Analista de Tecnologia da Informação - Segurança da Informação

LEIA ATENTAMENTE AS INSTRUÇÕES ABAIXO:

- É responsabilidade exclusiva do candidato a conferência de seus dados pessoais, impressos no Cartão de Respostas e no caderno de provas, em especial o nome, o número de inscrição, o número de seu documento de identidade, cargo de sua opção, assim como, a marcação e assinatura do seu Cartão de Respostas.
- Verifique se este caderno de prova contém **60** questões. Com quatro alternativas identificadas pelas letras **A, B, C,** e **D** das quais apenas uma será a resposta correta.
- Preencha o Cartão de Respostas da prova objetiva utilizando caneta esferográfica azul ou preta, ocupando totalmente o campo de marcação, ao lado dos números, que corresponde à resposta correta. Conforme ilustração: ○●○○○

  Atenção: Serão consideradas incorretas questões para as quais o candidato tenha preenchido no cartão resposta mais de uma opção, bem como questões em que o campo de marcação apresente rasuras, emendas ou que não esteja preenchido integralmente. Tenha muito cuidado para não danificar o código de barras utilizado na leitura óptica do Cartão de Respostas, por isso não **DOBRE, AMASSE ou MANCHE** o mesmo. O Cartão de Respostas será o único documento válido para a correção das provas, salvo à disposição do IDCAP.
- Os fiscais **NÃO** são autorizados a prestar informações de interpretação das questões. Sua função é apenas fiscalizar e orientar quanto ao funcionamento do certame.
- Ao concluir a prova, **entregue ao fiscal de sala o Cartão de Respostas da Prova Objetiva.** A não devolução implicará à eliminação sumária do candidato.
- **Assine a Lista De Presença, Cartão Resposta e transcreva a frase de segurança presente no Cartão Resposta da prova objetiva, sob pena de eliminação.**

NÃO SERÁ PERMITIDO:

- Folhear o caderno de provas antes da autorização do fiscal. Caso aconteça, implicará na eliminação do candidato.
- Qualquer tipo de comunicação entre os candidatos durante a aplicação da prova.
- O uso de calculadoras, dicionários, telefones celulares, pen drive, fone de ouvido, relógio de qualquer espécie, recursos didáticos, aparelhos eletrônicos e bonés.
- A permanência de candidatos no local de realização das provas após o término e a entrega do Cartão de Respostas, devendo o candidato retirar-se imediatamente do local, não sendo possível nem mesmo a utilização dos banheiros e bebedouros.

TEMPO DE PROVA:

- A prova terá duração máxima de **4 (quatro) horas e 30 (trinta) minutos**, incluído o tempo para preenchimento do Cartão de Respostas.
- O candidato somente poderá retirar-se do local de prova **após 1 (uma) hora de seu início.**
- O candidato poderá **levar o caderno de provas 1 (uma) hora antes de seu término.** Antes desse horário, será permitido ao candidato levar apenas o **RECORTE DO RODAPÉ DA CAPA DA PROVA** (parte que contém espaço para preenchimento do gabarito).
- Os 3 (três) últimos candidatos somente poderão retirar-se da sala de prova simultaneamente e devem fazê-lo após a assinatura da ata de sala.

1		7		13		19		25		31		37		43		49		55	
2		8		14		20		26		32		38		44		50		56	
3		9		15		21		27		33		39		45		51		57	
4		10		16		22		28		34		40		46		52		58	
5		11		17		23		29		35		41		47		53		59	
6		12		18		24		30		36		42		48		54		60	

RASCUNHO

Língua Portuguesa

O texto seguinte servirá de base para responder às questões de 1 a 10.

Fadiga visual: a visão na era do excesso de telas

Em uma era em que as telas dominam nossa vida cotidiana, uma epidemia silenciosa se espalha pelo mundo.

A fadiga ocular digital, antes considerada uma condição marginal entre as preocupações com a saúde ocupacional, tornou-se um grande problema de saúde pública, que afeta milhões de pessoas ao redor do mundo.

À medida que nossa dependência de dispositivos digitais para trabalho, educação e interação social só aumenta, há mais riscos à saúde de nossos olhos.

Estudos recentes apresentam um quadro sombrio. Até cinquenta por cento dos usuários de computador desenvolvem a chamada fadiga ocular digital.

Essa condição, caracterizada por uma variedade de sintomas oculares e visuais, como secura, lacrimejamento, coceira, queimação, visão turva ou até dupla, não é apenas um incômodo.

Ela indica problemas crônicos que afetam significativamente a qualidade de vida e a produtividade de um indivíduo.

A pandemia da covid-19 exacerbou essa tendência. Afinal, os confinamentos e as medidas de distanciamento social aumentaram o tempo de tela em uma escala sem precedentes.

Um aumento acentuado no uso de dispositivos digitais durante esse período está correlacionado a um crescimento das doenças na superfície ocular, distúrbios visuais e fadiga ocular digital.

O que acontece com nossos olhos quando olhamos para telas por longos períodos?

A resposta está na biologia complexa do nosso sistema visual. Ao focar em telas digitais, nossa taxa de piscadas diminui e nossos olhos se esforçam demais para focar em objetos próximos por longos períodos.

Piscar menos e manter o foco próximo desencadeia uma série de problemas oculares, desde irritação leve até ressecamento crônico.

Os sintomas da fadiga ocular digital são diversos e muitas vezes insidiosos. Eles variam desde sinais imediatamente perceptíveis, como fadiga ocular, secura e visão turva, até pistas mais sutis, como dores de cabeça e no pescoço.

Embora geralmente temporários, esses sintomas podem se tornar persistentes e debilitantes, se não forem tratados.

Ao contrário da crença popular, a luz azul emitida pelas telas não é a principal causa da vista cansada.

Embora a luz azul possa contribuir para a fadiga ocular e interromper os padrões de sono, não há evidências conclusivas de que ela cause danos oculares permanentes.

Os verdadeiros vilões são a ergonomia ruim, o trabalho por um tempo prolongado com foco próximo e a redução das piscadas.

Como podemos proteger a visão neste mundo centrado nas telas?

A solução está em uma abordagem multifacetada, que combina mudanças comportamentais, ajustes ambientais e, quando necessário, intervenções médicas.

https://www.bbc.com/portuguese/articles/cly569nwr1no.adaptado.

Questão 01

(Correta: C)

A fadiga ocular digital, antes considerada uma condição marginal entre as preocupações com a saúde ocupacional, tornou-"se" um grande problema de saúde pública.

De acordo com as regras de colocação pronominal, é correto afirmar que, morfologicamente, o vocábulo destacado trata-se de:

(A) Objeto direto com função de complemento.
(B) Partícula apassivadora com função de objeto direto.
(C) Pronome oblíquo com função reflexiva.
(D) Conjunção integrante com função recíproca.

Questão 02

(Correta: A)

Ela indica problemas crônicos que afetam significativamente a qualidade de vida e a produtividade de um indivíduo.

O número de preposições presentes na frase em questão é de: (considere as repetidas, se houver.)

(A) Três.
(B) Cinco.
(C) Seis.
(D) Quatro.

Questão 03

(Correta: C)

"Piscar" menos e manter o foco próximo "desencadeia" uma série de problemas oculares, desde irritação leve até ressecamento crônico.

