Roraima
Assembleia Legislativa
O Poder do Povo

Colégio M0001 | Sala 0001 | Ordem 0001

Junho/2026

ASSEMBLEIA LEGISLATIVA DO ESTADO DE RORAIMA

IV Concurso Público para Provimento de Vagas nos Cargos de

Analista Legislativo
Analista de Segurança da Informação

Nome do Candidato: Caderno de Prova '13', Tipo 005

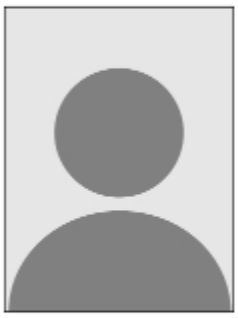
Nº de Inscrição: MODELO

Nº do Caderno: TIPO-005

Nº do Documento: 0000000000000000

ASSINATURA DO CANDIDATO

PROVA Conhecimentos Gerais
Conhecimentos Específicos
Discursiva-Redação



INSTRUÇÕES

Quando autorizado pelo fiscal de sala, transcreva a frase abaixo, com sua caligrafia usual, no espaço apropriado na Folha de Respostas.

Galileo di Vincenzo Bonaulti de Galilei, conhecido como Galileu Galilei, foi um astrônomo, físico e engenheiro florentino.

- Verifique se este caderno corresponde à sua opção de cargo, se contém 80 questões numeradas de 1 a 80 e se contém a proposta e o espaço para o rascunho da Prova Discursiva-Redação.
- Caso contrário, solicite imediatamente ao fiscal da sala a substituição do caderno.
- Não serão aceitas reclamações posteriores.
- Para cada questão existe apenas UMA resposta certa.
- Leia cuidadosamente cada uma das questões e escolha a resposta certa.
- Essa resposta deve ser marcada na FOLHA DE RESPOSTAS que você recebeu.

VOCÊ DEVE

- Procurar, na FOLHA DE RESPOSTAS, o número da questão que você está respondendo.
- Verificar no caderno de prova qual a letra (A,B,C,D,E) da resposta que você escolheu.
- Marcar essa letra na FOLHA DE RESPOSTAS, conforme o exemplo: Ⓐ ● Ⓒ Ⓓ Ⓔ
- Ler o que se pede na Prova Discursiva-Redação e utilizar, se necessário, o espaço para rascunho.

ATENÇÃO

- Marque as respostas com caneta esferográfica de material transparente e tinta preta ou azul. Não será permitida a utilização de lápis, lapiseira, marca-textos, régua ou borracha durante a realização da prova.
- Marque apenas uma letra para cada questão. Será anulada a questão em que mais de uma letra estiver assinalada.
- Responda a todas as questões.
- Não será permitida nenhuma espécie de consulta ou comunicação entre os candidatos, nem a utilização de livros, anotações, códigos, manuais, notas ou impressos não permitidos, máquina calculadora ou similar, nem qualquer espécie de aparelho eletrônico.
- Em hipótese alguma o rascunho da Prova Discursiva-Redação será corrigido.
- Você deverá transcrever a sua Prova Discursiva-Redação a tinta, no espaço apropriado.
- A duração da prova é de 5 horas, para responder a todas as questões objetivas, preencher a Folha de Respostas e fazer a Prova Discursiva-Redação (rascunho e transcrição) na folha correspondente.
- Ao terminar a prova, chame o fiscal da sala e devolva todo o material recebido para conferência.
-

CONHECIMENTOS GERAIS

Língua Portuguesa

Atenção: Para responder às questões de números 1 a 10, baseie-se no texto a seguir.

As ruas abertas à livre circulação de pessoas e veículos representam uma das imagens mais vivas da cidade moderna. Apesar de as cidades ocidentais incorporarem várias e até contraditórias versões da modernidade, há um grande consenso a respeito de quais são os elementos básicos da experiência moderna de vida pública urbana: a primazia e a abertura de ruas; a circulação livre; os encontros impessoais e anônimos de pedestres; o uso público e espontâneo das ruas e praças; e a presença de pessoas de diferentes grupos sociais passeando e observando os outros que passam, olhando vitrines, fazendo compras, sentando nos cafés, participando de manifestações políticas, apropriando as ruas para seus festivais e comemorações, ou usando os espaços especialmente designados para o lazer das massas. Esses elementos são associados à vida moderna em cidades capitalistas pelo menos desde a reforma de Paris promovida pelo barão de Haussmann na segunda metade do século XIX.

No cerne da concepção de vida pública urbana incorporada na Paris moderna estavam as noções de que o espaço da cidade é aberto para ser usado e usufruído por qualquer um e de que a sociedade de consumo que ele abriga poderia tornar-se acessível a todos. É claro que esse nunca foi exatamente o caso, em Paris ou em qualquer outro lugar. As cidades modernas foram sempre marcadas por desigualdades sociais e segregação espacial e nunca deixaram de ser apropriadas de formas bastante diferentes por diversos grupos, dependendo de sua posição social e de seu poder. No entanto, a despeito das persistentes desigualdades e injustiças sociais, as cidades ocidentais modernas sempre mantiveram vários sinais de abertura, sobretudo no que diz respeito à circulação e ao consumo. Esses sinais contribuíram para manter o valor positivo associado à ideia de um espaço público aberto, acessível a todos e a qualquer um.

As cidades modernas têm servido de cenário para todo tipo de manifestação política. Na verdade, a promessa de incorporação à sociedade moderna incluía não só a cidade e o consumo, mas também a ordem política. As imagens da cidade moderna são análogas àquelas da ordem liberal-democrática, consolidada a partir da ficção do contrato social entre pessoas livres e iguais e que moldou a esfera política moderna. Essa ficção, tão radical quanto aquela da cidade aberta, ajudou a destruir a ordem social estamental que a precedeu. No entanto, foi só depois de muitas lutas que as definições de quem poderia ser considerado "livre e igual" foram pouco a pouco expandidas. Tanto a cidade aberta e sem exclusões quanto a ordem política incorporando todos os cidadãos como iguais nunca existiram, mas seus ideais fundadores e suas promessas de incorporação mantiveram seu poder por pelo menos dois séculos, dando forma a experiências de cidadania e de vida urbana e legitimando as ações de vários grupos excluídos em suas reivindicações por incorporação.

(Adaptado de: CALDEIRA, Teresa Pires do Rio. **Cidade de muros: crime, segregação e cidadania em São Paulo**. São Paulo: Editora 34; Edusp, 2011, pp 302 a 305)

1. Conforme o texto, ilustra fatores concretos da experiência de vida pública urbana no Ocidente, ao menos nos últimos dois séculos, o que se encontra em:

   (A) A nova cidade já não é marcada por um tempo em que se produz uma identidade; ela é marcada pela consolidação de um terreno de disputas políticas silenciosas.

   (B) A primazia de espaços privados, a centralidade da produção industrial e a divisão rígida entre espaços de trabalho, de circulação e de moradia.

   (C) Apesar das persistentes desigualdades e injustiças, as cidades ocidentais modernas conservam indícios de abertura, especialmente no que se refere à circulação e ao consumo.

   (D) A construção de ambientes planejados cujo símbolo maior é a previsibilidade. É a cidade do movimento estritamente necessário, de preferência em automóveis.

   (E) A organização comunitária baseada em laços pessoais estratificados, com forte controle estatal nos espaços urbanos e pouca mobilidade social.

2. As atribuições da ordem liberal-democrática, presentes no último parágrafo, correspondem a

   (A) uma estrutura social que valoriza relações pessoais restritivas. A participação na esfera pública não deve estabelecer uma correlação de forças entre igualdade e cidadania.

   (B) um sistema político centrado exclusivamente no desenvolvimento econômico, sem qualquer conexão com os direitos civis.

   (C) um sistema político baseado na hierarquia estamental, no qual os direitos são definidos pela posição social de cada indivíduo.

   (D) um modelo que restringe o acesso à cidade e à organização social apenas a determinados grupos econômicos e políticos.

   (E) uma organização política fundamentada no contrato social entre indivíduos livres e iguais, associada ao ideal de participação plena na vida pública.

3. Segundo o texto de Teresa Caldeira, a cidade moderna ideal seria

   (A) um espaço público aberto e acessível a todos, marcado pela livre circulação, encontros anônimos, diversidade social e uso coletivo das ruas e praças.

   (B) uma cidade em que o controle estatal limitaria o uso dos espaços públicos, priorizando a ordem e a segurança em detrimento da plena liberdade de circulação.

   (C) caracterizada pela forte segregação espacial, na qual diferentes grupos sociais ocupam áreas rigidamente separadas e com pouca interação entre si.

   (D) um espaço urbano voltado prioritariamente à produção industrial, onde o acesso aos bens e serviços se restringiria às elites econômicas.

   (E) organizada em torno de tradições comunitárias estáveis, com relações pessoais duradouras e pouca circulação de grupos sociais cuja identidade instaurasse diferenças radicais.

4. O uso adequado do sinal indicativo de crase encontra-se em:

(A) Às cidades ocidentais modernas sempre mantiveram vários sinais de abertura, sobretudo no que diz respeito a circulação e ao consumo.

(B) À promessa de incorporação a sociedade moderna incluía não só à cidade e o consumo, mas também a ordem política.

(C) Às ruas abertas à livre circulação de pessoas e veículos representam uma das imagens mais vivas da cidade moderna.

(D) Esses elementos são associados à vida moderna em cidades capitalistas pelo menos desde a reforma de Paris.

(E) Às imagens da cidade moderna são análogas àquelas da ordem liberal-democrática.

5. A correção gramatical e a regência são plenamente contempladas no seguinte período:

(A) Muitos estudiosos defendem que há consenso com a importância desses espaços para a vida urbana, embora nem sempre se reconheça sua relação sob a experiência cotidiana dos cidadãos.

(B) A noção de cidade aberta foi incorporada em discursos políticos desde o século XIX. Ela está frequentemente ligada para com projetos de modernização urbanos que valorizam a circulação e o consumo.

(C) As cidades modernas foram sempre marcadas por desigualdades sociais e segregação espacial e nunca deixaram de ser apropriadas de formas bastante diferentes por diversos grupos, dependendo de sua posição social e de seu poder.

(D) Há consenso diante a quais são os elementos básicos da vida pública urbana. As ruas abertas e a livre circulação de pessoas são fundamentais para uma concepção democrática de cidade moderna.

(E) As cidades foram marcadas em desigualdades sociais profundas. Apesar disso, o discurso de abertura política, típico das democracias burguesas, foram hegemônicos no ocidente, ao menos até as primeiras décadas do século XXI.

6. *Essa ficção, tão radical quanto aquela da cidade aberta, ajudou a destruir a ordem social estamental que a precedeu. No entanto, foi só depois de muitas lutas que as definições de quem poderia ser considerado "livre e igual" foram pouco a pouco expandidas.* (3º parágrafo)

O termo sublinhado no trecho acima indica a

(A) adição de dois pontos de vista sobre um mesmo objeto.

(B) relativização de uma afirmativa anterior.

(C) oposição entre duas premissas.

(D) conclusão de um determinado processo.

(E) negação absoluta de um argumento anterior.

7. Considere as frases a seguir:

É claro que esse nunca foi exatamente o caso, em Paris ou em qualquer outro lugar. As cidades modernas foram sempre marcadas por desigualdades sociais e segregação espacial e nunca deixaram de ser apropriadas de formas bastante diferentes por diversos grupos, dependendo de sua posição social e de seu poder. (2º parágrafo)

Essa ficção, tão radical quanto aquela da cidade aberta, ajudou a destruir a ordem social estamental que a precedeu. (3º parágrafo)

Os termos sublinhados referem-se, respectivamente, a

(A) cidades modernas – grupos – ordem social

(B) desigualdades sociais – segregação – ficção

(C) cidades modernas – grupos – ficção

(D) desigualdades sociais – grupos – ficção

(E) cidades modernas – segregação – ordem social

8. *No cerne da concepção de vida pública urbana incorporada na Paris moderna estavam as noções de que o espaço da cidade é aberto para ser usado e usufruído por qualquer um e de que a sociedade de consumo que ele abriga poderia tornar-se acessível a todos.*

Uma nova redação para a frase acima, em que se mantêm a correção e, em linhas gerais, o sentido original, encontra-se em:

(A) Residia na essência da Paris moderna, a crença de que qualquer um pode aspirar o uso das áreas comuns e de que a sociedade de mercado ali estabelecida, visa incluir toda a população sem distinções.

(B) Existia no âmago do projeto de urbanidade parisiense, as visões de livre fruição das ruas por qualquer indivíduo, garantindo que o acesso aos bens de consumo assistissem por todos de forma igualitária.

(C) No centro da concepção de vida pública urbana presente na Paris moderna, estavam as ideias de que o espaço urbano deveria ser franqueado ao uso e usufruto de qualquer pessoa e de que a sociedade de consumo ali existente poderia se tornar acessível a todos.

(D) A ideia de esfera pública na Paris da modernidade fundamentava na premissa de que o território urbano é de livre acesso, e que a dinâmica do consumo presente nele deve estar ao encalço de todos cidadãos.

(E) O conceito de vida coletiva nas cidades, que a Paris moderna personificou, traziam o princípio de que o espaço público pertence ao povo; além disso a acessibilidade à essa cultura de consumo seria um direito universal.

