-- CONHECIMENTOS ESPECÍFICOS --

Julgue os seguintes itens, relativos a banco de dados.

51 Os modelos de dados físicos estabelecem uma visão abstrata do banco de dados, identificando as entidades principais e os relacionamentos entre elas.
JUSTIFICATIVA - Errado. O modelo conceitual estabelece uma visão abstrata do banco de dados, identificando as entidades principais e os relacionamentos entre elas. Ele fornece uma compreensão de alto nível do domínio do problema e serve como base para os modelos subsequentes.

52 Um esquema de banco de dados corresponde a um conjunto de registros formado por colunas, entre as quais se inclui a chave primária.
JUSTIFICATIVA - Errado. Um esquema de banco de dados corresponde às declarações de variáveis em um programa. Cada variável tem um valor particular em dado instante. Os valores das variáveis em um programa em um ponto no tempo correspondem a uma instância de um esquema de banco de dados. O termo "esquema de banco de dados" refere-se a uma representação visual de um banco de dados, um conjunto de regras que governa um banco de dados ou todo o conjunto de objetos pertencentes a um determinado usuário.

53 Uma tabela estará na primeira forma normal (1FN) se e somente se não houver duplicação de linhas ou colunas e se cada coluna tiver apenas um valor para cada registro na tabela.
JUSTIFICATIVA - Certo. A primeira forma normal (1NF) é o primeiro nível de normalização e obedece aos seguintes critérios: cada célula na tabela deve conter apenas um valor (atomicidade); a tabela deve ter uma chave primária para identificação única de cada registro; não pode haver duplicação de linhas ou colunas; cada coluna deve ter apenas um valor para cada registro na tabela.

54 Metadados são informações estruturadas adicionais, relativas a certo conjunto de dados, que podem ser utilizadas para descrevê-lo e manipulá-lo da forma mais eficiente possível.
JUSTIFICATIVA - Certo. As interfaces de metadados podem ser usadas para uma variedade de tarefas. Por exemplo, elas podem ser usadas para escrever um navegador de banco de dados que permite que um usuário encontre as tabelas em um banco de dados, examine seu esquema, examine linhas em uma tabela, aplique seleções para ver as linhas desejadas e assim por diante. As informações de metadados podem ser usadas para tornar genérico o código usado para essas tarefas; por exemplo, o código para exibir as linhas em uma relação pode ser escrito de tal forma que funcione em todas as relações possíveis, independentemente de seu esquema. Da mesma forma, é possível escrever um código que pegue uma *string* de consulta, execute a consulta e imprima os resultados como uma tabela formatada; o código pode funcionar independentemente da consulta real enviada.

55 A operação projeção na álgebra relacional seleciona todas as tuplas que satisfazem um dado predicado.
JUSTIFICATIVA - Errado. A operação projeção na álgebra relacional é uma operação unitária que retorna sua relação de argumento, com certos atributos deixados de fora. Como uma relação é um conjunto, quaisquer linhas duplicadas são eliminadas.

56 Uma chave primária garante que um valor que aparece em uma relação para determinado conjunto de atributos também apareça para determinado conjunto de atributos em outra relação.
JUSTIFICATIVA - Errado. O conceito apresentado no item é o de chave estrangeira.

Julgue os próximos itens, a respeito de linguagem de manipulação de dados (DML), de linguagem de definição de dados (DDL), de modelagem dimensional e de linguagem de consulta estruturada (SQL).

57 O comando SQL a seguir permite extrair todas as colunas da tabela `TB_PESSOA` com atributo `ALTURA` superior a `1.5`.
`EXTRACT ALL COLUMN FROM TABLE TB_PESSOA WHERE COLUMN ALTURA > 1.5`
JUSTIFICATIVA - Certo. A execução do referido comando resultará na extração de todas as colunas da tabela `TB_PESSOA` cujo atributo `ALTURA` seja maior que `1.5`.

58 O comando SQL `MODIFY` é usado para atualizar dados existentes em uma tabela do banco de dados.
JUSTIFICATIVA - Errado. O comando `UPDATE` é usado para atualizar linhas existentes em uma tabela.

59 Um esquema em estrela é um modelo multidimensional no qual os atributos das tabelas fato e dimensão podem ser usados para filtrar, agrupar e agregar os fatos.
JUSTIFICATIVA - Certo. Um esquema em estrela é um modelo multidimensional que organiza os dados em um banco de dados para torná-los mais fáceis de entender e analisar. Pode ser aplicado a data *warehouses*, bancos de dados, *data marts* e outras ferramentas. O *design* do esquema em estrela é otimizado para a consulta de grandes conjuntos de dados.

60 O comando SQL `SELECT FROM` permite que se leia certa coluna de uma tabela.
JUSTIFICATIVA - Certo. O comando SELECT FROM realizar a leitura de uma coluna de certa tabela.

61 O comando SQL `DROP TABLE` é usado para excluir uma tabela existente em um banco de dados.
JUSTIFICATIVA - Certo. O comando `DROP TABLE` é usado para excluir uma tabela e todos os registros dessa tabela.

