CONCURSO PÚBLICO
MINISTÉRIO PÚBLICO DO ESTADO DO ESPÍRITO SANTO

NÍVEL SUPERIOR – MANHÃ

AGENTE ESPECIALIZADO
ANALISTA DE SEGURANÇA DA INFORMAÇÃO

PROVA OBJETIVA E DISCURSIVA
TIPO 1

SUA PROVA

Além deste caderno de questões contendo **60 (sessenta)** questões objetivas e **2 (duas)** questões discursivas, você receberá do fiscal de sala o cartão de respostas e a folha de textos definitivos.

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 e 30 (trinta) minutos** é o período disponível para a realização da prova, **já incluído o tempo para a marcação da folha de respostas** e o preenchimento da **folha de textos definitivos**.
- **3 (três) 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 e na folha de textos definitivos, 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 e na folha de textos definitivos.
- Confira o tipo do seu caderno de questões. Caso tenha recebido caderno de questões com tipo diferente do impresso em seu cartão de respostas ou em sua folha de textos definitivos, 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 ou da folha de textos definitivos em caso de erro cometido por você.
- Para fins de avaliação, serão levadas em consideração apenas as marcações realizadas no cartão de respostas e na folha de textos definitivos.
- Os candidatos serão submetidos ao sistema de detecção de metais quando do ingresso e da saída de sanitários durante a realização das provas.

Boa prova!

Conhecimentos Básicos
Língua Portuguesa

1

"Consideramos estas verdades como evidentes por si: que todos os homens são criados iguais; que são dotados pelo seu Criador de certos direitos inalienáveis; que entre esses direitos estão a vida, a liberdade e a procura da felicidade."

Thomas Jefferson, Declaração de Independência dos EUA. (1776)

Sobre a significação e a estruturação desse segmento, assinale a afirmativa correta.

(A) Os três direitos citados ao final do texto são todos os direitos inalienáveis dos homens.
(B) O fato de a forma verbal "Consideramos" estar no plural indica que são vários os autores do texto.
(C) O termo "estas verdades" se refere a algo dito anteriormente, que não está registrado neste segmento.
(D) Ao afirmar que "todos os homens são criados iguais", o texto indica que todos os homens têm os mesmos direitos.
(E) Ao dizer que as verdades citadas são "evidentes por si", o autor do texto indica que elas necessitam de demonstração.

2

"O direito de voto para eleger representantes é o direito básico pelo qual os demais são protegidos. Retirar esse direito equivale a reduzir a pessoa à escravidão, pois escravidão consiste em estar sujeito à vontade de outrem."

Thomas Paine. *Dissertação sobre os Primeiros Princípios do Governo.* (1795)

Sobre a significação ou a estruturação desse fragmento textual, assinale a afirmativa correta.

(A) O termo "para eleger representantes" poderia ser adequadamente substituído por "para a eleição de representantes".
(B) Ao dizer que o direito de voto é "o direito básico", o autor indica que a democracia é o melhor dos regimes.
(C) O termo "os demais" se refere a todas as demais pessoas.
(D) O termo "são protegidos" poderia ser passado para a voz ativa com a forma "pelo qual se protegiam".
(E) A parte final do texto mostra o entendimento pessoal que o autor do texto dá à palavra "escravidão".

3

"As leis são como as teias de aranha: as simples mosquinhas e as pequenas borboletas se prendem nelas, enquanto as grandes varejeiras malfazejas as rompem e passam através."

Sobre esse fragmento textual, assinale a afirmativa correta.

(A) A condenação expressa no texto se utiliza de linguagem lógica.
(B) O autor condena certas leis que não se dirigem a reais problemas da sociedade.
(C) O fragmento textual acima condena os privilégios de uma classe social sobre outras.
(D) No segmento "se prendem nelas", o pronome pessoal "elas" se refere às "simples mosquinhas".
(E) Segundo o texto, as leis são como teias de aranha porque servem para prender todos os que cometem crimes.

4

As frases a seguir têm as leis como tema; assinale a frase que mostra uma visão positiva das leis.

(A) Em meio às armas, calam-se as leis.
(B) Existem leis, mas não quem as proveja.
(C) O mais corrupto dos Estados tem o maior número de leis.
(D) A quem poderá ser aprazível uma cidade, se não lhe agradam as leis?
(E) A lei é a razão humana, enquanto governa todos os povos da Terra.

5

Leia o texto a seguir.

"Não devemos fazer da lei um espantalho / Armado para assustar a aves de rapina, / Mas deixado sempre estático, de modo que com o hábito / Ele não seja mais o terror delas, e sim o seu poleiro."

Shakespeare, William. ***Medida por Medida*** (Ato 2, Cena 1).

A afirmação correta sobre as leis, que está implícita no texto, é que elas devem

(A) proteger a todos.
(B) modificar-se conforme as circunstâncias.
(C) funcionar, devido ao medo que provocam.
(D) ser amplamente divulgadas entre os cidadãos.
(E) ajudar a todos em sua tarefa de obter alimentação.

6

Uma das marcas de um bom texto é a utilização de palavras em seu sentido adequado; assinale a opção em que a palavra sublinhada está adequadamente empregada.

(A) As leis <u>cumpridas</u> são difíceis de entender.
(B) É uma autoridade <u>eminente</u> e por isso ninguém o respeita.
(C) A lei tem dois e <u>apenas</u> dois fundamentos: a equidade e a utilidade.
(D) As leis são sempre úteis aos que <u>possuem</u> posses e nocivas aos que nada têm.
(E) Quando vou a um país, não examino se <u>tem</u> boas leis, mas se as que lá existem são executadas.

7

Assinale a opção que indica a frase que está rigorosamente dentro dos modelos da norma culta.

(A) Todos os convidados vestiam trajes à rigor.
(B) Os policiais estavam cara a cara com os delinquentes.
(C) Os promotores ficaram receiosos ante seus adversários.
(D) As festas beneficientes nem sempre produzem dinheiro.
(E) Entreguei a Constituição as advogadas para que ficassem bem-informadas.

8

As opções a seguir mostram duas formas corretas de uma mesma frase, ***<u>à exceção de uma</u>***. Assinale-a.

(A) Voltamos de Alagoas. / Voltamos das Alagoas.
(B) Vá até o tribunal e procure o Juiz. / Vá até ao tribunal e procure o Juiz.
(C) Houve um acidente grave durante o julgamento. / Houve um incidente grave durante o julgamento.
(D) A Constituição foi criada a 13 de junho de 1888. / A Constituição foi criada em 13 de junho de 1888.
(E) À exceção de Bernardo, todos estiveram presentes. / Com exceção de Bernardo, todos estiveram presentes.

9

Leia o segmento a seguir.

"Agora que expliquei o título, passo a escrever o livro. Antes disso, porém, digamos os motivos que me põem a pena na mão. Vivo só, com um criado. A casa em que moro é própria; fi-la construir de propósito, levado de um desejo tão particular, que me vexa imprimi-lo, mas vá lá.

Um dia, há bastantes anos, lembrou-me reproduzir no Engenho Novo a casa em que me criei na Rua de Matacavalos, dando-lhe o mesmo aspecto e economia daquela outra, que desapareceu."

Machado de Assis. *Dom Casmurro.* Livraria Garnier. 1ª ed. em 1899.

Sobre a estruturação ou a significação desse texto, assinale a afirmativa ***incorreta.***

(A) O segmento inicial "Agora que expliquei o título" se refere a algo já dito anteriormente.
(B) O pronome "isso", na expressão "Antes disso" se refere à ação de explicar o título do livro.
(C) O pronome relativo "que" no segmento "que me põem a pena na mão" se refere ao substantivo "motivos".
(D) A frase "Vivo só, com um criado" mudaria de sentido se retirássemos a vírgula.
(E) O pronome indefinido "outra" e o pronome relativo "que" no segmento "daquela outra, que desapareceu" mostram o mesmo antecedente.

10

Os segmentos textuais a seguir foram retirados do romance *Dom Casmurro.*

Assinale aquele que exemplifica o *modo descritivo* de organização discursiva.