9. *As ruas abertas à livre circulação de pessoas e veículos representam uma das imagens mais vivas da cidade moderna. Apesar de as cidades ocidentais incorporarem várias e até contraditórias versões da modernidade, há um grande consenso a respeito de quais são os elementos básicos da experiência moderna de vida pública urbana* [...].

No trecho acima, indicam juízos de valor os seguintes termos:

(A) *mais vivas*, *grande consenso*
(B) *veículos*, *experiência moderna*
(C) *ruas abertas*, *circulação de pessoas e veículos*
(D) *cidades ocidentais*, *versões da modernidade*
(E) *livre circulação*, *consenso*

10. O verbo que possui o mesmo tipo de complemento que o da frase "*as cidades ocidentais modernas sempre mantiveram vários sinais de abertura*", está sublinhado em:

(A) "As cidades modernas foram sempre marcadas por desigualdades sociais..."
(B) "As ruas abertas representam uma das imagens mais vivas da cidade moderna."
(C) "Esses sinais contribuíram para manter o valor positivo..."
(D) "Essa ficção ajudou a destruir a ordem social estamental que a precedeu."
(E) "O espaço da cidade é aberto para ser usado e usufruído por qualquer um..."

Atenção: Para responder às questões de números 11 a 20, baseie-se no texto a seguir.

Uma vela para Dario

Dario vem apressado, guarda-chuva no braço esquerdo. Assim que dobra a esquina, diminui o passo até parar, encosta-se a uma parede. Por ela escorrega, senta-se na calçada, ainda úmida de chuva. Descansa na pedra o cachimbo.

Dois ou três passantes à sua volta indagam se não está bem. Dario abre a boca, move os lábios, não se ouve resposta. O senhor gordo, de branco, diz que deve sofrer de ataque.

Ele reclina-se mais um pouco, estendido na calçada, e o cachimbo apagou. O rapaz de bigode pede aos outros se afastem e o deixem respirar. Abre-lhe o paletó, o colarinho, a gravata e a cinta. Quando lhe tiram os sapatos, Dario rouqueja feio, bolhas de espuma surgem no canto da boca.

Cada pessoa que chega ergue-se na ponta dos pés, não o pode ver. Os moradores da rua conversam de uma porta a outra, as crianças de pijama acodem à janela. O senhor gordo repete que Dario sentou-se na calçada, soprando a fumaça do cachimbo, encostava o guarda-chuva na parede. Mas não se vê guarda-chuva ou cachimbo ao seu lado.

A velhinha de cabeça grisalha grita que ele está morrendo. Um grupo o arrasta para o táxi da esquina. Já no carro a metade do corpo, protesta o motorista: quem pagará a corrida? Concordam chamar a ambulância. Dario conduzido de volta e recostado à parede – não tem os sapatos nem o alfinete de pérola na gravata.

Alguém informa da farmácia na outra rua. Não carregam Dario além da esquina; a farmácia no fim do quarteirão e, além do mais, muito peso. É largado na porta de uma peixaria. Enxame de moscas lhe cobrem o rosto, sem que faça um gesto para espantá-las.

Ocupado o café próximo pelas pessoas que apreciam o incidente e, agora, comendo e bebendo, gozam as delícias da noite. Dario em sossego e torto no degrau da peixaria, sem o relógio de pulso.

Um terceiro sugere lhe examinem os papéis, retirados – com vários objetos – de seus bolsos e alinhados sobre a camisa branca. Ficam sabendo do nome, idade, sinal de nascença. O endereço na carteira é de outra cidade.

Registra-se correria de uns duzentos curiosos que, a essa hora, ocupam toda a rua e as calçadas: é a polícia. O carro negro investe a multidão. Várias pessoas tropeçam no corpo de Dario, pisoteado dezessete vezes.

O guarda aproxima-se do cadáver, não pode identificá-lo – os bolsos vazios. Resta na mão esquerda a aliança de ouro, que ele próprio – quando vivo – só destacava molhando no sabonete. A polícia decide chamar o rabecão.

A última boca repete – Ele morreu, ele morreu. E a gente começa a se dispersar. Dario levou duas horas para morrer, ninguém acreditava estivesse no fim. Agora, aos que alcançam vê-lo, todo o ar de um defunto.

Um senhor piedoso dobra o paletó de Dario para lhe apoiar a cabeça. Cruza as mãos no peito. Não consegue fechar olho nem boca, onde a espuma sumiu. Apenas um homem morto e a multidão se espalha, as mesas do café ficam vazias. Na janela alguns moradores com almofadas para descansar os cotovelos.

Um menino de cor e descalço vem com uma vela, que acende ao lado do cadáver. Parece morto há muitos anos, quase o retrato de um morto desbotado pela chuva.

Fecham-se uma a uma as janelas. Três horas depois, lá está Dario à espera do rabecão. A cabeça agora na pedra, sem o paletó. E o dedo sem a aliança. O toco de vela apaga-se às primeiras gotas da chuva, que volta a cair.

(Adaptado de: TREVISAN, Dalton. **33 contos escolhidos**. Rio de Janeiro: Record, 2005)

11. A frase *O rapaz de bigode pede aos outros se afastem e o deixem respirar* está corretamente transposta para o discurso direto em:

(A) O rapaz de bigode pede: – Os outros que se afastem e que lhe deixem respirar.
(B) O rapaz de bigode pede aos outros: "Afastem-se e deixem-no respirar".
(C) "Afasta-o e deixe-o respirar", pedem aos outros o rapaz de bigode.
(D) O rapaz de bigode solicita que os outros: "Se afastem e o deixem respirar".
(E) – O rapaz de bigode pede aos outros: – Que se afastem, que deixem-no respirar.

12. Simbolizam a morte de Dario todas as seguintes expressões:

(A) *abre a boca / move os lábios / não se ouve resposta*

(B) *carro negro investe a multidão / correria de uns duzentos curiosos / tropeçam no corpo de Dario*

(C) *comendo e bebendo / gozam as delícias da noite / ocupam toda a rua e as calçadas*

(D) *guarda-chuva no braço esquerdo / diminui o passo até parar / encosta-se a uma parede*

(E) *o cachimbo apagou / a espuma sumiu / O toco de vela apaga-se às primeiras gotas da chuva*

13. *Várias pessoas tropeçam no corpo de Dario, pisoteado dezessete vezes.*

O verbo flexionado no mesmo tempo, modo e voz que o da frase acima está sublinhado em:

(A) (...) *quem pagará a corrida?*

(B) *A velhinha de cabeça grisalha gritou* (...)

(C) *Dario levou duas horas para morrer.*

(D) *Ele reclina-se mais um pouco.*

(E) *Abre-lhe o paletó, o colarinho, a gravata e a cinta.*

14. No trecho *Assim que dobra a esquina, diminui o passo até parar, encosta-se a uma parede. Por ela escorrega, senta-se na calçada, ainda úmida de chuva. Descansa na pedra o cachimbo*, o pronome sublinhado refere-se a

(A) chuva.

(B) pedra.

(C) esquina.

(D) parede.

(E) calçada.

15. Respeita plenamente as normas de regência verbal e nominal o livre comentário a respeito do texto:

(A) Os curiosos que ocupavam a rua assistiram o triste espetáculo da morte de Dario sem ao qual ninguém pudesse de fato ajudar.

(B) O guarda aproximou-se ao corpo de Dario para tentar identificar-lhe, mas não encontrou documentos nos bolsos do falecido.

(C) A multidão presente no local não aspirava o fim trágico de Dario, em que permaneceu estendido na calçada por duas horas.

(D) A polícia decidiu por chamar o rabecão após constatar que Dario já não apresentava sinais vitais.

(E) Dario era muito apegado com sua aliança de ouro, objeto a que ele raramente retirava do dedo.

16. No trecho *O senhor gordo repete que Dario sentou-se na calçada, soprando a fumaça do cachimbo, encostava o guarda-chuva na parede. Mas não se vê guarda-chuva ou cachimbo ao seu lado*, o conectivo sublinhado relaciona ideias introduzindo um valor semântico de

(A) adição.

(B) consequência.

(C) oposição.

(D) explicação.

(E) retificação.

17. No trecho *Ocupado o café próximo pelas pessoas que apreciam o incidente e, agora, comendo e bebendo, gozam as delícias da noite. Dario em sossego e torto no degrau da peixaria, sem o relógio de pulso*, os termos destacados sugerem que

(A) a morte de Dario gerara uma comoção superficial e convertera-se em mero espetáculo.

(B) a situação levou ao encerramento das atividades do café e dispersão das pessoas em virtude do luto.

(C) Dario foi rapidamente assistido e retirado do local pelos passantes, embora não tenha sobrevivido.

(D) os frequentadores do café estavam preocupados em prestar socorro a Dario, ainda que desordenadamente.

(E) o ambiente descrito é de luto coletivo e comoção entre os presentes, apesar da aparente indiferença geral.

18. Apresenta uma síntese coerente com o sentido geral do texto o que se encontra em:

(A) A história enfatiza o isolamento de Dario como consequência de sua escolha voluntária de permanecer na rua, sem esboçar qualquer interesse em uma intervenção externa.

(B) O conto descreve uma ação coletiva espontânea em torno de um acontecimento urbano; a morte de Dario é tratada como motivo de intervenção positiva comunitária.

(C) O conto retrata a comoção coletiva diante de um homem que recebe imediato socorro e atenção solidária de todos os que passam pelo local.

(D) A narrativa evidencia a transformação de uma tragédia urbana em espetáculo público, marcado pela indiferença e curiosidade das pessoas diante da morte de Dario.

(E) O texto apresenta uma crítica ao sistema de saúde, destacando a ineficiência dos serviços de emergência no atendimento rápido às vítimas em vias públicas.

19. *Segundo o escritor e crítico Ricardo Piglia, o conto clássico é aquele que narra em primeiro plano a história 1 e constrói em segredo uma história 2, de modo que as duas se encontrem ao fim. Piglia afirma: "A arte do contista consiste em saber cifrar a história 2 nos interstícios da história 1. Um relato visível esconde um relato secreto, narrado de um modo elíptico e fragmentário".*

(Adaptado de: Ricardo Piglia, "Teses sobre o conto", em Formas breves. Trad. de José Marcos Mariani de Macedo. São Paulo: Companhia das Letras, 2004. pp. 89-90).

Em conformidade com o texto acima, os dois planos que compõem a narrativa de "Uma vela para Dario" estão mais bem definidos em:

(A) "Uma vela para Dario" conta em primeiro plano o ataque cardíaco do personagem, enquanto no segundo plano vai se consumando o roubo de seus bens.

(B) O texto apresenta, em primeiro plano, a morte de Dario; em segundo plano, desenvolve-se uma investigação policial acerca da possível causa de sua morte.

(C) O texto narra, em primeiro plano, a vida cotidiana dos moradores da rua, enquanto, em segundo plano, destacam-se os aspectos particulares da vida pregressa de Dario.

(D) O conto apresenta, em primeiro plano, a tentativa organizada de socorro ao personagem, enquanto, em segundo plano, revela-se a ineficiência das instituições públicas.

(E) A narrativa mostra, em primeiro plano, a movimentação desordenada da multidão, enquanto, em segundo plano, constrói-se a humanização gradual de Dario.

20. *Um menino de cor e descalço vem com uma vela, que acende ao lado do cadáver. Parece morto há muitos anos, quase o retrato de um morto desbotado pela chuva.*

Com a passagem acima o autor pretende destacar que

(A) a presença do menino indica que a polícia já havia encerrado a ocorrência e liberado o corpo para remoção imediata.

(B) a atitude do menino configura um ato solidário e desinteressado praticado por alguém socialmente vulnerável.

(C) o ato do menino reforça o caráter cômico da narrativa, transformando a cena da morte em uma situação de humor involuntário.

(D) a atitude representa uma tentativa de exploração econômica da situação de morte de Dario, já que o menino vende uma vela no local do acidente.

(E) o gesto do menino confirma a indiferença geral das pessoas, pois ele apenas observa o corpo sem qualquer envolvimento emocional.

Noções de Direito Constitucional

21. Foi editada no estado de Roraima lei proibindo a prática de queimadas para limpeza de terreno e manejo de pastagens. Insatisfeitos com tal medida, os agricultores da região impugnaram a lei, argumentando que o estado não detém competência para dispor sobre o assunto. Diante do caso hipotético acima mencionado, os agricultores

(A) têm razão, pois o estado deveria propor iniciativas legislativas em conjunto com os demais entes da federação, tendo em vista que a competência para legislar sobre a proteção ao meio ambiente interessa às três esferas federativas, sendo, pois, a lei inconstitucional.

(B) têm razão, uma vez que a Constituição Federal estabelece que compete à União legislar privativamente sobre proteção ao meio ambiente, observadas as premissas constitucionais.

(C) não têm razão, haja vista que o estado possui competência para legislar sobre a proteção do meio ambiente, observada a legislação federal sobre normas gerais na matéria.

(D) não têm razão, pois o estado tem competência exclusiva para legislar sobre a proteção ao meio ambiente, de modo que a lei estadual em questão é constitucional.

(E) têm razão, pois o estado somente é competente para legislar sobre assuntos de interesse local; diante disso, a proteção do meio ambiente engloba interesse das três esferas da federação, sendo a lei, portanto, inconstitucional.

