever a consulta evitando subconsultas desnecessárias.

18

O *pipeline* que carrega dados de execução orçamentária do sistema operacional para o *Data Warehouse* deve garantir que o volume de dados seja carregado no ambiente analítico de forma eficiente, seguindo todas as transformações já aplicadas.

Assinale a opção que apresenta a principal responsabilidade e o desafio da fase *Load* no processo ETL, especialmente em relação ao *design* de índice e particionamento da Tabela de Fato.

(A) Criar e gerenciar a *Cloud Platform* onde o ETL será executado

(B) Definir as regras de limpeza e padronização (transformação) dos dados.

(C) Gerenciar a Consistência Externa Forte entre diferentes regiões geográficas.

(D) Identificar e extrair as alterações incrementais (*deltas*) da fonte de dados operacional (OLTP).

(E) Realizar o carregamento dos dados transformados para o *Data Warehouse* e garantir que os mecanismos de otimização sejam utilizados.

19

Um órgão estadual de finanças migrou sua base de dados relacional crítica para um serviço gerenciado em nuvem (ex: AWS RDS ou Azure SQL Database) e configurou o recurso de Alta Disponibilidade (HA).

O objetivo é garantir que, em caso de falha completa da Zona de Disponibilidade (AZ) onde a instância primária reside, o serviço possa ser restaurado rapidamente com perda mínima de dados.

Assinale a opção que indica o principal mecanismo arquitetural usado por esses serviços gerenciados para Alta Disponibilidade, que minimiza o RPO (*Recovery Point Objective*) em um cenário Multi-AZ e garante a rápida transição (*failover*) sem a necessidade de intervenção manual.

(A) A utilização de *Snapshots* diários para reconstrução da instância em outra AZ.

(B) O uso de um *Load Balancer,* distribuindo a carga de escrita (*writes*) entre as réplicas em todas as AZs.

(C) A replicação dos dados para uma instância *standby* (secundária), localizada em uma AZ diferente, com o uso de replicação síncrona ou semi-síncrona para garantir RPO próximo a zero.

(D) A configuração de *Read Replicas* em diversas regiões geográficas com replicação assíncrona para o tráfego de leitura.

(E) A estratégia de *Sharding* (fragmentação) de dados entre diversas instâncias para escalabilidade de escrita.

20

Em um ambiente *Data Mesh*, os dados não são apenas armazenados, mas sim tratados como *Data Products*. Para que um Produto de Dados seja verdadeiramente útil e auto-serviço em uma malha de dados governada, ele deve aderir a certas características.

Assinale a opção que apresenta a característica mandatória para que um *Data Product* em um Data Mesh seja considerado auto-descritivo e possa ser descoberto e consumido por outros domínios, sem a necessidade de contato direto com o time produtor.

(A) O *Data Product* deve ser fisicamente armazenado em uma única instância de banco de dados relacional e ser consultável apenas por *Stored Procedures.*

(B) O *Data Product* deve ser acessível exclusivamente por meio de um *Data Lake* centralizado, com todos os arquivos no formato CSV.

(C) O *Data Product* deve ser endereçável, seguro, e obrigatoriamente incluir Metadados Descobertos e Estruturais que são publicados em um catálogo unificado.

(D) O *Data Product* deve eliminar totalmente a necessidade de Governança Federada, permitindo a livre manipulação dos dados por qualquer consumidor.

(E) O *Data Product* deve ser obrigatoriamente replicado de forma síncrona para todas as regiões geográficas do Estado e permitir o armazenamento em uma única instância do banco de dados relacional.

21

Um DBA está avaliando o desempenho de uma consulta que frequentemente busca dados na tabela Auditoria (com 500 milhões de registros) usando a coluna DataHora_Acesso na cláusula WHERE. O DBA decide criar um índice clusterizado nessa coluna (após remover o índice existente na chave primária autoincremento, se necessário).

Assinale a opção que apresenta a principal implicação técnica de criar um índice clusterizado na coluna DataHora_Acesso de uma tabela tão grande no MS SQL Server, e a consequência direta para a ordenação física dos dados.

(A) Permite que a tabela tenha um índice clusterizado e um índice não clusterizado na mesma coluna.

(B) O índice clusterizado não afeta a ordenação física dos dados, mas armazena a tabela em um *heap* (estrutura desordenada) contribuindo para a desnormalização da base de dados.

(C) O índice clusterizado é apenas um *bookmark* lógico, e a ordenação física é sempre determinada pela chave primária autoincremento original.

(D) O MS SQL Server permite que uma tabela tenha múltiplos índices clusterizados, aumentando a velocidade de todas as consultas.

(E) O índice clusterizado define a ordem física de armazenamento das linhas de dados na tabela, o que acelera as consultas por intervalo nessa coluna, mas pode degradar o desempenho de *INSERTs/UPDATEs* em outras colunas.

22

A Controladoria possui vários *pipelines* críticos que transportam dados de regulamentação fiscal. Uma mudança no *schema* da tabela de origem exigiu alterações no código SQL de transformação e nos metadados associados. A prática de DataOps exige que todas as alterações sejam rastreáveis e que seja possível reverter o *pipeline* para uma versão anterior de forma atômica.

No contexto do DataOps, assinale a opção que apresenta a combinação de práticas e ferramentas que garante a rastreabilidade de

I. código de transformação (SQL/ETL);

II. alterações no *schema* do DW; e

III. *rollback*, coordenação automatizada, em caso de falha de *deployment*.

(A) Utilização de GIT para versionar o código do *pipeline*; aplicação de ferramentas de Versionamento de Banco de Dados para o *schema*; e orquestração CI/CD com estratégias de *rollback* automático.

(B) Adoção de um Catálogo de Metadados para registrar o código de transformação; uso do Modelo *Star Schema* para o versionamento do *schema*; e *restore* do ambiente de *Data Warehouse* em caso de falha.

(C) Implementação do *Data Fabric* e da técnica de Virtualização de Dados para evitar alterações no código de transformação; registro manual do *schema* no Glossário; e delegação da reversão ao *Data Protection Officer*.

(D) Uso de Kubernetes para orquestrar os *containers* do *pipeline*; dependência do Modelo *Entity-Relationship* para rastrear o *schema* do DW; e execução de Subconsultas Correlacionadas para validar a transformação dos dados.