Os verbos destacados, nesta frase, comportam-se, respectivamente, como verbos:

(A) Transitivo direto – bitransitivo.
(B) Bitransitivo – bitransitivo.
(C) Intransitivo – transitivo direto.

(D) Transitivo direto – transitivo direto.

Questão 04

(Correta: C)

Estudos recentes apresentam um quadro sombrio.

No contexto do texto, qual das alternativas apresenta um antônimo adequado para a palavra "sombrio", considerando seu sentido na expressão "quadro sombrio"?

(A) Efêmero, pois "sombrio" expressa a ideia de algo duradouro e profundo, ao passo que "efêmero" remeteria a uma preocupação passageira e superficial.
(B) Nebuloso, pois "sombrio" transmite a ideia de obscuridade e incerteza, e "nebuloso" reforça apenas um conceito de falta de clareza e pessimismo.
(C) Radiante, pois "sombrio" é empregado no sentido de algo negativo e alarmante, enquanto "radiante" remete a uma condição otimista, favorável e luminosa.
(D) Restrito, pois "sombrio" sugere um panorama abrangente e grave, ao passo que "restrito" indicaria algo de menor escala e impacto reduzido.

Questão 05

(Correta: A)

Em uma era em que as telas dominam nossa vida cotidiana, uma epidemia silenciosa se espalha pelo mundo.

A frase em questão encontra-se predominantemente no sentido:

(A) Conotativo.
(B) Conativo.
(C) Fático.
(D) Denotativo.

Questão 06

(Correta: B)

Com a pandemia, as doenças oculares causadas pelo uso excessivo de telas aumentaram. De acordo com um estudo recente, até metade dos usuários de computador podem desenvolver fadiga ocular digital.

Qual das alternativas a seguir melhor sintetiza a abordagem do texto base em relação à fadiga ocular digital?

(A) Segundo o texto, a fadiga ocular digital é resultado direto do excesso de exposição à luz azul, o que compromete permanentemente a saúde ocular dos indivíduos.
(B) O texto apresenta a fadiga ocular digital como um problema de saúde pública, exacerbado pelo uso excessivo de dispositivos eletrônicos, influenciado pela ergonomia inadequada e redução da frequência de piscadas, e não apenas pela emissão de luz azul.
(C) O texto responsabiliza exclusivamente a pandemia da covid-19 pelo aumento da fadiga ocular digital, argumentando que, antes desse período, a condição era insignificante.
(D) O texto sugere que a fadiga ocular digital pode ser prevenida por meio de intervenções médicas, descartando ajustes comportamentais e ambientais como soluções viáveis.

Questão 07

(Correta: B)

Essa condição, caracterizada por uma variedade de sintomas oculares e visuais, como secura, lacrimejamento, coceira, queimação, visão turva ou até dupla, não "é" apenas um incômodo.

Em relação à concordância, o verbo destacado na frase refere-se ao vocábulo:

(A) secura
(B) condição
(C) variedade
(D) visão

Questão 08

(Correta: A)

"À medida que" nossa dependência de dispositivos digitais para trabalho, educação e interação social só aumenta, há mais riscos à saúde de nossos olhos.

Morfologicamente, o termo destacado, nesta frase, trata-se de:

(A) Locução conjuntiva.
(B) Complemento nominal.
(C) Adjunto adnominal.
(D) Adjunto adverbial.

Questão 09

(Correta: C)

Embora geralmente temporários, esses sintomas podem se tornar persistentes e debilitantes, se não forem tratados.

Assinale a alternativa correta quanto à nova pontuação sem alteração do sentido original da frase.

(A) Embora se, não forem tratados geralmente, temporários esses sintomas podem: se tornar persistentes e debilitantes.
(B) Embora se não forem tratados geralmente, temporários esses sintomas podem se tornar persistentes e debilitantes.

(C) Se não forem tratados, embora geralmente temporários, esses sintomas podem se tornar persistentes e debilitantes.

(D) Se não forem tratados, embora geralmente, temporários, esses sintomas podem se tornar persistentes: e debilitantes.

Questão 10

(Correta: A)

A solução "está" em uma abordagem multifacetada, que "combina" mudanças comportamentais, ajustes ambientais e, quando necessário, intervenções médicas.

Conjugando os verbos destacados no futuro do pretérito do indicativo e no pretérito imperfeito do subjuntivo, respectivamente, tem-se: (considere as alterações se necessário)

(A) A solução estaria em uma abordagem multifacetada, se combinasse mudanças comportamentais, ajustes ambientais e, quando necessário, intervenções médicas.

(B) A solução estava em uma abordagem multifacetada, combinando mudanças comportamentais, ajustes ambientais e, quando necessário, intervenções médicas.

(C) A solução estivera em uma abordagem multifacetada, que combinou mudanças comportamentais, ajustes ambientais e, quando necessário, intervenções médicas.

(D) A solução estará em uma abordagem multifacetada, quando combinar mudanças comportamentais, ajustes ambientais e, quando necessário, intervenções médicas.

Língua Inglesa

O texto seguinte servirá de base para responder às questões de 11 a 16.

Biden administration, in its last days, proposes new protections for Arctic Alaska land

Lakes and connecting streams in the northeastern part of the National Petroleum Reserve in Alaska, June 2014.

Four days before President Joe Biden is set to leave office, his administration recommended that about 3 million more acres in Alaska's western Arctic be protected from development and issued a guideline, effective immediately, requiring additional protections for traditional Native subsistence harvests of fish, caribou and other resources.

The new recommendations and guidance, which apply to the 23-million-acre National Petroleum Reserve in Alaska, run counter to President-elect Donald Trump's expressed plans to expand oil drilling in the Arctic and elsewhere and to overturn Biden administration environmental policies more broadly.

The recommendations for additional land to be protected as part of what are termed "special areas" and the guidance for elevating the importance of subsistence and tribal consultation could be ignored or scrapped by the incoming Trump administration.

The northeastern part of the reserve is the area considered most likely to hold oil and where development has spread in recent years. There is already production in that area, and the most notable production expected in the future is from ConocoPhillips' Willow project. Willow won Biden administration approval in 2023. Production is expected to start by the end of the decade and peak at 180,000 barrels per day; current production from all North Slope fields amounts to less than 470,000 barrels per day.

Like the existing Teshekpuk special area, which holds important habitat for caribou, fish and migratory birds, the village of Nuiqsut is in the general area of the reserve's northeastern corner, where new oil development has occurred. Nuiqsut is so close that oilfield infrastructure can be seen from the village.

Pipelines extend across the landscape outside Nuiqsut, Alaska, May 2019.

"But at the same time, I think we and our partners have also made it abundantly clear that we're going to keep fighting, and keep fighting for protections in the Western Arctic," she said.

(From ROSEN, Yereth. Biden administration, in its last days, proposes new protections for Arctic Alaska land, Alaska Beacon, January 17, 2025. In alaskabeacon.com/2025/01/17/biden-administration-in-its-last-days-proposes-new-protections-for-arctic-alaska-land/, accessed on February 19th, 2025)

Questão 11

(Correta: C)

The term *likely* in *the area considered most likely to hold oil* (line 12) means:

(A) prominence.
(B) promptness.
(C) potentiality.
(D) predilection.

