

-- CONHECIMENTOS ESPECÍFICOS --

A respeito de conceitos básicos de segurança da informação, de métodos de autenticação e autorização, de ameaças e vulnerabilidades em aplicações e de segurança em aplicativos *web*, julgue os seguintes itens.

- 51 No contexto do conjunto de *frameworks*, guias e boas práticas da OWASP aplicáveis a testes em aplicações *web*, a análise de segurança inclui a identificação sistemática de pontos de entrada, a manipulação controlada de dados fornecidos à aplicação e a observação de suas respostas, com o objetivo de evidenciar vulnerabilidades, tais como injeções, falhas de controle de acesso e exposição indevida de dados.
- 52 No OAuth 2.0, o uso do fluxo Authorization Code com PKCE garante a confidencialidade dos dados transmitidos entre cliente e servidor de recursos, ao impedir a interceptação do conteúdo das comunicações durante o acesso aos recursos protegidos.
- 53 O não repúdio em segurança da informação constitui uma propriedade relacionada à disponibilidade das informações, que assegura que ações realizadas por usuários permaneçam acessíveis para verificação futura.
- 54 A vulnerabilidade de LDAP *injection* decorre da execução de consultas LDAP por meio de protocolos não criptografados, o que permite a interceptação e a alteração das requisições durante a comunicação com o diretório.
- 55 Em arquiteturas baseadas em OpenID Connect, a autenticação de múltiplos fatores integra o processo de autenticação no provedor de identidade, sendo refletida no ID Token, que pode conter informações sobre o contexto de autenticação, como *acr* e *amr*, permitindo ao cliente avaliá-las como insumo para decisões de autorização.

No que se refere à prevenção e combate a ataques a redes de computadores, a sistemas criptográficos simétricos, a *antispam* e a *firewalls*, julgue os itens a seguir.

- 56 Serviços de *journaling* em sistemas de *email* destinam-se ao bloqueio e à filtragem de mensagens de *spam*, impedindo sua entrega aos usuários, e constituem o principal mecanismo *antispam* desses sistemas.
- 57 *Firewalls* com inspeção de estado mantêm tabelas de estado das conexões e, com base nessas informações, correlacionam os fluxos de ida e retorno, permitindo o reconhecimento de tráfego pertencente a sessões ou fluxos previamente estabelecidos por meio da associação a entradas existentes na tabela de estados, inclusive quando utilizam portas efêmeras dinamicamente alocadas, tipicamente no lado do cliente.
- 58 A implementação de DNSSEC em um domínio garante proteção contra ataques de DNS *spoofing*, ao assegurar a autenticidade das respostas DNS por meio de validação criptográfica.
- 59 O emprego de algoritmos robustos de criptografia simétrica dispensa mecanismos de distribuição segura de chaves, pois a segurança das chaves decorre do próprio processo de cifragem dos dados.
- 60 A adoção combinada de controles em múltiplas camadas, com limitação de taxa, filtragem de tráfego e uso de redes de distribuição de conteúdo, constitui abordagem eficaz para a mitigação e a redução do impacto de ataques de negação de serviço distribuído (DDoS).

Acerca de assinatura e certificação digital e da proteção de dados pessoais, julgue os itens que se seguem.

- 61 Nos termos da Lei Geral de Proteção de Dados Pessoais, o tratamento de dados pessoais pode ser realizado pela administração pública quando necessário à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres.
- 62 No processo de verificação de uma assinatura digital em infraestrutura de chaves públicas, além da validação da cadeia de certificação, realiza-se a checagem do *status* de revogação do certificado, por meio de mecanismos como CRL ou OCSP, bem como da vigência do certificado no instante da assinatura.

Acerca de arquiteturas e topologias de redes de computadores, de operação de protocolos e do endereçamento IP, de arquitetura e operação do gerenciamento de redes e do funcionamento da camada de enlace da infraestrutura, julgue os itens a seguir.