Julgue os itens seguintes, a respeito de Oracle e de MySQL.

62 Um banco de dados de chave-valor armazena dados como um conjunto de pares de chave-valor em que uma chave atua como identificador exclusivo.
JUSTIFICATIVA - Certo. Um banco de dados de chave-valor é um tipo de banco de dados não relacional, também conhecido como banco de dados NoSQL, que usa um método simples de chave-valor para armazenar dados. Ele armazena dados como um conjunto de pares de chave-valor em que uma chave atua como um identificador exclusivo. Tanto as chaves quanto os valores podem ser qualquer coisa, desde objetos simples até objetos compostos complexos. Os bancos de dados de chave-valor (ou armazenamentos de chave-valor) são altamente particionáveis e permitem escalabilidade horizontal em um nível que outros tipos de bancos de dados não conseguem alcançar.

63 No Oracle, gatilhos podem invocar procedimentos armazenados.
JUSTIFICATIVA - Certo. Os gatilhos são semelhantes aos procedimentos armazenados. Um gatilho armazenado no banco de dados pode incluir instruções SQL e PL/SQL para serem executadas como uma unidade e pode invocar procedimentos armazenados. No entanto, procedimentos e gatilhos diferem na maneira como são invocados. Um procedimento é executado explicitamente por um usuário, aplicativo ou gatilho. Os gatilhos são disparados implicitamente pelo Oracle quando um evento de disparo ocorre, não importa qual usuário esteja conectado ou qual aplicativo esteja sendo usado.

64 A versão mais recente do MySQL oferece suporte a chaves estrangeiras, que permitem referência cruzada de dados relacionados entre tabelas, entretanto essa versão não suporta restrições de chave estrangeira.
JUSTIFICATIVA - Errado. O MySQL oferece suporte a chaves estrangeiras, que permitem referência cruzada de dados relacionados entre tabelas, e restrições de chave estrangeira, que ajudam a manter os dados relacionados consistentes.

A respeito de arquitetura, segurança, integridade, concorrência, recuperação após falhas e gerenciamento de transições em sistemas de gerenciamento de banco de dados (SGDB), julgue os próximos itens.

65 Em ambientes com alta latência ou alto número de falhas, recomenda-se como primeira opção a utilização do protocolo 2PC (*Two-Phase Commit*), dada a sua eficiência em situações dessa natureza.
JUSTIFICATIVA - Errado. O protocolo Two-Phase Commit (2PC) é essencial para garantir atomicidade em transações distribuídas, mas o processo é vulnerável em redes de alta latência ou quando há falhas de comunicação, pois pode bloquear recursos por longos períodos. A complexidade do 2PC o torna menos eficiente em situações de latência elevada e falhas de rede.

66 A implementação de auditorias de acesso e a aplicação de políticas de criptografia em um SGBD são suficientes para garantir a segurança dos dados sensíveis armazenados no banco, mesmo que não haja no sistema controle de acesso granular.
JUSTIFICATIVA - Errado. Embora as auditorias de acesso e políticas de criptografia sejam essenciais para a segurança de um banco de dados, elas não garantem, sozinhas, a proteção completa dos dados sensíveis, especialmente no contexto da segurança pública. Um controle de acesso granular é igualmente importante, pois permite definir diferentes níveis de permissões para usuários e funções, restringindo o acesso a dados críticos apenas a pessoas autorizadas e minimizando o risco de vazamentos ou acessos não autorizados.

67 Se a recuperação de falhas for realizada por meio do *rollback*, o SGDB que utiliza *log* de transações retornará todas as transições, tanto as confirmadas quanto as não confirmadas, a fim de garantir que o sistema retorne ao estado anterior à falha.
JUSTIFICATIVA - Errado. Em SGBDs que utilizam log de transações, o processo de recuperação de falhas usa "rollback" para desfazer transações não confirmadas, assegurando que apenas as transações confirmadas permaneçam no banco de dados. Isso mantém a integridade dos dados, revertendo operações não concluídas em caso de falha.

68 Em um SGBD que visa garantir a segurança e a integridade dos dados, o uso de controle de transações não é suficiente para assegurar que todas as operações realizadas sejam recuperáveis em caso de falha nem para garantir que não haja inconsistências ou problemas de concorrência entre transações simultâneas.
JUSTIFICATIVA - Certo. Embora o controle de transações seja essencial para a integridade e a recuperação dos dados, ele, por si só, não é suficiente para garantir a completa segurança, recuperação e consistência em um SGBD. Em um cenário real, especialmente em sistemas críticos como os da área de segurança pública, é necessário que se implementem, também, mecanismos de controle de concorrência, rotinas de recuperação de falha e políticas de acesso restrito e criptografia.

69 Um SGBD que implementa um sistema de *log* de transações segundo o princípio WAL (*write-ahead logging*) é capaz de garantir que, mesmo após uma falha inesperada, todas as transações confirmadas possam ser recuperadas ao estado consistente anterior à falha.
JUSTIFICATIVA - Certo. O princípio do *write-ahead logging* (WAL) estabelece que todas as alterações feitas por uma transação sejam registradas em um *log* de transações antes de serem aplicadas definitivamente no banco de dados. Em caso de falha, o SGBD pode consultar o *log* de transações para identificar quais transações foram confirmadas e quais ficaram incompletas no momento da interrupção. Dessa forma, ele pode reexecutar ou desfazer as transações, conforme necessário, garantindo que o banco de dados seja restaurado para um estado consistente.