Questão 12

(Correta: B)

Donald Trump's stated plans are to:

(A) fight for protections of 180,000 barrels of oil per day.
(B) invalidate Joe Biden's guidelines for Arctic Alaska protection.
(C) develop the village of Nuiqsut infrastructure abundantly.
(D) guide native subsistence policies more largely.

Questão 13

(Correta: C)

The expression *the most notable production expected in the future* is formed by the same pattern as:

(A) It has been noticed a production shortage in the latest reports.
(B) What are the best things to see and do in your city?
(C) The most distant planet known from the sun is Jupiter.
(D) August is considered the worst month of the year.

Questão 14

(Correta: D)

Mark the sentence that correctly represents the passive voice of *I think we and our partners have also made it abundantly clear that we're going to keep fighting* (lines 32 and 33):

(A) It is believed by us and our partners that it has been made abundantly clear the fighting will be kept.
(B) I think it will be made abundantly clear the fighting is going on.
(C) It is abundantly clear that the fight might be continued by us and our partners.
(D) It is thought it has been made abundantly clear the fighting is going to be kept.

Questão 15

(Correta: D)

The 23-million-acre in Alaska, and its additional land are regarded as "special areas" because:

(A) the planet requires a variety of animals, plants of importance to biodiversity.
(B) of the expected oil production from North Slope fields.
(C) the oilfield pipelines can be seen from Nuigsut village.
(D) they consist of areas of conservation of special habitats and species.

Questão 16

(Correta: B)

The pronouns *which* (line 25) and *where* (line 27) are respectively subordinated to:

(A) new oil development, Western Arctic.
(B) Teshekpuk special area; the reserve's northeastern corner.
(C) new recommendations and guidance; Teshekpuk special area.
(D) caribou, fish and migratory birds; the village of Nuiqsut.

O texto seguinte servirá de base para responder às questões de 17 a 20.

Mother Goose and Grimm cartoon, by Mike Peters

Questão 17

(Correta: C)

Which are countable and uncountable nouns examples in the comic strip:

(A) energy, mines.
(B) uranium, power.
(C) company, energy.
(D) mines, wells.

Questão 18

(Correta: D)

The question: *Can you solve our energy crisis?*, made by Ralph, the dog character is given in the direct speech. Choose the alternative with its appropriate conversion into the reported speech:

(A) Ralph asked Mr. Oil Company when it was possible to solve his energy crisis.
(B) Ralph persuaded Mr. Oil Company to solve their energy crisis.
(C) Ralph said Mr. Oil Company is able to solve the energy crisis.
(D) Ralph asked Mr. Oil Company if he could solve their energy crisis.

Questão 19

(Correta: C)

In Mr. Big Oil's last statement: *Solar and Wind isn't feasible* there is a different use of subject and verb agreement, such as in:

(A) Everyone has to take the course to earn an AA degree.
(B) The nurse told us not to make so much noise.
(C) One of my friends like to cook Italian food.
(D) Leading the club meeting today are Francesca and Oliver.

Questão 20

(Correta: D)

The questions Mr. Oil Company asked Ralph: *You want coal? You want oil and gas? You want nuclear energy? You want solar or wind power?* are acceptable forms in colloquial English. In standard English, however, the word order of those sentences is applied for the affirmatives. The option with the correct interrogative word order is:

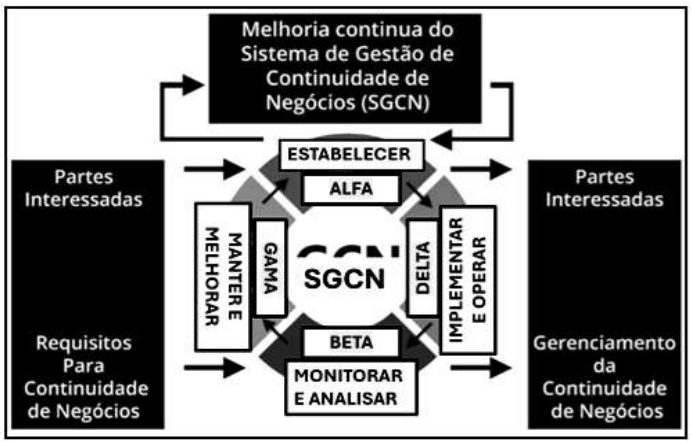
(A) Wanna try that again?
(B) How you feel today?
(C) He is a fan of Marvel movies.
(D) Will you open the window for me, please?

Conhecimentos Específicos

Questão 21

(Correta: B)

Seguindo o padrão de outras normas de gestão, a *ISO 22301* adota o ciclo *PDCA*, mostrado na figura, para a eficácia do SISTEMA DE GESTÃO DE CONTINUIDADE DE NEGÓCIOS - SGCN e requer que o plano possua uma política, pessoal competente com responsabilidades definidas, processos de gestão e documentações que apoiem o controle operacional e avaliação de desempenho.



Os identificadores ALFA – BETA – GAMA – DELTA mostrados na figura, correspondem no ciclo PDCA, respectivamente a:

(A) A (Act) – D (Do) – P (Plan) – C (Check)
(B) P (Plan) – C (Check) – A (Act) – D (Do)
(C) D (Do) – P (Plan) – C (Check) – A (Act)
(D) C (Check) – A (Act) – D (Do) – P (Plan)

Questão 22

(Correta: B)

No mundo da cibernética e da segurança em redes e na internet, existem muitas formas de se lidar com a privacidade, e uma consiste em usar uma rede de camada de soquete seguro, que utiliza o protocolo SSL para estabelecer uma conexão criptografada entre o dispositivo do usuário e o servidor, garantindo que os dados transmitidos entre eles estejam seguros e protegidos contra interceptação ou acesso não autorizado, podendo ser implementada de dois modos, via portal ou túnel.

Essa rede é conhecida pelo seguinte termo técnico:

(A) WPA SSL
(B) VPN SSL
(C) WEP SSL
(D) PROXY SSL

Questão 23

(Correta: B)

Blockchain é definido como um registro digital descentralizado de transações compartilhadas em uma rede imutável ou inalterável, que usa o que se chama de tecnologia de registro distribuído. Entre as características da tecnologia *blockchain*, uma se destaca pela natureza distribuída e criptografada do *blockchain*, que dificulta a ação de *hackers*, fato importante e promissor para a

proteção dos negócios e a Internet das Coisas (IoT), enquanto que outra se caracteriza pelo fato do *blockchain* ser programável, o que permite desencadear ações, eventos e pagamentos automaticamente quando as condições são atendidas. Para finalizar, uma terceira se deve ao fato de que, enquanto as informações são verificadas e adicionadas ao blockchain por meio de um processo de consenso, os dados em si são traduzidos em uma série de letras e números por um código *hash* e, por consequência, os participantes da rede não têm como traduzir essas informações sem uma chave.

As três características são conhecidas, respectivamente, como:

(A) Automação, privacidade e transparência.
(B) Segurança, automação e privacidade.
(C) Transparência, segurança e automação.
(D) Privacidade, transparência e segurança.

Questão 24

(Correta: A)

A Gestão de Riscos Cibernéticos tem um novo referencial técnico em português - a norma internacional e brasileira *NBR ISO/IEC 27005*, baseada no Processo de Gestão de Riscos estabelecido na I*SO 31000*. *A NBR ISO/IEC 27005* visa traçar ações para lidar com os riscos de Segurança da Informação, além de realizar atividades de gerenciamento na área, especificamente avaliação e tratamento de riscos, podendo ser aplicada a todas as organizações, independente de tipo, tamanho ou setor. As ações para tratamento de risco, são denominadas respostas ao risco, havendo quatro possibilidades, das quais três são caracterizadas a seguir.

