



CONCURSO PÚBLICO DA EMPRESA DE TECNOLOGIA E
INFORMAÇÕES DA PREVIDÊNCIA
DATAPREV

NÍVEL SUPERIOR – TARDE
**ANALISTA DE TECNOLOGIA DA INFORMAÇÃO
SEGURANÇA CIBERNÉTICA E PROTEÇÃO DE DADOS**

PROVA OBJETIVA - TIPO 2



SUA PROVA

Além deste caderno de questões contendo **70 (setenta)** questões objetivas, você receberá do fiscal de sala o cartão de respostas.

As questões objetivas têm **5 (cinco)** opções de resposta (A, B, C, D e E) e somente uma delas está correta.



TEMPO

- **4 (quatro) horas** é o período disponível para a realização da prova, **já incluído o tempo para a marcação da folha de respostas.**
- **2 (duas) horas** após o início da prova, é possível retirar-se da sala, sem levar o caderno de questões nem qualquer tipo de anotação de suas respostas.
- **30 (trinta) minutos** antes do término do período de prova, é possível retirar-se da sala, **levando o caderno de questões.**



NÃO SERÁ PERMITIDO

- Qualquer tipo de comunicação entre os candidatos durante a aplicação da prova.
- Usar o sanitário ao término da prova, após deixar a sala.
- Anotar informações relativas às respostas em qualquer outro meio que não seja este caderno de questões.



INFORMAÇÕES GERAIS

- Verifique se este caderno de questões está completo e sem falhas de impressão. Caso contrário, **notifique imediatamente o fiscal da sala**, para que sejam tomadas as devidas providências.
- No cartão de respostas confira seus dados pessoais, especialmente nome, número de inscrição e documento de identidade, e leia atentamente as instruções para preenchê-lo.
- **Use somente caneta esferográfica, fabricada em material transparente, com tinta preta ou azul.**
- Assine seu nome apenas no espaço reservado na folha de respostas.
- Confira o tipo do seu caderno de questões. Caso tenha recebido caderno de questões com tipo diferente do impresso em seu cartão de respostas, o fiscal deve ser **obrigatoriamente** informado para o devido registro na ata da sala.
- O preenchimento das respostas é de sua responsabilidade e não será permitida a substituição do cartão de respostas em caso de erro cometido por você.
- Para fins de avaliação, serão levadas em consideração apenas as marcações realizadas no cartão de respostas.
- Os candidatos serão submetidos ao sistema de detecção de metais quando do ingresso e da saída das salas e dos sanitários durante a realização das provas.

Boa prova!

Conhecimentos Gerais

Língua Portuguesa

1

As opções a seguir apresentam frases em que há a repetição de uma mesma palavra.

Assinale aquela em que as palavras mostram sentidos **diferentes**.

- (A) Morrer por uma causa não faz com que essa causa seja justa.
- (B) Para mim, velho é aquele sujeito 15 anos mais velho do que eu.
- (C) Depois dos 70, tudo se resume a remendar, remendar, remendar.
- (D) Fala-se muito em loucuras da juventude; não sei, porém, porque nada se diz das loucuras da velhice.
- (E) Quarenta anos é uma idade terrível. Porque é a idade em que chegamos a ser o que somos.

2

Leia com atenção o texto a seguir.

Processamento de dados é a conversão de dados brutos em informações úteis por meio de etapas estruturadas, como coleta, preparação, análise e armazenamento de dados. As organizações podem ter insights praticáveis e informar a tomada de decisão processando dados de forma eficaz.

Historicamente, as empresas dependiam de processamento de dados e calculadoras para gerenciar conjuntos de dados menores. Como as empresas geravam volumes cada vez maiores de dados, tornaram-se essenciais os métodos avançados de processamento de dados.

KRANTZ, Tom. JONKER, Alexandra. *O que é processamento de dados?* IBM. 2025.

As opções a seguir apresentam observações corretas sobre esse pequeno texto, **à exceção de uma**. Assinale-a.

- (A) O texto se inicia pela definição de “processamento de dados”.
- (B) As duas ocorrências do conectivo “como” possuem o mesmo significado.
- (C) Por meio do processamento de dados, informações úteis resultam da conversão de dados brutos.
- (D) De acordo com o texto, os métodos avançados de processamento são respostas a uma necessidade.
- (E) O advérbio “historicamente” se refere a realidades passadas no terreno do processamento de dados.

3

Leia com atenção o trecho a seguir.

“Se os navios geralmente vão melhor do que os Estados, isso ocorre pela única razão de que naqueles cada um aceita a parte que lhe compete, enquanto nestes, na maioria das vezes, quanto menos se sabe, mais se tem o desejo de comandar.”

Sobre esse trecho, assinale a afirmativa correta.

- (A) A conjunção “Se” inicial indica uma condição.
- (B) O pronome demonstrativo “naqueles” tem como referente os navios.
- (C) O advérbio “geralmente” se opõe semanticamente à expressão “na maioria das vezes”.
- (D) Na comparação entre navios e Estados, o trecho indica a superioridade dos Estados sobre os navios.
- (E) Enquanto o demonstrativo “isso” se refere a algo já dito, o pronome “cada um” se refere a algo futuro do trecho.

4

No texto a seguir, os pronomes demonstrativos sublinhados estão bem empregados.

Se os navios geralmente vão melhor do que os Estados, isso ocorre pela única razão de que naqueles cada um aceita a parte que lhe compete, enquanto nestes, na maioria das vezes, quanto menos se sabe, mais se tem o desejo de comandar.

Assinale a opção que mostra a frase em que o demonstrativo está **erradamente** empregado.

- (A) Esta é a regra de ouro dos governantes: respeitem os votos dos eleitores.
- (B) Antigamente, as leis eram observadas com mais rigor, mas, naqueles tempos tudo era diferente.
- (C) Os advogados devem manter sigilo sobre seus clientes e isso deve ser rigorosamente respeitado.
- (D) Dicionários e enciclopédias fazem parte de boas bibliotecas, mas entre estes e aqueles há diferença de volume.
- (E) Para os que não conseguem governar a própria casa nem os povos, uma boa desculpa é dizer que estes são ingovernáveis.

5

Leia o texto a seguir.

Quem governa uma instituição pública ou privada é sempre objeto do ódio e das queixas dos governados. Os homens estão sempre descontentes porque estão sempre infelizes. Por isso ficam descontentes com o próprio Estado, e também por isso ficam descontentes com quem o governa... Entretanto, no que concerne ao ato de governar, infelizmente existem apenas duas alternativas realmente sensatas: ou abster-se do governo, seja ele público ou privado, ou administrá-lo totalmente em vantagem própria e não dos governados.

Leopardi, Giacomo. Ensaísta italiano.

As opções a seguir apresentam observações de caráter linguístico sobre o texto.

Assinale a única observação **incorreta**.

- (A) Os adjetivos “pública ou privada” são de conteúdo subjetivo, expressando uma opinião do enunciador do texto.
- (B) O segundo período do texto traz uma justificativa para o que é afirmado no período anterior.
- (C) O termo “e também” traz uma redundância, que é normalmente aceita.
- (D) As duas ocorrências de “por isso” mostram o mesmo antecedente.
- (E) O termo “Entretanto” traz o valor de oposição.

6

Os que trabalham em espaços profissionais em que inserem textos devem preocupar-se com a correção gramatical.

Entre as frases a seguir, assinale a que se mostra integralmente correta.

- (A) Vimos hoje aqui depois das aulas.
- (B) Vieram ela e eu para a festa no mesmo táxi.
- (C) Os policiais requisaram nossos documentos.
- (D) Não restou nenhum segredo entre eu e meu advogado.
- (E) As autoridades interviram nos problemas políticos surgidos na semana passada.

7

Assinale a opção que apresenta o único texto coerente.

- (A) Na Europa, nesta época, faz muito frio: vamos comprar roupas mais leves.
- (B) A verdade é que ninguém pretende descobrir nada com essas investigações.
- (C) A despeito dos altos preços dos restaurantes, não comemos fora durante a semana.
- (D) Nessas situações há duas coisas a fazer: dirigir-se imediatamente a uma delegacia.
- (E) Ela não sabia desde que momento de sua vida ela trazia aquela marca de nascença na testa.

8

As frases a seguir mostram um termo sublinhado que se refere a um termo anterior, estabelecendo coesão na frase.

Assinale a opção em que a identificação do antecedente do termo sublinhado está correta.

- (A) A morte é um jeito de a natureza lhe dizer para pegar leve. / a natureza.
- (B) Que apertada é a porta e que estreito o caminho que conduz à vida. / a porta.
- (C) Todo homem deveria ser incendiário até os 25 anos de idade e bombeiro daí em diante. / 25 anos.
- (D) O jovem não raciocina, age; o velho raciocina e põe os outros para agirem em seu lugar. / o jovem.
- (E) Qual pode ser a vida que começa pelos gritos da mãe, que a dá, e os choros do filho que a recebe. / a vida.

ATENÇÃO: O texto a seguir refere-se às duas próximas questões.

Leia o texto abaixo, sobre gestão e governança.

A governança não se confunde com gestão: enquanto a gestão executa atividades e processos, a governança direciona, define políticas, estabelece prioridades e supervisiona resultados, garantindo que os objetivos organizacionais da empresa sejam alcançados de forma ética e eficiente. Ela envolve a definição de responsabilidades, a alocação de recursos e a criação de mecanismos de controle de atividades e monitoramento.

9

Sobre a estruturação desse texto, assinale a afirmativa correta.