22. À luz do que dispõe a Constituição Federal acerca dos direitos e garantias fundamentais:

I. Será declarada a perda da nacionalidade do brasileiro nato que fizer pedido expresso perante autoridade competente, ressalvadas situações que acarretem apatridia, não havendo impedimento para eventual reaquisição da nacionalidade brasileira originária, na forma da lei.

II. É assegurada a participação dos trabalhadores e empregadores nos colegiados dos órgãos públicos em que seus interesses profissionais ou previdenciários sejam objeto de discussão e deliberação.

III. É admitida a cassação de direitos políticos em hipóteses excepcionais previstas em lei complementar, desde que observados o contraditório e a ampla defesa.

IV. Os partidos políticos podem receber recursos financeiros de entidade ou governo estrangeiros, desde que haja prestação de contas à Justiça Eleitoral.

Está correto o que se afirma APENAS em

(A) I e IV.
(B) I e III.
(C) I e II.
(D) III e IV.
(E) II e III.

23. De acordo com o que dispõe a Constituição Federal acerca do processo legislativo,

(A) a Casa legislativa na qual tenha sido concluída a votação enviará o projeto de lei ordinária ao Presidente do Congresso Nacional, que, concordando, o sancionará.
(B) a matéria constante de projeto de lei rejeitado só poderá constituir objeto de novo projeto, na mesma sessão legislativa, mediante proposta de 2/3 dos membros do Congresso Nacional.
(C) é vedada a edição de medidas provisórias sobre matéria orçamentária, financeira e tributária.
(D) é de iniciativa privativa do Presidente da República lei que disponha sobre criação de cargos, funções ou empregos públicos na administração direta e autárquica ou aumento de sua remuneração.
(E) a discussão e votação dos projetos de lei de iniciativa do Presidente da República, do Supremo Tribunal Federal e dos Tribunais Superiores terão início no Senado Federal.

24. O Governador de Roraima propôs uma emenda à Constituição do Estado buscando facilitar o processo legislativo para aprovação de leis ordinárias e complementares. Tal proposta busca a aprovação das leis caso atingido apenas o quórum de maioria simples dos presentes na sessão da Assembleia Legislativa do Estado, sem estabelecimento de quórum mínimo de presença. Diante da situação hipotética apresentada, tal proposta é

(A) inconstitucional, pois, em virtude da matéria, a iniciativa da referida proposta de emenda deveria caber aos membros da Assembleia Legislativa, e não ao Governador do Estado.
(B) constitucional, em obediência ao princípio constitucional da eficiência, ao buscar a modernização dos processos legislativos de acordo com a necessidade de cada ente federativo.
(C) inconstitucional, por violar normas de processo legislativo estabelecidas na Constituição Federal que devem ser observadas por todos os entes da federação.
(D) constitucional em razão da autonomia do Estado-membro para a elaboração das regras relativas ao processo legislativo estadual.
(E) inconstitucional, pois somente seria possível proposta que dificultasse a aprovação do processo legislativo estadual.

Noções de Direito Administrativo

25. Eurípides é servidor público estadual, ocupando o cargo efetivo de Analista Legislativo na Assembleia Legislativa do Estado de Roraima. O presidente da Assembleia recebeu uma denúncia anônima relatando que Eurípides está envolvido em casos de corrupção em contratos da Administração Pública. Foi, então, instaurada uma sindicância que, durante seu curso regular, obteve elementos suficientes para a instauração, por meio de portaria, de processo administrativo disciplinar. Diante da situação hipotética acima descrita, Eurípides alega nulidade em razão de seu processo administrativo ter se iniciado por meio de notícia anônima. Tal alegação

(A) não deve prosperar, pois não mais se admite no ordenamento jurídico brasileiro a "verdade sabida" em procedimentos de punição ao servidor faltoso.
(B) não encontra respaldo no ordenamento jurídico brasileiro, pois é permitida a instauração de processo administrativo disciplinar com base em denúncia anônima, em razão do exercício do poder-dever de autotutela da Administração.
(C) merece prosperar, tendo em vista que é direito subjetivo do servidor público saber quem foi o autor da denúncia e sua motivação, proporcionado o exercício da exceção da verdade.
(D) deve prosperar por violação ao princípio administrativo da publicidade e do devido processo legal.
(E) deve prosperar por violação aos princípios constitucionais do contraditório e de ampla defesa.

26. O Estado de Roraima, visando a modernização de seus hospitais públicos, adquiriu equipamentos médicos diversos, substituindo os antigos que, até então, serviam às equipes de saúde lotadas nos referidos hospitais. Apesar de os antigos equipamentos ainda funcionarem, eles deixaram de ter utilidade para o Estado, razão pela qual foi instaurado processo administrativo visando à sua alienação. Consignou-se a existência de interesse público devidamente justificado para a alienação dos equipamentos, razão pela qual foi realizada sua avaliação. Diante da situação hipotética acima mencionada, a alienação desses equipamentos inservíveis se dará, em regra, na modalidade

(A) diálogo competitivo.
(B) concurso.
(C) leilão.
(D) concorrência.
(E) pregão.

27. De acordo com o que estabelece a Lei de Licitações e Contratos Administrativos (Lei nº 14.133/2021), o edital poderá, na forma disposta em regulamento, exigir que percentual mínimo da mão de obra responsável pela execução do objeto da contratação seja constituído por

(A) mulheres vítimas de violência doméstica.

(B) pessoas trans, travestis e não binárias.

(C) negros, pardos e indígenas.

(D) jovens aprendizes.

(E) pessoas maiores de 60 anos.

28. De acordo com o que estabelece a Lei Geral de Proteção de Dados Pessoais (LGPD),

(A) é permitido às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários.

(B) sua aplicação se dá ao tratamento de dados pessoais realizado, inclusive, para fins exclusivamente jornalísticos e artísticos.

(C) o tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado no interesse de seus genitores, ou de seu responsável legal, nos termos da legislação pertinente.

(D) em nenhuma hipótese é permitida a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica.

(E) a defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva.

Noções de Administração Financeira e Orçamentária

29. Sobre a classificação das despesas públicas, é correto afirmar que

(A) a classificação por categoria econômica separa as despesas entre correntes e de capital, refletindo, respectivamente, na manutenção da máquina pública e formação de novos ativos.

(B) a classificação por natureza da despesa se restringe à distinção entre despesas obrigatórias e discricionárias, não envolvendo outros critérios analíticos.

(C) a classificação funcional da despesa tem como objetivo principal identificar a unidade orçamentária responsável pela execução do gasto.

(D) despesas correntes incluem gastos com pessoal e encargos sociais, sendo vedada a inclusão de outras naturezas de despesa nessa categoria.

(E) despesas de capital são aquelas que não produzem variação patrimonial no setor público, pois representam apenas transferências financeiras entre entes.

30. O orçamento público possui natureza jurídica

(A) híbrida, sendo simultaneamente norma jurídica e ato administrativo vinculante que obriga a execução integral de todas as despesas aprovadas.

(B) de instrumento meramente político, sem força normativa, cuja função se limita a expressar intenções de governo sem relevância jurídica.

(C) de lei formal de conteúdo autorizativo e estimativo, não criando, por si só, direitos subjetivos à realização da despesa nem obrigação absoluta de execução.

(D) de ato administrativo discricionário, sem caráter normativo, funcionando apenas como instrumento interno de planejamento governamental.

(E) de lei em sentido material, dotada de generalidade e abstração, impondo obrigatoriamente a execução integral das despesas nele previstas.

31. Os princípios orçamentários funcionam como diretrizes estruturantes da elaboração e execução do orçamento público e, dentre esses, o princípio da

(A) legalidade orçamentária restringe a atuação do gestor público à execução do orçamento, dispensando qualquer observância às normas durante a fase de elaboração.

(B) clareza exige que o orçamento seja elaborado de forma a permitir compreensão por diferentes usuários, incluindo a padronização de classificações e a transparência na apresentação dos dados fiscais.

(C) programação estabelece que o orçamento deve priorizar exclusivamente despesas obrigatórias, deixando despesas discricionárias fora da estrutura de planejamento.

(D) não afetação impede que receitas específicas sejam vinculadas a determinadas despesas, sem qualquer exceção, inclusive para transferências constitucionais entre entes federativos.

(E) publicidade garante apenas a divulgação formal do orçamento aprovado, não se aplicando às etapas de execução e acompanhamento da despesa pública.

32. Considerando a interação entre classificadores orçamentários, a classificação

(A) institucional permite identificar o responsável pela execução do orçamento, enquanto a programática evidencia os objetivos e resultados das ações governamentais.

(B) por fonte de recursos tem como finalidade indicar a natureza econômica da despesa, distinguindo entre gastos correntes e de capital.

(C) econômica da despesa tem como foco principal a mensuração de resultados, sendo substituta dos indicadores de desempenho.

(D) programática organiza as despesas com base na origem dos recursos financeiros, permitindo rastrear a arrecadação pública.

(E) funcional e a classificação programática são equivalentes, pois ambas identificam os órgãos responsáveis pela execução das políticas públicas.

Legislação Institucional

33. De acordo com o Regimento Interno da Assembleia Legislativa do Estado de Roraima (Resolução Legislativa nº 08, de 13 de dezembro de 2023, e suas alterações), os projetos de resolução legislativa destinam-se a regular matéria de caráter político ou administrativo, com eficácia de lei ordinária, de competência privativa, sobre o que deva a Assembleia pronunciar-se, tal como

(A) denúncia contra o Governador e Secretário de Estado.

(B) concessão de título honorífico.

(C) pedido de intervenção federal.

(D) apreciação das contas anuais do Tribunal de Contas do Estado.

(E) conclusão de Comissão Permanente sobre proposta de fiscalização e controle.

34. De acordo com o que estabelece a Resolução nº 015/2024, que disciplina a estrutura administrativa da Assembleia Legislativa do Estado de Roraima, é competência do Controlador-Geral

(A) elaborar e promover a atualização anual da Política Estratégica de Segurança da Assembleia Legislativa através do Plano de Segurança aprovado pela Mesa Diretora.

(B) planejar, coordenar e executar, de acordo com a orientação da Mesa Diretora, recepções, solenidades, comemorações internas e externas.

(C) avaliar a regularidade das licitações e contratos, bem como da programação e execução orçamentária e financeira.

(D) contactar órgãos governamentais dos poderes Executivo, Legislativo e Judiciário no âmbito federal, estadual e municipal.

(E) resgatar e preservar a memória institucional da Assembleia Legislativa do Estado de Roraima.

35. De acordo com o que estabelece a Constituição do Estado de Roraima, poderá ser feita a convocação extraordinária da Assembleia Legislativa mediante

(A) ato do Presidente do Tribunal de Justiça do Estado, em caso de decretação de intervenção do estado em município.

(B) requerimento de Secretário de Estado, em caso de decretação de intervenção no estado.

(C) ato do Governador do Estado, em caso de urgência ou interesse público relevante.

(D) ato do Presidente da Casa, no dia 1º de janeiro do primeiro ano da legislatura, para posse de seus membros e eleição da nova Mesa Diretora.

(E) requerimento de 1/3 de seus membros, em caso de decretação de estado de calamidade pública que atinja o território do estado.

36. De acordo com o que estabelece o Regimento Interno da Assembleia Legislativa do Estado de Roraima (Resolução Legislativa nº 08, de 13 de dezembro de 2023, e suas alterações), acerca da Mesa Diretora,

(A) é de sua competência propor ação de inconstitucionalidade, a requerimento de Prefeito Municipal ou mediante requisição de Procurador-Geral do Município.

(B) será considerado vago o cargo de presidente quando este estiver substituindo o Governador do Estado, em caso de impedimento ou vacância, na forma da Constituição Estadual.

(C) esta contará com o assessoramento direto do superintendente legislativo e do Procurador-Geral do Estado.

(D) os titulares de quaisquer de seus cargos poderão, mediante requerimento do interessado, solicitar licença da respectiva função, por interesse particular.

(E) a licença do cargo da Mesa Diretora importará na suspensão das atividades parlamentares do deputado licenciado.

Geografia e História de Roraima

37. O século XX representou um período de transformações significativas no *status* político-administrativo e na dinâmica de ocupação de Roraima. Considerando a sequência de eventos que marcaram o desenvolvimento do estado neste período,

(A) a região permaneceu como parte integrante do estado do Amazonas até o final do século XX, sendo apenas reconhecida como estado na Constituição de 1988, tal como Tocantins, que só se desmembrou de Goiás no mesmo processo constitucional.

(B) a transformação de território federal para estado ocorreu gradualmente entre 1943 e 1962, sem necessidade de qualquer ato legislativo federal adicional.

(C) o Território Federal de Roraima foi criado em 1962 e transformado em estado apenas em 1988, após a aprovação de um plebiscito realizado entre os roraimenses, tendo como base econômica no período: mineração, extrativismo, agricultura, pecuária extensiva, salários e transferências federais.

(D) Roraima foi elevada à categoria de estado em 1962, quando deixou de ser território federal, durante as Reformas de Base, consolidando sua autonomia política junto a outras duas unidades federativas da Região Norte: Amapá e Rondônia.

(E) Roraima foi estabelecida em 1943 como Território Federal do Rio Branco (desmembrado do Amazonas no governo Vargas), renomeada Território de Roraima em 1962 e elevada a estado em 1988; sua economia baseava-se em mineração, extrativismo, agricultura, pecuária extensiva, salários e transferências federais.

