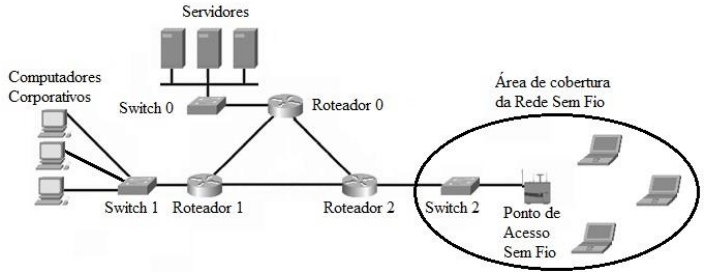
-- CONHECIMENTOS ESPECÍFICOS --



O diagrama lógico precedente ilustra uma rede cujos roteadores estão conectados via cabo metálico, com velocidade de transmissão de dados igual a 1 Gbps, e funcionam no nível de rede do modelo OSI. Os serviços de rede (DNS, FTP, SSH, DNS, SMTP, POP, IMAP, HTTP, HTTPS, SSL, DNS, RDP, DHCP) funcionam nos servidores conectados ao Switch 0 e o Ponto de Acesso Sem Fio fornece segurança para os dispositivos que se conectarem de forma sem fio.

Considerando o diagrama apresentado, julgue os próximos itens.

51 Cabos metálicos de par trançado categoria 6 são suficientes para realizar a conexão entre os Roteadores 0, 1 e 2.
JUSTIFICATIVA - Certo. Categoria 6: Categoria de cabos originalmente desenvolvida para trabalhar nativamente no padrão Gigabit Ethernet. Largura de banda especificada até 250 Mhz e velocidades de 1 Gbps até 10 Gbps.

52 A rede formada pelo Switch 1 e pelos Computadores Corporativos possui topologia em estrela.
JUSTIFICATIVA - Certo. Uma rede usa topologia em estrela se todos os computadores se conectam a um ponto central, que é a forma como está conectada a rede formada a partir do Switch 1.

53 A conexão física que liga os servidores ao barramento é realizada através de transceptores ou transceptores-vampiros.
JUSTIFICATIVA - Certo. Os nós são conectados ao barramento por meio de cabos transceptores e transceptores-vampiros. Um cabo transceptor é uma conexão que vai de um dispositivo ao cabo principal (barramento). Um transceptor-vampiro é um conector que se une ao cabo principal ou perfura a blindagem de um cabo para criar um contato com o núcleo metálico.

A respeito de elementos de interconexão de redes de computadores, bem como de noções dos modelos de referência OSI (*open system interconnection reference model*), julgue os próximos itens.

54 A camada de apresentação do modelo OSI é responsável pelo controle de diálogo e pela sincronização no estabelecimento de conexões.
JUSTIFICATIVA - Errado. Tais responsabilidades são da camada de sessão, e não da de apresentação.

55 Na estratégia de *poison reverse*, utilizada em roteadores, em vez de inundar a tabela por meio de cada interface, cada nó envia apenas parte de sua tabela por intermédio de cada interface.
JUSTIFICATIVA - Errado. Isso ocorre na estratégia de *split horizon*, na qual, em vez de inundar a tabela por meio de cada interface, cada nó envia apenas parte de sua tabela por intermédio de cada interface. Se, de acordo com sua tabela, o nó B pensar que a rota ótima para chegar a X é via A, ele não precisa anunciar esta informação a A; a informação proveio de A (A já sabe disso)".

56 As funções das camadas de apresentação, sessão e aplicação do modelo OSI são realizadas pela camada de aplicação do modelo TCP/IP.
JUSTIFICATIVA - Certo. A camada de aplicação no TCP/IP equivale à combinação das camadas de sessão, de apresentação e de aplicação do modelo OSI. Muitos protocolos são definidos nessa camada.

Julgue os itens a seguir, considerando os padrões e protocolos das redes de comunicação de dados.

57 O serviço de compressão de dados é obrigatório na implementação de segurança de redes com o SSL (*secure sockets layer*).
JUSTIFICATIVA - Errado. O SSL fornece diversos serviços para os dados recebidos da camada de aplicação, entre eles a compressão. Nesta, cada fragmento de dados é compactado por meio de um dos métodos de compressão sem perdas negociados entre o cliente e o servidor. Esse serviço é opcional.

58 O protocolo IPSec, operando em modo de transporte, protege o cabeçalho IP de um pacote de dados.
JUSTIFICATIVA - Errado. O IPSec, no modo de transporte, não protege o cabeçalho IP; ele protege apenas a carga útil proveniente da camada de transporte.

