

-- CONHECIMENTOS ESPECÍFICOS --

Julgue os próximos itens, relativos a redes de computadores.

- 49** Na topologia em estrela, todos os dispositivos estão conectados a um único ponto central, geralmente um *switch* ou *hub*.
- 50** *Switches* operam na camada de rede do modelo OSI, decidindo o melhor caminho para o encaminhamento de pacotes.
- 51** O protocolo HTTP é utilizado para transferência de *emails* entre servidores de correio eletrônico e clientes de *email*.
- 52** O protocolo TCP garante a entrega de pacotes de dados na mesma ordem em que foram enviados.

Acerca da configuração e do gerenciamento dos sistemas Linux e Windows, julgue os seguintes itens.

- 53** No Linux, o comando `chmod` é utilizado para modificar as permissões de arquivos e diretórios.
- 54** No Windows, o comando `ipconfig` é utilizado para exibir e configurar informações relacionadas à rede.

No que se refere a virtualização e *containers*, julgue os itens a seguir.

- 55** O Kubernetes não dispõe de mecanismos de balanceamento de carga para distribuir o tráfego de rede entre *containers*.
- 56** No Docker, cada *container* compartilha o mesmo *kernel* do sistema operacional *host*, mas possui seu próprio espaço de usuário isolado.

Com relação à computação em nuvem, julgue os itens subsequentes.

- 57** Na plataforma Azure, é possível configurar máquinas virtuais tanto com o sistema operacional Microsoft Windows Server quanto com distribuições Linux, bem como realizar a administração dessas máquinas por meio do portal Azure, CLI ou PowerShell.
- 58** No modelo de serviço PaaS (plataforma como serviço), o provedor da nuvem gerencia a infraestrutura subjacente, enquanto o cliente é responsável pela gestão do sistema operacional e do *middleware*.
- 59** A computação em nuvem privada permite que recursos de TI sejam utilizados por várias organizações diferentes, oferecendo serviços de maneira compartilhada.
- 60** A escalabilidade automática é uma das principais vantagens da computação em nuvem, pois permite que recursos sejam ajustados dinamicamente conforme a demanda.

Considerando os conceitos de IDS (*intrusion detection systems*) e IPS (*intrusion prevention systems*), julgue os itens a seguir.

- 61** Caso um IPS com capacidade de operar *inline* detecte ataques, esse sistema adotará medidas adicionais para bloqueá-los em tempo real.
- 62** IDS podem ser definidos como um tipo de ferramenta de *software* ou *appliance* capaz de detectar eventos com base em assinatura e em características que os tornam suspeitos na rede sob análise.

No que se refere às características e técnicas de criptografia simétrica e assimétrica, julgue os itens que se seguem.

- 63** De maneira geral, chaves de algoritmos simétricos devem seguir uma propriedade de aleatoriedade com um vetor de inicialização que é conhecido pelo destino da comunicação.
- 64** Na criptografia assimétrica, o algoritmo RSA utiliza chave privada de tamanho fixo, limitado a 1.024 *bits*, e chave pública de tamanho variado (2.048 *bits* ou maior) em função do certificado digital.

Acerca do OAuth2, julgue os próximos itens.

- 65** No OAuth 2, por padrão, os *tokens* de acesso devem ser do tipo JWT.
- 66** OAuth2 é um protocolo de autorização.

Julgue os itens subsequentes, relativos a ataques em aplicações *web* e ao *firewall* pfSense.

- 67** O pfSense não suporta interface gráfica, por isso todos os comandos são feitos por interface de linha de comando, por meio de um *shell*.
- 68** SSRF (*server-side request forgery*) é um tipo de falha que ocorre sempre que aplicativos *web* buscam recursos remotos sem validar a URL fornecida pelo usuário.
- 69** O pfSense baseia-se no sistema operacional FreeBSD, com *kernel* customizado para fazer funções de *firewall* de rede e roteamento.
- 70** XSS (*cross-site scripting*) é um tipo de ataque classificado como *run time execution*, em que binários maliciosos são injetados em campos de aplicação *web*.

Acerca de assinaturas digitais, julgue os itens a seguir.

- 71** Por padrão, assinaturas digitais garantem a confidencialidade dos documentos.
- 72** Técnicas de assinatura digital visam garantir integridade em documentos digitais.

Julgue os próximos itens, a respeito de segurança e auditoria de bancos de dados.

- 73** Ocorre transação confirmada (*commit*) quando há informações suficientes no *log* do banco de dados para garantir que, mesmo se houver falha no sistema, as atualizações da transação serão refeitas.
- 74** Auditoria de banco de dados consiste na revisão de seu *log* para examine de todos os acessos e operações aplicadas a ele durante determinado período.
- 75** Injeção de SQL consiste na inserção, por usuário malicioso, de código escrito em linguagem de *script* no lado do cliente, em vez da inserção de comentário válido, o que faz que o navegador execute esse *script*, que, por sua vez, poderá realizar ações que comprometam a segurança das informações do usuário ou do sistema.

No que se refere à administração de banco de dados, julgue os itens que se seguem.

