

CONCURSO PÚBLICO NÍVEL SUPERIOR

102 – ANALISTA DE TECNOLOGIA DA INFORMAÇÃO TIPO A

Frase: **Aja agora e veja a transformação.**

(Transcrever a frase acima para o cartão de respostas)



SUA PROVA

O candidato receberá do fiscal de sala:

- Este caderno de prova, contendo **65 (sessenta e cinco)** questões objetivas; e
- Um **Cartão de Respostas** destinado às respostas das questões objetivas.



TEMPO

- **4 (quatro) horas** é o tempo disponível para a realização da prova, já incluindo o tempo para a marcação no **Cartão de Respostas** da prova objetiva.
- Em hipótese alguma o candidato levará consigo o caderno de prova.



NÃO SERÁ PERMITIDO

- ausentar-se da sala ou do local de prova sem o acompanhamento de um fiscal;
- fazer uso de calculadora, relógio de qualquer espécie e/ou agenda eletrônica ou similar;
- portar, após o início das provas, qualquer equipamento eletrônico e/ou sonoro e/ou de comunicação ligados ou desligados;
- comunicar-se com outro candidato ou terceiros, verbalmente ou por escrito, bem como fazer uso de material não permitido para a realização da prova;
- lançar meios ilícitos para a realização da prova;
- deixar de devolver ao fiscal qualquer material de aplicação da prova, fornecido pelo **IDECAN**;
- usar sanitários após o término da prova, ao deixar a sala.



INFORMAÇÕES GERAIS

- Verifique se o **CARGO** deste caderno de prova coincide com o registrado no cabeçalho de cada página e com o cargo para o qual você está inscrito. Caso contrário, notifique imediatamente o fiscal da sala, para que sejam tomadas as devidas providências.
- Confira seus dados pessoais, cargo, número de inscrição e documento de identidade e leia atentamente as instruções para preencher o **Cartão de Respostas**.
- Identifique no **Cartão de Respostas** o **TIPO** de caderno de prova, a não identificação no **Cartão de Respostas**, pelo candidato, acarretará em nota final igual a **0,00 (zero)**.
- Assine seu nome, no espaço reservado, com caneta esferográfica em material transparente, de tinta cor azul ou preta.
- Em hipótese alguma haverá substituição do **Cartão de Respostas** por erro do candidato.
- O candidato deverá transcrever as respostas da prova objetiva para o **Cartão de Respostas**, sendo este o único documento válido para a correção da prova. O preenchimento do **Cartão de Respostas** será de inteira responsabilidade do candidato, que deverá proceder em conformidade com as instruções específicas contidas no **Edital**, no **Caderno de Prova**, e no **Cartão de Respostas**.
- O **IDECAN** realizará identificação datiloscópica de todos os candidatos. A identificação datiloscópica compreenderá a coleta das impressões digitais dos candidatos.
- Ao terminar a prova, o candidato deverá, **OBRIGATORIAMENTE**, devolver ao fiscal o **Caderno de Prova** e o **Cartão de Respostas** devidamente assinados, apenas, nos locais indicados.
- Durante a realização da prova, o envelope de segurança com os equipamentos e materiais não permitidos, devidamente lacrado, deverá permanecer embaixo ou ao lado da carteira/cadeira utilizada pelo candidato, devendo permanecer lacrado durante toda a realização da prova e somente poderá ser aberto no ambiente externo do local de provas.
- Os **3 (três) últimos** candidatos de cada sala só poderão sair juntos.
- O gabarito oficial preliminar da prova será divulgado na Internet, no endereço eletrônico www.idecan.org.br, juntamente com os Cadernos de Prova, conforme Edital.

PREENCHA MANUALMENTE:

INSCRIÇÃO

NOME COMPLETO



CONHECIMENTOS COMUNS

Língua Portuguesa

- Texto para as questões de 1 a 10.

TECNOFEUDALISMO

No livro “Sobre a China”, Henry Kissinger elogia Mao Tsé-Tung por ter ordenado seu exército a se manter “comedido e probo” em antiga guerra da China contra a Índia. A vitória sobre posições indianas gerou nova fronteira. Mao determinou a volta ao limite anterior e a devolução dos armamentos pesados retidos. A China usou a força não para conquistar territórios, senão “para obrigar a Índia a voltar à mesa de negociações”. A China de hoje faria o mesmo? E Putin? E Trump? A mídia nos diz que este deseja tomar a Groenlândia, o Canadá e capturar Gaza. E, sem garantir a proteção aos ataques russos, exigiu da Ucrânia US\$ 500 bilhões em terras com minerais raros e 50% da renda gerada pela exploração desses recursos.

Em 2001, o consultor internacional Kenichi Ohmae lançou o livro “O Continente Invisível”. Nele destacou a descoberta e a colonização dos continentes e o advento da internet, “o continente invisível”, que, em seu dizer, seria colonizado, porém, com futuro imprevisível. Após 24 anos, Bolívar Torres, no “O Globo”, comenta o compêndio “Tecnofeudalismo”, de Yanis Varoufakis, ex-ministro das Finanças da Grécia, a ser lançado no Brasil em abril, em que o autor compara as *big techs* a senhores feudais e defende que o capitalismo morreu e foi substituído por algo pior.

Varoufakis afirma que os mercados teriam sido trocados “por plataformas de comércio digital que, na prática, operam como os antigos feudos. Os usuários digitais se tornariam ‘servos’, enquanto os detentores do capital tradicional [...] se limitariam ao papel de ‘vassalos’. E o lucro, motor do capitalismo, teria sido substituído por seu antecessor feudal: a renda. [...] Os usuários não são clientes no sentido clássico, mas servos que geram dados e precisam dessas plataformas para acessar informações, trabalho e serviços essenciais”. Para Arthur Bezerra, também citado por Torres, a influência das *big techs* sobre Trump leva muitos a achar que Elon Musk é o “verdadeiro” chefe de Estado dos EUA. Será o tecnofeudalismo uma das respostas às indagações de Kenichi Ohmae sobre o continente invisível? O futuro dirá.

Tales M. de Sá Cavalcante

1. Atente-se à significação e à função contextual da expressão **em seu dizer**, de modo a assinalar a alternativa correta em se tratando da intenção comunicativa modalizadora do articulista ao utilizá-la no trecho:

“Em 2001, o consultor internacional Kenichi Ohmae lançou o livro “O Continente Invisível”. Nele destacou a descoberta e a colonização dos continentes e o advento da internet, “o continente invisível”, que, **em seu dizer**, seria colonizado, porém, com futuro imprevisível.”

- (A) Deôntica por volição.
- (B) Deôntica por obrigação.
- (C) Epistêmica delimitadora.
- (D) Epistêmica asseverativa.
- (E) Epistêmica quase-asseverativa.

2. No livro “Sobre a China”, Henry Kissinger elogia Mao Tsé-Tung por ter ordenado seu exército a se manter “comedido e **probo**” em antiga guerra da China contra a Índia. **Probo**, nesse contexto, é o mesmo que

- (A) inane.
- (B) solerte.
- (C) argucioso.
- (D) hermético.
- (E) consciencioso.

3. “Em 2001, o consultor internacional Kenichi Ohmae lançou o livro “O Continente Invisível”. Nele destacou a descoberta e a colonização dos continentes e o advento da internet, “o continente invisível”, que, em seu dizer, seria colonizado, **porém**, com futuro imprevisível.

O termo demarcado, no excerto anterior, trata-se de um operador intraparagráfico adversativo, cuja função coesiva é

- (A) sequencial frástica.
- (B) sequencial parafrástica.
- (C) referencial elíptica.
- (D) referencial por pró-forma.
- (E) referencial por forma lexical.

4. “Varoufakis afirma **que**¹ os mercados teriam sido trocados “por plataformas de comércio digital **que**², na prática, operam como os antigos feudos [...]”

Os termos enumerados, no trecho em evidência, desempenham função de

- (A) pronome em 1 e em 2.
- (B) conjunção em 1 e em 2.
- (C) preposição em 1 e em 2.
- (D) conjunção em 1 e de pronome em 2.
- (E) pronome em 1 e de conjunção em 2.

5. A oração destacada, na passagem a seguir, é tipificada como

“Para Arthur Bezerra, também citado por Torres, a influência das *big techs* sobre Trump leva muitos a achar **que Elon Musk é o “verdadeiro” chefe de Estado dos EUA.**”

- (A) subordinada adverbial causal.
- (B) subordinada substantiva subjetiva.
- (C) subordinada adverbial consecutiva.
- (D) subordinada substantiva predicativa.
- (E) subordinada substantiva objetiva direta.

6. A regência verbal trata-se da relação de subordinação entre um verbo e um termo regido ou ainda da independência sintático-semântica de um verbo em relação ao processo de complementação. Partindo desse pressuposto, assinale a alternativa em que se descreve corretamente esse processo linguístico, tendo por base o verbo ressaltado no trecho “A mídia nos **diz** que este deseja tomar a Groenlândia, o Canadá e capturar Gaza.”

- (A) Regência transitiva direta, pois o verbo **dizer**, nesse contexto, é complementado por um objeto direto, a oração subsequente a ele.
- (B) Regência transitiva direta, uma vez que o verbo **dizer** é transitivo e não exige o auxílio de uma preposição para complementá-lo; sendo, dessa forma, o elemento sintático **nos** seu objeto direto.
- (C) Regência intransitiva, em que o verbo **dizer** possui autonomia sintático-semântica, sendo, portanto, a oração posposta a ele apenas um elemento circunstancial e acessório.
- (D) Regência bitransitiva, em que o pronome oblíquo **nos** desempenha a função sintática de objeto indireto do verbo **dizer**, e a oração subsequente ao verbo ressaltado tem função de objeto direto.
- (E) Regência transitiva indireta, porque, sendo o verbo **dizer** transitivo, seu complemento é introduzido por um elemento preposicionado (**que**), o qual liga o verbo realçado ao seu objeto indireto, a oração que o sucede.

7. O título do texto em voga, “**Tecnofeudalismo**”, apresenta um vocábulo composto etimologicamente por

- (A) síncope.
- (B) aférese.
- (C) apócope.
- (D) hibridismo.
- (E) braquissmia.

8. “A China de hoje **faria** o mesmo?”

