-- CONHECIMENTOS ESPECÍFICOS --

Conforme os preceitos da NBR ISO/IEC 27002:2013 acerca da classificação e do controle de ativos de informação, julgue os itens a seguir.

51 Recomenda-se que o inventário de ativos contenha a indicação de um responsável para cada ativo identificado.

52 Convém que o armazenamento dos ativos de tecnologia da informação siga as especificações dos fabricantes.

53 Convém que o ativo seja protegido e classificado pelo proprietário.

54 O proprietário deve assegurar o tratamento adequado do ativo durante seu uso, mas não quando da sua exclusão ou destruição.

55 Para os ativos inventariados, deve haver regras de uso aceitável das informações, ao passo que, quanto aos ativos não inventariados, basta incluí-los na análise de riscos.

56 É responsabilidade do gestor de segurança da informação a classificação das informações dos ativos.

57 Os procedimentos desenvolvidos para o tratamento dos ativos incluem seu armazenamento e a manutenção de um registro formal dos destinatários, mas não abrangem restrições de acesso para cada nível de classificação da informação.

De acordo com as previsões da NBR ISO/IEC 27002:2013 a respeito da segurança de ambientes físicos, julgue os itens seguintes.

58 Recomenda-se a implantação de uma área de recepção ou outro meio para o controle de acesso físico a áreas onde se encontram informações críticas.

59 A utilização de sistemas de detecção de fumaça e alarme de incêndio é desnecessária se existirem portas corta-fogo no perímetro de segurança.

60 Recomenda-se que os sistemas de detecção de intrusos sejam testados regularmente.

61 Instalações de processamento de informação gerenciadas pela organização devem ser fisicamente integradas e conectadas àquelas gerenciadas por partes externas, que são registradas e auditadas a cada acesso.

62 Por ser elevado o nível de proteção do cabeamento de dados, são dispensáveis a instalação de conduítes blindados e a blindagem eletromagnética dos cabos.

63 Para a proteção de instalações onde existem informações confidenciais, é recomendável instalar controles contra visibilidade e audição das informações, como uma proteção eletromagnética.

À luz do que estabelece a NBR ISO/IEC 27002:2013 acerca da segurança de ambientes lógicos, julgue os itens subsequentes.

64 Quando as cópias de segurança contiverem informações que necessitem de elevado nível de confidencialidade, o acesso ao ambiente físico onde elas ficam deve ser controlado, sendo contraindicado o uso de encriptação.

65 No controle de *malwares*, *whitelisting* é uma lista de *softwares* de uso não autorizado.

66 O gerenciamento de vulnerabilidades técnicas e as análises críticas regulares dos *softwares* que suportam processos críticos de negócio são exemplos de controles contra *malware*.

67 O administrador de sistemas deve manter as mídias das cópias de segurança em local protegido contra interferências magnéticas, preferencialmente no mesmo local dos computadores, para que, em caso de desastres, o tempo de restauração das cópias seja o menor possível.

A respeito da gestão de riscos segundo a NBR ISO/IEC 27005, julgue os próximos itens.

68 A lista de componentes com responsáveis e localidades é obtida no processo de identificação dos riscos.

69 Experiências internas de incidentes e avaliações anteriores das ameaças não devem ser consideradas em avaliação de riscos após a ocorrência dos eventos relevantes.

70 Na avaliação da probabilidade dos incidentes, tem-se como entrada uma lista de cenários de incidentes identificados como relevantes.

71 Na etapa de identificação das consequências, tem-se como entrada uma lista de ameaças e vulnerabilidades relacionadas aos ativos.

Com base na NBR ISO/IEC 22313, julgue os itens subsequentes, acerca da continuidade de negócio.

72 Para o plano de continuidade do negócio, a organização deve providenciar os recursos necessários, prevendo treinamento, educação e conscientização a respeito desse plano, por exemplo.

73 No estabelecimento do plano de continuidade do negócio, deve ser incluído o compromisso com a melhoria contínua do sistema de gestão de continuidade de negócio.

Julgue os itens subsequentes, a respeito de ataques a redes de computadores.

74 Um ataque de *brute force* consiste em adivinhar, por tentativa e erro, um nome de usuário e sua senha, para obter acesso a determinado sistema.

