- Cada um dos itens das provas objetivas está vinculado ao comando que imediatamente o antecede. De acordo com o comando a que cada um deles esteja vinculado, marque, na **Folha de Respostas**, para cada item: o campo designado com o código **C**, caso julgue o item **CERTO**; ou o campo designado com o código **E**, caso julgue o item **ERRADO**. A ausência de marcação ou a marcação de ambos os campos não serão apenadas, ou seja, não receberão pontuação negativa. Para as devidas marcações, use a **Folha de Respostas**, único documento válido para a correção das suas provas objetivas.
- Em seu caderno de provas, caso haja item(ns) constituído(s) pela estrutura **Situação hipotética:** ... seguida de **Assertiva:** ..., os dados apresentados como situação hipotética devem ser considerados premissa(s) para o julgamento da assertiva proposta.
- Nos itens que avaliarem **conhecimentos de informática** e(ou) **tecnologia da informação**, a menos que seja explicitamente informado o contrário, considere que todos os programas mencionados estão em configuração-padrão e que não há restrições de proteção, de funcionamento e de uso em relação aos programas, arquivos, diretórios, recursos e equipamentos mencionados.
- Eventuais espaços livres — identificados ou não pela expressão "Espaço livre" — que constarem deste caderno de provas poderão ser utilizados para rascunho.

-- PROVAS OBJETIVAS --

-- CONHECIMENTOS GERAIS --

LÍNGUA PORTUGUESA

A cibersegurança, embora seja um tema há muito discutido em âmbito global, é um campo relativamente novo no Brasil. No entanto, tem ganhado destaque por conta da intensa migração de dados para ambientes em nuvem e da interconexão praticamente global de dispositivos na Internet. A proliferação de dispositivos conectados à Internet, desde eletrodomésticos até equipamentos industriais, aumentou consideravelmente a superfície de ataque, transformando o cenário de riscos. O que antes parecia ficção científica, como geladeiras ou medidores de pressão de gasodutos conectados à rede de computadores, agora é uma realidade tangível.

Entretanto, a adoção apressada de tecnologias conectadas à Internet muitas vezes ocorre sem a devida atenção à segurança. Essa falta de consideração em relação à cibersegurança pode expor empresas a riscos substanciais, pois a falta de preparação e avaliação da superfície de ataque pode permitir que brechas sejam exploradas por agentes maliciosos.

Uma das principais questões, quando se fala em cibersegurança, é a de que não existe uma "bala de prata", ou seja, uma solução única para todas as falhas que podem ocorrer. Cada organização possui características, riscos e necessidades distintos, o que exige a criação de soluções personalizadas para mitigar ameaças específicas.

Nesse sentido, a Lei Geral de Proteção de Dados (LGPD) desempenhou um papel significativo no cenário de cibersegurança ao estabelecer diretrizes para a prevenção de vazamentos e a proteção de dados. Empresas são agora obrigadas a adotar medidas proativas para evitar incidentes de segurança e garantir a privacidade dos dados. O investimento em cibersegurança deve ser entendido como um seguro de carro: deve-se investir na prevenção para minimizar os danos de um eventual incidente.

Internet: <economiasc.com> (com adaptações).

Julgue os itens que se seguem, com base nas ideias, no vocabulário e na estruturação linguística do texto precedente.

1 De acordo com o texto, a intensa migração de dados para ambientes em nuvem e a interconexão de dispositivos na Internet ofereceram destaque ao tema relativo à cibersegurança.

2 Entende-se do texto que a observância das medidas recomendadas de cibersegurança é suficiente para eliminar as possibilidades de ataques de agentes maliciosos.

3 Segundo as informações contidas no texto, a LGPD apresenta diretrizes para a prevenção de vazamentos e a proteção de dados.

4 No último período do texto, estabelece-se uma comparação entre o investimento em cibersegurança e o seguro de um carro.

5 O termo "proliferação" (terceiro período do primeiro parágrafo) é sinônimo da expressão **grande quantidade**.

6 No trecho "desde eletrodomésticos até equipamentos industriais" (terceiro período do primeiro parágrafo), a expressão "desde... até..." exprime um tipo de gradação da complexidade dos dispositivos mencionados, em que os eletrodomésticos seriam os mais simples, e os equipamentos industriais, os mais complexos.