(E) Aplicação de *Self-Service Analytics* para validar o código de transformação; utilização de TDD para o versionamento de *schema* do DW; e dependência de *Triggers* do SGBD para gerenciar a reversão atômica do *deployment*.

23

A integridade referencial entre a tabela Pedidos (Chave Estrangeira FK_ClienteID) e a tabela Clientes (Chave Primária PK_ClienteID) foi estabelecida. O administrador do banco de dados precisa garantir que, se um registro for excluído da tabela Clientes, todos os registros de pedidos associados a esse cliente na tabela Pedidos sejam automaticamente excluídos em cascata.

Assinale a opção que indica a cláusula específica da restrição de Chave Estrangeira que deve ser usada para implementar esse comportamento de propagação da exclusão.

(A) ON UPDATE CASCADE
(B) ON DELETE NO ACTION
(C) ON DELETE SET NULL
(D) ON DELETE CASCADE
(E) ON DELETE RESTRICT

24

Um desenvolvedor inicia uma série de comandos DML (*Data Manipulation Language*) em uma sessão do SGBD.

Ele executou um UPDATE seguido de um DELETE. Após a execução, ele percebeu que o resultado da alteração estava incorreto e decidiu que as modificações feitas na sessão não deviam ser persistidas no banco de dados.

Assinale a opção que indica o comando SQL Transacional que o desenvolvedor deve executar para desfazer todas as modificações realizadas desde o início da transação na sessão atual, e a principal característica que define uma transação em andamento na regra ACID.

(A) COMMIT / Durabilidade.
(B) CHECKPOINT / Isolamento.
(C) SAVEPOINT seguido de ROLLBACK TO SAVEPOINT / Consistência.
(D) ROLLBACK / Atomicidade.
(E) VACUUM / Integridade.

25

Em projetos de *Business Intelligence* (BI) modernos, a tendência é capacitar os usuários de negócio a explorar dados sem depender exclusivamente do time de TI ou de *data scientists*.

Assinale a opção que indica o conceito de BI que descreve a prática de fornecer ferramentas intuitivas e acesso direto aos dados para que os usuários de negócio possam criar seus próprios relatórios, *dashboards* e análises *ad hoc*, independentemente do time de TI.

(A) *ETL Pipeline*.
(B) *Olap Cube*.
(C) *Data Fabric*.
(D) *Self-Service Analytics*.
(E) *Threat Modeling*.

26

Em um contexto de Governança de Dados, o cumprimento da LGPD (Lei Geral de Proteção de Dados) é essencial. O papel de *Data Steward* é fundamental para garantir a conformidade e a qualidade dos dados.

No que tange à LGPD e à Qualidade de Dados em um ambiente de *Data Governance*, assinale a opção que indica a principal responsabilidade do *Data Steward.*

(A) Desenvolver a arquitetura de *Data Mesh* para descentralizar os dados.
(B) Configurar os serviços de nuvem para escalabilidade automática.
(C) Ser o único responsável pelo desenvolvimento de todos os *pipelines* ETL.
(D) Atuar como o DPO (*Data Protection Officer*) da empresa, que é um papel legalmente definido e central.
(E) Garantir a definição, a qualidade, a integridade e o uso ético/legal dos dados, em seu domínio de responsabilidade.

27

No SQL Server, uma das práticas recomendadas para otimizar o desempenho de consultas complexas, é o uso de índices compostos. Considere a seguinte situação:

Uma tabela de vendas (Vendas) contém as colunas *data_venda*, *id_cliente*, *valor_total*. Deseja-se otimizar a consulta que filtra registros por *id_cliente* e ordena por *data_venda*.

Assinale a opção que indica a configuração de índice mais adequada.

(A) Índice apenas em *valor_total*.
(B) Índice apenas em *data_venda*.
(C) Índice composto em (*data_venda*, *id_cliente*).
(D) Índice composto em (*id_cliente*, *data_venda*).
(E) Índice filtrado em *valor_total* com condição *valor_total* > 1000.

28

Na modelagem de um *Data Warehouse* para análise de vendas, o arquiteto optou pela modelagem dimensional. A tabela central contém métricas (fato) e é conectada a diversas tabelas de dimensão (tempo, produto, cliente).

Assinale a opção que indica a principal técnica de modelagem dimensional utilizada, em que a tabela central armazena as métricas (*o fato*), e a desnormalização das tabelas de contexto (dimensões) é intencional para otimizar o desempenho das consultas OLAP.

(A) Modelo Entidade-Relacionamento (ER).
(B) Modelo de Banco de Dados Hierárquico.
(C) Modelo de Rede (*Network Model*).
(D) Modelo *Star Schema* (Esquema Estrela).
(E) Modelo *Data Fabric*.

29

Sobre as características de bancos NoSQL, assinale a afirmativa correta.

(A) Bancos orientados a documentos armazenam dados em pares chave/valor simples.
(B) Bancos de grafos usam estrutura relacional para representar arestas.
(C) Bancos chave/valor suportam transações ACID complexas por padrão.
(D) Bancos orientados a documentos permitem consultas estruturadas por atributos aninhados.
(E) Bancos de grafos não permitem relacionamentos direcionados.

30

Ao usar um serviço gerenciado de Banco de Dados Relacional em Nuvem (ex: AWS RDS ou Azure SQL Database), a arquitetura de Alta Disponibilidade (HA) é essencial para minimizar o *downtime* em caso de falha de infraestrutura.

Em um SGBD em nuvem configurado para Alta Disponibilidade Multi-AZ/Multi-Region, assinale a opção que indica o mecanismo de replicação e *failover* que permite a transição rápida para uma réplica em caso de falha da instância primária.

(A) O *Failover* exige a recriação manual da instância e o *restore* de um *snapshot*.
(B) A replicação de log é feita via *File Transfer Protocol* (FTP) entre as regiões.
(C) A replicação é Assíncrona, mas o *failover* é instantâneo e sem perda de dados (RPO zero).
(D) Apenas o serviço *Google Cloud Spanner* oferece HA, os demais usam replicação simples.
(E) É usado um modelo de replicação Síncrona entre a instância primária e a secundária em outra Zona de Disponibilidade, permitindo um *failover* automático e rápido (*RTO baixo*).