No contexto em que se insere, a estrutura verbal demarcada indica

- (A) uma ação que ainda não aconteceu no momento da fala.
- (B) uma ação passada que ocorreu antes de outra, também no passado.
- (C) uma ação inacabada, ocorrida no passado, dando ideia de continuidade.
- (D) uma ação que ocorrerá em um futuro próximo, possibilitando que em breve algo irá acontecer.
- (E) uma ação que se refere a algo que poderia ter acontecido posteriormente a uma situação no passado.

9. “E o lucro, motor do capitalismo, teria sido substituído por **seu antecessor feudal¹: a renda².**”

A relação coesiva, respectivamente, entre o termo 1 e o 2, no período entre aspas, é do tipo

- (A) anafórica, pois resgata, de forma remissiva, um termo já citado anteriormente.
- (B) endofórica, estabelecendo uma relação semântica direta entre um termo hipônimo e outro hiperônimo.
- (C) epanofórica, indicando uma repetição semântica de intensidade entre um termo geral e outro mais específico.
- (D) catafórica, porque há a antecipação do referente em relação a um elemento linguístico que ainda será anunciado.
- (E) exóforica, ou seja, a referência apoia-se em uma evidência situacional compartilhada apenas pelos interlocutores do ato comunicativo.

10. Analise a passagem a seguir, a fim de demarcar o item correto a partir da função desempenhada pelo vocábulo ressaltado.

‘Após 24 anos, Bolívar Torres, no “O Globo”, comenta o compêndio “Tecnofeudalismo”, de Yanis Varoufakis, ex-ministro das Finanças da Grécia, a ser lançado no Brasil em abril, em **que** o autor compara as *big techs* a senhores feudais e defende que o capitalismo morreu e foi substituído por algo pior.’

- (A) Sua função é referencial, podendo ainda ser substituído por **onde**, sem infração à norma-padrão.
- (B) Sua função é remissiva e, como seu referente se trata do termo “**Tecnofeudalismo**”, deve ser mantido como conector universal.
- (C) Sua função é remissiva e, como seu referente se trata da locução **em abril**, o paralelismo **em que** foi mantido de forma a respeitar a norma-padrão.
- (D) Sua função é referencial e delimita-se à referência de um termo temporal, podendo ser substituído por **enquanto**, sem prejuízo sintático-semântico à sentença.
- (E) Sua função é referencial e delimita-se à substituição da locução adverbial **no Brasil**, podendo, junto à preposição **em**, ser trocado por **onde**, conectivo de termos locativos.

Raciocínio Lógico Matemático

11. Pedro recebeu seu salário e fez as seguintes transações: primeiro, gastou 25% em impostos. Em seguida, do que restou, investiu 20% em um fundo. Depois, pagou R\$ 600 em contas. Finalmente, do que sobrou, gastou 10% em lazer. Após todas essas transações, Pedro ficou com R\$ 1.620. Determine o valor original do salário de Pedro.

- (A) R\$ 2.000,00.
- (B) R\$ 3.600,00.
- (C) R\$ 4.000,00.
- (D) R\$ 4.500,00.
- (E) R\$ 5.000,00.

12. Em uma sequência de figuras geométricas, cada figura é composta por um número de triângulos. A primeira figura tem 1 triângulo, a segunda tem 3 triângulos, a terceira tem 6 triângulos, a quarta tem 10 triângulos, e assim por diante. Determine quantos triângulos estarão na sexta figura da sequência.

- (A) 16.
- (B) 19.
- (C) 21.
- (D) 23.
- (E) 25.

13. Um terreno tem a forma de um trapézio retângulo, com bases de 15 metros e 21 metros, e altura de 8 metros. Uma cerca será construída ao redor do terreno, mas apenas nos lados não paralelos (as laterais). Calcule o comprimento total da cerca necessária.

- (A) 15 metros.
- (B) 18 metros.
- (C) 21 metros.
- (D) 24 metros.
- (E) 26 metros.

14. Em uma sala de aula, há 9 meninos e 5 meninas. O professor precisa escolher 4 alunos para formar um grupo, mas com a condição de que haja pelo menos 2 meninas no grupo. Determine de quantas maneiras diferentes o professor pode formar esse grupo.

- (A) 230.
- (B) 325.
- (C) 430.
- (D) 455.
- (E) 520.

15. Dados os conjuntos $A = \{2, 4, 6, 8, 10\}$, $B = \{2, 3, 5, 7, 11\}$ e $C = \{4, 5, 6, 7, 8\}$, determine o conjunto $(A \cup B) \cap C$.

- (A) $\{2, 4, 6, 8\}$.
- (B) $\{4, 5, 6, 7, 8\}$.
- (C) $\{2, 4, 6, 7, 8, 10\}$.
- (D) $\{4, 6, 7, 8, 10\}$.
- (E) $\{2, 4, 6, 7\}$.

Informática

16. No Microsoft Excel 2021, diversas funções avançadas permitem automatizar cálculos e manipular grandes volumes de dados de maneira eficiente. Para otimizar o uso de referências dinâmicas e evitar erros em fórmulas, é essencial considerar que

- (A) a função ÍNDICE() no Excel retorna exclusivamente a posição numérica de um valor dentro de um intervalo de dados, sem permitir a extração do próprio valor contido na célula.
- (B) o operador & no Excel é utilizado para realizar operações matemáticas de adição entre valores numéricos em células distintas.
- (C) a função DESLOC() é utilizada para retornar a soma de um intervalo dinâmico de células sem precisar especificar a altura e a largura da área de referência.
- (D) o uso de referências absolutas, indicado pelo símbolo \$, impede qualquer modificação na célula referenciada, mesmo em operações de cópia e colagem para outras células da planilha.
- (E) a função ÍNDICE() pode ser utilizada para retornar o valor contido em uma célula específica de um intervalo de dados, permitindo a combinação com a função CORRESP() para localização dinâmica de valores.

17. No Windows 11, a manipulação de arquivos e pastas foi aprimorada para proporcionar maior eficiência e flexibilidade ao usuário. Considerando as funcionalidades e recursos do sistema, é correto afirmar que

- (A) o Windows 11 permite que um arquivo seja renomeado enquanto estiver em uso por outro programa, garantindo a integridade do sistema.
- (B) a opção “Cortar” e “Colar” pode ser utilizada para mover arquivos entre diferentes diretórios, mantendo a integridade dos dados e evitando a duplicação de arquivos.
- (C) o comando Ctrl + Z pode ser utilizado para desfazer qualquer ação realizada no Explorador de Arquivos, incluindo a recuperação de um arquivo permanentemente excluído da Lixeira.
- (D) a criação de um Ponto de Restauração no Windows 11 permite recuperar versões anteriores de arquivos individuais, independentemente de eles terem sido modificados ou excluídos.
- (E) a funcionalidade OneDrive Backup no Windows 11 impede que qualquer arquivo armazenado na nuvem seja acessado offline, exigindo conexão constante com a internet.

18. Os dispositivos de armazenamento desempenham um papel essencial na retenção, recuperação e proteção de dados em sistemas computacionais modernos. Em relação às tecnologias e características desses dispositivos, é correto afirmar que

- (A) os discos rígidos (HDDs) armazenam dados em células de memória flash, garantindo maior velocidade de acesso e menor latência em comparação aos SSDs.
- (B) a tecnologia NVMe (*Non-Volatile Memory Express*) é utilizada exclusivamente em dispositivos de armazenamento externo, como pen drives e cartões de memória.
- (C) o armazenamento em SSDs baseados em memória NAND Flash apresenta menor tempo de acesso aos dados e maior resistência a impactos físicos do que os HDDs convencionais.
- (D) a implementação da tecnologia RAID 0 aumenta a redundância dos dados ao armazená-los simultaneamente em discos diferentes, garantindo alta disponibilidade em caso de falha de um dos discos.
- (E) o sistema de arquivos NTFS não oferece suporte a permissões de segurança e criptografia de dados, tornando-o inadequado para ambientes empresariais que exigem controle de acesso.

19. Os navegadores web permitem que os usuários acessem páginas na internet, realizem buscas e imprimam conteúdos diretamente da interface. Para garantir um uso eficiente dessas funcionalidades, é essencial compreender que

- (A) o protocolo HTTPS é utilizado exclusivamente para sites governamentais e não pode ser implementado em sites de comércio eletrônico ou redes sociais.
- (B) a barra de endereços de um navegador aceita apenas URLs digitadas manualmente, sem permitir a utilização de mecanismos de busca ou sugestões automáticas.
- (C) a impressão de páginas da web pode ser ajustada diretamente no navegador, permitindo a exclusão de elementos desnecessários, como anúncios e rodapés, dependendo das configurações disponíveis.
- (D) os hiperlinks utilizados em páginas da web podem ser apenas do tipo absoluto, exigindo a especificação completa do endereço do site para redirecionamento.
- (E) o domínio de um site é apenas um identificador visual e não está relacionado ao endereço IP do servidor que hospeda a página acessada.

20. Os princípios básicos da informática abrangem conceitos fundamentais sobre hardware, software e funcionamento dos sistemas computacionais. No contexto da arquitetura e operação dos computadores, é correto afirmar que

- (A) o barramento de dados é responsável pela comunicação entre o processador e os dispositivos de entrada, saída e armazenamento, permitindo a transferência de informações dentro do sistema computacional.
- (B) a memória cache é um tipo de armazenamento não volátil que mantém os dados gravados mesmo após o desligamento do computador, sendo utilizada para preservar informações de uso frequente.
- (C) o sistema operacional é um software que realiza exclusivamente a interação entre o usuário e a interface gráfica, sem influenciar no gerenciamento de hardware ou na execução de processos.
- (D) a unidade de controle da CPU tem a função de executar cálculos matemáticos e operações lógicas, sendo responsável pela realização das operações aritméticas dentro do processador.
- (E) o *firmware* de um computador é um software de alto nível que permite ao usuário instalar aplicativos e realizar operações diretamente no sistema operacional, sem a necessidade de interação com o hardware.

Legislação

21. Regula a Constituição da República Federativa do Brasil que são direitos dos trabalhadores urbanos e rurais, além de outros que visem à melhoria de sua condição social:

- (A) jornada de oito horas para o trabalho realizado em turnos ininterruptos de revezamento, independentemente de negociação coletiva; dentre outros.
- (B) remuneração do trabalho diurno superior à do noturno; dentre outros.
- (C) salário-mínimo, fixado em lei, nacionalmente unificado, capaz de atender às suas necessidades vitais básicas e às de sua família com moradia, alimentação, educação, saúde, lazer, vestuário, higiene, transporte e previdência social, com reajustes periódicos que lhe preservem o poder aquisitivo, sendo vedada sua vinculação para qualquer fim; dentre outros.
- (D) licença à gestante, sem prejuízo do emprego e do salário, com a duração de cento e oitenta dias.
- (E) salário-família pago em razão do dependente do trabalhador, nos termos da lei; dentre outros.