(A) Agora que expliquei o título, passo a escrever o livro.
(B) Fiquei tão alegre com esta ideia, que ainda agora me treme a pena na mão.
(C) Ia entrar na sala de visitas, quando ouvi proferir o meu nome e escondi-me atrás da porta.
(D) Cumprimentou-se, sentou-se ao pé de mim, falou da lua e dos ministros e acabou recitando-me versos.
(E) Não consultes dicionários. *Casmurro* não está aqui no sentido que eles lhe dão, mas no que lhe pôs o vulgo de homem calado e metido consigo.

Raciocínio Lógico-matemático

11

Um sistema de criptografia atribuiu valores numéricos às letras do alfabeto. Cada letra recebeu um único valor. Letras distintas têm valores distintos.

Nesse sistema:

- a soma das letras da palavra NARA é 19;
- a soma das letras da palavra MARIA é 25;
- a soma das letras da palavra MAIARA é 27;
- a soma das letras da palavra MARIANA é 31.

Com base nessas informações, é correto afirmar que a valor atribuído a R foi

(A) 10.
(B) 11.
(C) 12.
(D) 13.
(E) 14.

12

A figura a seguir ilustra dois retângulos, *A* e *B*, dispostos lado a lado de duas formas diferentes.

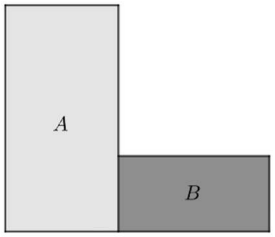

FIGURA 1

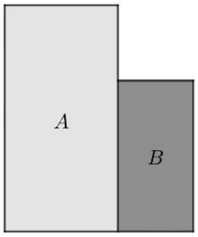

FIGURA 2

Na Figura 1, o menor lado de *B* está encostado no maior lado de *A*, de modo que o maior lado de *B*, na sua parte inferior, está perfeitamente alinhado com o menor lado de *A*, na sua parte inferior, formando uma figura em L cujo perímetro é 32 cm.

Na Figura 2, o maior lado de *B* está encostado no maior lado de *A*, de modo que o menor lado de *B*, na sua parte inferior, está perfeitamente alinhado com o menor lado de *A*, na sua parte inferior, formando uma nova figura cujo perímetro é 26 cm.

No retângulo *B*, a diferença entre as medidas do maior lado e do menor lado vale

(A) 7,5 cm.
(B) 6,0 cm.
(C) 4,5 cm.
(D) 3,0 cm.
(E) 1,5 cm.

13

Em um jogo, sorteiam-se ao acaso, sucessivamente e sem reposição, números do conjunto {1,2,3,4,5,6,7,8}. Cada jogador recebe uma cartela com 6 números distintos desse conjunto. Duas cartelas quaisquer nunca têm exatamente os mesmos 6 números.

A quantidade máxima de cartelas distintas que se pode ter nesse jogo é

(A) 28.
(B) 36.
(C) 42.
(D) 48.
(E) 56.

14

O "grau" do álcool doméstico indica a concentração de etanol presente na mistura com água. No Brasil, essa medida é expressa em **INPM.** Por exemplo, o álcool 46° INPM possui, a cada 100 gramas de produto, 46 gramas de etanol e 54 gramas de água e outros componentes.

Misturando-se 200g de álcool 46° INPM com 300 gramas de álcool 70° INPM, produz-se 500g de álcool com concentração INPM igual a

(A) 59,4°.
(B) 59,6°.
(C) 59,8°.
(D) 60,2°.
(E) 60,4°.

15

Considere a proposição *P* dada por:

"*Pelo menos um livro da minha biblioteca é sobre Matemática e nenhum dos discos da minha discoteca é importado*."

Assinale a opção que contém a negação de *P*.

(A) Pelo menos um livro da minha biblioteca não é sobre Matemática e algum disco da minha discoteca é importado.
(B) Pelo menos um livro da minha biblioteca não é sobre Matemática ou algum disco da minha discoteca é importado.
(C) Pelo menos um livro da minha biblioteca não é sobre Matemática e todos os discos da minha discoteca são importados.
(D) Nenhum livro da minha biblioteca é sobre Matemática ou algum disco da minha discoteca é importado.
(E) Nenhum livro da minha biblioteca é sobre Matemática e algum disco da minha discoteca é importado.

Legislação e Código de Ética do MPES

16

João, servidor do Ministério Público do Estado do Espírito Santo, foi promovido e passou a ocupar uma classe distinta daquela que ocupava, o que levou ao seu enquadramento na nova situação da carreira.

À luz dessa constatação, é correto afirmar que João

(A) alcançou o vigésimo nível da classe anterior.
(B) passou a ocupar o nível inicial da classe atual.
(C) preencheu os requisitos da promoção por merecimento.
(D) foi promovido em razão da existência de vaga na nova classe.
(E) obteve o padrão temporal mínimo de 2 (dois) anos na classe anterior.

17

Determinada estrutura orgânica do Ministério Público do Estado do Espírito Santo entendeu que seria necessária a revisão de uma meta do Plano Estratégico (PE) da Instituição.

Ao analisar os balizamentos estabelecidos pela Portaria nº 8.565/2017, a referida estrutura concluiu, corretamente, que

(A) a revisão somente é admitida em relação aos indicadores, não em relação às metas.
(B) a Assessoria de Gestão Estratégica deve exarar manifestação técnica sobre a proposta.
(C) o PE é caracterizado pela estabilidade e permanência, sendo incompatível com o instituto da revisão.
(D) a revisão somente é admitida em relação aos indicadores e às ações estratégicas, não em relação às metas.
(E) o início do processo de revisão deve ser autorizado na reunião de gestão estratégica, cabendo a deliberação final e irrecorrível à plenária.

18

O Ministério Público do Estado do Espírito Santo, pelo órgão de execução com atribuição, pretende realizar operações de classificação e avaliação de dados pessoais de alguns investigados em procedimentos de investigação criminal que tramitam no âmbito da Instituição.

Ao decidir pela realização dessas atividades, o órgão de execução concluiu, corretamente, que

(A) a atividade desenvolvida configura tratamento da informação, logo, por tal razão, é exigida a observância da Lei Geral de Proteção de Dados Pessoais.
(B) o tratamento da informação, nas circunstâncias indicadas, pressupõe prévia autorização judicial, como é exigido pela Lei Geral de Proteção de Dados Pessoais.
(C) a atividade desenvolvida somente atrairia a aplicação da Lei Geral de Proteção de Dados Pessoais se houvesse tratamento de dados pessoais, o que não é o caso.
(D) a Lei Geral de Proteção de Dados Pessoais é aplicada indistintamente a qualquer atividade que tenha por objeto dados pessoais, independente da sua natureza.
(E) o tratamento de dados pessoais é realizado no âmbito de uma atividade de investigação de infração penal, o que afasta a incidência da Lei Geral de Proteção de Dados Pessoais.

19

Ana, servidora ocupante de cargo em comissão no âmbito do Ministério Público do Estado do Espírito Santo (MPES), foi informada sobre uma reunião que seria realizada pelo conselho responsável pela gestão do Fundo Estadual de Reparação de Interesses Difusos Lesados, que teria uma pauta de grande relevância para a atuação finalística da Instituição.

Ao delinear as medidas de apoio que tinha o *munus* de adotar na referida reunião, Ana partiu da premissa correta de que o Fundo

(A) conta com a atuação de representante do MPES em seu conselho, apesar de integrar a estrutura do Poder Executivo.
(B) integra a estrutura do MPES, sendo que o seu conselho conta com a participação de membros da Instituição, do Poder Executivo e de associações.
(C) é estrutura autônoma e independente, cuja atuação é fiscalizada pelo MPES, que participa das reuniões do seu conselho sem ter direito a voto.
(D) é parte integrante do Fundo Especial do MPES, sendo que os seus recursos estão finalisticamente comprometidos com a defesa de interesses difusos e coletivos.
(E) conta com representantes dos três poderes e instituições constitucionalmente autônomas, bem como com representantes da sociedade civil organizada, sendo presidido pelo Procurador-Geral de Justiça.

