

TÉCNICO EM DESENVOLVIMENTO – ANALISTA DE SISTEMAS (ÊNFASE EM ANALISTA DE SEGURANÇA DA INFORMAÇÃO)




BADESUL DESENVOLVIMENTO S.A. –
AGÊNCIA DE FOMENTO/RS
Concurso Público 01/2026

PROVA TEÓRICO-OBJETIVA

70 questões

 5 alternativas


PROVA DISCURSIVA

 02 questões

TEMPO DE PROVA

 5 horas

 Saída permitida somente após 1 hora de prova

 O candidato só poderá levar este Caderno após 1 hora de prova

INSTRUÇÕES



Confira se esse Caderno de Prova contém a quantidade de questões indicadas e 2 (duas) questões discursivas. A substituição deste Caderno de Prova ocorre apenas antes de iniciar a prova.

- ▣ O tempo de prova inclui o preenchimento do Cartão-Resposta e da Folha Definitiva da Prova Discursiva.
- ▣ Nenhuma informação acerca do conteúdo das questões será fornecida pelo Fiscal de Sala, pois é parte integrante da prova.
- ▣ Ao concluir estas provas, entregue o Cartão-Resposta ao Fiscal de Sala, **devidamente assinado**, e a Folha Definitiva da Prova Discursiva.
- ▣ Ao final da prova, os 03 (três) últimos candidatos deverão permanecer na Sala de Prova até que o último termine a sua prova, devendo ambos testemunhar a devolução e o lacre dos documentos.
- ▣ A divulgação do gabarito preliminar e do padrão de respostas se dará conforme Cronograma de Execução do certame.

TODOS OS DIREITOS RESERVADOS AO INSTITUTO LEGALLE. PROIBIDO REPRODUÇÃO.

RASCUNHO PARA GABARITO

01	06	11	16	21	26	31	36	41	46	51	56	61	66
02	07	12	17	22	27	32	37	42	47	52	57	62	67
03	08	13	18	23	28	33	38	43	48	53	58	63	68
04	09	14	19	24	29	34	39	44	49	54	59	64	69
05	10	15	20	25	30	35	40	45	50	55	60	65	70

Para responder às questões 01 a 10, leia o texto abaixo.

Da renda à ciência, desigualdade racial segue moldando o Brasil

Neste 21 de março, Dia Internacional contra a Discriminação Racial, olhar para a desigualdade no Brasil é, inevitavelmente, olhar para o que persiste. Não apenas nos indicadores, mas nas estruturas que atravessam o tempo e organizam silenciosamente a vida social. Como resume o economista Mário Theodoro — ex-pesquisador do Instituto de Pesquisa Econômica Aplicada (Ipea) e uma das principais referências no tema —, “a pobreza, a miséria e, principalmente, a desigualdade são fenômenos que remontam à própria criação do Brasil e têm raízes na questão racial”.

Os dados mais recentes do Ipea não deixam espaço para dúvida: mesmo diante de avanços importantes nas políticas públicas, a desigualdade racial permanece como uma presença constante. Ela não se limita a um campo específico — infiltra-se na renda, atravessa o acesso a serviços, delimita trajetórias e chega, inclusive, à forma como o país produz e organiza seus próprios dados.

Mais do que um desvio ou uma exceção, trata-se de um padrão que se repete. Uma engrenagem que se ajusta ao tempo, mas não se desfaz, e que segue desafiando tanto a ação do Estado quanto a capacidade de compreender, em profundidade, o Brasil que se constrói todos os dias.

O estudo Desigualdade de raça e gênero e impactos distributivos dos gastos públicos com saúde e educação no Brasil mostra que as políticas públicas têm, sim, potência transformadora. Ao incorporar serviços de saúde e educação ao cálculo da renda ampliada, a desigualdade diminui de forma expressiva — o índice de Theil (medida estatística de desigualdade econômica e concentração de renda) recua de 0,62 para 0,38, sinalizando o efeito redistributivo do Estado.

Mas há camadas que resistem.

Entre 11% e 12% da desigualdade total ainda se explica por fatores como raça e gênero, revelando que essas dimensões continuam a organizar o acesso a oportunidades. Mesmo quando o Estado atua, as marcas da desigualdade não desaparecem por completo — elas se reconfiguram.

Essa distância se amplia quando se observa o gasto privado: entre as famílias de maior renda no país, por exemplo, as chefiadas por homens brancos chegam a investir em saúde até 150% do que é gasto por famílias negras. Em um mesmo país, convivem realidades profundamente distintas, separadas por barreiras que nem sempre são visíveis, mas são persistentemente eficazes.

E quando raça e gênero se cruzam, o cenário se torna ainda mais complexo. As desigualdades não apenas se somam — elas se aprofundam, revelando um tecido social

onde as diferenças se entrelaçam e se reforçam mutuamente.

Há ainda um outro desafio, mais silencioso: o de medir a desigualdade. O estudo Avanços entre desafios: uma análise da evolução da qualidade das informações de raça/cor na Rais e no Novo Caged aponta melhorias importantes na qualidade dos registros, como a redução de informações ignoradas ao longo do tempo. Mas revela também que os dados ainda carregam distorções.

Bases administrativas seguem apresentando sobrerrepresentação de pessoas brancas e sub-representação de pessoas pretas quando comparadas a outras fontes, como a PNAD Contínua. Em anos recentes, essa diferença ultrapassou três pontos percentuais — e já foi ainda maior.

São pequenas distâncias nos números, mas grandes no que elas significam.

Porque medir mal é, muitas vezes, enxergar menos. E enxergar menos é também limitar a capacidade de agir.

Quando reunidos, os estudos apontam para uma mesma direção: a desigualdade racial no Brasil não é episódica. Não é um resíduo do passado. É uma presença ativa, que se reorganiza e se mantém ao longo do tempo.

Ela atravessa a renda, o acesso a serviços, os espaços de poder e até os instrumentos que deveriam revelá-la. Está nas trajetórias individuais, mas também nas estruturas que as condicionam.

E é justamente essa persistência que torna o desafio mais complexo — e mais urgente.

Fonte: <https://www.ipea.gov.br/portal/categorias/45-todas-as-noticias/noticias/16302-da-renda-a-ciencia-desigualdade-racial-segue-moldando-o-brasil> (adaptado).

Questão 01. Ao mobilizar os dados do estudo sobre os impactos distributivos dos gastos públicos com saúde e educação, o texto sustenta que:

- (A) A atuação estatal anulou as disparidades sociais historicamente vinculadas à raça e ao gênero, tornando residual a desigualdade no país.
- (B) Os avanços observados na renda ampliada resultam, sobretudo, da expansão do gasto privado das famílias de menor renda em saúde e educação.
- (C) Os estudos citados indicam que raça e gênero perderam relevância analítica, uma vez que o acesso a oportunidades passou a depender prioritariamente do mérito individual.
- (D) A redução estatística da desigualdade demonstra que os serviços públicos produzem efeito redistributivo, embora não eliminem integralmente as assimetrias estruturais.
- (E) O índice de Theil comprova que a desigualdade racial deixou de ser um problema central, passando a predominar, no Brasil, uma diferenciação apenas econômica.

Questão 02. Ao afirmar que **há camadas que resistem**, o texto passa a desenvolver a ideia de que:

- (A) A persistência das diferenças decorre, predominantemente, de escolhas individuais das famílias diante das oportunidades oferecidas.
- (B) Os indicadores de desigualdade deixaram de ser confiáveis, razão pela qual não permitem mais interpretar a realidade social brasileira.
- (C) A desigualdade, embora reduzida pelos gastos públicos, preserva núcleos de permanência associados a fatores estruturais, como raça e gênero.
- (D) O problema central da desigualdade brasileira está restrito à insuficiência de dados estatísticos sobre renda e consumo.
- (E) O estado, ao ampliar serviços sociais, intensificou diferenças antes inexistentes entre grupos raciais e econômicos.

Questão 03. No trecho em que o texto aborda a qualidade das informações de raça/cor em bases administrativas, a argumentação conduz à conclusão de que:

- I. A melhora nos registros administrativos foi suficiente para tornar dispensável a comparação com outras fontes estatísticas nacionais.
- II. Distorções na produção dos dados comprometem a visibilidade do fenômeno social, podendo restringir a formulação e a eficácia das ações de enfrentamento.
- III. A sub-representação de pessoas pretas decorre da oscilação natural dos levantamentos, sem impacto relevante para a compreensão da realidade brasileira.

Das assertivas, pode-se afirmar que:

- (A) I, II e III estão corretas.
- (B) Apenas I está incorreta.
- (C) Apenas I e II estão corretas.
- (D) Apenas II não está incorreta.
- (E) Apenas III não está incorreta.