38. No século XX, a questão indigenista em Roraima foi também uma questão de geografia econômica. As formas de pressão sobre os povos indígenas variaram conforme a localização no lavrado, nas serras e nas áreas de fronteira, bem como segundo a incidência de fazendas pecuaristas, rodovias, missões, mineração e aparelhos do estado. À luz dessa articulação entre espaço, economia e política indigenista,

(A) a abertura da BR-174 ampliou a presença não indígena nas terras do norte de Roraima, tradicionalmente reduto de territórios indígenas mais protegidos pelo isolamento, assim impactando especialmente áreas indígenas tradicionais do Noroeste do estado pela sua construção no local.

(B) as demarcações do século XX desconsideraram a distribuição histórica dos povos indígenas e foram traçadas, basicamente, segundo limites municipais, arrecadação estadual e conveniência administrativa, e sinergias de atividades econômicas similares das nações indígenas.

(C) a territorialidade indígena de Roraima tornou-se parcialmente urbana ao longo do século XX, o que deslocou a pauta indigenista da terra para temas basicamente sociais/culturais.

(D) nas áreas de lavrado e de fronteira leste, povos como Macuxi, Wapichana e Taurepang sofreram mais cedo e de forma mais contínua a pressão da pecuária e, depois, de eixos como a BR-174; já nas áreas serranas, como as ocupadas pelos Ingarikó, a inserção territorial foi distinta, o que ajuda a explicar ritmos e formatos diferenciados de conflito e reconhecimento.

(E) a geografia teve papel central, pois os conflitos fundiários e as políticas indigenistas se distribuíram de maneira homogênea, por todo o território roraimense, diluindo assim a intensidade dos conflitos em sua territorialidade.

39. A vida na região do Vale do Rio Branco durante quase todo o século XIX caracterizava-se por um contexto socioeconômico específico, marcado por transformações graduais na ocupação territorial. Sobre as condições de vida e a dinâmica social em Roraima em meados do século XIX,

(A) a ocupação não indígena já existia, mas a região era pouco atrativa para colonos, com uma economia voltada ao abastecimento interno, baseada no extrativismo e na pecuária em campos naturais, e com baixo intercâmbio exterior.

(B) a economia monetária era baseada na exploração de ouro e diamantes que, durante o Império e início da República, atraía um grande fluxo de garimpeiros de todo o Brasil.

(C) a região era pouco povoada por colonizadores portugueses e estava sob controle de povos indígenas organizados em confederações, base da organização clânica que, com processo de miscigenação ocorrido no século XIX, constituiria as grandes famílias proprietárias.

(D) a região apresentava ocupação diversificada, com centros urbanos estruturados e manufaturas para o abastecimento interno, além de agricultura de subsistência e pecuária de exportação.

(E) a população era majoritariamente composta por povos indígenas ligados ao extrativismo e à pecuária, e secundariamente por escravizados que trabalhavam em latifúndios produtores de algodão e de açúcar.

40. A criação do Território Federal do Rio Branco em 1943 representou um marco político-administrativo que visava consolidar a presença brasileira nas fronteiras amazônicas. A partir desse momento, a ocupação territorial de Roraima intensificou-se, com transformações significativas na estrutura econômica e demográfica. Sobre a relação entre a criação do Território Federal, os fluxos migratórios e os ciclos econômicos em Roraima,

(A) desde a criação do Território Federal a agropecuária roraimense foi baseada em produção de abastecimento interno, e para exportação de cultivos de soja, milho e café, tendo a pecuária sido introduzida como atividade complementar a da mineração, pois o deslocamento livre do rebanho, como ali era feito, favorecia a busca por garimpos.

(B) com a criação do Território Federal intensificaram-se incentivos à agropecuária, com atração de migrantes nordestinos. A pecuária em campos naturais predominou até os anos 1990, tornando-se, depois, intensiva e tecnificada. Tal processo consolidou Roraima como um dos principais produtores de gado da Amazônia, com cerca de 1,3 milhão de cabeças em 2025.

(C) o rebanho bovino de Roraima permaneceu inferior a 200 mil cabeças até o fim do século XX, aumentando significativamente apenas após 2010 com maior crédito à pecuária e ganhos do garimpo de cassiterita, que realocaram investimentos para o setor.

(D) a atividade pecuária em Roraima remonta à segunda metade do séc. XVIII, mas sua expansão intensiva, baseada em pequenas propriedades familiares e com impacto internacional na exportação brasileira, é sequencial a 1988, quando a elevação a estado permitiu créditos federais para a modernização.

(E) a criação do Território Federal em 1943 não teve conexão com o desenvolvimento agropecuário, sendo a pecuária uma atividade iniciada no séc. XVIII, mas secundária e complementar à ocupação de Roraima, que foi economicamente centrada na mineração.

CONHECIMENTOS ESPECÍFICOS

41. Uma Assembleia Legislativa conduz um processo formal de gestão de riscos conforme a norma ABNT NBR ISO/IEC 27005:2023, na qual foram identificados riscos relacionados à indisponibilidade de sistemas legislativos críticos onde existem controles previamente implementados sem avaliação recente de efetividade. Diante da necessidade de determinar quais controles devem compor o plano de tratamento de riscos, o critério técnico que fundamenta corretamente essa determinação é a

(A) definição de controles com base na categorização dos riscos, com menor ênfase nas condições operacionais e organizacionais.

(B) manutenção de controles alinhados a práticas consolidadas, ainda que não estejam diretamente associados aos riscos priorizados.

(C) inclusão de controles previamente existentes focando em sua formalização documental e viabilidade de implementação.

(D) seleção de controles cuja aplicação produza impacto relevante na probabilidade ou nas consequências dos riscos identificados.

(E) priorização de controles classificados como preventivos, com o objetivo de reduzir a necessidade de monitoramento e resposta operacional.

42. Uma Assembleia Legislativa mantém sistemas críticos de tramitação de projetos em ambiente híbrido (*on-premises* e *cloud*). Diante da necessidade de prevenir a execução de *softwares* não autorizados, identificados em estações de trabalho administrativas, de acordo com os CIS Controls v8, a abordagem que atende corretamente ao requisito de controle de *software* é a

(A) configuração de *logs* de auditoria para registrar execução de aplicações nos *endpoints* registrados.

(B) segregação de ambientes de desenvolvimento e produção para os sistemas legislativos usando práticas DEVSECOPS.

(C) utilização de ferramentas automatizadas para inventariar *softwares* instalados nos ativos corporativos.

(D) adoção de criptografia de dados sensíveis armazenados em bancos de dados institucionais e manipulados por *software*.

(E) implementação de mecanismos de *allowlisting* para garantir que apenas *softwares* autorizados sejam executados.

43. Uma Assembleia Legislativa implementa um SGSI conforme a norma ABNT NBR ISO/IEC 27001:2024, com múltiplas unidades administrativas conduzindo avaliações de riscos. Diante da necessidade de assegurar aplicação uniforme de critérios, rastreabilidade decisória e comparabilidade direta dos resultados entre ciclos, a prática que atende integralmente aos requisitos normativos de definição e aplicação do processo de avaliação de riscos, de acordo com a seção da norma que trata de riscos e oportunidades, é a

(A) revisão periódica dos riscos com base em indicadores institucionais e eventos relevantes para os processos de negócio da organização.

(B) documentação dos riscos avaliados com registro das decisões adotadas pelas unidades responsáveis.

(C) definição e aplicação uniforme de critérios de risco, incluindo aceitação e avaliação, garantindo comparabilidade direta dos resultados.

(D) consolidação dos resultados das avaliações com harmonização posterior conduzida por instância de governança institucional.

(E) condução das avaliações com adaptação de critérios entre unidades, resultando em variações consistentes nos resultados obtidos.

44. Em uma Assembleia Legislativa, a auditoria interna identificou inconsistências na classificação de informações relacionadas a projetos de lei, pareceres técnicos e documentos preparatórios, resultando simultaneamente em compartilhamento indevido de conteúdos sensíveis e restrições excessivas a documentos de caráter público. Considerando explicitamente as diretrizes de Classificação da Informação da norma ABNT NBR ISO/IEC 27002:2022, e a necessidade de alinhar proteção, valor, sensibilidade e criticidade ao longo do ciclo de vida da informação, a prática correta que deve ser adotada, nesse cenário, é

(A) transferir a responsabilidade pela classificação das informações para a área de tecnologia da informação, considerando critérios de armazenamento, processamento e segurança da infraestrutura, que são críticos para o negócio.

(B) definir níveis de classificação com base no impacto do comprometimento da informação, atribuir a responsabilidade aos proprietários da informação e estabelecer revisões periódicas conforme alterações de valor, sensibilidade e criticidade.

(C) estabelecer níveis de classificação no momento da criação da informação, mantendo-os constantes ao longo do tempo para assegurar consistência organizacional e rastreabilidade documental para processos de auditoria.

(D) padronizar um nível de classificação institucional fundamentado em requisitos legais amplos, com o objetivo de reduzir variações operacionais e simplificar a gestão de acesso às informações para favorecer os processos de negócio.

(E) derivar os níveis de classificação a partir das permissões previamente configuradas nos mecanismos de controle de acesso existentes no ambiente tecnológico institucional para manter consistência com sistemas de autenticação e autorização.

45. Uma Assembleia Legislativa realiza estudos estatísticos para subsidiar políticas públicas com base em dados coletados em audiências públicas, operando sob necessidade de proteção de direitos fundamentais e governança institucional, e pretende divulgar resultados agregados. Nesse caso, de acordo com a LGPD, a condição que caracteriza a conformidade com a base legal e com as técnicas de proteção de dados é

(A) a realização de estudos com dados pessoais, com aplicação de anonimização quando tecnicamente viável e uso de ambiente controlado.

(B) a pseudonimização dos dados com circulação entre unidades administrativas para análise descentralizada conforme demanda institucional.

(C) o tratamento fundamentado em consentimento formal dos titulares, com aplicação de anonimização na etapa de divulgação dos resultados.

(D) a utilização de dados sensíveis com aplicação de anonimização antes da disponibilização para análise estatística interna.

(E) o tratamento voltado à execução de políticas públicas, com adoção de controles administrativos e registro das operações.

46. Em uma Assembleia Legislativa, um sistema eletrônico de votação é utilizado para registrar votos de parlamentares em sessões deliberativas, exigindo que cada voto registrado seja posteriormente auditável e não possa ser negado pelo parlamentar que o proferiu, mesmo em processos administrativos ou judiciais. Considerando esse cenário, com requisitos de integridade, autenticidade e impossibilidade de retratação da autoria do voto, o mecanismo criptográfico que deve ser utilizado é

(A) o armazenamento dos votos em banco de dados redundante e criptografado com replicação síncrona entre servidores.

(B) a utilização de assinatura digital baseada em criptografia assimétrica vinculada à identidade do parlamentar.

(C) o uso de funções de *hash* criptográfico para garantir que o conteúdo do voto não seja alterado após o registro.

(D) a aplicação de criptografia simétrica com chave compartilhada entre os parlamentares e o sistema de votação.

(E) o estabelecimento de canal seguro utilizando protocolo de transporte criptografado para envio dos votos.

47. Considere a infraestrutura de TI de uma Assembleia Legislativa que possui sistema de processo legislativo eletrônico, portal institucional exposto à internet, integração com órgãos externos (como tribunais e portais de transparência) e estações de trabalho de gabinetes e áreas administrativas na mesma infraestrutura IP. Após um incidente de segurança com movimentação lateral entre sistemas internos, a arquitetura que melhor atende ao requisito de reduzir a exposição do perímetro e conter a propagação entre ambientes é a

(A) disponibilização dos serviços de integração com órgãos externos diretamente na rede corporativa, com uso de listas de controle de acesso (ACLs) no roteamento central e monitoramento contínuo das conexões estabelecidas.

(B) replicação dos sistemas críticos da assembleia em sub-redes distintas, com conectividade operacional entre elas e prioridade para continuidade de serviço em caso de falhas localizadas.

(C) publicação do portal institucional em uma DMZ, com segmentação interna da rede por função e sensibilidade, definição de políticas explícitas de comunicação entre zonas e bloqueio por padrão de todo tráfego não autorizado entre os segmentos.

(D) concentração dos sistemas legislativos, administrativos e de apoio parlamentar em uma mesma VLAN lógica, com inspeção reforçada no tráfego de entrada e aplicação de controles adicionais nos dispositivos internos.

(E) concentração dos controles de segurança no *firewall* de borda, mantendo os sistemas legislativos, administrativos e de gabinetes no mesmo segmento interno, desde que o NAT oculte os endereços privados.

48. Uma Assembleia Legislativa mantém uma base de dados de cidadãos para participação em consultas públicas digitais, observando requisitos de transparência e controle institucional. Com o objetivo de reduzir riscos aos titulares e limitar o tratamento ao mínimo necessário, adotou técnica de pseudonimização, com segregação da informação adicional de reidentificação em ambiente controlado e seguro. De acordo com a Lei Geral de Proteção de Dados (LGPD), representa uma prática compatível com a técnica adotada e com o princípio da necessidade, a

(A) aplicação de mascaramento dos dados em relatórios externos, preservando integralmente os dados identificáveis no ambiente operacional para uso amplo.

