-- CONHECIMENTOS ESPECÍFICOS --

A respeito do modelo de referência OSI, julgue os itens a seguir.

51 A camada de enlace de dados consegue transformar dados recebidos, desde que esses estejam íntegros e sem erros, senão correções devem ser feitas pela camada de rede.

52 A transmissão de bites 0 e 1 por meios elétricos que se conectam a uma interface de rede opera na camada física.

Acerca do modelo de referência TCP/IP, julgue os itens que se seguem.

53 O protocolo ICMP (*internet control message protocol*) opera na camada de enlace.

54 O protocolo TCP tem capacidade de operar no controle da transmissão, que permite a entrega sem erros de um fluxo de *bytes* entre dois computadores.

55 O protocolo IP opera na camada de transporte, que permite que *hosts* se comuniquem.

Com relação ao endereçamento IP e ao roteamento, julgue os itens subsequentes.

56 O protocolo OSPF (*open shortest path first*) é utilizado para roteamento dinâmico e possui suporte a enlaces ponto a ponto e redes de *broadcast*.

57 Uma máscara de rede de 23 bites pode ser utilizada em uma rede na qual seja necessário colocar 500 computadores para se comunicar diretamente.

58 Os endereços inseridos em um intervalo de 0.0.0.0 a 129.0.0.0 integram exclusivamente a classe A.

59 A demanda de um bloco de endereços com máscara de rede de 24 bites que necessite ser segmentado em pelo menos quatro sub-redes, capazes de comportar no mínimo 60 computadores cada uma, pode ser atendida utilizando-se uma máscara de 27 bites para cada sub-rede.

Quanto a serviços IP, julgue os itens subsecutivos.

60 O serviço SSH utiliza criptografias simétrica e assimétrica.

61 O serviço de DNS tem capacidade de associar nomes a endereços IPs.

62 O serviço SMTP é capaz de disponibilizar acesso remoto a servidores Linux, para que sejam executadas tarefas administrativas, como instalar e remover *softwares* em um servidor.

63 O serviço NTP é utilizado para o compartilhamento de arquivos em um ambiente de rede Unix.

64 O serviço DHCP pode ser utilizado para se atribuir um intervalo de endereços IP a um conjunto de computadores em uma mesma rede.

65 A principal função do serviço IMAP é controlar a lista de acesso aos arquivos compartilhados e por ele é possível compartilhar arquivos em uma rede local.

No que concerne a fundamentos de IPSEC, julgue os próximos itens.

66 São necessárias duas fases para se estabelecer uma VPN com IPSEC.

67 O 3DES e o AES podem ser utilizados como algoritmos de autenticação.

68 Na pilha de protocolos do IPSEC, existe o ESP (*encapsulating security payload*), que serve para a proteção *anti-replay* na comunicação.

Com base nas normas ABNT NBR ISO 27001 e 27005, julgue os próximos itens.

69 O processo de aceitação do risco da gestão de riscos e segurança da informação está alinhado com o processo de planejamento do SGSI (sistema de gestão de segurança da informação).

70 A tarefa específica de comprar um determinado risco com critérios predefinidos de risco, com objetivo de determinar a grandeza desse risco, é denominada análise de riscos.

71 A norma ABNT NBR ISO 27001 oferece diretrizes para um sistema de gestão de segurança da informação, enquanto a norma ABNT NBR ISO 27005 esclarece como gerenciar riscos de segurança da informação.

72 Quanto ao tratamento, a transferência de um risco para outra entidade pode criar novos riscos ou alterar os riscos já existentes.

A respeito do plano de continuidade de negócios (PCN), julgue os itens seguintes.

73 No PCN, o plano de contingência operacional (PCO) apresenta um conjunto de cenários de crises previamente definidos e de respectivos procedimentos de gestão da crise.

74 O processo de *Business Impact Analysis* (BIA) tem como objetivo produzir um relatório descrevendo os riscos potenciais específicos para a entidade, caso haja uma interrupção em seus negócios.

75 O grupo de administração de crises (GAC) estabelecido pelo PCN é responsável por acionar o grupo executivo em situações de emergência.

Com relação a criptografia e segurança de servidores e sistemas operacionais, julgue os itens subsequentes.

76 Em um servidor, o mecanismo de controle de roteamento atua nos serviços de autenticação da origem de dados, de confidencialidade e de integridade dos dados.

77 Funções *hash* têm como objetivo encriptar um texto claro para um texto cifrado utilizando uma chave secreta, garantindo que não seja possível o processo ao contrário (texto cifrado para texto claro).

78 Irretratabilidade é o mecanismo de segurança que prova que a mensagem foi enviada pela origem especificada e que foi recebida pelo destino especificado.

A respeito de segurança da informação, julgue os itens que se seguem.

79 No modelo PDCA (*Plan-Do-Check-Act*), a fase de *Plan* é responsável por avaliar e mensurar o desempenho de um processo de acordo com o SGSI.

80 Um *worm* tem como características a infecção de estações de trabalho, ao invés de arquivos, e a dispersão pela rede, utilizando múltiplas técnicas de replicação.

Quanto a tecnologias de LAN, MAN e WAN, julgue os próximos itens.

81 Em uma LAN com topologia anel, a rede inteira é desativada se houver ruptura em um dos cabos.

82 Com o uso de CSMA/CD, quando ocorre uma colisão de dados, imediatamente os computadores envolvidos tentam uma retransmissão, o que pode ocasionar outra colisão de dados.