75 Considere-se que um usuário tenha recebido uma mensagem de *email* em que os campos do cabeçalho tenham sido alterados de forma a aparentar que o *email* tivesse sido enviado por um remetente diferente do remetente real. Nesse caso, foi usada a técnica de falsificação denominada *spoofing*.

Considerando conceitos e aplicações da criptografia, julgue os itens a seguir.

76 Algoritmos de chaves assimétricas dispensam a necessidade de um canal seguro para o compartilhamento de chaves.

77 A cifra de César, que substitui uma letra do alfabeto por outra sem seguir um padrão regular, é um aprimoramento da cifra monoalfabética.

78 A cifra de bloco é uma das classes gerais de técnicas de criptografia simétrica utilizada em muitos protocolos seguros da Internet, como o PGP e o SSL.

79 DES (*data encryption standard*) e AES (*advanced encryption standard*) são exemplos de cifras de blocos em que as mensagens a serem criptografadas são processadas em blocos de *kilobits* (Kb).

A respeito de algoritmos de *hash*, julgue os itens que se seguem.

80 É possível utilizar uma função de resumo para verificar a integridade de um arquivo ou mesmo para gerar assinaturas digitais.

81 Os algoritmos de *hash* MD5 e SHA-1 apresentam, respectivamente, mensagem de resumo de 160 *bits* e de 128 *bits*.

82 *Hash* é o resultado único e de tamanho fixo de um método criptográfico aplicado sobre uma informação, conhecido como função de resumo.

83 A ferramenta mais utilizada para reduzir a probabilidade de acontecerem colisões em uma função de resumo (*hash*) é o ajuste de distribuição, de maneira que, quanto mais heterogênea e dispersa for a função resumo, menor será a sua probabilidade de colisão.

84 O uso de *hashes* na geração de assinaturas digitais garante a autenticidade, a confidencialidade e a integridade de uma informação.

Acerca da certificação digital e de suas aplicações, julgue os itens subsequentes.

85 Entre os componentes de uma PKI, como ICP-Brasil, a autoridade certificadora raiz (AC-raiz) é a responsável pela emissão da lista de certificados revogados (LCR).

86 O componente que faz a interface entre o titular do certificado digital e a autoridade certificadora é a autoridade de registro (AR).

87 O certificado digital valida uma assinatura digital por meio da vinculação de um arquivo eletrônico a essa assinatura, de modo que tanto a assinatura quanto esse arquivo são protegidos por criptografia pelo certificado digital.

88 Existem versões específicas de certificados digitais para determinados profissionais liberais, como advogados, contadores e médicos, o que lhes permite executar atividades afins às suas respectivas áreas de atuação.

No que se refere aos ataques cibernéticos, julgue os itens seguintes.

89 Um dos objetivos do ataque de DDoS (*distributed denial of service*) é deixar um sistema indisponível para que um ataque diferente seja lançado.

90 O *ransomware* é um tipo de *malware* que, em vez de bloquear o acesso aos dados da vítima, criptografa seus arquivos de forma a evitar o acesso a eles ou mesmo sua recuperação.

91 O *worm* se diferencia do vírus pelo fato de se propagar por meio da inclusão de cópias de si mesmo em outros programas ou arquivos, consumindo, assim, muitos recursos computacionais.

92 O ataque em que se explora a utilização do *buffer* de espaço durante a inicialização de uma sessão do protocolo de controle de transmissão é conhecido como TCP SYN *flood*.

Em relação à segurança cibernética, julgue os próximos itens.

93 A etapa de recuperação antecede a etapa de erradicação e se encarrega de restaurar os dados de negócio, executando, entre outras atividades, a de recriar ou alterar usuários e senhas de todos os colaboradores.

94 Definir políticas, regras e práticas para orientar os processos de segurança é uma das ações que devem ser executadas na etapa de preparação do processo de tratamento de incidentes, etapa essa que ocorre antes mesmo de o ataque acontecer.

95 Na etapa de contenção do processo de tratamento de incidentes, é feita a detecção do impacto do incidente.

96 As ações recomendadas para a resolução do problema durante a etapa de erradicação são a exclusão dos *softwares* maliciosos e *backdoors* descobertos, a alteração das credenciais de acesso aos sistemas e a aplicação de atualizações e correções nos sistemas afetados.