(B) utilização de criptografia com compartilhamento de chaves entre unidades administrativas, permitindo acesso descentralizado aos dados completos conforme demanda institucional.

(C) substituição dos identificadores por funções criptográficas, eliminando a possibilidade de reidentificação e reduzindo permanentemente o conjunto de dados tratados.

(D) manutenção dos dados identificáveis em base única, com controle de acesso por perfis institucionais, garantindo que apenas usuários autorizados acessem todos os dados disponíveis.

(E) separação dos identificadores diretos em ambiente distinto, permitindo reidentificação apenas mediante uso de informação adicional protegida, com acesso restrito aos dados estritamente necessários.

49. Uma instituição pública está sujeita a auditorias que exigem verificação de assinaturas digitais anos após sua emissão, inclusive em cenários onde certificados possam estar expirados ou revogados, assumindo o uso de infraestrutura de chaves públicas com mecanismos de validação e preservação de evidências ao longo do ciclo de vida das assinaturas. Nesse cenário, o recurso técnico que a instituição deverá utilizar é

(A) a aplicação de carimbo do tempo emitido por autoridade confiável, associando o resumo criptográfico do documento a um instante verificável.

(B) a utilização de certificado digital válido no momento da geração da assinatura, considerando sua cadeia de certificação e período de vigência.

(C) a verificação do estado do certificado por meio de consulta a serviço OCSP quando a assinatura é analisada pelo sistema.

(D) a validação da cadeia de certificação com base em listas de certificados revogados disponíveis durante o processo de conferência da assinatura digital.

(E) o armazenamento do documento assinado juntamente com seu resumo criptográfico e metadados estruturados de identificação do signatário e do contexto da transação realizada.

50. Uma Assembleia Legislativa implementa criptografia de dados sensíveis em repouso utilizando AES, sob requisito de confidencialidade e integridade sem aumento significativo de latência. Diante da necessidade de evitar vulnerabilidades como *padding oracle* e reutilização de IV, o modo de operação correto é

(A) o uso do modo OFB, que transforma o bloco em fluxo e evita reutilização de estados internos.

(B) a aplicação do modo CFB com segmentação variável, garantindo proteção contra análise de padrões.

(C) a aplicação do modo CBC com IV fixo, pois garante encadeamento determinístico entre blocos.

(D) a utilização do modo CTR com contador reiniciado por chave, permitindo paralelismo e integridade implícita.

(E) a adoção do modo GCM, que combina criptografia e autenticação com uso de IV único por operação.

51. Uma Assembleia Legislativa opera um sistema de tramitação eletrônica com *backup* completo diário à 0h e *backups* incrementais realizados em intervalos regulares de 4 horas. O ambiente possui replicação assíncrona para um *site* de contingência, na qual as atualizações são propagadas periodicamente, admitindo defasagem limitada ao ciclo de replicação configurado. Em caso de falha do ambiente principal, a restauração por *backups* exige 100 minutos, enquanto a ativação do ambiente contingente depende da execução sequencial de cinco procedimentos operacionais de 5 minutos cada. Considerando um incidente ocorrido às 13h10 e a alternativa de recuperação que reduz simultaneamente a perda de dados e o tempo de indisponibilidade do serviço, o valor do RTO, em minutos, é

(A) 70.

(B) 100.

(C) 15.

(D) 25.

(E) 40.

52. Considere uma Assembleia Legislativa responsável por sistemas eletrônicos de tramitação de projetos de lei e registros de votação, submetida a auditorias institucionais e a requisitos de conformidade baseados na norma ABNT NBR ISO/IEC 27001:2024 e na LGPD, operando em ambiente distribuído e sujeita à necessidade de apresentar registros de eventos como evidência técnica verificável sob contestação administrativa ou judicial, inclusive diante de possíveis tentativas de adulteração interna. Nesse cenário, o mecanismo que assegura a detectabilidade inequívoca de modificações na sequência histórica dos *logs* é

(A) encadeamento criptográfico sequencial dos registros de *log*, no qual cada entrada incorpora o *hash* da entrada anterior.

(B) replicação síncrona dos *logs* em múltiplos domínios administrativos com verificação de consistência entre cópias.

(C) aplicação de função de *hash* criptográfico individual sobre cada registro de *log*, armazenado juntamente com seu respectivo valor de verificação.

(D) assinatura digital periódica de lotes de *logs* utilizando chaves assimétricas sob controle da organização.

(E) armazenamento de *logs* em repositório imutável com controle de versão e restrição de sobrescrita.

53. Uma Assembleia Legislativa disponibiliza uma API REST para consulta e gestão de documentos legislativos. Um *endpoint* permite acessar documentos por meio da seguinte requisição:

```
GET /api/documentos/{documentId}
Authorization: Bearer <JWT>
```

Durante testes de segurança, foi identificado que usuários autenticados conseguem acessar documentos de outros gabinetes simplesmente alterando o valor de `{documentId}` na URL, sem qualquer validação adicional no *backend*.

Considerando o cenário descrito e as boas práticas de segurança da OWASP API Security Top 10 (2023), é possível concluir que se trata de uma vulnerabilidade

(A) que poderia ser completamente mitigada somente substituindo os identificadores sequenciais por UUIDs aleatórios.

(B) que poderia ser prevenida por meio da comparação entre o ID do usuário presente no JWT e o `{documentId}` na requisição.

(C) de autenticação, pois o uso de JWT não impede que usuários acessem recursos de outros usuários.

(D) de *Broken Object Level Authorization* (BOLA), pois o sistema não valida se o usuário autenticado tem permissão para acessar o objeto identificado por `{documentId}`.

(E) de *Broken Function Level Authorization* (BFLA), pois o *endpoint* não restringe quais funções podem ser executadas.

54. Em uma Assembleia Legislativa, o sistema de acesso interno permite autenticação de servidores via *endpoint* `POST /graphql`, com limitação de 3 requisições por minuto por IP. Durante uma auditoria, verificou-se que um agente malicioso utilizou *batching* de *queries* GraphQL para submeter múltiplas combinações de credenciais em uma única requisição, contornando o controle existente. Considerando esse cenário e a necessidade de mitigar ataques de força bruta e *credential stuffing*, o controle que deve ser utilizado é

(A) adotar assinatura criptográfica robusta nos JSON Web Tokens e ampliar seu tempo de expiração para o tempo de duração da sessão, reduzindo assim a frequência de autenticação.

(B) registrar eventos de autenticação malsucedida, implementar mecanismo de *cache* para respostas de autenticação inválida e acionar alertas automáticos para o SOC após volume elevado de tentativas oriundas de um mesmo endereço IP.

(C) aplicar limitação de tentativas de autenticação no nível lógico da operação de *login*, contabilizando individualmente cada par usuário-senha processado dentro de requisições compostas.

(D) reduzir o tamanho máximo permitido das requisições GraphQL para menos de 256 *bytes*, limitando a quantidade de operações incluídas em um único *payload* para menos de 3 requisições.

(E) exigir uso obrigatório de canal criptografado TLS para todas as requisições de autenticação realizadas pelos sistemas internos e usar criptografia AES para as transações internas.

55. A Assembleia Legislativa identificou o uso indevido de seu domínio para campanhas de *spoofing* e alta incidência de mensagens maliciosas. Para implementar uma solução técnica que proteja a reputação institucional e a integridade das comunicações, o Analista de Segurança deve garantir que

(A) o *SPF* liste os servidores autorizados, o *DKIM* garanta a integridade via assinatura criptográfica e o *DMARC* oriente a política de descarte ou quarentena para falhas de autenticação.

(B) a política de *DMARC* substitua a necessidade de filtros de *antivírus* e *Anti-Spam*, sendo que o *DKIM* gerencie o limite de conexões simultâneas via protocolo SMTP nos servidores de correio da nuvem.

(C) o registro *SPF* autentique o conteúdo da mensagem via criptografia e o *DKIM* limite o envio de anexos por servidores externos, permitindo que o *firewall* filtre o tráfego de entrada.

(D) o mecanismo de *Anti-Spam* valide o cabeçalho das mensagens via chaves públicas, enquanto o registro *DMARC* automatize a exclusão de *e-mails* que não contenham assinaturas digitais do tipo *S/MIME*.

(E) o registro *SPF* identifique os endereços IP autorizados a enviar mensagens, e o *DMARC* realize a verificação de integridade do corpo do *e-mail* através de certificados de infraestrutura de rede.

56. A Assembleia Legislativa detectou ataques de *spear phishing* direcionados ao setor financeiro, utilizando *e-mail spoofing* para simular ordens de pagamento da presidência. Para mitigar esses ataques e proteger os usuários, a solução técnica correta deve prever que

(A) o servidor de correio desabilite o tráfego de saída para domínios externos não mapeados e o sistema de proteção de usuários utilize criptografia de disco para evitar o redirecionamento de DNS.

(B) a política de segurança implemente o bloqueio de *scripts* em navegadores, fazendo com que a proteção contra *spoofing* ocorra via inspeção de pacotes em redes locais para identificar o endereço MAC do remetente.

(C) o filtro de *Anti-Spam* bloqueie mensagens com base em palavras-chave de engenharia social, enquanto o treinamento de conscientização substitua o uso de chaves de segurança física em dispositivos móveis.

(D) a solução de *e-mail gateway* valide o alinhamento de protocolos de autenticação de domínio, enquanto a proteção de *endpoint* monitore comportamentos de *phishing* em URLs e anexos suspeitos.

(E) o mecanismo de *spoofing protection* realize o bloqueio de domínios similares (*typosquatting*) via *firewall* de aplicação, com base nos certificados de segurança do *site*.

57. A Assembleia Legislativa precisa estabelecer uma política de gestão de ativos para assegurar a proteção de dados parlamentares e administrativos. Para implementar o inventário e a classificação de acordo com a criticidade e o ciclo de vida, a solução correta determina que

(A) a proteção dos ativos de informação dependa da instalação de agentes de monitoramento no *hardware* físico, enquanto as garantias associadas sejam imputadas ao provedor de nuvem pública.

(B) o ciclo de vida da informação seja definido pela gestão de capacidade de armazenamento dos *storages*, vinculando a proteção do ativo ao provedor de nuvem pública.

(C) o inventário de ativos seja atualizado via *cloud security* e as responsabilidades de classificação sejam delegadas aos usuários finais com base no volume de dados armazenados em cada servidor da nuvem.

(D) a classificação de criticidade dos ativos ocorra via protocolos de criptografia assimétrica na rede de borda (*edge network*), garantindo que o ciclo de vida da informação seja gerido por ferramentas de gestão da informação.

(E) o inventário identifique a propriedade e a criticidade de cada ativo, permitindo que a classificação oriente os controles de proteção e os procedimentos de descarte seguro ao final do ciclo de vida.

58. O Analista de Segurança deve implementar o ciclo de gestão de vulnerabilidades nos servidores que hospedam os sistemas de votação da Assembleia. Para assegurar a integridade do ambiente e a continuidade dos serviços, a solução técnica que equilibra proteção proativa e remediação exige que

(A) a gestão de vulnerabilidades dependa da substituição integral do *hardware* afetado, enquanto a gestão de *patches* ocorra via atualização de tabelas de roteamento na base de segurança do provedor de nuvem.

(B) a priorização das falhas seja baseada no volume de *logs* gerados pelos sistemas, enquanto o contexto do *hardening* foque na instalação de agentes de monitoramento de tráfego em redes locais e virtuais.

(C) o escaneamento identifique falhas e as priorize via *CVSS (Common Vulnerability Scoring System)*, aplicando o *hardening* para reduzir a superfície de ataque e automatizando a gestão de *patches* em ambiente de homologação.

(D) a análise de vulnerabilidades ocorra via varredura de portas na rede de borda, responsabilizando, para a correção de falhas, o suporte do fabricante e aplicando o *hardening* para evitar latência nos serviços.

(E) o ciclo de correção priorize a instalação imediata de *patches* em servidores de produção, enquanto o *hardening* foque na alteração de chaves de criptografia assimétrica em dispositivos de rede.

59. A Assembleia Legislativa promoveu um ciclo de conscientização em segurança da informação para equipes técnicas e usuários finais. O Analista de Segurança deve estruturar esse programa alinhando boas práticas operacionais às diretrizes do ITIL v4, garantindo que os processos de educação continuada integrem a gestão de serviços de TI. A solução técnica correta prevê que

(A) o programa integre *continual improvement* e *knowledge management* do ITIL v4, com trilhas diferenciadas por perfil, simulações práticas de ameaças reais, indicadores de efetividade revisados periodicamente e alinhamento às políticas de governança institucional.

(B) a conscientização seja incorporada à prática de *service desk* do ITIL v4, com o registro de chamados de segurança alimentando os conteúdos de treinamento, métricas de reincidência orientando as campanhas e revisão anual do programa vinculada ao ciclo de *release management*.

(C) o programa de conscientização seja conduzido como projeto especial, com trilhas distintas para usuários e equipes técnicas, avaliado por métricas de conclusão de módulos e integrado ao processo de *change management* do ITIL v4 para registro das atualizações de conteúdo.

(D) a educação em segurança seja tratada como prática de *continual improvement* no ITIL v4, com campanhas periódicas baseadas em incidentes recorrentes, simulações de *phishing* e indicadores de efetividade revisados em ciclos de melhoria documentados.