83 A Ethernet opera a 10 Mbps, a Fast Ethernet opera a 100 Mbps e a Metro Ethernet opera a 1 Gbps.

84 O *hardware bridge* é utilizado para estender uma LAN, encaminhando adiante quadros completos, sem repassar interferências, entre dois segmentos de cabo.

No que se refere a equipamentos de redes, julgue os itens subsecutivos.

85 Para interconectar redes, os roteadores não são considerados computadores; um roteador tem como objetivo a transferência de dados entre as redes que ele conecta.

86 O *switch* possui a capacidade de aprender os endereços MAC dos equipamentos que estão conectados em suas portas.

Acerca de voz sobre IP e protocolos SIP e H.323, julgue os itens a seguir.

87 SIP e H.323 são capazes de negociar parâmetros de criptografia.

88 O protocolo H.323 possui padrões definidos a partir do seu projeto elaborado pelo IETF (Internet Engineering Task Force).

89 O protocolo SIP possui arquitetura monolítica e compatibilidade para comunicar-se com a Internet.

90 O término de chamadas por *timeout* é suportado pelo protocolo SIP.

91 O protocolo SIP é capaz de atender a conferências com recursos multimídia.

92 O formato de mensagens binário faz parte do protocolo SIP.

93 No protocolo H.323, o endereçamento pode ser feito por URL (*uniform resource locator*) e número de telefone.

Sobre VPN (*virtual private network*) IPSec e SSL, julgue os itens que se seguem.

94 A VPN SSL faz uso de recursos de certificados digitais como um dos mecanismos de controle de segurança.

95 VPNs do tipo SSL não suportam o uso de TLS para criptografar dados transmitidos em sua comunicação.

96 O IPSec faz uso da SA (*security association*), que agrega protocolos como o AH (*authentication header*), capazes de controlar a autenticidade e a integridade do pacote.

97 Em uma VPN do tipo IPSec, uma SA (*security association*) é identificada pelos seguintes parâmetros: endereço IP de destino e de origem e identificador do protocolo ESP (*encapsulating security payload*).

Com relação a gerenciamento de projetos com base no PMBOK V6, julgue os itens subsequentes.

98 Fatores ambientais da empresa e ativos de processos organizacionais são entradas do processo que determinam o orçamento.

99 O processo de criar a estrutura analítica do projeto (EAP) contém o registro de premissas como uma de suas saídas.

100 Nas entradas do processo de planejamento do escopo, estão previstos o termo de abertura do projeto e o plano de gerenciamento de riscos.

101 Durante o planejamento do gerenciamento da qualidade, é possível utilizar ferramentas e técnicas, sendo uma delas o planejamento de testes e inspeções.

102 O plano de gerenciamento de benefícios é uma das saídas do plano de gerenciamento do projeto.

103 Para que sejam estimados os custos do projeto, o processo considera documentos como o de registro de riscos e o de registro de lições aprendidas.

A respeito de ataques em redes e aplicações corporativas, julgue os próximos itens.

104 A técnica de IP *spoofing* consiste em um atacante alterar o cabeçalho IP de um pacote, como se partisse de uma origem diferente.

105 SQL *injection* consiste em inserir ou manipular consultas efetuadas pela aplicação, com o objetivo de diminuir sua *performance*.

106 Ataques da *ransonware* podem ser detectados de forma preditiva, logo depois de começar a infecção e antes de finalizar a infecção.

107 SYN *flooding* é um ataque do tipo DoS, em que uma grande quantidade de requisições de conexão causa o estouro da pilha de memória.

108 Enquanto ataques DoS têm como objetivo derrubar um servidor, ataques DDoS têm como objetivo derrubar o banco de dados da aplicação.

109 Uma das técnicas para *phishing* é a clonagem de sítios de instituições financeiras, com o objetivo de obter as credenciais de acesso do usuário.

No que se refere a becape, julgue os itens subsecutivos.

110 Uma política de becape deve abordar quais os dados a serem armazenados, a frequência de execução e quem será responsável pelo acompanhamento dos processos de becape.

111 Ao optar por becape na nuvem, a organização deve atentar para a armazenagem, que envolve o tempo para restauração em caso de incidente.

112 Uma das vantagens do becape diferencial, quando comparado com o becape incremental, é que ele utiliza um espaço menor de armazenamento.

113 No tipo de becape incremental, são copiados apenas os dados alterados ou criados após o último becape completo ou incremental.

Julgue os itens subsecutivos, com relação a *cloud computing*.

114 As aplicações do modelo SaaS (*Software as a Service*) devem utilizar banco de dados separado, tal que os dados de cada empresa ficam isolados dos dados das demais empresas.

115 Com parte de IaaS (*Infrastructure as a Service*), as máquinas virtuais (VM) persistentes utilizam discos virtuais para armazenamento de dados após seu desligamento.

116 Uma das premissas do PaaS (*Plataform as a Service*) é a oferta das mesmas funcionalidades para todos os usuários, a fim de garantir a estabilidade dos sistemas.

117 No modelo SaaS (*Software as a Service*), as aplicações oferecem interfaces customizadas para cada cliente.

Com base nas normas NR10 e NR35, julgue os itens subsequentes.

118 A norma NR10 define uma programação mínima de cursos exigida para considerar um profissional como autorizado a trabalhar em instalações elétricas de alta tensão.

119 De acordo com a norma NR10, é responsabilidade do trabalhador zelar pela sua própria segurança e também pela segurança de outras pessoas afetadas pelas suas ações ou omissões.

120 De acordo com a norma NR35, os sistemas de proteção coletiva e individual contra quedas são complementares e devem ser utilizados simultaneamente.