

-- CONHECIMENTOS ESPECÍFICOS --

Acerca de conceitos básicos de segurança da informação, OAuth 2.0, OpenID Connect e JWT, julgue os itens a seguir.

- 51 Em um sistema de assinatura digital baseado em criptografia assimétrica, a assinatura vinculada a um certificado digital permite verificar a integridade do documento assinado e atribuir sua autoria ao titular da chave privada, em conformidade com o atributo do não repúdio.
- 52 Em arquiteturas de autenticação e autorização que utilizam JWT assinado, a verificação criptográfica da assinatura do *token*, calculada sobre o cabeçalho e o *payload*, permite validar a integridade do *token* e a autenticidade do emissor, viabilizando seu uso em modelos *stateless*.
- 53 Em uma organização, a adoção de controle de versões e de trilhas de auditoria em seus sistemas de gestão documental garante a disponibilidade da informação, pois assegura a integridade e a confiabilidade dos registros ao longo do tempo.
- 54 Em uma arquitetura de autenticação federada, o OpenID Connect é empregado para conceder às aplicações acesso a recursos protegidos em nome do usuário, assumindo o papel de protocolo de autorização em substituição ao OAuth 2.0.

Acerca de ameaças e vulnerabilidades em aplicações, da segurança em aplicativos *web*, da metodologia OWASP e de prevenção e combate a ataques a redes de computadores, julgue os itens a seguir.

- 55 Na prevenção de ataques que envolvem manipulação de respostas DNS em ambientes que utilizam DNSSEC com validação habilitada nos resolvers recursivos, a integridade dos dados DNS assinados é garantida por mecanismo de criptografia ponta a ponta no processo de resolução, de modo que os registros manipulados sejam recusados durante a resolução de nomes.
- 56 No contexto do combate e da prevenção a ataques DDoS em arquiteturas que empregam *anycast* global combinado a serviços externos de *scrubbing* e distribuição geográfica de tráfego, a absorção e a filtragem do volume malicioso ocorrem na borda da rede, blindando os recursos internos da infraestrutura contra quaisquer efeitos diretos desses ataques.
- 57 Em uma aplicação *web* em produção, a exibição de mensagens detalhadas de erro do servidor e a exposição de arquivos de configuração em diretórios acessíveis constituem falha de configuração de segurança, ainda que o código da aplicação não apresente vulnerabilidades lógicas.
- 58 O ataque de *cross-site request forgery* caracteriza-se pela inserção de código malicioso no navegador da vítima, permitindo ao invasor executar código arbitrário no contexto da aplicação *web*.
- 59 Em aplicações *web* que utilizem identificadores de objetos em parâmetros de requisição para recuperar registros internos, a ausência de verificação de autorização associada ao objeto solicitado pode permitir que um usuário autenticado acesse objetos pertencentes a outros usuários sem a devida autorização.
- 60 Em aplicações *web* que utilizem *prepared statements* para compor consultas SQL, um ataque de injeção de SQL pode ser bem-sucedido quando os dados fornecidos pelo usuário são vinculados como parâmetros da instrução.

Acerca de criptografia, tecnologias de segurança, assinatura e certificação digital, julgue os itens subsequentes.

- 61 Em uma aplicação corporativa que estabelece conexões TLS com autenticação baseada em certificados X.509, a aceitação do certificado apresentado pelo servidor exige a validação da cadeia de certificação até uma âncora de confiança presente no repositório confiável do cliente, bem como a verificação do período de validade, da correspondência do nome do servidor e do *status* de revogação, antes do estabelecimento da sessão segura.
- 62 Em infraestruturas de chaves públicas, a validação de uma assinatura digital inclui a verificação criptográfica da assinatura sobre o *hash* do documento e a validação da cadeia de certificação associada ao certificado do signatário para estabelecer a autenticidade e a integridade do documento.
- 63 Em sistemas que utilizam criptografia simétrica para a proteção de dados em repouso, a confidencialidade e a integridade dos dados armazenados são propriedades inerentes à resistência criptoanalítica da cifra empregada e ao uso de chaves longas.
- 64 Em protocolos que empregam a troca de chaves Diffie-Hellman com parâmetros distintos a cada conexão, o material de chave derivado decorre de segredo compartilhado independente da chave privada estática do servidor, configurando propriedade de sigilo futuro.
- 65 Em sistemas *antispam* contemporâneos, a decisão sobre a aceitação ou rejeição de mensagens pode incluir a combinação de mecanismos de autenticação do domínio remetente, a análise de reputação de IP e a classificação baseada em aprendizado de máquina aplicada a características estruturais e de conteúdo da mensagem.
- 66 Em arquiteturas que utilizam mecanismo de inspeção de estado baseado no acompanhamento de conexões nas camadas de rede e transporte, a correlação entre pacotes pertencentes ao mesmo fluxo consiste em mecanismo de inspeção semântica de protocolos de aplicação que trafegam em conexões estabelecidas.