Questão 04. Em **Ela não se limita a um campo específico — infiltra-se na renda, atravessa o acesso a serviços, delimita trajetórias e chega, inclusive, à forma como o país produz e organiza seus próprios dados**, a expressão **delimita trajetórias** foi empregada com o sentido de:

- (A) Amplia percursos sociais, ao multiplicar de modo equilibrado as possibilidades de ascensão individual.
- (B) Define caminhos livres de obstáculos, ao distribuir de maneira uniforme o acesso a bens e serviços.
- (C) Reorganiza escolhas subjetivas, ao substituir condicionamentos estruturais por decisões exclusivamente individuais.
- (D) Condiciona percursos de vida, ao impor barreiras que restringem oportunidades e possibilidades de deslocamento social.
- (E) Descreve percursos pessoais, ao registrar neutralmente os diferentes modos de inserção dos indivíduos na sociedade.

Questão 05. No trecho **Mesmo quando o Estado atua, as marcas da desigualdade não desaparecem por completo — elas se reconfiguram**, a palavra **reconfiguram** exemplifica um caso de:

- (A) Derivação prefixal, pois houve acréscimo de prefixo à palavra base, com alteração de sentido.
- (B) Composição por aglutinação, pois ocorreu fusão de elementos com alteração estrutural da base.
- (C) Derivação sufixal, pois houve acréscimo de sufixo nominal à forma primitiva.
- (D) Composição por justaposição, pois dois radicais foram unidos sem perda fonética.
- (E) Derivação regressiva, pois a palavra resulta da redução de uma forma verbal anterior.

Questão 06. No período **E quando raça e gênero se cruzam, o cenário se torna ainda mais complexo**, a oração **quando raça e gênero se cruzam** classifica-se como:

- (A) Oração subordinada adverbial condicional, pois indica hipótese necessária para a complexidade do cenário.
- (B) Oração subordinada adverbial temporal, pois expressa circunstância de tempo em relação à oração principal.
- (C) Oração subordinada adjetiva restritiva, pois caracteriza o substantivo **cenário**.
- (D) Oração coordenada sindética aditiva, pois acrescenta uma informação autônoma à oração seguinte.
- (E) Oração subordinada substantiva subjetiva, pois exerce a função de sujeito da oração principal.

Questão 07. O vocábulo **que** pertence ao grupo das palavras de grande versatilidade na língua portuguesa, pois pode assumir diferentes classificações gramaticais conforme o contexto em que aparece. No período **Mas há camadas que resistem**, o vocábulo **que** classifica-se como:

- (A) Conjunção subordinativa causal.
- (B) Conjunção integrante.
- (C) Pronome indefinido.
- (D) Partícula expletiva.
- (E) Pronome relativo.

Questão 08. A relação entre letras e sons nem sempre ocorre de forma direta na língua portuguesa, razão pela qual a análise de fonemas e dígrafos exige observar a realização sonora efetiva de cada vocábulo. Considerando essa perspectiva, assinale a alternativa INCORRETA.

- (A) **exemplo** apresenta 7 letras e 7 fonemas.
- (B) **profundidade** apresenta 11 fonemas e 1 dígrafo.
- (C) **expressiva** apresenta 10 letras, 9 fonemas e 1 dígrafo.
- (D) **chefiadas** apresenta 1 dígrafo consonantal e 8 fonemas.
- (E) **atravessa** apresenta 8 fonemas e 1 dígrafo consonantal.

Questão 09. Os sujeitos das orações podem apresentar diferentes classificações, conforme a forma como o termo a que o verbo se refere se manifesta na estrutura sintática. Entre os tipos mais recorrentes, estão o sujeito simples; o sujeito composto; o sujeito oculto; o sujeito indeterminado; e a oração sem sujeito. Assim, no trecho **a pobreza, a miséria e, principalmente, a desigualdade são fenômenos que remontam à própria criação do Brasil**, o sujeito da forma verbal **são** classifica-se como:

- (A) Sujeito indeterminado.
- (B) Oração sem sujeito.
- (C) Sujeito composto.
- (D) Sujeito simples.
- (E) Sujeito oculto.

Questão 10. A colocação pronominal em língua portuguesa refere-se à posição do pronome oblíquo átono em relação ao verbo. A identificação dessa colocação depende da estrutura da oração e da forma verbal a que o pronome se vincula. No trecho **Ela atravessa a renda, o acesso a serviços, os espaços de poder e até os instrumentos que deveriam revelá-la**, a colocação pronominal presente em **revelá-la** classifica-se como:

- (A) Ênclise.
- (B) Próclise.
- (C) Epêntese.
- (D) Hipérclise.
- (E) Mesóclise.

LEGISLAÇÃO APLICÁVEL

Questão 11. Analise o texto a seguir, conforme Lei Federal nº 13.303/2016:

As licitações realizadas e os contratos celebrados por empresas públicas e sociedades de economia mista destinam-se a assegurar a seleção da proposta mais economicamente financeira, inclusive no que se refere ao ciclo de vida do objeto, e a evitar operações em que se caracterize sobrepreço ou superfaturamento, devendo observar os princípios da impessoalidade, da moralidade, da igualdade, da publicidade, da eficiência, da proibidade administrativa, da economicidade, do desenvolvimento nacional sustentável, da vinculação ao instrumento convocatório, da obtenção de competitividade e do julgamento objetivo.

Acerca do texto, pode-se afirmar que ele está:

- (A) Plenamente adequado, visto que observa a legislação vigente.
- (B) Parcialmente adequado, visto que a seleção citada busca a proposta mais vantajosa.
- (C) Parcialmente adequado, visto que não se evita sobrepreço, o qual é interessante para o poder público.
- (D) Plenamente inadequado, visto que em nada observa a legislação vigente.
- (E) Parcialmente adequado, visto que o julgamento objetivo não deve ser buscado, e sim o subjetivo.

Questão 12. As instituições autorizadas a funcionar pelo Banco Central do Brasil devem manter registros de todas as operações realizadas, produtos e serviços contratados, inclusive _____, recebimentos, transferências de recursos e operações no mercado de câmbio.

Quantos dos seguintes itens podem preencher a lacuna acima? **I.** saques; **II.** aportes; **III.** depósitos; **IV.** pagamentos.

- (A) Nenhum deles.
- (B) Apenas 1 deles.
- (C) Apenas 2 deles.
- (D) Apenas 3 deles.
- (E) Todos os 4.

Questão 13. O servidor público que utilizar ou viabilizar a utilização de qualquer informação obtida em decorrência da quebra de sigilo de que trata a Lei Complementar nº 105/2001, responde pessoal e diretamente pelos danos decorrentes, sem prejuízo da responsabilidade objetiva da entidade pública, quando comprovado que o servidor agiu de acordo com orientação oficial. A quebra de sigilo, fora das hipóteses autorizadas na Lei citada, constitui crime e sujeita os responsáveis à pena de _____ e multa, aplicando-se, no que couber, o Código Penal, sem prejuízo de outras sanções cabíveis.

Preenche CORRETAMENTE a lacuna:

- (A) detenção.
- (B) repreensão pública.
- (C) advertência.
- (D) moção de repúdio.
- (E) reclusão.

Questão 14. O Cadastro Nacional de Empresas Punidas - CNEP reúne e dá publicidade às sanções aplicadas pelos órgãos ou entidades dos Poderes Executivo, Legislativo e Judiciário de todas as esferas de governo com base na Lei Federal nº 12.846/2013. O CNEP contém, entre outras, as informações acerca das sanções aplicadas previstas em quantos dos seguintes itens? **I.** Tipo de sanção; **II.** Dados pessoais dos componentes da Comissão Penalizadora; **III.** Razão social e número de inscrição da pessoa jurídica ou entidade no Cadastro Nacional da Pessoa Jurídica - CNPJ; **IV.** Data de aplicação e data final da vigência do efeito limitador ou impeditivo da sanção, quando for o caso.

- (A) Nenhum deles.
- (B) Apenas 1 deles.
- (C) Apenas 2 deles.
- (D) Apenas 3 deles.
- (E) Todos os 4.

Questão 15. As instituições autorizadas a funcionar pelo Banco Central do Brasil devem requerer dos sacadores clientes e não clientes solicitação de provisionamento com, no mínimo, três dias úteis de antecedência, das operações de saque, inclusive as realizadas por meio de cheque ou ordem de pagamento, de valor igual ou superior a:

- (A) Dois mil reais.
- (B) Dez mil reais.
- (C) Quinze mil reais.
- (D) Vinte e cinco mil reais.
- (E) Cinquenta mil reais.

Questão 16. Acerca dos agentes de tratamento de dados pessoais, conforme a Lei Geral de Proteção de Dados Pessoais, analise as assertivas:

- I. A autoridade nacional poderá dispor sobre padrões de interoperabilidade para fins de portabilidade, livre acesso aos dados e segurança, assim como sobre o tempo de guarda dos registros, tendo em vista especialmente a necessidade e a transparência.
- II. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.
- III. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, salvo quando baseado no legítimo interesse.

Está(ão) CORRETA(S):

- (A) Apenas I e II.
- (B) Apenas III.
- (C) I, II e III.
- (D) Apenas II.
- (E) Apenas I e III.