I.Consiste em alterar a probabilidade de ocorrência de um evento ou alterar a gravidade da consequência. O risco fica mais difícil de ocorrer ou menos impactante.

II.Consiste em reconhecer o risco e não tomar nenhuma ação. É uma estratégia muito adotada quando o custo para atuar sobre o risco ultrapassa a consequência que ele traria.

III.Consiste em dividir responsabilidades com outras partes, interna ou externamente. O exemplo clássico é contratar um seguro.

As três respostas ao risco descritas em I, em II e em III são conhecidas, respectivamente, como:

(A) Mitigar/Modificar, Aceitar/Reter e Transferir/Compartilhar.
(B) Aceitar/Reter, Transferir/Compartilhar e Evitar/Eliminar.
(C) Evitar/Eliminar, Mitigar/Modificar e Aceitar/Reter.
(D) Transferir/Compartilhar, Evitar/Eliminar e Mitigar/Modificar.

Questão 25

(Correta: D)

A computação em nuvem é um modelo de serviços que fornece recursos computacionais, como armazenamento, infraestrutura, rede, software, análise e inteligência, por meio da internet. Dentre os principais tipos de computação em nuvem, o primeiro fornece aplicativos de software completos como um serviço, o segundo um ambiente virtualizado, como máquinas virtuais, armazenamento e redes e o terceiro e último, uma arquitetura para desenvolver, testar e gerenciar aplicativos.

Esses três tipos de computação em nuvem são conhecidos, respectivamente, pelas siglas:

(A) Infraestrutura como Serviço (IaaS), Plataforma como Serviço (PaaS) e Contêiner como como Serviço (CaaS).
(B) Contêiner como como Serviço (CaaS), Software como Serviço (SaaS) e Infraestrutura como Serviço (IaaS).
(C) Plataforma como Serviço (PaaS), Contêiner como como Serviço (CaaS) e Software como Serviço (SaaS).
(D) Software como Serviço (SaaS), Infraestrutura como Serviço (IaaS) e Plataforma como Serviço (PaaS).

Questão 26

(Correta: D)

No uso da computação em nuvem, a segurança da informação nunca foi tão desafiadora, sendo que como o aumento da digitalização, a quantidade de dados gerados e armazenados pelas empresas cresceu exponencialmente. Nesse sentido, essa digitalização acelerada também trouxe consigo uma explosão de ameaças cibernéticas, elevando o grau de importância da preocupação com os pilares da segurança da informação. Nesse contexto, a integridade dos dados é crucial para assegurar que as informações permaneçam exatas e consistentes ao longo do tempo, sem alterações não autorizadas, garantindo que os dados transmitidos ou armazenados não sejam adulterados, seja de forma intencional ou acidental. Para proteger a integridade dos dados, as empresas utilizam alguns recursos, dos quais três são descritos a seguir.

I.Funciona como uma marca de verificação para sinalizar qualquer alteração não autorizada.

II.Constitui uma prática comum, permitindo que as organizações acompanhem as mudanças nos documentos e revertam para versões anteriores se necessário.

III.São fundamentais para verificar a precisão dos dados e identificar quaisquer inconsistências.

Esses três recursos são conhecidos, respectivamente, como:

(A) Autenticação multifator, assinatura digital e controles de versão.
(B) Controles de versão, auditorias regulares, autenticação multifator.

(C) Auditorias regulares, autenticação multifator, assinatura digital.

(D) Assinaturas digitais, controles de versão e auditorias regulares.

Questão 27

(Correta: D)

O COBIT 2019 é um framework de governança e gestão de Informação e Tecnologia desenvolvido pela ISACA, usado por empresas para desenvolver, organizar e implementar estratégias de gestão de informação e governança. De acordo como o COBIT 2019, os objetivos de gestão estão agrupados em quatro domínios, dos quais três são caracterizados a seguir.

I.Trata da prestação e suporte dos serviços de TI, inclusive os de segurança.

II.Trata da organização em geral, a estratégia e as atividades de gestão da TI.

III.Trata da definição, aquisição e implementação de soluções de TI e suas integrações nos processos de negócio.

Os três domínios caracterizados em I, II e III, são conhecidos, respectivamente, como:

(A) Construir, Adquirir e Implementar / Monitorar, Avaliar e Analisar / Entregar, Servir e Suportar.

(B) Alinhar, Planejar e Organizar / Construir, Adquirir e Implementar / Monitorar, Avaliar e Analisar.

(C) Monitorar, Avaliar e Analisar / Entregar, Servir e Suportar / Alinhar, Planejar e Organizar.

(D) Entregar, Servir e Suportar / Alinhar, Planejar e Organizar / Construir, Adquirir e Implementar.

Questão 28

(Correta: C)

O *GitLab* representa um gerenciador de repositórios de software, cujo funcionamento se baseia em *Git* — sistema de versões distribuído usado para desenvolver softwares. O *GitLab Ci* caracteriza-se como um ambiente de Integração Contínua, que pertence ao *GitLab*, e oferece suporte para integração contínua, implantação contínua) e entrega contínua. Desse produto, o usuário deve criar uma conta para acessar o *GitLab* e, logo em seguida, criar um repositório. Nesse processo, há que se configurar um arquivo específico, com o intuito de promover o controle do projeto conforme o seu andamento. Após concluir a criação do arquivo, deve-se adicionar alguns comandos que garantem o seu funcionamento adequado, com destaque para três, descritos a seguir.

I.Responsável por determinar as fases que podem ser executadas ao longo do projeto.

II.Tem a finalidade de especificar a lista de arquivos e diretórios a serem anexados ao job depois do seu sucesso.

III.Detalha o caminho que vai ser trilhado pelo arquivo.

O nome do arquivo a ser criado e os três comandos descritos são, respectivamente:

(A) gitlab-ci.cfg, stages, root e standards

(B) gitlab-ci.yml, labels, root e paths

(C) gitlab-ci.yml, stages, artifacts e paths

(D) gitlab-ci.cfg, stages, artifacts e standards

Questão 29

(Correta: D)

No uso dos recursos de sintaxe do HTML5/CSS3, uma cor pode ser especificada usando matiz, saturação e luminosidade no formato HSL, onde matiz é um grau entre 0 a 360, que define o padrão de cores básicas, saturação é um valor percentual, finalizando por luminosidade que também é expressa em porcentagem.

Nesse cenário, observe o código exemplificado a seguir.

```
<html>
<body>
<h1> Especificando cores usando padrão HSL</h1>
<h2 style="background-color:hsl(0,100%,50%);">
GASOLINA</h2>
<h2 style="background-color:hsl(240,100%,50%);">
DIESEL</h2>
</body>
</html>
```

Na execução desse código em um browser, as palavras GASOLINA e DIESEL serão exibidas com fonte na cor preta, com fundos, respectivamente, nas cores básicas:

(A) amarelo e verde.

(B) amarelo e azul.

(C) vermelho e verde.

(D) vermelho e azul.

