

-- CONHECIMENTOS ESPECÍFICOS --

Com relação à Lei de Acesso à Informação, à Lei de Delitos Informáticos, ao Marco Civil da Internet e à Lei Geral de Proteção de Dados Pessoais, julgue os itens a seguir.

- 51** No âmbito da Lei de Acesso à Informação, a Controladoria-Geral da União é a máxima instância recursal administrativa para os casos em que for negado o acesso à informação não classificada como sigilosa.
- 52** De acordo com a Lei de Delitos Informáticos, no crime de invadir dispositivo informático alheio, procede-se mediante representação se o crime for cometido contra empresa concessionária de serviço público.
- 53** Quando o tratamento de dados pessoais for realizado para fins exclusivamente jornalísticos e artísticos, a Lei Geral de Proteção de Dados Pessoais não é aplicável.
- 54** O Marco Civil da Internet assegura ao usuário a não suspensão da sua conexão à internet, salvo por débito diretamente decorrente de sua utilização.

A respeito da Estratégia Nacional de Segurança Cibernética, da Estratégia Nacional de Segurança de Infraestruturas Críticas, do Plano Nacional de Segurança de Infraestruturas Críticas, da Política Nacional de Segurança da Informação e da Rede Federal de Gestão de Incidentes Cibernéticos, julgue os itens a seguir.

- 55** Na Estratégia Nacional de Segurança Cibernética, elevar o nível de maturidade em segurança cibernética da sociedade é uma das iniciativas da ação estratégica “promover ambiente participativo, colaborativo, confiável e seguro”.
- 56** No âmbito do Plano Nacional de Segurança de Infraestruturas Críticas, a estrutura operacional idealizada para subsidiar o acompanhamento e o monitoramento permanentes da segurança das infraestruturas críticas do país é denominada Sistema Integrado de Dados de Segurança de Infraestruturas Críticas.
- 57** De acordo com a Estratégia Nacional de Segurança de Infraestruturas Críticas, investir de forma preventiva e reativa em segurança de infraestruturas críticas auxilia a redução de custos financeiros, sociais e políticos.
- 58** Está entre os princípios formulados pela Política Nacional de Segurança da Informação fomentar a formação e a qualificação dos recursos humanos necessários à área de segurança da informação.
- 59** No âmbito da Rede Federal de Gestão de Incidentes Cibernéticos, as equipes de coordenação setorial são as equipes de prevenção, tratamento e resposta a incidentes cibernéticos responsáveis por ativos de informação de serviços essenciais, cuja interrupção ou destruição provoca sério impacto social, ambiental, econômico, político, internacional ou à segurança do Estado e da sociedade.

Com relação ao Plano de Gestão de Incidentes Cibernéticos e às Instruções Normativas GSI n.º 1, n.º 2, n.º 3, n.º 5 e n.º 6, julgue os seguintes itens.

- 60** No Plano de Gestão de Incidentes Cibernéticos para a administração pública federal, as atividades de verificar se há correlação com outros incidentes e de estabelecer a prioridade para o tratamento do incidente estão incluídas no processo de análise de um incidente cibernético.
- 61** De acordo com a Instrução Normativa GSI n.º 1, nos órgãos da administração pública federal, a elaboração da Política de Segurança da Informação será coordenada pelo gestor de segurança da informação do órgão, com a participação do comitê de segurança da informação interno.
- 62** Conforme a Instrução Normativa GSI n.º 3, o processo de gestão de continuidade de negócios em segurança da informação fornece à organização um relatório de identificação, análise e avaliação dos riscos de segurança da informação e um relatório de tratamento de riscos de segurança da informação.
- 63** De acordo com a Instrução Normativa GSI n.º 2, a criação de uma equipe de prevenção, tratamento e resposta a incidentes cibernéticos é compulsória para todos os órgãos e entidades da administração pública federal que possuem a competência de administrar a infraestrutura de rede de sua organização.
- 64** A Instrução Normativa GSI n.º 6 proíbe expressamente aos servidores, empregados públicos, militares e prestadores de serviço a publicação de conteúdo ofensivo, de ódio, discriminatório ou difamatório em mídias sociais institucionais.
- 65** A Instrução Normativa GSI n.º 5 estabelece que a transferência de sistemas estruturantes para um provedor de serviço de nuvem seja realizada nos modelos de implementação de nuvem pública, ou de nuvem híbrida, vinculada à infraestrutura local de cada órgão ou entidade.