Questão 17. Tem-se que as agências de fomento podem empregar em suas atividades, além de recursos próprios, os provenientes do previsto em quantos dos seguintes itens? **I.** Orçamentos federal, estadual e municipal; **II.** Fundos e programas oficiais; **III.** Organismos e instituições financeiras nacionais e internacionais de desenvolvimento; **IV.** Captação de depósito interfinanceiro vinculado a operações de microfinanças.

- (A) Nenhum deles.
- (B) Apenas 1 deles.
- (C) Apenas 2 deles.
- (D) Apenas 3 deles.
- (E) Todos os 4.

Questão 18. Observe as afirmações que seguem:

As agências de fomento devem constituir e manter, permanentemente, fundo de liquidez equivalente, no mínimo, a _____ do valor de suas obrigações, a ser integralmente aplicado em títulos públicos federais.

Para isso, consideram-se obrigações os valores registrados no _____ circulante, as coobrigações por cessão de crédito e as garantias prestadas.

Preenche, CORRETA e respectivamente, as lacunas:

- (A) sete por cento; ativo.
- (B) dez por cento; passivo.
- (C) doze por cento; ativo.
- (D) quinze por cento; passivo.
- (E) vinte por cento; ativo.

Questão 19. Analise as partes que seguem: Além dos estabelecimentos bancários oficiais ou privados, das sociedades de crédito, financiamento e investimentos, das caixas econômicas e das cooperativas de crédito ou a seção de crédito das cooperativas que a tenham, também se subordinam às disposições e disciplina da Lei Federal nº 4.595/1964 no que for aplicável (**1ª parte**) as bolsas de valores, companhias de seguros e de capitalização, as sociedades que efetuam distribuição de prêmios em imóveis, mercadorias ou dinheiro, mediante sorteio de títulos de sua emissão ou por qualquer forma (**2ª parte**), e as pessoas, desde que jurídicas, que exerçam, por conta própria ou de terceiros, atividade relacionada com a compra e venda de ações e outros quaisquer títulos, realizando nos mercados financeiros e de capitais operações ou serviços de natureza dos executados pelas instituições financeiras (**3ª parte**).

Acerca das partes, pode-se afirmar que:

- (A) Apenas a 1ª parte está incorreta.
- (B) Apenas a 2ª parte está incorreta.
- (C) Apenas a 3ª parte está incorreta.
- (D) Apenas a 1ª parte está correta.
- (E) Apenas a 2ª parte está correta.

Questão 20. Quantos dos seguintes itens constituem o Sistema Financeiro Nacional, estruturado e regulado pela Lei Federal nº 4.595/1964? **I.** Banco do Brasil S.A.; **II.** Conselho Monetário Nacional; **III.** Banco Central do Brasil; **IV.** Demais instituições financeiras, desde que públicas.

- (A) Nenhum deles.
- (B) Apenas 1 deles.
- (C) Apenas 2 deles.
- (D) Apenas 3 deles.
- (E) Todos os 4.

RACIOCÍNIO LÓGICO

Questão 21. Uma agência de fomento estabeleceu a seguinte norma para a concessão de crédito a startups: "Se o projeto apresenta inovação disruptiva ou a garantia real é superior a 150% do empréstimo, então o desembolso é aprovado e os juros são subsidiados." Considere que, em um processo de auditoria, descobriu-se que a norma acima foi descumprida em um processo específico (ou seja, a proposição lógica é falsa). Nesse caso, é logicamente CORRETO afirmar que:

- (A) O projeto apresenta inovação disruptiva, mas o desembolso não foi aprovado.
- (B) O projeto não apresenta inovação disruptiva e a garantia real é inferior a 150% do empréstimo.
- (C) O desembolso foi aprovado, mas os juros não foram subsidiados.
- (D) Se o projeto não é disruptivo, então a garantia real é superior a 150%.
- (E) O projeto é disruptivo ou a garantia é superior a 150%, e o desembolso foi aprovado.

Questão 22. Uma agência de fomento possui um orçamento anual de R\$ 250 milhões, dos quais R\$ 34 milhões são destinados ao desenvolvimento econômico de um projeto social de impacto regional. Buscando ampliar a captação de recursos, os analistas da agência submeteram uma proposta a um fundo internacional. A condição estabelecida para a liberação do novo aporte é que o valor total destinado a esse projeto social passe a representar exatamente 20% do novo orçamento anual total da agência. Considere que todo o recurso adicional obtido pelos analistas será somado tanto ao orçamento total da agência quanto à verba específica do projeto social. Para atender à exigência do fundo internacional, o valor, em milhão de real, que os analistas conseguiram a mais para a agência foi de:

- (A) 66.
- (B) 50.
- (C) 22.
- (D) 20.
- (E) 16.

Questão 23. Para processar os pedidos de subvenção econômica de um novo edital, a agência estima que 12 analistas, com a mesma capacidade de trabalho, operando 6 horas por dia, conseguem analisar 180 projetos em 20 dias. Devido à alta demanda, a agência precisa analisar 300 projetos em apenas 15 dias. Para cumprir esse novo cronograma, mantendo a mesma eficiência, quantos analistas serão necessários se a jornada diária for estendida para 8 horas?

- (A) 15 analistas.
- (B) 18 analistas.
- (C) 20 analistas.
- (D) 22 analistas.
- (E) 24 analistas.

Questão 24. O cronograma de liberação de recursos para a construção de um polo tecnológico prevê 12 parcelas mensais que formam uma Progressão Aritmética. Sabe-se que a soma da 3ª parcela com a 10ª parcela totaliza R\$ 800.000,00. A diretoria da agência de fomento aprovou um teto total de investimento para este projeto (a soma das 12 parcelas), em milhão de real, de exatamente:

- (A) 4,0.
- (B) 4,8.
- (C) 5,2.
- (D) 5,6.
- (E) 6,0.

Questão 25. O comitê de avaliação de risco de uma agência de fomento é composto por 10 membros, sendo 6 especialistas em Economia e 4 especialistas em Engenharia. Para garantir uma análise criteriosa e multidisciplinar de projetos estratégicos — como os voltados ao setor de saneamento básico — a agência realiza o sorteio aleatório de uma comissão técnica formada por 4 membros distintos dentre os integrantes do comitê. Considerando que todos os membros têm a mesma chance de serem selecionados e que a escolha é feita de forma aleatória, deseja-se avaliar a composição dessa comissão sob o ponto de vista da diversidade de formação acadêmica. Com base nisso, qual é a probabilidade de que essa comissão seja formada por pelo menos um engenheiro e pelo menos um economista?

- (A) $\frac{97}{210}$
- (B) $\frac{97}{105}$
- (C) $\frac{1}{2}$
- (D) $\frac{1}{210}$
- (E) $\frac{13}{14}$

Questão 26. Uma agência de fomento utiliza um sistema lógico para decidir o status de projetos, com base na seguinte proposição:

$$(A \rightarrow B) \wedge (\neg B \rightarrow C) \wedge (A \vee C)$$

Considerando a construção da tabela verdade dessa proposição, é CORRETO afirmar que ela será falsa quando:

- (A) A for verdadeira, B for verdadeira e C for falsa.
- (B) A for verdadeira, B for falsa e C for falsa.
- (C) A for falsa, B for falsa e C for verdadeira.
- (D) A for falsa, B for verdadeira e C for falsa.
- (E) A for verdadeira, B for falsa e C for verdadeira.

Questão 27. Em certo estudo sobre instituições financeiras, alguns pesquisadores organizaram, por meio de um diagrama lógico, três conjuntos de entidades, sendo:

- Conjunto A: Órgãos governamentais.
- Conjunto B: Empresas de economia mista.
- Conjunto C: Agências de fomento.

Quando analisaram o diagrama, verificou-se que:

- Todo elemento de C pertence também a B.
- Alguns elementos de B pertencem a A.
- Nenhum elemento de A está totalmente contido em C.

Com base nessas relações lógicas entre os conjuntos, a classificação CORRETA para uma instituição que é empresa de economia mista e atua como agência de fomento, sem ser órgão governamental direto, será:

- (A) Pertence apenas ao conjunto A.
- (B) Pertence simultaneamente aos conjuntos A, B e C.
- (C) Pertence aos conjuntos B e C, mas não necessariamente ao conjunto A.
- (D) Pertence apenas ao conjunto C.
- (E) Pertence aos conjuntos A e C, mas não ao conjunto B.

Questão 28. Numa instituição pública, os projetos de fomento a aprendizagem de estudantes da Educação Básica aparecem no sistema da instituição sendo divididos nas seguintes condições:

- Projetos aprovados com financiamento (120 unidades).
- Projetos aprovados (180 unidades).
- Projetos aprovados (30 unidades) em reestruturação.
- Projetos em reestruturação para aprovação futura (80 unidades).
- Projetos recusados (40 unidades).