Julgue os itens seguintes com base na Lei Geral de Proteção de Dados Pessoais (LGPD).

- 67 No tratamento de dados pessoais com fundamento no legítimo interesse do controlador, são exigidas a demonstração da necessidade do tratamento e a adoção de medidas para garantir a transparência e a proteção dos direitos e liberdades fundamentais do titular.
- 68 Uma empresa que trata dados pessoais exclusivamente para a execução de contrato com o titular está dispensada de atender às solicitações de acesso e à correção de dados previstas na LGPD, uma vez que o tratamento decorre de obrigação contratual regularmente estabelecida.

As redes de computadores evoluíram muito nos últimos anos, permitindo a interconexão de inúmeros tipos de recursos computacionais. Entretanto, alguns conceitos não mudaram ao longo dos anos. Acerca de redes de computadores, julgue os itens a seguir.

- 69 Enlaces transmitem dados na mesma taxa, independentemente da tecnologia de transmissão, e são medidos em *bytes* por minuto.
- 70 Os *hosts* são conectados entre si por enlaces de comunicação e comutadores de pacotes.

Considere que a combinação do seguinte IP com uma máscara de rede produza resultados diferentes, conforme a aplicação: IP 10.10.10.10. A esse respeito, julgue os itens seguintes.

- 71 No caso de uso de uma máscara de rede 255.255.0.0 com o IP 10.10.10.10, a sub-rede em questão é 10.10.0.0, a qual comporta até 65.534 hosts.
- 72 Usando-se uma máscara de rede /24, a sub-rede em questão é 10.10.10.0/24 e o endereço 10.10.10.10 é do tipo classe C.

Sabendo que o uso de MIBs em conjunto com SNMPv3 é prática comum em gerenciamento de redes, julgue os itens a seguir, referentes a MIB e SNMPv3.

- 73 MIBs devem seguir uma linguagem de descrição de dados.
- 74 Uma requisição do protocolo SNMPv3 é incapaz de modificar o conteúdo de uma MIB.

O protocolo WPA2 possui diversas características técnicas que o diferem de seus antecessores. Considerando as características de segurança no WPA2, julgue os itens subseqüente.

- 75 O WPA2 requer um protocolo de apresentação de duas vias que executa a autenticação individual de cada entidade sem derivação de chaves.
- 76 O WPA2 requer o uso de criptografia simétrica com o algoritmo AES.

Redes privadas virtuais (VPNs) são úteis para proteger canais de comunicação. Considerando o uso de VPNs, julgue os itens seguintes.

- 77 No modo de funcionamento transporte, apenas o cabeçalho da camada de rede é encriptado.
- 78 No modo de funcionamento tunelado, todo o pacote que passa por uma VPN é encriptado.

Entre os diversos algoritmos de criptografia assimétrica, há o RSA. Considerando as características do RSA, julgue os itens a seguir.

- 79 O processo de exponenciação exigido pelo RSA pode ser ignorado do ponto de vista de uma implementação prática, pois o tempo para executar suas operações é irrelevante matematicamente.
- 80 A aritmética de módulo-n é amplamente utilizada no RSA.

Em relação aos processos de instalação e requisitos necessários para o funcionamento de sistemas operacionais Windows Server 2016, julgue os próximos itens.

- 81 A opção de instalação Desktop Experience fornece uma interface gráfica de instalação do Windows Server 2016.
- 82 A instalação Server Core inclui os componentes principais do Windows Server, mas não inclui uma GUI local.