22. À luz da CRFB/88, a União não intervirá nos Estados nem no Distrito Federal, exceto:

- (A) para reorganizar as finanças da unidade da Federação que suspender o pagamento da dívida fundada por mais de dois anos consecutivos, salvo motivo de força maior; dentre outros.
- (B) para assegurar a observância dos seguintes princípios constitucionais da autonomia privada; dentre outros.
- (C) para por termos o grave comprometimento da segurança pública; dentre outros.
- (D) para repelir invasão estrangeira; dentre outros.
- (E) para prover a execução de lei federal, ordem ou decisão judicial, desde que autorizada pelo STF; dentre outros.

23. A partir das lições emanadas da CFRB/88, para efeitos administrativos, a União poderá articular sua ação em um mesmo complexo geoeconômico e social, visando a seu desenvolvimento e à redução das desigualdades regionais. Assim, assinale a alternativa correta.

- (A) Os estados incentivarão a recuperação de terras áridas e cooperarão com os pequenos e médios proprietários rurais para o estabelecimento, em suas glebas, de fontes de água e de pequena irrigação.
- (B) Dependerá de sanção dos prefeitos a composição dos organismos regionais que executarão, na forma da lei, os planos regionais, integrantes dos planos nacionais de desenvolvimento econômico e social, aprovados juntamente com estes.
- (C) Sempre que possível, a concessão dos incentivos regionais a que se refere o art. 43, §2º, III (CFRB/88), considerará critérios de sustentabilidade ambiental e redução das emissões de carbono.
- (D) Lei delegada disporá sobre a composição dos organismos regionais que executarão, na forma da lei, os planos regionais, integrantes dos planos nacionais de desenvolvimento econômico e social, aprovados juntamente com estes.
- (E) Lei complementar disporá sobre isenções, reduções ou diferimento temporário de tributos federais devidos por pessoas físicas ou jurídicas.

24. Sabe-se que a Lei Federal nº 11.091, de 12/01/2005, dispõe sobre a estruturação do Plano de Carreira dos Cargos Técnico-Administrativos em Educação, no âmbito das Instituições Federais de Ensino vinculadas ao Ministério da Educação, e dá outras providências. Dentre outras especificidades, a posição do servidor na escala de vencimento da carreira em função do cargo e nível de classificação é corretamente chamada apenas de:

- (A) nível de classificação.
- (B) plano de carreira.
- (C) padrão de vencimento.
- (D) ambiente organizacional.
- (E) atribuição funcional.

25. Conforme regulado pelo Decreto Federal nº 1.171, de 22/06/1994, em todos os órgãos e entidades da Administração Pública Federal direta, indireta autárquica e fundacional, ou em qualquer órgão ou entidade que exerça atribuições delegadas pelo poder público, deverá ser criada uma Comissão de Ética, encarregada de:

- (A) fiscalizar o recebimento de qualquer tipo de ajuda financeira, gratificação, prêmio, comissão, doação ou vantagem de qualquer espécie, para si, familiares ou qualquer pessoa, para o cumprimento da sua missão ou para influenciar outro servidor para o mesmo fim.
- (B) orientar e aconselhar sobre a ética profissional do servidor, no tratamento com as pessoas e com o patrimônio público, competindo-lhe conhecer concretamente de imputação ou de procedimento susceptível de censura.
- (C) interferir no uso de artifícios para procrastinar ou dificultar o exercício regular de direito por qualquer pessoa, causando-lhe dano moral ou material.
- (D) coibir o uso de informações privilegiadas obtidas no âmbito interno de seu serviço, em benefício próprio, de parentes, de amigos ou de terceiros.
- (E) facilitar a todas as pressões de superiores hierárquicos, de contratantes, interessados e outros que visem obter quaisquer favores, benesses ou vantagens indevidas em decorrência de ações imorais, ilegais ou aéticas e denunciá-las.

26. Na forma da Lei Federal nº 14.133, de 01/04/2021, é inexigível a licitação quando inviável a competição, em especial nos casos de:

- (A) contratação que envolva valores inferiores a R\$ 50.000,00 (cinquenta mil reais), no caso de outros serviços e compras.
- (B) contratação que possa acarretar comprometimento da segurança nacional, nos casos estabelecidos pelo Ministro de Estado da Defesa, mediante demanda dos comandos das Forças Armadas ou dos demais ministérios.
- (C) aquisição de materiais, de equipamentos ou de gêneros ou contratação de serviços que só possam ser fornecidos por produtor, empresa ou representante comercial exclusivos.
- (D) a União tiver que intervir no domínio econômico para regular preços ou normalizar o abastecimento.
- (E) contratação de profissional do setor artístico, diretamente ou por meio de empresário exclusivo, desde que consagrado pela crítica especializada ou pela opinião pública; desde que alinhado com o espectro político da administração pública federal.

27. Vaticina a Lei Federal nº 14.133, de 01/04/2021, que o licitante ou o contratado será responsabilizado administrativamente pelas seguintes infrações:

- (A) não suportar os danos que provierem da Administração Pública.
- (B) ensejar o retardamento da execução ou da entrega do objeto da licitação com motivo justificado.
- (C) praticar atos ilícitos com vistas a frustrar os objetivos da administração pública.
- (D) comportar-se de modo inidôneo ou cometer fraude de qualquer natureza.
- (E) não manter a proposta, mesmo em decorrência de fato superveniente devidamente justificado.

28. Diploma a Lei Federal nº 14.133, de 01/04/2021, que as contratações públicas deverão submeter-se a práticas contínuas e permanentes de gestão de riscos e de controle preventivo, inclusive mediante adoção de recursos de tecnologia da informação, e, além de estar subordinadas ao controle social, sujeitar-se-ão à seguinte linha de defesa:

- (A) primeira linha de defesa, integrada pelo órgão central de controle interno da Administração e pelo tribunal de contas.
- (B) segunda linha de defesa, integrada por servidores e empregados públicos, agentes de licitação e autoridades que atuam na estrutura de governança do órgão ou entidade.
- (C) segunda linha de defesa, integrada pelo órgão central de controle interno da Administração e pelo tribunal de contas.
- (D) terceira linha de defesa, integrada por servidores e empregados públicos, agentes de licitação e autoridades que atuam na estrutura de governança do órgão ou entidade.
- (E) segunda linha de defesa, integrada pelas unidades de assessoramento jurídico e de controle interno do próprio órgão ou entidade.

29. Aduz a Lei Federal nº 8.112, de 11/12/1990, que dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais, ser o deslocamento do servidor, a pedido ou de ofício, no âmbito do mesmo quadro, com ou sem mudança de sede, chamado corretamente de:

- (A) Reversão.
- (B) Remoção.
- (C) Trânsito.
- (D) Reinstalação.
- (E) Exoneração.

30. Conforme dispõe a Lei Federal nº 8.112, de 11/12/1990, assinale o item que constitui indenização ao servidor.

- (A) Quinquênio.
- (B) Auxílio-moradia.
- (C) Salário-família.
- (D) Terço de Férias.
- (E) Adicionais.

31. Diz a Carta Magna que a República Federativa do Brasil, a administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência e, também, ao seguinte:

- (A) é garantido ao servidor público militar o direito à livre associação política; dentre outros.
- (B) os acréscimos pecuniários percebidos por servidor público não serão computados nem acumulados para fins de concessão de acréscimos ulteriores; dentre outros.
- (C) a lei estabelecerá os casos de contratação por tempo indeterminado para atender a necessidade temporária de excepcional interesse público; dentre outros.
- (D) é permitida a vinculação ou equiparação de quaisquer espécies remuneratórias para o efeito de remuneração de pessoal do serviço público; dentre outros.
- (E) o prazo de validade do concurso público será de até dois anos, prorrogável uma vez, por mais um ano; dentre outros.

32. Instam as disposições constitucionais gerais da Constituição da República Federativa do Brasil que:

- (A) nos dez primeiros anos da criação de Estado o Governo terá no máximo 15 (quinze) secretarias.
- (B) qualquer Tribunal de Justiça terá, no mínimo, dezessete Desembargadores.
- (C) o Colégio Pedro II, localizado na cidade do Rio de Janeiro, será mantido na órbita federal.
- (D) a fiscalização e o controle sobre o comércio exterior, essenciais à defesa dos interesses fazendários nacionais, serão exercidos pelo Ministério do Comércio Exterior.
- (E) os serviços notariais e de registro serão exercidos em caráter público.

33. Constitucionalmente, compete ao Conselho da República:

- (A) pronunciar-se sobre as questões relevantes para a estabilidade das instituições democráticas.
- (B) propor os critérios e condições de utilização de áreas indispensáveis à segurança do território nacional e opinar sobre seu efetivo uso, especialmente na faixa de fronteira e nas relacionadas com a preservação e a exploração dos recursos naturais de qualquer tipo.
- (C) estudar, propor e acompanhar o desenvolvimento de iniciativas necessárias a garantir a independência nacional e a defesa do Estado democrático.
- (D) decretar o bloqueio de sinais de rádio, televisão e internet.
- (E) opinar nas hipóteses de declaração de guerra e de celebração da paz, nos termos da própria Constituição.

34. Define a Lei Federal nº 12.527, de 18/11/2011, que dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações, que no caso de indeferimento de acesso a informações ou às razões da negativa do acesso, poderá o interessado interpor recurso contra a decisão, observadas as regras da própria lei, pelo que podemos apontar corretamente apenas o arrazoadado em:

- (A) Negado o acesso à informação pelos órgãos ou entidades do Poder Executivo Federal, o requerente poderá recorrer à Controladoria-Geral da União, que deliberará no prazo de 10 (dias).
- (B) Verificada a procedência das razões do recurso, a Controladoria-Geral da União recomendará ao órgão ou entidade que adote as providências necessárias para dar cumprimento ao disposto na própria Lei.
- (C) O recurso previsto na lei somente poderá ser dirigido à Controladoria-Geral da União depois de submetido à apreciação de pelo menos duas autoridades hierarquicamente superiores àquela que exarou a decisão impugnada, que deliberará no prazo de 15 (quinze) dias.
- (D) Negado o acesso à informação pela Controladoria-Geral da União, poderá ser interposto recurso à Comissão Mista de Reavaliação de Informações.
- (E) No caso de indeferimento de pedido de desclassificação de informação protocolado em órgão da administração pública federal, poderá o requerente recorrer ao Ministro de Estado da área, e este, por sua vez, acionar as competências da Comissão Mista de Reavaliação de Informações.