7 É facultativo o emprego do sinal indicativo de crase no vocábulo "a" presente no trecho "pode expor empresas a riscos substanciais" (segundo período do segundo parágrafo).

8 No segundo período do segundo parágrafo, a conjunção "pois" poderia ser substituída por **então**, sem prejuízo do sentido e da correção gramatical do texto.

9 O emprego das aspas na expressão 'bala de prata' (primeiro período do terceiro parágrafo) indica que essa expressão consiste em um termo técnico.

10 O deslocamento da palavra "agora" (segundo período do último parágrafo) para o início do período, com o devido ajuste das letras iniciais maiúsculas e minúsculas, manteria o sentido e a correção gramatical do texto.

Espaço livre

A expectativa de vida da população brasileira ao nascer subiu no ano de 2021, segundo dados da Tábua Completa de Mortalidade de 2021 divulgados em novembro do ano passado pelo Instituto Brasileiro de Geografia e Estatística (IBGE). Os dados, publicados no Diário Oficial da União, mostram que o número subiu de 76,8 para 77 anos na comparação com 2020. Anualmente, o IBGE divulga esses números para o total da população brasileira, com data de referência em 1.º de julho do ano anterior e para todas as idades, conforme prevê o artigo 2.º do Decreto n.º 3.266/1999.

As informações sobre a expectativa de vida da população são usadas para a tomada de decisão em várias políticas públicas. Esse dado é utilizado, por exemplo, para determinar o fator previdenciário no cálculo das aposentadorias do Regime Geral de Previdência Social. Na divulgação dos números de 2020, o IBGE informou que as mortes decorrentes da pandemia de covid-19 não foram incluídas no levantamento e que essas informações só devem ser incorporadas na divulgação de 2023, referente ao ano de 2022. Mesmo assim, a inclusão seria apenas em caráter preliminar. Portanto, a divulgação seguiu a mesma metodologia do ano anterior, sem o impacto da pandemia.

"É bem provável que em 2023 a gente tenha uma Tábua preliminar (corrigida pela covid-19) para o Brasil; para as unidades da Federação, são necessários os dados do Ministério da Saúde, que demoram um pouco mais", explicou a demógrafa Izabel Guimarães Marri, gerente de população do IBGE na ocasião. "Em 2024, a gente vai ter a Tábua (referente a 2023) com todos os ajustes e estudos por unidades da Federação", previu.

Internet: <noticias.uol.com.br> (com adaptações).

Julgue os itens que se seguem, relativos às ideias e a aspectos linguísticos do texto precedente.

11 Depreende-se do texto que a expectativa de vida do brasileiro vem subindo a cada ano.

12 De acordo com o texto, a informação a respeito da expectativa de vida no país é relevante, entre outros fatores, para o cálculo das aposentadorias.

13 Segundo as informações do texto acerca da mencionada pesquisa do IBGE, a pandemia de covid-19 não impactou negativamente a expectativa de vida do brasileiro em 2020.

14 De acordo com as informações do texto, a Tábua Completa de Mortalidade referente ao ano de 2020 foi publicada com atraso em decorrência da pandemia de covid-19, deflagrada naquele ano.

15 A supressão das vírgulas que isolam a expressão "publicados no Diário Oficial da União" (segundo período do primeiro parágrafo) manteria a correção gramatical do texto.

16 A substituição da palavra "sobre" (primeiro período do segundo parágrafo) por **sob** não prejudicaria a correção gramatical nem a coerência do texto, mas alteraria o seu sentido original.

17 No terceiro período do segundo parágrafo, ambas as orações iniciadas pelo vocábulo "que" expressam circunstância de causa em relação à primeira oração do período — "Na divulgação (...) informou".

18 No primeiro período do último parágrafo, o vocábulo 'bem' intensifica o sentido do termo 'provável'.

19 A substituição de 'a gente vai ter' (último período do texto) por **será divulgada** conferiria mais formalidade ao trecho do texto em questão.