Questão 30

(Correta: C)

Entre os padrões IEEE 802.11, um é também conhecido por Wi-Fi5, sendo amplamente utilizado, suporta velocidades máximas de transferência de dados de até 6,93 Gb/s nominais, largura de canal mínimo de 80 MHz, podendo chegar a até 160 MHz, frequência de operação exclusivamente em 5 GHz, modulação 256 QAM, suporte MIMO para transmissões simultâneas entre um mesmo dispositivo e protocolos de segurança WEP, WPA e WPA2.

Esse padrão é conhecido como:

(A) IEEE 802.11/n

(B) IEEE 802.11/ax

(C) IEEE 802.11/ac
(D) IEEE 802.11/b

Questão 31

(Correta: C)

A norma NBR ISO 22301:2020 é um padrão internacional que estabelece requisitos para o SISTEMA DE GESTÃO DE CONTINUIDADE DE NEGÓCIOS - SGCN, sendo aplicável a organizações de todos os tamanhos e tipos, com o objetivo de garantir a resiliência e a segurança. Nesse contexto, esse padrão estabelece quatro perspectivas, sendo duas destacadas a seguir. A primeira P1, tem por metas apoiar os objetivos estratégicos, criar vantagem competitiva, proteger e melhorar a reputação e credibilidade além de contribuir para a resiliência organizacional, enquanto que a segunda P2 visa reduzir a exposição legal e financeira e reduzir custos diretos e indiretos de disrupções.

Nesse contexto, P1 e P2 são denominadas, respectivamente, perspectivas:

(A) do negócio e operacional
(B) da qualidade e financeira
(C) do negócio e financeira
(D) da qualidade e operacional

Questão 32

(Correta: B)

"NIST Cybersecurity Framework" constitui uma ferramenta para organizar e melhorar o programa de segurança cibernética de uma empresa, que estabelece um conjunto de diretrizes e práticas. A estrutura apresenta um conjunto de recomendações e padrões que permitem que as organizações sejam melhor preparadas para identificar e detectar ataques cibernéticos. Esse recurso estabelece cinco princípios, dos quais três são caracterizados a seguir.

I.Tem por função definir as bases para um programa eficaz de segurança cibernética, para gerenciar o risco de segurança para sistemas, pessoas, ativos, dados e recursos. Para permitir que uma organização concentre e priorize seus esforços, consistente com sua estratégia de gerenciamento de riscos e necessidades de negócios, esse princípio enfatiza a importância de entender o contexto de negócios, os recursos que suportam funções críticas e os riscos de segurança cibernética relacionados.

II.Tem por função definir as atividades para verificar e levantar a ocorrência de eventos de segurança cibernética em tempo hábil.

III.Tem por função se concentrar em atividades próximas com o objetivo de agir em caso de um incidente de segurança cibernética detectado, além de apoiar a capacidade de conter o impacto de um possível incidente de segurança cibernética.

Esses três princípios são conhecidos, respectivamente, como:

(A) Recuperar, Identificar e Detectar.
(B) Identificar, Detectar e Responder.
(C) Proteger, Recuperar e Identificar.
(D) Detectar, Responder e Proteger.

Questão 33

(Correta: C)

O *NIST SP 800-61* constitui um framework que fornece orientações para o gerenciamento de respostas a incidentes cibernéticos, sendo uma ferramenta essencial para que as empresas possam se preparar para lidar com os incidentes. De acordo com as orientações, são definidas quatro etapas a serem projetadas para apoiar tanto no planejamento, durante a ocorrência de um incidente. Uma dessas etapas prevê que uma vez que o incidente é declarado, o primeiro objetivo passa visa reduzir o impacto ao máximo possível, com destaque para algumas ações a serem tomadas , como coleta e preservação de evidências, determinação da causa raiz, controle do incidente, mapeamento do impacto, comunicação com stakeholders e possivelmente com o público externo e clientes, finalizando com a restauração de backups.

Essa etapa é conhecida como:

(A) Atividades pós-incidente.
(B) Preparação.
(C) Contenção, erradicação e recuperação.
(D) Identificação e análise.

Questão 34

(Correta: C)

No contexto da segurança da informação, um termo diz respeito a um dado definido como aquele que, originariamente, era relativo a uma pessoa, mas que passou por etapas que garantiram a desvinculação dele a essa pessoa. Os dados que se encontram nessa situação são essenciais para o crescimento da inteligência artificial, da internet das coisas, do aprendizado das máquinas, das cidades Inteligentes e da análise de comportamentos. Eles indicam ainda que, sempre que possível, uma organização, pública ou privada, aplica a técnica associada a esse termo aos dados pessoais, pois isso aperfeiçoa a segurança da informação na organização e gera, assim, mais confiança em seus serviços e para seus públicos.

Esse termo é conhecido como:

(A) reidentificação.
(B) generalização.
(C) anonimização.
(D) pseudonimização.

Questão 35

(Correta: D)

A Lei Geral de Proteção de Dados Pessoais – LGPD tem como objetivo proteger os direitos de liberdade e privacidade das pessoas, além de garantir a livre formação de sua personalidade. A lei se aplica a dados pessoais tratados por pessoas físicas ou jurídicas, em meios físicos ou digitais. De acordo com o Art. 6º, as atividades de tratamento de dados pessoais deverão observar a boa-fé e diversos princípios, dos quais um refere-se à garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais, enquanto que outra refere-se à utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

Os dois princípios descritos são denominados, respectivamente:

(A) Qualidade dos dados e transparência.
(B) Qualidade dos dados e segurança.
(C) Livre acesso e transparência.
(D) Livre acesso e segurança.

Questão 36

(Correta: C)

Atualmente, a maioria das redes de computadores cabeadas padrão Ethernet têm sido implementadas empregando um tipo de cabo de par trançado não blindado e um padrão de conector, usando uma topologia física na qual os computadores são ligados a um dispositivo central, encarregado do gerenciamento das informações. É a topologia mais comum, que emprega um concentrador como elemento central, que se encarrega de retransmitir todos os dados para todas as estações, mas com a vantagem de tornar mais fácil a localização dos problemas, considerando que se um dos cabos ligado a uma das portas do concentrador ou uma das placas de rede estiver com problemas, apenas o nó ligado ao componente defeituoso ficará fora da rede.

A referência para o cabo, a denominação para a topologia descrita, a sigla e a figura que identificam o conector são, respectivamente:

(A) UTP, anel, PS2 e 

(B) STP, malha, RJ45 e 

(C) UTP, estrela, RJ45 e 

(D) STP, hierárquica, PS2 e 

Questão 37

(Correta: C)

React é uma biblioteca *JavaScript* para criar interfaces de usuário, sendo que os aplicativos são feitos de componentes. Um componente é uma parte da interface do usuário, que tem sua própria lógica e aparência, podendo ser tão pequeno quanto um botão ou tão grande quanto uma página inteira. Entre os principais componentes, um corresponde a uma técnica avançada do *React* para reutilizar lógica em componentes, sendo uma função que recebe um componente como argumento e retorna um novo componente com funcionalidades adicionais.