35. Balizado pela Lei Federal nº 9.784, de 29/01/1999, que regula o processo administrativo no âmbito da Administração Pública Federal, o administrado tem os seguintes direitos perante a Administração, sem prejuízo de outros que lhe sejam assegurados:

- (A) Expor os fatos conforme a verdade.
- (B) Formular alegações e apresentar documentos antes da decisão, os quais serão objeto de consideração pelo órgão competente.
- (C) Prestar as informações que lhe forem solicitadas e colaborar para o esclarecimento dos fatos.
- (D) Proceder com lealdade, urbanidade e boa-fé.
- (E) Agir de modo temerário.

36. Na forma estrita da CFRB/88, temos que são crimes de responsabilidade os atos do Presidente da República que atentem contra a Constituição Federal e, especialmente, contra:

- (A) o voto direto, secreto, universal e periódico.
- (B) o cumprimento das leis e das decisões judiciais, quando confirmadas pelo STF.
- (C) a autonomia das Forças Armadas.
- (D) o livre exercício do Poder Legislativo, do Poder Judiciário, do Ministério Público e dos Poderes constitucionais das unidades da Federação.
- (E) a segurança externa do país.

37. Tomando por base o prescrito e regulado pela Lei Federal nº 11.091, de 12/01/2005, temos que caberá à Instituição Federal de Ensino avaliar anualmente a adequação do quadro de pessoal às suas necessidades, propondo ao Ministério da Educação, se for o caso, o seu redimensionamento, consideradas, entre outras, as seguintes variáveis:

- (A) garantia de programas de capacitação que contemplem a formação específica e a geral, nesta incluída a educação formal.
- (B) vinculação ao planejamento estratégico e ao desenvolvimento organizacional das instituições.
- (C) dinâmica dos processos de pesquisa, de ensino, de extensão e de administração, e as competências específicas decorrentes.
- (D) inovações tecnológicas e modernização dos processos de trabalho no âmbito da Instituição.
- (E) reconhecimento do saber não instituído resultante da atuação profissional na dinâmica de ensino, de pesquisa e de extensão.

38. Quanto ao Procedimento Administrativo e do Processo Judicial previstos na Lei Federal nº 8.429, de 02/06/1992, que dispõe sobre as sanções aplicáveis em virtude da prática de atos de improbidade administrativa, marque a alternativa correta.

- (A) Será anulável a decisão de mérito total ou parcial da ação de improbidade administrativa que condenar o requerido por tipo diverso daquele definido na petição inicial.
- (B) Da decisão que converter a ação de improbidade em ação civil pública caberá embargos de declaração.
- (C) A assessoria jurídica que emitiu o parecer atestando a legalidade prévia dos atos administrativos praticados pelo administrador público não se obriga a defendê-lo judicialmente.
- (D) Da decisão que deferir ou indeferir a medida relativa à indisponibilidade de bens caberá recurso em sentido estrito, nos termos do Código de Processo Penal vigente.
- (E) Para cada ato de improbidade administrativa, deverá necessariamente ser indicado apenas um tipo dentre aqueles previstos nos arts. 9º, 10 e 11 da própria Lei.

39. Conforme vemos nas disposições penais da Lei Federal nº 8.429, de 02/06/1992, podemos assinalar corretamente apenas o que se afirma em:

- (A) A aplicação das sanções previstas na lei depende da efetiva ocorrência de dano ao patrimônio público.
- (B) A autoridade judicial competente deverá determinar o afastamento do agente público do exercício do cargo, do emprego ou da função, sem prejuízo da remuneração, quando a medida for necessária à instrução processual ou para evitar a iminente prática de novos ilícitos.
- (C) Sanções eventualmente aplicadas em outras esferas serão independentes das sanções aplicadas nos termos da própria Lei.
- (D) A autoridade policial poderá se valer da teoria do fruto da árvore envenenada no sentido de obter provas que permitam esclarecimento das condutas.
- (E) A autoridade judicial competente poderá determinar o afastamento do agente público do exercício do cargo, do emprego ou da função, sem prejuízo da remuneração, quando a medida for necessária à instrução processual ou para evitar a iminente prática de novos ilícitos.

40. Na forma da lei federal que regula o processo administrativo no âmbito da Administração Pública Federal, os atos do processo administrativo não dependem de forma determinada senão quando a lei expressamente a exigir. Dito isso, assinale a alternativa correta.

- (A) Os atos do processo devem realizar-se preferencialmente na sede do órgão, cientificando-se o interessado se outro for o local de realização.
- (B) Os atos do processo podem realizar-se fora dos dias úteis, no horário normal de funcionamento da repartição na qual tramitar o processo.
- (C) Serão concluídos depois do horário comercial padrão do local os atos já iniciados, cujo adiamento prejudique o curso regular do procedimento ou cause danos ao interessado ou à Administração.
- (D) O reconhecimento de firma somente será feito pelo próprio órgão administrativo.
- (E) Inexistindo disposição específica, os atos do órgão ou autoridade responsável pelo processo e dos administrados que dele participem devem ser praticados no prazo de dez dias úteis, salvo motivo de força maior.

CONHECIMENTOS ESPECÍFICOS

41. Uma instituição de pesquisa desenvolveu um sistema de análise de dados sensíveis na área da saúde, onde informações confidenciais de pacientes são processadas para geração de relatórios epidemiológicos. Devido ao caráter sigiloso dos dados e ao risco de exposição indevida, a equipe de segurança cibernética decidiu aplicar técnicas de modelagem de ameaças antes da implantação do sistema.

Durante a análise, os especialistas identificaram que o sistema pode ser vulnerável a ataques que exploram a elevação de privilégios, vazamento de dados e injeção de código malicioso. Para mitigar esses riscos, a equipe adotou o modelo STRIDE, desenvolvido pela Microsoft, visando uma categorização precisa das possíveis ameaças e a implementação de controles adequados.

Com base nessa abordagem, assinale a seguir a alternativa que apresenta corretamente as ameaças classificadas pelo modelo STRIDE e sua relação com os riscos identificados.

- (A) O modelo STRIDE categoriza as ameaças em seis grupos: *Spoofing*, *Tampering*, *Repudiation*, *Information Disclosure*, *Denial of Service* e *Elevation of Privilege*. No caso apresentado, a elevação de privilégios corresponde ao *Elevation of Privilege* (E), o vazamento de dados à *Information Disclosure* (I) e a injeção de código malicioso ao *Spoofing* (S).
- (B) O modelo STRIDE identifica apenas ameaças voltadas a infraestrutura e comunicação, não sendo adequado para análise de aplicações voltadas ao processamento de dados sensíveis.
- (C) No modelo STRIDE, as ameaças são classificadas em categorias baseadas nos impactos que causam aos ativos da organização, mas ele não cobre ataques relacionados à elevação de privilégios ou vazamento de dados.
- (D) STRIDE é um modelo voltado exclusivamente para identificação de ataques de negação de serviço (*Denial of Service*), sendo inadequado para avaliar ameaças como injeção de código malicioso.
- (E) O modelo STRIDE categoriza as ameaças de segurança em seis classes: *Spoofing* (S), *Tampering* (T), *Repudiation* (R), *Information Disclosure* (I), *Denial of Service* (D) e *Elevation of Privilege* (E). No caso apresentado, a elevação de privilégios corresponde a *Elevation of Privilege* (E), o vazamento de dados a *Information Disclosure* (I) e a injeção de código malicioso a *Tampering* (T).

42. Uma grande empresa do setor financeiro está expandindo sua infraestrutura de TI para suportar uma crescente demanda por serviços online. Para garantir a segurança e o desempenho da rede, a equipe de engenharia de redes precisa implementar mecanismos que garantam a comunicação confiável entre os servidores, otimizem o tráfego de pacotes e mitiguem ataques cibernéticos.

Durante a análise do tráfego da rede, foram identificados problemas como pacotes corrompidos, sessões interrompidas e falhas de retransmissão de dados críticos. A equipe suspeita que a origem desses problemas pode estar na camada de transporte do modelo TCP/IP, onde os protocolos TCP e UDP operam com diferentes características.

Com base nos conceitos de arquitetura e segurança de redes, assinale a seguir a alternativa que apresenta corretamente as diferenças entre TCP e UDP e como essas diferenças impactam a segurança e confiabilidade da comunicação.

- (A) O protocolo TCP (*Transmission Control Protocol*) garante confiabilidade na comunicação ao utilizar um mecanismo de *handshake* de três vias (*three-way handshake*) e retransmissão de pacotes perdidos. Já o UDP (*User Datagram Protocol*) é orientado à conexão, permitindo correções automáticas de pacotes corrompidos.
- (B) TCP é um protocolo de transporte que utiliza controle de fluxo e verificação de integridade para garantir que os pacotes sejam entregues corretamente e na ordem esperada. Já o UDP é um protocolo sem estado, sem garantias de entrega, sendo amplamente utilizado para aplicações em tempo real, como *streaming* e VoIP.
- (C) Diferente do TCP, que realiza verificações de integridade e retransmissão de pacotes perdidos, o UDP evita qualquer verificação, tornando-se mais vulnerável a ataques de *spoofing* e *man-in-the-middle*, mas garantindo maior segurança contra ataques de negação de serviço (DoS).
- (D) No modelo TCP/IP, tanto TCP quanto UDP garantem integridade e confiabilidade no transporte de dados. No entanto, TCP é mais rápido, pois utiliza menos *overhead* de processamento, enquanto UDP é usado para aplicações que exigem alta segurança, como VPNs e sistemas bancários.
- (E) O protocolo UDP é mais seguro que o TCP, pois não mantém estados de conexão e não é suscetível a ataques como SYN flood. Já o TCP utiliza *checksum* para correção de erros, mas não oferece retransmissão de pacotes, sendo menos confiável para aplicações críticas.

43. Uma instituição governamental precisa garantir a integridade, autenticidade e confidencialidade de documentos digitais que circulam entre seus departamentos. Para isso, foi decidido o uso de um sistema baseado em criptografia assimétrica e assinatura digital, utilizando algoritmos como RSA e SHA-256.

Durante a implementação, um dos desafios foi garantir que os documentos não sejam alterados sem detecção e que a identidade do remetente possa ser verificada de forma inequívoca. Além disso, a equipe de segurança precisou escolher entre os principais algoritmos de chave pública para equilibrar desempenho e nível de proteção.