20

No primeiro mês do exercício financeiro X, Inês, que atua em um setor de controle interno do Ministério Público do Estado do Espírito Santo (MPES), recebeu a informação de que a Instituição recebera recursos previstos na lei orçamentária anual (LOA) aprovada pela Assembleia Legislativa.

Sobre a situação descrita, à luz da Lei Complementar Estadual nº 95/1997, assinale a afirmativa correta.

(A) Os recursos foram postos à disposição em duodécimo.
(B) A LOA foi aprovada a partir de projeto de lei apresentado pelo MPES.
(C) Os recursos foram depositados no Fundo de Despesas Correntes do MPES.
(D) Os recursos recebidos estão vinculados a despesas e a cotas definidas na programação financeira.
(E) Os recursos foram solicitados à Secretaria de Estado de Fazenda mediante comprovação das despesas a serem realizadas.

Conhecimentos Específicos

21

Uma empresa de Tecnologia da Informação decidiu implementar um Sistema de Gestão da Qualidade baseado na ISO 9001 para melhorar a confiabilidade de seus serviços e a satisfação dos clientes.

Com base nos requisitos e boas práticas de gestão de serviços de TI, analise as afirmativas a seguir e assinale (V) para a verdadeira e (F) para a falsa.

( ) O registro estruturado de chamados e a análise de causa raiz de incidentes contribuem para a melhoria contínua dos processos e para a tomada de decisão baseada em evidências.
( ) Na gestão de infraestrutura de TI, processos como controle de mudanças e gestão de configuração contribuem para a estabilidade operacional e para a rastreabilidade das alterações no ambiente tecnológico.
( ) O controle de versões no desenvolvimento de *software* constitui uma ferramenta operacional de apoio aos desenvolvedores, não sendo relevante para os requisitos de controle de informação documentada previstos na ISO 9001.

As afirmativas são, respectivamente,

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

22

Em relação ao uso de OKRs e KPIs em uma sociedade empresária que desenvolve soluções digitais, assinale a afirmativa correta.

(A) Os OKRs acompanham performance contínua de serviços de TI.
(B) Os KPIs substituem integralmente os OKRs em um modelo de gestão orientado por resultados.
(C) Os KPIs possuem caráter estratégico e são definidos em ciclos periódicos, normalmente trimestrais.
(D) Os KPIs são utilizados para definir metas de transformação e inovação, enquanto os OKRs monitoram a estabilidade dos processos operacionais.
(E) Os OKRs em TI promovem o alinhamento estratégico e a transparência, permitindo que as equipes foquem em resultados de alto impacto e compartilhem seus objetivos com toda a organização.

23

Em relação aos requisitos de qualidade em TI, analise as afirmativas a seguir.

I. A *eficiência de desempenho* refere-se ao uso adequado de recursos de *hardware* e rede.
II. A *autenticação forte* e a *criptografia de dados* são consideradas requisitos de segurança para proteção contra acessos não autorizados.
III. A *usabilidade* diz respeito à operação sem falhas frequentes.

Está correto o que se afirma em

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

24

No contexto de redes de computadores, existem dois modelos de referência consagrados na literatura: o modelo OSI e o modelo TCP/IP (ou arquitetura TCP/IP).

Com relação aos dois modelos, analise as afirmativas a seguir e assinale (V) para a verdadeira e (F) para a falsa.

( ) Os dois modelos se baseiam no conceito de camadas de protocolos independentes.
( ) O modelo TCP/IP não contempla o uso do protocolo UDP (User Datagram Protocol).
( ) Uma das funções precípuas da camada de enlace de dados do modelo OSI é o controle de congestionamento.

As afirmativas são, respectivamente,

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

25

Com relação aos conceitos de topologias de redes de computadores e seus equipamentos, analise os itens a seguir.

I. O *switch* é o elemento responsável pela escolha de caminhos do tráfego de dados em redes WAN.

II. Em redes LAN, o *switch* encaminha dados com base em endereços IP.

III. O roteador é um dispositivo que interconecta LAN e WAN.

Analise as afirmativas a seguir.

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

26

Durante uma vistoria na infraestrutura de rede do edifício-sede, o analista identificou que as ligações VoIP do setor jurídico apresentavam perda de pacotes nos horários de maior acesso de visitantes à rede Wi-Fi.

A análise revelou que os três perfis de usuário — administrativo, VoIP e visitantes — compartilhavam o mesmo domínio de *broadcast*. A solução adotada foi segmentar logicamente o tráfego nos *switches* existentes, sem aquisição de novos equipamentos, e configurar o enlace entre o *switch* de distribuição e o roteador central para transportar os três grupos simultaneamente.

Sobre o funcionamento desse enlace, assinale a afirmativa correta.

(A) Cada quadro Ethernet recebe uma marcação de 4 *bytes* com o identificador do grupo ao qual pertence, permitindo que o roteador processe cada fluxo de forma isolada.
(B) O *switch* encapsula os quadros de cada grupo em pacotes IP distintos antes de encaminhá-los ao roteador, que os desencapsula e aplica as políticas de segurança.
(C) A marcação do tráfego ocorre no cabeçalho IP, onde um campo específico identifica a qual segmento lógico o pacote pertence, sendo interpretado pelo roteador central.
(D) O enlace entre *switch* e roteador opera com múltiplos endereços MAC virtuais, um para cada grupo, sendo o roteamento feito com base nos identificadores de camada 2.
(E) A separação dos grupos é feita pelo roteador central por meio da leitura das portas TCP de destino em cada pacote, que são mapeadas para interfaces lógicas distintas.

27

O MPES registrou reclamações recorrentes de lentidão nos sistemas processuais e travamentos durante audiências virtuais, especialmente entre 9 e 12 horas. A análise técnica apontou saturação dos *links* MPLS nos horários de pico. Uma das propostas foi a adição de *links* de internet com gerenciamento SD-WAN.

Sobre a tecnologia SD-WAN, assinale a afirmativa correta.

(A) Ela permite direcionar cada fluxo de dados pelo caminho mais adequado, medindo a qualidade dos *links* em tempo real.
(B) Ela melhora o desempenho ao comprimir pacotes na camada física, reduzindo o tempo de transmissão nos *links* MPLS.
(C) Ela atua substituindo os equipamentos MPLS por roteadores com tabelas de roteamento estático pré-configuradas.
(D) Ela depende exclusivamente de *links* MPLS para funcionar, sendo inoperante sobre conexões de internet convencional.
(E) Ela opera como um protocolo de camada 2, utilizando comutação de rótulos para priorizar o tráfego crítico.

28

Em uma rede sem fio corporativa usada também para ramais VoIP, a equipe técnica decidiu empregar autenticação individualizada de usuários, mantendo criptografia adequada para proteção do tráfego na WLAN.

Nesse contexto, assinale a opção que distingue corretamente as propriedades do EAP e do WPA2.

(A) O EAP é responsável por criptografar diretamente os quadros de dados transmitidos na WLAN; o WPA2 define mecanismos de proteção para redes sem fio baseados no IEEE 802.11i.
(B) O EAP é um protocolo de roteamento usado para encaminhar pacotes entre redes sem fio; o WPA2 pode empregar criptografia para proteger o tráfego transmitido na WLAN.
(C) O EAP pode ser utilizado em ambientes corporativos para autenticação de usuários; o WPA2 não oferece mecanismos de confidencialidade, atuando apenas na identificação do SSID da rede.
(D) O EAP possui uma estrutura que permite o uso de diferentes métodos de autenticação; o WPA2 utiliza mecanismos de segurança baseados no padrão IEEE 802.11i, com criptografia forte, como AES/CCMP.
(E) O EAP permite o uso de métodos variados de autenticação em redes de acesso; o WPA2 é utilizado exclusivamente para autenticação por endereço MAC, sem emprego de criptografia de dados.

29

Um analista está implementando um *pipeline* no *Logstash*, da pilha ELK, para tratar registros de acesso HTTP oriundos de um servidor *Apache*.