(E) o programa seja estruturado com base no catálogo de serviços do ITIL v4, vinculando cada módulo de treinamento a um serviço crítico da instituição, usando *knowledge management* para manter a base de conteúdos atualizada conforme mudanças no ambiente.

60. O Analista de Segurança deve estruturar um programa de conscientização em segurança da informação para a Assembleia Legislativa, integrando boas práticas educacionais às diretrizes do PMBOK 7ª edição. A solução técnica adequada prevê que

(A) o domínio de *measurement* do PMBOK 7 seja adotado para estruturar indicadores de maturidade dos usuários, integrando os resultados das simulações de *phishing* ao painel de desempenho do programa e revisando trilhas conforme os dados coletados.

(B) o programa seja estruturado com base no domínio de *stakeholders* do PMBOK 7, mapeando perfis de usuários como partes interessadas, definindo planos de engajamento por grupo e usando *lessons learned* de incidentes para atualizar os conteúdos de conscientização.

(C) o programa seja gerenciado como projeto com escopo fixo, usando o princípio de *stewardship* do PMBOK 7 para orientar a entrega de trilhas de treinamento, com métricas de conclusão como principal indicador de valor gerado.

(D) o programa aplique os princípios de *value delivery* e *stakeholder engagement* do PMBOK 7, com trilhas diferenciadas por perfil, simulações de ameaças reais, indicadores de efetividade revisados em ciclos adaptativos e alinhamento às políticas de governança institucional.

(E) a gestão do programa utilize o domínio de desempenho de *uncertainty* do PMBOK 7 para mapear ameaças ao programa de treinamento, com campanhas baseadas em incidentes anteriores e revisão de conteúdo vinculada ao registro de riscos do ambiente de TI.

61. A Assembleia Legislativa migrou parte de seu banco de dados parlamentar para um ambiente de nuvem pública. Para garantir a proteção dos dados em repouso, seguindo as melhores práticas de governança e conformidade técnica, o Analista de Segurança deve implementar uma solução que preveja

(A) a implementação de perímetros de segurança via *Azure Bastion* para acesso externo, mantendo os *logs* de auditoria de leitura e escrita no *Audit Database Cloud* para otimizar o custo operacional da solução de monitoramento.

(B) a segregação de redes via *VPC/VNet*, o gerenciamento de chaves criptográficas através de serviços de *KMS* e a aplicação do princípio do menor privilégio via políticas de *IAM* em todos os recursos.

(C) o uso de grupos de segurança (*Security Groups*) para gerenciar a criptografia de disco, responsabilizando o provedor de nuvem pela gestão das chaves privadas do banco de dados via política de acesso *IAM*.

(D) a configuração de instâncias em sub-redes públicas para permitir a inspeção de tráfego pelo WAF, utilizando chaves SSH globais compartilhadas como processo facilitador da administração remota da infraestrutura.

(E) o isolamento de recursos via *VPC* e a proteção contra ataques de negação de serviço através do *Cloud Armor*, controlando a integridade dos dados da aplicação via *protection engine SAV*.

62. Uma Assembleia Legislativa opera sistemas críticos em nuvem pública e precisa estruturar um modelo integrado de controle de acesso, monitoramento e proteção de dados. O Analista de Segurança deve implementar mecanismos que garantam rastreabilidade, segregação de funções e proteção contra acesso indevido, considerando ambientes distribuídos e dinâmicos.

A solução técnica adequada exige que

(A) o controle de acesso seja estruturado por identidades de serviço com permissões dinâmicas baseadas em contexto, o monitoramento utilize coleta de métricas e eventos em múltiplas camadas e a proteção de dados adote criptografia em repouso com chaves vinculadas ao ciclo de vida das aplicações.

(B) a gestão de acesso utilize autenticação adaptativa com base em risco, o monitoramento correlacione eventos de rede e aplicação com análise comportamental e a proteção de dados utilize criptografia com segregação lógica por ambiente e classificação da informação.

(C) o controle de acesso utilize perfis agregados por função organizacional com permissões herdadas, o monitoramento correlacione eventos via *logs* de aplicação e a proteção de dados adote criptografia gerenciada pelo provedor com rotatividade automática padrão.

(D) a autenticação federada seja integrada a diretórios corporativos com emissão de *tokens* de curta duração, o monitoramento consolide eventos em plataforma de *SIEM* e a proteção de dados utilize criptografia em trânsito com certificados emitidos por autoridade interna.

(E) o controle de acesso implemente políticas granulares com *least privilege* e segregação de funções via IAM, o monitoramento centralize *logs*, trilhas de auditoria e eventos em serviços nativos integrados a análise contínua, e a proteção de dados utilize criptografia em repouso e em trânsito com gerenciamento de chaves por *KMS* sob controle da organização.

63. A Assembleia Legislativa está na fase de planejamento para a contratação de uma solução de *Disaster Recovery* (DR). Para garantir a sustentabilidade econômica e a governança operacional do contrato, o Analista de Segurança deve estruturar o processo de forma que a

(A) pesquisa de preços priorize as notas fiscais de fornecedores locais, a matriz RACI defina as sanções contratuais por atraso e a gestão de riscos analise a compatibilidade do *software* com o sistema de Compras Corporativas.

(B) gestão de riscos estabeleça o orçamento máximo da contratação, enquanto a matriz RACI gerencie o inventário de ativos em nuvem e a pesquisa de preços utilize orçamentos de empresas sem registro no SICAF (Sistema de Cadastramento Unificado de Fornecedores).

(C) pesquisa de preços utilize fontes diversificadas como o Painel de Preços e contratações similares, enquanto a matriz RACI defina as responsabilidades de execução, aprovação, consulta e informação de cada entrega técnica.

(D) análise de riscos mapeie as falhas de *hardware* no site principal, a pesquisa de preços ocorra via cotação direta com fabricantes e a matriz RACI estabeleça os níveis de serviço para a equipe de suporte.

(E) matriz RACI identifique os riscos de indisponibilidade do *link* de dados, a pesquisa de preços valide o menor valor global e a gestão de riscos oriente o plano de comunicação entre os parlamentares.

---

64. A Assembleia Legislativa precisa contratar o desenvolvimento de um sistema de gestão parlamentar sob demanda e garantir sua sustentação contínua. O Analista de Segurança deve estruturar o modelo contratual que melhor equilibre controle técnico, conformidade e economicidade. A solução adequada prevê que

(A) o desenvolvimento sob demanda seja contratado via fábrica de *software* com métrica de ponto de função, a sustentação seja objeto de contrato autônomo com ANS por severidade, e a escolha entre IaaS e PaaS seja orientada pelo nível de controle operacional que o órgão pretende manter sobre o ambiente.

(B) o sistema seja desenvolvido sob demanda com entrega por *sprints* documentados, a sustentação seja incorporada ao contrato de desenvolvimento para simplificar a gestão e a infraestrutura seja contratada via SaaS para eliminar a necessidade de gerenciamento de plataforma pela equipe interna.

(C) o desenvolvimento seja contratado como *software* sob demanda via fábrica de *software*, com entregas medidas por pontos de função, e a sustentação seja coberta por contrato SaaS com o mesmo fornecedor, unificando responsabilidades técnicas e contratuais.

(D) o licenciamento de *software* pronto cubra as funcionalidades parlamentares, com customizações entregues pela fábrica de *software* sob contrato separado, e a infraestrutura seja provisionada via IaaS para manter o controle do ambiente pelo órgão.

(E) a fábrica de *software* desenvolva o sistema sob demanda com métricas de produtividade por ponto de função, a sustentação seja contratada separadamente com SLA definido por severidade de chamados e a infraestrutura seja provisionada via PaaS para reduzir a gestão operacional.

---

65. A Assembleia Legislativa deve revisar sua estrutura de governança para assegurar o alinhamento das ações de segurança da informação às metas institucionais. Para integrar o planejamento estratégico à gestão operacional de riscos e conformidade, a solução técnica correta determina que

(A) a gestão de riscos foque na identificação de falhas de *hardware* em *switches*, orientando o *PETIC* no treinamento de suporte técnico para que a governança monitore o tráfego de dados do portal.

(B) o *PETIC* estabeleça a visão estratégica de segurança, o *PDTIC* detalhe os projetos e investimentos na área e a gestão de mudanças e riscos garanta a conformidade técnica das alterações no ambiente.

(C) o *PETIC* defina as especificações de *hardening* de servidores, delegando ao *PDTIC* a definição da periodicidade de trocas de senhas e à gestão de mudanças a automação dos *backups* em nuvem.

(D) a gestão de riscos identifique ameaças ao ambiente físico, possibilitando que a conformidade valide a substituição de perímetros de *firewall* por políticas de conscientização em redes sociais no *PETIC*.

(E) o *PDTIC* priorize a aquisição de licenças de antivírus, cabendo à gestão de mudanças o inventário de ativos de rede e à conformidade técnica a validação do uso de *software* livre no setor de RH.

---

66. A Assembleia Legislativa planeja contratar uma nova solução de *Security Operations Center* (SOC). Para assegurar a conformidade com o rito administrativo e a eficácia técnica da aquisição, a equipe de planejamento da contratação deve garantir que

(A) o Projeto Básico contenha a estimativa de preços baseada em notas fiscais de órgãos parceiros, enquanto o Estudo Técnico Preliminar (ETP) foque na descrição dos requisitos de *hardware* e o Termo de Referência na governança.

(B) o planejamento das contratações utilize o Termo de Referência para avaliar alternativas de mercado, enquanto o Estudo Técnico Preliminar (ETP) defina as sanções administrativas e o Projeto Básico determine o índice de reajuste.

(C) o Estudo Técnico Preliminar (ETP) defina o modelo de licenciamento de *software*, enquanto o Termo de Referência estabeleça a análise de viabilidade econômica e o Projeto Básico foque no mapa de riscos.

(D) o Estudo Técnico Preliminar (ETP) demonstre a viabilidade técnica e a justificativa da solução, enquanto o Termo de Referência detalhe o objeto, deveres da contratada e critérios de aceitação baseados em níveis de serviço.

(E) as etapas da contratação iniciem pela elaboração do Termo de Referência para balizar o mercado e, depois, o Estudo Técnico Preliminar (ETP) complete o processo com a descrição da metodologia de execução e medição.

67. Um analista de segurança da informação de uma Assembleia Legislativa Estadual precisa proteger o portal institucional hospedado em um servidor *web* na DMZ. O portal recebe diariamente milhares de acessos de cidadãos e servidores externos, armazena dados sensíveis de parlamentares e funcionários e integra-se a sistemas internos de tramitação de projetos. O analista identificou que o portal já sofreu tentativas de ataque do tipo *SQL Injection* e *Cross-Site Scripting* (XSS), além de ataques de DDoS do tipo *SYN flood* originados de redes externas. A Assembleia possui um *link* dedicado de 10 Gbps e um *firewall* de borda com funcionalidades básicas de estado de conexão. Considerando o cenário e as boas práticas de segurança para proteção de aplicações *web* e mitigação de DDoS em perímetro, a solução consiste em

(A) um IPS posicionado na rede interna, pois os ataques identificados são geralmente originados a partir de computadores internos comprometidos e uma solução WAF para lidar com ataques do DDoS.

(B) uma VPN *site-to-site* entre a DMZ e cada usuário externo, criptografando o tráfego do portal contra ataques *web* e uma solução UTM contra ataques de camada de aplicação.

(C) um WAF para proteção específica contra *SQL Injection* e XSS, e uma solução UTM com anti-DDoS para proteção contra DDoS e outras ameaças de perímetro.

(D) um sistema IPS em modo passivo contra *SQL Injection* na porta SPAN do *switch* da DMZ e um IDS com capacidade reativa para detecção e eliminação de ataques do tipo DDoS.

(E) um *proxy* reverso como balanceamento de carga entre múltiplos servidores *web* para suportar ataques DDoS, e uma inspeção proteção do tipo NAC para controle de acesso às aplicações.

68. Um analista de segurança da informação de uma Assembleia Legislativa Estadual está configurando o portal institucional para garantir a confidencialidade e integridade dos dados trafegados entre os cidadãos e o servidor *web*. O analista está em dúvida sobre a implantação do protocolo HTTPS utilizando certificados digitais baseados nos padrões TLS e SSL. Durante a configuração, o analista precisa escolher as opções corretas para garantir um nível adequado de segurança, considerando as vulnerabilidades conhecidas. Considerando as boas práticas atuais para implementação segura de HTTPS, o analista deve configurar o protocolo

(A) SSL 2.0 com certificado de chave simétrica, pois esse algoritmo é mais rápido que a criptografia assimétrica utilizada no TLS.

(B) TLS 3.0 com certificado *wildcard* para os subdomínios, e autoassinado por uma Autoridade Certificadora (CA) confiável.

(C) SSL 3.0 com certificado autoassinado, emitido por uma Autoridade Certificadora (CA) confiável.

(D) TLS 1.0 com certificado *wildcard* para os subdomínios, e estabelecendo a validação da origem do emissor do certificado.

(E) TLS 1.3 com certificado emitido por uma Autoridade Certificadora (CA) pública confiável, e desabilitar versões antigas.

