-- CONHECIMENTOS ESPECÍFICOS --

Julgue os itens que se seguem, relativos a endereçamento e protocolos da família TCP/IP, SNMP (Simple Network Management Protocol) e MIB (Management Information Base) e redes cabeadas.

51 Os cabos CAT 6 podem ser usados em substituição aos cabos CAT 5 e CAT 5e, suportando um tráfego de dados com velocidade de até 10 Gbps.

52 O MIB fornece uma maneira de definir objetos gerenciados e seus comportamentos, em que o OID define um único objeto a ser gerenciado.

53 Nos endereços IP (IPv4) pertencentes à classe A, o primeiro *byte* varia entre 1 e 127 e o primeiro *bit* desse *byte* é fixo e identifica a classe do endereço.

54 O endereço de *broadcast* é reservado como rota-padrão: quando um destino for requisitado, se o endereço não estiver presente na rede local, o protocolo procurará o endereço 255.255.255.255 e avaliará a rota configurada previamente.

55 O protocolo SNMP utiliza o protocolo UDP na camada de transporte e recebe as requisições nas portas 161 (agente) e 162 (*traps*).

Acerca de redes sem fio dos padrões 802.11, WEP, WPA e WPA2, conceitos relativos a *routing* e *switching* e IDS, julgue os itens subsequentes.

56 O IDS faz análise das atividades de uma rede, com o objetivo de descobrir atividades inapropriadas e alertar os administradores, tendo como vantagens o sistema *failover* e a filtragem de pacotes.

57 O padrão 802.11 possui o protocolo CSMA/CA, projetado para padronizar os equipamentos de rede sem fio produzidos por diferentes fabricantes, a fim de evitar incompatibilidades.

58 O roteador interliga redes LAN, atuando nas camadas 1, 2 e 3 do modelo de referência TCP/IP, interpretando o endereço IP contido no pacote de dados, consultando a sua tabela de roteamento e enviando esse pacote para a porta específica.

59 O padrão 802.11i utiliza WEP, que é uma técnica de criptografia simples que garante a privacidade na transmissão de dados pelo meio sem fio.

60 O WPA original utiliza algoritmo RC4, garantindo a segurança da conexão pela troca periódica da chave de encriptação, enquanto o WPA2 utiliza AES, que é um sistema de encriptação mais seguro que o RC4, com chaves de 128 *bits* a 256 *bits*.

Em relação a NAT e VPN, bem como a ataques dos tipos *flood* e *keylogger*, julgue os itens a seguir.

61 *Keylogger* é um programa capaz de capturar e armazenar o que é digitado no teclado pelo usuário, sendo sua ativação condicionada a uma ação prévia do usuário.

62 NAT é uma função desempenhada pelo *gateway* e tem o objetivo de fazer a tradução de endereços de uma rede interna para uma rede externa, usando um *bastion host* para a tradução dos pacotes IP entre as duas redes.

63 Em um ataque do tipo SYN *flood*, são enviados diversos pacotes ICMP (*ping*) e o computador da vítima é obrigado a responder aos pacotes com o ICMP *echo reply*, sobrecarregando a capacidade de processamento.

64 Quando implementada uma VPN usando-se o protocolo IPSEC, no modo tunelamento, a mensagem (*payload*) é criptografada, mantendo os cabeçalhos IP originais na abertura da conexão.

Acerca de criptografia simétrica e de certificados digitais, julgue os seguintes itens.

65 Algoritmos de *hash*, em conjunto com certificados digitais, são empregados em uma das etapas do processo de assinatura digital.

66 A chave utilizada em conjunto com um algoritmo criptográfico simétrico representa um segredo compartilhado entre duas ou mais partes.

67 Normalmente, a chave privada está incluída em um certificado digital, assim, o destinatário de uma mensagem assinada digitalmente é capaz de fazer a verificação de assinatura.

68 A criptografia simétrica pode usar cifras de fluxo ou cifras de bloco, dependendo da implementação do algoritmo e de suas características internas.

Em relação à gestão de processos e à administração de sistemas operacionais, julgue os itens que se seguem.

69 O Linux impede que dois usuários diferentes tenham o mesmo UID, com exceção do usuário *root*.

70 Qualquer novo usuário criado no Linux, por padrão, recebe um identificador de usuário (UID), que é utilizado quando um processo é criado pelo usuário em seu espaço de usuário (*user space*).

71 Como parte integral do funcionamento do sistema operacional, um processo pode ser criado e terminado, mas não pode ser agendado porque, em caso de agendamento, é necessário que a parte do usuário (*user space*) seja invocada.