Com base no disposto na Lei Geral de Proteção de Dados (LGPD), julgue os itens seguintes.

- 66** O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, anonimização a qualquer momento e mediante requisição.
- 67** A multa simples, de 5% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R\$ 50.000.000 por infração constitui sanção administrativa aplicável pela autoridade nacional aos agentes de tratamento de dados em razão das infrações cometidas às normas previstas nessa lei.
- 68** O Conselho Diretor da Autoridade Nacional de Proteção de Dados (ANPD) será composto de 5 diretores, incluído o diretor-presidente.
- 69** O encarregado é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.
- 70** Anonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

Acerca do GDPR (General Data Protection Regulation), julgue os itens subsequentes.

- 71** O GDPR é um regulamento do direito europeu a respeito de privacidade e proteção de dados pessoais, aplicável a todos os indivíduos na União Europeia e Espaço Econômico Europeu.
- 72** Para o tratamento efetuado para fins jornalísticos ou para fins de expressão acadêmica, artística ou literária, os Estados-membros podem estabelecer isenções ou derrogações se tais ações forem necessárias para conciliar o direito à proteção de dados pessoais com a liberdade de expressão e informação.
- 73** O referido regulamento complementa a Diretiva de Proteção de Dados Pessoais de 1995 (95/46/CE).
- 74** O regulamento em questão aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, mas não ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros ou a eles destinados.

A respeito de direito digital, políticas de segurança e regulamentos afins, julgue os itens seguintes.

- 75** O ciclo de Deming, modelo de implementação de um sistema de gestão de segurança da informação (SGSI), garante a melhoria contínua e oferece uma abordagem de prevenção e de correção de falhas encontradas.
- 76** É recomendável que as empresas que desejem fazer uso de processos de biometria implementem e colham assinaturas de seus funcionários e(ou) usuários em documento específico de “termo de concessão” referente aos dados biométricos que serão coletados e armazenados, devendo o tempo de guarda desses dados ser sempre indeterminado, pois, após o encerramento da relação entre as partes, a empresa não precisa eliminar os dados biométricos coletados.
- 77** Para o direito digital, o IP constitui uma forma de identificação virtual.

Considerando conceitos e padrões criptográficos, conceitos de *blockchain* e detecção, resposta, tratamento e recuperação de incidentes cibernéticos, julgue os itens subsequentes.

- 78** A criptografia de chave pública e privada é um método no qual são utilizadas duas chaves, uma para cifrar e outra para decifrar a mensagem.
- 79** A criptografia que utiliza as duas chaves (pública e privada) é também conhecida como criptografia simétrica.
- 80** No teste de acompanhamento, um grupo é designado para verificar quaisquer problemas que necessitem ser resolvidos e quaisquer alterações que devam ser feitas no ambiente de recuperação de desastres.
- 81** *Blockchain* é um livro-razão distribuído ponto a ponto, protegido por criptografia, apenas anexado, praticamente imutável, que pode ser atualizado apenas por consenso das partes ou com o acordo entre elas.
- 82** Denomina-se *phishing* a ação de o agente do ataque colocar-se entre a comunicação de dois usuários válidos, interceptar as mensagens enviadas, passando-se por uma das partes, e poder alterá-las ou bloqueá-las.

Julgue os itens seguintes, relativos aos conceitos de computação em nuvem.

- 83** A computação em nuvem é um modelo para permitir o acesso onipresente e conveniente à rede sob demanda a um *pool* compartilhado de recursos de computação não configuráveis.
- 84** No *infrastructure as a service* (IaaS), o provedor de nuvem gerencia toda a infraestrutura da plataforma e executa o *software* que fornece os componentes da plataforma, como banco de dados e outros de *middleware*.
- 85** Entre os modelos de serviço da computação em nuvem definidos pelo National Institute of Standards and Technology (NIST), inclui-se o denominado *service as a software* (SaaS).
- 86** O *business intelligence* (BI) é um exemplo do modelo *platform as a service* (PaaS).