20 Mantendo-se as ideias do texto, o trecho 'para as unidades da Federação, são necessários os dados do Ministério da Saúde, que demoram um pouco mais' (último parágrafo) poderia ser reescrito, de maneira gramaticalmente correta, da seguinte forma: **É necessário, para as unidades da Federação, dados do Ministério da Saúde, que demoram um pouco mais**.

LÍNGUA INGLESA

Welcome To the Next Generation Of Business Intelligence

The Business Intelligence (BI) industry has long promised a future where every worker can use data to make smarter business decisions. Although that promise continues to be out of reach for most companies, the industry has come a long way over the past few decades, and we believe we are on the cusp of a new generation of BI that will finally turn that promise into reality.

Business Intelligence is built on an old data culture that relies on technical experts. In the early days of reporting, those experts were called IT. As technology evolved and tools became easier, the progression of BI moved to reports and dashboards delivered by new experts—analysts. This made analytics more accessible, but still didn't make self-service data insights a reality across the business. Here's why: Instead of using technology to put data in front of people where they already are working, we continue to ask people to leave their business apps and turn to dedicated tools or dashboards for answers.

This process is disruptive and inefficient, and often causes users to write it off completely. Dashboards don't have built-in analytics processes; they share information but do not provide recommended courses of action at the right moment or in a decision maker's workflow. Business professionals want exactly that: They want a final answer and recommendations on what to do next. They would rather have data and actionable insights come in easily digestible bites versus needing to dig for answers in dashboards and reports. And the truth is they are digging; dashboards are often too broad to address multiple questions, too difficult to customize, and frankly, have too many insights.

For analytics to advance, we must extend dashboards or deliver personalized intelligence to more decision makers. In fact, experts predict that "dashboards will be replaced with automated, conversational, mobile and dynamically generated insights customized to a user's needs and delivered to their point of consumption. This shifts the insight knowledge from a handful of data experts to anyone in the organization." Now, instead of wasting time jumping from where the data resides (in dashboards) to where work is done, embedded analytics enables users to do both simultaneously: get insights and take action.

Internet: <www.forbes.com> (adapted).

Based on the preceding text, judge the following items.

21 The promise that the Business Intelligence industry has made about workers being able to use data to make smarter decisions has already become reality.

22 Technical experts, who were previously called IT, had no influence in the construction of BI.

23 Embedded analytics do not allow users to get insights and take action at the same time.

24 The evolution of technology and the emergence of easier tools helped Business Intelligence to progress, and made analytics more accessible.

25 Business professionals would prefer receiving data and practical insights in easily understandable portions, as opposed to having to search for answers within complex dashboards and reports.

Microplastics found in human heart for first time

A new study suggests invasive medical procedures may be an overlooked route of microplastics exposure, raising concerns about potential health risks. Minute particles of plastic (called microplastics) are everywhere. They've been found in our water, in our food, and in the air we breathe, according to a 2021 scientific review. Just a year later, another study found microplastics in the human bloodstream. Now, in what researchers are calling a first, microplastics have been detected in the heart tissues of individuals who underwent cardiac surgery.

According to the author of the research, the detection of microplastics *in vivo* is alarming, and more studies are necessary to investigate how the microparticles enter the cardiac tissues and the potential effects of microplastics on long-term prognosis after cardiac surgery. The author and his team used direct infrared imaging, and identified 20 to 500 micrometer-wide particles made from eight types of plastic. The scientists also found plastic particles in blood samples collected from participants. They added that "microplastics are highly likely to distribute in various organs throughout the body."

A fraction of the plastic pieces identified had a diameter too large to likely enter the body through inhalation or ingestion, according to the analysis. This indicated that the heart operation itself may permit direct access of microplastics to the bloodstream and tissues. The researchers cited previous scientific investigation showing that microplastics have been detected in the air in operating rooms and could directly enter a patient whose organs are exposed to the air during surgery.

Such large particles may also come from equipment and materials used in a heart operation, including surgical incision protective film, intravenous therapy bags, tubing, and syringes. The types of plastics detected might also offer evidence that microplastics could be introduced during surgery, which may raise the risk of heart disease.

Internet: <www.everydayhealth.com> (adapted).

Based on the preceding text, judge the following items.