A partir das condições, é possível afirmar, CORRETAMENTE, que o total de projetos que estão no sistema da instituição é de:

- (A) 300, considerando que os projetos aprovados englobam aqueles com financiamento e os em reestruturação, sendo somados apenas os conjuntos disjuntos restantes.
- (B) 420, ao somar todos os conjuntos apresentados, admitindo que não há interseção entre projetos aprovados, em reestruturação e recusados.
- (C) 260, ao excluir os projetos aprovados em reestruturação do total de aprovados e somar apenas os projetos não sobrepostos.
- (D) 340, considerando que os projetos aprovados em reestruturação devem ser contabilizados separadamente dos aprovados com financiamento.
- (E) 220, ao considerar exclusivamente os projetos aprovados e em reestruturação, desconsiderando os recusados por não integrarem o ciclo ativo.

Questão 29. Ao longo de uma análise sobre padrões utilizados por uma agência de fomento para codificação interna de projetos culturais desenvolvidos em uma universidade, verificou-se que adotaram um padrão lógico em uma sequência em que cada letra representa um número conforme sua posição no alfabeto de 26 letras, o que é representado a seguir:

A – C – F – J – O

Considerando o padrão de formação da sequência, o próximo projeto após **O** será representado, CORRETAMENTE, pela letra:

- (A) R.
- (B) S.
- (C) T.
- (D) U.
- (E) V.

Questão 30. Uma agência de fomento estabeleceu alguns títulos para projetos internos em análise receberem financiamento. Um dos títulos adotados no sistema da agência diz o seguinte:

Se um projeto é aprovado, então recebe financiamento. Caso não tenha recebido financiamento, é porque não foi aprovado ou precisa de reformulação.

Analisando o título acima, pode-se dizer que os conectivos lógicos abordados são:

- (A) Se A, então B. Não B implica em não A ou C.
- (B) Não A então B. B implica em não A ou B.
- (C) Se A, então B. Não B implica em não A ou B.
- (D) A implica B. Não A implica em não B ou C.
- (E) A implica B, B implica A ou C.

UTILIZE ESTE ESPAÇO PARA CÁLCULOS

UTILIZE ESTE ESPAÇO PARA CÁLCULOS

CONHECIMENTOS ESPECÍFICOS

Questão 31. Sobre segurança da informação, analise a situação a seguir:

O setor de segurança da informação de um órgão registrou uma ocorrência em que servidores receberam um e-mail aparentemente enviado pela área de TI, solicitando que acessassem um link para atualizar suas credenciais no sistema corporativo. A página aberta pelo link era visualmente idêntica ao portal legítimo da organização, mas estava hospedada em um domínio falso criado para capturar os dados inseridos pelos usuários.

Considerando o caso acima, assinale a alternativa que identifica CORRETAMENTE o tipo de golpe descrito.

- (A) Pharming, que redireciona o usuário a um site falso por meio de envenenamento de cache DNS ou modificação do arquivo hosts, sem que a vítima precise interagir com um link malicioso.
- (B) Phishing, que utiliza mensagens fraudulentas para induzir a vítima a clicar em um link e fornecer dados pessoais ou credenciais em uma página falsa que imita um serviço legítimo.
- (C) Spam, que consiste no envio em massa de mensagens não solicitadas com finalidade publicitária ou maliciosa, sem o objetivo específico de capturar credenciais por meio de páginas falsas.
- (D) Defacement, que consiste na modificação não autorizada do conteúdo de páginas web hospedadas em servidores vulneráveis, geralmente com fins de protesto ou demonstração de comprometimento.
- (E) Man-in-the-Middle, que intercepta ativamente a comunicação entre dois hosts para ler, modificar ou injetar dados no fluxo sem o conhecimento das partes envolvidas.

Questão 32. A segurança da informação é sustentada por um conjunto de propriedades fundamentais que orientam a proteção dos ativos de uma organização. Sobre essas propriedades, assinale a alternativa INCORRETA.

- (A) A confidencialidade garante que a informação seja acessível apenas por pessoas, entidades ou processos devidamente autorizados, protegendo seu conteúdo contra divulgação não autorizada.
- (B) A integridade assegura que a informação não seja alterada ou destruída de maneira não autorizada, preservando sua exatidão e completude ao longo de todo o seu ciclo de vida.
- (C) A disponibilidade determina que a informação e os recursos associados estejam acessíveis e utilizáveis sob demanda por entidades autorizadas, no momento em que forem necessários.
- (D) A irretratabilidade (não repúdio) garante que o emissor de uma mensagem não possa negar sua autoria, sendo obtida tipicamente por meio de assinaturas digitais baseadas em criptografia simétrica.
- (E) A autenticidade assegura que uma entidade é de fato quem afirma ser, sendo um requisito essencial para o estabelecimento de comunicações seguras e para o controle de acesso baseado em identidade.

Questão 33. O Analista de Sistemas de uma organização precisa dimensionar o armazenamento de um servidor de arquivos crítico. Ele dispõe de 5 discos de 1 TB cada e optou pela implementação de RAID 5. Diante disso, assinale a alternativa que descreve CORRETAMENTE as características desse array.

- (A) Capacidade utilizável de 5 TB; o array tolera a falha simultânea de até 2 discos sem perda de dados, pois a paridade distribuída entre todos os discos permite reconstruir o conteúdo de qualquer par de discos perdidos.
- (B) Capacidade utilizável de 4 TB; o array tolera a falha de 1 disco; durante a reconstrução após a troca do disco falho, o array opera em modo degradado e uma segunda falha de disco, nesse período, causa perda total dos dados, pois não há paridade suficiente para recuperação.
- (C) Capacidade utilizável de 3 TB; o array tolera a falha de até 2 discos simultaneamente, pois mantém dois blocos de paridade por faixa distribuídos entre os discos restantes, característica que o distingue do RAID 6.
- (D) Capacidade utilizável de 4 TB; após a falha e substituição de um disco, o processo de reconstrução é imediato e não impõe carga adicional de leitura nos discos remanescentes, pois os dados de paridade são recalculados exclusivamente com base no disco substituído.
- (E) Capacidade utilizável de 4 TB; caso um segundo disco falhe durante a reconstrução do primeiro, o array continua operando em modo degradado com redundância reduzida, aguardando a substituição dos dois discos para recuperação completa.

Questão 34. Em sistemas GNU/Linux, o gerenciamento de propriedade de arquivos e diretórios é uma das responsabilidades centrais do administrador de sistemas, sendo essencial para garantir o controle de acesso adequado aos recursos. Comandos dedicados permitem alterar o usuário proprietário e o grupo associado a um arquivo de forma individual ou combinada. Durante a administração de um servidor Linux, um Analista de Sistemas precisa transferir a propriedade do arquivo *relatorio.txt* para o usuário *auditoria* e ao grupo *seguranca* simultaneamente, utilizando um único comando. Diante disso, assinale a alternativa que apresenta o comando CORRETO para realizar essa alteração de propriedade.

- (A) `chown auditoria relatorio.txt`
- (B) `chmod auditoria:seguranca relatorio.txt`
- (C) `chown auditoria:seguranca relatorio.txt`
- (D) `chgrp auditoria:seguranca relatorio.txt`
- (E) `chown -R auditoria:seguranca relatorio.txt`

Questão 35. Durante uma auditoria de segurança em um servidor Linux, uma Analista executou o seguinte comando para investigar possíveis alterações não autorizadas em arquivos de configuração do sistema: `find /etc -mtime -1 -type f`. Diante desse caso, assinale a alternativa que apresenta a descrição CORRETA do que esse comando realiza.

- (A) Localiza todos os arquivos regulares em `/etc`, cuja data de criação ocorreu nas últimas 24 horas.
- (B) Localiza todos os arquivos regulares em `/etc`, cujo tempo de alteração de metadados do inode ocorreu nas últimas 24 horas.
- (C) Localiza todos os arquivos regulares em `/etc`, cujo conteúdo foi modificado nas últimas 24 horas.
- (D) Localiza todos os arquivos regulares em `/etc`, cujo conteúdo foi modificado nos últimos 60 minutos.
- (E) Localiza todos os arquivos regulares em `/etc`, cuja data de modificação é mais recente que 1 ano.

Questão 36. O setor de segurança de informação recebeu um alerta sobre um possível acesso não autorizado ao servidor Linux. Para investigar o incidente, o Analista precisa exibir o histórico de logins bem-sucedidos realizados no sistema, incluindo o nome do usuário, o terminal utilizado, o endereço IP de origem e os horários de início e encerramento de cada sessão, com base nos registros armazenados no arquivo `/var/log/wtmp`. Diante disso, assinale a alternativa que apresenta o comando CORRETO para obter essas informações.

- (A) `last`
- (B) `id`
- (C) `who`
- (D) `wwho`
- (E) `lastb`

Questão 37. A Zona Desmilitarizada (DMZ) é um conceito amplamente adotado na arquitetura de segurança de redes corporativas para proteger a rede interna de acessos externos indevidos. Sobre a Zona Desmilitarizada (DMZ), assinale a alternativa CORRETA.