- 76** Uma instância de um banco de dados SQL compreende a organização lógica dos dados com seus atributos e seus domínios correspondentes.
- 77** O sistema de *backup* de um sistema gerenciador de banco de dados deve fazer cópias do banco de dados para outro disco igual à unidade de armazenamento principal, excetuando-se os *logs*, que devem ser mantidos, por questão de segurança, no mesmo disco.

Julgue os itens subsequentes, no que concerne a bancos de dados NoSQL.

- 78** O nível de consistência de um banco de dados Cassandra somente é considerado ativo quando configurado em um provedor de nuvem.
- 79** Em um banco de dados NoSQL, a exemplo do MongoDB, a replicação melhora a disponibilidade dos dados e pode melhorar o desempenho de leitura, pois as solicitações de leitura geralmente podem ser atendidas em qualquer um dos nós de dados replicados.
- 80** No MongoDB, a fragmentação de documentos na coleção divide documentos em partições disjuntas, conhecidas como fragmentos, e permite que o sistema, conforme necessário, adicione mais nós por meio de um processo conhecido como dimensionamento horizontal do sistema distribuído, além de armazenar fragmentos da coleção em nós diferentes, para atingir o balanceamento de carga.
- 81** Em bancos de dados NoSQL, o JSONPath usa expressões de caminho para navegar elementos, elementos aninhados e matrizes em um documento JSON.
- 82** A execução da seguinte expressão do MongoDB criará uma tabela denominada `projeto`, com dois campos: `size` e `max`.

```
db.createCollection("projeto", { capped : true,
size : 1310720, max : 500 } )
```

Acerca da modelagem de dados, julgue os próximos itens.

- 83** O modelo de dados relacional representa um banco de dados como uma estrutura de árvore hierárquica e utiliza os conceitos de modelos de representação de documentos, sendo os dados, nesse tipo de modelagem, representados como elementos.
- 84** O esquema estrela constitui-se de uma tabela de fatos, várias tabelas de dimensão e chaves estrangeiras da tabela de fatos para as tabelas de dimensão.

No que se refere a ferramentas de automação e orquestração e análise de sistemas, julgue os itens subsequentes.

- 85** O monitoramento da experiência do usuário em ferramentas APM (*application performance monitoring*) pode ser feito na forma de monitoramento sintético, em que é analisado o tráfego de rede sem a necessidade de instalação de agentes de *software* em aplicações monitoradas.
- 86** Kubernetes é um sistema para automação, gerência, escalabilidade e *deploy* de aplicações baseadas em contêineres.
- 87** No Kubernetes, na criação de um *pod* no modelo declarativo, são inseridas todas as informações em um arquivo de manifesto que possui a estrutura-base a seguir, na qual o campo `kind` define o objeto a ser criado.

```
{
  "apiVersion": "",
  "kind": "",
  "metadata": { },
  "spec": { }
}
```

- 88** O nó *master* do Kubernetes é composto pelo *engine* do Docker, sendo responsável por executar os contêineres em estruturas denominadas *pods*.

Julgue os itens a seguir, acerca de infraestrutura como código (IaC) com Terraform e planejamento e implementação de estratégias de continuidade e recuperação.

- 89** Uma estratégia abrangente de recuperação de desastres deve incluir a métrica objetivo do ponto de recuperação (RPO), que é o período máximo aceitável em que sistemas e aplicativos podem ficar inativos sem que isso cause danos significativos aos negócios.
- 90** Ao se implementar padrão morno para um cenário de recuperação de desastres, o objetivo de tempo de recuperação (RTO) e o objetivo do ponto de recuperação (RPO) são mantidos no menor valor possível, com baixo custo-benefício entre orçamento e alta disponibilidade.
- 91** Provedores são *plugins* que permitem ao Terraform interagir com serviços de nuvem específicos; módulos são blocos de código reutilizáveis que permitem organizar e compartilhar definições de recursos.
- 92** Conforme a sintaxe do Terraform, no bloco de configuração a seguir, o provedor `bdmg` está sendo configurado com a região `br-mg-1`.

```
provider "bdmg" {
  region = "br-mg-1"
}
```

Julgue os próximos itens, relativos a ferramentas e soluções para DevOps, DevSecOps e Docker.

- 93** No Docker, volumes são diretórios externos ao contêiner e sua principal função é fazer que os dados escritos persistam, independentemente do estado do contêiner.
- 94** O *kubectl*, cliente oficial Kubernetes, é uma ferramenta de linha de comando que interage com a API do Kubernetes, gerenciando a maioria dos objetos, como `Pods`, `ReplicaSets` e `Services`.
- 95** Na fase de compilação do ciclo de vida do DevSecOps, os desenvolvedores, os operadores de aplicativos e as equipes de operadores de *cluster* trabalham juntos para estabelecer controles de segurança para os *pipelines* de implantação contínua (CD), a fim de construir código seguro no ambiente de produção.
- 96** Se um processo dentro de um *pod* sofrer um *deadlock*, deve-se utilizar a verificação de sanidade de processo para resolver esse problema e garantir que a aplicação esteja sempre no estado ativo.