Para isso, foi utilizada a seguinte configuração de filtro:

```
filter                                                              {
 grok                                                               {
  match                                 =>                          {
   "message" => "%{IP:client_ip} - - \[%{HTTPDATE:raw_date}\]
\"%{WORD:http_method}                %{URIPATHPARAM:request}
HTTP/%{NUMBER:http_version}\"        %{NUMBER:status_code}
%{NUMBER:bytes}"
  }
 }

 date                                                               {
  match => [ "raw_date", "dd/MMM/yyyy:HH:mm:ss Z" ]
 }

 mutate                                                             {
  convert    =>    {    "status_code"    =>    "integer"    }
  rename     =>    {    "client_ip"      =>    "[source][ip]"    }
 }
}
```

Considere que uma linha de entrada válida seja:

192.168.1.10 - - [22/Mar/2026:14:09:58 +0000] "GET /index.php HTTP/1.1" 200 5120

Com base no funcionamento do *Logstash* e dos *plugins* utilizados, com a específica configuração e sintaxe apresentados, assinale a afirmativa correta.

(A) O *plugin date* converte o campo *raw_date* em inteiro *epoch*, sobrescrevendo automaticamente o campo *status_code*, desde que o *grok* tenha sido executado com sucesso.

(B) Após o processamento, o campo *client_ip* permanece no evento e, adicionalmente, é copiado para o campo aninhado *[source][ip],* já que a operação *rename* não remove o campo original.

(C) O campo *status_code* será convertido para tipo numérico inteiro, enquanto o campo *bytes* permanecerá textual, salvo conversão adicional explícita.

(D) O padrão %{*URIPATHPARAM:request*} captura exclusivamente o caminho da URI, mas nunca parâmetros de consulta (*query string*), razão pela qual o filtro falharia caso a URL contenha ?id=10.

(E) O *plugin grok* já converte automaticamente os campos %{*NUMBER:status_code*} e %{*NUMBER:bytes*} para tipo numérico, tornando redundante o uso de *mutate* { *convert* => ... }.

30

Em um ambiente de microsserviços, uma aplicação expõe a métrica:

*http_requests_total{job="api", instance="*10.0.0.5:8080", *method="GET", code*="500"}

A equipe deseja calcular, no Prometheus, a taxa média por segundo de crescimento dessa métrica ao longo dos últimos 5 minutos, suavizada ao longo da janela de tempo completa, para alimentar um painel de erro no Grafana.

Assinale a opção que apresenta a expressão em PromQL conceitualmente mais adequada para esse objetivo.

(A) delta(http_requests_total[5m])

(B) rate(http_requests_total[5m])

(C) irate(http_requests_total[5m])

(D) avg_over_time(http_requests_total[5m])

(E) count_over_time(http_requests_total[5m])

31

Uma equipe de redes deseja monitorar a utilização de CPU de um roteador utilizando SNMP no Zabbix.

Para isso, foi configurado um item com os seguintes parâmetros:

- Tipo: SNMP agent
- OID: .1.3.6.1.2.1.25.3.3.1.2.1

Sabe-se que o dispositivo suporta SNMP e que o OID retorna um valor numérico correspondente ao uso de CPU.

Considerando o funcionamento do Zabbix, do SNMP e dos OIDs, assinale a afirmativa correta.

(A) O Zabbix utiliza esse OID para realizar *scraping* contínuo via *push,* sem necessidade de *polling.*

(B) O valor retornado pelo OID é interpretado como texto e não pode ser usado em *triggers* numéricas.

(C) O uso de OIDs elimina a necessidade de *triggers,* pois o SNMP já fornece alertas diretamente ao Zabbix.

(D) O OID representa um endereço IP do dispositivo monitorado, sendo usado para identificação do *host.*

(E) O Zabbix consulta periodicamente o OID via SNMP, caracterizando um modelo de *polling* para coleta de métricas.

32

Considere os seguintes *logs* coletados durante o processamento de requisições em um sistema distribuído de *e-commerce*.

</> JSON

{"time":"10:01:02","service":"gateway","level":"INFO","message":"Requisição recebida","request_id":"abc123"}
{"time":"10:01:02","service":"A","level":"INFO","message":"Pedido recebido","request_id":"abc123"}
{"time":"10:01:03","service":"B","level":"INFO","message":"Processando pagamento","request_id":"abc123"}
{"time":"10:01:03","service":"C","level":"ERROR","message":"Erro no estoque","request_id":"abc123"}
{"time":"10:01:04","service":"B","level":"WARN","message":"Retry pagamento","request_id":"abc123"}
{"time":"10:01:05","service":"D","level":"INFO","message":"Notificação enviada","request_id":"abc123"}
{"time":"10:01:06","service":"gateway","level":"ERROR","message":"Falha na requisição","request_id":"abc123"}

Durante a análise de um incidente, a equipe conseguiu reconstruir o fluxo completo da requisição entre os diferentes serviços envolvidos, identificando o ponto exato de falha e as tentativas de recuperação.

Nesse cenário, assinale a opção que identifica corretamente a prática de estruturação de *logs* que foi determinante para viabilizar essa análise.

(A) Separação dos *logs* por serviço, facilitando a análise individualizada de cada componente.
(B) Inclusão de níveis de severidade nos registros, possibilitando a priorização dos eventos relevantes.
(C) Registro de *timestamps* consistentes entre os serviços, viabilizando a ordenação cronológica dos eventos.
(D) Padronização do formato dos *logs* em estrutura JSON, permitindo a indexação e a consulta eficiente dos registros.
(E) Utilização de identificador único de requisição propagado entre os serviços, permitindo a correlação determinística dos eventos.

33

Considerando as diretrizes da Lei Geral de Proteção de Dados (LGPD) em relação à Segurança da Informação, assinale a afirmativa correta.

(A) A LGPD não classifica informações sobre religião e dados relacionados à saúde como dados pessoais sensíveis.
(B) A criptografia é citada na LGPD como uma medida técnica obrigatória para todos os tipos de tratamento de dados pessoais.
(C) A LGPD permite o tratamento de dados pessoais sem medida de segurança, quando forem utilizados apenas internamente pela organização.
(D) O princípio da Prevenção na LGPD estabelece que os agentes de tratamento devem adotar medidas para prevenir a ocorrência de danos decorrentes do tratamento de dados pessoais.
(E) A LGPD determina que, em caso de incidente de segurança que possa acarretar risco aos titulares, o controlador deverá comunicar à Autoridade Nacional de Proteção de Dados (ANPD), não havendo necessidade de comunicar ao titular.

34

Considerando a classificação de riscos e o tratamento dos riscos, analise o cenário a seguir.

Uma sociedade empresária de Segurança da Informação identificou um risco relacionado aos Testes de Software, classificado com probabilidade 5 (muito alto) e Impacto 4 (alto) em sua matriz de riscos.

Sobre o nível de risco e a estratégia mais adequada para tratá-lo, assinale a afirmativa correta.

(A) Trata-se de um risco alto, não sendo necessária a elaboração de Plano de contingência e estratégia de tratamento.
(B) Trata-se de um risco médio, sendo adequada uma estratégia de mitigação, com ações para reduzir a probabilidade ou o impacto do risco.
(C) Trata-se de um risco médio, que deve ser transferido para um fornecedor externo especializado, apesar do custo / benefício adequado.
(D) Trata-se de um risco extremo, exigindo a estratégia de evitação, com paralisação imediata das atividades de teste até que o risco seja completamente eliminado.
(E) Trata-se de um risco extremo, sendo adequada uma estratégia de mitigação, com ações para reduzir a probabilidade de ocorrência ou minimizar o impacto, em razão do custo / benefício adequado.

35

No contexto da segurança da informação, os controles podem ser classificados em físicos e lógicos, conforme sua natureza e forma de atuação.

Considerando esse contexto, assinale a afirmativa correta.

(A) O *firewall* é um mecanismo de segurança física voltado à proteção do perímetro organizacional.
(B) A autenticação por senha é um mecanismo de segurança física, pois restringe o acesso aos equipamentos computacionais.
(C) A criptografia de dados, o registro de logs e os mecanismos de auditoria são exemplos de controles de segurança física, pois atuam na proteção da infraestrutura.
(D) A proteção ambiental de instalações críticas e a política de descarte seguro de mídias digitais constituem, respectivamente, controles de segurança lógica e de segurança física.
(E) O uso de *tokens* FIDO2 para autenticação de usuários em sistemas corporativos e a instalação de câmeras de monitoramento (CFTV) em *data centers* constituem, respectivamente, controles de segurança lógica e de segurança física.