- (A) O texto tem a finalidade de definir os dois processos.
- (B) O texto pretende mostrar a superioridade da governança sobre a gestão.
- (C) O texto pretende mostrar objetivamente a diferença entre gestão e governança.
- (D) O texto pode ser definido como argumentativo, pois expõe opiniões do enunciador do texto.
- (E) O texto indica uma série de atividades da governança em ordem cronológica, montando um texto narrativo.

10

Nas opções a seguir, assinale aquela que traz uma função diferente do conectivo de.

- (A) objetivos organizacionais da empresa.
- (B) definição de responsabilidades.
- (C) alocação de recursos.
- (D) criação de mecanismos.
- (E) controle de atividades.

ATENÇÃO: O texto a seguir refere-se às duas próximas questões.

Um Analista de Negócios de TI desempenha um papel crucial em unir a tecnologia e os objetivos empresariais. Este profissional é responsável por garantir que as soluções de TI estejam alinhadas com as necessidades e objetivos empresariais, promovendo assim eficiência e inovação. Dentro da categoria de alinhamento entre TI e negócios, o Analista de Negócios de TI (IT BA) identifica áreas de melhoria, documenta requisitos e garante que as soluções tecnológicas sejam implementadas de forma eficaz para aprimorar os processos estruturais das empresas modernas.

11

Pela sua estrutura, esse pequeno texto deve ser classificado, quanto ao seu tipo, como

- (A) injuntivo.
- (B) informativo.
- (C) descritivo e narrativo.
- (D) descritivo e expositivo.
- (E) argumentativo e expositivo.

12

Entre os adjetivos que aparecem nas opções abaixo, assinale aquele que mostra uma opinião do enunciador, indicando uma qualidade.

- (A) papel crucial.
- (B) objetivos empresariais.
- (C) soluções tecnológicas.
- (D) processos estruturais.
- (E) empresas modernas.

Língua Inglesa

READ TEXT I AND ANSWER NEXT SEVEN QUESTIONS.

TEXT I

AI is getting better at writing. Humans must get better at editing.

Writing is hard. For Franz Kafka, putting words on the page was a process of “unending torments”. George Orwell said it felt like “a long bout of some painful illness”. Hunter S. Thompson, a journalist, saw it as the opposite of sex: “only good when it’s over”. Now AI has come to the rescue. Large language models (LLMs) eagerly offer reams of text without any pain or torment. Bots can spew out emails (excellently), longer prose (passably) and poetry (poorly). To them, writer’s block is a 500-sheet pack of paper: any user of an LLM can produce as many words in a day as Kafka did in his life.

For human writers this is a blessing and a curse. If you claim to be an author but use AI, you look like a fraud—bot-busting tools like Pangram are good at spotting when someone has had an AI helping hand. [...]

If LLMs keep improving, in a few years they could be as good as professional wordsmiths. In the meantime, though, their baggy prose puts a premium on editing skills. After all, even the best writers need a good editor to keep them sharp. Editing is something *The Economist* deals with day in, day out, so here are our tips for rewriting AI prose.

First, commission well. George R.R. Martin once said the job of editors is to “clip the wings” of writers, and “tell them in which direction to fly”. When it comes to LLMs, that means giving clear instructions about exactly what you want, and asking them to refine their output as many times as necessary. You’ll get less pushback from machines than men. Mr Martin said editors were “the writer’s natural enemy”; AI would probably say “great observation!” and “love the enemy analogy!”

Second, pay attention to detail. AI writers will make mistakes and offer phrases that sound good but mean nothing. They like to lavish their prose with Latinate words, talking about the “bi-directional flow” and how to “expedite grid enhancements”; remind them that Anglo-Saxon words are often punchier. They like clichéd metaphors: there are lots of “Achilles’ heels”. And AI tends to use the “rule of three” far more than humans. *The Economist* also likes this rhetorical trick. But whereas we try to group three sensible bits of advice, AI offers such redundant sentences as: “The mystery has been solved—not partially, not ambiguously, but definitively.” Such lines should be cut—definitively.

Finally, know your audience. The editor is an intermediary between writer and reader. LLMs are sycophants and their smarmy tone is often off-key. If you are writing an email to break some bad news to your boss, tell your bot to skip the exclamation marks. AI can be pretentious or pontificating (it was trained on human writing, after all). Most people are short of time, but a verbose AI pins you to the wall like a bore at a party.

“Write drunk, edit sober,” goes the old writers’ maxim. If that’s right, when the AI-human team gets down to work, the AIs will have all the fun.

Adapted from <https://www.economist.com/leaders/2026/07/30/ai-is-getting-better-at-writing-humans-must-get-better-at-editing>

13

Based on Text I, mark the statements below as true (T) or false (F).

- () The first paragraph refers to authors who assert that writing is an easy task.
- () At times, the tone of LLM-generated prose can be rather inappropriate.
- () It is argued that nowadays editing has lost its relevance.

The statements are, respectively,

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

14

In the expression “*bout of some painful illness*” (1st paragraph), “*bout*” can be replaced, without significant change in meaning, by

- (A) cause.
- (B) period.
- (C) recovery.
- (D) symptom.
- (E) diagnosis.

15

In the first paragraph, the sentence “*Now AI has come to the rescue*” means that LLMs can

- (A) reduce memory loss.
- (B) discard important data.
- (C) win literary competitions.
- (D) provide considerable help.
- (E) avoid using personal input.

16

“*For human writers this is a blessing and a curse*” (2nd paragraph) contains a(n)

- (A) personification.
- (B) repetition.
- (C) command.
- (D) antithesis.
- (E) solution.

17

The word “*like*” in “*bot-busting tools like Pangram are good at spotting*” (2nd paragraph) is used in the same way as in

- (A) AI writers like to indulge in words that come from Latin.
- (B) The likes of AI bots are changing the way humans write.
- (C) Some AI programs tend to use words like “leveraging”.
- (D) Editors know what texts written by AI tools look like.
- (E) LLMs like to use predictable figurative expressions.

18

In the sentence “*Anglo-Saxon words are often punchier*” (5th paragraph), “*punchier*” indicates that these words tend to be more

- (A) complex and obscure.
- (B) powerful and effective.
- (C) mysterious and intricate.
- (D) formal and sophisticated.
- (E) ambiguous and confusing.

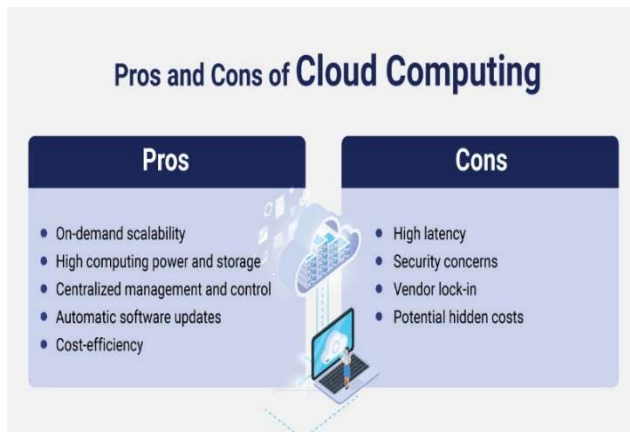
19

The action mentioned in "skip the exclamation marks" (6th paragraph) is semantically equivalent to

- (A) bring in.
- (B) carry on.
- (C) put back.
- (D) leave out.
- (E) move around.

READ TEXT II AND ANSWER NEXT TWO QUESTIONS.

TEXT II



From: https://www.rishabsoft.com/wp-content/uploads/2024/01/Blog\Pros-and-Cons-of-Cloud-Computing_Image.jpg

20

As regards the pros and cons of cloud computing, analyse the assertions below:

- I. It may adjust resources depending on the needs.
- II. It can reduce spending according to usage.
- III. It is immune to all types of cyberattacks.

Choose the correct answer.

- (A) Only I is correct.
- (B) Both I and II are correct.
- (C) Both I and III are correct.
- (D) Both II and III are correct.
- (E) All three assertions are correct.

21

The term "vendor lock-in" indicates the customer is in a situation that is

- (A) binding.
- (B) negligible.
- (C) forbidden.
- (D) disengaged.
- (E) unrestricted.

READ TEXT III AND ANSWER NEXT THREE QUESTIONS.

TEXT III



"We were looking for a non-hackable, energy efficient data center. Thanks for the file cabinet."

From: https://images.cartoonstock.com/lowres/computers-file_cabinet-file-paperwork-unhackable-security-CS630961_low.jpg

22

The saying that best expresses the point of this cartoon is

- (A) beauty is in the eye of the beholder.
- (B) the new broom sweeps clean.
- (C) every cloud has a silver lining.
- (D) health is wealth.
- (E) old is gold.

23

The phrasal verb "looking for" can be replaced, without significant change of meaning, by

- (A) seeking.
- (B) finding.
- (C) picking.
- (D) acquiring.
- (E) surveying.

24

In the cartoon, the adjective "non-hackable" refers to a system that cannot be

- (A) set up.
- (B) turned off.
- (C) shut down.
- (D) broken into.
- (E) brought back.

Raciocínio lógico-matemático

25

Em determinado período de monitoramento, a equipe responsável por um centro de processamento adotou a regra a seguir.

“Se a taxa de ocupação dos servidores for superior a 80%, então as rotinas não prioritárias serão transferidas para o período noturno.”