Ciência de Dados

31

Uma equipe de Ciência de Dados do setor público precisa analisar um grande *dataset* de características de cidadãos (alta dimensionalidade) para identificar grupos naturais de comportamento (segmentação) e, posteriormente, reduzir a dimensionalidade dos dados sem perder muita informação.

Sobre as técnicas de *Clustering* e Redução de Dimensionalidade, avalie as afirmativas a seguir.

I. O algoritmo DBSCAN é mais adequado que o K-Means para *datasets* com *clusters* de formato não convexo e tem a vantagem de ser robusto a ruídos e *outliers*.
II. O algoritmo K-Means exige que o número de *clusters* (K) seja definido previamente e é sensível à escala das variáveis de entrada e à presença de *outliers*.
III. A Análise de Componentes Principais (PCA) é uma técnica não supervisionada que é utilizada para redução de dimensionalidade, e deve ser aplicada *antes* de qualquer etapa de *scaling* dos dados para preservar a variância.

Está correto o que se afirma em

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

32

Um cientista de dados da Controladoria está preparando um *dataset* de despesas públicas para ser utilizado em um algoritmo de *Machine Learning* baseado em distâncias como K-Nearest Neighbors - KNN.

A coluna *Valor_Despesa* varia amplamente, com valores entre R$ 100,00 (mínimo) e R$ 5.000.000,00 (máximo).

Assinale a opção que indica a técnica de Normalização Numérica mais adequada para reescalonar os dados da coluna *Valor_Despesa*, para que todos os seus valores sejam mapeados para um intervalo fixo entre 0 e 1.

(A) Discretização baseada em largura (*Equal Width Binning*).
(B) Padronização (*Standardization* ou *Z-Score*).
(C) Discretização baseada em frequência.
(D) Codificação *One-Hot Encoding.*
(E) Normalização Min-Max.

33

O Processamento *MapReduce* é o paradigma fundamental para o processamento distribuído de *Big Data* em *clusters*.

Um cientista de dados usou essa técnica para processar milhões de *logs* de auditoria, em que a fase *Map* já emitiu pares chave-valor intermediários (ex: (UsuárioID, 1)).

De acordo com modelo *MapReduce,* assinale a opção que apresenta a função exata e sequencial da fase *Shuffle & Sort* que é crítica para preparar os dados para a posterior agregação na fase *Reduce.*

(A) Coletar a saída intermediária dos *Mappers*, transportar, particionar e ordenar esses pares chave-valor, garantindo que todas as ocorrências de uma mesma chave sejam agrupadas e enviadas ao mesmo *Reducer*.
(B) Coletar os dados brutos da fonte de dados distribuída e aplicar a função de filtragem inicial (Map) em cada nó de processamento.
(C) Aplicar a função de agregação de redução (*Reduce*) nas chaves recebidas, calculando a soma final em uma única operação.
(D) Persistir a saída final no HDFS e coordenar a distribuição de blocos entre os *DataNodes* do *cluster*.
(E) Realizar o *split* lógico dos arquivos de entrada em blocos menores e garantir a tolerância a falhas através da replicação automática.

34

Um analista da Controladoria está utilizando a linguagem R para armazenar dados de uma planilha importada que contém diferentes tipos de variáveis: uma coluna de texto (*Nome_Gestor*), uma coluna de números inteiros (*ID_Contrato*) e uma coluna de valores monetários decimais (*Valor_Total*). É necessário que a estrutura de dados permita o armazenamento de colunas de diferentes tipos e suporte às operações vetoriais para análise estatística.

Assinale a opção que indica a estrutura de dados fundamental na linguagem R que é mais apropriada para armazenar dados tabulares, aceitando colunas com tipos de dados heterogêneos e nomes descritivos.

(A) *List*.
(B) *Matrix*.
(C) *Factor*.
(D) *Vector*.
(E) *Data.frame*.

35

Um cientista de dados utiliza a linguagem Python e a biblioteca Pandas para processar um *dataset* de despesas da Controladoria.

Ele precisa realizar uma operação que combine dados de dois DataFrames (despesas_2023 e despesas_2024) com base em uma coluna-chave comum (*ID_Gestor*), mas o novo DataFrame resultante deve incluir apenas os registros que possuem correspondência em ambos os DataFrames.

Assinale a opção que indica a operação fundamental do Pandas, análoga a uma operação de *join* em SQL, que deve ser usada para alcançar esse resultado, que inclui apenas a intersecção dos registros.

(A) pd.concat(), usando o argumento axis=0 para empilhamento vertical.
(B) pd.merge(),usando o argumento how='inner'.
(C) pd.merge(),usando o argumento how='left'.
(D) pd.join(), usando a função pd.apply() para intersecção manual.
(E) pd.pivot_table(), para agregação e resumo.

36

No desenvolvimento de um sistema de recomendação para auxiliar cidadãos a encontrar serviços públicos correlacionados, a equipe avaliou o uso de diferentes técnicas, como Filtragem Colaborativa (FC) e Regras de Associação.

Sobre o tema, avalie as afirmativas a seguir.

I. As Regras de Associação como a *Apriori* são avaliadas pelo Suporte, Confiança e *Lift*, sendo o *Lift* maior que 1 o indicador da força da associação por considerar a frequência esperada das ocorrências.
II. A Filtragem Colaborativa é uma técnica robusta ao problema de *Cold Start* (novos usuários/itens), uma vez que não depende do histórico de interações.
III. Sistemas de recomendação do tipo *Content-Based* têm o risco de criar uma câmara de eco porque tendem a recomendar apenas itens com características muito semelhantes às interações passadas do usuário.

Está correto o que se afirma em

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

37

Um cientista de dados de uma agência reguladora está desenvolvendo modelos de *Machine Learning* para dois problemas distintos: classificar empresas de alto e baixo risco de fraude focando na Classificação Binária e prever o valor futuro de um indicador econômico tendo por base os fundamentos da Regressão.

Sobre as técnicas de modelagem e avaliação mais adequadas para cada cenário, avalie as afirmativas a seguir.

I. No problema de Classificação Binária com uma base desbalanceada, a métrica do coeficiente de determinação R^2 deve ser priorizada sobre a acurácia.