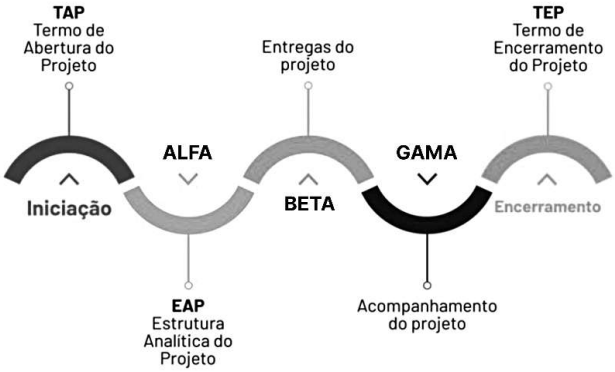
Essa descrição diz respeito ao componente *React*:

(A) Memoizado.
(B) Funcional.
(C) De ordem superior.
(D) De classe inferior.

Questão 38

(Correta: D)

A gestão de TI trata da execução das ações necessárias para atingir as metas estabelecidas, ao passo que a governança de TI é responsável por desenvolver a estratégia do setor de tecnologia. Nesse contexto, em conformidade com os princípios da gestão de projetos, observe a figura que destaca cinco etapas fundamentais para se desenvolver um bom projeto, sendo "Iniciação" a primeira a e "Encerramento" a última.



As três etapas intermediárias ALFA, BETA e GAMA são conhecidas, respectivamente, como:

(A) Execução, Monitoramento e Elicitação
(B) Monitoramento, Elicitação e Planejamento
(C) Elicitação, Planejamento e Execução
(D) Planejamento, Execução e Monitoramento

Questão 39

(Correta: C)

O protocolo *Simple Network Management Protocol – SNMP* pertence ao conjunto *TCP/IP* usado para monitorar e gerenciar dispositivos como servidores, *storages*, roteadores e *switches*, sendo que opera na coleta, organização e envio de dados dos elementos de uma rede IP, auxiliando na identificação de eventuais falhas. Entre as operações básicas do protocolo *SNMP*, duas são básicas, a primeira é utilizada para alterar o valor da variável, sendo que o gerente solicita que o agente faça uma alteração no valor da variável, enquanto que a segunda é utilizada para ler o valor da variável, sendo que o gerente solicita que o agente obtenha o valor da variável.

Essas operações são, respectivamente:

(A) SET e READ
(B) TRAP e GET
(C) SET e GET
(D) TRAP e READ

Questão 40

(Correta: B)

Entre os conceitos relacionados à segurança da informação, um está associado e definido como a realização de cópia de segurança dos dados originais ou conjunto de dados mantidos por questão de segurança, a fim de garantir sua disponibilidade e integridade.

Esse conceito é conhecido como:

(A) firewall.
(B) backup.
(C) swapping.
(D) flooding.

Questão 41

(Correta: C)

As normas *ABNT NBR ISO IEC 27001* e *ABNT NBR ISO IEC 27002* representam padrões internacionais, que fazem referência aos códigos de práticas que tratam, respectivamente, dos seguintes aspectos da segurança da informação:

(A) Aceitação e controles.
(B) Aceitação e testes.
(C) Gestão e controles.
(D) Gestão e testes.

Questão 42

(Correta: A)

Certificado digital é uma identidade eletrônica de uma pessoa ou empresa, tendo surgido com o objetivo de facilitar a identificação virtual e permitir a assinatura de documentos à distância com o mesmo valor jurídico da assinatura feita de próprio punho, com a vantagem de não necessitar o reconhecimento de firma em cartório. Um dos principais modelos de certificado digital é também o mais conhecido e um dos mais utilizados, sendo que funciona a partir da instalação de um software diretamente no computador do usuário, onde será gerada a chave criptográfica. Como ele está instalado diretamente em seu computador, ele se torna rápido e ágil para ser utilizado, além de poder ser desativado a qualquer momento caso desejável. O contrato tem uma duração razoavelmente curta, de apenas um ano, precisando ser revisado ao fim desse período.

Esse modelo é conhecido como Certificado Digital:

(A) A1
(B) A4
(C) A2
(D) A3

Questão 43

(Correta: A)

A cibersegurança é uma área da segurança da informação que tem por objetivo assegurar a proteção dos dados contidos em dispositivos como servidores, computadores, redes e aplicações contra vazamentos, ataques e invasões, sendo uma prática que envolve a segurança de dados, a recuperação de desastres e a continuidade do negócio, além dos armazenados em sistemas computacionais, como informações pessoais e comerciais, de serem roubadas, acessadas ou

danificadas por criminosos. Aplicações e serviços que dependem de dados precisam estar sempre atualizados e protegidos, envolvendo medidas de cibersegurança para proteger os dados contra diversas ameaças. Entre essas, três tipos de ataques são caracterizados a seguir.

I.Usa e-mails ou sites falsos para enganar os usuários e conseguir informações sensíveis, como nomes, dados bancários e senhas.

II.Envolve softwares capazes de descobrir uma senha por meio da tentativa sistemática de todas as combinações possíveis de letras, números e símbolos.

III.Sobrecarrega um sistema, rede ou site com tráfego, tornando-o inacessível aos usuários legítimos e expõe possíveis falhas de segurança.

Esses tipos de ataques são conhecidos, respectivamente, como de:

(A) phishing, força bruta e DoS/DDoS
(B) DoS/DDoS, Man-in-the-Middle (MitM) e phishing
(C) Man-in-the-Middle (MitM), phishing e força bruta
(D) força bruta, DoS/DDoS e Man-in-the-Middle (MitM)

Questão 44

(Correta: B)

Um sistema de prevenção de intrusão (IPS) é uma ferramenta de segurança de rede, podendo pode ser um dispositivo de hardware ou software, que monitora continuamente uma rede em busca de atividades maliciosas e toma medidas para preveni-las, incluindo relatar, bloquear ou desativá-las, quando ocorrem. Existem diversos tipos de IPS, dos quais três são caracterizados a seguir.

I.É instalado apenas em pontos estratégicos para monitorar todo o tráfego de rede e verificar proativamente se há ameaças.

II.É instalado em um endpoint como um microcomputador e monitora apenas o tráfego de entrada e saída daquela máquina.

III.É instalado para verificar uma rede Wi-Fi em busca de acesso não autorizado e expulsar dispositivos não autorizados da rede.

Os três tipos caracterizados são conhecidos, respectivamente, Sistema de Prevenção de Intrusão:

(A) de host (HIPS), de rede (NIPS) e virtual (VIPS).
(B) de rede (NIPS), de host (HIPS) e sem fio (WIPS).
(C) de host (HIPS), de rede (NIPS) e sem fio (WIPS).
(D) de rede (NIPS), de host (HIPS) e virtual (VIPS).

Questão 45

(Correta: C)

O Microsoft 365 E5 oferece várias funcionalidades de proteção de informações, como detecção e mitigação de ameaças, proteção de dados sensíveis e conformidade regulatória. Entre as funcionalidades, uma protege contra ameaças como phishing, ransomware e outros ataques cibernéticos, monitora e-mails, links e anexos, e oferece detecção proativa e resposta a incidentes.

Essa funcionalidade é conhecida como Microsoft:

(A) Purview for Office 365.
(B) SkyDrive for Office 365.
(C) Defender for Office 365.
(D) Antivírus for Office 365.