59 O padrão 802.1q permite a execução do STP (*spanning tree protocol*) em conjunto de redes logicamente independentes que compartilhem o mesmo meio físico.
JUSTIFICATIVA - Certo. O padrão IEEE 802.1q fornece uma maneira de executar a *spanning tree* em um conjunto de redes logicamente independentes que compartilham um meio físico sem qualquer confusão ou interferência entre as redes lógicas.

60 O padrão 802.3 define redes de comunicação com velocidades de transmissão de até 100 Mbps.
JUSTIFICATIVA - Errado. Os cabos utilizados para a conexão de dispositivos em redes locais com o padrão 802.3 podem ser de pares trançados, coaxiais ou fibras óticas, operando em velocidades de 10Mbps, 100Mbps ou 1000Mbps (1Gbps).

61 Desde sua versão 802.11n, o padrão 802.11 utiliza a técnica de transmissão através de MIMO (*multiple-input multiple-output)*.
JUSTIFICATIVA - Certo. O padrão utiliza uma técnica conhecida como múltiplas entradas e múltiplas saídas (MIMO – *multiple-input multiple-output*) para superar o problema de ruído em LANs sem fio.

Considerando conceitos relativos a gerenciamento de redes e seus protocolos, julgue os itens a seguir.

62 O RMON1 permite o gerenciamento de redes nas camadas física, de enlace de dados e de rede do modelo OSI.
JUSTIFICATIVA - Errado. A solução RMON1 foi desenvolvida estando associada à camada de enlace, e posteriormente levou ao desenvolvimento da RMON2, que passou a ser capaz de monitorar e gerenciar as camadas superiores do modelo OSI: da camada de rede à camada de aplicação.

63 No processo de sondagem, ao se utilizar o RMON, a *probe* é composta por um agente SNMP, que coleta informações e as retransmite a um aplicativo de gerenciamento SNMP.
JUSTIFICATIVA - Certo. Uma sonda (denominada *probe* dentro da estrutura RMON) é composta por um agente SNMP, que coleta informações e as retransmite para um aplicativo de gerenciamento SNMP. Nesse processo, um ou mais RMON MIBs definem os objetos de rede a serem gerenciados. Geralmente, os dispositivos utilizados para gerenciar a rede por SNMP (como os roteadores)

precisam ter um *software* que tenha como função transformá-los em *probes* e fornecer funções RMON.

64 O protocolo SNMP utiliza conexões TCP (*transmission control protocol*) para garantir a confiabilidade de transferência dos dados gerenciados.
JUSTIFICATIVA - Errado. O SNMP usa serviços UDP em duas portas conhecidas, 161 e 162. A porta conhecida 161 é usada pelo servidor (agente) e a porta 162, pelo cliente (gerente).

65 Um pacote do tipo SNMPv2 *trap* é encaminhado do agente até o gerente SNMP a fim de notificá-lo de um evento anormal, por exemplo, a reinicialização do agente.
JUSTIFICATIVA - Certo. *Trap* (também denominado SNMPv2 *trap* para diferenciá-lo do PDU SNMPv1 *trap*) é enviado do agente até o gerente para notificar um evento anormal. Por exemplo, se o agente for reiniciado, ele notifica o gerente e informa o horário da reinicialização.

No que se refere a noções de telefonia digital, VoIP e videoconferência, julgue os próximos itens.

66 O protocolo RSVP resolve o problema da escalabilidade a partir da implementação de QoS em redes com alta quantidade de nós.
JUSTIFICATIVA - Errado. O RSVP tem muitas limitações que evitam que ele seja usado universalmente na Internet. Em um cenário de pior caso para redes que usem o RSVP, um roteador de núcleo deve gerenciar milhares de reservas RSVP e enfileirar cada fluxo de acordo com aquela reserva. Os problemas de escalabilidade que cercam o RSVP o relegam às fronteiras da rede e forçam o uso de outras ferramentas de QoS no núcleo da rede.

67 O protocolo SIP exige a configuração de rede em *multicast* para a realização de chamadas em conferência, enquanto o padrão H323 utiliza a unidade de controle multiponto (MCU), não necessitando de *multicast* para realizar conferências.
JUSTIFICATIVA - Certo. O H323 usa uma unidade de hardware especial conhecida como MCU para suportar chamadas em conferência. O SIP depende de *multicast* para chamadas em conferência.

68 Nas ligações realizadas através de VoIP, o áudio é codificado por meio da técnica Manchester diferencial.
JUSTIFICATIVA - Errado. Em chamadas VoIP, o áudio é codificado por meio da modulação por código de pulso (PCM – *pulse code modulation*).