II. No problema de Regressão, o erro quadrático médio (MSE - *Mean Squared Error*) é altamente sensível a outliers, e sua raiz quadrada RMSE possui a mesma unidade de medida da variável alvo.

III. O modelo de Regressão Logística é uma técnica de classificação que é adequada para estimar a probabilidade de um evento, mas é incorreto utilizá-lo para prever um valor contínuo como na Regressão.

Está correto o que se afirma em

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

38

A Controladoria está iniciando um programa formal de qualidade de dados com o objetivo de elevar a confiança nos seus relatórios de auditoria. Uma das primeiras e mais fundamentais ações é estabelecer clareza sobre o significado e as regras de validação para campos críticos, como CNPJ e Classificação Orçamentária.

Para documentar e formalizar de forma centralizada o significado de termos de negócio e as regras de validação associadas, servindo como a principal fonte de verdade para a qualidade de dados, a boa prática fundamental que deve ser adotada é a

(A) criação de um grande *Data Lake* centralizado.
(B) migração de todos os bancos de dados para a nuvem.
(C) implementação de um sistema de segurança de dados com *firewall*.
(D) padronização de todos os *dashboards* de BI com a ferramenta Power BI.
(E) adoção de um Glossário de Negócio ou de Dados, e um Catálogo de Metadados para formalizar as definições.

39

Em um projeto de auditoria da Controladoria, foi identificado que o campo CPF (Cadastro de Pessoa Física) em uma tabela possui, em alguns registros, valores vazios (*NULL*), o que impede a correta identificação dos envolvidos nos processos.

Assinale a opção que apresenta a Dimensão da Qualidade de Dados, na visão do DMBOK, que está sendo violada quando um campo, como o CPF, apresenta valores ausentes (*NULL*) na base de dados.

(A) Precisão.
(B) Integridade.
(C) Completude.
(D) Consistência.
(E) Tempestividade.

40

Um servidor da Controladoria deseja usar um *Large Language Model* (LLM), como o GPT ou *Llama*, em sua versão padrão pré-treinada, para uma tarefa imediata e genérica de processamento de texto. A tarefa consiste em receber um longo relatório jurídico e criar um resumo conciso de um parágrafo.

Assinale a opção que indica a aplicação fundamental dos LLMs que permite que eles processem um texto extenso de entrada e gerem uma saída textual mais curta e coerente, como um resumo, sem a necessidade de ajuste fino (*fine-tuning*).

(A) Detecção de *outliers* em Séries Temporais.
(B) Classificação Binária de *Datasets* Tabulares.
(C) Geração de Linguagem ou Geração de Texto.
(D) Geração de Imagem por Modelos de Difusão.
(E) Agrupamento não Supervisionado de Dados Numéricos.

Desenvolvimento de Sistemas

41

Considere um sistema desenvolvido com base nos princípios da Orientação a Objetos. O sistema possui uma classe base abstrata *Funcionario* e duas classes derivadas: Gerente e Vendedor.

A classe *Funcionario* define um método calcularSalario() que é implementado de forma diferente em Gerente (com bônus de gestão) e Vendedor (com comissão de vendas). A capacidade de utilizar uma referência do tipo *Funcionario* para chamar o método calcularSalario() e ter a versão correta do método (Gerente ou Vendedor) sendo executada em tempo de execução, é uma característica fundamental do seguinte conceito da Orientação a Objetos:

(A) polimorfismo, especificamente o polimorfismo de inclusão.
(B) encapsulamento, protegendo os dados internos das classes.
(C) herança, definindo a relação 'é um tipo de' entre as classes.
(D) abstração, garantindo que apenas detalhes essenciais sejam expostos.
(E) coesão, medindo o quão relacionados estão os elementos dentro de um módulo.

42

O *Test-Driven Development* (TDD) é uma prática de *Extreme Programming* (XP) que integra o desenvolvimento com a qualidade de *software*, seguindo o ciclo rigoroso de *Red, Green, Refactor*.

Assinale a opção que indica a principal atividade realizada na fase *Refactor* do TDD e o seu objetivo primário em relação à qualidade do código.

(A) Escrever o teste de unidade que falha; e garantir que a cobertura de testes seja 100% confiável.
(B) Escrever o código de produção mínimo para o teste passar e provar que o teste é válido no domínio aplicado e no problema tratado.
(C) Criar um novo *feature branch* no Git e isolar as alterações de forma segura e atômica.
(D) Reestruturar o código de produção e o código de teste sem alterar seu comportamento funcional e melhorar a legibilidade, reduzir a duplicação e otimizar o design interno.
(E) Iniciar a integração contínua e o *deployment* automático e entregar valor rapidamente ao cliente.

43

O padrão de arquitetura *Model-View-Controller* (MVC) é amplamente usado em aplicações web, separando responsabilidades para facilitar a manutenção, a reutilização de código e a testabilidade.

Assinale a opção que indica, no MVC, o componente que é responsável por receber as requisições do usuário, processar a entrada, determinar a lógica de negócio que deve ser executada, interagindo com o Model e, por fim, selecionar a *View* que deve ser apresentada ao usuário.

(A) View.
(B) Model.
(C) Controller.
(D) Repository.
(E) Service.

44

No *framework* Scrum, a gestão do produto e a maximização do valor do trabalho realizado pelo time de desenvolvimento são responsabilidades que exigem uma visão estratégica e de negócio.

Assinale a opção que indica o papel do Scrum, o principal responsável por gerenciar o *Product Backlog*, garantindo que ele seja visível, transparente e claro para todos, e por decidir o que deve ser construído a seguir.

(A) *Scrum Master*.
(B) *Development Team*.
(C) *Stakeholder*.
(D) *Product Owner*.
(E) *Release Train Engineer* (RTE).

45

Ao estilizar um *website* responsivo, o desenvolvedor precisa de flexibilidade no layout, garantindo que o cabeçalho (<header>) ocupe toda a largura disponível e que seus itens internos (logotipo, menu e barra de busca) sejam distribuídos horizontalmente com espaçamento igual entre eles. Além disso, o logotipo deve permanecer fixo no canto esquerdo, enquanto o menu e a barra de busca devem se alinhar à direita, ocupando o espaço restante.

