-- 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.

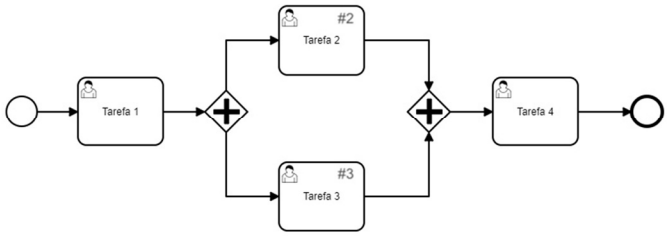
Com base no COBIT 2019, julgue os próximos itens.

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.

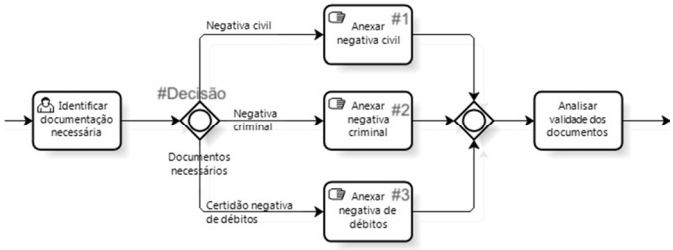
118 O processo estratégia gerenciada do domínio alinhar, planejar e organizar (APO) visa garantir que cada iniciativa da organização esteja claramente conectada a uma estratégia abrangente, de modo que haja transformação digital na organização.

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