Considerando a lógica proposicional, essa regra é logicamente equivalente a

- (A) A taxa de ocupação dos servidores é inferior a 80% ou as rotinas não prioritárias serão transferidas para o período noturno.
- (B) A taxa de ocupação dos servidores é menor ou igual a 80% ou as rotinas não prioritárias serão transferidas para o período noturno.
- (C) A taxa de ocupação dos servidores é menor ou igual a 80% e as rotinas não prioritárias serão transferidas para o período noturno.
- (D) A taxa de ocupação dos servidores é superior a 80% ou as rotinas não prioritárias não serão transferidas para o período noturno.
- (E) Se as rotinas não prioritárias forem transferidas para o período noturno, então a taxa de ocupação dos servidores será superior a 80%.

26

Um sistema utiliza um contador que apresenta inicialmente o número 1. A cada comando executado, o número exibido é substituído por um dos seguintes valores:

- o número exibido acrescido de uma unidade;
- o dobro do número exibido.

O menor número de comandos necessários para que o contador passe a exibir o número 100 é

- (A) 6.
- (B) 7.
- (C) 8.
- (D) 9.
- (E) 10.

27

Considere o conjunto não vazio dos equipamentos examinados durante uma conferência patrimonial. Ao término do procedimento, foi apresentada a afirmação a seguir.

“Todos os equipamentos examinados receberam etiqueta patrimonial e tiveram sua localização registrada no inventário.”

Assinale a opção que apresenta a negação lógica dessa afirmação.

- (A) Pelo menos um equipamento examinado recebeu etiqueta patrimonial e teve sua localização registrada no inventário.
- (B) Nenhum equipamento examinado recebeu etiqueta patrimonial nem teve sua localização registrada no inventário.
- (C) Nenhum equipamento examinado recebeu simultaneamente etiqueta patrimonial e teve sua localização registrada no inventário.
- (D) Pelo menos um equipamento examinado não recebeu etiqueta patrimonial e não teve sua localização registrada no inventário.
- (E) Pelo menos um equipamento examinado não recebeu etiqueta patrimonial ou não teve sua localização registrada no inventário.

28

Um sistema de monitoramento utiliza dois sensores e pode operar em modo de manutenção.

Considere as proposições:

- p : o sensor A detecta uma anomalia;
- q : o sensor B detecta uma anomalia; e
- r : o modo de manutenção está ativado.

O sistema aciona um alerta quando pelo menos um dos sensores detecta uma anomalia e o modo de manutenção não está ativado, ou quando ambos os sensores detectam uma anomalia.

A proposição que representa o acionamento do alerta é

- (A) $[(p \vee q) \wedge \neg r] \vee (p \wedge q)$
- (B) $[(p \wedge q) \wedge \neg r] \vee (p \wedge q)$
- (C) $[(p \vee q) \wedge r] \vee (p \wedge \neg q)$
- (D) $[(p \vee q) \vee \neg r] \vee (p \wedge q)$
- (E) $[(p \vee q) \wedge \neg r] \wedge (p \vee q)$

29

Em relação às alterações processadas por determinada organização, considere verdadeiras as seguintes afirmações:

- toda alteração classificada como emergencial foi implantada no mesmo dia em que foi autorizada;
- toda alteração implantada no mesmo dia em que foi autorizada foi submetida a uma revisão posterior.

Uma dessas alterações, denominada *Alfa*, não foi submetida a uma revisão posterior.

Com base exclusivamente nessas informações, conclui-se necessariamente que a alteração *Alfa*

- (A) não foi autorizada.
- (B) foi autorizada, mas não foi implantada.
- (C) não foi classificada como emergencial.
- (D) foi implantada em dia posterior ao de sua autorização.
- (E) foi classificada como emergencial, mas não foi implantada no mesmo dia em que foi autorizada.

Atualidades e Inteligência Artificial

30

A expansão dos modelos de inteligência artificial tem impulsionado a construção de data centers de grande porte. Isso tem suscitado conflitos em razão dos impactos socioambientais desses empreendimentos, sobretudo quando instalados em regiões vulneráveis ou próximas a comunidades tradicionais.

Assinale a opção que identifica o impacto ambiental mais diretamente relacionado aos data centers.

- (A) A redução da cobertura vegetal pela instalação de cabos, cuja transmissão exige faixas desmatadas entre o data center e seus usuários.
- (B) O descarte frequente de eletrônicos junto aos resíduos domiciliares, o que sobrecarrega os serviços municipais de coleta urbana.
- (C) A contaminação do solo por fluidos de refrigeração, liberados regularmente durante a transferência de dados entre os equipamentos.
- (D) O aumento das emissões locais de gases pela atividade de processamento, que depende da combustão realizada no interior dos servidores.
- (E) A pressão sobre a disponibilidade de água e energia, demandadas pelo processamento contínuo e por certos sistemas de refrigeração.

31

Em julho de 2026, o Brasil acionou a Organização Mundial do Comércio (OMC) para contestar as tarifas impostas pelos Estados Unidos a produtos brasileiros. Os norte-americanos aceitaram participar da fase de consultas, e a China solicitou ingresso nessa etapa por considerar que também possui interesses comerciais afetados.

Nesse caso, a atuação da OMC pode

- (A) suspender os Estados Unidos da organização até que o governo retire as tarifas questionadas pelo Brasil.
- (B) determinar o pagamento de indenizações às empresas brasileiras afetadas pelas tarifas norte-americanas.
- (C) instaurar um painel para avaliar se as tarifas norte-americanas são compatíveis com os acordos em vigor.
- (D) impor aos produtos norte-americanos tarifas equivalentes às aplicadas pelos Estados Unidos às exportações brasileiras.
- (E) cancelar as tarifas norte-americanas e restabelecer as condições comerciais vigentes antes da decisão do governo.

32

Em 28 de fevereiro de 2026, os Estados Unidos e Israel iniciaram uma ofensiva militar conjunta contra o Irã. No centro do conflito está o Estreito de Ormuz, passagem marítima utilizada por importantes exportadores de petróleo e gás do Golfo Pérsico e com poucas rotas alternativas.

Assinale a opção que apresenta o impacto imediato dessa situação sobre o comércio internacional de energia.

- (A) O redirecionamento dos navios pelo Canal de Suez, que passou a substituir Ormuz nas rotas comerciais entre o Golfo e a Ásia.
- (B) O deslocamento dos embarques para oleodutos terrestres, preservando o volume de petróleo destinado aos mercados internacionais.
- (C) A retração do tráfego de petroleiros, acompanhada pela elevação dos custos de transporte e das cotações internacionais.
- (D) A concentração dos efeitos nas exportações iranianas, sem alteração relevante nos embarques realizados pelos demais países do Golfo.
- (E) A compensação imediata da oferta pelos demais membros da OPEP, que ampliaram a produção para estabilizar o mercado internacional.

33

No contexto da Inteligência Artificial (IA), os modelos de linguagem de grande porte (*Large Language Models*) pertencem à categoria dos modelos generativos.

O funcionamento básico desses modelos, com objetivo de geração de textos, fundamenta-se em

- (A) consultar um banco de dados fixo, contendo respostas pré-programadas por um humano que correspondam à entrada recebida.
- (B) limitar-se à correção ortográfica e gramatical de textos já existentes, sendo incapazes de estruturar novas frases ou argumentos de forma autônoma.
- (C) realizar buscas em tempo real em enciclopédias virtuais, para coletar trechos exatos de artigos acadêmicos que correspondam à pergunta do usuário.
- (D) calcular estatisticamente a probabilidade de ocorrência das próximas palavras ou termos em uma sequência, baseando-se nos padrões identificados em seu treinamento.
- (E) executar um escaneamento do disco rígido do computador do usuário, para identificar preferências pessoais e replicar o estilo de escrita do proprietário da máquina.

34

Sobre métodos de Aprendizado de Máquina, analise as afirmativas a seguir e assinale (V) para a verdadeira e (F) para a falsa.

- () Na aprendizagem bayesiana, as previsões sobre um dado novo são feitas considerando todo o espaço de hipóteses, ponderadas por suas probabilidades.
- () No aprendizado por reforço ativo, o agente deve decidir autonomamente quais ações tomar em cada estado para minimizar sua função de utilidade a longo prazo.
- () No aprendizado profundo, as hipóteses são estruturadas como redes complexas de funções algébricas interconectadas por pesos numéricos ajustáveis.

As afirmativas são, respectivamente,

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

35

Acerca dos conceitos de Inteligência Artificial (IA), analise as afirmativas a seguir.

- I. As redes neurais artificiais são sistemas computacionais distribuídos compostos de unidades de processamento interconectadas que computam funções matemáticas.
- II. No contexto de IA, o processamento de linguagem natural envolve o desenvolvimento de métodos computacionais para permitir que sistemas reproduzam a habilidade humana de compreender a linguagem falada ou escrita.
- III. O teste de Turing é uma metodologia utilizada para medir a capacidade de processamento numérico e a velocidade de cálculo de um sistema de IA.

Está correto o que se afirma em

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

Legislação Acerca de Segurança da Informação e Proteção de Dados

36

Um órgão federal está organizando um concurso público para provimento de cargos de nível superior e precisa publicar o resultado preliminar das provas objetivas e a lista de candidatos que concorrem às vagas reservadas para Pessoas com Deficiência (PcD), bem como daqueles que solicitaram atendimento especial por razões de saúde. De forma a garantir a transparência do certame, a Comissão do Concurso planejou publicar na internet uma planilha contendo o nome completo, o número completo do CPF, o relatório médico detalhado e o diagnóstico CID (Classificação Internacional de Doenças) de cada candidato aprovado nessa cota.