Questão 46

(Correta: A)

Dispositivos de Internet das Coisas (IoT) são objetos computadorizados conectados à internet, tais como câmeras de segurança em rede, refrigeradores inteligentes e automóveis com recursos WiFi. A segurança da IoT é o processo de proteger esses dispositivos e garantir que eles não introduzam ameaças em uma rede. Nesse contexto, para esses dispositivos é empregado um tipo de autenticação mútua, que ocorre quando ambos os lados de uma conexão de rede se autenticam. Nesse sentido, um recurso é importante para a segurança da IoT, porque garante que apenas dispositivos e servidores legítimos possam enviar comandos ou solicitar dados. Além de usar a criptografia em todas as comunicações na rede para que os invasores não possam interceptá-las.

Esse recurso é conhecido como:

(A) mTLS.
(B) API Shield.
(C) Filtragem de DNS.
(D) Bootnet DDoS.

Questão 47

(Correta: B)

Contêineres são pacotes leves do código do aplicativo com dependências, como versões específicas de ambientes de execução de linguagem de programação e bibliotecas necessárias para executar seus serviços de software. Os *contêineres* tem por função oferecerem um mecanismo de empacotamento lógico em que os aplicativos podem ser abstraídos pelo ambiente em que são efetivamente executados. Os desenvolvedores usam a estruturação em *contêiner* para criar e implantar aplicações modernas devido a diversas vantagens, das quais uma é caracterizada por meio da utilização da estruturação em contêiner para implantar aplicações em vários ambientes sem precisar reescrever o código do programa. Nesse caso, os desenvolvedores criam uma aplicação uma vez e a implantam em vários sistemas operacionais. Por exemplo, eles executam os mesmos *contêineres* nos sistemas operacionais Linux e Windows.

Essa vantagem é conhecida como:

(A) Escalabilidade.
(B) Portabilidade.

(C) Agilidade.
(D) Modularidade.

Questão 48

(Correta: C)

Um Sistema de Detecção de Invasão - IDS é uma tecnologia de rede desenvolvida originalmente para detectar exploits de vulnerabilidades em um aplicativo ou computador específicos, podendo ser também um dispositivo que só detecta. O IDS monitora o tráfego e informa os resultados a um administrador. Um IDS funciona apenas na detecção de ameaças potenciais, sendo colocado fora da banda na infraestrutura da rede. Em consequência, um IDS não está no caminho de comunicação em tempo real entre o remetente e o destinatário da informação. Entre os tipos mais comuns de IDS, dois são descritos a seguir.

I.Monitora uma rede totalmente protegida, sendo implantado em toda a infraestrutura em pontos estratégicos, como nas sub-redes mais vulneráveis. Esse tipo monitora todo o tráfego que flui de e para dispositivos na rede, fazendo determinações com base no conteúdo dos pacotes e nos metadados.

II.Monitora a infraestrutura do computador na qual está instalado, sendo implantado em um endpoint específico para protegê-lo contra ameaças internas e externas. Esse tipo de IDS faz isso analisando o tráfego, registrando atividades maliciosas e notificando as autoridades designadas.

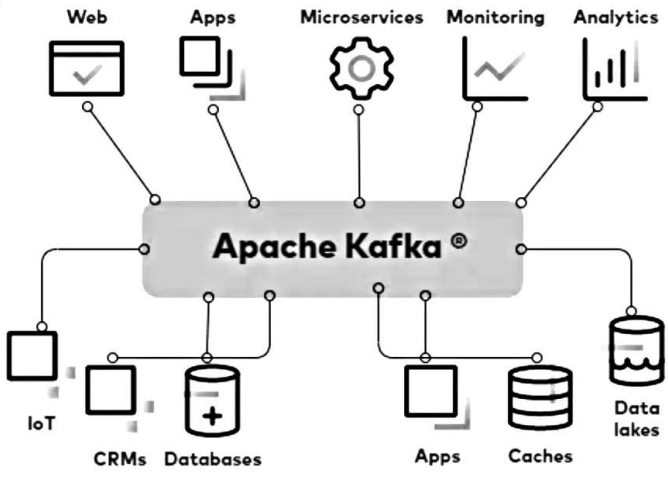
Esses dois tipos de IDS são conhecidos, respectivamente, pelas siglas:

(A) AIDS e HIDS.
(B) NIDS e PIDS.
(C) NIDS e HIDS.
(D) AIDS e PIDS.

Questão 49

(Correta: B)

Apache Kafka é uma plataforma *open-source* para *streaming* de dados, mensagens e eventos, possuindo alta performance, escalabilidade e disponibilidade. Nesse contexto, observe a figura abaixo:



Por uma visão mais simplificada, o *Kafka* parte de uma estrutura de Tópico, com produtores e consumidores, que internamente pode ter uma ou muitas partições . Outra divisão do *Kafka* são miniclusters/servidores de armazenamento internos de um Servidor/*cluster Kafka*, que constituem cópias uns dos outros para garantir escalabilidade e disponibilidade de mensagens. Um outro elemento importante que precisa ser mencionado é um serviço de gerenciamento de recursos e configurações entre os corretores, responsável por fazer a sincronização distribuída, e caso um dos corretores venha a falhar e fique indisponível, outro corretor assume a responsabilidade pois ele estará devidamente atualizado.

Os miniclusters/servidores de armazenamento internos e serviço de gerenciamento de recursos e configurações entre os corretores são conhecidos, respectivamente, como:

(A) Templates e Zookeper.
(B) Brokrers e Zookeper.
(C) Brokrers e RabbitMQ.
(D) Templates e RabbitMQ.

Questão 50

(Correta: B)

No contexto da Internet, portas são muito usadas para determinar quais aplicações podem rodar em um dispositivo na rede e quais não podem, ressaltando que sem elas, qualquer aplicação poderia rodar, criando uma enorme brecha de segurança para códigos maliciosos. Com as portas, um firewall pode ser usado para bloquear todas as portas, exceto aquelas que rodam serviços realmente necessários para o dispositivo. Uma porta é um número de 16 bits, variando de 0 a 65535, valendo para o TCP e para o UDP. Existem muitas portas bem-conhecidas e registradas.

Na comunicação com o DNS, HTTPS e SMTP TLS as portas são, respectivamente:

(A) 22, 465 e 587
(B) 53, 443 e 587
(C) 22, 443 e 143
(D) 53, 465 e 143

Questão 51

(Correta: A)

Java, como plataforma de programação, é composta de uma máquina virtual java (JVM), um completo conjunto de APIs (bibliotecas) e a linguagem Java orientada a objetos, constituindo uma tecnologia independente de sistema operacional e hardware. Em Java, o acesso direto a uma variável de instância de um objeto pode não estar habilitado. Quando se declara uma variável de instância, pode-se, opcionalmente, definir um modificador de variável, seguido pelo tipo e identificador daquela variável. O escopo de uma variável de instância pode ser controlado pelo uso dos modificadores de variáveis, de acordo com a classificação listada a seguir.

I.MA1 - Quando qualquer um pode acessar variáveis de instância públicas.

II.MA2 - Quando métodos do mesmo pacote ou subclasse podem acessar variáveis de instância protegidas.

III.MA3 -Quando apenas métodos da mesma classe, excluindo métodos de uma subclasse, podem acessar variáveis de instâncias privadas.

Os modificadores de acesso MA1, MA2 e MA3 são denominados, respectivamente:

(A) public, protected e private.
(B) private, protected e public.
(C) private, public e protected.
(D) public, private e protected.