36

No contexto da segurança da informação e da proteção de dados pessoais (LGPD), a classificação da informação é um processo crítico para a gestão de riscos.

Sobre esse tema, assinale a afirmativa correta.

(A) A classificação de um ativo de informação deve ser imutável ao longo de todo o seu ciclo de vida, desde a criação até o descarte.

(B) O processo de classificação permite a aplicação de controles de segurança proporcionais ao valor da informação e ao impacto potencial de sua divulgação indevida.

(C) De acordo com a LGPD, todos os dados pessoais devem ser classificados como "Confidenciais", independentemente de serem dados comuns ou sensíveis.

(D) A responsabilidade pela atribuição do nível de classificação de uma informação cabe exclusivamente ao Encarregado de Dados (DPO).

(E) Informações classificadas como "Uso Interno" são aquelas cujo acesso é livre para qualquer cidadão, desde que solicitadas via Lei de Acesso à Informação (LAI).

37

A Gestão de Identidades e Acesso (IAM – *Identity and Access Management)* é considerada um dos pilares da segurança da informação e da governança de TI.

Com base nesse contexto, analise as afirmativas a seguir.

I. Modelos de controle de acesso baseados em papéis (RBAC) e em atributos (ABAC) são utilizados em IAM para definir e restringir permissões de acesso a sistemas e dados organizacionais.

II. A autenticação multifatorial (MFA) pode ser dispensada para contas administrativas em ambientes críticos, uma vez que o uso de múltiplos fatores pode comprometer a agilidade da resposta a incidentes de infraestrutura.

III. Os princípios de menor privilégio e de segregação de funções são considerados boas práticas de segurança da informação, contribuindo para a redução de riscos de acesso indevido ou abuso de privilégios.

Está correto o que se afirma em

(A) II, apenas.

(B) I e II, apenas.

(C) I e III, apenas.

(D) II e III, apenas.

(E) I, II e III.

38

No contexto da gestão de riscos em segurança da informação, a *Gestão de Identidades e Acessos* (IAM) é estruturada para mitigar riscos operacionais e de conformidade.

Sobre o tema, avalie as afirmativas a seguir e assinale (V) para a verdadeira e (F) para a falsa.

( ) O provisionamento automatizado de acessos eleva a eficiência operacional, reduzindo erros operacionais e aumentando a consistência na atribuição de permissões.

( ) A adoção de mecanismos de *Single Sign-On* em ambientes corporativos dispensa a necessidade de auditoria e rastreabilidade de acessos, uma vez que a autenticação ocorre de forma centralizada.

( ) O modelo de controle de acesso *Attribute-Based Access Control* utiliza atributos como localização, horário, perfil do usuário ou tipo de dispositivo para determinar a autorização de acesso a recursos de TI.

As afirmativas são, respectivamente,

(A) V – V – V.

(B) V – V – F.

(C) F – F – V.

(D) V – F – F.

(E) V – F – V.

39

Em relação à utilização dos Métodos de Autenticação Multifatorial (MFA) em ambientes corporativos e às boas práticas de segurança da informação, assinale a afirmativa correta.

(A) O uso de chaves físicas baseadas no padrão FIDO2 apresenta nível de segurança intermediário, sendo recomendado apenas para ambientes de baixo risco.

(B) A implementação de MFA em todos os sistemas corporativos dispensa a necessidade de auditoria de acessos e monitoramento de eventos de autenticação.

(C) A autenticação multifatorial exige a combinação de fatores pertencentes a categorias distintas, como "*algo que o usuário sabe*", "*algo que ele possui*" ou "*algo que ele é*".

(D) O uso de mecanismos biométricos garante proteção absoluta contra falsificação de identidade, uma vez que se baseia em fatores de inerência exclusivos de cada indivíduo.

(E) O envio de códigos de autenticação por SMS é considerado um método altamente seguro de MFA, por ser imune a ataques de interceptação de rede e engenharia social.

40

Uma instituição pública está revisando seus controles de acesso. O objetivo é permitir que servidores utilizem uma única identidade corporativa para acessar diferentes sistemas internos, reforçar a autenticação em acessos sensíveis e limitar privilégios administrativos apenas ao período necessário para execução de tarefas críticas.

Nesse cenário, uma implementação adequada de IAM (*Identity and Access Management*) consiste em

(A) implementar SSO (*Single Sign-On*) como mecanismo de autorização granular, pois ele substitui controles como RBAC (*Role-Based Access Control*), ABAC (*Attribute-Based Access Control*) e PAM (*Privileged Access Management*) na definição de privilégios de acesso.
(B) substituir o MFA (*Multi-Factor Authentication*) por senhas complexas, pois a autenticação multifator é incompatível com ambientes de SSO e dificulta a integração entre sistemas corporativos.
(C) adotar SSO para centralizar a autenticação, MFA para reforçar acessos sensíveis, RBAC ou ABAC para controle de autorização e PAM para gerenciar acessos privilegiados.
(D) utilizar PAM para autenticar todos os usuários comuns da organização, dispensando o uso de políticas de autorização como RBAC ou ABAC.
(E) aplicar RBAC exclusivamente para criptografar credenciais armazenadas, deixando a concessão de permissões a cargo de cada usuário final.

41

O OWASP Top 10:2025 apresenta as principais categorias de riscos de segurança em aplicações web, incluindo falhas relacionadas à manipulação inadequada de entradas fornecidas pelo usuário.

Uma aplicação web, hospedada no endereço http://www.eth0123.com, permite acesso a informações jornalísticas por meio do seguinte endereço:

" *http://www.eth0123.com/acesso.php?arq=jornal* "

Durante uma análise de segurança, verificou-se que o parâmetro "*arq"* é utilizado pela aplicação para carregar conteúdos armazenados no servidor. Em razão de falha na validação de entradas fornecidas pelo usuário, foi possível manipular o endereço de acesso conforme apresentado abaixo, permitindo visualizar o conteúdo de um arquivo sensível do sistema:

http://www.eth0123.com/acesso.php?arq=../../etc/passwd

Assinale a opção que apresenta, corretamente, a técnica de exploração usada nesse cenário.

(A) SQL *Injection.*
(B) LFI – *Local File Inclusion.*
(C) XSS – *Cross-Site Scripting.*
(D) FPD – *Full Path Disclosure.*
(E) RFI – *Remote File Inclusion.*

42

A criptografia é pilar fundamental da segurança da informação. A sua utilização correta permite que diversas aplicações sejam feitas de forma segura e mantenha os dados seguros e longe do acesso por partes indevidas.

Quanto ao uso de *criptografia*, assinale a afirmativa correta.

(A) A *Quântica* (por exemplo, BB84) utiliza os fenômenos quânticos no processo de troca de chaves, o que permite a detecção da interceptação da chave trocada com alta probabilidade.
(B) A *Assimétrica* (por exemplo, RSA) é usada para garantir o sigilo nas comunicações do TLS (Transport Layer Security) por ser bastante eficiente.
(C) A *Simétrica* (por exemplo, AES) é usada quando se quer garantir o sigilo e a autenticidade nas comunicações.
(D) A de *Curvas Elípticas* (por exemplo, ECC) ainda encontra resistência no seu uso, pois gera chaves maiores, entretanto é eficiente.
(E) A *pós-Quântica* (por exemplo, Kyber) utiliza algoritmos simétricos mais eficientes e rápidos no contexto emergente da computação quântica.

43

Com relação à *Gestão de Continuidade de Negócios* (GCN), assinale a afirmativa correta.

(A) O *Disaster Recovery Plan* (DRP) define o RTO (tempo de parada) e o RPO (perda de dados) para cada serviço.
(B) A *Business Impact Analysis* (BIA) é voltada à recuperação de sistemas e infraestrutura de TI, sendo parte integrante da estratégia de continuidade do negócio.
(C) O *Plano de Continuidade de Negócio* (BCP) abrange exclusivamente os sistemas de TI, sendo responsável pela restauração técnica dos serviços após incidentes.
(D) A *Business Impact Analysis* (BIA) tem como finalidade identificar processos críticos e avaliar os impactos decorrentes de sua interrupção, subsidiando a definição de prioridades de recuperação.
(E) O *Business Continuity Plan* (BCP) e o *Disaster Recovery Plan* (DRP) não possuem relação de dependência, sendo o DRP focado em processos manuais de negócio e o BCP focado na restauração de servidores.