O Encarregado pelo Tratamento de Dados Pessoais (DPO) do órgão interveio, ressaltando que o diagnóstico de saúde constitui dado pessoal sensível e que a exposição integral de dados de identificação extrapola o limite necessário para a finalidade de controle social do concurso.

Considerando os preceitos da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD), assinale a opção que apresenta a solução correta que o órgão deve adotar para conciliar a transparência do concurso com a proteção de dados dos candidatos:

- (A) A Comissão do Concurso pode manter a publicação integral com laudos e CPFs completos sem qualquer alteração, tendo em vista que a LGPD não se aplica às autarquias federais quando agem no exercício do poder de império e na realização de concursos públicos.
- (B) O órgão deve decretar o sigilo absoluto de todo o resultado da cota de Pessoas com Deficiência, divulgando apenas o resultado geral da ampla concorrência no Portal da Transparência, encaminhando o resultado da cota de forma individual e privada ao e-mail de cada candidato.
- (C) O órgão deve aplicar os princípios da necessidade e da minimização de dados, publicando a lista oficial apenas com informações indispensáveis (como nome/inscrição, CPF parcialmente mascarado e a condição de 'deferido/aprovado' na cota), franqueando o acesso ao laudo médico detalhado estritamente ao próprio candidato e à banca examinadora.
- (D) O órgão deve exigir o consentimento prévio, escrito e inequívoco de todos os candidatos participantes da cota para publicar seus laudos e diagnósticos médicos completos, sob pena de eliminação sumária do concurso caso o candidato se recuse a assinar o termo de autorização.
- (E) O órgão deve promover a anonimização irreversível e definitiva de todos os dados dos candidatos na lista pública e no sistema interno do concurso, de modo que nem mesmo a comissão examinadora consiga vincular a nota do exame ao indivíduo titular.

37

Nos termos do Marco Civil da Internet (Lei nº 12.965/2014), a lei estabelece obrigações claras sobre a guarda de dados dos usuários para equilibrar a privacidade e a segurança.

Sobre os deveres de retenção de dados aplicáveis aos diferentes tipos de provedores (conexão e aplicação), assinale a afirmativa correta.

- (A) O provedor de conexão à internet (como as operadoras de telecomunicações) deve manter os registros de conexão, sob sigilo e em ambiente controlado, pelo prazo obrigatório de 6 (seis) meses.
- (B) O provedor de conexão à internet tem o dever de guardar, além dos registros de conexão, o histórico detalhado de navegação do usuário (registros de acesso a aplicações) pelo prazo de 1 (um) ano.
- (C) O provedor de aplicações de internet é proibido de guardar registros de acesso preventivamente, só podendo reter esses dados caso receba uma ordem judicial prévia determinando a guarda.
- (D) O provedor de aplicações de internet (como redes sociais e portais), desde que constituído de forma empresarial e com fins econômicos, deve manter os registros de acesso a aplicações de internet pelo prazo obrigatório de 6 (seis) meses.
- (E) Para facilitar investigações criminais, o Marco Civil da Internet unificou as regras, determinando que tanto provedores de conexão quanto de aplicação guardem todos os registros de uso e conexão pelo prazo comum de 5 (cinco) anos.

38

Com base na Lei Geral de Proteção de Dados Pessoais – LGPD, (Lei nº 13.709/2018), no que diz respeito à segurança e às boas práticas, à fiscalização e à Autoridade Nacional de Proteção de Dados (ANPD), analise as afirmativas a seguir.

- I. Os controladores e operadores podem formular regras de boas práticas e de governança relacionadas ao tratamento de dados pessoais.
- II. Compete à ANPD, entre outras atribuições previstas na LGPD, zelar pela proteção dos dados pessoais, fiscalizar e aplicar sanções nos casos de tratamento realizado em descumprimento à legislação e promover o conhecimento sobre proteção de dados pessoais e privacidade.
- III. Na aplicação das sanções administrativas, a ANPD considera a gravidade da infração e o dano causado, desconsiderando a adoção de mecanismos internos de prevenção e de medidas corretivas pelo infrator.

Está correto o que se afirma em

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

39

Roberto é Analista de Tecnologia da Informação em um órgão federal e, em razão de seu cargo, possui credenciais legítimas (*login*, senha e *token*) com autorização expressa para acessar, consultar e gerir o banco de dados sigiloso de licitações do órgão. Aproveitando-se de seu acesso regular e cotidiano, Roberto extraiu dados sigilosos de propostas comerciais de empresas concorrentes e os vendeu para uma organização criminosa, visando fraudar um certame.

Considerando estritamente a tipificação do crime de "*Invasão de Dispositivo Informático*" (Art. 154-A do Código Penal), introduzido pela Lei nº 12.737/2012, sobre a conduta de Roberto assinale a afirmativa correta.

- (A) Roberto responderá pelo crime de invasão de dispositivo informático, na sua forma qualificada, pois a lei prevê que o repasse de informações sigilosas a terceiros configura o delito mesmo quando o agente possui credenciais legítimas de acesso.
- (B) A conduta configura o crime de invasão de dispositivo informático apenas se Roberto tiver precisado instalar alguma vulnerabilidade (vírus ou *malware*) no sistema para baixar os arquivos; caso contrário, a conduta é atípica no Direito Penal brasileiro.
- (C) Roberto praticou o crime de invasão de dispositivo informático com causa de aumento de pena de um terço à metade, devendo responder por meio de ação penal pública condicionada à representação do Ministério Público, por se tratar de crime cibernético.
- (D) Roberto responderá pelo crime da Lei nº 12.737/2012 porque o crime se consumou no momento em que ele conectou o banco de dados à rede mundial de computadores (internet) para extrair as propostas comerciais, configurando a violação de segurança do órgão.
- (E) A conduta de Roberto não configura o crime de invasão de dispositivo informático (Art. 154-A do CP), pois a elementar do tipo penal exige que a ação ocorra "sem autorização expressa ou tácita". Como Roberto possuía acesso legítimo, ele responderá por outros crimes (como violação de sigilo funcional) mas não por este, amparado na Lei nº 12.737/2012.

40

Uma universidade federal, visando modernizar e dar celeridade ao processo de inscrição de seu novo concurso público, decidiu desenvolver um sistema de inscrição inteligente. O objetivo é que o candidato digite apenas o seu CPF e, a partir de uma integração de banco de dados, o sistema preencha automaticamente informações cadastrais básicas, como nome completo e data de nascimento, oriundas do Cadastro Base do Cidadão (ou da base da Receita Federal).

Considerando as normativas de compartilhamento de dados na Administração Pública, a Lei de Acesso à Informação (Lei nº 12.527/2011) e a Lei Geral de Proteção de Dados (Lei nº 13.709/2018), assinale a opção que indica corretamente como a universidade deve proceder para ter acesso a esses dados para o seu sistema.

- (A) Deve formular um pedido via Serviço de Informações ao Cidadão (SIC) da Receita Federal com base na transparência passiva da LAI, solicitando o envio da base de dados completa dos cidadãos para alimentar o seu sistema local de inscrições.
- (B) Está impedida de realizar essa integração automatizada, pois o cruzamento de dados pessoais (como CPF, nome e data de nascimento) entre órgãos da Administração Pública exige, obrigatoriamente, o consentimento prévio, expresso e inequívoco de cada cidadão titular dos dados, não havendo exceção legal.
- (C) Deve solicitar que o ente gestor do banco de dados publique a relação de CPFs, nomes e datas de nascimento no Portal da Transparência, garantindo a transparência ativa da LAI, para que então o sistema da universidade possa extrair os dados livremente por meio de ferramentas de automação.
- (D) Deve utilizar os mecanismos oficiais de interoperabilidade governamental (ou firmar convênio/acordo de compartilhamento de dados), justificando que o acesso aos dados pessoais é estritamente necessário para o atendimento da finalidade pública e para a execução de suas competências legais, dispensando-se, neste caso, o consentimento do candidato.
- (E) Deve ser concedido, de forma ampla e irrestrita, o acesso ao banco de dados a todos os servidores da universidade, sob a justificativa de que, por serem dados geridos pelo Estado, aplica-se o princípio constitucional da publicidade absoluta sobre qualquer informação não classificada como ultrassecreta.

Conhecimentos Específicos

41

Um técnico de segurança da informação foi encarregado de projetar a interconexão entre a filial recém-inaugurada e a matriz por meio de uma Rede Privada Virtual (VPN).

O projeto estabelece os seguintes requisitos mandatórios de segurança para o tráfego que transitará pela rede pública (internet):

- Garantia de confidencialidade ponta a ponta dos dados trafegados entre os *gateways*;
- Proteção contra ataques de repetição (*anti-replay*) e garantia de integridade e autenticidade da origem;
- Ocultação do endereçamento IP interno da rede de origem e de destino durante o tráfego pela Internet.

Assinale a opção que indica o protocolo e o modo de operação da suíte IPsec a serem configurados nos roteadores de borda para atender a todos os requisitos estabelecidos.

- (A) *Authentication Header* (AH), em modo Túnel.
- (B) *Authentication Header* (AH), em modo Transporte.
- (C) *Encapsulating Security Payload* (ESP), em modo Túnel.
- (D) *Encapsulating Security Payload* (ESP), em modo Transporte.
- (E) *Internet Key Exchange* (IKEv2), operando isoladamente sem uso de AH ou ESP.