69 Sistemas de telefonia VoIP necessitam de técnicas de criptografia de chaves assimétricas para a garantia de integridade, privacidade e autenticidade.
JUSTIFICATIVA - Errado. Dados os requisitos de segurança para serviços VoIP, as tecnologias disponíveis para assegurar a integridade, privacidade e autenticidade são a chave compartilhada e a criptografia por chave pública.

A respeito da arquitetura de rede TCP/IP, julgue os itens subsequentes.

70 O teste para avaliar a conectividade com a rede e o tempo de resposta é feito por meio do comando `ping`, que utiliza os protocolos IP e ARP.
JUSTIFICATIVA - Errado. Um dos principais testes realizados pelos usuários para avaliar a conectividade com a rede e o tempo de resposta é feito pelo comando `ping`, que utiliza os protocolos IP e ICMP, presentes na camada Internet.

71 Na camada de aplicação estão os protocolos do mais alto nível, como HTTP, SSH, SMTP e DNS.
JUSTIFICATIVA - Certo. Os criadores do modelo de referência TCP/IP decidiram que os protocolos de mais alto nível, como HTTP, SSH, Telnet, SMTP, DNS, POP3, FTP etc., deveriam incluir os detalhes da camada de aplicação, apresentação e de sessão.

72 O TCP requisita que o destinatário informe, por meio do envio de um ACK (*acknowledgement*), qual foi o último pacote recebido com sucesso.
JUSTIFICATIVA - Certo. TCP requisita que o destinatário informe, por meio do envio de um ACK (*acknowledgement*), qual foi o último pacote recebido com sucesso.

73 O cabeçalho do UDP requer o uso de *bits* adicionais para o correto sequenciamento da informação, bem como o *checksum* obrigatório, para a integridade do cabeçalho e dos dados.
JUSTIFICATIVA - Errado. O correto seria cabeçalho do TCP.

No que se refere à arquitetura *hardware* de servidores e a armazenamento em disco, julgue os itens subsecutivos.

74 Uma SAN roda um sistema operacional completo e funciona como um servidor de arquivos conectado diretamente na rede, que pode ser acessado simultaneamente por vários clientes.
JUSTIFICATIVA - Errado. A característica apresentada no item é a de um NAS, que, por sua vez, roda um sistema operacional completo e funciona como um servidor de arquivos, ligado diretamente na rede.

75 O armazenamento de arquivos é uma tecnologia usada para armazenar dados em blocos, com transferência de dados rápida e confiável, sendo uma forma eficiente de se guardar dados em discos.
JUSTIFICATIVA - Errado. O armazenamento de blocos, às vezes chamado de armazenamento em nível de bloco, é uma tecnologia usada para armazenar dados em blocos. Eles são, então, armazenados como peças separadas, cada uma com um identificador único. Os desenvolvedores preferem o armazenamento de blocos para situações de computação que exigem transferência de dados rápida, eficiente e confiável.

76 O PCI Express é um barramento serial e ponto a ponto, em que cada periférico possui um canal exclusivo de comunicação com o *chipset*.
JUSTIFICATIVA - Certo. A característica fundamental do PCI Express é que ele é um barramento ponto a ponto, em que cada periférico possui um canal exclusivo de comunicação com o *chipset*.

77 Uma RPS (*redundant power supply*) baseia-se no uso de módulos substituíveis e, em caso de falha, pode ser trocada sem a necessidade de desligar o servidor.
JUSTIFICATIVA - Certo. As fontes redundantes são chamadas de RPS (*redundant power supply*) e se baseiam no uso de módulos substituíveis.

Julgue os itens que se seguem, referentes a formatação de dados, virtualização VMWare e HyperV, e *cluster*.

78 Em um *cluster* ativo/passivo, o segundo servidor assume a posição do primeiro em caso de falha; em um *cluster* ativo/ativo, os servidores dividem as requisições, balanceando as cargas.
JUSTIFICATIVA - Certo. Em vez de montar um único servidor com componentes redundantes, existe também a opção de usar um

cluster de alta disponibilidade (chamados de *high-availability clusters* ou *failover clusters*), onde são usados dois servidores completos, sendo a única função do segundo servidor assumir a posição do primeiro em caso de falhas (modo chamado de ativo/passivo), diferentemente de um *cluster* com balanceamento de carga, onde os servidores dividem as requisições (ativo/ativo).