Questão 52

(Correta: B)

No que diz respeito aos malwares maliciosos, um constitui um tipo projetado para dar aos hackers acesso e controle sobre um dispositivo, sendo que além de afetarem o software e o sistema operacional, alguns também podem infectar o hardware e o firmware do computador. Esses malwares são especializados em ocultar a sua presença, mas enquanto permanecem escondidos, eles estão ativos. Na verdade é um software usado por criminosos cibernéticos para obter controle sobre um computador ou rede alvo, podendo por vezes aparecer como uma única peça de software, mas frequentemente são compostos por uma coleção de ferramentas que permitem aos hackers o controle a nível de administrador sobre o dispositivo alvo.

Esse malware é conhecido por:

(A) kaspersky
(B) rootkit
(C) sniffer
(D) avira

Questão 53

(Correta: A)

No que tange à prevenção de riscos na segurança da informação, os controles têm por objetivo neutralizar eventos potencialmente negativos que venham a ocorrer numa organização. Nesse sentido, existem três tipos de controles de segurança para um sistema de informação, descritos a seguir.

I.Foca a gestão do risco e a gestão da segurança do sistema de informação.

II.É primariamente implementado e executado por pessoas, em oposição a sistemas.

III.É primariamente executado e implementado pelo sistema de informação, através de mecanismos contidos nos componentes de hardware, software ou firmware presentes no sistema.

Esses controles de segurança são conhecidos, respectivamente, como:

(A) Gerencial, operacional e técnico.
(B) Gerencial, técnico e operacional.
(C) Operacional, gerencial e técnico.
(D) Operacional, técnico e gerencial.

Questão 54

(Correta: A)

Na ITILv4, o modelo de gestão de TI foi alterado para atender as necessidades da Era Digital , com foco na criação do Sistema de Valor de Serviço (SVS) para os usuários, na condução de estratégias de negócios e na adaptação à transformação digital. As práticas do ITIL 4 constituem um conjunto de recursos necessários para realizar o trabalho ou atingir um objetivo, enfocando uma visão holística do sistema de serviços, ao considerar elementos como cultura, tecnologia, informações e gerenciamento de dados.

No contexto da ITILv4, duas são práticas de gestão de serviço, respectivamente, os Gerenciamentos de:

(A) Ativos de TI e Catálogo de Serviços.
(B) Segurança da Informação e Riscos de Incidentes.
(C) Desenho do Serviço e Implantação.
(D) Análise do Negócio e Projetos de Testes.

Questão 55

(Correta: A)

No que tange à segurança da informação, um tipo visa evitar/dificultar as falhas nos equipamentos e instalações como, por exemplo, que causam problemas com ativos,

furtos e acidentes. Outro tipo tem por objetivo evitar/dificultar o uso inadequado de dados, softwares, programas e sistemas como, por exemplo, invasões hacker e roubo de dados.

Esses tipos são conhecidos, respectivamente, como segurança:

(A) Física e lógica.
(B) Preditiva e corretiva.
(C) Corretiva e preditiva.
(D) Lógica e física.

Questão 56

(Correta: D)

Protocolos de redes para cibersegurança são aqueles que garantem a integridade e segurança dos dados transmitidos pelas conexões de rede. Nesse contexto, o tipo específico usado vai depender dos protegidos e da conexão de rede, sendo definida as técnicas e procedimentos necessários para proteger os dados da rede contra tentativas não autorizadas ou maliciosas de ler ou filtrar informações. Um desses protocolos oferece segurança a nível de IP, protegendo a comunicação entre redes ou hosts, enquanto que outro oferece autenticação e criptografia para gerenciamento de dispositivos de rede.

Esses dois protocolos de cibersegurança são conhecidos, respectivamente, como:

(A) IPSec e H-323
(B) SIP e H-323
(C) SIP e SNMPv3
(D) IPSec e SNMPv3

Questão 57

(Correta: A)

A criptografia é usada para proteger os dados contra roubo, alteração ou comprometimento e funciona transformando os dados em um código secreto que só pode ser desbloqueado com uma chave digital exclusiva. A criptografia simétrica usa a mesma chave para criptografia e descriptografia. A criptografia assimétrica usa duas chaves separadas para criptografar e descriptografar dados.

Duas siglas que representam dois exemplos de criptografia, sendo uma simétrica e outra assimétrica são, respectivamente:

(A) AES e RSA
(B) RSA e ECC
(C) DES e AES
(D) ECC e DES

Questão 58

(Correta: D)

Atualmente, existem diversas ferramentas para emprego na área da segurança cibernética, cada uma com suas peculiaridades. Duas delas são caracterizadas a seguir.

I.Foi projetada especificamente para minimizar a tomada de decisões, usando um processo de três etapas para coletar dados de sistemas e dispositivos de TI, que inclui orquestração, automação e resposta. Essa ferramenta busca e identifica vulnerabilidades com base em grandes quantidades de dados coletados, tomando as decisões imediatas e precisas e eliminando o risco de erro humano.

II.Foi projetada como uma solução de segurança cibernética que usa algoritmos e aprendizado de máquina para detectar anomalias no comportamento dos usuários, bem como nos roteadores, servidores e endpoints da rede. È uma ferramenta que busca comportamentos incomuns e irregularidades de padrões e alerta o administrador da rede ou usa funções de desconexão automática para anular ameaças antes que elas se tornem sérias.

Essas ferramentas são conhecidas, respectivamente, pelas siglas:

(A) CASB e XDR
(B) SOAR e XDR
(C) CASB e UEBA
(D) SOAR e UEBA

Questão 59

(Correta: C)

Tendo por foco o Modelo de Referência OSI/ISO, o TCP é um protocolo dito com conexão que opera em uma determinada camada, que tem por função garantir que os dados sejam entregues ao destino de forma eficiente e correta, responsável pela comunicação de ponta a ponta na rede, enquanto que o IP é sem conexão, opera em outra camada desse modelo, identifica origem e destino dos dados transferidos, sendo responsável por produzir os pacotes de rede e roteá-los pelo melhor caminho possível.

Os protocolos TCP e IP operam nas camadas do Modelo OSI/ISO conhecidas, respectivamente, como:

(A) Apresentação e rede.
(B) Transporte e enlace.
(C) Transporte e rede.
(D) Apresentação e enlace.

Questão 60

(Correta: B)

A computação em nuvem é a disponibilidade sob demanda de recursos computacionais, que incluem armazenamento e infraestrutura, como serviços pela Internet, eliminando a necessidade de indivíduos e empresas gerenciarem os próprios recursos físicos enquanto pagam apenas pelo que usarem. Entre os tipos de implantação de computação em nuvem, duas são

descritas a seguir.

I.É definida como aquelas criadas, gerenciadas e pertencentes a uma única organização e hospedadas de modo particular nos data centers dela, geralmente conhecidos como "no local". Essas nuvens oferecem maior controle, segurança e gerenciamento de dados, enquanto ainda permitem que usuários internos se beneficiem de um pool compartilhado de recursos de computação, armazenamento e rede.

II.É definida como aquelas que são executadas por provedores de serviços de nuvem de terceiros. Eles oferecem recursos de computação, armazenamento e rede pela Internet, permitindo que as empresas acessem recursos compartilhados sob demanda com base nos requisitos exclusivos e nas metas de negócios.

Esses dois tipos de implantação são conhecidos, respectivamente, como nuvens:

(A) híbridas e públicas.

(B) privadas e públicas.

(C) privadas e compartilhadas.

(D) híbridas e compartilhadas.