69. A Assembleia Legislativa planeja migrar seus sistemas legados para um ambiente de nuvem e contratar o desenvolvimento de um novo portal de transparência. Para garantir a segurança e a conformidade técnica no modelo contratual, a solução deve prever que

(A) a migração ocorra para um modelo *Public Cloud* com criptografia de ponta a ponta gerida pelo provedor, os requisitos técnicos de sustentabilidade foquem no descarte de *hardware* e o desenvolvimento seja entregue via *SaaS* para reduzir a superfície de ataque local.

(B) o contrato de infraestrutura priorize o modelo *On-premises* para manter a soberania dos dados, a segurança da informação seja tratada como um requisito funcional específico de cada entrega e a acessibilidade seja orientada por meio do uso de ferramentas de tradução automática.

(C) o desenvolvimento seja medido por *story points* em regime *Agile*, a infraestrutura utilize o modelo *Community Cloud* para isolamento lógico total e os requisitos de acessibilidade sigam a norma ISO 27001 para garantir a inclusão digital dos cidadãos.

(D) o edital exija certificações *SOC 2 Type II* (*Service Organization Control 2*) do provedor de nuvem, o desenvolvimento utilize métricas de Ponto de Função com análise estática de código (*SAST*) integrada e o contrato preveja sanções por descumprimento de níveis de serviço de segurança.

(E) a arquitetura seja baseada em *Multicloud* para evitar o *vendor lock-in*, a sustentação seja contratada por postos de trabalho presenciais para controle físico e os requisitos não funcionais de segurança sejam validados após a homologação final do *software*.

70. Um analista de segurança da informação de uma Assembleia Legislativa Estadual está projetando a arquitetura de rede para um novo anexo funcional. O analista decidiu implementar uma DMZ em um *firewall* para hospedar os servidores de aplicações *web* (10.20.30.41/29) e o servidor de arquivos públicos (10.20.30.42/29), enquanto a rede interna (10.10.0.0/16) está conectada a outra interface do *firewall*. Considerando as boas práticas de segurança para implementação de DMZ, o analista deve

(A) permitir seletivamente o tráfego da rede interna para a DMZ e bloquear todo o tráfego da internet para a DMZ, pois os servidores devem ser acessados apenas pelos funcionários internos.

(B) configurar um túnel VPN entre a DMZ e cada estação de trabalho da rede interna, garantindo que o tráfego entre essas redes seja criptografado, dispensando regras de *firewall* específicas.

(C) permitir todo o tráfego da internet para a DMZ sem restrições e bloquear todo o tráfego da DMZ para a rede interna, garantindo que servidores comprometidos não afetem a rede interna.

(D) permitir apenas o tráfego necessário da internet para a DMZ para o servidor *web* e servidor de arquivos e permitir apenas o tráfego essencial da DMZ para a rede interna.

(E) configurar a DMZ em modo *bridge* com a interface externa, eliminando a necessidade de regras de *firewall*, pois o isolamento é garantido pelo próprio conceito de DMZ.

71. Em um ambiente com Active Directory executando Windows Server, um analista de segurança descobre que o domínio permite consultas LDAP anônimas. Para resolver essa vulnerabilidade de forma nativa, segura e garantindo a compatibilidade do ambiente, o analista deve

(A) ativar a política `RestrictAnonymous` no nível 0 para impedir qualquer comunicação de rede que não utilize autenticação mútua Kerberos.

(B) ativar a política `RestrictALL` no nível 0 para impedir qualquer comunicação de rede que não utilize autenticação mútua LDAP.

(C) configurar uma GPO para exigir LDAP *Signing* e ajustar as permissões de controle de acesso (ACLs) para remover o acesso de leitura do grupo Logon Anônimo.

(D) habilitar o serviço de DNSSec do Active Directory e forçar a comunicação via protocolo SMB assinado de forma anônima.

(E) migrar os serviços para a porta 636, e forçar a utilização de certificados autoassinados gerados individualmente em cada estação de trabalho para garantir que o atacante utilize um certificado comum a todos os usuários.

72. Um analista de segurança precisa realizar o *hardening* de um servidor Ubuntu que hospeda uma aplicação *web* (https) crítica. O objetivo é garantir que o servidor obtenha proteção contra ataques de interceptação. De acordo com as melhores práticas e recomendações, e considerando as capacidades nativas das versões recentes do Ubuntu, o conjunto de ações que representa a implementação correta do *hardening* de transporte é:

(A) Instalar o módulo `mod_ssl` via repositórios *universe* e definir a diretiva `SSLHonorCipherOrder` como `off`, permitindo que o navegador do cliente escolha a cifra mais segura disponível, independentemente da configuração do servidor.

(B) Habilitar o cabeçalho `Strict-Transport-Security` (HSTS) com o parâmetro `includeSubDomains`, configurar o `ssl_protocols` para utilizar TLSv1.2 e TLSv1.3.

(C) Configurar o parâmetro `ssl_protocols` para aceitar TLSv1.1 e TLSv1.2, desabilitar o suporte a compressão GZIP no nível do HTTP para evitar ataques CRIME e forçar o uso de cifras baseadas em RC4 para maior compatibilidade.

(D) Migrar os certificados para o formato PKCS#7 (P7B), desabilitar a renovação automática para evitar alterações não autorizadas no sistema de arquivos e configurar o parâmetro `keepalive_timeout` para 0, visando fechar conexões HTTPS imediatamente após cada requisição.

(E) Desabilitar o *firewall* UFW para evitar latência no *handshake* TLS, configurar o servidor para operar na porta 80 e realizar o redirecionamento via *software* para a porta 443, garantindo que o tráfego inicial seja sempre monitorado.

73. Um analista de segurança da informação de uma Assembleia Legislativa Estadual está estudando os principais conceitos relacionados à autenticação, controle de acesso e gerenciamento de identidades para implementar na Assembleia. Sobre esses temas ele concluiu corretamente que

(A) Federação de identidades é um conceito aplicável a redes sociais, não podendo ser implementado em ambientes corporativos com servidores locais.

(B) OpenID Connect (OIDC) é uma camada de autenticação que fornece informações sobre a identidade do usuário autenticado através de um *token* ID.

(C) IAM tem como função o gerenciamento de senhas de usuários e a autenticação por mecanismos biométricos.

(D) RBAC é um modelo de controle de acesso onde as permissões são atribuídas diretamente a usuários individuais de cada grupo.

(E) OAuth 2.0 é um protocolo de autenticação que substitui o uso de senhas, permitindo que o usuário acesse sistemas sem fornecer credenciais que ele conhece.

74. Um analista de segurança da informação de um órgão governamental está revisando a arquitetura do servidor de *e-mail* corporativo. O objetivo é mitigar ataques de interceptação (*sniffing*) de credenciais transmitidas em texto claro e do conteúdo das mensagens durante a comunicação entre os clientes de *e-mail* dos funcionários e o servidor. Para garantir a confidencialidade tanto no envio quanto no recebimento das mensagens, o analista deve configurar as portas e os protocolos adequados. Considerando as boas práticas de segurança para comunicação de serviços de *e-mail*, a configuração mais adequada que o analista deve implementar consiste em

(A) utilizar o SMTPS na porta 2525 para o envio de mensagens e o IMAP encapsulado na porta 22, aproveitando a criptografia do protocolo SSH para a sincronização das caixas de entrada.

(B) exigir o uso de IMAPS na porta 993 ou POP3S na porta 995 para o recebimento de mensagens, e configurar o envio por submissão SMTP na porta 587 com uso obrigatório de STARTTLS.

(C) utilizar o SMTP na porta 25, o POP3 na porta 110 e o IMAP na porta 143, aplicando as tecnologias SPF e DKIM para garantir a criptografia do tráfego.

(D) desabilitar os protocolos IMAP e POP3, centralizando o envio e o recebimento de *e-mails* de forma bidirecional e criptografada na porta 25 do protocolo SMTP.

(E) manter o IMAP na porta 143 e o POP3 na porta 110, pois esses protocolos possuem criptografia nativa para a autenticação, exigindo o uso de TLS para o SMTP via porta 465.

75. O SOC de uma Assembleia Legislativa Estadual identificou diversos alertas no SIEM nas últimas 24 horas. Após a triagem inicial, o analista isolou os seguintes eventos:

1. Evento 1: Múltiplas tentativas de autenticação com falha para um usuário de nível estagiário, seguidas de um *login* bem-sucedido em horário comercial.
2. Evento 2: Execução de um binário em uma estação de trabalho com nome `svchost.exe`, porém localizado no diretório `C:\Users\Public\`, sem conexões de rede ativas.
3. Evento 3: Identificação de tráfego de saída massivo (exfiltração) para um endereço IP listado em bases de *Threat Intelligence* como comando e controle (C2), originado da estação de trabalho de um assessor legislativo.
4. Evento 4: Notificação de alteração de configuração em um terminal de autoatendimento que não processa dados sigilosos.

Considerando os Indicadores de Comprometimento (IoC) apresentados e as melhores práticas de resposta a incidentes, o evento que deve ser priorizado pelo SOC e a primeira ação técnica a ser tomada são: Evento

(A) 4; primeira ação: desligar o servidor central de arquivos da assembleia imediatamente para evitar propagação.

(B) 3; primeira ação: realizar o *backup* completo do disco rígido antes de desconectar a máquina da rede.

(C) 2; primeira ação: desabilitar o antivírus para permitir que a equipe de forense execute ferramentas de análise sem interferência.

(D) 1; primeira ação: resetar a senha do usuário e aguardar o próximo relatório semanal de auditoria.

(E) 3; primeira ação: isolar a estação de trabalho da rede para conter a exfiltração de dados e a comunicação com o invasor.

---

76. Um analista de segurança da informação de uma Assembleia Legislativa Estadual precisa proteger o sistema de consulta de processos licitatórios, hospedado em um ambiente de nuvem híbrida. O sistema é acessado por servidores públicos internos, prefeitura municipal e cidadãos em geral, armazenando dados sigilosos sobre lances e propostas comerciais. O analista identificou tentativas recentes de ataque do tipo *Path Traversal* e um ataque de DDoS do tipo HTTP *Slowloris*, que sobrecarrega a camada de aplicação. A infraestrutura atual conta com um *firewall* de última geração (NGFW) com inspeção superficial de tráfego HTTPS e um balanceador de carga básico, sem proteção específica para ataques de camada 7. Considerando o cenário e as boas práticas de segurança para proteção de aplicações *web* e de perímetro, a solução que o analista deve implementar consiste em

(A) um NAC na rede interna, pois CSRF geralmente se origina de estações internas comprometidas, e um UTM na borda para bloquear *Path Traversal* e DDoS simultaneamente.

(B) uma VPN SSL para cada usuário externo, criptografando todo o tráfego do portal contra ataques de aplicação, e um balanceador de carga avançado contra DDoS de camada 7.

(C) um WAF para proteção específica contra *Path Traversal* e uma solução DDoS de camada de aplicação baseada em comportamento ou desafios para mitigar ataques como *Slowloris*.

(D) um IDS em linha na porta espelhada do *switch* para detectar CSRF e um *firewall* de borda com regras estáticas para bloquear *Path Traversal*, mantendo o NGFW existente contra DDoS.

(E) um *proxy* reverso com *cache* para aliviar a carga de requisições repetitivas e um antivírus de *gateway* para impedir *Path Traversal*, pois CSRF é mitigado com *token* anti-CSRF no código.

---

77. Uma Assembleia Legislativa Estadual utiliza 300 estações (Windows) e 30 servidores (Linux/Windows) para atividades legislativas, incluindo votação eletrônica, acesso a sistemas sigilosos e armazenamento de projetos de lei. Recentemente, um ataque de *ransomware* propagou-se via dispositivo USB infectado utilizado por um assessor parlamentar, explorando uma vulnerabilidade dia-zero em um editor de PDF. O antivírus tradicional baseado apenas em assinaturas não detectou a ameaça. A equipe de segurança da Assembleia determinou a implantação de uma solução moderna de proteção de *endpoints* que atenda aos seguintes requisitos obrigatórios:

- Detecção baseada em comportamentos;
- Resposta automatizada a incidentes (isolamento de máquina, encerramento de processos suspeitos);
- Monitoramento contínuo de processos e chamadas de sistema;
- Controle rigoroso de dispositivos removíveis (USB, CD/DVD);
- Capacidade de análise forense em memória e disco.

Considerando as melhores práticas de segurança para órgãos públicos e os requisitos estabelecidos, a solução que melhor atende os requisitos da equipe de segurança é:

(A) Implementação de uma plataforma unificada de proteção de *endpoints* que integra capacidades de EDR, permitindo resposta automatizada a incidentes e controle nativo de dispositivos removíveis.

(B) *Antimalware open-source* configurado para varreduras diárias completas nos servidores da Câmara, associado a uma política interna de proibição de uso de dispositivos USB por meio de assinatura de termo de compromisso pelos deputados.

(C) Solução XDR com a capacidade de isolamento de *endpoints* e suporte a controle de dispositivos USB por meio de um antivírus tradicional.

(D) Configurar Antivírus corporativo com atualizações de assinaturas a cada 4 horas, combinado com uma GPO que desabilita todas as portas USB dos computadores do Legislativo.

(E) *Firewall* de próxima geração (NGFW) posicionado no *Data Center* do Legislativo com inspeção TLS, combinado com um antivírus gratuito em cada estação parlamentar, com agente central de gerenciamento.