Sabendo que o Active Directory (AD) possui funcionalidades específicas, que dependem de como um controlador de domínio está configurado em Windows Server 2016, julgue os itens que se seguem, acerca do funcionamento do AD.

- 83 Por padrão, a autenticação de usuários com protocolo Kerberos no AD requer o uso de *smart cards*.
- 84 A autenticação de clientes Windows com os protocolos NTLM foi descontinuada no Windows Server 2016.

Julgue o item abaixo, acerca de RAID 5.

- 85 Em um arranjo de disco RAID 5 com 10 discos físicos iguais, a capacidade total de armazenamento será o equivalente à soma de 9 discos, já que um disco será utilizado para a paridade de dados.

Julgue os itens seguintes, referentes a sistemas operacionais e serviços de diretório.

- 86 A administração de sistemas operacionais inclui atividades como aplicação de atualizações, definição de políticas de segurança e monitoramento do uso de recursos do sistema.
- 87 Em sistemas operacionais modernos, o núcleo do sistema, conhecido como *kernel*, é responsável por intermediar o acesso do *software* aplicativo aos recursos de *hardware*, promovendo isolamento e controle entre processos.
- 88 A técnica de memória virtual permite que o sistema operacional execute processos cujo espaço de endereçamento lógico seja maior que a memória física disponível.
- 89 Em sistemas operacionais, o gerenciamento de dispositivos de entrada e saída elimina a necessidade de *drivers* específicos, pois todo o controle é feito diretamente pelo *hardware*.
- 90 Em um sistema operacional multitarefa, cada processo possui acesso direto e exclusivo ao processador durante todo o seu tempo de execução.

A respeito de conceitos e funcionalidades de sistemas operacionais, Windows Server, RedHat Enterprise Linux e serviços de diretório, julgue os itens subseqüentes.

- 91 No RedHat Enterprise Linux 8, o *systemd* é utilizado como sistema de inicialização e gerenciamento de serviços, substituindo mecanismos tradicionais de inicialização.
- 92 A paginação de memória assegura que todos os acessos a dados ocorram na memória física principal, sem envolver o armazenamento secundário.
- 93 No Windows Server 2019, o serviço de domínio funciona de forma independente do Active Directory, sendo configurado como serviço opcional sem integração, com autenticação centralizada.
- 94 A interoperabilidade entre Active Directory e ambientes Linux pode ser alcançada por meio da integração de serviços LDAP e Kerberos para autenticação descentralizada.
- 95 O protocolo LDAP é restrito a ambientes Microsoft e funciona em conjunto com o Active Directory.

No que se refere a sistemas operacionais, Windows Server e serviços de diretório, julgue os itens a seguir.

- 96 No Windows Server 2019, o Active Directory é utilizado para autenticação de usuários, mas não está relacionado a políticas de segurança ou gerenciamento de recursos.
- 97 O escalonamento preemptivo permite que o sistema operacional interrompa a execução de um processo em andamento para alocar a CPU a outro processo considerado mais prioritário.
- 98 Em sistemas operacionais, a distinção entre modo usuário e modo *kernel* é irrelevante para a segurança do sistema, pois ambos têm o mesmo nível de privilégio de acesso ao *hardware*.
- 99 A fragmentação interna ocorre quando blocos de memória contíguos livres são separados por áreas ocupadas, dificultando a alocação de grandes blocos contínuos.

Acerca de sistemas operacionais e serviços de diretório, julgue os itens que se seguem.

- 100 O uso de *buffers* no gerenciamento de entrada e saída contribui para reduzir o impacto da diferença de velocidade entre dispositivos periféricos e o processador.
- 101 A interoperabilidade entre ambientes Linux e Active Directory elimina a necessidade de configuração adicional nos sistemas Linux, pois o suporte ao domínio é nativo e automático.
- 102 No Active Directory, o protocolo LDAP é empregado para consulta e manipulação de objetos do diretório, e o Kerberos é utilizado como principal mecanismo de autenticação.

Com base nos *frameworks* e normas de governança corporativa de tecnologia da informação (TI), gestão de riscos e gestão de serviços de TI — COBIT 2019, ISO 31000:2018 e ITIL v4 —, julgue os itens a seguir.