70 Em um ambiente Oracle, a implementação de controle de concorrência por meio de isolamento de transações, combinada ao uso de *backups* incrementais e de *log* de *redo*, é suficiente para garantir a integridade e a recuperação completa dos dados após falha inesperada.
JUSTIFICATIVA - Certo. No Oracle, o gerenciamento da concorrência por meio de níveis de isolamento, juntamente à utilização de *redo logs* e *backups* incrementais, é uma abordagem robusta para garantir a integridade e a recuperação de dados.
No isolamento de transições, é possível que múltiplas operações ocorram simultaneamente sem que se comprometa a consistência dos dados, recurso crucial em sistemas de segurança com alta demanda.

Acerca de linguagens de consulta e de banco de dados distribuídos, julgue os itens subsequentes.

71 Em um sistema de banco de dados distribuído, a técnica de replicação síncrona garante que todas as cópias dos dados em diferentes locais estejam sempre atualizadas simultaneamente, eliminando qualquer possibilidade de inconsistência.
JUSTIFICATIVA - Certo. A replicação síncrona em um sistema de banco de dados distribuído assegura que todas as cópias dos dados sejam atualizadas ao mesmo tempo. Isso significa que, quando uma transação é realizada, ela é aplicada a todas as réplicas antes de ser considerada concluída. Dessa forma, a consistência dos dados é mantida em todas as localidades, eliminando a possibilidade de inconsistência entre as cópias.

72 Em um banco de dados distribuído, a replicação de dados garante que todas as réplicas permaneçam sincronizadas automaticamente, eliminando a necessidade de mecanismos adicionais de controle de consistência.
JUSTIFICATIVA - Errado. A replicação de dados em um banco de dados distribuído, por si só, não garante a sincronização automática entre todas as réplicas. Para manter a consistência, é necessário o uso de protocolos de controle, como o algoritmo de consenso Paxos ou Raft, especialmente em ambientes com alta latência e falhas. Sem esses mecanismos, as réplicas podem divergir e provocar inconsistências temporárias.

73 No Oracle, o uso de PL/SQL é ideal para operações avançadas de controle e análise de segurança, pois permite que se criem consultas complexas, que incluem laços de repetição e tratamento de exceções.
JUSTIFICATIVA - Certo. PL/SQL (Procedural Language/Structured Query Language) é uma extensão da SQL usada especificamente em Oracle para criar programas e procedimentos mais complexos. Diferentemente da SQL, que é declarativa, a PL/SQL é uma linguagem procedural, o que permite que se crie laços de repetição, condições, e tratamento de exceções.

74 Os comandos SQL, tais como `SELECT`, `INSERT`, `UPDATE` e `DELETE`, são aplicáveis em SGDBs relacionais.
JUSTIFICATIVA - Certo. Esses comandos são aplicáveis e

amplamente utilizados em SGBDs relacionais, pois esses sistemas compartilham a estrutura relacional e utilizam SQL como linguagem de consulta para realizar operações de manipulação e consulta de dados.

75 Em um banco de dados Oracle, a execução do comando SQL `GRANT SELECT ON employees TO security_team;` permite que o grupo de usuários `security_team` insira novos registros na tabela `employees`.
JUSTIFICATIVA - Errado. A execução do referido comando apenas permitirá que o grupo de usuários `security_team` leia os registros da tabela `employees`.

Julgue os itens subsequentes, relativos a administração de banco de dados PostgreSQL, SQL Server e MongoDB.

76 MongoDB utiliza um modelo de dados orientado a documentos e permite a replicação de dados entre diferentes nós através de um conjunto de réplicas (*replica set*), sendo o nível de consistência eventual (*eventual consistency*) a única opção para consultas em réplicas secundárias.
JUSTIFICATIVA - Errado. No MongoDB, é possível configurar o nível de consistência para consultas em réplicas secundárias, e o usuário pode optar por um modelo de consistência mais forte se necessário, através do uso de *read concern*. Embora a consistência eventual seja comum, ela não é a única opção para consultas em réplicas secundárias.

77 No PostgreSQL, a funcionalidade de replicação nativa em modo assíncrono permite que uma réplica de leitura seja utilizada imediatamente para consultas, ainda que não haja garantia de que todos os dados estejam atualizados em relação ao nó primário.
JUSTIFICATIVA - Certo. O PostgreSQL oferece replicação assíncrona nativa, permitindo que réplicas de leitura sejam utilizadas para consultas, mesmo que os dados possam estar ligeiramente defasados em relação ao nó primário. Esse tipo de replicação é útil para distribuir a carga de leitura, mas não garante consistência forte.