26 Besides being in all places, microplastics were found, according to a 2022 study, in the human bloodstream.

27 The text suggests that the possibility of exposure to microplastics during surgery could increase the risk of heart disease.

28 The text informs that microplastics were detected in the body of patients who died during heart surgeries.

29 We can infer that the scientists did not like the way microplastics were distributed in many organs of the body.

30 Because of the size of some of the plastic pieces found, the researchers believe that they probably could not have entered the patients' bodies through their mouth or nose.

RACIOCÍNIO LÓGICO

P_1: "Se houver resistência de populares ou depredação de patrimônio, a polícia agirá."

P_2: "Se a polícia agir, a ambulância será necessária."

P_3: "Não houve depredação de patrimônio, mas a ambulância foi necessária."

C: "Houve resistência de populares."

Tomando por referência as proposições precedentes, julgue os itens seguintes.

31 O argumento que tem por premissas as proposições P_1, P_2 e P_3, e, por conclusão, a proposição C, é válido.

32 A tabela-verdade da proposição P_1 tem menos de 6 linhas.

33 A proposição P_2 é equivalente à proposição "Se a polícia não agir, a ambulância não será necessária.".

34 A negação de P_1 pode ser escrita como "Houve depredação de patrimônio ou a ambulância não foi necessária.".

35 Caso seja verdadeira a proposição "A ambulância será necessária.", a proposição P_2 será também verdadeira, independentemente do valor lógico de sua outra proposição simples constituinte.

ATUALIDADES

No que se refere a temas atuais no Brasil e no mundo, julgue os itens a seguir.

36 Em 2023, um incêndio no Havaí devastou boa parte da ilha, mas a tecnologia utilizada nas buscas por sobreviventes mapeou de imediato o tamanho da tragédia e a classificou como a mais mortal dos Estados Unidos da América.

37 O contexto da invasão militar da Ucrânia pela Rússia provocou instabilidade na política interna do grupo formado por Brasil, Rússia, Índia, China e África do Sul (BRICS), o que levou o presidente russo Vladimir Putin a solicitar seu afastamento do bloco.

38 Uma vez que o modelo de gerenciamento e transmissão de energia utilizado no Brasil é o Sistema Interligado Nacional (SIN), em caso de queda de energia elétrica nesse sistema, todas as unidades federativas conectadas a ele são impactadas.

39 No Brasil, houve aumento, em 2023, da taxa do Sistema Especial de Liquidação e de Custódia (SELIC) pelo Comitê de Política Monetária (COPOM) do Banco Central, o que provocou um aumento do empréstimo pessoal, do consumo e da inadimplência entre a população brasileira.

40 Na Argentina, em agosto de 2023, período em que se executaram as eleições primárias — cujo objetivo é definir os candidatos que concorrerão à Presidência da República —, a inflação ao consumidor cresceu mais de 100% em comparação ao mesmo mês do ano anterior.

LEGISLAÇÃO ACERCA DE SEGURANÇA DE INFORMAÇÕES E PROTEÇÃO DE DADOS

Considerando o disposto na legislação referente à segurança da informação e à proteção de dados, julgue os próximos itens.

41 Apesar de, nos termos da Lei de Acesso à Informação, o serviço de busca e fornecimento de informação ser gratuito, o órgão ou a entidade consultada poderá cobrar do solicitante o valor necessário ao ressarcimento de custos quando esse serviço demandar a reprodução de documentos.

42 De acordo com a Lei n.º 12.737/2012, que dispõe sobre delitos informáticos, quem produz dispositivo ou programa de computador com o intuito de permitir a prática de invasão de dispositivo informático incorre na mesma pena de quem efetivamente procede à conduta de invadir dispositivo informático alheio.

43 De acordo com o que dispõe a Lei n.º 12.965/2014 — Marco Civil da Internet —, o provedor responsável pela guarda dos registros de conexão e de acesso a aplicativos de Internet está impedido de disponibilizar, sem expressa ordem judicial, quaisquer dados cadastrais de seus usuários, inclusive a entidades ou autoridades administrativas que detenham competência legal para requisitá-los.