Assinale a opção que indica a combinação de propriedades CSS mais adequada para alcançar a distribuição horizontal flexível e o espaçamento igual dentro do <header>, e o valor da propriedade que deve ser aplicado ao item de menu ou barra de busca para que ele ocupe todo o espaço intermediário, empurrando o restante dos elementos para a direita.

(A) *display: grid no <header>; grid-template-areas* no elemento que ocupa o espaço.
(B) *display: flex no <header>; align-items: center* no elemento que ocupa o espaço.
(C) *display: flex no <header>; margin-right:* auto aplicado ao elemento que deve empurrar o restante.
(D) *display: flex no <header>; flex-grow:* 1 aplicado ao elemento que deve ocupar o espaço intermediário.
(E) *display: block no <header>; float: right* aplicado ao elemento que ocupa o espaço.

46

A arquitetura de *software* é importante para a qualidade, sustentabilidade e escalabilidade.

Correlacione os conceitos e padrões listados a seguir às suas respectivas características, finalidades ou princípios de aplicação.

1. Arquitetura Monolítica
2. Arquitetura em camadas (N-Tier)
3. Encapsulamento
4. Qualidade de *Software*
5. Arquitetura de Microsserviços

( ) Princípio de Orientação a Objetos que se refere à capacidade de proteger o estado interno de um objeto e expor apenas uma interface controlada.
( ) Modelo de aplicação que, por ser unificado, geralmente apresenta desafios na escalabilidade granular e na implantação contínua (*Continuous Deployment*).
( ) Foco na separação de responsabilidades (e.g., Apresentação, Lógica de Negócios e Persistência), permitindo que alterações em uma camada não afetem diretamente outras.
( ) Conjunto de práticas e medições que visam garantir que o software atenda aos requisitos implícitos e explícitos do cliente, sendo adequado para o uso.
( ) Estrutura que permite que serviços sejam desenvolvidos por times independentes, utilizando diferentes tecnologias (poliglotismo), e se comunicando via APIs leves.

Assinale a opção que indica a correlação correta, na ordem apresentada.

(A) 3 – 1 – 2 – 4 – 5.
(B) 1 – 5 – 2 – 4 – 3.
(C) 4 – 2 – 3 – 1 – 5.
(D) 3 – 2 – 4 – 1 – 5.
(E) 5 – 1 – 2 – 4 – 3.

47

Em uma organização de desenvolvimento de *software* em larga escala, adotou-se o *Scaled Agile Framework* (SAFe). O time está se preparando para o evento de planejamento do *Program Increment* (*PI Planning*), que define o conteúdo para o próximo incremento de valor.

Durante o planejamento, o time de desenvolvimento precisa se comprometer com a entrega de funcionalidades e estimar o trabalho.

Assinale a opção que indica o produto ou resultado principal (*output*) do evento de *PI Planning* que serve como guia para a execução do trabalho nos próximos *sprints*, e a técnica utilizada pelos times para quantificar o esforço das histórias de usuário durante este evento.

(A) O *Value Stream Map* (VSM) e a técnica de *Affinity Grouping*.
(B) O *Roadmap* de Produto de 5 anos e a técnica de *T-Shirt Sizing*.
(C) Os *Team and Program PI Objectives*, o *Program Board* e a técnica de *Planning Poker*.
(D) O *Sprint Backlog* final e a técnica de *Wideband Delphi*.
(E) O *Release Train Engineer Report* (RTE) e a técnica de MoSCoW.

48

Em um ambiente que adota a cultura DevSecOps, a segurança é integrada em todas as fases do *Secure SDLC*.

Um engenheiro de segurança está automatizando ferramentas para identificar vulnerabilidades. Ele usa uma ferramenta que analisa o código-fonte ou binário sem executá-lo, focando em erros de programação segura e falhas de *design*, e outra que interage com a aplicação em execução (ambiente de *staging* ou teste) para encontrar vulnerabilidades como XSS ou *SQL Injection*.

Assinale a opção que apresenta o termo que define, respectivamente, a análise de segurança que opera sem executar o código-fonte ou binário (focando em padrões inseguros) e a análise de segurança que opera interagindo com a aplicação em tempo de execução.

(A) Análise Manual (MR) e Análise Estática de Código (SAST).
(B) Análise Dinâmica de Código (DAST) e *Penetration Testing*.
(C) Análise Estática de Código (SAST) e Análise Dinâmica de Código (DAST).
(D) Análise de Composição de *Software* (SCA) e Análise Estática de Código (SAST).
(E) Análise Dinâmica de Código (DAST) e Análise de Composição de *Software* (SCA).

49

Em um projeto de transformação digital, o analista está usando a notação BPMN 2.0 para mapear o fluxo de "aprovação de crédito". O processo envolve um sistema automatizado que checa dados do cliente (atividade 1) e, dependendo do *score*, o processo pode ser finalizado (crédito aprovado) ou encaminhado para análise manual (atividade 2). Se a análise manual for concluída, o processo retorna a um ponto onde o cliente é notificado do resultado.

Indique o elemento da notação BPMN que deve ser usado para representar o ponto no fluxo em que o processo se divide com base no resultado do *score* (encaminhando para análise manual ou finalizando a aprovação) e o elemento que deve ser usado para permitir que o fluxo retorne após a análise manual, aguardando um evento (como a notificação) para prosseguir.

(A) *Pool* para a divisão e *Swimlane* para o retorno.
(B) *Sub-processo* para a divisão e *Data Object* para o retorno.
(C) *Gateway* Exclusivo (XOR) para a divisão e *Task* (Tarefa) para o retorno.
(D) *Gateway* Paralelo (AND) para a divisão e *Gateway* Inclusivo (OR) para o retorno.
(E) *Gateway* Exclusivo (XOR) para a divisão e *Intermediate Catching Event* (Evento Intermediário de Captura) para o retorno.

50

Um desenvolvedor utiliza o *framework Spring Boot* para construir uma API REST que gerencia o recurso *Produto*. É necessário implementar a operação de exclusão de um produto específico através de seu identificador único. A API deve seguir os princípios de *Statelessness* e utilizar a semântica de métodos HTTP para representar a ação.

Assinale a opção que indica o método HTTP que deve ser utilizado no *endpoint* RESTful para representar a exclusão do recurso *Produto* e a *annotation* do *Spring Web* que o desenvolvedor deve usar na *controller* para mapear esse método HTTP a uma função Java.