Dado esse contexto, assinale a alternativa que apresenta corretamente o funcionamento da assinatura digital e sua relação com criptografia assimétrica.

- (A) A assinatura digital garante a confidencialidade dos documentos, pois utiliza apenas criptografia assimétrica para cifrar o conteúdo, garantindo que somente o destinatário possa acessá-lo.
- (B) No processo de assinatura digital, o remetente gera um *hash* do documento e cifra esse *hash* com sua chave privada. O destinatário, ao receber o documento, usa a chave pública do remetente para decifrar o *hash* e compará-lo com um novo *hash* gerado localmente, verificando assim a autenticidade e a integridade do documento.
- (C) Assinaturas digitais utilizam apenas criptografia simétrica, pois os algoritmos assimétricos são ineficientes para esse tipo de operação. Dessa forma, apenas quem compartilha a chave secreta pode validar a autenticidade do documento.
- (D) No modelo de assinatura digital, a chave privada é compartilhada entre os usuários para garantir que apenas destinatários autorizados possam validar a assinatura, impedindo que terceiros acessem o conteúdo dos documentos.
- (E) O principal objetivo da assinatura digital é garantir a confidencialidade, pois ela impede que terceiros leiam o conteúdo do documento sem a chave privada correta.

44. Uma empresa de tecnologia está migrando sua infraestrutura de servidores locais para um ambiente de computação em nuvem. Durante o planejamento da migração, a equipe técnica avaliou diferentes modelos de serviço disponíveis, como *IaaS (Infrastructure as a Service)*, *PaaS (Platform as a Service)* e *SaaS (Software as a Service)*, bem como diferentes modelos de implantação, como nuvem pública, privada e híbrida.

A empresa decidiu adotar uma solução híbrida, mantendo sistemas críticos em um ambiente privado enquanto utiliza uma nuvem pública para escalabilidade e serviços complementares. No entanto, uma preocupação central da equipe de segurança é garantir proteção de dados, conformidade regulatória e controle adequado dos acessos.

Com base nesse cenário, assinale a alternativa que melhor descreve os desafios e boas práticas de segurança em um ambiente de nuvem híbrida.

- (A) Em uma nuvem híbrida, a segurança dos dados é garantida integralmente pelo provedor de nuvem, eliminando a necessidade de controles internos por parte da empresa.
- (B) No modelo de nuvem híbrida, a organização deve adotar estratégias como criptografia de dados em repouso e em trânsito, gestão de identidade e acesso (IAM) e monitoramento contínuo de atividades para garantir segurança e conformidade.
- (C) A principal vantagem da nuvem híbrida é a eliminação da necessidade de um plano de contingência, pois a resiliência da infraestrutura de nuvem pública garante a disponibilidade contínua dos serviços críticos.
- (D) A migração para nuvem híbrida elimina a necessidade de configurar *firewalls*, VPNs ou mecanismos de autenticação multifator (MFA), pois a infraestrutura já fornece proteção integrada contra ameaças.
- (E) No modelo de nuvem híbrida, as responsabilidades de segurança são exclusivamente do provedor de nuvem, não havendo necessidade de monitoramento ativo por parte da empresa.

45. Uma grande organização está passando por uma reestruturação dos seus processos de Gestão de Serviços de TI para aumentar a eficiência operacional e garantir alinhamento com os objetivos estratégicos do negócio. Para isso, decidiu adotar *frameworks* reconhecidos como ITIL v4 e COBIT 2019, cada um com abordagens distintas para governança e gerenciamento de TI.

A equipe de TI foi encarregada de definir papéis, responsabilidades e processos de governança com base nessas metodologias. Um dos principais desafios foi garantir conformidade regulatória, gestão de riscos e entrega eficiente de serviços de TI para as diversas áreas da empresa.

Considerando as diferenças entre ITIL v4 e COBIT 2019, assinale a alternativa que melhor representa suas abordagens e como elas se complementam na governança e gestão de TI.

- (A) ITIL v4 se concentra exclusivamente na governança de TI, fornecendo um modelo prescritivo para tomada de decisão estratégica, enquanto COBIT 2019 é voltado apenas para a gestão de serviços operacionais.
- (B) ITIL v4 é um *framework* voltado para o gerenciamento de serviços de TI, focando no ciclo de vida dos serviços e na entrega de valor ao cliente, enquanto COBIT 2019 é um modelo de governança de TI, fornecendo diretrizes para a tomada de decisão estratégica, conformidade e gestão de riscos.
- (C) COBIT 2019 tem como principal objetivo a implementação de práticas ágeis e DevOps, sendo mais adequado para empresas que buscam modernização e inovação na gestão de TI do que o ITIL v4.
- (D) ITIL v4 e COBIT 2019 são *frameworks* concorrentes e incompatíveis entre si, pois possuem abordagens divergentes para a gestão de TI, impossibilitando sua aplicação conjunta em uma organização.
- (E) ITIL v4 trata exclusivamente da governança de TI em alto nível, sem definir diretrizes para gestão de serviços, enquanto COBIT 2019 foca apenas na operação diária de TI, sem ligação com a estratégia organizacional.

46. Uma grande empresa do setor financeiro enfrenta desafios crescentes relacionados à segurança cibernética, especialmente devido ao aumento de ataques direcionados, como *ransomware*, *spear phishing* e exploração de vulnerabilidades *zero-day*. Para mitigar riscos e reduzir o tempo de resposta a incidentes, a organização decidiu investir em uma abordagem baseada em SIEM (*Security Information and Event Management*), EDR (*Endpoint Detection and Response*) e SOAR (*Security Orchestration, Automation and Response*).

A equipe de segurança busca aprimorar sua capacidade de identificação, análise, resposta e mitigação de ameaças em tempo real. No entanto, um dos desafios enfrentados é garantir integração eficiente entre as soluções, correlação de eventos e automação de processos de resposta, minimizando o impacto de ataques.

Diante desse cenário, assinale a alternativa que descreve corretamente as funções e a relação entre SIEM, EDR e SOAR no contexto da detecção e resposta a incidentes.

- (A) O SIEM (*Security Information and Event Management*) é responsável exclusivamente pelo bloqueio de ataques em tempo real, enquanto o SOAR se limita à coleta de logs sem executar nenhuma automação de resposta.
- (B) O EDR (*Endpoint Detection and Response*) é um sistema que substitui completamente a necessidade de um SIEM, pois já realiza correlação de eventos de segurança e automação de resposta a incidentes.
- (C) O SOAR (*Security Orchestration, Automation and Response*) tem como principal função substituir o SIEM e o EDR, integrando diretamente sistemas de firewall e antivírus para bloquear ameaças sem necessidade de monitoramento humano.
- (D) O SIEM é responsável pelo gerenciamento de logs, mas não permite correlação de eventos ou análise forense, tornando-se ineficaz para detecção de ameaças avançadas.
- (E) O SIEM centraliza e correlaciona logs de diversos sistemas para identificar padrões suspeitos, o EDR monitora e responde a ameaças em *endpoints* (dispositivos finais), e o SOAR automatiza e padroniza fluxos de resposta a incidentes, permitindo ações rápidas e coordenadas contra ataques cibernéticos.

47. Uma startup brasileira especializada em análise de dados utiliza algoritmos avançados de *machine learning* para processar informações de clientes e oferecer recomendações personalizadas. Para expandir seu mercado, a empresa pretende operar na União Europeia e, para isso, precisa garantir conformidade tanto com a Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018) quanto com o Regulamento Geral sobre a Proteção de Dados (GDPR - *General Data Protection Regulation*, da União Europeia). A equipe jurídica da startup identificou que ambas as regulamentações compartilham princípios fundamentais, como transparência, segurança, responsabilização e direitos do titular dos dados. No entanto, algumas diferenças precisam ser consideradas para garantir que a operação internacional cumpra as exigências de cada legislação.

Diante desse contexto, assinale a alternativa que descreve corretamente um aspecto fundamental da conformidade com LGPD e GDPR.

- (A) A LGPD e o GDPR possuem princípios semelhantes, como transparência e segurança, mas o GDPR impõe regras mais rigorosas sobre transferência internacional de dados, exigindo garantias adicionais, como cláusulas contratuais específicas ou certificações de proteção de dados.
- (B) Diferente do GDPR, a LGPD não concede aos titulares dos dados o direito à portabilidade, impedindo que usuários transfiram seus dados entre diferentes serviços de forma automatizada.
- (C) No GDPR, as multas por não conformidade são limitadas a valores simbólicos, sem impacto significativo nas operações empresariais, ao contrário da LGPD, que estabelece penalidades financeiras elevadas para infrações graves.
- (D) Enquanto a LGPD permite a coleta e o processamento de dados pessoais sem consentimento do titular em qualquer circunstância, o GDPR exige que toda coleta de dados seja baseada exclusivamente em consentimento explícito.
- (E) No Brasil, a LGPD estabelece um modelo de responsabilidade exclusiva para o controlador de dados, isentando operadores de qualquer penalidade, enquanto no GDPR tanto controladores quanto operadores podem ser responsabilizados por incidentes de segurança.

48. Uma empresa de grande porte está expandindo sua infraestrutura de TI para suportar um aumento no tráfego de rede e novas aplicações baseadas em IoT (Internet das Coisas). Como parte dessa modernização, a equipe de redes identificou a necessidade de migrar parte da sua infraestrutura para IPv6, garantindo maior escalabilidade e segurança.

Durante a implementação, os administradores de rede precisaram compreender as diferenças fundamentais entre os protocolos IPv4 e IPv6, especialmente no que diz respeito a endereçamento, roteamento e segurança. Além disso, a equipe considerou a adoção de mecanismos de transição entre IPv4 e IPv6, como *dual stack*, tunelamento e tradução de endereços (NAT64 e NAT-PT).

Diante desse cenário, assinale a alternativa que apresenta corretamente uma característica do IPv6 que o diferencia do IPv4.