78 No SQL Server, o recurso de Always On Availability Groups permite a replicação síncrona entre instâncias, oferecendo alta disponibilidade, mas não permite que réplicas de leitura sejam consultadas diretamente em caso de falhas.
JUSTIFICATIVA - Errado. O recurso de Always On Availability Groups no SQL Server permite tanto a replicação síncrona quanto assíncrona entre instâncias, e as réplicas de leitura podem ser consultadas diretamente, inclusive em cenários de alta disponibilidade. Esse recurso foi projetado para oferecer disponibilidade e balanceamento de carga de leitura em caso de falhas.

Julgue os itens subsequentes, relativos ao PMBOK 7.ª edição.

79 As entregas em projetos podem ocorrer em tempos e frequências diferentes, sendo a entrega contínua aquela em que são entregues incrementos de funcionalidades imediatamente aos clientes por meio de pequenos lotes de trabalho.
JUSTIFICATIVA - Certo. Essa é, de fato, a definição de entrega contínua, em contraposição aos demais tipos de entrega: única, periódica, múltipla e contínua.

80 O ambiente regulatório e as condições de mercado possuem vários níveis de influência sobre a entrega de valor e fazem parte do ambiente interno do projeto.
JUSTIFICATIVA - Errado. Eles fazem parte do ambiente externo do projeto e não do interno.

81 O valor é o indicador final do sucesso do projeto e, portanto, só pode ser percebido após a conclusão do projeto.
JUSTIFICATIVA - Errado. O valor pode ser percebido ao longo, no final e também após a conclusão do projeto.

82 A equipe de gerenciamento do projeto é a responsável pela execução do trabalho do projeto para que seus objetivos possam ser alcançados.
JUSTIFICATIVA - Errado. Essa é a definição de equipe do projeto. A equipe de gerenciamento do projeto é aquela cujos membros estão diretamente envolvidos no gerenciamento do projeto, não na execução.

83 Inserem-se entre os domínios de desempenho de projeto: abordagem de desenvolvimento e ciclo de vida; medição; e incerteza.
JUSTIFICATIVA - Certo. Esses fazem parte dos 8 domínios, quais sejam: partes interessadas; equipe; abordagem de desenvolvimento e ciclo de vida; planejamento; trabalho do projeto; entrega; medição; incerteza.

Acerca do COBIT 2019, julgue os itens que se seguem.

84 O princípio da abordagem holística do COBIT 2019 está essencialmente voltado para a definição da estratégia da governança de TI e para o monitoramento do desempenho dessa governança.
JUSTIFICATIVA - Errado. O item apresenta o princípio do sistema de governança de ponta a ponta. A abordagem holística considera todos os aspectos da governança e gestão de TI, incluindo pessoas, processos, tecnologia e informações.

85 O gerenciamento da estrutura de gestão da TI é um dos objetivos da governança do COBIT 2019.
JUSTIFICATIVA - Errado. O objetivo apresentado é o de gestão. O objetivo da governança é gerenciar a estrutura de gestão de TI, a estratégia, a arquitetura, a inovação, o portfólio, orçamento e custos, recursos humanos e relacionamento.

86 No COBIT 2019, a modelagem de dados encontra-se no processo que consiste em gerenciar dados do domínio construir, adquirir e implementar.
JUSTIFICATIVA - Certo. A gestão de bancos de dados no COBIT 2019 está principalmente relacionada ao processo BAI05 – gerenciar dados, que se encontra no domínio BAI (construir, adquirir e implementar).

87 A definição de um sistema de gestão da segurança da informação é um dos processos do domínio avaliar, dirigir e monitorar.
JUSTIFICATIVA - Errado. Esse é um processo do domínio alinhar planejar e organizar do COBIT 2019.

No que se refere ao CMMI 2.0, julgue os itens a seguir.

88 O gerenciamento de configurações de produtos e serviços é uma área de processo da categoria de gestão de processos.
JUSTIFICATIVA - Errado. O gerenciamento de configurações faz parte da categoria de suporte.

89 O nível 4 do CMMI 2.0, gerenciado quantitativamente, é alcançado quando dados quantitativos são usados para medir e controlar uma área de processo.
JUSTIFICATIVA - Certo. O nível 4 do CMMI 2.0, gerenciado quantitativamente, possui essa característica.

90 As áreas de prática de verificação e validação estão contidas na categoria de engenharia.

JUSTIFICATIVA - Certo. A categoria engenharia abrande desenvolvimento de requisitos, solução técnica, verificação e validação.

Acerca da gestão de segurança da informação, de métodos de autenticação e de ameaças e vulnerabilidades em aplicações, julgue os itens a seguir.

91 No contexto do protocolo OpenID Connect, um *identity token* representa o resultado de um processo de autenticação, com assinatura digital, que contém declarações descritoras do usuário e os detalhes da autenticação, como, por exemplo, informações sobre como e quando o usuário foi autenticado.
JUSTIFICATIVA - Certo. Um *token* de identidade representa o resultado de um processo de autenticação. Ele contém, no mínimo, um identificador para o usuário (chamado de sub, também conhecido como reivindicação de assunto) e informações sobre como e quando o usuário foi autenticado. Ele pode conter dados de identidade adicionais.