72 Em relação aos estados de um processo em execução, o estado bloqueado ocorre quando o administrador do sistema operacional determina que o processo espere a conclusão de um processo prioritário.

Julgue os próximos itens, a respeito da administração de AD (Active Directory) usando linha de comando, considerando que `minhaprova.com.br` seja um domínio AD hipotético.

73 O comando `net view cpu1212 / minhaprova.com.br` mostra as informações do computador `cpu1212`, considerando que este computador exista no domínio em questão.

74 O comando `whoami /groups in minhaprova.com.br` permite listar os grupos do referido domínio.

Acerca de computação em nuvem, julgue os seguintes itens.

75 O modelo IaaS proíbe a virtualização da camada de armazenamento (*storage*).

76 Na infraestrutura como serviço (IaaS), a camada de virtualização é responsável por permitir o compartilhamento de determinados recursos de *hardware* entre várias máquinas virtuais diferentes.

Julgue os itens subsequentes, que se referem ao LDAP.

77 CN (*Common name*) é a maior unidade de toda uma árvore LDAP.

78 DC (*Domain componente*) refere-se ao domínio no qual o serviço de diretórios atua: `DC=minhaprova`, `DC=com`, `DC=br` corresponde ao DC para uma organização que possui o domínio `minhaprova.com.br`.

Acerca de servidores de aplicação, julgue os próximos itens.

79 Servidores de aplicação têm acesso limitado a sistemas de bancos de dados e, por isso, não são indicados para serviços corporativos.

80 Os servidores de aplicação são também conhecidos como *softwares* de *backend*, pois abstraem algumas complexidades do sistema operacional para o desenvolvedor.

81 Em serviços *web*, a solicitação do usuário é encaminhada primeiro por um servidor *web* para, depois, se necessário, ser encaminhada para um servidor de aplicação.

82 O balanceamento de carga dos servidores de aplicação distribui as chamadas de maneira que as diferentes máquinas do *cluster* funcionem como uma única.

83 Diferentemente dos servidores *web*, os servidores de aplicação fornecem conteúdo estático para atender ao usuário.

84 A utilização de servidores de aplicação é incompatível com os servidores *web*, pois se trata de tecnologias distintas.

85 Os servidores de aplicação utilizam *multithreading* de forma nativa, para garantir alta escalabilidade e eficiência para seus processos.

A respeito de *data centers*, julgue os itens que se seguem.

86 Em um *data center*, os servidores NAS trabalham exclusivamente com armazenamento de dados e solicitações de compartilhamento de arquivo.

87 *Data centers* classificados como *tier* III operam no formato 24×7, em que podem ocorrer manutenções preventivas sem suspensão de suas operações.

88 Uma das medidas para dimensionar o tamanho de um *data center* é a quantidade de clientes remotos que acessam simultaneamente os seus servidores.

89 No *backup*, os dados armazenados em um *data center* são copiados para outro *data center*, evitando-se a cópia em nuvem, para que não ocorra a exposição dos próprios dados.

90 Na configuração RAID 1, são necessárias, pelos menos, duas unidades de armazenamento para fornecer redundância a falhas.

91 A redundância em *data centers* diz respeito à multiplicidade de equipamentos e serviços que cumprem o mesmo objetivo: evitar paradas por falha e para manutenção.

92 Negócios que exigem 100% de disponibilidade devem utilizar *data centers* dos tipos *tier* II, III e IV, pois estes possuem redundância nos circuitos elétricos, arrefecimento e rede.

Em relação à gestão de segurança da informação, julgue os itens subsequentes.

93 Segundo a NBR ISO/IEC 27001, um processo de avaliação de riscos de segurança da informação deve estabelecer e manter critérios de risco que incluam a eliminação e a avaliação dos riscos.

94 De acordo com a NBR ISO/IEC 27001, quando uma não conformidade acontece, a organização deve, entre outras providências, avaliar a necessidade de realizar ações para a eliminação de sua causa, a fim de evitar que tal evento volte a acontecer.

95 Conforme a NBR ISO/IEC 27002, os requisitos legais, estatuários, regulamentares e contratuais constituem uma das principais fontes de requisitos de segurança da informação.

96 Nos controles organizacionais previstos na NBR ISO/IEC 27002, o inventário de informações e outros ativos associados abrangem as seguintes propriedades de segurança da informação: confidencialidade, integridade e disponibilidade.

A respeito da autenticação e proteção de sistemas, julgue os itens que se seguem.