44

No contexto da gestão de serviços de Tecnologia da Informação (TI), os diferentes tipos de *backup* apresentam características específicas quanto à forma de armazenamento e ao processo de restauração.

Sobre o tema, assinale a afirmativa correta.

(A) O *backup* diferencial armazena apenas as alterações realizadas desde o último *backup*, independentemente de sua natureza.
(B) O *backup* completo (*full*) permite a restauração mais rápida dos dados e dispensa a adoção de estratégias de contingência.
(C) O *backup* diferencial apresenta como principal vantagem a maior rapidez em sua execução quando comparado aos demais tipos de *backup.*
(D) O *backup* incremental armazena apenas os dados modificados desde o último *backup* completo ou incremental, exigindo a utilização de todos os incrementos para a restauração dos dados.
(E) O *backup* incremental armazena apenas as alterações realizadas desde o último *backup* completo e, por exigir poucos conjuntos de dados, garante a restauração mais rápida entre todos os tipos de *backup.*

45

No contexto da elaboração de documentos técnicos na área de Tecnologia da Informação, analise os itens a seguir.

I. O *Parecer Técnico* é o instrumento adequado quando se exige de um Analista de TI uma análise de conformidade das funcionalidades entregues frente ao Termo de Referência, visando subsidiar a decisão de pagamento de uma fatura contratual.

II. O *Laudo Técnico* é o documento recomendado para o registro de constatações objetivas resultantes de um exame pericial ou de uma auditoria de segurança em sistemas.

III. O *Laudo Técnico* possui natureza predominantemente opinativa e conclusiva, enquanto o *Parecer Técnico* possui natureza essencialmente descritiva e fática.

Está correto o que se afirma:

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

46

No que tange à elaboração de *laudos técnicos*, assinale a afirmativa correta.

(A) O laudo técnico caracteriza-se predominantemente por seu caráter opinativo, baseado na interpretação do profissional responsável.
(B) A seção de identificação do laudo técnico é facultativa, podendo ser dispensada quando o documento se destinar ao uso interno da organização.
(C) A seção de conclusão pode conter opiniões de caráter subjetivo, ainda que não estejam fundamentadas nas evidências obtidas durante a análise técnica.
(D) A metodologia deve explicitar os procedimentos, as técnicas, ferramentas e normas adotadas, de modo a permitir a reprodutibilidade e a verificação dos resultados.
(E) O escopo (ou objetivo) do laudo técnico deve ser definido ao final do documento, após a análise dos dados, a fim de refletir com maior precisão os resultados obtidos.

47

Em relação à Legislação e aos aspectos éticos na área de Tecnologia da Informação, assinale a afirmativa correta.

(A) Um analista de TI que, durante atividade de manutenção, copia documentos estratégicos da organização para dispositivo pessoal, ainda que sem intenção de obter vantagem, incorre em violação do sigilo profissional e da responsabilidade técnica.
(B) A Responsabilidade Técnica limita-se à garantia de que os sistemas estejam disponíveis, não abrangendo as falhas de configuração que resultem em acessos indevidos.
(C) O profissional de TI pode compartilhar dados internos da organização, desde que não haja identificação direta dos titulares das informações.
(D) O dever de sigilo profissional cessa após o desligamento do colaborador, exceto se houver cláusula contratual específica de não divulgação.
(E) A Ética Profissional em TI foca na eficiência técnica dos algoritmos, sendo as questões de privacidade de responsabilidade do setor jurídico.

48

Um agente técnico-estatístico na área de Tecnologia da Informação está elaborando um relatório para avaliar o desempenho de um sistema corporativo de gestão de serviços digitais. Para isso, ele utiliza dados oficiais de bases institucionais, como registros de chamados, tempo de resposta, disponibilidade do sistema e índices de satisfação dos usuários.

Com base na utilização de estatísticas oficiais e na construção de indicadores de desempenho em ambientes de TI na Administração Pública, assinale a afirmativa correta.

(A) Os indicadores de desempenho em TI devem ser usados apenas para fins operacionais, não sendo adequados para avaliação estratégica de serviços públicos digitais.
(B) Os indicadores de desempenho permitem avaliar a eficiência e a qualidade dos serviços de TI, apoiando a tomada de decisão e a melhoria contínua dos sistemas.
(C) Os indicadores estatísticos em TI não podem ser usados para comparações entre diferentes períodos, devido à variabilidade dos sistemas tecnológicos.
(D) Os relatórios estatísticos na área de TI devem apresentar exclusivamente dados técnicos, sem interpretação ou análise gerencial.
(E) A utilização de dados institucionais limita a criação de novos indicadores de desempenho em ambientes de TI.

49

No que tange às contratações de bens e serviços de Tecnologia da Informação (TI), conforme as disposições da Lei nº 14.133/2021, analise as afirmativas a seguir.

I. Nas contratações de TI, a Administração poderá definir o objeto da licitação com base exclusiva em marca ou modelo específico, desde que isso facilite a padronização tecnológica da organização.

II. O Diálogo Competitivo é uma modalidade de licitação que pode ser aplicada em projetos de TI que envolvam inovação tecnológica ou quando a Administração não consegue definir, com precisão suficiente, as especificações técnicas do objeto.

III. A contratação de soluções de TI deverá priorizar, sempre que possível, especificações baseadas em desempenho ou requisitos funcionais, evitando restrições indevidas à competitividade.

Está correto o que se afirma em

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

50

No contexto da gestão e fiscalização de contratos administrativos previstos na Lei nº 14.133/2021, avalie as afirmativas a seguir e assinale (V) para a verdadeira e (F) para a falsa.

( ) As contratações públicas deverão submeter-se a duas linhas de defesa, estruturadas para promover práticas contínuas e permanentes de gestão de riscos e controle preventivo na Administração Pública.

( ) Na fiscalização contratual poderão ser considerados critérios como a oportunidade, a materialidade, a relevância e o risco.

( ) A execução do contrato deverá ser acompanhada e fiscalizada por apenas um fiscal de contrato, responsável por todas as atividades de controle da execução contratual.

As afirmativas são, respectivamente,

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

51

No que diz respeito à gestão de riscos fundamentada na norma ISO 31000 e sua integração com as políticas de segurança da informação, analise as afirmativas a seguir.

I. A melhoria contínua e a criação e proteção de valor são princípios da ISO 31000.

II. A ISO 31000 orienta a identificação, a análise e o tratamento de riscos, servindo como base para a definição de políticas de segurança alinhadas aos riscos organizacionais.

III. A ISO 31000 é uma norma certificável internacional que funciona como um guia de boas práticas.

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.

52

A ISO 22301 é a norma que garante Gestão de Continuidade de Negócios (GCN).

Nesse cenário, a equipe de TI definiu que, em caso de falha em ambientes de computação em nuvem, o sistema deve estar funcional em até 2 horas, com uma perda máxima de dados de 15 minutos.

Esses parâmetros referem-se, respectivamente, a

(A) RPO (Recovery Point Objective) e RTO (Recovery Time Objective).
(B) SLA (Service Level Agreement) e BIA (Business Impact Analysis).
(C) Backup Incremental e Espelhamento de Disco.
(D) MAO (Maximum Acceptable Outage) e RPO (Recovery Point Objective).
(E) RTO (Recovery Time Objective) e RPO (Recovery Point Objective).

53

Uma equipe de desenvolvimento decidiu aprimorar a segurança de suas aplicações e passou a adotar práticas de Secure SDLC integradas ao *pipeline* de DevSecOps.

Como parte dessa iniciativa, a equipe incorporou ao processo de integração contínua (CI) a ferramenta de análise estática de segurança Checkmarx.

Com o uso dessa ferramenta, diversos alertas passaram a ser gerados durante o desenvolvimento, indicando possíveis vulnerabilidades relacionadas ao uso de entradas externas diretamente na construção de instruções, inclusive em trechos de código que ainda não haviam sido executados.