- (A) A DMZ elimina a necessidade de firewall ao criar uma rede completamente isolada, em que nenhum pacote externo pode alcançar os servidores hospedados na zona sem autenticação prévia.
- (B) A DMZ é implementada por meio de tunelamento criptografado entre a rede interna e a internet, protegendo os dados transmitidos pelos servidores expostos ao tráfego externo.
- (C) A DMZ permite comunicação irrestrita entre os servidores da zona e a rede interna da organização, concentrando os controles de segurança apenas na fronteira com a internet.
- (D) A DMZ é um segmento de rede posicionado entre a rede interna e a internet, que hospeda servidores acessíveis externamente enquanto isola a rede interna de acessos diretos provenientes desses servidores.
- (E) A DMZ é uma política de controle de acesso aplicada a um único firewall que filtra o tráfego de entrada com base em listas de endereços IP bloqueados.

Questão 38. A equipe de segurança de um órgão federal está avaliando a implementação de uma solução de acesso remoto para servidores em teletrabalho. Após análise técnica, o Analista de Sistemas recomendou o uso de VPN com protocolo IPSec. Durante a revisão, surgiram dúvidas sobre as características da tecnologia. Diante disso, analise as afirmativas a seguir:

- I. A VPN utiliza encapsulamento para transportar pacotes da rede privada dentro de pacotes da rede pública, criando um túnel virtual que isola logicamente o tráfego corporativo dos demais usuários da internet.
- II. No modo de tunelamento completo (full tunnel), todo o tráfego do dispositivo remoto é roteado pela VPN, enquanto no split tunneling apenas o tráfego destinado à rede corporativa passa pelo túnel, e o restante segue diretamente para a internet.
- III. O protocolo IPSec opera na camada de aplicação do modelo OSI, sendo incompatível com soluções de VPN que necessitem de encapsulamento em camadas inferiores, como a camada de rede.
- IV. A VPN, por si só, garante a disponibilidade dos servidores internos, eliminando a necessidade de redundância de links e mecanismos de failover na infraestrutura da organização.

Está(ão) CORRETA(S):

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

Questão 39. Durante uma análise de incidentes, o time de resposta a segurança identificou que um atacante externo estava falsificando o endereço IP de origem dos pacotes enviados à rede da organização, fazendo com que o tráfego malicioso aparentasse ser originado por um servidor interno confiável e, assim, contornasse as regras do firewall. Nesse caso, assinale a alternativa que identifica CORRETAMENTE o tipo de ataque descrito.

- (A) Sniffing, que consiste na captura e monitoramento passivo dos pacotes que trafegam na rede com o objetivo de interceptar informações, incluindo endereços IP e dados transmitidos, sem interferir no tráfego.
- (B) Man-in-the-Middle, que consiste na interceptação ativa da comunicação entre dois hosts, permitindo ao atacante visualizar e manipular os endereços IP de origem e destino dos pacotes para ler, modificar ou injetar dados no fluxo sem o conhecimento das partes.
- (C) Defacement, que consiste na alteração não autorizada do conteúdo de páginas ou aplicações web após o atacante identificar o endereço IP do servidor-alvo, geralmente com fins de protesto ou demonstração de comprometimento do servidor.
- (D) Spoofing, que consiste na falsificação do endereço IP de origem dos pacotes para que o tráfego aparente ser proveniente de um host legítimo ou confiável da rede.
- (E) Força bruta, que consiste em tentativas automáticas e sistemáticas direcionadas a um endereço IP específico para descobrir credenciais por meio de teste exaustivo de combinações de usuário e senha.

Questão 40. O algoritmo MD5 (*Message Digest 5*) é amplamente referenciado em contextos de segurança da informação tanto por suas aplicações práticas quanto por suas limitações conhecidas. Diante disso, analise as afirmativas a seguir sobre as características e usos do MD5:

- I. O MD5 é um algoritmo de hash que produz um resumo de 128 bits a partir de uma entrada de tamanho arbitrário, podendo ser utilizado para verificar a integridade de arquivos transmitidos ou armazenados.
- II. O MD5 é um algoritmo de criptografia simétrica, e o resumo por ele gerado pode ser revertido ao conteúdo original por meio da chave utilizada durante o processamento.
- III. O MD5 é considerado seguro para uso em assinaturas digitais e autenticação em sistemas modernos, pois não apresenta vulnerabilidades de colisão documentadas.
- IV. Qualquer alteração no conteúdo de um arquivo, por menor que seja, resulta em um hash MD5 completamente diferente, propriedade conhecida como efeito avalanche.

Está(ão) CORRETA(S):

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

Questão 41. A equipe de resposta a incidentes de um órgão identificou diferentes amostras de malware durante uma análise forense. Para classificar corretamente cada ameaça e adotar as contramedidas adequadas, o Analista precisou aprofundar seu conhecimento sobre as características e o funcionamento dos vírus de computador. Diante desse caso, analise as afirmativas a seguir:

- I. O vírus polimórfico mantém o corpo do código malicioso cifrado e altera apenas a rotina de decifragem a cada nova infecção, dificultando a detecção por antivírus baseados em assinatura estática; já o vírus metamórfico vai além: reescreve completamente seu próprio código a cada ciclo de replicação, sem depender de cifragem, tornando sua detecção ainda mais complexa.
- II. Vírus residentes em memória carregam-se na RAM durante a execução do arquivo hospedeiro e permanecem ativos para infectar outros arquivos à medida que são acessados pelo sistema operacional; vírus não residentes, por sua vez, realizam a infecção diretamente no momento da execução do hospedeiro e não mantêm presença persistente na memória.
- III. Vírus de macro infectam documentos que suportam linguagens de script ou automação, como planilhas e processadores de texto, e são ativados quando o documento infectado é aberto; por explorarem a plataforma da aplicação e não o sistema operacional subjacente, podem afetar máquinas independentemente do SO instalado, desde que a aplicação vulnerável esteja presente.
- IV. Diferentemente de um worm, um vírus de computador é capaz de se propagar de forma autônoma pela rede, sem necessidade de arquivo hospedeiro ou interação do usuário, explorando vulnerabilidades em serviços de rede para infectar máquinas remotas diretamente.

Está(ão) CORRETA(S):

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

Questão 42. Um Analista de Sistemas precisa conectar-se remotamente a um servidor Linux cujo endereço IP é 10.0.0.50, utilizando o usuário "admin". Por razões de segurança, o administrador do servidor alterou a porta padrão do SSH para a porta 2222. Com isso, assinale a alternativa que apresenta o comando ssh CORRETO para estabelecer essa conexão.

- (A) ssh admin@10.0.0.50 2222
- (B) ssh 2222 admin@10.0.0.50
- (C) ssh -p 2222 10.0.0.50 admin
- (D) ssh admin@10.0.0.50:2222
- (E) ssh -p 2222 admin@10.0.0.50

Questão 43. Um Analista de Sistemas precisa implementar uma política de backup para os servidores de arquivos do órgão. Durante o planejamento, ele avalia diferentes modalidades de cópia de segurança para equilibrar o tempo de realização do backup, o espaço de armazenamento consumido e o tempo necessário para a recuperação dos dados em caso de incidente. Sobre os tipos de backup, assinale a alternativa CORRETA.

- (A) O backup incremental copia todos os arquivos do sistema, garantindo uma cópia autossuficiente que não depende de backups anteriores.
- (B) O backup completo copia apenas arquivos criados ou modificados desde o último backup completo, reduzindo o espaço de armazenamento.
- (C) O backup incremental copia somente os arquivos alterados ou criados desde o último backup realizado, seja ele completo ou incremental, exigindo, para a restauração completa, o backup completo mais todos os backups incrementais subsequentes.
- (D) O backup completo copia apenas os arquivos modificados desde o último backup incremental, agilizando a restauração.
- (E) Backups incrementais e completos têm o mesmo volume de dados e tempo de restauração, diferindo apenas no formato do arquivo final.

Questão 44. Durante o planejamento de infraestrutura de um novo datacenter, o Analista de Sistemas avaliou diferentes configurações de RAID para os servidores de missão crítica. Sobre as características e aplicações dos níveis de RAID, assinale a alternativa CORRETA.