44 De acordo com a Lei Geral de Proteção de Dados Pessoais, o tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico de um dos pais ou responsável legal, devendo o controlador realizar todos os esforços razoáveis, consideradas as tecnologias disponíveis, para verificar que o consentimento foi dado pelo responsável pela criança.

45 No âmbito da Estratégia Nacional de Segurança Cibernética, a ação da indústria de adotar padrões internacionais de segurança e privacidade no desenvolvimento de novos produtos tecnológicos desde a sua concepção está vinculada à ação estratégica de incentivar a concepção de soluções inovadoras em segurança cibernética.

46 Segundo o Decreto n.º 10.748/2021, a Rede Federal de Gestão de Incidentes Cibernéticos deve ser coordenada por um colegiado técnico composto por representantes dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional.

47 De acordo com a Política Nacional de Segurança da Informação, regulamentada pelo Decreto n.º 9.637/2018, a participação de membros indicados no Comitê Gestor da Segurança da Informação será considerada prestação de serviço público especificamente remunerada.

48 Entre as ações de prevenção destacadas no Plano de Gestão de Incidentes Cibernéticos para a administração pública federal incluem-se a implementação de controles de segurança; o gerenciamento de vulnerabilidades; e a conscientização e capacitação.

49 Segundo o disposto no Decreto n.º 11.200/2022 — Plano Nacional de Segurança de Infraestruturas Críticas —, dos órgãos e das entidades que atuam na segurança de infraestruturas críticas requer-se que acompanhem e avaliem continuamente a situação das infraestruturas críticas e que implementem, quando necessário, medidas de proteção a elas.

50 No âmbito da Instrução Normativa GSI n.º 1, a segurança da informação abrange, entre outros aspectos, a segurança pública lógica, a defesa aeroespacial digital e a segurança das infraestruturas de comunicação.

Espaço livre

-- CONHECIMENTOS ESPECÍFICOS --

Julgue os itens a seguir, relativos aos protocolos SNMPv1, SNMPv2 e SNMPv3.

51 Uma das características de segurança do SNMPv1 é o uso de comunidades na forma de textos simples.

52 No SNMPv1, as comunidades estão restritas a dois tipos apenas, leitura e leitura e escrita.

53 O SNMPv2 utiliza, por padrão, as portas UDP 31 para agente e UDP 32 para o gerente.

54 Mesmo com funcionalidades adicionais de segurança, o SNMPv3 permite violação de integridade, pois é possível garantir que um pacote foi alterado em trânsito.

55 No SNMPv2, foram acrescentadas as PDUs (*protocols data units*) *getbulk request* e *inform*.

56 Diferentemente do SNMPv1 e do SNMPv2, o SNMPv3 fornece serviços de autenticação e privacidade.

Com base no *management information base* (MIB), elemento que consta dentro das especificações de RMON, julgue os itens a seguir.

57 A MIB RMON apresenta mecanismos para um gerente configurar e controlar um monitor remoto, mas não consegue coletar seus dados nem receber seus alarmes.

58 Uma das características da MIB-II é que o gerenciamento é realizado em cada dispositivo individualmente, ou seja, cada dispositivo deve ter sua MIB e seu agente.

Julgue os itens a seguir, relativos ao RMON.

59 A versão RMON1 define vinte e dois grupos de MIB para o monitoramento básico de rede.

60 Existem duas versões do RMON, conhecidas por RMON1 ou RMONv1, e RMON2 ou RMONv2.

Acerca de criptografia, julgue os itens subsequentes.

61 Utilizando algoritmo de chave pública, a criptografia pode implementar o princípio da autenticidade e o da irretratabilidade ou não repúdio.

62 Em uma conexão criptografada, o princípio da disponibilidade é, de fato, atingido.

63 *Blowfish* é uma cifra simétrica de blocos que utiliza chave com tamanho variável de 32 *bits* a 448 *bits* e que foi criada como alternativa gratuita e rápida aos algoritmos criptográficos existentes.

64 AES é um método de criptografia de cifra em bloco, de tamanho de 64 bits, considerado inseguro para muitas aplicações.

65 Em algoritmo de criptografia simétrica, a mensagem cifrada com chave pública pode somente ser decifrada pela sua chave privada correspondente.