(A) Método PUT; *Annotation @PutMapping.*
(B) Método POST; *Annotation @PostMapping.*
(C) Método GET; *Annotation @GetMapping.*
(D) Método DELETE; *Annotation @DeleteMapping.*
(E) Método PATCH; *Annotation @PatchMapping.*

Infraestrutura Tecnológica

51

Uma aplicação crítica em Kubernetes, monitorada com Prometheus, Grafana, Loki e Jaeger (*OpenTelemetry*), apresenta um disparo em sua latência de cauda (p99), que saltou de 200 ms para 2000 ms. No entanto, a latência média segue estável em ~300 ms, sem qualquer alteração na taxa de erros. O *Service Level Objective* (SLO) de performance da aplicação é p95 < 500 ms.

Simultaneamente, a equipe de FinOps alerta para um aumento de 40% nos custos de armazenamento, impulsionado por um volume excessivo de logs de nível DEBUG nas últimas 24 horas.

Considerando a integração dos pilares de observabilidade (métricas, *logs, traces*), o SLO definido e o impacto financeiro (FinOps), assinale a afirmativa correta.

(A) Tratar como latência de cauda. Filtrar *traces* > 1s no Jaeger para identificar *spans* lentos (BD/APIs). Usar *trace_id* no Loki para inspecionar os logs DEBUG associados. Para FinOps, habilitar *tail-based sampling* (capturar 100% dos traces lentos) e reverter o nível de log da aplicação para INFO.
(B) A anomalia no p99 sugere violação do SLO, caracterizando quebra de SLA. A ação imediata é executar *rollback* via kubectl, aumentar o *replicas count* (HPA) para absorver a carga e, preventivamente, investigar a rede física com polling SNMP mais agressivo nos *switches* do datacenter.
(C) A estabilidade da média indica que os alertas estão mal configurados. Ajustar o SLO para se basear na latência média (p50), que reflete melhor o usuário comum. Para resolver o FinOps, pausar o *distributed tracing* (Jaeger) em produção, removendo o *overhead* de coleta e o custo de amostragem.
(D) O SLO (p95) e a média estão saudáveis; o p99 é um *outlier* não prioritário. Focar no FinOps: aplicar *head-based sampling* de 1% no OpenTelemetry e reduzir a ingestão de logs no Loki. A economia de custos deve ser a ação principal e imediata para normalizar os gastos do projeto.
(E) O p99 alto e o excesso de logs DEBUG indicam contenção de recursos (CPU ou I/O) nos *nodes*. A ação é alocar mais recursos, aumentando *requests/limits* de CPU e Memória dos *pods* e escalando verticalmente o *cluster*. O custo de FinOps é secundário e deve ser tratado após o incidente.

52

Um órgão estadual está implementando arquitetura SASE (*Secure Access Service Edge*) para modernizar a segurança de rede e o acesso em contexto de força de trabalho híbrida e a adoção de aplicações SaaS. A solução proposta integra SD-WAN, CASB, ZTNA e FWaaS em plataforma *cloud-native.*

Um auditor interno questiona a arquitetura, citando que o órgão já possui *firewall* de borda tradicional, VPN IPsec para acesso remoto e *proxy web on-premises.*

Nesse contexto, assinale a opção que apresenta corretamente as limitações da arquitetura tradicional e os benefícios da abordagem SASE.

(A) A arquitetura tradicional mantém perímetro definido e inspeção centralizada, mas SASE elimina a necessidade de *backhauling* de tráfego SaaS através do datacenter (*hairpinning*). Entretanto, SASE exige que todo tráfego corporativo seja roteado por um único PoP regional para garantir consistência de políticas, o que pode gerar latência similar ao modelo VPN tradicional.

(B) VPN tradicional concede acesso em nível de rede *(layer* 3) independente de contexto de sessão, enquanto SASE com ZTNA provê acesso microssegmentado por aplicação baseado em identidade contínua. Porém, SASE depende exclusivamente de DLP em nuvem (CASB), tornando desnecessárias soluções *on-premises* de prevenção de vazamento de dados e classificação de informações sensíveis.

(C) O modelo perimetral tradicional força *hairpinning* de tráfego SaaS para inspeção centralizada e VPN IPsec provê acesso amplo à rede interna. SASE distribui controles de segurança em PoPs próximos aos usuários, implementa ZTNA com acesso contextual por aplicação, oferece visibilidade/DLP em SaaS via CASB, permite *breakout* local de tráfego via SD-WAN e consolida políticas através de FWaaS unificado.

(D) *Firewall* tradicional e *proxy on-premises* oferecem inspeção profunda adequada, mas SASE agrega CASB para descoberta de Shadow IT e ZTNA para substituir VPN. A principal vantagem é que SD-WAN em arquitetura SASE elimina a necessidade de *links* MPLS, mas mantém topologia *hub-and-spoke* com inspeção centralizada obrigatória para conformidade regulatória em órgãos públicos.

(E) SASE permite consolidação de fornecedores e redução de *appliances* físicos, mas o modelo de segurança permanece baseado em perímetro de rede confiável, apenas transferido para *cloud*. O ZTNA em SASE funciona como VPN SSL melhorada com MFA, mantendo lógica de confiança implícita pós-autenticação, enquanto CASB apenas replica funcionalidades de *proxy web* existente para tráfego HTTPS.

53

No contexto de automação e integração via API REST em *scripts* Python com a biblioteca *requests*, uma API exige que o *token* de acesso seja enviado no cabeçalho HTTP *Authorization* usando o esquema *Bearer.*

A assinale a opção cujo trecho envia corretamente o *token* em uma requisição GET.

(A)
```
meu_ _token = "xyz123"
x = {"Authorization": f"Bearer {meu_token}"}
y = requests.get(url, headers=x)
```

(B)
```
meu_token = "xyz123"
x = {"Authorization": f"Bearer {meu_token}"}
y = requests.get(url, params=x)
```

(C)
```
meu_token = "xyz123"
x = {"Authorization": meu_token}
y = requests.get(url, headers=x)
```

(D)
```
meu_token = "xyz123"
x = {"access_token": meu_token}
y = requests.get(url, params=x)
```

(E)
```
meu_token = "xyz123"
x = {"Authentication": f"Bearer {meu_token}"}
y = requests.get(url, headers=x)
```

54

Um órgão público está planejando a contratação de serviços de desenvolvimento de sistema de auditoria com recursos de Inteligência Artificial.