Julgue os próximos itens, relacionados a redes de computadores e protocolos de comunicação.

- 87** TCP e UDP são os principais protocolos da camada de transporte do modelo de referência TCP/IP, desenvolvido para descrever como é feita a comunicação e as funções de uma rede.
- 88** O IPsec necessita de maior carga de processamento que os demais protocolos.
- 89** Os protocolos da camada de aplicação do modelo de referência TCP/IP são DNS, DHCP, HTTP, Telnet, FTP, SNMP, SMTP e X.25.

Considerando os conceitos de linguagem de programação e conceitos de contêineres, julgue os itens seguintes.

- 90** Programas desenvolvidos com a linguagem Assembly possuem alta capacidade de analisar e proteger o computador de vírus.
- 91** Um aplicativo *containerizado* pode ser testado como uma unidade e implantado como instância de uma imagem de contêiner no sistema operacional hospedeiro.
- 92** A linguagem Python pode ser adotada para a análise de *malwares*, o envio e a decodificação de pacotes, o acesso a servidores, a varredura de portas e de redes, e até mesmo para testes de intrusão.

A respeito das funcionalidades de proteção da informação da Suíte Microsoft 365 E5, julgue o próximo item.

- 93** O Power BI Pro não é funcionalidade exclusiva do Microsoft 365 E5.

A respeito dos princípios da privacidade e segurança desde a concepção e por padrão (*privacy and security by design and by default*), julgue os itens que se seguem.

- 94** O princípio *security by design* deve ser implementado após a fase de *design* do ciclo de vida de desenvolvimento de um produto.
- 95** *Privacy by design* visa garantir a privacidade do usuário ao longo de todo o ciclo de vida de uma aplicação, serviço ou processo de negócio, ao passo que *privacy by default* visa garantir que os dados pessoais sejam automaticamente protegidos.

A respeito dos principais produtos e soluções da AWS (Amazon Web Service), da Google Cloud Platform e do Microsoft Azure, julgue os itens a seguir.

- 96** Blob Storage é a solução de *cloud computing* para armazenamento de dados do Microsoft Azure.
- 97** Considere-se que um empregado da área de arquitetura de *software* esteja desenvolvendo um projeto de DMZ com a utilização da nuvem Microsoft Azure. Considere-se, ainda, que esse empregado, em sua posição, oriente a utilização do Azure Bastion, produto em *cloud* que permite que *logons* sejam realizados em máquinas virtuais (VM), na rede virtual, por meio de protocolos, como o SSH ou o RDP, sem expor as VM diretamente à Internet. Nesse caso, o Bastion irá requerer uma sub-rede dedicada chamada AzureBastionSubnet.
- 98** Google Cloud DataProc é a solução para análise de dados da Google Cloud.

Julgue os itens seguintes, relativos à gestão de riscos.

- 105** A análise de riscos inclui a consideração das causas e fontes de risco, a probabilidade de ocorrer um evento específico, a probabilidade de que este evento provoque consequências e a gravidade dessas eventuais consequências.
- 106** Na gestão de riscos, o nível de risco refere-se à significância de um risco, demonstrada pela combinação das consequências e de seu impacto.

Considerando a ITIL 4, julgue os itens a seguir.

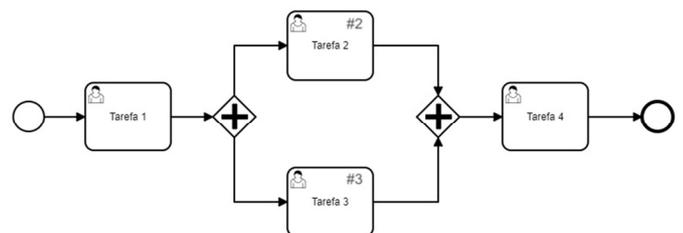
- 107** A solicitação de um usuário que inicia uma ação de serviço acordada como parte regular da entrega de serviço deve ser gerenciada pela prática de gerenciamento de incidente, de modo que se restaure a operação normal do serviço o mais rápido possível.
- 108** A prática de gerenciamento de segurança da informação tem como objetivo principal a elaboração e manutenção da política de segurança da informação da organização.