- (A) Diferente do IPv4, onde os endereços IP podem ser atribuídos de forma estática ou dinâmica, no IPv6 a atribuição de endereços é exclusivamente manual, eliminando a necessidade de protocolos como DHCP.
- (B) No IPv6, os endereços possuem 48 bits de comprimento, permitindo maior escalabilidade e alocação eficiente de sub-redes, enquanto no IPv4 os endereços possuem 32 bits.
- (C) O protocolo IPv6 elimina a necessidade de qualquer forma de tradução de endereços (NAT), garantindo compatibilidade total e direta com redes IPv4 sem necessidade de mecanismos de transição.
- (D) O IPv6 incorpora nativamente o IPsec (*Internet Protocol Security*), garantindo maior segurança nas comunicações sem depender de configurações adicionais, enquanto no IPv4 o IPsec é opcional e deve ser implementado manualmente.
- (E) Ao contrário do IPv4, que utiliza o conceito de ARP (*Address Resolution Protocol*) para mapear endereços IP para endereços MAC, o IPv6 mantém esse mesmo mecanismo, garantindo compatibilidade total entre os dois protocolos.

49. Uma empresa de tecnologia está desenvolvendo um novo sistema de gestão financeira baseado em arquitetura web e precisa garantir que sua aplicação esteja protegida contra ameaças comuns, como injeção de código, vazamento de informações e exploração de vulnerabilidades conhecidas. Para isso, a equipe de segurança implementou uma abordagem de desenvolvimento seguro, integrando testes automatizados ao longo do ciclo de vida do software.

A organização avaliou diferentes técnicas de análise e decidiu combinar SAST (*Static Application Security Testing*), DAST (*Dynamic Application Security Testing*) e IAST (*Interactive Application Security Testing*) para aprimorar a detecção e mitigação de vulnerabilidades.

Diante desse cenário, assinale a alternativa que descreve corretamente as diferenças entre SAST, DAST e IAST e como elas contribuem para o desenvolvimento seguro.

- (A) O SAST é uma técnica de teste dinâmico que analisa a aplicação em tempo de execução para identificar falhas de segurança exploráveis durante sua execução normal.
- (B) O DAST é um método de análise estática que examina o código-fonte da aplicação antes da compilação, permitindo identificar vulnerabilidades sem a necessidade de execução.
- (C) O IAST é uma abordagem puramente manual, baseada em testes exploratórios conduzidos por especialistas em segurança para encontrar vulnerabilidades impossíveis de serem detectadas automaticamente.
- (D) O SAST e o DAST são métodos equivalentes e podem ser usados de forma intercambiável, pois ambos testam o código-fonte da aplicação antes da sua implantação.
- (E) O SAST analisa o código-fonte estaticamente antes da execução, identificando falhas estruturais e lógicas; o DAST testa a aplicação em execução, simulando ataques externos; e o IAST combina elementos de ambos, analisando o comportamento da aplicação em tempo real durante sua execução.

50. Uma *fintech* especializada em transações financeiras internacionais está avaliando a adoção de uma solução baseada em *blockchain* para aumentar a segurança, transparência e eficiência no processamento de pagamentos entre diferentes países.

A equipe de tecnologia precisa compreender os mecanismos de consenso, a imutabilidade dos registros e as diferenças entre *blockchains* públicas, privadas e permissionadas para tomar uma decisão estratégica sobre qual modelo se adapta melhor ao negócio.

Além disso, um dos desafios enfrentados é garantir proteção contra ataques, como o ataque de 51%, além de equilibrar descentralização e desempenho.

Diante desse cenário, assinale a alternativa que descreve corretamente um aspecto fundamental do funcionamento do *blockchain* e seus mecanismos de segurança.

- (A) Em *blockchains* públicas, as transações são privadas e acessíveis apenas para os nós validados da rede, garantindo anonimato absoluto e impedindo qualquer rastreamento de transações.
- (B) O *blockchain* permite a alteração retroativa dos blocos já registrados por meio de consenso entre os nós participantes, garantindo maior flexibilidade para ajustes em transações passadas.
- (C) O mecanismo de consenso *Proof of Work* (PoW) protege a rede contra ataques, pois exige um alto custo computacional para validar blocos, tornando inviável um ataque de 51%, onde um invasor tenta controlar a maioria do poder de mineração.
- (D) O uso de *blockchain* elimina a necessidade de qualquer mecanismo de criptografia, pois a segurança da rede é garantida apenas pela descentralização dos nós participantes.
- (E) Em *blockchains* privadas, qualquer usuário pode participar da rede e validar transações sem necessidade de autorização prévia, garantindo o mesmo nível de descentralização de *blockchains* públicas.

51. Uma equipe de desenvolvimento de software foi encarregada de criar um novo sistema de gestão acadêmica para uma instituição de ensino. Para garantir eficiência, flexibilidade e entregas incrementais, a equipe decidiu adotar o *Scrum* como metodologia ágil, integrando práticas de gestão de ciclo de vida do desenvolvimento de software (SDLC).

Durante o planejamento do projeto, o *Scrum Master* destacou a importância de papéis, eventos e artefatos do *Scrum*, bem como a necessidade de alinhar essas práticas às fases tradicionais do SDLC, garantindo qualidade e previsibilidade nas entregas.

Diante desse cenário, assinale a alternativa que descreve corretamente a relação entre *Scrum* e SDLC no contexto do desenvolvimento de software ágil.

- (A) No *Scrum*, a equipe de desenvolvimento trabalha sem a necessidade de planejamento formal ou definição de requisitos, pois o *framework* ágil elimina qualquer documentação prévia.
- (B) O SDLC tradicional e o *Scrum* são modelos incompatíveis, pois o SDLC segue um processo rígido e linear, enquanto o *Scrum* adota um fluxo contínuo e iterativo, tornando impossível sua integração.
- (C) O *Scrum* pode ser integrado ao SDLC ao adotar ciclos iterativos de desenvolvimento, nos quais cada *Sprint* corresponde a uma fase incremental do SDLC, permitindo entregas contínuas e *feedback* rápido.
- (D) No *Scrum*, o *backlog* do produto é equivalente à fase de codificação do SDLC, eliminando a necessidade de planejamento detalhado ou revisões formais de requisitos.
- (E) O uso de *Scrum* elimina qualquer necessidade de fases de testes e validação, pois a metodologia prioriza a entrega rápida e incremental, sem necessidade de revisões estruturadas.

52. Uma grande corporação implementou um Centro de Operações de Segurança (SOC) para aprimorar a proteção de sua infraestrutura de TI contra ameaças cibernéticas. Como parte da estratégia, a equipe de segurança configurou um *firewall* de próxima geração (NGFW), um sistema de detecção e prevenção de intrusão (IDS/IPS) e uma solução de monitoramento de tráfego de rede (SIEM).

Apesar dessas medidas, incidentes de tentativas de acesso não autorizado, exploração de vulnerabilidades e movimentação lateral de atacantes continuam sendo detectados. Para mitigar esses riscos, a equipe precisa compreender as funções e limitações das tecnologias implementadas e avaliar ajustes necessários para reforçar a segurança.

Diante desse contexto, assinale a alternativa que descreve corretamente a função de *firewalls*, IDS/IPS e monitoramento de tráfego na defesa contra ameaças cibernéticas.

- (A) O *firewall* de próxima geração (NGFW) protege contra ataques internos e externos, substituindo completamente a necessidade de um IDS/IPS ou monitoramento de tráfego em redes corporativas.
- (B) O *firewall* atua como a primeira linha de defesa, filtrando tráfego com base em regras predefinidas; o IDS/IPS monitora atividades suspeitas e ataques em tempo real, enquanto o SIEM correlaciona eventos de segurança e fornece alertas detalhados sobre incidentes, permitindo uma resposta mais eficiente.
- (C) O IDS/IPS é responsável apenas pela detecção de ataques externos e não influencia o tráfego dentro da rede, pois sua atuação se limita à borda da infraestrutura corporativa.
- (D) Um *firewall* de próxima geração (NGFW) pode detectar e bloquear ataques internos automaticamente sem necessidade de um IDS/IPS ou SIEM, pois possui inteligência artificial embarcada para prever qualquer ameaça.
- (E) A função principal de um IDS/IPS é garantir que apenas usuários autenticados acessem a rede, eliminando a necessidade de políticas de controle de acesso (IAM) e autenticação multifator (MFA).

53. Uma empresa de desenvolvimento de software está expandindo suas operações e decidiu migrar parte de sua infraestrutura para a nuvem, buscando escalabilidade, redução de custos e maior disponibilidade.

Durante a fase de planejamento, a equipe técnica avaliou diferentes modelos de serviço de computação em nuvem, incluindo IaaS (*Infrastructure as a Service*), PaaS (*Platform as a Service*) e SaaS (*Software as a Service*), e analisou os desafios de segurança envolvidos na adoção da nuvem pública, privada e híbrida.

A equipe precisa tomar decisões estratégicas sobre quais camadas da infraestrutura serão gerenciadas internamente e quais serão delegadas ao provedor de nuvem, considerando segurança, flexibilidade e responsabilidade compartilhada.

Diante desse contexto, assinale a alternativa que descreve corretamente os modelos de serviço de nuvem e suas diferenças na gestão da infraestrutura.

- (A) No modelo IaaS, o provedor de nuvem gerencia toda a infraestrutura, incluindo o sistema operacional e os aplicativos, permitindo que os clientes se concentrem apenas no desenvolvimento de software.
- (B) No modelo SaaS, o usuário final é responsável pela manutenção da infraestrutura e da segurança dos dados armazenados na nuvem, enquanto o provedor gerencia apenas a conectividade e a disponibilidade do serviço.
- (C) No modelo IaaS, o cliente gerencia apenas os aplicativos e bancos de dados, enquanto o provedor cuida da infraestrutura e do código das aplicações hospedadas na nuvem.
- (D) No modelo PaaS, a infraestrutura subjacente, incluindo servidores, armazenamento e sistema operacional, é gerenciada pelo provedor, enquanto os desenvolvedores têm controle sobre a criação e execução de aplicações, sem se preocupar com a configuração do ambiente.
- (E) No modelo PaaS, o provedor fornece apenas servidores físicos e conectividade de rede, exigindo que o cliente instale e configure todo o ambiente operacional e suas dependências.

54. Uma empresa do setor financeiro está implementando um novo sistema de autenticação e proteção de dados sensíveis para transações bancárias online. Para garantir segurança, integridade e autenticidade, a equipe de TI avaliou diferentes técnicas criptográficas, incluindo criptografia simétrica e assimétrica, além de métodos de assinatura digital.

Durante a análise, os especialistas identificaram que as transações precisam ser rápidas e seguras, exigindo um equilíbrio entre desempenho e robustez criptográfica. Além disso, a equipe considerou o uso de protocolos como TLS (*Transport Layer Security*) para proteger a comunicação entre os clientes e os servidores bancários.