O gestor do contrato questiona a aplicabilidade da Instrução Normativa SGD/ME nº 01/2019 e da Instrução Normativa ME nº 40/2020.

Com base nesse contexto, assinale a opção que apresenta corretamente o escopo e a aplicação dessas normativas.

(A) A IN SGD/ME 01/2019 aplica-se exclusivamente a contratações de infraestrutura e recursos computacionais em nuvem, enquanto a IN 40/2020 regulamenta contratações de soluções de TIC, incluindo desenvolvimento de software customizado. Ambas devem ser observadas nessa contratação.

(B) A IN SGD/ME 01/2019 estabelece o processo de contratação de soluções de TIC e aplica-se a desenvolvimento de sistemas, exigindo Estudo Técnico Preliminar, Análise de Riscos e Documento de Oficialização da Demanda. A IN 40/2020 trata de uso de recursos de TIC pelo Poder Executivo Federal e não se aplica diretamente a Estados.

(C) A IN SGD/ME 01/2019 regulamenta contratações de TIC no âmbito federal e estabelece fases de Planejamento da Contratação, Seleção do Fornecedor e Gestão do Contrato. A IN 40/2020 disciplina exclusivamente contratações de serviços na modalidade de computação em nuvem e não se aplica a desenvolvimento de *software.*

(D) A IN SGD/ME 01/2019 é aplicável apenas a órgãos da administração pública federal direta, autárquica e fundacional, não vinculando Estados. A IN 40/2020 estabelece governança de TIC e pode servir como referência de boas práticas para Estados, mas não tem força normativa obrigatória em âmbito estadual.

(E) Ambas as normativas se aplicam obrigatoriamente a Estados, Distrito Federal e Municípios por força de normas gerais de licitações. A IN 01/2019 deve ser seguida integralmente em todas as fases da contratação, e a IN 40/2020 estabelece requisitos mínimos de segurança da informação para contratações de TIC.

55

No contexto de Kubernetes gerenciado e serviços de contêiner nas nuvens AWS, Azure e GCP, avalie as afirmativas a seguir.

I. No *Azure Kubernetes Service* (AKS), o plano de controle é gerenciado pela Microsoft sem cobrança direta; os custos concentram-se em *pools* de nós e recursos consumidos (*compute, storage,* rede), podendo haver cobrança adicional apenas se contratado SLA específico de *Uptime* do *control plane*.

II. No *Google Kubernetes Engine* (GKE) *Autopilot*, é permitido criar *DaemonSets* para agentes que rodem em todos os nós e executar *pods* privilegiados, desde que configuradas as *capabilities* adequadas.

III. No Amazon EKS utilizando AWS *Fargate*, não há gerenciamento de nós pelo cliente e *DaemonSets* não são suportados; além disso, a cobrança do *control plane* do EKS permanece ativa por *cluster,* independentemente do uso de *Fargate.*

Está correto o que se afirma em

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

56

Um órgão estadual está migrando sua infraestrutura de telefonia de um sistema PBX tradicional baseado em *hardware* para uma solução de Comunicações Unificadas em nuvem (UCaaS).

Considerando os protocolos e componentes de uma arquitetura de telefonia IP, analise as afirmativas a seguir.

I. O protocolo SIP opera na camada de aplicação e utiliza portas TCP/UDP 5060 (não criptografado) ou 5061 (TLS) para sinalização, sendo responsável por estabelecer, modificar e terminar sessões de comunicação, mas não transporta o áudio da chamada.

II. Implementação de QoS (*Quality of Service*) com priorização de tráfego VoIP por meio de DSCP (*Differentiated Services Code Point*) é essencial para garantir baixa latência, *jitter* reduzido e minimizar perda de pacotes, recomendando-se latência inferior a 150ms para chamadas de voz.

III. Em uma arquitetura UCaaS, o SIP Trunk conecta a infraestrutura local (*on-premises*) ao provedor de serviços em nuvem, e o componente *Session Border Controller* (SBC) é responsável por segurança (proteção contra *DoS, toll fraud),* interoperabilidade entre diferentes redes SIP e travessia de NAT.

Está correto o que se afirma em

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

57

No contexto de Kubernetes gerenciado e serviços de contêiner nas nuvens AWS, Azure e GCP, avalie as afirmativas a seguir.

( ) Na nuvem pública, os recursos são obrigatoriamente *multi-tenant* e sempre acessíveis pela Internet pública, não havendo opção de isolamento dedicado ou conectividade privada.

( ) Na modalidade PaaS, a organização contratante é responsável por configurar o sistema operacional em que a aplicação é executada.

( ) A computação *serverless* requer manter, em paralelo, uma versão *on-premises* da aplicação para a continuidade de serviços.

( ) Cargas de trabalho (*workloads*) com alto grau de processamento paralelo tendem a obter melhor desempenho em instâncias com GPU, quando o *software* é compatível.

As afirmativas são, respectivamente,

(A) F – F – F – V.
(B) F – V – V – F.
(C) V – F – V – F.
(D) V – V – F – F.
(E) V – V – V – F.

58

Um órgão estadual implementará monitoramento de transporte escolar em veículos que operam em zona rural com conectividade móvel intermitente.

Cada veículo terá computador embarcado com capacidade de processamento local, sensores IoT (GPS e acelerômetro) e câmeras.

Os pátios municipais possuem servidores locais com conectividade Wi-Fi.

O sistema deve detectar eventos críticos de segurança (porta aberta em movimento, frenagens bruscas, desvios de rota) com resposta imediata ao motorista, operar autonomamente por períodos prolongados sem conectividade externa, e transmitir apenas dados essenciais pela rede móvel limitada.

Considerando os conceitos de *edge computing, fog computing* e *cloud computing* em arquitetura de processamento distribuído, assinale a afirmativa correta.

(A) *Edge computing* processa dados centralizadamente na nuvem, *fog computing* nos servidores dos pátios, e a integração entre as camadas exige conectividade permanente. A detecção de eventos críticos depende da transmissão de vídeo para os servidores *fog*, que analisam e retornam alertas aos veículos.