42

A DATAPREV pretende migrar três sistemas institucionais para serviços de computação em nuvem. Após a análise dos requisitos, foram definidas as seguintes soluções:

- Sistema A: os usuários utilizarão uma aplicação disponibilizada pelo próprio provedor, sem administrar os servidores, os sistemas operacionais ou o armazenamento que dão suporte ao serviço, nem controlar as capacidades individuais da aplicação, admitindo-se apenas configurações limitadas específicas dos usuários.
- Sistema B: a equipe da DATAPREV administrará o sistema operacional, o armazenamento e as aplicações implantadas. O provedor disponibilizará recursos fundamentais de processamento, armazenamento e rede, sem que a equipe administre a infraestrutura de nuvem que dá suporte a esses recursos.
- Sistema C: a equipe da DATAPREV implantará aplicações desenvolvidas por ela, utilizando linguagens de programação, bibliotecas, serviços e ferramentas suportadas pelo provedor. A equipe manterá o controle sobre as aplicações implantadas, mas não administrará os servidores, os sistemas operacionais e o armazenamento que dão suporte à plataforma.

Considerando os modelos do serviço de computação em nuvem, os sistemas A, B e C correspondem, respectivamente, a

- (A) SaaS, PaaS e IaaS.
- (B) PaaS, IaaS e SaaS.
- (C) IaaS, SaaS e PaaS.
- (D) PaaS, SaaS e IaaS.
- (E) SaaS, IaaS e PaaS.

43

Um Analista de Segurança da Informação registrou dois incidentes relacionados aos sistemas da empresa.

- I. Após um volume anormal de requisições simultâneas, um sistema utilizado para prestação de serviços aos cidadãos permaneceu inacessível aos usuários legítimos durante várias horas, sem evidências de alteração dos dados armazenados.
- II. Um relatório com dados cadastrais e financeiros confidenciais foi enviado por falha operacional e acessado por destinatários que não possuíam nível de permissão para visualizá-lo, embora o conteúdo do documento não tenha sofrido qualquer modificação.

Considerando os princípios fundamentais da Segurança da Informação, os incidentes I e II violaram, respectivamente, os princípios de

- (A) integridade e autenticidade.
- (B) confidencialidade e disponibilidade.
- (C) disponibilidade e confidencialidade.
- (D) confidencialidade e integridade.
- (E) disponibilidade e autenticidade.

44

Durante uma auditoria de segurança em um Tribunal, um analista de TI elaborou um relatório de modernização para um sistema legado de tramitação processual que não recebe atualizações de arquitetura há duas décadas. No documento, o analista aponta que os dados em repouso no banco de dados são cifrados de forma simétrica com o algoritmo DES.

Além disso, constatou-se que a assinatura digital das peças processuais aplica o algoritmo assimétrico RSA sobre um resumo criptográfico do documento gerado nativamente pela função de *hash* MD5.

Considerando o cenário descrito e os fundamentos dos algoritmos criptográficos em uso, analise as afirmativas relativas ao diagnóstico do analista.

- I. O sistema legado, ao manter o uso do DES para cifrar os documentos, apresenta uma vulnerabilidade crítica a ataques de força bruta sobre o espaço de chaves, se comparado a um sistema atualizado que utilize o AES-128.
- II. A geração periódica de um novo par de chaves RSA para os Magistrados eliminaria os riscos de colisão associados à verificação de integridade das peças processuais assinadas no sistema.
- III. A continuidade do uso da função MD5, ou mesmo sua eventual substituição direta pelo algoritmo SHA-1, mantém o sistema exposto ao risco de que dois documentos com teores diferentes produzam o mesmo resumo criptográfico.

Com base nas propriedades matemáticas e na segurança técnica dos algoritmos citados, está correto o que se afirma em

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

45

O *OWASP IoT Top 10* (2018) apresenta categorias de riscos de segurança associados ao desenvolvimento, à implantação e ao gerenciamento de dispositivos de Internet das Coisas (IoT).

Durante uma auditoria da DATAPREV em um lote recém-adquirido de sensores IoT, a equipe técnica constatou que

- a senha administrativa inicial atende aos critérios de complexidade e deve ser alterada no primeiro acesso;
- o dispositivo dispõe de funcionalidade própria para atualização de *firmware* pela rede local;
- após receber um pacote de atualização, o dispositivo inicia sua instalação sem verificar a assinatura digital do pacote nem empregar mecanismo criptográfico para confirmar sua integridade.

Considerando especificamente a falha encontrada no processo de atualização, assinale a opção que apresenta, segundo o *OWASP IoT Top 10* (2018), sua classificação correta.

- (A) *Insecure Network Services* (I2), porque a existência de uma funcionalidade de atualização acessível pela rede caracteriza, por si só, a exposição de um serviço de rede inseguro.
- (B) *Lack of Secure Update Mechanism* (I4), porque o dispositivo instala o *firmware* sem validar criptograficamente sua integridade e sua autenticidade antes da aplicação.
- (C) *Insecure Data Transfer and Storage* (I7), porque a falha está necessariamente relacionada à proteção dos dados transmitidos pela rede durante a transferência do pacote de atualização.
- (D) *Lack of Device Management* (I8), porque qualquer deficiência relacionada ao gerenciamento e à implantação de atualizações em dispositivos já instalados pertence prioritariamente a essa categoria.
- (E) *Weak, Guessable, or Hardcoded Passwords* (I1), porque a existência de uma credencial administrativa inicial constitui a vulnerabilidade determinante, independentemente da política de alteração adotada.

46

No contexto das operações modernas de segurança cibernética, a postura defensiva combina a geração contínua de conhecimento sobre ameaças com a investigação ativa no ambiente corporativo. Relacione as práticas de segurança a seguir às suas respectivas características operacionais.

1. *Threat Hunting*
 2. *Cyber Threat Intelligence (CTI)*
- () Atividade proativa e iterativa conduzida internamente no ambiente, que parte do pressuposto de que os controles automatizados falharam e de que o invasor já pode ter obtido acesso à rede.
- () Compartilhamento e consumo de dados estruturados sobre ameaças e relatórios de tendências do cenário global de ataques.
- () Formulação e validação de hipóteses investigativas orientadas a anomalias para inspecionar minuciosamente a telemetria interna (como *logs* de *endpoints* e fluxos de rede) em busca de atividades não alertadas.
- () Coleta, processamento e análise de informações sobre motivações, capacidades e campanhas de agentes maliciosos externos, visando orientar tomadas de decisão táticas e estratégicas na organização.

Assinale a opção que indica a relação correta.

- (A) 1, 2, 2 e 1.
(B) 1, 2, 1 e 2.
(C) 2, 1, 1 e 2.
(D) 2, 1, 2 e 1.
(E) 1, 1, 2 e 2.

47

Um engenheiro de redes foi incumbido de atualizar a infraestrutura de comunicações de um grande complexo hospitalar. O projeto envolve o provimento de conectividade cabeada para equipamentos de monitoramento de pacientes e a modernização do acesso à rede sem fio.

De acordo com as diretrizes normativas, as quais o engenheiro deve seguir, mais precisamente a família IEEE 802, assinale a afirmativa correta.

- (A) O padrão IEEE 802.3 (*Ethernet*) utiliza nativamente o protocolo CSMA/CA (*Collision Avoidance*) para prevenir colisões na rede cabeada.
- (B) O padrão IEEE 802.11a, já de uso legado, operava em 2,4 GHz com até 11 Mbps, características superadas pelo 802.11b, que atua em 5 GHz com até 54 Mbps.
- (C) O padrão IEEE 802.11ac (Wi-Fi 5) entrega taxas na ordem de gigabits operando exclusivamente na frequência de 2,4 GHz com tecnologia MIMO (*Multiple Input Multiple Output*).
- (D) O padrão IEEE 802.11n introduziu a tecnologia MIMO (*Multiple Input Multiple Output*), oferecendo suporte opcional a operação em banda dupla, em 2,4 GHz e 5 GHz.
- (E) O padrão IEEE 802.3ab, que especifica conexões *Gigabit Ethernet* para redes locais, determina a utilização exclusiva de cabeamento de fibra óptica para garantir a integridade do sinal na taxa de transmissão de 1000 Mbps.

48

Considere o *script* Bash a seguir, denominado *processa.sh*, armazenado em um servidor Linux e com permissão de execução:

```
#!/bin/bash
total=0
for item in "$*"; do
    total=$((total + 1))
done

if [ $# -eq 3 ]; then
    total=$((total + 20))
fi
```

```
[ "$1" = "srv01" ]
echo "$total-$#-$?"
```

Em um terminal Linux, um administrador executou a seguinte linha de comando:

```
./processa.sh srv01 srv02 srv03
```

A saída exibida no terminal, após a execução do *script*, será

- (A) 21-3-0
(B) 21-3-1
(C) 23-3-0
(D) 23-1-1
(E) 20-3-0

49

No passado, o tratamento de incidentes era realizado quase exclusivamente por especialistas da própria equipe de resposta a incidentes da organização. Hoje, embora esses especialistas continuem sendo fundamentais, a maioria das organizações reconhece, cada vez mais, que o sucesso de seus esforços de resposta a incidentes depende da participação de diversas partes internas e externas.

Dessa forma, de acordo com a NIST SP 800-61 Rev. 3, assinale a opção que corresponde ao cargo que possui as seguintes responsabilidades: *“supervisiona a resposta a incidentes, aloca recursos financeiros e pode deter autoridade decisória sobre ações de resposta de alto impacto, como a interrupção ou a reconstrução de serviços críticos.”*

- (A) Liderança.
(B) Relações públicas.
(C) Especialista jurídico.
(D) Engenheiro de *software*.
(E) Proprietário dos processos de negócios.

50

O *framework* MITRE ATT&CK (*Adversarial Tactics, Techniques, and Common Knowledge*) organiza o comportamento dos adversários cibernéticos em uma matriz composta por táticas, técnicas e procedimentos.