- (A) O RAID 0 distribui os dados em faixas entre dois ou mais discos sem nenhuma redundância, aumentando o desempenho de leitura e escrita, porém sem qualquer tolerância a falhas; a falha de qualquer disco do array resulta em perda total dos dados armazenados.
- (B) O RAID 1, também denominado espelhamento, armazena os dados de forma idêntica em dois ou mais discos e aproveita integralmente a capacidade total somada de todos os discos do array para armazenamento efetivo, sem desperdício de espaço com redundância.
- (C) O RAID 5 exige no mínimo 4 discos para sua implementação, distribui dois blocos de paridade por faixa entre os discos e suporta a falha simultânea de até 2 discos sem perda de dados, o que o torna superior ao RAID 6 em termos de tolerância a falhas.
- (D) O RAID 10 combina espelhamento e distribuição em faixas, requer, no mínimo, 2 discos e garante que nenhuma combinação de falhas simultâneas de disco, independentemente da quantidade, resultará em perda de dados enquanto houver ao menos um disco funcional no array.
- (E) O RAID 6 difere do RAID 5 exclusivamente pelo número mínimo de discos requeridos para implementação, sendo idêntico em todas as demais características, incluindo o número de falhas de disco simultâneas que cada nível suporta sem perda de dados.

Questão 45. A estratégia de defesa em profundidade prevê a adoção de múltiplas camadas de controle de segurança, combinando ferramentas preventivas, detectivas e reativas para proteger a infraestrutura de uma organização contra ameaças internas e externas. Entre os mecanismos disponíveis, alguns são projetados especificamente para atrair, identificar e estudar o comportamento de atacantes em ambiente controlado. Durante a elaboração do plano de segurança da informação, a equipe técnica listou diferentes ferramentas e mecanismos para compor a estratégia de defesa em profundidade da organização. Sobre o conceito de honeypot, assinale a alternativa CORRETA.

- (A) Honeypot é um sistema de detecção de intrusão baseado em assinatura que compara padrões de tráfego com uma base de ataques conhecidos.
- (B) Honeypot é um dispositivo de rede em série que atua como substituto do firewall para bloquear ativamente conexões maliciosas.
- (C) Honeypot é um recurso de segurança deliberadamente configurado para parecer atrativo a atacantes simulando sistemas, serviços ou dados vulneráveis, com o objetivo de detectar, registrar e analisar tentativas de intrusão sem comprometer a infraestrutura real da organização.
- (D) Honeypot é uma técnica de criptografia aplicada a servidores críticos para proteger informações em caso de roubo físico do equipamento.
- (E) Honeypot é um mecanismo de redundância que mantém cópias espelhadas de dados para mitigar ataques de negação de serviço.

Questão 46. Durante uma conexão HTTPS entre o navegador de um usuário e o portal do órgão, ocorre internamente um processo de negociação criptográfica. O servidor envia seu certificado digital, o cliente verifica sua autenticidade e ambos negociam uma chave de sessão que será utilizada para cifrar os dados transmitidos durante a comunicação. Sobre os sistemas criptográficos envolvidos nesse processo, assinale a alternativa CORRETA.

- (A) Todo o processo HTTPS utiliza exclusivamente criptografia simétrica, como o AES, para proteger a troca de chaves e a sessão.
- (B) O certificado digital e a negociação inicial da conexão utilizam criptografia de chave pública (assimétrica), enquanto os dados efetivos da sessão são cifrados com uma chave de sessão simétrica negociada durante o handshake, caracterizando um modelo híbrido.
- (C) A criptografia assimétrica é mais eficiente para cifrar grandes dados, sendo usada tanto na troca de chaves quanto na sessão HTTPS.
- (D) Na criptografia simétrica, cada participante utiliza um par de chaves pública e privada para realizar a comunicação.
- (E) A vantagem da criptografia simétrica é a sua facilidade de distribuição segura de chaves em redes abertas, sem trocas prévias.

Questão 47. Na estrutura da ISO 27001:2022, as cláusulas principais organizam o Sistema de Gestão de Segurança da Informação (SGSI) em etapas que abrangem desde o entendimento do contexto organizacional até a melhoria contínua dos processos. Considerando isso, assinale a alternativa que apresenta CORRETAMENTE a sequência das cláusulas principais da norma e o foco de cada uma delas.

- (A) Contexto, Liderança, Planejamento, Suporte, Operação, Avaliação de desempenho, Melhoria; respectivamente: escopo, direção e responsabilidades, riscos, recursos, execução, monitoramento, melhoria contínua.
- (B) Liderança, Contexto, Suporte, Planejamento, Operação, Melhoria, Avaliação de desempenho; respectivamente: direção e responsabilidades, escopo, recursos, riscos, execução, melhoria contínua, monitoramento.
- (C) Contexto, Suporte, Planejamento, Liderança, Operação, Avaliação de desempenho, Melhoria; respectivamente: escopo, recursos, riscos, direção e responsabilidades, execução, monitoramento, melhoria contínua.
- (D) Planejamento, Contexto, Liderança, Suporte, Operação, Avaliação de desempenho, Melhoria; respectivamente: riscos, escopo, direção e responsabilidades, recursos, execução, monitoramento, melhoria contínua.
- (E) Contexto, Liderança, Suporte, Operação, Planejamento, Avaliação de desempenho, Melhoria; respectivamente: escopo, direção e responsabilidades, recursos, execução, riscos, monitoramento, melhoria contínua.

Questão 48. O setor de segurança da informação de um órgão emitiu um alerta interno sobre uma categoria de malware que tem causado impactos severos em instituições públicas e privadas ao redor do mundo. Diante disso, assinale a alternativa que apresenta uma afirmação INCORRETA sobre ransomware.

- (A) Ransomware cifra arquivos e exige resgate em criptomoedas, dificultando o rastreamento via blockchain.
- (B) Variantes modernas adotam "dupla extorsão": cifram os dados e ameaçam vazá-los se o resgate não for pago.
- (C) O pagamento do resgate, quando efetuado dentro do prazo estipulado pelos atacantes, assegura tecnicamente a recuperação integral dos arquivos cifrados, uma vez que os grupos criminosos dependem de sua reputação para manter a credibilidade de seus esquemas.
- (D) Manter backups off-line e atualizados é a principal medida de mitigação, permitindo restaurar dados sem o pagamento.
- (E) Ransomwares propagam-se por e-mails de phishing, exploração de vulnerabilidades e movimentos laterais na rede.

Questão 49. A criptografia é um dos pilares da segurança da informação, e a escolha adequada dos algoritmos criptográficos impacta diretamente a confidencialidade e a integridade dos dados. Os algoritmos criptográficos são classificados em categorias distintas, como simétricos e assimétricos, e cada categoria possui características, níveis de segurança e casos de uso específicos. Diante disso, um Analista de Sistemas está revisando a política criptográfica da instituição e identificou o uso dos algoritmos RSA e DES em sistemas legados e em comunicações seguras. Sobre esses algoritmos, assinale a alternativa CORRETA.

- (A) O DES é um algoritmo de criptografia assimétrica de 56 bits usado em certificados digitais e na troca segura de chaves na internet.
- (B) O RSA é um algoritmo simétrico baseado na fatoração de números primos, ideal para cifrar grandes volumes de dados rapidamente.
- (C) O DES é um algoritmo de criptografia simétrica com chave de 56 bits que, devido ao tamanho reduzido de sua chave, é considerado inseguro para uso em sistemas modernos, tendo sido sucedido pelo 3DES e posteriormente pelo AES como padrões criptográficos recomendados.
- (D) O RSA e o DES são algoritmos simétricos que diferem apenas no tamanho e no método de geração de suas chaves.
- (E) O RSA é um algoritmo de bloco que cifra dados em segmentos de 64 bits, enquanto o DES utiliza curvas elípticas para gerar chaves.

Questão 50. No contexto da segurança da informação, os sistemas computacionais de um órgão público utilizam diferentes mecanismos para verificar a identidade dos usuários antes de conceder acesso a recursos protegidos. Uma Analista foi designada para elaborar uma política de autenticação que estabeleça o uso de múltiplos fatores de verificação. Sobre os mecanismos de autenticação e controle de acesso, analise as afirmativas a seguir:

- I. A autenticação por biometria é classificada como fator "algo que você é", pois utiliza características físicas ou comportamentais únicas do indivíduo, como impressão digital, íris ou reconhecimento facial.
- II. Um token de hardware, como um dispositivo OTP (*One-Time Password*), é classificado como fator "algo que você tem", pois gera códigos temporários vinculados a um dispositivo físico de posse do usuário.
- III. Uma senha considerada forte é aquela composta exclusivamente por letras maiúsculas e minúsculas, sem necessidade de inclusão de números ou caracteres especiais, desde que contenha no mínimo oito caracteres.
- IV. O uso combinado de dois ou mais fatores de autenticação distintos é denominado autenticação multifator (MFA) e aumenta significativamente a segurança do controle de acesso em comparação ao uso de fator único.

Estão CORRETAS:

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

Questão 51. Durante uma auditoria de segurança, o Analista de Sistemas identificou que alguns servidores tentaram executar softwares não autorizados nas estações de trabalho utilizadas para manipulação de dados financeiros e informações estratégicas. Essa prática representa risco de instalação de malwares, vazamento de informações sigilosas e comprometimento de sistemas críticos. Considerando as boas práticas da ISO/IEC 27002, qual medida seria a MAIS ADEQUADA para impedir que programas não autorizados sejam executados nesse ambiente?