- 63 O SNMPv3 destaca-se de versões mais antigas por trazer recursos de segurança embutidos no modelo USM, o que garante autenticação e criptografia para proteger a comunicação entre gerentes e agentes.
- 64 Quando atua na camada 2 de uma rede local, o papel principal de um *switch* é ler o endereço MAC de destino no quadro *ethernet* e enviar essa informação apenas para a porta onde o equipamento correto está ligado.
- 65 Para distribuir endereços IPv4 na rede, o DHCP adota o protocolo TCP como padrão, pois isso garante que os pacotes de concessão de IP cheguem aos computadores de forma confiável e na ordem certa.
- 66 Nas redes definidas por *software* (SDN), separar o plano de controle, que decide as rotas, do plano de dados, que encaminha os pacotes, é o que possibilita gerenciar e programar toda a infraestrutura de forma centralizada.

A respeito de segurança em redes e tratamento de incidentes, das propriedades avançadas de algoritmos criptográficos, da gestão de processos em sistemas operacionais Linux e da arquitetura lógica em serviços de diretório, julgue os itens seguintes.

- 67 Dentro do Active Directory, a unidade organizacional funciona como o principal contêiner físico de *hardware*, servindo exclusivamente para agrupar servidores em *racks* diferentes, sem poder armazenar contas de usuários ou grupos.
- 68 Ao emitir um certificado digital no padrão ICP-Brasil, a autoridade certificadora valida o documento, assinando-o com a chave privada do próprio usuário, o que garante o não repúdio de ponta a ponta.
- 69 No ataque DDoS conhecido como SYN Flood, o invasor derruba o serviço ao disparar milhares de pacotes com a *flag* FIN ativada, o que acaba esgotando rapidamente a tabela de roteamento do *firewall* do alvo.
- 70 No RedHat Linux 7 e versões mais recentes, a utilização do comando `systemctl mask` é uma forma mais agressiva que o `disable` para impedir que um serviço se inicie sem que o usuário o queira, pois ele vincula a unidade diretamente ao `/dev/null`.

Julgue os itens a seguir, no que diz respeito a conceitos arquiteturais de *cloud computing* e virtualização, à otimização de topologias para sistemas de missão crítica, à otimização e às rotinas das tecnologias de armazenamento e a ciclos de lançamento e metodologias de automação em DevOps.

- 71 Nas esteiras de DevOps, a integração contínua (CI) representa a etapa final do ciclo, sendo a responsável por fazer a implantação automática da aplicação em produção, sem a necessidade de processos de *build* ou testes prévios.
- 72 Quando um servidor de aplicação recebe muitas requisições simultâneas, usar um *pool* de conexões com o banco de dados ajuda a poupar recursos, pois evita o peso e a lentidão decorrentes dos atos de abrir e fechar conexões TCP continuamente.
- 73 Para ambientes críticos de *data centers*, os hipervisores do tipo 2 (*bare-metal*) são uma excelente escolha, pois são executados diretamente no *hardware* do servidor, sem que haja a necessidade de sistema operacional por baixo.
- 74 O *backup* incremental é caracterizado por salvar apenas os arquivos que foram criados ou modificados desde o último *backup* que tenha sido feito, independentemente de esse *backup* anterior ter sido completo ou também incremental.

Julgue os itens a seguir, relativos aos fundamentos e à gestão de sistemas operacionais.

- 75 No gerenciamento de entrada e saída, o uso de *spooling* em impressoras corporativas garante que cada processo administrativo seja atendido em ordem de chegada, sem possibilidade de reordenação das filas de impressão.
- 76 Na gestão de processos, o escalonamento por prioridade garante que processos administrativos críticos, como rotinas de *backup*, sempre sejam executados antes de qualquer outro processo, independentemente da carga do sistema.
- 77 Em ambiente corporativo, o sistema operacional atua como intermediário entre os usuários e os recursos de *hardware*, garantindo que aplicações administrativas, como sistemas de folha de pagamento, possam ser executadas sem que o analista precise lidar diretamente com instruções de baixo nível da CPU.
- 78 Em sistemas administrativos que utilizam memória virtual, o mecanismo de paginação permite que programas maiores do que a memória física disponível sejam executados, mas implica possíveis quedas de desempenho devido ao fenômeno conhecido como *thrashing*.

Julgue os itens seguintes, relativos à instalação, configuração e administração de sistemas operacionais.