A respeito de desenvolvimento seguro e ferramentas de segurança, julgue os itens a seguir.

- 97** Um dos riscos de segurança do OWASP Top 10 é a falha no controle de acesso, o que propicia a exposição de informações sensíveis, como senhas e dados financeiros.
- 98** A aplicação da análise SWOT em uma organização visa à identificação das forças e fraquezas, que são internas à organização, e das oportunidade e ameaças, que são externas a ela.

No que se refere a gerenciamento de identidades, julgue os próximos itens.

- 99** A funcionalidade do IAM (*identity access management*) denominada federação de identidade permite que o usuário utilize credenciais de outros lugares para acessar determinado sistema.
- 100** Em sistemas IAM (*identity access management*), processos de autenticação e de autorização são utilizados para comprovar a identidade do usuário.

No que se refere a DevOps, julgue os itens subsequentes.

- 101** Em uma *pipeline* ideal de CI/CD, os *commits* devem ser executados semanalmente, de preferência no mesmo dia da semana.
- 102** Na integração contínua, o desenvolvedor deve executar uma *build* local e depois atualizar seu repositório local do projeto, trazendo as alterações do repositório central.

A respeito de governança de segurança da informação e de testes de segurança, julgue os itens subsecutivos.

- 103** O *red team* defende os sistemas e monitora atividades suspeitas, enquanto o *blue team* simula ataques para identificar vulnerabilidades e falhas nos sistemas.
- 104** No alinhamento estratégico, o planejamento de TI de uma organização é composto de objetivos, de estratégias e do ambiente de operação.
- 105** Em relação ao trabalho remoto, a norma ISO 27001 define as informações que podem ser acessadas remotamente.
- 106** No *framework* NIST, a categoria proteger envolve os aspectos de gestão de ativos e de avaliação de riscos.
- 107** A estratégia *bug bounty* caracteriza-se pelo oferecimento, a *hackers* éticos, de recompensas para testar aplicações e identificar vulnerabilidades, no sentido de viabilizar a correção de eventuais falhas.
- 108** IAST é uma ferramenta de teste de segurança de aplicativos que combina SAST e DAST, com a inserção de agentes no código em execução, para coleta de informações sobre seu comportamento.

Julgue os próximos itens, relativos a metodologias ágeis.

- 109** Considere que o *product owner* de certo projeto tenha delegado as atividades de criação, comunicação e ordenação dos itens do *product backlog* a um integrante da equipe. Nesse caso, ainda que o *product owner* continue a ser o responsável pelas citadas atividades, de acordo com o Scrum, a ordenação dos itens do *product backlog* não poderia ter sido delegada a outra pessoa.
- 110** No Scrum, o *product owner* é responsável por maximizar o valor do produto resultante do trabalho do *scrum team*, além de criar o *sprint backlog*.
- 111** Na metodologia XP, os *releases* devem ser tão grandes quanto possível, de maneira a conter a maior quantidade de requisitos importantes implementados e entregues para o cliente.
- 112** Nas metodologias ágeis, as medições de entrega estão associadas ao trabalho em andamento, indicam o número de itens do projeto que estão sendo executados no momento e estão relacionadas diretamente ao WIP (*work in progress*) do Kanban.
- 113** Na metodologia XP, o refatoramento consiste na implementação das funcionalidades cujos componentes do código-fonte devem ser integrados várias vezes, à medida que tais funcionalidades sejam desenvolvidas e testadas unitariamente.
- 114** Na metodologia XP, os programadores estimam cada estória e predizem a quantidade de estórias que podem ser implementadas no final do *release*.

Julgue os próximos itens, relativos a indicadores de desempenho e gestão de projetos ágeis.

- 115** No acrônimo SMART, o critério *specific* é o que determina que as medidas devem estar vinculadas ao *business case*, às linhas de base e aos requisitos do projeto.
- 116** No gerenciamento de projetos adaptativos, o *product owner* prioriza o *backlog* do projeto de forma contínua, para que os itens de alta prioridade sejam concluídos; assim, ele poderá considerar concluído um projeto, em razão do cronograma ou do orçamento, quando os itens de maior prioridade tiverem sido entregues.
- 117** Os indicadores-chave de desempenho (KPIs) são medidas quantificáveis utilizadas para se avaliar o sucesso de um projeto, podendo, portanto, ser utilizados como valores mensuráveis que se relacionam com as metas, os objetivos e as estratégias específicas do projeto.

Considerando o PMBOK (7.^a edição), julgue os itens a seguir.

- 118** Caminho crítico, em projetos adaptativos, é a sequência de atividades de maior valor para o cliente, determinada de acordo com os custos, o cronograma e as entregas prioritárias do projeto.
- 119** Os domínios planejamento, trabalho do projeto e entrega são executados simultaneamente ao longo do projeto, independentemente de o valor ser entregue de forma frequente, periódica ou no final do projeto.
- 120** As partes interessadas, que incluem indivíduos, grupos e organizações, definem e priorizam os requisitos do projeto por meio da sua participação e dos ajustes no planejamento, além de determinar os critérios de aceitação e os resultados do projeto.

Espaço livre