92 Um ataque do tipo *cross-site request forgery* tem como alvo funcionalidades que causem mudanças de estado no servidor de uma aplicação autenticada, como, por exemplo, alteração do endereço de *e-mail* ou da senha da vítima, ou realização de compras em nome da vítima.
JUSTIFICATIVA - Certo. Os ataques de CSRF têm como alvo a funcionalidade que causa uma mudança de estado no servidor, como alterar o endereço de *e-mail* ou a senha da vítima, ou comprar algo. Forçar a vítima a recuperar dados não beneficia o invasor porque o invasor não recebe a resposta, a vítima recebe. Como tal, os ataques de CSRF têm como alvo solicitações de mudança de estado.

93 De acordo com a NBR ISO/IEC 27001, ao estabelecer o programa de auditoria interna, a organização deve desconsiderar resultados de auditorias anteriores para minimizar possíveis vieses, e sortear os auditores encarregados entre aqueles capacitados, de modo a evitar influências políticas no processo da auditoria interna.
JUSTIFICATIVA - Errado. A organização deve planejar, estabelecer, implementar e manter programa(s) de auditoria, incluindo frequência, métodos, responsabilidades, requisitos de planejamento e relato. Ao estabelecer programa(s) de auditoria interna, a organização deve considerar a importância dos processos pertinentes e os resultados de auditorias anteriores.

94 Conforme a NBR ISO/IEC 27002, a organização está isenta de responsabilidade legal ou contratual quando componentes defeituosos ou vulneráveis da infraestrutura de TIC de um fornecedor causarem violações de segurança de dados compartilhados da organização ou de terceiros, desde que haja acordo de confidencialidade assinado entre a organização e o fornecedor.
JUSTIFICATIVA - Errado. A organização deve estar ciente de que a responsabilidade legal ou contratual pela proteção das informações dos clientes permanece com a organização mesmo se violações de segurança de dados compartilhados da organização ou de terceiros forem causados por componentes defeituosos ou vulneráveis da infraestrutura de TIC de certo fornecedor.

No que se refere a segurança de aplicativos *web*, prevenção e combate a ataques a redes de computadores e sistemas criptográficos, julgue os itens seguintes.

95 Em um sistema de comunicação em rede, a criptografia assimétrica, como o RSA, pode ser usada para proteger o processo de troca de uma chave secreta entre duas partes; após o compartilhamento seguro dessa chave, um algoritmo de criptografia simétrica, como o AES, pode ser utilizado para proteger a transmissão de grandes volumes de dados, devido à sua maior eficiência em comparação aos algoritmos assimétricos para esse tipo de tarefa.
JUSTIFICATIVA - Certo. Um algoritmo de troca de chaves, como o RSA ou Diffie-Hellman, usa o par de chaves público-privadas para concordar com as chaves de sessão, que são usadas para criptografia simétrica assim que o *handshake* for concluído.

96 Na execução de uma aplicação *web*, a possibilidade de um usuário não autenticado agir como um usuário autenticado ou de um usuário comum autenticado agir como um administrador representa falha de segurança de elevação de privilégios relacionada ao controle de acesso da aplicação.
JUSTIFICATIVA - Certo. O controle de acesso aplica a política de modo que os usuários não possam agir fora de das permissões pretendidas. Falhas normalmente levam à divulgação não autorizada de informações, modificação ou destruição de todos os dados ou à execução de uma função comercial fora dos limites do usuário.

97 Na análise de vulnerabilidades em aplicações *web*, a determinação precisa do tipo de servidor *web* em que um aplicativo é executado viabiliza que testadores de segurança verifiquem se o aplicativo é vulnerável, identificando, por exemplo, servidores que executem versões mais antigas de *software* suscetíveis a *exploits* conhecidos.
JUSTIFICATIVA - Certo. A impressão digital do servidor *web* é a identificação do tipo e da versão do servidor *web* em que um alvo está sendo executado. Embora a impressão digital do servidor *web* seja frequentemente encapsulada em ferramentas de teste automatizadas, é importante que os pesquisadores entendam o modo como essas ferramentas tentam identificar *software* e por que isso é útil. Descobrir com precisão o tipo de servidor *web* em que um aplicativo é executado pode permitir que testadores de segurança determinem se o aplicativo é vulnerável a ataques. Em particular, servidores que executam versões mais antigas de *software* sem *patches* de segurança atualizados podem ser suscetíveis a *exploits* específicos de versão conhecida.

98 Um cliente que receba um *e-mail* aparentemente legítimo em nome de seu banco corporativo e insira suas credenciais para acessar, por meio de um *link* fornecido no *e-mail*, um sítio falso visualmente idêntico ao original, poderá autenticar-se com segurança, caso exista um certificado SSL ativo no sítio, o que garante que os dados enviados serão protegidos contra interceptações durante a comunicação com o servidor.
JUSTIFICATIVA - Errado. No exemplo, o cliente está vulnerável porque o certificado SSL não protege contra a entrega de suas credenciais a um *site* malicioso, que pode então usá-las para acessar o banco corporativo real ou outros serviços. A segurança não depende apenas da criptografia no transporte, mas também da verificação da legitimidade do *site* antes de inserir informações sensíveis.