- 79 Durante a instalação de um servidor corporativo, a configuração de partições no RedHat Enterprise Linux 8 pode ser realizada de forma automática pelo instalador (Anaconda), porém, em ambientes administrativos críticos, é recomendável que o analista configure manualmente pontos de montagem como */var* e */home*, visando à maior segurança e ao controle de recursos.
- 80 Em um ambiente corporativo, tanto no Windows Server 2019 quanto no RedHat Enterprise Linux 8, é possível configurar serviços de rede, como servidores *web*, de forma que sejam inicializados automaticamente junto ao sistema operacional, garantindo disponibilidade imediata após reinicializações.
- 81 No Windows Server 2019, a função ADFS (Active Directory Federation Services) é utilizada para gerenciar permissões de acesso a arquivos compartilhados em pastas locais, garantindo que apenas usuários autenticados possam abrir documentos administrativos.

No que concerne aos serviços de diretório e à sua interoperabilidade, julgue os itens que se seguem.

- 82 No Active Directory, a criação de unidades organizacionais (OUs) tem o objetivo principal de armazenar objetos de diretório de forma hierárquica, mas impede a aplicação de políticas de segurança específicas a grupos de usuários.
- 83 O protocolo LDAP é utilizado exclusivamente em sistemas Linux, sendo incompatível com ambientes Windows Server, o que inviabiliza sua interoperabilidade em redes corporativas heterogêneas.
- 84 Em uma empresa que utiliza Windows Server 2019 para autenticação de usuários, e RedHat Enterprise Linux 8 para serviços de aplicação, é possível configurar interoperabilidade entre Active Directory e LDAP, permitindo que usuários autenticados no domínio Windows acessem serviços Linux sem necessidade de múltiplas credenciais.
- 85 Em um ambiente corporativo, o Active Directory permite centralizar a autenticação de usuários e a aplicação de políticas de segurança, como restrição de acesso a pastas administrativas, facilitando a gestão por parte do analista de sistemas.

Acerca da interoperabilidade de sistemas, da arquitetura orientada a serviços (SOA) e dos *web services*, julgue os itens a seguir.

- 86 Em arquitetura orientada a serviços (SOA), a integração entre os sistemas requer que o consumidor e o provedor do serviço sejam desenvolvidos na mesma linguagem de programação, a fim de garantir a padronização das mensagens trafegadas.
- 87 Em arquitetura orientada a serviços (SOA), a utilização de *web services* tipicamente viabiliza a interoperabilidade entre sistemas heterogêneos ao adotar padrões abertos de comunicação e contratos de serviço que ocultam os detalhes de implementação e a linguagem de programação subjacente.
- 88 No design avançado de *web services*, enquanto a abordagem baseada em SOAP utiliza contratos estáticos e predefinidos via WSDL para expor suas operações, um serviço estritamente aderente às restrições do estilo arquitetural REST incorpora a restrição HATEOAS.

Considerando os conceitos fundamentais de arquitetura e linguagem orientadas a objetos, bem como o desenvolvimento e a integração via interfaces de programação de aplicações (API), julgue os itens subsequentes.

- 89 Na arquitetura orientada a objetos, o polimorfismo baseado em ligação dinâmica (*late binding*) faz com que a implementação invocada de um método em tempo de execução seja determinada pelo tipo real do objeto instanciado, e não apenas pelo tipo estático da variável de referência.
- 90 Uma interface de programação de aplicações (API) estabelece o contrato de comunicação entre diferentes componentes de *software*, incluindo em sua especificação formal o código-fonte dos algoritmos responsáveis pelo processamento interno das requisições.
- 91 No desenvolvimento de interfaces de programação de aplicações (API) baseadas no estilo arquitetural REST, o servidor deve obrigatoriamente manter o estado da sessão do cliente entre as requisições, visando garantir a integridade dos dados trafegados.
- 92 Na arquitetura orientada a objetos, o encapsulamento é o princípio que visa ocultar os detalhes de implementação interna e proteger o estado de um objeto, restringindo o acesso direto aos seus atributos e mediando a interação do meio externo por meio de métodos públicos definidos.

Com o objetivo de modernizar seus sistemas de atendimento ao cidadão, determinado órgão público está reestruturando a infraestrutura e o *design* de sua plataforma *web* principal. O projeto de modernização prevê a adoção de padrões arquiteturais no *front-end* para melhorar a responsividade, além de uma topologia de *back-end* que separa rigorosamente do processamento intensivo de regras de negócio transacionais o recebimento de requisições e a entrega de conteúdo estático.

Considerando essa situação hipotética, julgue os itens seguintes, relativos a conceitos fundamentais de arquitetura de aplicações para ambiente *web*, servidores *web* e servidores de aplicação.