Relacione as táticas do MITRE ATT&CK listadas a seguir aos seus respectivos objetivos primários.

1. *Persistence*
2. *Defense Evasion*
3. *Discovery*
4. *Lateral Movement*

- () O invasor estende seu acesso e pivota o controle para outros sistemas, servidores e estações conectados à rede corporativa interna.
- () O invasor aplica mecanismos para sustentar o canal de comando e garantir a reativação do acesso perante intervenções corriqueiras de reinício ou revogação de sessões.
- () O invasor adota medidas ativas para mitigar a geração de alertas em soluções de monitoramento, adulterando registros, ofuscando código ou neutralizando agentes de inspeção.
- () O invasor tenta obter conhecimento e visibilidade sobre a rede interna, os sistemas operacionais, as permissões e as configurações do ambiente corporativo.

Assinale a opção que indica a relação correta, segundo a ordem apresentada.

- (A) 4, 2, 1 e 3.
- (B) 4, 1, 3 e 2.
- (C) 4, 1, 2 e 3.
- (D) 1, 4, 2 e 3.
- (E) 1, 2, 4 e 3.

51

O recurso de operações de segurança (SecOps) capaz de integrar diversas ferramentas de segurança (como *firewall*, SIEM e EDR) e padronizar o fluxo de triagem e contenção de incidentes por meio da execução de fluxos de trabalho pré-configurados (*playbooks*), corresponde ao

- (A) *Breach and Attack Simulation* (BAS).
- (B) *Cloud Access Security Broker* (CASB).
- (C) *Extended Detection and Response* (XDR).
- (D) *User and Entity Behavior Analytics* (UEBA).
- (E) *Security Orchestration, Automation and Response* (SOAR).

52

A DATAPREV pretende implantar uma aplicação institucional crítica em nuvem. A solução será hospedada em uma única região e deverá reduzir o risco de interrupção do serviço decorrente da indisponibilidade de uma instalação física. Para isso, a equipe de TI avalia distribuir os componentes da aplicação entre zonas de disponibilidade distintas.

Considerando a organização da infraestrutura em regiões e zonas de disponibilidade, analise as afirmativas a seguir.

- I. A distribuição de componentes da aplicação entre zonas de disponibilidade distintas de uma mesma região pode favorecer a continuidade do serviço diante da indisponibilidade de uma das zonas, desde que a arquitetura da solução esteja preparada para operar nessas condições.
- II. Por estarem localizadas em uma mesma região, diferentes zonas de disponibilidade compartilham necessariamente a mesma infraestrutura física, de modo que a distribuição de componentes entre elas não proporciona isolamento em relação a falhas de instalações.
- III. A utilização de múltiplas zonas de disponibilidade pode reduzir a exposição da aplicação a falhas que afetem uma zona específica, mas não elimina a necessidade de considerar eventos capazes de afetar uma região inteira.

Está correto o que se afirma em

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

53

A DATAPREV pretende ampliar o uso de computação em nuvem para aplicações institucionais, buscando aproveitar características desse ambiente para responder a variações de demanda e aumentar a continuidade dos serviços.

Considerando os benefícios associados à computação em nuvem, analise as afirmativas a seguir e assinale (V) para a verdadeira e (F) para a falsa.

- () A utilização de recursos de nuvem pode favorecer estratégias de recuperação de desastres ao possibilitar, conforme a arquitetura adotada, a replicação de dados e a recuperação de cargas de trabalho em ambiente distinto daquele afetado pelo evento.
- () A elasticidade permite que capacidades computacionais sejam provisionadas e liberadas rapidamente em função da demanda, podendo esse ajuste ocorrer automaticamente.
- () O escalonamento horizontal permite aumentar ou diminuir a capacidade computacional de uma única instância, por exemplo, alterando a quantidade de memória ou de capacidade de processamento a ela atribuída.

As afirmativas são, respectivamente,

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

54

A equipe de resposta a incidentes da DATAPREV identificou, em curto intervalo de tempo, quatro incidentes de segurança. Como os recursos disponíveis são limitados, o coordenador precisa estabelecer critérios para definir a prioridade de tratamento desses incidentes.

Para esse caso, de acordo com a NIST SP 800-61 Rev. 3, assinale a afirmativa correta.

- (A) Os incidentes devem ser tratados preferencialmente na ordem cronológica de identificação, pois esse procedimento reduz o risco de atrasos injustificados.
- (B) A priorização deve considerar exclusivamente a criticidade dos ativos afetados, pois esse fator é suficiente para determinar a severidade de qualquer incidente.
- (C) A triagem, a priorização e a escalada dos incidentes devem ser baseadas em fatores de avaliação de risco, podendo considerar, entre outros, a criticidade dos ativos, o impacto funcional, o impacto sobre dados, o estágio da atividade observada, a caracterização do agente da ameaça e a recuperabilidade.
- (D) A decisão sobre iniciar a recuperação deve ocorrer imediatamente após a declaração de um incidente, independentemente do impacto operacional que as atividades de recuperação possam causar.
- (E) A organização deve priorizar primeiro os incidentes que apresentem maior complexidade técnica, ainda que seu impacto potencial seja menor.

55

No âmbito das operações de segurança da informação (*SecOps*), diferentes ferramentas e tecnologias defensivas são empregadas para mitigar riscos e conter ameaças em pontos distintos da infraestrutura de rede corporativa.

Relacione as ferramentas de segurança listadas a seguir às suas respectivas funções e características operacionais primárias.

1. *Intrusion Prevention System* (IPS)
 2. *Proxy Web*
 3. Antivírus
 4. *Web Application Firewall* (WAF)
- () Atua como intermediário nas requisições dos usuários da rede interna para a Internet, possibilitando a filtragem e o controle de acesso com base em URLs, domínios e categorias de conteúdo.
 - () Analisa o tráfego da camada 7 do modelo OSI direcionado a servidores e serviços web, sendo projetado especificamente para detectar e bloquear ameaças direcionadas ao ecossistema web.
 - () Opera tipicamente nas estações de trabalho e servidores, realizando a varredura e a monitoração de arquivos e processos em execução na memória para detectar, bloquear ou colocar em quarentena códigos maliciosos.
 - () É um dispositivo posicionado em linha (*inline*) no fluxo de rede que inspeciona pacotes, identificando assinaturas de ataques conhecidos ou desvios de protocolo e descartando ativamente o tráfego hostil em tempo real.

Assinale a opção que indica a relação correta, segundo a ordem apresentada.

- (A) 2, 4, 3 e 1.
- (B) 1, 4, 3 e 2.
- (C) 2, 1, 4 e 3.
- (D) 4, 2, 1 e 3.
- (E) 3, 1, 2 e 4.

56

Um analista de infraestruturas do DATAPREV está avaliando as ferramentas de Infraestrutura como Código (IaC), disponíveis no mercado para compor o seu plano de automação e implantação multinuvem.

O arquiteto responsável elaborou um parecer técnico comparando o *HashiCorp Terraform* e o *Red Hat Ansible*.

Considerando as características arquiteturais e as formas de operação dessas ferramentas, assinale a opção que apresenta um ponto de diferenciação correto entre elas.

- (A) O *Ansible* necessita de um servidor mestre dedicado ativo para coordenar a distribuição das configurações nos servidores clientes, ao passo que o *Terraform* é estritamente *masterless* por operar apenas com chamadas de API do provedor de nuvem.
- (B) O *Terraform* adota uma arquitetura baseada em agentes que devem ser pré-instalados em todas as instâncias EC2 do usuário, enquanto o *Ansible* é um *framework agentless* que se conecta via protocolo SSH ou WinRM.
- (C) O *Terraform* é uma ferramenta focada primordialmente em provisionamento de infraestrutura que utiliza uma linguagem declarativa, enquanto o *Ansible* é tradicionalmente focado gerenciamento de configuração e automação e utiliza *playbooks* escritos em YAML para organizar *plays* e *tasks*.
- (D) O *Ansible* utiliza um arquivo de estado global compartilhado e centralizado para gerenciar a dependência dos recursos de *hardware* criados, ao passo que o *Terraform* dispensa qualquer tipo de gerenciamento de estado por ser uma ferramenta declarativa *masterless*.
- (E) O *Ansible* é a ferramenta ideal recomendada para automação de provisionamento em ambientes *multicloud* complexos devido à sua capacidade de persistir as dependências físicas dos recursos na API nativa do *CloudFormation*.

57

Durante o planejamento da continuidade dos serviços de processamento de dados da DATAPREV, a equipe responsável identificou informações essenciais para a retomada de atividades prioritárias após uma possível interrupção.

Considerando as orientações da ABNT NBR ISO 22313:2020 relativas a informações e dados, assinale a opção que apresenta, corretamente, uma ação recomendada para a organização.

- (A) Evitar a utilização de meios físicos para cópia de informações, restringindo o armazenamento a formatos eletrônicos.
- (B) Priorizar a disponibilidade dos dados, dispensando requisitos de confidencialidade e integridade durante a recuperação.
- (C) Manter as cópias de informações e dados em locais distantes da fonte original, independentemente dos requisitos de disponibilidade.
- (D) Armazenar as cópias de segurança o mais próximo possível da fonte original, de modo a facilitar sua recuperação em caso de interrupção.
- (E) Proteger as informações e os dados vitais e assegurar sua recuperação dentro dos períodos de tempo identificados na análise de impacto nos negócios.