97 O JSON Web Token consiste em três partes separadas por pontos: o cabeçalho, que contém informações sobre o tipo de *token* e o algoritmo de criptografia usado para assinar o *token*; o *payload*, que contém as informações do usuário; e a assinatura, usada para garantir que o *token* não tenha sido alterado.

98 O OpenID Connect é um protocolo de identidade simples, construído no protocolo do JSON Web Token, e permite que os aplicativos clientes confiem na autenticação executada por um provedor OpenID Connect para verificar a identidade de um usuário.

99 Na notificação por *push*, os métodos de autenticação de dois fatores (2FA) exigem uma senha para aprovar o acesso a um sítio ou aplicativo.

100 A biometria pode ser usada em conjunto com outros métodos de autenticação — principalmente senhas e PIN — como parte de uma configuração 2FA.

Em relação a ameaças e vulnerabilidades em aplicações, julgue os próximos itens.

101 XSS (*cross-site scripting*) é um método pelo qual um invasor explora vulnerabilidades na maneira como um banco de dados executa consultas de pesquisa.

102 O objetivo do ataque de LDAP *injection* é manipular as consultas LDAP, por meio da inserção de um código malicioso na consulta, que passa a ser interpretada de forma diferente do esperado.

103 Um ataque de *cross-site request forgery* é aquele que induz um usuário a usar acidentalmente suas credenciais para invocar uma ação indesejada.

Acerca da segurança de aplicativos *web*, julgue os itens que se seguem.

104 O uso de componentes com vulnerabilidades conhecidas é uma das categorias de riscos de segurança do OWASP Top 10 que resulta da desserialização de dados de fontes não confiáveis.

105 Entre os riscos de segurança incluídos no relatório OWASP Top 10, a quebra de controle de acesso é um ataque contra um aplicativo *web* que analisa a entrada XML.

106 Quando um invasor encontra falhas em um mecanismo de autenticação, ele pode obter acesso às contas de outros usuários.

A respeito das características de um ataque de negação de serviço distribuído, julgue os próximos itens.

107 Um *firewall* de borda é considerado como o elemento capaz de fazer a mitigação de ataques DDoS de maneira eficiente, já que o tráfego da camada de aplicação tem que ser bloqueado na entrada da rede.

108 Em um ataque que envolve a amplificação de dados, o atacante gera uma mensagem para um elemento falho na rede e este, por sua vez, gera uma resposta que aumenta o volume de dados direcionados à vítima.

Julgue os itens a seguir, a respeito de estratégia de criptografia para dados em trânsito em uma rede de computadores.

109 O uso da última versão do TLS é recomendado para a criação de túneis de comunicação criptografados, considerando as versões de algoritmos simétricos e assimétricos seguros.

110 Como solução de verificação de integridade, o algoritmo MD5 seria uma boa escolha, já que ele é resistente a colisões e garante confidencialidade.

Acerca de assinatura e certificação digital, julgue os itens que se seguem.

111 No caso de um certificado digital com o algoritmo RSA, o tamanho adequado e seguro da chave é de 512 *bits*.

112 O algoritmo SHA512 é inseguro porque o ataque de repetição (*replay attack*) permite a colisão dos primeiros 64 *bits* de saída.

Com base na NBR ISO/IEC 27005, julgue os itens seguintes.

113 Na organização deve existir treinamento de gestores e de pessoal sobre riscos e ações de mitigação.

114 O processo de gestão de riscos deve contribuir para a identificação dos riscos de segurança da informação.

Conforme o que preconiza a LPGD para o encarregado de dados, julgue os itens subsequentes.

115 Cabe ao encarregado aceitar reclamações e comunicações dos titulares de dados.

116 A identidade e as informações de contato do encarregado de dados devem ser mantidas em sigilo, podendo ser publicadas mediante solicitação do interessado.

Julgue os itens a seguir, em relação ao processo de negociação de parâmetros criptográficos e múltiplas conexões conforme o protocolo TLS 1.3.

117 O TLS impede a abertura de múltiplas conexões HTTP paralelas.

118 O servidor processa a mensagem `ClientHello` enviada pelo cliente, entretanto, quem determina os parâmetros apropriados criptográficos para a conexão é o cliente.

A respeito do processo de gestão de riscos estabelecido pela NBR ISO/IEC 27005, julgue os seguintes itens.

119 O encerramento do processo de gestão de risco inclui decisões sobre a aceitação do risco e consequente comunicação às partes envolvidas.

120 Uma das etapas do processo de gestão de risco consiste em definir o contexto.

Espaço livre