A respeito de meios de pagamento, julgue os itens a seguir.

97 O PIX, meio de pagamento instantâneo e digital criado pelo Banco Central do Brasil, oferece a tecnologia de QR *code* como opção para a realização de transferências de recursos entre contas bancárias.

98 A diferença básica entre DOC e TED é o fato de que, neste último, independentemente da hora em que a operação for realizada, o valor só será creditado na conta de destino no dia útil seguinte.

99 Uma das vantagens do uso das carteiras digitais é possibilitar que o consumidor faça compras pela Internet sem compartilhar diretamente os seus dados bancários no momento do pagamento.

100 Considerado uma versão mais sofisticada do RFID, o NFC utiliza tecnologia de radiofrequência, operando na frequência constante de 13,56 GHz.

Acerca da arquitetura de rede TCP/IP, julgue os itens subsequentes.

101 Pertencem à camada de aplicação os protocolos de mais alto nível, como o SSH e o DNS.

102 A camada de Internet, que é orientada à conexão, se comunica por meio de pacotes IP ou ARP com garantia de chegada ao destino.

103 O protocolo UDP, que é orientado à conexão e confiável, implementa *acknowledgements* e o controle *checksum* dentro do seu próprio *header*.

104 O comando *ping* utiliza-se do protocolo ICMP, responsável por garantir que roteadores e equipamentos interligados a roteadores sejam informados de que um destino não está mais disponível na rede.

105 Protocolos TCP, UDP e questões de QoS fazem parte da camada de transporte.

A respeito da arquitetura de rede TCP/IP e dos equipamentos de redes, julgue os itens a seguir.

106 O estabelecimento e encerramento de conexões, o sincronismo de quadro e o controle de erros são funções da camada de Internet.

107 Em uma rede Ethernet, o protocolo CSMA/CD é utilizado pela placa de rede, para detecção de colisões, e pela rede, para prevenção de colisões.

108 Com a utilização do protocolo STP em *switches* interligados em anel, evitam-se a geração de *loops* infinitos e a interrupção da comunicação entre os equipamentos.

109 Inundação dos quadros recebidos, colisões e operação em *half-duplex* são desvantagens dos s*witches* em relação aos *hubs*.

110 Em redes nas quais um grande número de computadores é interligado por roteador, recomenda-se usar, como *default gateway*, o endereço de *loopback*, para evitar conflito de IPs.

111 O roteador é o equipamento responsável por interligar LANs, atuando nas camadas 1, 2 e 3 do modelo de referência TCP/IP e decidindo o caminho do tráfego da informação.

Em relação aos equipamentos de redes, julgue os itens que se seguem.

112 Dentre os métodos de transmissão de quadros, que são operações realizadas pelo *switch*, destacam-se *store and forward*, *cut-through* e *bridging*.

113 O protocolo RIP disponível em roteadores gera pacotes que são transmitidos via protocolo UDP, carregados em pacotes IP.

114 O *firewall* cria um perímetro de segurança entre a rede interna e a ZDM, atuando com mecanismo para manter os bons *bits* e descartar os maus *bits*.

115 O *patch panel* é um equipamento que traz como benefício grande flexibilidade para a ativação de pontos de dados ou telefonia, além de possibilitar manobras do cabeamento.

No que se refere aos equipamentos de redes e a sistemas de segurança, julgue os próximos itens.

116 No IPsec, o modo de transporte acrescenta um cabeçalho IP extra, aumentando substancialmente o tamanho dos pacotes.

117 No *firewall*, o processamento que examina e distingue o tráfego usado para a navegação *web* do tráfego usado para compartilhamento de arquivos *peer-to-peer* é chamado de *gateways* em nível de aplicação.

118 Conceitualmente, as *bridges* visam unificar diferentes tipos de LANs, oferecendo desempenho superior ao dos *hubs*.

119 O IPsec, presente na camada IP para orientação da conexão, pode ser utilizado nos modos de operação túnel e transporte.

120 Uma VPN é utilizada em redes de pequeno porte, sendo configurada no *firewall*, e tem como desvantagem a falta de autenticação e criptografia.

Espaço livre