Diante desse cenário, assinale a alternativa que descreve corretamente uma diferença fundamental entre criptografia simétrica e assimétrica e sua aplicação na segurança da informação.

- (A) A criptografia simétrica utiliza a mesma chave para cifrar e decifrar dados, tornando-a mais rápida que a criptografia assimétrica, que usa um par de chaves (pública e privada), sendo mais adequada para troca segura de chaves e assinaturas digitais.
- (B) Na criptografia assimétrica, a mesma chave é usada para criptografar e descriptografar os dados, garantindo maior eficiência computacional e segurança em comparação com a criptografia simétrica.
- (C) A criptografia simétrica não pode ser usada para proteger dados em comunicação de redes, pois requer um método de troca de chaves inseguro, tornando-a obsoleta em aplicações modernas.
- (D) A criptografia assimétrica é mais rápida que a simétrica, pois exige menos processamento para cifrar e decifrar dados, sendo amplamente utilizada para grandes volumes de informação.
- (E) Em um ambiente de segurança digital, a criptografia simétrica é exclusivamente utilizada para assinaturas digitais, enquanto a criptografia assimétrica é usada apenas para criptografia de dados em repouso.

55. Uma grande organização do setor de telecomunicações identificou um aumento significativo em tentativas de ataques cibernéticos, incluindo movimentação lateral na rede, persistência de ameaças e roubo de credenciais.

Para fortalecer sua estratégia de defesa, a equipe de segurança adotou o *framework* MITRE ATT&CK, que fornece um modelo de referência baseado em táticas e técnicas utilizadas por adversários reais. O objetivo é aprimorar a detecção de ameaças, desenvolver mecanismos de mitigação e estruturar uma resposta eficiente a incidentes.

Com base nesse contexto, assinale a alternativa que descreve corretamente a função do *framework* MITRE ATT&CK na cibersegurança.

- (A) O MITRE ATT&CK é um framework que organiza e categoriza táticas e técnicas utilizadas por atacantes durante o ciclo de um ataque cibernético, auxiliando equipes de segurança na identificação, mitigação e resposta a ameaças.
- (B) O MITRE ATT&CK é uma base de dados exclusiva para empresas do setor financeiro, contendo registros históricos de ataques reais, mas sem aplicação direta na detecção e mitigação de ameaças em outros setores.
- (C) O *framework* MITRE ATT&CK substitui completamente outras metodologias de segurança, eliminando a necessidade de soluções como *firewalls*, IDS/IPS e SIEMs, pois cobre todos os aspectos da proteção contra ataques.
- (D) O MITRE ATT&CK é uma ferramenta de proteção que bloqueia automaticamente ataques em tempo real, sem necessidade de configuração ou integração com outras soluções de segurança.
- (E) O MITRE ATT&CK é um modelo de governança de TI focado exclusivamente em requisitos regulatórios, sendo utilizado apenas para auditorias e conformidade, sem impacto direto na resposta a ameaças cibernéticas.

56. Uma empresa de tecnologia especializada em serviços de computação em nuvem está aprimorando sua política de gestão de identidade e acesso (IAM) para mitigar riscos relacionados a acessos não autorizados, vazamento de credenciais e ataques de escalonamento de privilégios.

Como parte da nova estratégia de segurança, a equipe de TI implementou mecanismos de autenticação multifator (MFA), controle baseado em papéis (RBAC) e princípios de privilégio mínimo para garantir que cada usuário tenha apenas as permissões estritamente necessárias para suas funções.

Além disso, a organização adotou soluções de log centralizado e auditoria contínua para monitorar atividades suspeitas e detectar anomalias no acesso a recursos críticos.

Diante desse cenário, assinale a alternativa que representa corretamente um princípio essencial da gestão de identidade e acesso (IAM).

- (A) A autenticação multifator (MFA) permite que um usuário acesse sistemas críticos com apenas um fator de autenticação (por exemplo, senha), desde que o acesso ocorra a partir de um dispositivo confiável.
- (B) No modelo de controle de acesso baseado em papéis (RBAC), as permissões são concedidas diretamente a cada usuário individualmente, eliminando a necessidade de agrupar usuários em funções específicas.
- (C) O princípio do privilégio mínimo (PoLP) estabelece que cada usuário, sistema ou processo deve receber apenas as permissões estritamente necessárias para executar suas funções, reduzindo riscos de exploração de credenciais comprometidas.
- (D) A gestão de identidade e acesso (IAM) substitui completamente a necessidade de monitoramento de logs e auditoria, pois a aplicação de regras de acesso é suficiente para garantir segurança.
- (E) Em um ambiente de segurança *zero trust*, os usuários autenticados dentro da rede corporativa são considerados confiáveis, eliminando a necessidade de reautenticação ao acessar os recursos críticos.

57. Uma multinacional que opera em diversos países precisa garantir a segurança e integridade das comunicações entre suas filiais, protegendo os dados transmitidos contra interceptações e ataques cibernéticos. Para isso, a equipe de TI está avaliando diferentes soluções de proteção de tráfego de rede, incluindo VPNs (*Virtual Private Networks*), *firewalls* e servidores proxy.

O objetivo é implementar uma infraestrutura que controle acessos, proteja contra ataques externos e forneça conexões seguras para funcionários remotos. Além disso, a empresa precisa evitar que usuários internos acessem conteúdos não autorizados e minimizar riscos de exposição a sites maliciosos.

Diante desse cenário, assinale a alternativa que descreve corretamente o papel das VPNs, *firewalls* e proxies na segurança de redes corporativas.

- (A) O *firewall* atua como uma barreira contra ameaças externas, mas não é capaz de bloquear tráfego interno malicioso nem impedir a comunicação com sites suspeitos.
- (B) O servidor proxy é uma tecnologia equivalente à VPN, pois ambos garantem comunicação segura e criptografada de ponta a ponta, eliminando a necessidade de *firewalls*.
- (C) O *firewall* de próxima geração (NGFW) elimina a necessidade de VPNs em redes corporativas, pois pode realizar tunelamento seguro e substituir totalmente os mecanismos de criptografia de tráfego.
- (D) Uma VPN garante apenas privacidade da navegação, mas não protege a integridade dos dados transmitidos nem impede a interceptação por atacantes durante a comunicação.
- (E) O *firewall* controla o tráfego de rede bloqueando ameaças e acessos não autorizados, a VPN protege a transmissão de dados criando túneis criptografados entre redes, e o proxy atua como intermediário, filtrando conteúdos acessados e reforçando políticas de segurança.

58. Uma organização do setor público está aprimorando sua governança de TI para garantir que a tecnologia da informação esteja alinhada aos objetivos estratégicos do negócio e que os riscos sejam devidamente gerenciados. Para isso, a empresa decidiu adotar o COBIT 2019 (*Control Objectives for Information and Related Technologies*), um *framework* que fornece diretrizes para gestão e governança eficazes de TI.

Além disso, a organização implementou um modelo de Gestão de Riscos baseado na norma ISO/IEC 27005:2019, focado na identificação, avaliação e mitigação de riscos de segurança da informação.

Diante desse cenário, assinale a alternativa que descreve corretamente a relação entre COBIT 2019 e a gestão de riscos em TI.

- (A) O COBIT 2019 é um modelo exclusivo para gerenciamento de serviços de TI e não inclui diretrizes para gestão de riscos ou conformidade regulatória.
- (B) A ISO/IEC 27005:2019 estabelece diretrizes para auditoria de TI, mas não se relaciona com a governança de TI definida pelo COBIT 2019.
- (C) O COBIT 2019 substitui completamente a necessidade de normas como a ISO/IEC 27005:2019, pois já abrange todos os aspectos da segurança da informação e da gestão de riscos em TI.
- (D) O COBIT 2019 fornece um modelo estruturado de governança de TI que inclui diretrizes para gestão de riscos, alinhando a tecnologia com os objetivos estratégicos da organização, enquanto a ISO/IEC 27005:2019 detalha metodologias específicas para análise e tratamento de riscos de segurança da informação.
- (E) O principal objetivo do COBIT 2019 é fornecer um guia técnico para implementação de infraestrutura de TI, sem relação com gestão de riscos ou governança corporativa.

59. Uma empresa do setor de logística e transporte está implementando um sistema baseado em Internet das Coisas (IoT) para rastreamento em tempo real da frota de veículos e monitoramento das condições de carga.

Os dispositivos IoT instalados nos veículos enviam dados constantemente para servidores na nuvem, incluindo localização GPS, temperatura interna dos compartimentos de carga e nível de combustível. Esses dados precisam ser processados e analisados para otimizar rotas, prevenir falhas mecânicas e garantir que os produtos transportados permaneçam em condições ideais.

No entanto, a equipe de TI da empresa identificou desafios relacionados à latência, segurança na transmissão dos dados e interoperabilidade entre dispositivos IoT de diferentes fabricantes.

Diante desse cenário, assinale a alternativa que apresenta corretamente um protocolo eficiente para comunicação segura entre dispositivos IoT e servidores na nuvem.

- (A) O protocolo HTTP é a melhor escolha para IoT, pois permite comunicação direta entre dispositivos e servidores sem necessidade de otimização para redes de baixa largura de banda.
- (B) O protocolo FTP é amplamente utilizado para comunicação IoT, pois garante segurança na transmissão de dados e suporta ambientes de conectividade intermitente.
- (C) O protocolo ICMP é a melhor opção para IoT, pois fornece suporte para controle de fluxo de dados e comunicação bidirecional entre sensores e servidores.
- (D) O MQTT (*Message Queuing Telemetry Transport*) é um protocolo eficiente para IoT, pois utiliza um modelo de comunicação assíncrono baseado em publicadores e assinantes, sendo otimizado para redes instáveis e dispositivos com recursos limitados.
- (E) O SMTP é um protocolo essencial para IoT, pois permite que dispositivos conectados enviem grandes volumes de dados diretamente para servidores de e-mail, garantindo integridade e baixa latência.

60. Uma grande empresa do setor financeiro foi vítima de um ataque de *ransomware*, no qual os sistemas críticos foram criptografados e os atacantes exigiram um pagamento em criptomoedas para fornecer a chave de recuperação.

A equipe de segurança identificou que o ataque teve origem em um arquivo malicioso baixado por um funcionário, explorando uma vulnerabilidade conhecida no sistema operacional e se espalhando rapidamente pela rede corporativa. Como contramedida, a organização implementou um plano de prevenção, detecção e resposta para evitar futuros incidentes, incluindo:

Uso de soluções de EDR (*Endpoint Detection and Response*);

Monitoramento contínuo com SIEM (*Security Information and Event Management*);

Aplicação de políticas de backup e restauração segura;

Educação e treinamento dos funcionários sobre ameaças cibernéticas.