99 A implantação de criptografia ponta a ponta nas comunicações elimina a necessidade de monitoramento ativo da rede para a detecção de atividades suspeitas relacionadas a ataques de *eavesdropping*.
JUSTIFICATIVA - Errado. Embora a criptografia ponta a ponta seja uma medida fundamental para proteger a confidencialidade dos dados, ela não elimina a necessidade de outras medidas de segurança, como o monitoramento ativo da rede. A criptografia é uma peça importante, mas não suficiente, para garantir a proteção contra ataques de *eavesdropping* sem o suporte de práticas adicionais, como o monitoramento ativo e outras medidas de defesa.

Julgue os itens a seguir, relativos à certificação digital, à gestão de riscos e ao disposto na Lei n.º 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD).

100 Uma empresa de *e-commerce* no Brasil que coleta endereços de IP dos usuários deve justificar o tratamento de dados pessoais com base na LGPD, mediante o consentimento do titular ou para atender ao legítimo interesse do controlador, sendo assegurados ao titular o acesso e a eliminação dos dados tratados, salvo exceções legais.
JUSTIFICATIVA - Certo. De acordo com a previsão da Lei n.º 13.709/2018 (LGPD), o endereço de IP pode identificar, direta ou indiretamente, um indivíduo (LGPD, art. 5º), sendo, portanto, considerado um dado pessoal. O tratamento dos dados pessoais deve observar as hipóteses previstas no art. 7.º da LGPD. E deve ser assegurado ao titular dos dados pessoais, a qualquer momento e mediante requisição, o acesso aos dados (LGPD, art. 18, II) e a eliminação dos dados pessoais tratados com o consentimento do titular (LGPD, art. 18, VI).

101 Um certificado digital X.509 pode ser considerado confiável para estabelecer a identidade de uma entidade se o campo CN (*common name*) contiver o nome correto da entidade, pois o CN é suficiente para validar a autenticidade do certificado.
JUSTIFICATIVA - Errado. A autenticidade de um certificado digital X.509 não depende de um único campo, como o *common name* (CN), mas de uma análise conjunta de sua cadeia de certificação, a validade do próprio certificado, a confiabilidade da CA emissora e a correção do uso dos campos e extensões.

102 De acordo com a NBR ISO/IEC 27005, um propósito viável para a gestão de riscos de segurança da informação é definir a execução de políticas e procedimentos, incluindo-se a implementação dos controles selecionados.
JUSTIFICATIVA - Errado. O item aponta como propósito um item a ser avaliado pela organização na abordagem da gestão de risos em termos de recursos disponíveis para realizar, o que não é um propósito entre os possíveis mencionados na NBR ISO/IEC 27005.

Julgue os itens a seguir, à luz do disposto na Nova Lei de Licitações e Contratos (Lei n.º 14.133/2021).

103 Em regra, o processo licitatório deve observar as seguintes fases, nesta ordem: preparatória; de divulgação do edital de licitação; de apresentação de propostas e lances, quando for o caso; de habilitação; de julgamento; de homologação; e recursal.
JUSTIFICATIVA - Errado. De acordo com o art. 17 da Lei nº 14.133/2021, a fase de julgamento precede a de habilitação e a de homologação precede a recursal.
O processo licitatório observará as seguintes fases, em sequência:
I preparatória;
II de divulgação do edital de licitação;
III de apresentação de propostas e lances, quando for o caso;
IV de julgamento;
V de habilitação;
VI recursal;
VII de homologação.

104 Termo de referência é o documento constitutivo da primeira etapa do planejamento de uma contratação, ou seja, ele embasa a elaboração do projeto básico e caracteriza o interesse público envolvido e a sua melhor solução.
JUSTIFICATIVA - Errado. A definição apresentada no item é de estudo técnico preliminar, de acordo com o art. 6.º, XX, da Lei n.º 14.133/2021. A definição correta de termo de referência está prevista no art. 6.º, XXIII, da referida lei.

105 Nas licitações para contratação de bens e serviços especiais de tecnologia da informação e comunicação (TIC), o critério de julgamento por técnica e preço será adotado quando o estudo técnico preliminar demonstrar que a avaliação e a ponderação da qualidade técnica que superarem os requisitos mínimos estabelecidos no edital forem relevantes aos fins pretendidos pela administração pública.
JUSTIFICATIVA - Certo. A assertiva está de acordo com o disposto no art. 36, § 1.º, III, da Lei n.º 14.133/2021.

106 Os contratos de prestação continuada de sistemas estruturantes de tecnologia da informação podem ter vigência máxima de 15 anos.
JUSTIFICATIVA - Certo. Segundo o art. 114 da Lei n.º 14.133/2021, o contrato que previr a operação continuada de sistemas estruturantes de tecnologia da informação poderá ter vigência máxima de 15 anos.