Considerando o cenário apresentado, assinale a opção que melhor descreve a atuação dessa ferramenta de análise estática no contexto de um SDLC seguro.

(A) Executa a aplicação para identificar falhas relacionadas ao uso de entradas do usuário, com base no comportamento observado em tempo de execução.
(B) Realiza análise por meio do envio de entradas manipuladas, avaliando como o sistema responde às instruções construídas durante sua execução.
(C) Identifica padrões inseguros no código-fonte, como o uso direto de entradas externas na construção de instruções, sem necessidade de execução, podendo gerar alertas que exigem validação quanto à sua efetiva explorabilidade.
(D) Acompanha o comportamento da aplicação em execução, correlacionando entradas do usuário com eventos registrados para identificar possíveis incidentes de segurança.
(E) Realiza testes automatizados com foco na exploração de falhas, simulando interações reais com a aplicação em ambiente de execução.

54

No âmbito da segurança da informação, o *spoofing* é uma violação do princípio da autenticidade, na qual o atacante forja a origem de uma mensagem ou requisição, buscando fazer passar-se por uma origem distinta.

Dadas as diversas formas de operacionalizar o *spoofing*, torna-se importante correlacionar cada tipo de *spoofing* às suas técnicas de mitigação.

Nesse contexto, analise as afirmativas a seguir.

I. O ARP *spoofing* é um ataque focado na rede local, onde se altera o MAC *address* em um *frame*, e pode ser mitigado utilizando-se listas de MAC estático no *firewall* de borda.

II. O IP *spoofing* envolve a alteração do cabeçalho no campo do endereço de origem, e pode ser mitigado aceitando-se apenas pacotes com endereços de origem válidos.

III. O DNS *spoofing* funciona alterando-se os endereços de IP resolvidos para determinado domínio, e pode ser mitigado utilizando-se DNSSEC que valida a autenticidade e integridade das respostas de DNS.

Está correto o que se afirma em

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

55

O XSS (*Cross-site Scripting*) é um ataque do tipo *injection,* que traz riscos se não for tratado corretamente. O *site OWASP top* 10 na sua lista de 2025, elenca o ataque de *injection* na quinta posição, mostrando a importância da sua mitigação para um desenvolvimento seguro.

Assinale a opção que indica o procedimento correto para mitigar ataques do tipo XSS.

(A) Sanitizar as tabelas *lookup*, evitando que *scripts* sejam executados no CSS.
(B) Evitar que as URL contenham comandos em SQL, assim impedindo o XSS *server-side*.
(C) Proteger o servidor contra execução de *scripts* indevidos, o que impede qualquer forma de XSS.
(D) Garantir que os scripts *inline* possam ser executados, o que permite que esses funcionem conforme o desejado pelo programador.
(E) Validar todas as entradas fornecidas pelos usuários, impedindo que *payloads* maliciosos sejam inseridos e executados no ambiente *client-side*.

56

A segurança dos dados modernos não pode ser dissociada do uso de diversos algoritmos de criptografia, capazes de garantir a confidencialidade e integridade dos dados, tanto em trânsito quanto em repouso.

A respeito dos principais algoritmos criptográficos em uso – o AES (*Advanced Encryption Standard*) e o RSA (*Rivest – Shamir – Adleman*), assinale a afirmativa correta.

(A) O AES é um algoritmo de criptografia assimétrico, não apresentando assim o risco da distribuição de chaves em redes abertas e inseguras como a Internet.
(B) O AES usa um par de chaves pública – privada, o que o torna ideal para cifrar grandes volumes de dados sem a necessidade de compartilhar uma chave secreta previamente.
(C) O RSA é classificado como criptografia simétrica, pois exige que tanto o remetente quanto o destinatário possuam a mesma chave para realizar as operações de cifragem e decifragem.
(D) O RSA baseia sua segurança na complexidade matemática da fatoração de números inteiros primos muito grandes, sendo, por isso, um processo computacional mais leve e rápido que o processamento do AES.
(E) O AES, devido à sua eficiência, é usado para cifrar a mensagem em si em um cenário de comunicação segura, enquanto o RSA é usado para cifrar e transmitir com segurança a chave simétrica do AES.

57

A integridade da identidade digital e a autenticidade de documentos em ambientes de rede dependem de uma arquitetura estruturada conhecida como Infraestrutura de Chaves Públicas (PKI – *Public Key Infrastructure*).

Graças ao uso de certificados digitais e a uma hierarquia de confiança, é possível garantir que uma chave pública pertence, de fato, à entidade que a apresenta, evitando ataques de personificação.

Com relação aos componentes desse ecossistema e o seu funcionamento, assinale a afirmativa correta.

(A) O certificado X.509 armazena, primordialmente, a chave simétrica do usuário, funcionando como um repositório público para simplificar a decifragem de informações.
(B) A Autoridade de Registro (AR) é a entidade responsável por assinar digitalmente o certificado final, substituindo a necessidade de uma Autoridade Certificadora (AC) em redes locais.
(C) A Autoridade Certificadora (AC) utiliza a sua própria chave pública para realizar a assinatura digital dos certificados dos usuários, garantindo que o conteúdo do documento seja criptografado e ilegível para terceiros.
(D) As Listas de Revogação de Certificados (*Certificate Revocation List* – CRL) armazenam todas as chaves privadas que já foram utilizadas em uma PKI, permitindo que qualquer usuário recupere sua chave em caso de perda.
(E) A confiança em um certificado digital baseia-se em uma "cadeia de confiança", onde a validade do certificado de um *site* é atestada pela assinatura digital de uma Autoridade Certificadora (AC) reconhecida pelo sistema ou navegador.

58

As funções de resumo criptográfico, conhecidas como *hashes*, são ferramentas fundamentais para garantir a integridade de arquivos e o armazenamento seguro de credenciais.

O *hashing* gera uma "impressão digital" única de um dado original, sendo amplamente aplicado em verificações de autenticidade e em sistemas de autenticação modernos.

Sobre os principais algoritmos e mecanismos de *hash*, assinale a afirmativa correta.

(A) O SHA-1 é a variante do mecanismo SHA que tem a mais baixa resistência à colisão, o que significa que é impossível que dois arquivos diferentes gerem o mesmo *hash*.
(B) O HMAC (*Hash-based Message Authentication Code*) é um tipo de *hash* simples que dispensa o uso de chaves secretas, servindo apenas para verificar se um arquivo foi corrompido durante o download via HTTP.
(C) O algoritmo *bcrypt* foi especificamente projetado para o armazenamento de senhas, pois incorpora um recurso de *salt* e possui um fator de custo ajustável que o torna resistente a ataques de força bruta e *rainbow tables*.
(D) O SHA-3 foi a primeira variante SHA a empregar *hashing* triplo, tendo sido utilizado no protocolo SSL, mas acabou descontinuado devido às vulnerabilidades encontradas com o crescimento da capacidade das CPUs.
(E) O SHA-256 é considerado uma função criptográfica reversível, permitindo que o administrador de um banco de dados recupere a senha original de um usuário caso este a esqueça, sendo empregado também em protocolos TLS.

59

Durante a investigação de um incidente, um analista identificou tráfego suspeito saindo de um servidor interno para um endereço externo na porta 8081, não usual para o ambiente.

O analista, usando o *Wireshark*, realizou a captura de pacotes diretamente do servidor interno, sem perdas, aplicou o filtro tcp.port == 8081 e, ao selecionar uma das conexões, utilizou o recurso *Follow TCP Stream,* obtendo o seguinte diálogo:

POST /sync HTTP/1.1
Host: update-service.external.net
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
Content-Length: 1024

file=clientes.csv&data=Q2xpZW50ZTosQ1BGLENhcnRhbwoxMjMsMDAwMDAw... *(trecho exibido pelo Follow TCP Stream)"*

Com base nesse cenário, assinale a opção que apresenta a interpretação mais adequada.