- 103 No ITIL, as quatro dimensões da gestão de serviços podem interagir de maneira imprevisível, conforme o nível de complexidade e de incerteza em que a organização opera.
- 104 Falhas no *hardware* de servidores do consumidor são exemplos de riscos impostos ao consumidor pelo serviço, por integrarem a proposta de valor do serviço prestado.
- 105 O nível de satisfação de clientes com a capacidade de entrega de serviço é uma métrica utilizada para avaliar o objetivo empresarial de otimizar a funcionalidade dos processos de negócios internos.
- 106 O gerenciamento de riscos deve ser integrado a todas as atividades organizacionais, independentemente do contexto e customização interna e externa das organizações.
- 107 O *sourcing* de TI é fator de *design* passível de assumir os modelos *outsourcing*, *cloud*, *insourcing* ou híbrido, conforme o contexto e a estratégia da organização.

Com base nos conceitos e práticas de gestão de projetos e metodologias ágeis, conforme o PMBOK – 7.ª edição e o Scrum, julgue os itens a seguir.

- 108 No Scrum, cada *sprint* pode ser considerado um projeto curto, pois possui um objetivo definido e permite avaliação frequente de do progresso.
- 109 Segundo o PMBOK 7.ª edição, acurácia diz respeito à forma de expressar a estimativa, e precisão refere-se à proximidade em relação ao valor real, de tal modo que uma estimativa pode ser acurada sem ser precisa.
- 110 Segundo o PMBOK 7.ª edição, os domínios de desempenho de projeto devem ser aplicados em ordem fixa e sequencial, iniciando-se por planejamento e finalizando-se em entrega.
- 111 No Scrum, o *sprint planning* inicia o *sprint* e, de forma colaborativa, define o *sprint goal*, sendo os *developers* os responsáveis por decidir como transformar os itens do *backlog* em incrementos de valor.
- 112 No PMBOK 7.ª edição, o gerenciamento de projetos integra atividades de gestão e liderança centralizadas ou distribuídas, sendo a liderança esperada em ambientes colaborativos.
- 113 De acordo com o PMBOK 7.ª edição, o salário é um fator motivacional, conforme a teoria de Herzberg: se o salário aumenta de forma adequada, garantem-se os níveis de satisfação e motivação dos membros de equipe de projetos.

Considerando as normas que regem o planejamento e a gestão de contratações de soluções de tecnologia da informação e comunicação (TIC) no setor público brasileiro, bem como as diretrizes e *frameworks* internacionais de cibersegurança, gestão de riscos e continuidade de negócios (ISO/IEC 27001 e 27002), julgue os itens a seguir.

- 114 No contexto da ISO/IEC 27001, os requisitos das partes interessadas podem incluir obrigações legais, regulatórias e contratuais relevantes para o sistema de gestão da segurança da informação.
- 115 Na ISO/IEC 27002, os temas organizam estruturalmente os controles, sendo cada controle classificado em um único tema principal — pessoas, físico, tecnológico ou organizacional —, de acordo com seu foco principal.
- 116 Em relação às contratações de soluções de TIC, os normativos legais autorizam a substituição do agente de contratação por comissão de contratação, quando houver consórcio ou subcontratação da solução.
- 117 Segundo a ISO/IEC 27002, o controle de gerenciamento de vulnerabilidades técnicas é classificado como corretivo e relaciona-se tecnicamente ao conceito de cibersegurança de recuperação e ao atributo de não repúdio.
- 118 É permitida, nas contratações de soluções de TIC, a participação de pessoas jurídicas em consórcio, condicionada à decisão motivada da administração.

Julgue os itens a seguir, relativos a Business Process Model and Notation (BPMN) e aos indicadores de desempenho, incluindo KPIs (*key performance indicators*) e BSC (*balanced scorecard*).

- 119 Os KPIs devem basear-se em métricas numéricas, evitando-se o uso de indicadores derivados de avaliações qualitativas ou subjetivas, devido à dificuldade de padronização dessas medidas.
- 120 Processos privados executáveis destinam-se principalmente à documentação conceitual interna do negócio, prescindindo de inclusão de detalhes técnicos para execução por motores de *workflow*.

Espaço livre