107 Os trabalhos relativos a treinamento e aperfeiçoamento de pessoal são considerados serviços técnicos especializados de natureza predominantemente intelectual.
JUSTIFICATIVA - Certo. A assertiva está de acordo com o disposto no art. 6.º, XVIII, alínea f, da Lei n.º 14.133/2021.

Julgue os itens a seguir, com base na Instrução Normativa SGD/SEDGG/ME n.º 94/2022, que dispõe sobre o processo de contratação de soluções de TIC.

108 Os órgãos e as entidades que necessitem renovar uma infraestrutura de centro de dados deverão fazê-lo por meio da contratação de serviços de computação em nuvem, a não ser que um estudo técnico preliminar da contratação demonstre sua inviabilidade.
JUSTIFICATIVA - Certo. A assertiva está de acordo com o previsto no Anexo I (Diretrizes Específicas de Planejamento da Contratação) da referida Instrução Normativa. No tópico 4.1 (relativo à contratação de infraestrutura de centro de dados, serviços em nuvem, sala-cofre e sala segura), é previsto que os órgãos e as entidades que necessitem criar, ampliar ou renovar infraestrutura de centro de dados deverão fazê-lo por meio da contratação de serviços de computação em nuvem, salvo quando demonstrada a inviabilidade em estudo técnico preliminar da contratação.

109 Na contratação de serviços de desenvolvimento, sustentação e manutenção de *software*, não é permitido estabelecer no edital um patamar de preço para presunção de inexequibilidade, com base em pesquisas de mercado e de contratações similares.
JUSTIFICATIVA - Errado. A assertiva contraria o disposto no Anexo I (Diretrizes Específicas de Planejamento da Contratação) da referida Instrução Normativa. No subtópico 3.3 (relativo à contratação de serviços de desenvolvimento, sustentação e manutenção de *software*), é previsto que o órgão ou a entidade poderá estabelecer no edital patamar de preço para presunção de inexequibilidade, com base em pesquisas de mercado e de contratações similares.

Julgue os itens seguintes, tendo como fundamento a Instrução Normativa SEGES/ME n.º 65/2021, que dispõe sobre o procedimento administrativo para a realização de pesquisa de preços para aquisição de bens e contratação de serviços em geral.

110 Para a obtenção do preço estimado, utiliza-se, como método, o maior valor obtido na pesquisa de preços, desconsiderados os valores inexequíveis, inconsistentes e os excessivamente elevados.
JUSTIFICATIVA - Errado. A assertiva contraria o disposto no art. 6.º da Instrução Normativa SEGES/ME n.º 65/2021, segundo o qual "serão utilizados, como métodos para obtenção do preço estimado, a média, a mediana ou o menor dos valores obtidos na pesquisa de preços, desde que o

cálculo incida sobre um conjunto de três ou mais preços, oriundos de um ou mais dos parâmetros de que trata o art. 5.º, desconsiderados os valores inexequíveis, inconsistentes e os excessivamente elevados".

111 A contratação de itens de TIC deve utilizar, como preço estimado, os preços constantes nos catálogos de soluções de TIC com condições padronizadas, publicados pela Secretaria de Governo Digital, a não ser que a pesquisa de preços realizada resulte em valor inferior.

JUSTIFICATIVA - Certo. O item está de acordo com o previsto no art. 8.º da Instrução Normativa SEGES/ME n.º 65/2021: "os preços de itens constantes nos Catálogos de Soluções de TIC com Condições Padronizadas, publicados pela Secretaria de Governo Digital da Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia, deverão ser utilizados como preço estimado, salvo se a pesquisa de preços realizada resultar em valor inferior."

112 A justificativa de preços, com base em valores de contratações de objetos idênticos, pode ser utilizada nas contratações diretas por inexigibilidade ou por dispensa de licitação, nos casos em que o valor do objeto da contratação não puder ser estimado, entre outros parâmetros, pela pesquisa direta com, no mínimo, três fornecedores.

JUSTIFICATIVA - Certo. O item está em conformidade com o disposto no art. 7.º, § 1.º, da Instrução Normativa SEGES/ME n.º 65/2021, segundo o qual "nas contratações diretas por inexigibilidade ou por dispensa de licitação, aplica-se o disposto no art. 5.º".

Considerando duas variáveis, X e Y, cujas variâncias da diferença e da soma entre elas sejam, respectivamente, $\text{Var}(X - Y) = 7$ e $\text{Var}(X + Y) = 5$, julgue os itens subsequentes.

113 A variância de X é igual a 6,5.

JUSTIFICATIVA - Errado. Sabe-se que
$\text{Var}(X - Y) = \text{Var}(X) + \text{Var}(Y) - 2\text{Cov}(X, Y) = 7$
e que
$\text{Var}(X + Y) = \text{Var}(X) + \text{Var}(Y) + 2\text{Cov}(X, Y) = 5$.
Ao se somarem as variâncias da soma e da diferença, $\text{Var}(X - Y) + \text{Var}(X + Y)$, obtém-se o seguinte cálculo.
$\text{Var}(X) + \text{Var}(Y) - 2\text{Cov}(X, Y) +$
$\text{Var}(X) + \text{Var}(Y) + 2\text{Cov}(X, Y) =$
$2\text{Var}(X) + 2\text{Var}(Y) = 12$
$\text{Var}(X) + \text{Var}(Y) = 6$.
Sabendo-se que a variância será sempre positiva, então $\text{Var}(X)$ deverá ser menor que 6.