- (A) Wireless.
- (B) Sniffer.
- (C) Logging.
- (D) Sign On.
- (E) Whitelisting.

Questão 52. Um órgão governamental que gerencia dados financeiros sensíveis precisa implementar um sistema de comunicação seguro entre suas agências distribuídas geograficamente. O objetivo é garantir que apenas o destinatário previsto consiga decifrar as mensagens enviadas, sem a necessidade de compartilhar previamente uma chave secreta entre remetente e destinatário. Considerando as características de criptografia, qual algoritmo seria o MAIS ADEQUADO para atender a essa necessidade?

- (A) RSA (Rivest-Shamir-Adleman).
- (B) AES (Advanced Encryption Standard).
- (C) DES (Data Encryption Standard).
- (D) 3DES (Triple DES).
- (E) RC6 (Rivest Cipher 6).

Questão 53. O IDS (*Intrusion Detection System*) é um sistema de segurança utilizado para monitorar atividades suspeitas ou maliciosas em ambientes computacionais, permitindo identificar possíveis tentativas de invasão, exploração de vulnerabilidades ou comportamentos anômalos. Esses sistemas podem analisar eventos em hosts individuais ou no tráfego de rede, gerando alertas para que administradores de segurança possam tomar medidas preventivas ou corretivas. Considerando os diferentes tipos de IDS, existe uma categoria específica projetada para monitorar o tráfego da rede, analisando pacotes que circulam pelos segmentos de comunicação a fim de identificar padrões de ataques ou comportamentos suspeitos. Assim, qual é o tipo de IDS responsável por realizar esse monitoramento em nível de rede?

- (A) HIDS (Host-based Intrusion Detection System).
- (B) APIDS (Application Protocol-based Intrusion Detection System).
- (C) DIDS (Distributed Intrusion Detection System).
- (D) NIDS (Network Intrusion Detection System).
- (E) PIDS (Protocol-based Intrusion Detection System).

Questão 54. Durante uma investigação de segurança, o Analista de Sistemas detectou que algumas estações de trabalho estavam registrando silenciosamente todas as teclas digitadas pelos usuários, incluindo senhas de sistemas internos e dados de formulários financeiros. Esse comportamento não autorizado representa risco de vazamento de informações sensíveis e comprometimento da segurança dos sistemas. Considerando os tipos de malwares, qual seria o MAIS PROVÁVEL responsável por essa atividade?

- (A) Backdoor.
- (B) Trojan.
- (C) Keylogger.
- (D) Ransomware.
- (E) Adware.

Questão 55. O backup, ou cópia de segurança, é uma prática essencial de segurança da informação que consiste em criar cópias de arquivos e dados para garantir sua disponibilidade e integridade em caso de falhas, perdas acidentais ou ataques cibernéticos. Sabendo disso, analise as assertivas abaixo e julgue-as em Verdadeiras (V) ou Falsas (F):

- () O backup frio é feito com o sistema desligado ou em modo offline.
- () O backup completo copia todos os arquivos e pastas selecionados no momento da execução.
- () O backup incremental copia apenas os arquivos que foram alterados ou criados desde o último backup diferencial.
- () O backup quente é feito enquanto o sistema está em operação.

Qual alternativa preenche, CORRETAMENTE, de cima para baixo, os parênteses acima?

- (A) V – V – V – F.
- (B) V – F – V – F.
- (C) F – V – V – V.
- (D) V – V – F – V.
- (E) F – F – F – V.

Questão 56. Durante a manutenção da infraestrutura de TI (Tecnologia da Informação) do Badesul, o Analista de Sistemas percebeu que algumas estações de trabalho estavam suscetíveis à instalação de malwares e arquivos infectados provenientes de anexos de e-mails e downloads de sites não confiáveis. Para proteger o ambiente e garantir a integridade dos sistemas, é necessário instalar um software específico de proteção contra vírus e ameaças cibernéticas. Qual das alternativas abaixo atende a essa necessidade?

- (A) Kaspersky.
- (B) Zoom.
- (C) Slack.
- (D) Spotify.
- (E) AutoCAD.

Questão 57. Durante a implementação de um sistema de gestão financeira em uma organização, o Analista de Sistemas precisa garantir que todas as transações eletrônicas e assinaturas de contratos sejam auditáveis e que os usuários não possam negar ter realizado determinadas ações. Para isso, são utilizadas técnicas como assinatura digital e registro de logs de transações financeiras, garantindo que cada operação seja rastreável e verificável. Considerando os princípios de segurança da informação, qual característica é MAIS diretamente atendida por essas medidas?

- (A) Confidencialidade.
- (B) Não-Repúdio.
- (C) Integridade.
- (D) Autenticidade.
- (E) Disponibilidade.

Questão 58. O NAT (*Network Address Translation*) é uma técnica utilizada em redes de computadores para traduzir endereços IP (*Internet Protocol*) privados em endereços IP públicos, permitindo que dispositivos em redes internas acessem redes externas, como a Internet. Existem diferentes tipos de NAT, como estático, dinâmico, NAT Overload (PAT) e Twice NAT, cada um com características específicas de mapeamento de endereços e portas. Com base nesses conceitos, analise as assertivas abaixo e julgue-as em Verdadeiras (V) ou Falsas (F):

- () No tipo de NAT dinâmico, é mapeado um endereço IP privado específico para um endereço IP público específico. É o chamado mapeamento um-para-um permanente.
- () No tipo de NAT estático, são mapeados endereços IP privados para endereços IP públicos de um pool disponível. É o chamado mapeamento um-para-um temporário.
- () No tipo de NAT Overloading (*PAT – Port Address Translation*) são mapeados múltiplos endereços IP privados para um único endereço IP público. Também são usados números de porta para distinguir conexões diferentes.
- () No tipo de Twice NAT (Double NAT), o NAT é aplicado duas vezes na mesma comunicação. É comum em cenários com múltiplos roteadores NAT em série.

Qual alternativa preenche, CORRETAMENTE, de cima para baixo, os parênteses acima?

- (A) V – F – V – F.
- (B) F – V – V – F.
- (C) F – F – V – V.
- (D) V – V – F – V.
- (E) F – V – F – V.

Questão 59. Durante a análise de segurança de uma rede do Badesul, o Analista implementou um sistema que simula vulnerabilidades reais, atraindo possíveis invasores e malwares. Esse sistema permite registrar atividades suspeitas e estudar técnicas de ataque sem colocar em risco os sistemas críticos da organização. Considerando as boas práticas de defesa cibernética, qual ferramenta ou técnica está sendo utilizada nesse caso?

- (A) Firewall.
- (B) IDS (Intrusion Detection System).
- (C) Honeypot.
- (D) VPN (Virtual Private Network).
- (E) Antivírus.

Questão 60. Em uma agência governamental, o setor de TI (Tecnologia da Informação) implementou medidas adicionais de autenticação para acessar sistemas críticos. Entre essas medidas, foi adotado um dispositivo ou aplicativo que gera códigos temporários, usados em conjunto com a senha do usuário para permitir o acesso seguro aos sistemas. Considerando os métodos de autorização para acesso, qual é a solução utilizada nesse caso?

- (A) Smartcard.
- (B) RFID.
- (C) Biometria.
- (D) Senha fraca.
- (E) Token.

Questão 61. O RAID (*Redundant Array of Independent Disks*) é uma tecnologia utilizada para combinar múltiplos discos físicos em um único sistema lógico, com o objetivo de melhorar o desempenho, aumentar a capacidade de armazenamento ou oferecer tolerância a falhas, dependendo do nível utilizado. Cada nível de RAID possui características específicas relacionadas ao uso de redundância, paridade ou distribuição de dados entre os discos. Considerando os diferentes níveis de RAID, assinale a alternativa que apresenta uma característica do RAID 0.

- (A) Redundante via código de Hamming.
- (B) Não redundante.
- (C) Paridade de bit intercalada.
- (D) Paridade de bloco intercalada.
- (E) Paridade de bloco dual distribuída e intercalada.

Questão 62. Durante a implantação de um novo servidor de arquivos em uma agência, o Analista precisa escolher um sistema de arquivos que ofereça maior confiabilidade na gravação de dados. Uma das exigências do projeto é o uso da técnica de journaling, que registra previamente as alterações no sistema de arquivos em um log (journal), permitindo a recuperação mais rápida e consistente dos dados em caso de falhas ou desligamentos inesperados. Considerando os sistemas de arquivos disponíveis, qual das alternativas abaixo atende a esse requisito?

- (A) FAT12
- (B) FAT16
- (C) FAT32
- (D) EXT2
- (E) EXT4

Questão 63. Durante a administração de um servidor que utiliza o sistema operacional GNU/Linux (em português), um Analista de Sistemas precisa verificar o conteúdo de um determinado diretório por meio do terminal. Para isso, ele utiliza o comando ls, responsável por listar os arquivos e diretórios existentes em um diretório específico. Entretanto, ele também precisa visualizar todos os arquivos presentes, incluindo aqueles que são ocultos. Considerando as opções do comando ls, qual parâmetro permite listar todos os arquivos do diretório, inclusive os ocultos?