- 93 Na topologia de *back-end* proposta na situação hipotética, a adoção do padrão API Gateway estabelece um ponto único de entrada para as requisições provenientes do *front-end*.
- 94 Na arquitetura proposta para o portal, a entrega eficiente de conteúdo estático decorre do processamento, pelo servidor *web*, de requisições associadas ao mapeamento de URLs de recursos estáticos para arquivos servidos localmente.
- 95 Ao adotar a arquitetura *single page application* (SPA) no *front-end* do portal, a responsividade será alcançada por meio do recarregamento completo da página no navegador a cada interação do cidadão com o sistema.
- 96 Na topologia de *back-end* pretendida para o novo portal, a separação rigorosa de responsabilidades será alcançada se os servidores *web* forem configurados para executar o processamento intensivo das regras de negócio transacionais, delegando aos servidores de aplicação a entrega exclusiva do conteúdo estático.

Acerca da metodologia BSC (*balanced scorecard*), do planejamento estratégico de TI e de aspectos relacionados a cibersegurança e continuidade de negócios, julgue os itens subsequentes.

- 97 No âmbito do planejamento governamental de TI, o Plano Diretor de Tecnologia da Informação (PDTI) é o instrumento responsável por estabelecer as diretrizes estratégicas de longo prazo e a visão de futuro da organização, cabendo ao Plano Estratégico de Tecnologia da Informação (PETI) a função estritamente operacional de listar as necessidades de contratação e o cronograma detalhado de execução de projetos para o biênio vigente.
- 98 No contexto do Plano Estratégico de Tecnologia da Informação (PETI) alinhado ao negócio, a metodologia do BSC supera a abordagem puramente contábil por meio de análise multidimensional, na qual a perspectiva de aprendizado e crescimento foca a infraestrutura intangível, como o capital humano, os sistemas de informação e a cultura organizacional, servindo de base para a excelência nos processos internos.
- 99 No âmbito da cibersegurança e da continuidade de negócios, o princípio da integridade refere-se à garantia de que a informação esteja acessível e utilizável por pessoas autorizadas sempre que necessário, enquanto a disponibilidade foca a proteção da informação contra modificações não autorizadas ou acidentais, assegurando a precisão dos dados durante todo o seu ciclo de vida.

Julgue os itens a seguir, a respeito de gestão de projetos, gestão de processos e metodologias ágeis.

- 100 No método Kanban, a aplicação de limites de trabalho em progresso (*WIP limits*) visa maximizar a capacidade de multitarefa da equipe de auditoria de TI, permitindo que o fluxo de entrega seja acelerado ao iniciar o maior número possível de itens simultaneamente, o que converge com o princípio da adaptabilidade e resiliência do PMBOK 7.^a edição, ao estimular a resposta rápida a diversas frentes de trabalho.
- 101 No *framework* Scrum, embora tanto o *product owner* quanto o *scrum master* colaborem para o sucesso do projeto, o primeiro é o responsável por maximizar o valor do produto resultante do trabalho do time Scrum, sendo a conta única pelo gerenciamento eficaz do *product backlog*, e o segundo atua como líder que serve ao time e à organização, focando a remoção de impedimentos e a eficácia do time através da promoção da teoria e prática do Scrum.
- 102 No contexto da gestão organizacional, os projetos são empreendimentos temporários destinados a criar um produto, serviço ou resultado exclusivo, podendo utilizar *frameworks* como o Scrum para lidar com incertezas; e os processos representam fluxos de trabalho contínuos e repetitivos, como os mapeados em BPMN, que visam à entrega padronizada de valor e à melhoria contínua, através de métodos como o Kanban para otimizar o fluxo.

Julgue os itens seguintes, a respeito de governança corporativa de TI.

- 103 De acordo com os princípios da ISO/IEC 38500 e com a estrutura do COBIT 2019, a governança de TI é responsável por avaliar, direcionar e monitorar o uso da tecnologia para atingir os objetivos da organização, e a gestão foca no planejamento, execução e controle das atividades operacionais, em conformidade com o direcionamento estabelecido pelo corpo diretivo.
- 104 No âmbito do COBIT 2019, os fatores de *design* são componentes fixos que determinam a priorização dos objetivos de governança e gestão sem sofrer influência da cascata de objetivos.