Com base no COBIT 2019, julgue os próximos itens.

- 109** No domínio entrega, serviço e suporte (DSS), há processos relacionados ao gerenciamento de solicitações e de incidentes de serviço, assim como ao gerenciamento de problemas e de continuidade.
- 110** O processo estratégia gerenciada do domínio alinhar, planejar e organizar (APO) visa garantir que cada iniciativa da organização esteja claramente conectada a uma estratégia abrangente, de modo que haja transformação digital na organização.

No que se refere ao uso da notação BPMN para a gestão de processos e para a modelagem de processos de negócio, julgue os itens que se seguem.

- 111** De acordo com a notação BPMN apresentada na figura a seguir, a Tarefa 2 (#2) e a Tarefa 3 (#3) serão executadas concomitantemente.



Considerando a figura precedente, que ilustra uma arquitetura AWS, julgue os itens a seguir.

- 99** É recomendado que a arquitetura ilustrada na figura precedente tenha previsão de um SLA (*service layer agreement*) de, no máximo, 89,99% em cargas de trabalho críticas para conectividade com o Vmware Cloud no AWS SDDC.
- 100** Na configuração apresentada na figura, um cliente usará duas conexões iguais do AWS Direct Connect de dois locais diferentes, o que garantirá resiliência à falha de conectividade.

Considerando o ambiente *multicloud* híbrido associado às melhores práticas de gestão de informações, julgue o item seguinte.

- 101** O Google ApiGee é fornecido nas modalidades PaaS e IaaS.

No que se refere à ferramenta de análise de dados em nuvem da Microsoft, julgue o próximo item.

- 102** A Azure Data Services fornece análise quase em tempo real para fluxo rápido, dados de *streaming* de inúmeros dispositivos e sensores de IOT.

Julgue os próximos itens, relativos a gerenciamento de projetos, de acordo com o PMBOK 7.ª edição.

- 103** Um dos princípios estipulados pelo PMBOK 7.ª edição é o enfoque no valor, segundo o qual valor é o indicador de sucesso definitivo do projeto; nesse sentido, as equipes podem, para apoiar a percepção de valor dos projetos, alterar o foco das entregas para os resultados pretendidos.
- 104** Os domínios de desempenhos são executados em *sprints* em sequência de importância.

- 112** De acordo com a notação BPMN apresentada na figura a seguir, apenas uma das tarefas #1, #2 e #3 será executada, ou seja, no momento de decisão (#Decisão), um único caminho deverá ser seguido.



Julgue os itens que se seguem, acerca de conceitos de computação em nuvem.

- 113 O IaaS é o serviço de computação em nuvem que utiliza um modelo de pagamento por demanda, de maneira que o cliente paga apenas pelos serviços utilizados.
 - 114 Em PaaS, o cliente não tem de se preocupar com a camada de infraestrutura, podendo concentrar-se somente nas aplicações que deseja disponibilizar.
 - 115 Escalabilidade é a característica flexível de um serviço em nuvem que permite o redimensionamento de recursos de acordo com a demanda do cliente em tempo real, de forma automatizada e instantânea.
 - 116 Uma das diferenças entre nuvens privadas e nuvens públicas é o fato de que as primeiras usam uma infraestrutura compartilhada.
-

No que se refere aos componentes centrais da arquitetura em nuvem, julgue os itens seguintes.

- 117 Apesar da automação do provisionamento da infraestrutura com a IaC, ainda é preciso fazer ajustes no gerenciamento de servidores e sistemas operacionais quando uma aplicação é criada ou implantada.
 - 118 Entre os componentes de uma arquitetura em nuvem, a plataforma de *front-end* é aquela que contém a infraestrutura do cliente, incluindo, por exemplo, recursos de armazenamento e mecanismos de segurança e gerenciamento.
 - 119 Uma região é composta por um conjunto de *data centers* isolados uns dos outros, o que se denomina zonas de disponibilidade.
 - 120 IaC refere-se ao gerenciamento e provisionamento da infraestrutura por meio de códigos, em vez de processos manuais, e o controle de versão é uma parte importante desse gerenciamento.
-

Espaço livre