(B) *Fog computing* substitui completamente o *edge computing* ao centralizar todo processamento nos servidores dos pátios municipais, eliminando a necessidade de capacidade computacional nos veículos. *Edge computing* é aplicável apenas a sensores simples que não processam dados localmente.

(C) *Edge computing* e *fog computing* são sinônimos que descrevem processamento em nuvem distribuída geograficamente. Ambos dependem de conexão contínua com datacenters centrais para funcionar, diferenciando-se apenas pela localização física dos servidores em diferentes regiões.

(D) *Edge computing* processa dados localmente nos veículos com resposta imediata e operação autônoma, *fog computing* agrega e processa dados de múltiplos veículos nos servidores dos pátios, e *cloud computing* realiza análises históricas e complexas centralizadamente. As três camadas formam arquitetura hierárquica complementar.

(E) *Cloud computing* é a única camada necessária para o sistema, pois tecnologias atuais de *streaming* de vídeo e conectividade 5G permitem processamento centralizado com latência desprezível. *Edge* e *fog computing* são conceitos obsoletos substituídos por redes de alta velocidade.

59

Durante um incidente crítico (P1) afetando o sistema de pagamentos de uma instituição de ensino, o *Service Desk* registrou:

- Detecção: 14:00 (monitoramento automático);
- Registro: 14:05 (*ticket* aberto);
- Categorização: 14:10 (financeiro/crítico);
- Escalação: 14:15 (*time* de sustentação);
- Resolução temporária: 14:45 (*workaround* aplicado);
- Resolução definitiva: 16:00 (*patch* aplicado).

Com base nos horários acima e no contexto das métricas de gerenciamento de incidentes, analise as afirmativas a seguir.

I. O MTTA corresponde a um terço do TTE e ambos foram inferiores a 20 minutos.

II. A diferença entre TTE e MTTA é igual ao intervalo entre Categorização (14:10) e Escalação (14:15).

III. A diferença de tempo decorrido entre o MTTR o MTTA é inferior a 115 minutos.

IV. O MTTR pode ser expresso como a soma do TTR e o tempo de aplicação do patch (Δ), em que esse tempo (Δ) corresponde a 62,5% do próprio MTTR.

Está correto o que se afirma em

(A) I e IV, apenas.

(B) II e III, apenas.

(C) I, II e III, apenas.

(D) II, III e IV, apenas.

(E) I, II, III e IV.

60

Um arquiteto de infraestrutura está revisando a adoção de *Infrastructure as Code* (IaC) com *Terraform* em um projeto de modernização. A equipe já criou módulos reutilizáveis e utiliza *workspaces* para isolar ambientes (*dev/hom/prod*).

Ao inspecionar o repositório, foram encontrados os seguintes arquivos: main.tf, variables.tf, terraform.tfstate, terraform.tfvars e .terraform.lock.hcl

Considerando as melhores práticas de segurança e gerenciamento de estado em Terraform, assinale a afirmativa correta.

(A) O arquivo .terraform.lock.hcl deve ser incluído no .gitignore para evitar conflitos entre ambientes, e o *state file* deve ser armazenado em *backend* remoto com *state locking* habilitado utilizando *DynamoDB* ou equivalente.

(B) O arquivo terraform.tfstate deve ser versionado no Git para garantir rastreabilidade de mudanças, enquanto terraform.tfvars contendo credenciais deve ser armazenado em *secrets manager* e referenciado via variáveis de ambiente.

(C) Os arquivos terraform.tfstate devem ser excluídos do controle de versão e armazenados em *backend* remoto com criptografia, enquanto .terraform.lock.hcl deve ser versionado para garantir consistência de versões de *providers* entre execuções.

(D) O arquivo variables.tf contendo valores sensíveis deve ser criptografado com GPG antes do *commit*, e múltiplos *state files* podem compartilhar o mesmo *backend S3 bucket* sem isolamento de *paths* desde que utilizem *workspace* diferente.

(E) O *state file* local deve ser mantido apenas em ambientes de desenvolvimento, e a produção deve utilizar *backend* remoto sem versionamento, priorizando performance de leitura através de *cache* local do Terraform.

Questão Discursiva (Tarde)

Leia o texto a seguir.

> A Controladoria Geral do Estado (CGE) lida com uma ampla e complexa teia de dados sensíveis e críticos, abrangendo desde informações financeiras e orçamentárias até dados pessoais de servidores e cidadãos, essenciais para a auditoria e transparência pública. A ausência de uma Arquitetura de Dados clara e o desconhecimento dos *Metadados* inibem a capacidade do gestor de dados de monitorar a qualidade, de garantir a conformidade regulatória, e de padronizar o vocabulário de negócio. Isso, por sua vez, impacta a confiabilidade das evidências usadas em processos de *accountability* de acordo com a Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018 - Art. 23 e seguinte, e Art. 6º).
>
> Segundo o Tribunal de Contas da União (TCU), "*A gestão inadequada dos dados prejudica, ainda, a transformação digital dos serviços prestados aos cidadãos, a abertura de dados públicos e o controle social, além de aumentar o risco de vazamento ou comprometimento da privacidade de dados…. A governança de dados é essencial para a administração pública, pois garante a qualidade, o compartilhamento e a transparência das informações, permitindo decisões mais embasadas, políticas públicas mais eficazes e maior confiança da sociedade nas instituições governamentais*."
>
> Fonte: https://sites.tcu.gov.br/listadealtorisco/governanca_e_gestao_de_dados_governamentais.html

Nesse contexto de alta exigência regulatória e analítica, a Governança de Dados é vital para transformar dados brutos em ativos estratégicos e confiáveis para a missão de controle do Estado.

A partir do texto apresentado e considerando a missão da Controladoria Geral do Estado, **discorra sobre a importância e os componentes da Governança de Dados,**

a) explicando a função e a interrelação entre Arquitetura de Dados e *Metadados*.

b) diferenciando as dimensões da Qualidade de Dados de Unicidade e Consistência, fornecendo um exemplo prático de violação de cada uma delas em um contexto de dados fiscais

c) apresentando o conceito básico de Governança de Dados.

d) justificando como a implementação de um programa de Governança de Dados pode mitigar os riscos de auditoria e melhorar a *accountability* (prestação de contas) no Setor Público.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30

31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60

Realização