58

Durante uma auditoria em uma sociedade empresária, a equipe de segurança da informação analisou o fluxo de aprovação eletrônica de pagamentos do Sistema Integrado de Gestão Financeira.

Constatou-se que, após a autenticação de um gestor, a confirmação do pagamento de despesas de grande vulto é gravada no banco de dados apenas com um registro simples de data e o nome do usuário em formato texto, sem a utilização de assinaturas digitais com certificados ICP-Brasil, sem carimbo do tempo (*timestamping*) confiável e sem trilhas de auditoria criptograficamente encadeadas e imutáveis.

O relatório da auditoria apontou formalmente que, devido a essa falha de arquitetura, caso um gestor legítimo autorize um pagamento indevido e, posteriormente, alegue perante uma comissão disciplinar que nunca realizou tal operação, a administração não disporá de evidências técnicas com validade pericial para contrapor a alegação do gestor e comprovar a verdadeira autoria.

No âmbito da modelagem de ameaças baseada no modelo STRIDE, a ameaça descrita nesse cenário é categorizada como

- (A) *Spoofing*.
- (B) *Tampering*.
- (C) *Repudiation*.
- (D) *Elevation of Privilege*.
- (E) *Information Disclosure*.

59

Uma sociedade empresária que processa informações pessoais decidiu atualizar seu programa de governança em segurança da informação com base no *NIST Cybersecurity Framework (CSF) versão 1.1*.

Durante o mapeamento de processos, a equipe de segurança da informação constatou grande dependência de fornecedores externos para sustentação de sistemas legados, aquisição de componentes de *software* de terceiros (*open source* e proprietários) e hospedagem de serviços em nuvem pública.

Visando mitigar ameaças decorrentes desse cenário, os gestores de segurança da informação determinaram a estruturação formal de processos alinhados à Gestão de Riscos na Cadeia de Suprimentos Cibernética (*Cyber Supply Chain Risk Management – C-SCRM*).

Considerando as diretrizes do NIST CSF v1.1 para a gestão de riscos na cadeia de suprimentos cibernética, assinale a opção que apresenta condutas alinhadas aos objetivos do C-SCRM.

- (A) Transferir formalmente a responsabilidade civil e técnica de resposta a incidentes para os fornecedores externos, desobrigando a empresa contratante de monitorar os riscos inerentes aos serviços terceirizados.
- (B) Avaliar previamente os riscos associados aos fornecedores e estabelecer requisitos contratuais que os obriguem a implementar controles adequados de cibersegurança e a cooperar nos processos de resposta a incidentes.
- (C) Restringir a análise de vulnerabilidades cibernéticas unicamente aos códigos-fonte desenvolvidos pela equipe interna da organização, pressupondo a conformidade técnica dos *softwares* homologados de terceiros.
- (D) Adotar o isolamento físico irrestrito em toda a infraestrutura computacional, dispensando a aplicação de cláusulas de auditoria de segurança em contratos de prestação de serviços de TI.
- (E) Dispensar a realização de auditorias ou revisões periódicas de conformidade para parceiros que já apresentem declarações prévias de conformidade com padrões de mercado.

60

A gestão ágil de projetos constitui uma abordagem orientada à entrega contínua de valor e à adaptação às mudanças ao longo do projeto.

Com base nesse assunto, analise as afirmativas a seguir.

- I. O *Scrum* é um *framework* ágil aplicável a ambientes complexos e sujeitos a mudanças, utilizando responsabilidades e eventos definidos para promover a entrega iterativa e incremental de valor.
- II. A abordagem ágil foi incorporada de forma abrangente ao Guia PMBOK em sua 5ª edição, que passou a estabelecer práticas específicas de métodos ágeis para o gerenciamento de projetos sujeitos a incertezas e mudanças.
- III. Embora aplicáveis a diferentes áreas, as abordagens ágeis são menos indicadas para projetos de desenvolvimento de software sujeitos a mudanças frequentes, pois pressupõem maior estabilidade dos requisitos ao longo do projeto.

Está correto o que se afirma em

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

61

O Microsoft Purview disponibiliza controles complementares para proteção da informação.

Os rótulos de sensibilidade (Sensitivity Labels) podem classificar arquivos e e-mails e aplicar mecanismos de proteção, incluindo criptografia e controle de acesso. Nas configurações de criptografia com permissões definidas pelo administrador, é possível determinar quais usuários podem acessar o conteúdo e estabelecer condições para o acesso offline.

O Data Loss Prevention (DLP) identifica informações sensíveis e aplica ações preventivas sobre diferentes localizações, aplicativos e formas de transmissão configuradas pela organização.

O Insider Risk Management utiliza indicadores de atividades potencialmente arriscadas para apoiar a identificação e a investigação de riscos internos, inclusive em cenários relacionados à possível exfiltração de dados por usuários em processo de desligamento.

A Double Key Encryption (DKE) utiliza duas chaves para proteger conteúdo de elevada sensibilidade: uma sob gerenciamento da Microsoft e outra mantida sob controle da própria organização, sendo indicada para situações que demandam requisitos mais rigorosos de custódia e soberania das chaves criptográficas.

Fonte: Microsoft Learn (<https://learn.microsoft.com/pt-br/purview/>)

A área de segurança da informação da DATAPREV identificou que determinados documentos confidenciais precisam continuar protegidos até depois de terem sido copiados para dispositivos ou contas de armazenamento que não são administrados pela organização. O requisito de segurança estabelece que, após o desligamento de um funcionário e a consequente retirada de sua autorização corporativa, ele não deverá conseguir abrir novamente uma cópia protegida que tenha recebido legitimamente durante o vínculo, mesmo armazenada em seu computador pessoal. Além disso, o acesso a documentos exige uma nova autorização sempre que necessário, não admitindo a licença de acesso *offline* que permita ao usuário continuar abrindo o conteúdo após a retirada de sua permissão. Não há requisito específico de manutenção de uma segunda chave criptográfica em infraestrutura própria da organização. Considerando as funcionalidades descritas e o requisito apresentado, indique a configuração mais adequada para atender à demanda da DATAPREV.

- (A) Aplicar uma política de *Data Loss Prevention* (DLP) ao conteúdo confidencial, pois o bloqueio das ações de compartilhamento permite invalidar posteriormente as permissões das cópias que já tenham sido transferidas para dispositivos não gerenciados.
- (B) Aplicar rótulo de sensibilidade com criptografia e permissões definidas pelo administrador, configurando o acesso *offline* como não permitido, de modo que o direito de abertura do conteúdo permaneça condicionado à autorização do usuário mesmo quando o arquivo estiver armazenado fora do ambiente corporativo.
- (C) Configurar uma política de *Insider Risk Management* para usuários em processo de desligamento, pois a identificação do evento de saída da organização faz com que as licenças de utilização dos documentos anteriormente acessados pelo usuário sejam automaticamente invalidadas.
- (D) Utilizar *Double Key Encryption*, pois essa funcionalidade é destinada especificamente ao gerenciamento da revogação individual de usuários que conservaram cópias de documentos corporativos, mesmo quando não existe requisito de custódia própria de chaves.
- (E) Aplicar um rótulo de sensibilidade apenas para classificação, associado a uma política de DLP, pois a persistência da classificação no arquivo é suficiente para impedir sua abertura após a retirada da identidade corporativa do antigo funcionário.

62

Uma equipe de dados da DATAPREV trata uma base de registros administrativos e substitui o número do CPF de cada titular por um código identificador único. A tabela que permite relacionar cada código ao CPF correspondente é armazenada em servidor distinto daquele que contém a base tratada, com acesso restrito a integrantes autorizados da própria equipe controladora.

Os analistas que trabalham apenas com a base tratada conseguem realizar as análises necessárias, mas não conseguem determinar a identidade dos titulares sem utilizar as informações armazenadas nesse servidor separado.

Diante dessas condições, o tratamento aplicado pela equipe se caracteriza, segundo a Lei nº 13.709/2018 (LGPD), como um caso de

- (A) *anonimização*, porque a retirada do CPF da base utilizada pelos analistas impede a identificação direta dos titulares, ainda que o controlador conserve informações capazes de restabelecer a associação.
- (B) *dado anonimizado*, porque os usuários que acessam rotineiramente a base tratada não dispõem, nesse mesmo ambiente, dos elementos necessários para identificar os titulares.
- (C) *reidentificação*, porque a manutenção de uma tabela capaz de relacionar os códigos aos CPFs significa que a identidade dos titulares já foi restabelecida no conjunto de dados tratado.
- (D) *anonimização*, porque o armazenamento separado da tabela de correspondência torna a identificação dos titulares dependente de uma operação adicional e, portanto, descaracteriza os códigos como dados pessoais.
- (E) *pseudonimização*, porque a associação dos códigos aos respectivos titulares depende do uso de informação adicional mantida separadamente pelo controlador em ambiente de acesso restrito.

63

Durante um teste de intrusão (*pentest*) em uma aplicação web corporativa, um analista observou que o sistema possui uma funcionalidade para importação de fotos de perfil a partir de uma URL fornecida pelo usuário.

```
POST /api/perfil/carregar-imagem
```

```
Content-Type: application/json
```

```
{"url": "https://servidor-externo.com/minha-foto.png"}
```

Para verificar se a aplicação estava protegida e realizava a devida validação e restrição do destino, o analista alterou o *payload* da requisição para:

```
{"url": "http://127.0.0.1:8080/admin/status"}
```

Como resposta, a própria aplicação executou a requisição de rede internamente e retornou no corpo da resposta HTTP o painel de administração e métricas internas do sistema, que estava configurado para escutar apenas na interface de *localhost* local e estava inacessível externamente.