79 Após a formatação de um disco, são necessárias partições para que múltiplos sistemas operacionais coexistam ou, em alguns casos, para serem usadas como área de troca (*swapping*).
JUSTIFICATIVA - Certo. Após a formatação de baixo nível ter sido concluída, o disco é dividido em partições. Logicamente, cada partição é como um disco separado. Partições são necessárias para permitir que múltiplos sistemas operacionais coexistam. Também, em alguns casos, uma partição pode ser usada como área de troca (*swapping*). No x86 e na maioria dos outros computadores, o setor 0 contém o registro mestre de inicialização (Master Boot Record — MBR), que contém um código de inicialização mais a tabela de partição no fim.

80 Na criação de uma máquina virtual Hyper-V de primeira geração, é possível utilizar a inicialização segura e gerar um volume de inicialização com até 64 TB.
JUSTIFICATIVA - Errado. A criação de inicialização segura e a criação de volume de inicialização com até 64 TB só são possíveis em máquinas virtuais de 2.ª geração.

81 Caso uma máquina virtualizada no VMWare falhe no aplicativo, o desempenho ou a operação de outros sistemas operacionais em execução no *host* serão afetados.
JUSTIFICATIVA - Errado. A VMWare virtualiza computadores físicos com seu principal produto de hipervisor. Um hipervisor é uma fina camada de *software* que interage com os recursos subjacentes de um computador físico (chamado *host*) e aloca esses recursos em outros sistemas operacionais (conhecidos como convidados). O sistema operacional convidado solicita recursos do hipervisor. O hipervisor separa cada sistema operacional convidado para que cada um possa ser executado sem interferência dos outros. Se um sistema operacional convidado sofrer uma falha no aplicativo, ficar instável ou for infectado por *malware*, o desempenho ou a operação de outros sistemas operacionais em execução no *host* não serão afetados.

Julgue os próximos itens, a respeito de computação em nuvem, conceitos de ambiente *bare metal*, servidores de aplicação IIS e servidores de páginas HTML.

82 O Nginx foi criado para manipular as solicitações com mais de 10 mil conexões simultâneas, o que resolveu o problema `c10k`, que afetava o desempenho no Apache.
JUSTIFICATIVA - Certo. O NGINX foi criado para resolver o conhecido problema c10k, o que significa que um servidor de Internet que usa mecanismos para manipular as solicitações do usuário não consegue gerenciar mais de 10 mil conexões ao mesmo tempo.

83 No IIS, o módulo de *log* chamado `HttpLoggingModule` dá suporte ao recurso de rastreamento de solicitação com falha e carrega módulos de *log* personalizados.
JUSTIFICATIVA - Errado. A descrição apresentada é a do módulo FailedRequestsTracingModule.

84 Uma nuvem pública é oferecida pelo provedor de serviço e seus recursos computacionais são compartilhados pelos seus clientes, ficando o controle das instâncias e máquinas virtuais delegados ao provedor.
JUSTIFICATIVA - Certo. Nuvem pública é aquela oferecida pela Internet por um provedor de serviços, em que os recursos computacionais são compartilhados pelos seus diversos clientes e o controle das instâncias, máquinas virtuais e recursos de processamento e armazenamento ficam completamente delegados ao provedor.

85 Uma das vantagens do serviço de nuvem privada é o seu baixo custo em relação a um *datacenter* comum, pois a contratada é responsável pelo custo e prestação de contas do gerenciamento da nuvem privada.
JUSTIFICATIVA - Errado. Uma desvantagem é que o departamento de TI da empresa é responsável pelo custo e prestação de contas do gerenciamento da nuvem privada. Sendo assim, as nuvens privadas exigem as mesmas despesas de alocação de pessoal, gerenciamento e manutenção que um *datacenter* comum de propriedade da empresa.

86 O *bare metal* caracteriza-se como um servidor físico dedicado a um único cliente com total controle da infraestrutura de memória, armazenamento e processamento.
JUSTIFICATIVA - Certo. O ambiente *bare metal* é um ambiente de TI que se caracteriza por ter um servidor físico dedicado a um único cliente, sem camadas adicionais de *software* ou hipervisores. O termo *bare metal* se refere a um servidor de locatário único que fornece acesso a 100% da capacidade de processamento, memória e armazenamento dos recursos do *hardware* físico.

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

87 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.

88 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.

89 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.

90 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.

91 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.

92 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.

93 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).

94 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.

95 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.

96 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.

97 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.

98 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.

99 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.

100 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.

101 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.

102 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.

103 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.

104 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.

105 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.

106 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.

107 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).

108 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).

109 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.

110 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).

111 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.

112 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.

113 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.

114 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.

115 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.

116 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.

117 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.

118 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".

119 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."

120 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".