- (A) -a
- (B) -l
- (C) -h
- (D) -r
- (E) -t

Questão 64. Durante o uso do Windows 11 (em português), muitos usuários utilizam atalhos de teclado para executar tarefas de forma mais rápida, sem a necessidade de navegar pelos menus do sistema. Um exemplo comum é a abertura do Explorador de Arquivos, ferramenta utilizada para visualizar e gerenciar pastas, arquivos e unidades de armazenamento do computador. Considerando os atalhos de teclado do Windows 11, qual combinação de teclas permite abrir diretamente o Explorador de Arquivos?

- (A) Tecla do Logotipo do Windows + D
- (B) Tecla do Logotipo do Windows + R
- (C) Tecla do Logotipo do Windows + L
- (D) Tecla do Logotipo do Windows + E
- (E) Tecla do Logotipo do Windows + I

Questão 65. As tecnologias de virtualização de plataformas permitem que múltiplos sistemas operacionais sejam executados em um mesmo hardware físico, utilizando recursos computacionais de forma mais eficiente. Nesse contexto, podem ser utilizados emuladores, máquinas virtuais e outras técnicas de virtualização, possibilitando a criação de ambientes isolados para execução de diferentes sistemas ou aplicações. Para que isso seja possível, existe um software específico responsável por criar, gerenciar e controlar as máquinas virtuais, além de realizar a mediação entre o hardware físico e os sistemas operacionais convidados. Considerando esse contexto, qual é o software responsável por criar e gerenciar máquinas virtuais em um ambiente de virtualização?

- (A) Container.
- (B) Emulador.
- (C) Hypervisor.
- (D) Snapshot.
- (E) Kernel.

Questão 66. Na Gerência de Processos dos sistemas operacionais, diferentes algoritmos de escalonamento são utilizados para definir qual processo deve utilizar a CPU e por quanto tempo. Entre os mais conhecidos estão SRTF, SJF, FCFS e Round Robin, cada um com características próprias quanto à preempção e ao critério de seleção dos processos. Com base nesses conceitos, analise as assertivas abaixo e julgue-as em Verdadeiras (V) ou Falsas (F):

- () SRTF (*Shortest Remaining Time First*) é um algoritmo não preemptivo que sempre executa o processo com menor tempo restante de execução. Se um processo mais curto chegar, ele interrompe o processo atual.
- () SJF (*Shortest Job First*) é um algoritmo preemptivo que executa primeiro o processo com menor tempo de execução.
- () FCFS (*First Come, First Served*) executa os processos na ordem em que chegam à fila de prontos. Os processos ficam organizados em uma fila FIFO (*First In, First Out*).
- () Round Robin (RR) é um algoritmo preemptivo que divide a CPU entre os processos usando um quantum de tempo. Cada processo executa por um tempo fixo e, caso não termine, retorna para o final da fila.

Qual alternativa preenche, CORRETAMENTE, de cima para baixo, os parênteses acima?

- (A) V – F – V – F.
- (B) F – F – V – V.
- (C) V – V – F – V.
- (D) F – V – V – F.
- (E) V – F – F – V.

Questão 67. No contexto da segurança da informação, existem diversos tipos de ataques e técnicas relacionadas à análise e exploração de redes, como DoS (*Denial of Service*), DDoS (*Distributed Denial of Service*), ping da morte, força bruta, defacement, spoofing, Man-in-the-Middle, além de mecanismos de defesa como antivírus, antimalware e honeypot. Algumas dessas técnicas são utilizadas para interceptar ou analisar comunicações que trafegam em uma rede.

Nesse contexto, qual é a técnica utilizada para capturar e analisar o tráfego de dados de uma rede, permitindo visualizar os pacotes transmitidos entre dispositivos?

- (A) Sniffing.
- (B) Spoofing.
- (C) Man-in-the-Middle.
- (D) Defacement.
- (E) Força bruta.

Questão 68. As redes sem fio utilizam diferentes protocolos e mecanismos de segurança para proteger a comunicação entre dispositivos e evitar acessos não autorizados. Entre essas tecnologias estão EAP (*Extensible Authentication Protocol*), WEP (*Wired Equivalent Privacy*), WPA (*Wi-Fi Protected Access*) e WPA2 (*Wi-Fi Protected Access II*), cada uma com características próprias relacionadas à autenticação e à criptografia dos dados transmitidos pela rede. Considerando essas tecnologias de segurança em redes Wi-Fi, o protocolo WEP (*Wired Equivalent Privacy*) utiliza criptografia baseada em qual algoritmo?

- (A) AES (Advanced Encryption Standard).
- (B) DES (Data Encryption Standard).
- (C) RC4 (Rivest Cipher 4).
- (D) RSA (Rivest–Shamir–Adleman).
- (E) SHA-256 (Secure Hash Algorithm 256).

Questão 69. Na Gerência de Memória dos sistemas operacionais, diversas técnicas são utilizadas para organizar o uso da memória principal e permitir que múltiplos processos sejam executados de forma eficiente. Entre essas técnicas estão paginação, segmentação, fragmentação de memória e estratégias de alocação, cada uma com características específicas de organização e gerenciamento. Com base nesses conceitos, analise as assertivas abaixo e julgue-as em Verdadeiras (V) ou Falsas (F):

- () A paginação divide a memória em blocos de tamanho variável. As páginas são blocos do processo, enquanto os quadros (frames) são blocos da memória física.
- () Fragmentação de memória ocorre quando a memória fica dividida em pequenos espaços inutilizáveis.
- () Na alocação de memória, o sistema operacional precisa reservar espaço na memória para os processos. Um dos tipos é a alocação contígua, em que o processo ocupa um único bloco contínuo de memória.
- () Na segmentação, a memória é dividida em segmentos de tamanho fixo. Cada segmento representa uma parte lógica do programa, como código, dados, pilha e funções.

Qual alternativa preenche, CORRETAMENTE, de cima para baixo, os parênteses acima?

- (A) V – F – V – F.
- (B) F – F – V – V.
- (C) V – V – F – V.
- (D) F – V – V – F.
- (E) V – F – F – V.

Questão 70. Na Gerência de Entrada e Saída dos sistemas operacionais, existem técnicas utilizadas para melhorar a organização e o desempenho das operações de comunicação entre os dispositivos de hardware e o sistema. Uma dessas técnicas permite organizar tarefas de entrada e saída em uma fila, possibilitando que diferentes processos enviem solicitações que serão atendidas gradualmente pelo dispositivo responsável. Considerando esse conceito, qual técnica é utilizada para organizar tarefas de entrada e saída em uma fila?

- (A) Spooling.
- (B) Buffering.
- (C) Caching.
- (D) Polling.
- (E) Interrupt.

PROVA DISCURSIVA

Leia o enunciado e responda as questões a seguir, observando-se o mínimo de 05 (cinco) e o máximo de 10 (dez) linhas para cada uma delas, fazendo correto uso do padrão culto da Língua Portuguesa. Não esqueça de transcrever as suas respostas para a **Folha Definitiva da Prova Discursiva**, pois a Folha Rascunho **NÃO** será considerada para correção.

A Agência de Fomento RGS, uma agência de fomento estruturada como sociedade de economia mista, iniciou um projeto de expansão de suas linhas de crédito digital, o que exigiu a integração de seus sistemas com bancos parceiros e a liberação de trabalho remoto para seus Analistas. Uma auditoria recente, baseada nas normas ABNT NBR ISO/IEC 27001:2022 e 27002:2022, revelou possíveis falhas críticas: a defesa de perímetro da instituição baseia-se exclusivamente em um filtro de pacotes *stateless*, com os servidores da aplicação web expostos na mesma rede interna dos bancos de dados. Além disso, os acessos remotos ocorrem sem o uso de túneis criptográficos, e a instituição não possui um plano estruturado de resposta a incidentes para conter possíveis invasões.

À luz da situação hipotética narrada e dos fundamentos da segurança da informação, responda de forma justificada às questões discursivas a seguir:

Questão 01. Explique como a implementação de um *firewall stateful*, a criação de uma DMZ (Zona Desmilitarizada) e a adoção de uma VPN resolvem as vulnerabilidades arquiteturais descritas. Em sua resposta, relacione o uso da VPN a duas propriedades fundamentais da segurança da informação que passarão a ser atendidas.

1	
2	
3	
4	
5	
6	
7	
8	
9	
10	

Questão 02. Considerando as diretrizes de gestão de incidentes de segurança, descreva o objetivo e cite as ações práticas que devem ser adotadas na fase de *contenção* caso ocorra uma invasão na rede da Agência. Justifique como a aplicação prévia do Princípio do Privilégio Mínimo auxilia na mitigação desse ataque.

1	
2	
3	
4	
5	
6	
7	
8	
9	
10	