Diante desse cenário, assinale a alternativa que apresenta uma medida essencial para mitigar ataques de *ransomware* e reduzir o impacto de futuras infecções.

- (A) O uso exclusivo de *firewalls* NGFW (*Next-Generation Firewall*) é suficiente para impedir ataques de *ransomware*, pois bloqueia qualquer tráfego malicioso e elimina a necessidade de antivírus ou backups.
- (B) A detecção baseada em assinaturas é a abordagem mais eficaz contra *ransomwares* modernos, pois permite bloquear novas variantes antes que elas sejam executadas no sistema.
- (C) A estratégia de backup e restauração segura, utilizando o modelo 3-2-1 (três cópias dos dados, em dois tipos de mídia, com uma cópia *offline*), é fundamental para garantir a recuperação dos sistemas após um ataque de *ransomware*.
- (D) Uma vez que um *ransomware* criptografa os arquivos, não há solução para recuperação, sendo o pagamento do resgate a única alternativa para restaurar os sistemas afetados.
- (E) A desativação do registro de logs nos servidores ajuda a impedir que *ransomwares* monitorem a atividade da rede e, consequentemente, reduz a superfície de ataque.

61. Uma empresa do setor de tecnologia deseja certificar-se conforme a norma ABNT NBR ISO/IEC 27001:2022 para fortalecer a gestão da segurança da informação e garantir conformidade com boas práticas globais.

Para isso, a organização precisa implementar um Sistema de Gestão de Segurança da Informação (SGSI), estruturando políticas, processos e controles para proteger a confidencialidade, integridade e disponibilidade dos dados.

Além disso, a equipe responsável pelo projeto identificou que a norma ABNT NBR ISO/IEC 27002:2022 fornece diretrizes complementares para a seleção e implementação de controles específicos de segurança.

Diante desse contexto, assinale a alternativa que descreve corretamente a relação entre a ABNT NBR ISO/IEC 27001:2022 e a ABNT NBR ISO/IEC 27002:2022.

- (A) A norma ABNT NBR ISO/IEC 27001:2022 define os requisitos para a implementação e certificação de um Sistema de Gestão de Segurança da Informação (SGSI), enquanto a ABNT NBR ISO/IEC 27002:2022 fornece diretrizes para a seleção e implementação de controles de segurança.
- (B) A norma ABNT NBR ISO/IEC 27002:2022 estabelece os requisitos obrigatórios para certificação em segurança da informação, enquanto a ABNT NBR ISO/IEC 27001:2022 apenas sugere boas práticas sem necessidade de auditoria formal.
- (C) A ABNT NBR ISO/IEC 27001:2022 é um guia técnico de segurança cibernética voltado exclusivamente para proteção contra ataques cibernéticos, enquanto a ABNT NBR ISO/IEC 27002:2022 trata apenas da segurança física dos ativos de TI.
- (D) A certificação em conformidade com a ABNT NBR ISO/IEC 27001:2022 dispensa a necessidade de implementar controles de segurança recomendados pela ABNT NBR ISO/IEC 27002:2022, pois a norma já garante proteção total da informação.
- (E) A norma ABNT NBR ISO/IEC 27002:2022 é responsável pela definição dos requisitos obrigatórios para auditoria e certificação, enquanto a ABNT NBR ISO/IEC 27001:2022 trata exclusivamente de conceitos teóricos sem aplicação prática.

62. Uma empresa do setor bancário enfrenta riscos operacionais críticos devido à sua dependência de sistemas informatizados para processar transações financeiras. Como parte da estratégia de resiliência organizacional, a equipe de governança de TI implementou um Plano de Continuidade de Negócios (PCN) alinhado às normas ISO 22301:2020 e ISO/IEC 27001:2022.

O objetivo do plano é assegurar a continuidade das operações essenciais mesmo em cenários adversos, como falhas de infraestrutura, ataques cibernéticos, desastres naturais e pandemias. Além disso, a empresa definiu processos para análise de impacto nos negócios (BIA – *Business Impact Analysis*), gestão de riscos e recuperação de desastres (DR – *Disaster Recovery*).

Diante desse contexto, assinale a alternativa que descreve corretamente a relação entre a ISO 22301:2020 e a ISO/IEC 27001:2022 na gestão da continuidade de negócios.

- (A) A ISO 22301:2020 trata exclusivamente de recuperação de desastres em TI, enquanto a ISO/IEC 27001:2022 é aplicada apenas à segurança física dos ativos da organização.
- (B) A ISO 27001:2022 define requisitos para certificação de um Sistema de Gestão de Continuidade de Negócios (SGCN), enquanto a ISO 22301:2020 apenas fornece recomendações gerais para proteção de dados em ambientes de TI.
- (C) A ISO 27001:2022 é focada exclusivamente na proteção contra ameaças cibernéticas, sem abordar continuidade de negócios, enquanto a ISO 22301:2020 trata apenas de estratégias de recuperação financeira após incidentes críticos.
- (D) A ISO 22301:2020 estabelece requisitos para implementação de um Sistema de Gestão de Continuidade de Negócios (SGCN), garantindo resiliência organizacional, enquanto a ISO/IEC 27001:2022 complementa esse processo ao definir controles de segurança para proteção da informação antes, durante e após incidentes.
- (E) A certificação em conformidade com a ISO 22301:2020 substitui a necessidade de atender aos requisitos da ISO/IEC 27001:2022, pois cobre todas as exigências relacionadas à segurança da informação e recuperação de desastres.

63. Uma empresa de grande porte percebeu que o tráfego de sua rede corporativa estava congestionado, reduzindo o desempenho de aplicações críticas. Além disso, a equipe de segurança detectou que dispositivos de diferentes departamentos estavam se comunicando sem restrições, aumentando os riscos de movimentação lateral de ameaças cibernéticas dentro da infraestrutura de TI.

Para resolver esses problemas, os administradores de rede decidiram implementar VLANs (*Virtual Local Area Networks*) para segmentar o tráfego, reduzir o domínio de *broadcast* e melhorar a segurança.

Diante desse cenário, assinale a alternativa que apresenta corretamente um benefício da segmentação de rede com VLANs.

- (A) As VLANs eliminam a necessidade de roteadores e *switches* gerenciáveis, pois segmentam a rede de forma automática sem necessidade de configuração adicional.
- (B) O uso de VLANs impede completamente qualquer tipo de ataque dentro da rede, pois os dispositivos ficam isolados, tornando impossível a movimentação lateral de ameaças.
- (C) A implementação de VLANs reduz a necessidade de controle de acesso, pois a segmentação por si só já garante que dispositivos não autorizados não consigam acessar recursos restritos.
- (D) VLANs são úteis apenas para organização lógica da rede, sem impacto significativo no desempenho ou na segurança da infraestrutura.
- (E) A segmentação de rede com VLANs reduz o domínio de *broadcast*, melhora a performance da rede ao minimizar tráfego desnecessário e aumenta a segurança ao isolar dispositivos de diferentes departamentos, dificultando ataques e movimentação lateral de ameaças.

64. Uma grande organização do setor financeiro precisa reforçar sua política de Gestão de Identidade e Acesso (IAM) para proteger sistemas críticos contra acessos não autorizados. Após uma auditoria de segurança, a equipe de TI identificou riscos associados ao uso de senhas fracas e reutilizadas, além de ataques como *phishing*, *credential stuffing* e *brute force*.

Para mitigar esses riscos, a empresa decidiu implementar autenticação multifator (MFA) e reforçar o controle de privilégios para evitar escalonamento indevido de acessos.

Diante desse contexto, assinale a alternativa que descreve corretamente o papel da autenticação multifator (MFA) na segurança da informação.

- (A) A autenticação multifator (MFA) adiciona uma camada extra de segurança ao exigir dois ou mais fatores de autenticação diferentes (como algo que o usuário sabe, possui ou é), reduzindo os riscos associados a ataques baseados em credenciais comprometidas.
- (B) O uso de autenticação multifator (MFA) substitui completamente a necessidade de senhas fortes, pois garante que um atacante nunca conseguirá acessar um sistema protegido por esse mecanismo.
- (C) O MFA é um mecanismo opcional de segurança que deve ser implementado apenas em sistemas administrativos, sendo desnecessário para contas de usuários comuns dentro de uma organização.
- (D) A implementação de MFA elimina completamente a necessidade de auditoria de acessos e registros de logs, pois sua adoção garante que nenhum acesso não autorizado ocorra.
- (E) O MFA utiliza apenas senhas dinâmicas de uso único (OTP – *One-Time Password*), sendo incompatível com outros métodos de autenticação, como biometria ou tokens físicos.

65. Uma empresa de tecnologia decidiu migrar sua infraestrutura de TI para um ambiente de computação em nuvem, visando escalabilidade, resiliência e redução de custos operacionais.

Durante a transição, a equipe de segurança identificou desafios relacionados à proteção de dados, controle de acesso e conformidade com regulamentações como LGPD e GDPR. Para garantir a segurança da informação e a conformidade regulatória, a empresa implementou criptografia de dados, controle de identidade e acesso (IAM) e ferramentas de monitoramento contínuo da infraestrutura em nuvem.

Diante desse cenário, assinale a alternativa que apresenta corretamente um princípio essencial da segurança em ambientes de computação em nuvem.

- (A) A responsabilidade pela segurança da infraestrutura e dos dados armazenados na nuvem cabe exclusivamente ao provedor de serviços, eliminando a necessidade de controles adicionais por parte da empresa usuária.
- (B) A criptografia de dados em repouso é suficiente para garantir a segurança da informação na nuvem, pois impede qualquer tipo de ataque ou acesso não autorizado aos dados armazenados.
- (C) O modelo de responsabilidade compartilhada estabelece que o provedor de nuvem é responsável pela segurança da infraestrutura, enquanto a empresa cliente deve gerenciar e proteger seus dados, configurações e acessos, garantindo conformidade com regulamentações.
- (D) A implementação de controle de acesso baseado em identidade (IAM) elimina completamente a necessidade de criptografia de dados na nuvem, pois impede qualquer acesso indevido.
- (E) Para garantir conformidade com regulamentações como LGPD e GDPR, basta assinar um contrato de nível de serviço (SLA) com o provedor de nuvem, sem necessidade de implementar medidas adicionais de proteção.