A respeito de proteção contra *softwares* maliciosos, sistemas de detecção de intrusão, segurança de servidores e sistemas operacionais, certificação digital, assinatura digital e gestão de riscos, julgue os itens que se seguem.

66 *Spyware* é um programa que coleta informações no computador do usuário e as envia para terceiros, violando a privacidade.

67 Os sistemas de detecção de intrusão (IDS, na sigla em inglês) fazem análise de atividades de uma rede, verificando o conteúdo das camadas superiores TCP/IP em busca de tentativas de ataque.

68 Em sistemas operacionais, há três tipos de sistemas de armazenamento de domínios de proteção, dos quais a lista de controle de acesso por coluna é o menos viável para grandes sistemas.

69 Segundo o padrão X.509, o certificado digital não deve conter a chave privada do usuário.

70 Gerenciamento de riscos é um processo contínuo que se aplica a todas as fases operacionais em que consequências de um risco específico são aceitas.

71 A assinatura digital em um documento garante a confidencialidade dos dados.

Considerando a ABNT NBR ISO/IEC 27005 e a NBR ISO 22301, julgue os itens subsequentes.

72 A ABNT NBR ISO/IEC 27005 provê metodologia específica para o gerenciamento de riscos em segurança da informação.

73 A definição e a seleção da estratégia de continuidade de negócios devem basear-se nos resultados da análise de impacto nos negócios e no processo de avaliação de riscos.

74 Na avaliação de desempenho, em desempenho deficitário, não devem ser incluídos não conformidades, quase acidentes e alarmes falsos.

75 Diante de riscos identificados que necessitam de tratamento, a organização deve tomar medidas proativas que reduzam a probabilidade de interrupção dos serviços ou diminuam o tempo de interrupção.

Com base na Lei Geral de Proteção de Dados Pessoais (LGPD), julgue os seguintes itens.

76 Aplica-se a LGPD na coleta e no tratamento de dados pessoais para fins particulares, jornalísticos, artísticos, de segurança pública e de defesa nacional.

77 O consentimento do titular para a realização da coleta de dados pessoais dispensa nova manifestação dele para o compartilhamento desses dados pelo controlador, por exemplo.

78 Dado pessoal é qualquer informação relacionada a uma pessoa natural identificada ou identificável.

79 A LGPD indica princípios de boa-fé que devem ser levados em consideração no tratamento de dados pessoais, como a transparência, que garante ao titular consulta facilitada e gratuita da integralidade dos seus dados pessoais.

Com relação aos conceitos de segurança cibernética, julgue os itens a seguir.

80 O objetivo do IDS (*intrusion detection system*) é detectar atitudes suspeitas, impróprias, incorretas ou anômalas. No entanto, ataques realizados por meio de portas legítimas do *firewall* não podem ser detectados por este sistema.

81 Ao contrário do IDS (*intrusion detection system*), que é um sistema passivo e que apenas analisa o tráfego, gerando alarmes, o IPS (*intrusion prevention system*) não faz só a detecção do acesso indevido, mas o bloqueio desse tráfego também.

82 A técnica BAS (*breach attack simulation*) é utilizada para proteger sistemas de TI contra ameaças de segurança, com acesso a meios centralizados de consultas e compartilhamento de informações sobre ameaças.

83 Apesar do SIEM ser uma solução usada para identificar ameaças e vulnerabilidades por meio da combinação dos gerenciamentos de informações de segurança e de eventos de segurança, ela não é adequada para investigações forenses de incidentes de segurança.

Considerando o *framework* de segurança cibernética do NIST, julgue os itens a seguir.

84 Das cinco funções do *framework* de segurança cibernética do NIST, a função identificar é aquela que é destinada a desenvolver um entendimento organizacional para a gestão dos riscos de segurança cibernética.

85 As cinco funções principais do referido framework estabelecem uma sequência de execução para formar uma cultura operacional que aborda o risco dinâmico de segurança cibernética.

Acerca de metodologia de operações de segurança, julgue os itens subsequentes.