(A) O protocolo HTTP na porta 8081 impede a transmissão de arquivos estruturados.
(B) A ferramenta Wireshark pode ter reconstruído incorretamente o fluxo TCP.
(C) O uso de Base64 garante que o conteúdo não possa ser interpretado como dado sensível.
(D) O tráfego indica possível exfiltração de dados sensíveis, disfarçada como requisição HTTP.
(E) Trata-se de atualização legítima de sistema, caracterizada pelo uso de HTTP em porta alternativa.

60

Uma sociedade empresária de serviços de TI revisou sua política de conformidade com a Lei Geral de Proteção de Dados (LGPD).

Para mitigar riscos, a equipe de Segurança da Informação aplicou técnicas de pseudonimização nos bancos de dados de produção e estabeleceu um protocolo de resposta a incidentes que prevê a notificação à Autoridade Nacional de Proteção de Dados (ANPD) em situações de risco relevante aos titulares.

Com base nesse cenário e nos preceitos da LGPD, assinale a afirmativa correta.

(A) O emprego da técnica de pseudonimização desobriga o controlador de realizar a notificação à ANPD, uma vez que o dado deixa de ser passível de identificação direta.
(B) A anonimização e a pseudonimização são conceitos equivalentes para a LGPD, sendo assim, os dados deixam de ser considerados dados pessoais para todos os fins legais.
(C) O Encarregado pelo Tratamento de Dados Pessoais (DPO) é o agente de tratamento a quem competem as decisões estratégicas e definitivas sobre o ciclo de vida dos dados.
(D) Segundo o princípio da prevenção, o controlador deve adotar medidas técnicas e administrativas aptas a prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.
(E) A comunicação de incidentes de segurança à ANPD é obrigatória em qualquer evento de acesso não autorizado, independentemente da probabilidade de risco ou dano relevante aos titulares.

Prova Discursiva

1

Durante o monitoramento dos sistemas do Ministério Público do Estado do Espírito Santo, a equipe de Segurança da Informação identificou alterações indevidas em configurações críticas de uma aplicação *web* institucional. Após a confirmação do incidente, foi solicitado ao Analista de Segurança da Informação responsável pela investigação que analisasse os registros do servidor web para subsidiar a resposta ao incidente e a elaboração do relatório técnico.

Durante a análise, foi extraído o seguinte trecho do arquivo *"/var/log/apache2/access.log"*, que contém os registros das ações associadas ao respectivo ataque ao servidor *web*:

192.168.1.10 - - [22/Mar/2026:14:09:58 +0000] "GET /index.php HTTP/1.1" 200 5120
198.51.100.20 - - [22/Mar/2026:14:09:59 +0000] "GET /products.php HTTP/1.1" 200 8450
192.168.1.15 - - [22/Mar/2026:14:10:00 +0000] "GET /contact.php HTTP/1.1" 200 2100
203.0.113.45 - - [22/Mar/2026:14:10:03 +0000] "POST /login.php HTTP/1.1" 401 560
192.168.1.12 - - [22/Mar/2026:14:10:03 +0000] "GET /index.php HTTP/1.1" 200 4980
203.0.113.45 - - [22/Mar/2026:14:10:04 +0000] "POST /login.php HTTP/1.1" 401 560
198.51.100.21 - - [22/Mar/2026:14:10:04 +0000] "GET /about.php HTTP/1.1" 200 1900
203.0.113.45 - - [22/Mar/2026:14:10:05 +0000] "POST /login.php HTTP/1.1" 401 560
192.168.1.11 - - [22/Mar/2026:14:10:05 +0000] "GET /products.php HTTP/1.1" 200 8300
203.0.113.45 - - [22/Mar/2026:14:10:06 +0000] "POST /login.php HTTP/1.1" 401 560
198.51.100.30 - - [22/Mar/2026:14:10:06 +0000] "GET /index.php HTTP/1.1" 200 5001
192.168.1.13 - - [22/Mar/2026:14:10:07 +0000] "GET /cart.php HTTP/1.1" 200 3200
203.0.113.45 - - [22/Mar/2026:14:10:08 +0000] "POST /login.php HTTP/1.1" 200 890
192.168.1.14 - - [22/Mar/2026:14:10:09 +0000] "GET /checkout.php HTTP/1.1" 200 4100
198.51.100.22 - - [22/Mar/2026:14:10:10 +0000] "GET /index.php HTTP/1.1" 200 5020
192.168.1.16 - - [22/Mar/2026:14:10:11 +0000] "GET /home.php HTTP/1.1" 200 4500
203.0.113.45 - - [22/Mar/2026:14:10:13 +0000] "POST /config.php HTTP/1.1" 200 120
192.168.1.17 - - [22/Mar/2026:14:10:14 +0000] "GET /products.php HTTP/1.1" 200 8350
198.51.100.23 - - [22/Mar/2026:14:10:15 +0000] "GET /contact.php HTTP/1.1" 200 2000

Com base exclusivamente nos logs e nas evidências apresentadas, responda aos itens a seguir justificando a sua resposta.

- **a. Delimite, de forma precisa, o intervalo temporal em que ocorreu o ataque, indicando os eventos que marcam seu início e seu término, assim como o IP de origem do atacante. Considere como início do ataque a primeira evidência de comportamento do atacante, o término a última evidência e que foi confirmado pela equipe de segurança de que não se trata de um comportamento de um usuário legítimo.**
- **b. Explique o encadeamento técnico das ações realizadas pelo atacante, descrevendo o objetivo de cada uma das 03 (três) etapas observadas nos logs.**

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15

2

Nos últimos anos, a segurança cibernética deixou de ser apenas uma preocupação técnica e passou a representar um risco estratégico. A indisponibilidade ou o comprometimento de sistemas institucionais decorrentes de incidentes de segurança cibernética afeta diretamente a continuidade dos serviços prestados pelos órgãos públicos, com impactos diretos na operação diária das organizações.

"As perdas reportadas por crimes cibernéticos chegaram a US$ 20,9 bilhões em 2025, com crescimento de 26% em relação ao ano anterior."

Adaptado de https://cyberscoop.com/fbi-internet-crime-complaint-center-annual-cybercrime-report/, acessado em 21/04/2026

Nesse contexto, o monitoramento dos ativos de rede e a resposta tempestiva a incidentes constituem atividades essenciais da gestão da segurança da informação. Na condição de Analista de Segurança da Informação do Ministério Público do Estado do Espírito Santo, responsável pelo monitoramento dos ativos de rede e pela elaboração de parecer técnico sobre incidentes de segurança, considere o contexto e os dois eventos a seguir.

Um dos ativos monitorados é um servidor web localizado na zona desmilitarizada (DMZ), com endereço IP 200.175.50.15, responsável pela disponibilização de serviços institucionais acessíveis externamente.

Evento I

Ao chegar para sua jornada de serviço, o analista configurou o seguinte filtro no *Wireshark* para monitorar o tráfego da DMZ destinado ao servidor:

```
tcp.flags.syn == 1 and tcp.flags.ack == 0 and not tcp.analysis.retransmission and ip.dst == 200.175.50.15
```

Evento II

Enquanto monitorava as requisições que chegavam ao servidor web utilizando o *Wireshark*, o analista notou que o número de requisições que usualmente eram da ordem de 100 por minuto, repentinamente passou a um volume de 2.000 requisições por minuto, provenientes de diversos endereços IP distintos. Diante desse comportamento, o analista suspeitou que se tratava de um ataque e reportou o incidente para o Centro de Tratamento e Resposta a Incidentes Cibernéticos (CTIR) da instituição e prosseguiu com as contramedidas para mitigar o possível ataque.

Com base na situação apresentada, elabore uma resposta que contemple os itens a seguir.

a) Qual foi o tipo de ataque que o funcionário buscava detectar ao implementar o filtro descrito no Evento I? Explique como cada uma das partes do filtro (separados pelos termos AND) contribui para a correta detecção desse tipo de ataque. Por fim, descreva um método para mitigar ou anular o ataque em questão.

b) Sobre o Evento II, qual foi o tipo de ataque sofrido pela organização? Explique que evidências suportam essa conclusão. Descreva uma contramedida para mitigar ou anular esse tipo de ataque, justificando como ela colabora para a solução do ataque, sem comprometer o funcionamento do serviço.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15

Realização