O teste de intrusão demonstrou a exploração bem-sucedida da vulnerabilidade, que é conhecida como:

- (A) *Cross-Site Scripting* (XSS).
- (B) *Local File Inclusion* (LFI).
- (C) *Full Path Disclosure* (FPD).
- (D) *Cross-Site Request Forgery* (CSRF).
- (E) *Server-Side Request Forgery* (SSRF).

64

Em um cenário hipotético, o *Blockchain* está sendo utilizado para registrar operações realizadas entre diferentes sistemas corporativos. Cada bloco contém 1.024 transações, cujos *hashes* são organizados em uma árvore de Merkle binária balanceada.

Nessa estrutura, cada nó interno é obtido a partir do *hash* da concatenação dos dois *hashes* de seus nós filhos, até a obtenção de um único valor no topo da árvore, denominado raiz de Merkle.

Um auditor possui o conteúdo de uma determinada transação e a raiz de Merkle registrada no cabeçalho do bloco. Para verificar se essa transação pertence ao bloco, sem receber todas as demais transações, ele recebe os *hashes* necessários para reconstruir o caminho entre a transação e a raiz.

O número de *hashes* adicionais, que o auditor deve receber para realizar essa verificação, é

- (A) 10.
- (B) 11.
- (C) 20.
- (D) 1023.
- (E) 1024.

65

Uma sociedade empresária está revisando seu Sistema de Gestão de Segurança da Informação (SGSI), com base nas normas ABNT NBR ISO/IEC 27001:2022 e ABNT NBR ISO/IEC 27002:2022.

Considerando as disposições das referidas normas, assinale a afirmativa correta.

- (A) A ABNT NBR ISO/IEC 27001:2022 tem como finalidade principal fornecer diretrizes e orientações detalhadas para a implementação dos controles de segurança da informação descritos no Anexo A.
- (B) A ABNT NBR ISO/IEC 27001:2022 exige a implementação compulsória e integral de todos os 93 controles listados em seu Anexo A, para que uma organização obtenha a certificação de seu SGSI.
- (C) A edição de 2022 da ABNT NBR ISO/IEC 27002 introduziu atributos para classificação dos controles, utilizando exclusivamente os princípios de confidencialidade, integridade e disponibilidade como critério de categorização.
- (D) A ABNT NBR ISO/IEC 27002:2022 estabelece os requisitos auditáveis para a certificação de um SGSI, enquanto a ABNT NBR ISO/IEC 27001:2022 possui caráter estritamente orientativo.
- (E) Os controles necessários ao tratamento dos riscos devem ser comparados com os do Anexo A da ABNT NBR ISO/IEC 27001:2022, a fim de verificar possíveis omissões e subsidiar a Declaração de Aplicabilidade.

66

O SNMP (*Simple Network Management Protocol*) baseia-se em um modelo de gerenciamento em que uma estação gerente consulta periodicamente agentes instalados nos dispositivos de rede, por meio de operações de leitura, para obter valores armazenados em uma base de informações de gerenciamento (MIB). Esse modelo de consulta periódica (*polling*) consome banda de gerenciamento proporcional à frequência das consultas e ao número de dispositivos monitorados.

A RFC 2819 define a MIB de RMON (*Remote Network Monitoring*), que estende esse modelo ao especificar uma sonda (*probe*) capaz de coletar e processar estatísticas localmente, no próprio segmento de rede monitorado, estruturando suas funcionalidades em diversos grupos de monitoramento e controle.

Fonte: RFC 2819, Remote Network Monitoring Management Information Base (IETF, maio de 2000).

A equipe de gerência de redes da DATAPREV monitora um enlace WAN de baixa capacidade que interliga o datacenter principal a uma agência remota. O *polling* SNMP tradicional, realizado a cada poucos segundos pela estação gerente, consome parte significativa da banda desse enlace, mesmo quando a interface opera dentro dos parâmetros normais. A equipe deseja configurar a sonda RMON instalada no roteador da agência para que a estação gerente seja notificada apenas quando a utilização da interface ultrapassar um limiar predefinido, sem depender de consultas SNMP constantes.

Assinale a opção que indica corretamente os grupos da RFC 2819 responsáveis por implementar esse comportamento e a respectiva dinâmica que reduz a dependência do *polling* tradicional.

- (A) Quando a sonda utiliza os grupos *alarm* e *event*, ela registra o cruzamento do limiar em um *log* local, e a estação gerente recupera essa informação no próximo ciclo de varredura, mantendo a dependência do *polling*.
- (B) Os grupos *alarm* e *event* permitem que a sonda monitore localmente a variável em relação ao limite configurado e envie uma notificação à estação gerente apenas quando esse limite é ultrapassado, sem depender de consultas SNMP constantes.
- (C) Apoiando-se no grupo *history*, que armazena periodicamente as amostras de tráfego, o grupo *alarm* depende desses registros para verificar se o limiar foi ultrapassado, dispensando a estação gerente de consultar a sonda a cada intervalo.
- (D) Estatísticas de tráfego por *host* e por par de endereços: essa é a contribuição dos grupos *hosts* e *matrix*, que concentram as informações na sonda e reduzem a frequência das consultas realizadas pela estação gerente.
- (E) O fato de selecionar e armazenar pacotes de interesse é a função dos grupos *filter* e *capture*, que assim substituem o *polling* da estação gerente pela captura contínua de tráfego na sonda.

67

Durante o planejamento de continuidade para um *data center* estratégico da DATAPREV, a equipe técnica debateu sobre os recursos de Tecnologia da Informação e Comunicação (TIC) necessários à continuidade das atividades prioritárias.

Com base nas diretrizes da ABNT NBR ISO 22313:2020 para requisitos de recursos de TIC, assinale a opção que apresenta uma ação recomendada para a organização.

- (A) Exigir a intervenção humana prioritária na restauração de serviços.
- (B) Concentrar a infraestrutura em um único ambiente de segurança máxima.
- (C) Descartar imediatamente equipamentos sistêmicos antigos que tenham sido substituídos.
- (D) Eliminar o uso de procedimentos manuais provisórios durante o restabelecimento dos sistemas.
- (E) Distribuir geograficamente as tecnologias, mantendo-as em diferentes localidades que não sejam afetadas pela mesma interrupção.

68

EX-AB1: uma estação de trabalho de um órgão governamental parceiro conectado à rede da DATAPREV foi infectada por um artefato malicioso.

Em poucos minutos, arquivos de banco de dados e documentos da rede local foram renomeados com extensões aleatórias e tornados ilegíveis. Paralelamente, os *logs* do sistema registraram a execução automatizada do comando `vssadmin.exe delete shadows / all /quiet`, visando inviabilizar a recuperação nativa do sistema operacional.

A análise do tráfego de rede confirmou que, antes da renomeação dos arquivos, os mesmos foram exfiltrados para uma infraestrutura externa. O único arquivo legível no diretório atacado continha uma nota de texto exigindo pagamento de resgate sob pena de vazamento público dos dados.

A descrição do incidente corresponde a uma infecção por

- (A) *Adware* invasivo com extorsão.
- (B) *Ransomware* com tática de dupla extorsão.
- (C) *Spyware* com sequestro leve de navegador.
- (D) *Botnet* sem controle de Comando e Controle.
- (E) *Rootkit* de *Firmware* com ataque de *Man-in-the-Middle*.

69

Uma equipe de TI, diante do acúmulo de demandas em andamento, adotou o método Kanban para visualizar o fluxo de trabalho e estabelecer limites de trabalho em andamento (WIP).

Sobre o método Kanban, assinale a afirmativa correta.

- (A) A existência de um limite de WIP impede a entrada de qualquer nova demanda enquanto houver ao menos uma atividade ainda não concluída no fluxo.
- (B) A adoção do Kanban exige que as demandas sejam agrupadas em ciclos de duração fixa, ao final dos quais todos os itens selecionados devem estar concluídos.
- (C) A utilização de um quadro Kanban torna desnecessário o acompanhamento do tempo de fluxo, pois a representação visual das atividades é suficiente para assegurar a melhoria contínua.
- (D) Os limites de WIP têm como finalidade assegurar que todos os integrantes da equipe permaneçam continuamente ocupados, ainda que isso implique aumentar a quantidade de demandas iniciadas.
- (E) O estabelecimento de limites de WIP restringe a quantidade de itens que podem permanecer simultaneamente em determinadas etapas do fluxo, contribuindo para evidenciar gargalos e favorecer a conclusão do trabalho iniciado.

70

Um engenheiro responsável pela segurança cibernética de uma sociedade empresária está analisando a utilização de mecanismos de detecção, prevenção e correlação de eventos de segurança no ambiente corporativo, avaliando, nesse contexto, as características de soluções HIDS, IPS e SIEM.

Com relação a essas soluções, analise as afirmativas a seguir e assinale (V) para a verdadeira e (F) para a falsa.

- () O HIDS monitora os segmentos de rede e analisa os pacotes que circulam pela infraestrutura em busca de padrões associados a ataques, emitindo alertas quando identifica atividades suspeitas.
- () O IPS, por operar de forma *inline*, pode bloquear ou descartar conexões consideradas suspeitas, diferentemente de um IDS configurado exclusivamente para monitoramento passivo, cuja função principal é identificar e alertar sobre possíveis intrusões.
- () O SIEM opera necessariamente de forma *inline* e substitui o IPS na função de bloquear ou descartar, em tempo real, o tráfego relacionado a eventos suspeitos.

As afirmativas são, respectivamente,

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

Realização