78. Um analista de segurança da informação de uma Assembleia Legislativa Estadual atende a um incidente no qual um servidor público suspeito de desviar recursos públicos teve seu *notebook* apreendido em sua sala. O equipamento está ligado e com a sessão de usuário aberta, exibindo uma planilha e um terminal de acesso a um sistema interno não autorizado. O analista precisa coletar evidências para uma investigação criminal, garantindo a integridade dos dados originais. Considerando as boas práticas de forense computacional, a conduta inicial mais adequada do analista é

(A) manter o *notebook* ligado, capturar a memória RAM e os processos ativos, documentar tudo, e então proceder ao desligamento conforme protocolo pericial, antes de realizar a imagem *bit* a *bit* do disco.

(B) fotografar a tela aberta exibindo a planilha e o terminal, desligar o *notebook* normalmente pelo sistema operacional e lacrar o equipamento em um saco antiestático.

(C) desligar o *notebook* imediatamente puxando o cabo de energia e a bateria, para evitar alterações acidentais nos arquivos, e depois realizar uma cópia *bit* a *bit* do disco rígido do equipamento apreendido.

(D) remover o disco rígido do *notebook*, conectá-lo a um segundo computador já limpo e copiar as pastas de documentos e os *e-mails* do servidor público suspeito investigado na operação.

(E) fazer *login* no sistema com uma conta administrativa alternativa, copiar a planilha e o histórico do terminal para um *pendrive*, e depois desligar o equipamento.

---

79. Um analista de segurança da informação de uma Assembleia Legislativa Estadual está revisando um Acordo de Confidencialidade (NDA) proposto por uma empresa terceirizada que prestará serviços de suporte técnico em bancos de dados contendo informações sigilosas de parlamentares e servidores. O documento apresentado pela empresa contém cinco cláusulas. Considerando as boas práticas de segurança da informação e a legislação aplicável, o analista verificou que apenas uma das cláusulas está totalmente adequada e deve ser mantida em um NDA válido:

(A) A qualificação das informações como confidenciais dependerá de notificação por escrito da contratante a cada documento específico a ser protegido.

(B) O signatário fica isento de responsabilidade em caso de vazamento de informações ocorrido por meio de equipamento pessoal não fornecido pela contratante.

(C) O signatário poderá reter cópias das informações confidenciais após o término do contrato para fins de comprovação de suas atividades profissionais.

(D) As informações confidenciais poderão ser utilizadas pelo signatário para fins de treinamento de novos funcionários da contratante, desde que os dados sejam anonimizados internamente.

(E) Ao término do contrato, o signatário deverá devolver ou destruir todas as informações confidenciais, mediante comprovação documental.

---

80. Um analista de segurança da informação do Ministério da Fazenda é responsável por proteger um banco de dados corporativo com informações fiscais e cadastrais de milhões de contribuintes, incluindo CPF, renda, endereços e dados bancários. O SGBD utilizado é um banco de dados relacional moderno, com acesso simultâneo de aplicações *web* internas, sistemas legados e equipes de suporte que realizam consultas administrativas diretamente via SQL. O analista identificou os seguintes requisitos obrigatórios:

1. Garantir que usuários de suporte vejam apenas os 4 primeiros dígitos do CPF em consultas diretas, mantendo o valor completo apenas para aplicações autorizadas.

2. Proteger os dados armazenados em disco contra acesso físico não autorizado ao *storage*.

A infraestrutura atual conta apenas com a autenticação nativa do SGBD (usuário e senha) e permissões básicas (GRANT/REVOKE). Não há qualquer mecanismo de ofuscação ou criptografia implementado.

Considerando esse cenário e as boas práticas de segurança em SGBDs, a solução mais adequada que o analista deve implementar consiste em

(A) usar criptografia de coluna usando AES-256 configurada estaticamente via *stored procedures*, e mascaramento de CPF nas telas da aplicação (não no banco).

(B) substituir o banco de dados relacional por um SGBD NoSQL que ofereça criptografia nativa, e utilizar ofuscação estática de CPF via funções de *hash* irreversíveis.

(C) mascaramento estático de dados (*Static Data Masking*) aplicar uma única vez sobre a coluna CPF, e criptografia de disco *full-disk* no *storage*.

(D) usar criptografia em nível de aplicação (antes de enviar ao banco) para todos os dados sensíveis, e visões para controlar o acesso ao CPF.

(E) usar criptografia transparente de dados (TDE) para proteger os dados em disco, e mascaramento dinâmico de dados para ofuscar o CPF conforme o perfil do usuário.

PROVA DISCURSIVA-REDAÇÃO

Instruções Gerais: *Conforme Edital publicado, Capítulo 10 [...] 10.8 Será atribuída nota ZERO à Prova Discursiva-Redação que: a) fugir ao tema proposto. Em caso de fuga completa ao tema proposto, a redação não será pontuada em qualquer outro de seus aspectos, recebendo nota 0 (zero) em todos os itens do critério. b) fugir à modalidade de texto solicitada. Em caso de fuga completa ao gênero/tipo de texto solicitado, a redação não será pontuada em qualquer outro de seus aspectos, recebendo nota 0 (zero) em todos os itens do critério. c) apresentar texto sob forma não articulada verbalmente (apenas com desenhos, números e palavras soltas ou versos) ou em outra língua que não a língua portuguesa; d) apresentar formas propositais e explícitas de anulação, como impropérios e trechos jocosos, ou predominância de rasura; e) for assinada fora do local apropriado; f) apresentar qualquer sinal, marca, risco, desenho, rubrica, assinatura ou nome, feito pelo candidato, nas linhas destinadas à resposta definitiva que, de alguma forma, possibilite a identificação do candidato; g) estiver em branco; h) apresentar predominantemente letra ilegível e/ou incompreensível; i) apresentar até 7 (sete) linhas escritas; j) apresentar texto idêntico ou produzido por outro candidato ou no qual se identifique cópia (em todo ou em parte) de modelos de textos prontos disponíveis para consulta em fontes de acesso público. k) apresentar texto idêntico (em todo ou em parte) ao produzido pelo mesmo candidato, ainda que em cargos diferentes; l) não atender aos requisitos definidos na grade de correção de critérios pela Banca Examinadora. 10.9 Na* ***Prova Discursiva-Redação****, a folha para rascunho no caderno de provas será de preenchimento facultativo. Em hipótese alguma o rascunho elaborado pelo candidato será considerado na correção pela Banca Examinadora. 10.9.1 O candidato deverá atentar para a folha destinada ao rascunho e a folha destinada à resposta definitiva, a fim de que não seja prejudicado. A folha para a resposta definitiva será a única válida para a avaliação da Prova Discursiva-Redação. 10.10 Na* ***Prova Discursiva-Redação****, deverá ser rigorosamente observado o* ***limite mínimo de 20 (vinte) linhas e máximo de 30 (trinta) linhas****, sob pena de perda de pontos a serem atribuídos à Prova-Discursiva-Redação. 10.11 A* ***Prova Discursiva-Redação*** *terá caráter eliminatório e classificatório e será avaliada na escala* ***de 0 (zero) a 100 (cem)****. 10.11.1 Considerar-se-á aprovado o candidato que tiver obtido nota* ***igual ou superior a 50,00 (cinquenta) pontos****.*

TEXTO 1

O termo inclusão digital tenta expressar a noção já tradicional, embora controversa, de que certos meios e/ou tecnologias podem ser aplicados de maneira planejada, eficaz e previsível ao desenvolvimento social. O qualificador "digital" aparece nessa expressão para ressaltar o fato de que, em anos recentes, uma gama ampla de sentidos do desenvolvimento tem sido associada às Novas Tecnologias da Informação e da Comunicação (TIC). Essas, por sua vez, têm sido vistas como "chaves para o crescimento, empregos, investimento e inovação" uma vez que "um uso mais amplo e eficiente das TIC por todos os setores da economia é uma clara oportunidade de fomento da competitividade, do desenvolvimento sustentável e da inclusão social".

Grosso modo, duas condições para a inclusão digital têm sido apontadas como essenciais, quando não como suficientes: o acesso à infraestrutura técnica mínima (computadores, software *e serviços de conexão à internet) e um grau mínimo de capacitação da população para o uso das TIC.*

(Adaptado de: BUZATO, Marcelo. Letramento e inclusão. Revista Delta: Documentação e Estudos em Linguística Aplicada. v. 25, n. 1, 2009. Disponível em: **<https://www.scielo.br/j/delta/a/kgCZ89jPSGTy85Z9ncL5m9c/?format=html&lang=pt>**)

TEXTO 2

Solicitação de Identidade, pagamento de impostos, agendamentos, alterações e transferência de titularidades – serviços que há alguns anos só poderiam ser realizados presencialmente, ou por documentos físicos – agora contam com plataformas digitais de fácil acesso.

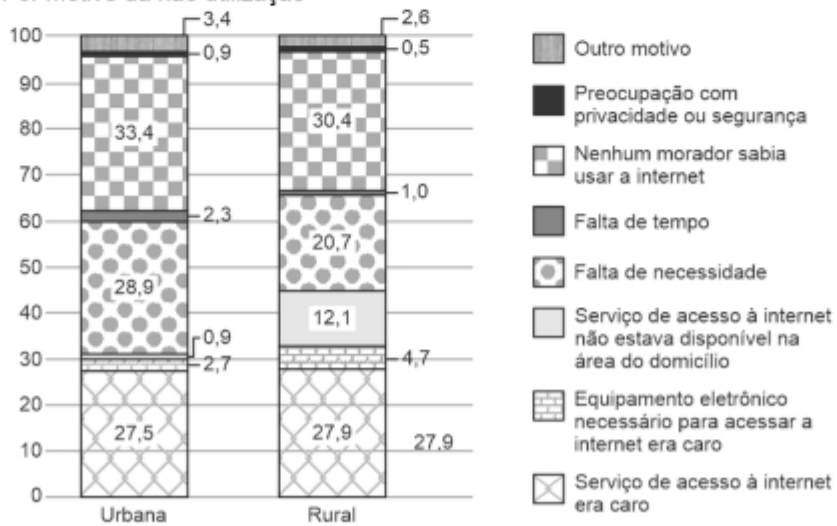
Segundo dados disponibilizados pelo governo federal, mais de 100 milhões de solicitações que teriam sido presenciais foram atendidas digitalmente graças à chamada transformação digital – a adoção de tecnologia e inovação para o atendimento de clientes.

Dos quase 4,5 mil serviços oferecidos pela administração pública para cidadãos e empresas, cerca de 3 mil já possuem trâmite totalmente digital e podem ser acessados pelo computador ou por smartphones. *Destes, 1,4 mil foram digitalizados ainda em 2019. "O objetivo é oferecer políticas públicas e serviços de melhor qualidade, mais simples e acessíveis a qualquer hora e lugar, a um custo menor para o cidadão", informa o levantamento.*

(Adaptado de: OLIVEIRA, Pedro. Mais de 70% dos serviços públicos brasileiros já são digitais. Agência Brasil. Disponível em: **< https://agenciabrasil.ebc.com.br/geral/noticia/2021-07/mais-de-70-dos-servicos-publicos-brasileiros-ja-sao-digitais>.** Publicado em: 27/07/2021. Acesso em: 30/04/2026)

TEXTO 3

Distribuição dos domicílios em que não havia utilização da Internet (%)
Por motivo da não utilização



(LOSCHI, Marília. Internet chega a 74,9 milhões de domicílios do país em 2024. Disponível em: **<https://agenciadenoticias.ibge.gov.br/agencia-noticias/2012-agencia-de-noticias/noticias/44031-internet-chega-a-74-9-milhoes-de-domicilios-do-pais-em-2024>**. Publicado em: 24/07/2025. Acesso em: 30/04/2026)

TEXTO 4

Hoje, cerca de 66% da população idosa brasileira utiliza a internet, segundo dados de 2023 do IBGE. Isso significa que, em um país onde a expectativa de vida já ultrapassa os 75 anos e há mais de 32 milhões de pessoas com 60 anos ou mais, aproximadamente dois terços desse grupo estão conectados. No entanto, mesmo entre os idosos que acessam a internet, muitos enfrentam o que especialistas chamam de "baixa conectividade significativa" – ou seja, acesso limitado em termos de frequência, qualidade da banda larga, tecnologia 4G e dispositivos adequados. De fato, cerca de 61% dos idosos apresentam níveis baixos de conectividade significativa, o que pode comprometer a plena utilização dos benefícios digitais.

Na prática, milhões de pessoas continuam à margem de serviços essenciais como o SUS (Serviço Único de Saúde), o INSS (Instituto Nacional de Seguro Social) e o Gov.br, cada vez mais digitalizados. Em nome da eficiência, estamos correndo o risco de trocar filas por exclusão. Afinal, se um benefício só pode ser acessado via aplicativo, ele está realmente garantido?

(Adaptado de: AGUSTINI, Gabriela. Importância da inclusão de pessoas longevas no digital. Nexo Jornal. Disponível em: **<https://www.nexojornal.com.br/etarismo-e-analfabetismo-digital-inclusao-idosos>**. Publicado em: 29/06/2025. Acesso em: 30/04/2026)

Considerando os textos acima, escreva um texto dissertativo-argumentativo sobre o tema:

A invisibilidade do cidadão analógico: a exclusão digital como barreira para o acesso pleno à cidadania

01	
02	
03	
04	
05	
06	
07	
08	
09	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	
22	
23	
24	
25	
26	
27	
28	
29	
30	