86 As tecnologias de *firewall* incluem filtros de pacotes, filtros de pacotes dinâmicos, servidores *proxy* e NAT.

87 Um *proxy* pode atuar no nível de aplicação, em que haverá um *proxy* diferente para cada aplicação, ou ainda no nível de transporte, em que haverá um *proxy* genérico para conexões TCP e UDP.

88 O SIEM (*security information and event management*) é um conjunto de ferramentas de segurança que são integradas e tem o objetivo de concentrar as informações de segurança em uma única ferramenta.

89 O IPS se diferencia do IDS pelo fato de apenas realizar um monitoramento ativo dos eventos, sem, contudo, interferir neles.

Julgue os próximos itens, relativos a testes de penetração e a modelagem de ameaças.

90 Aplica-se a abordagem de teste de penetração *BlackBox* quando o grupo de teste não possui nenhuma informação real sobre o alvo e, nesse caso, deve-se começar com a coleta de informações.

91 STRIDE é uma metodologia de identificação de ameaças à segurança baseada em um processo de sete etapas para identificar, enumerar e classificar as ameaças.

92 Um teste de conhecimento pode ser escolhido se o objetivo for testar um novo tipo de ataque ou mesmo se a equipe quiser focar em um *host* específico da empresa.

Com base na segurança da informação, julgue os próximos itens, a respeito de gerenciamento de resposta a incidente.

93 De acordo com o NIST SP 800-61, duas das ações que são tomadas na etapa *postpincident activity* são: a identificação de controles que detectaram o incidente; e o levantamento de métricas e KPI's.

94 O guia NIST SP 800-61 (*computer security incident handling guide*) define quatro etapas a serem projetadas para apoiar tanto no planejamento quanto durante uma crise: *preparation*; *detection and analysis*; *containment*, *eradication*, *and recovery*; e *post-incident activity*.

De acordo com o que dispõem os conceitos de segurança da informação, julgue os itens que se seguem.

95 Para um uso maximizado do *framework* ATT&CK, recomenda-se utilizar todas as técnicas na matriz ATT&CK, assim haverá uma priorização das técnicas que representam o maior risco.

96 Uma das diferenças entre DAST e SAST é que enquanto o primeiro é uma abordagem de caixa preta, sem acesso ao código-fonte, o outro, é uma abordagem de caixa branca, que analisa o código fonte durante a fase de desenvolvimento.

97 O Pandas é uma das bibliotecas de Python que é utilizada para trabalhar com análise de dados e é utilizada em mineração de dados, por exemplo, por oferecer uma série de funções que permitem a leitura e manipulação de dados.

98 Em função de sua codificação mais robusta, os *firmwares* de IoT são mais sofisticados que os sistemas operacionais executados em computadores e *smartphones*, o que os torna imunes a falhas consequentes das vulnerabilidades conhecidas.

Considerando o padrão de redes sem fio 802.11g, julgue os itens seguintes.

99 A camada física do 802.11b não usa o espalhamento espectral por sequência direta (DSSS) ao passo que o 802.11b usa transmissão fechada em *unicast* de rádio.

100 O 802.11g utiliza a frequência de 2,4 GHz e permite até 54 Mbps de taxa nominal de transmissão.

Com base nos fundamentos de roteamento entre VLANs, julgue os itens a seguir.

101 O protocolo 801.Q deve ser suportado em um roteador capaz de realizar o roteamento entre VLANs.

102 O roteamento entre VLANs consiste no processo de confinamento do tráfego de rede de uma VLAN para que este não seja encaminhado para outra VLAN.

Julgue os seguintes itens, relativos às camadas do modelo OSI.

103 Os protocolos de transporte no modelo OSI são orientados à conexão somente.

104 Por fundamento, no modelo OSI, a camada de rede fornece os meios necessários para fazer a transferência de pacotes de um nó para outro nó conectado em redes diferentes.

Acerca das características fundamentais do protocolo IEEE 802.3, julgue os itens subsequentes.

105 O IEEE 802.3 define o método de acesso à rede local usando o CSMA/CD (*carrier-sense multiple access with collision detection*).

106 O IEEE 802.3 define como deve ser o controle de acesso da camada física e da camada de enlace de dados do padrão Ethernet com fio.