114 A correlação linear entre X e Y é negativa.

JUSTIFICATIVA - Certo. Sabendo-se que $\text{Var}(X - Y) = 7$ e $\text{Var}(X + Y) = 5$, então, a covariância entre X e Y deve ser negativa. Consequentemente, a correlação entre X e Y também deve ser negativa.

Supondo que 15 ± 3 represente o intervalo de 95% para a média μ de uma população normal, obtido com base em uma amostra aleatória simples de tamanho igual a 400, julgue os próximos itens.

115 No teste de hipóteses $H_0{:}\mu = 17$ *versus* $H_1{:}\mu \neq 17$, caso o nível de significância do teste seja igual a 5%, não há evidências estatísticas para se rejeitar a hipótese nula H_0.

JUSTIFICATIVA - Certo. Como a margem de erro do intervalo de 95% foi igual a 3, a hipótese nula seria rejeitada se a média amostral fosse superior a 17 + 3 = 20 ou inferior a 17 – 3 = 14. Mas, como a média amostral foi $\bar{x} = 15$, não há evidências estatísticas para se rejeitar a hipótese nula (H_0) caso o nível de significância do teste seja igual a 5%.

116 Se $15 \pm \epsilon$ representasse o intervalo de 99,9% confiança, o valor de ϵ seria inferior a 3.

JUSTIFICATIVA - Errado. A elevação do nível de confiança implica aumento do comprimento do intervalo. Logo, se 15 ± 3 representa o intervalo de 95% para a média de uma população normal, o valor de ϵ para o intervalo de 99,9% confiança será superior a 3.

117 A amostra aleatória foi retirada de uma população normal com desvio padrão igual a 3.

JUSTIFICATIVA - Errado. O valor 3 representa a margem de erro na estimação da média, ou seja,
$3 \approx 2 \times \sigma \times 400^{-1/2}$.
Logo, o desvio padrão populacional σ seria aproximadamente igual a 30.

Julgue os seguintes itens, acerca de técnicas de amostragem.

118 Suponha que, na auditoria no banco de dados de certa delegacia, um analista de tecnologia da informação precise verificar a consistência de registros de boletins de ocorrência. Suponha, também, que esse analista decida selecionar 1 registro a cada 10 em ordem cronológica, começando de um registro inicial escolhido aleatoriamente entre os 10 primeiros registros. Suponha, ainda, que, após essa seleção, os registros escolhidos sejam analisados detalhadamente quanto à completude e precisão das informações. Com base nessa situação hipotética, é correto afirmar que o analista efetuará uma amostragem sistemática.

JUSTIFICATIVA - Certo. Essa situação caracteriza uma amostragem sistemática, pois após selecionar o primeiro registro aleatoriamente, os demais são escolhidos a partir de intervalos fixos (1 a cada 10), respeitando-se uma ordem pré-definida. Isso garante que a seleção seja sistemática, sem a necessidade de listar toda a população.

119 Suponha que certo analista tenha efetuado um levantamento estatístico para estimar o percentual de boletins de ocorrência inconsistentes considerando cinco diferentes tipos: roubo a residência, furto, acidente de trânsito, ameaça e estelionato. Suponha, ainda, que, embora alguns tipos sejam mais comuns que outros, o referido analista tenha selecionado aleatoriamente quantidades iguais de boletins de cada tipo. Nessa situação hipotética, o plano amostral descrito terá sido o da amostragem aleatória estratificada com alocação uniforme.

JUSTIFICATIVA - Certo. Na amostragem estratificada, a população é dividida em grupos homogêneos (estratos) com base em uma característica comum, como o tipo de boletim de ocorrência. Na alocação uniforme, cada estrato contribui com o mesmo número de elementos para a amostra, independentemente do tamanho de cada grupo na população. No caso descrito, são selecionadas quantidades iguais de boletins de cada tipo, o que caracteriza a alocação uniforme dentro da amostragem estratificada.

120 Considere que, em determinada rodovia, policiais em uma barreira selecionem veículos de forma aleatória. Considere, ainda, que os veículos selecionados sejam parados e todos os ocupantes adultos sejam questionados acerca de determinado assunto. Suponha, por fim, que, após essa ação, os policiais registrem o total de 120 pessoas questionadas em 80 veículos. Nessa situação hipotética, a amostragem será do tipo aleatória simples com tamanho amostral de 120 pessoas.

JUSTIFICATIVA - Errado. Essa situação descreve uma amostragem por conglomerados, representados pelos veículos, que foram selecionados aleatoriamente, e todos os ocupantes adultos (elementos do conglomerado) foram incluídos na amostra. Na amostragem aleatória simples, cada indivíduo da população teria igual probabilidade de ser selecionado diretamente, o que não ocorre nesse caso, já que a unidade primária de seleção é o veículo.