No que se refere a contratações de TI no setor público, à gestão de riscos de TI, à gestão de serviços de TI e à gestão de processos, julgue os itens que se seguem.

- 105 De acordo com as diretrizes da norma ISO 31000, o processo de tratamento de riscos restringe-se às incertezas que possam gerar impactos negativos à organização; a opção de compartilhar o risco é classificada como resposta para eventos de oportunidade; e a redução do risco deve ser aplicada obrigatoriamente a todos os riscos residuais identificados pela auditoria de TI.
- 106 No contexto da gestão de processos de negócio e melhoria contínua, a etapa *check* (verificar) do ciclo PDCA consiste na execução das atividades conforme modelado em BPMN, e a etapa *do* (fazer) constitui o momento exclusivo em que se realizam as auditorias e medições de desempenho para identificar desvios entre o processo planejado e o executado.
- 107 O termo de referência é o documento que deve obrigatoriamente prever um modelo de execução e gestão contratual que vincule o pagamento à entrega de resultados ou produtos mensuráveis, sendo vedada a remuneração baseada exclusivamente no transcurso do tempo ou na mera disponibilidade de pessoal, o que exige a definição clara de critérios de aceitação e indicadores de níveis de serviço para a conformidade do objeto contratado.
- 108 No *framework* ITIL v4, o sistema de valor de serviço (SVS) representa o modelo pelo qual a organização coordena seus diversos componentes e atividades para facilitar a cocriação de valor, integrando elementos como os princípios orientadores, a governança e a melhoria contínua, e tendo como núcleo a cadeia de valor de serviço, que transforma demandas e oportunidades em resultados de valor por meio de um conjunto de atividades interconectadas.

Espaço livre

No que se refere à linguagem Java 21, a processamento concorrente, a ferramentas de automação de infraestrutura, ao ecossistema Spring Boot para *backend* e a padrões de interoperabilidade de sistemas, julgue os itens a seguir.

- 109 Durante a criação de uma infraestrutura como código, o Terraform usa uma abordagem imperativa, na qual o administrador necessita definir a sequência exata de comandos para provisionar os recursos.
- 110 Em serviços *web* baseados em SOAP, o WSDL funciona como o protocolo de transporte binário que leva as mensagens pela rede na camada de aplicação.
- 111 Ao se executar o comando a seguir, o Java cria uma *thread* leve que é gerenciada diretamente pela JVM, sem precisar de um mapeamento exato (1:1) com as *threads* do sistema operacional.

```
Thread.startVirtualThread(() -> processar());
```

- 112 O recurso de autoconfiguração do Spring Boot verifica o `classpath` do projeto para registrar componentes de forma automática, priorizando convenções em vez de configurações manuais.

No que concerne aos componentes de arquitetura do Kubernetes, a arquiteturas de mensageria e processamento de eventos e a padrões de arquitetura e microsserviços, julgue os itens que se seguem.

- 113 No Kubernetes, o componente Kubelet tem a função de organizar e de agendar onde os *pods* serão executados.
- 114 Quando um sistema usa microsserviços com bancos de dados separados, é necessário adotar padrões como o Saga para lidar com transações que envolvem vários serviços e garantir que os dados fiquem consistentes no final.
- 115 No Apache Kafka, as mensagens são destruídas e apagadas do servidor assim que o cliente confirma que as leu.
- 116 No Kubernetes, o componente Kubelet é o agente que corre no nó mestre (Control Plane).

Julgue os próximos itens, relativos aos princípios da metodologia de desenvolvimento orientado a testes (TDD), às propriedades ACID em transações de bases de dados, às estruturas lógicas da linguagem PL/SQL e à administração da plataforma Moodle.

- 117 Caso duas transações ocorram simultaneamente, a propriedade de isolamento do ACID previne o acesso aos dados incompletos até que ambas as transações estejam completas.
- 118 Na plataforma Moodle, o perfil padrão de estudante tem permissões apenas de consumo e de interação.
- 119 As Stored Procedures ficam salvas e pré-compiladas direto no servidor de banco de dados, o que permite um processamento mais rápido das informações e diminui a quantidade de dados trafegando pela rede até a aplicação.
- 120 No desenvolvimento orientado a testes (TDD), o programador deve escrever todo o código da funcionalidade antes de criar os testes de unidade que vão validar esse código.