A respeito das características do protocolo UDP (*user datagram protocol*), julgue os itens que se seguem.

107 O UDP implementa por padrão a criptografia 3DES no modo de entrega de datagrama USER-MODE.

108 O UDP é um protocolo orientado à conexão e garante a entrega dos dados.

A respeito da Política de Segurança da Informação (POSIN), julgue os itens subsequentes.

109 Uma POSIN deve estar em conformidade com a legislação vigente, com as normas pertinentes, com os requisitos regulamentares e contratuais e com as melhores práticas de segurança da informação.

110 Competências e responsabilidades, apesar de serem importantes, não devem constar da POSIN, pois sua definição é restrita à alta administração da organização.

Julgue os próximos itens, relativos a gerenciamento de projetos, de acordo com o PMBOK 7.ª edição.

111 Um dos princípios estipulados pelo PMBOK 7.ª edição é o enfoque no valor, segundo o qual valor é o indicador de sucesso definitivo do projeto; nesse sentido, as equipes podem, para apoiar a percepção de valor dos projetos, alterar o foco das entregas para os resultados pretendidos.

112 Os domínios de desempenhos são executados em *sprints* em sequência de importância.

Julgue os itens seguintes, relativos à gestão de riscos.

113 A análise de riscos inclui a consideração das causas e fontes de risco, a probabilidade de ocorrer um evento específico, a probabilidade de que este evento provoque consequências e a gravidade dessas eventuais consequências.

114 Na gestão de riscos, o nível de risco refere-se à significância de um risco, demonstrada pela combinação das consequências e de seu impacto.

Considerando a ITIL 4, julgue os itens a seguir.

115 A solicitação de um usuário que inicia uma ação de serviço acordada como parte regular da entrega de serviço deve ser gerenciada pela prática de gerenciamento de incidente, de modo que se restaure a operação normal do serviço o mais rápido possível.

116 A prática de gerenciamento de segurança da informação tem como objetivo principal a elaboração e manutenção da política de segurança da informação da organização.

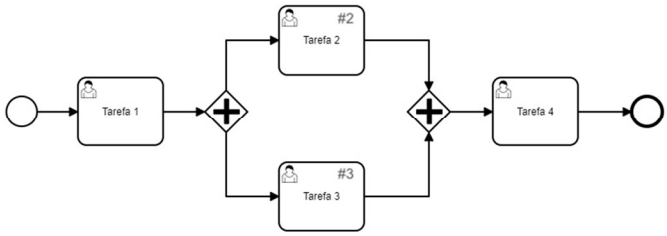
Com base no COBIT 2019, julgue os próximos itens.

117 No domínio entrega, serviço e suporte (DSS), há processos relacionados ao gerenciamento de solicitações e de incidentes de serviço, assim como ao gerenciamento de problemas e de continuidade.

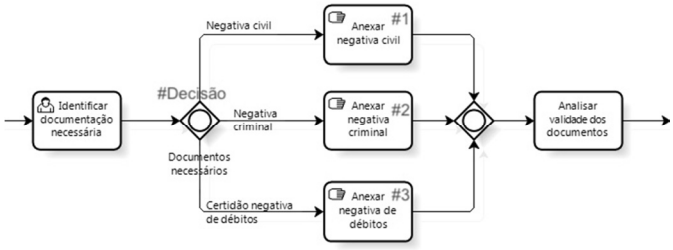
118 O processo estratégia gerenciada do domínio alinhar, planejar e organizar (APO) visa garantir que cada iniciativa da organização esteja claramente conectada a uma estratégia abrangente, de modo que haja transformação digital na organização.

No que se refere ao uso da notação BPMN para a gestão de processos e para a modelagem de processos de negócio, julgue os itens que se seguem.

119 De acordo com a notação BPMN apresentada na figura a seguir, a Tarefa 2 (`#2`) e a Tarefa 3 (`#3`) serão executadas concomitantemente.



120 De acordo com a notação BPMN apresentada na figura a seguir, apenas uma das tarefas `#1`, `#2` e `#3` será executada, ou seja, no momento de decisão (`#Decisão`), um único caminho deverá ser seguido.



Espaço livre