

-- CONHECIMENTOS ESPECÍFICOS --

Acerca de aspectos relativos a redes de computadores, julgue os itens a seguir.

- 51 Como possui alta taxa de velocidade, o cabo metálico é o meio de comunicação mais usado para o estabelecimento de conexão em redes de longa distância, entretanto ele apresenta algumas desvantagens em relação à fibra óptica, como o fato de ele ser de difícil manuseio e ter custo elevado.
- 52 A função do *switch*, em uma rede de comutação de circuitos, é ativar ou desativar a conexão, chamada de circuito, uma vez que ela está sempre disponível entre os dois sistemas finais.
- 53 Pontos de troca de tráfego são sistemas complexos de comutação que permitem a conexão das redes de *backbone*.
- 54 Na topologia em barramento, a rede não pode ser expandida, porque todos os computadores estão conectados a um único cabo.
- 55 As características físicas e de enlace das conexões de uma rede, como, por exemplo, sinais elétricos, protocolos de acesso ao meio e velocidade, influenciam na definição dos dispositivos físicos e do cabeamento.

Com relação aos protocolos da família TCP/IP, julgue os itens que se seguem.

- 56 Dada sua simplicidade, o protocolo UDP torna-se útil para um aplicativo que tem de enviar mensagens curtas e não consegue realizar a retransmissão de pacotes envolvida no TCP quando um pacote é corrompido ou perdido.
- 57 O IP (Internet Protocol), principal protocolo da família TCP/IP, é um protocolo orientado à conexão e realiza controle de congestionamento.
- 58 O SCTP é um protocolo confiável e orientado à conexão, a fluxos de *bytes* e a mensagens, tal qual o protocolo UDP.
- 59 O ARP (Address Resolution Protocol) é um protocolo que atua junto ao protocolo IP, com a finalidade de auxiliá-lo a localizar o endereço da camada de enlace do *host* ou do roteador, quando o endereço da camada de rede deste é fornecido.
- 60 A principal função do protocolo ICMP (Internet Control Message Protocol) é ajudar o protocolo IP em tarefas de *multicast*.

Em relação à arquitetura do gerenciamento de redes de Internet SNMP, à MIB (Management Information Base) e ao SMI (Structure of Management Information), julgue os próximos itens.

- 61 Uma rede gerenciada segundo o modelo de gerenciamento SNMP compõe-se, entre outros elementos, de um ou mais nós gerenciados, cada qual contendo uma entidade de processamento chamada de agente.
- 62 Em relação às operações no protocolo SNMP, cada classe de informação de gerenciamento recebe uma identificação única.
- 63 MIB pode ser definida como um conjunto de todos os objetos de um recurso gerenciado e tem como um de seus princípios fundamentais o fato de que os recursos gerenciados semelhantes possuem um conjunto básico de variáveis distintas.
- 64 Em relação à árvore de registro de objetos Internet da MIB-II, a sub-árvore *private*, reservada para identificar objetos utilizados em experimentos Internet, representa um dos nós dentro do ramo internet definidos pela SMI.
- 65 O RMON MIB (Remote Monitoring MIB) foi projetado com o objetivo de realizar monitoramento preemptivo, ou seja, o monitor fica sempre ativo, continuamente rodando diagnósticos e armazenando dados.

Julgue os itens subsequentes, relativos à arquitetura MPLS e aos protocolos usados em redes sem fio.

- 66 Apesar de o protocolo WPA2 possuir um bom mecanismo de segurança, ele também tem vulnerabilidades.
- 67 O elemento de entrada da rede responsável pelo recebimento de datagramas, no modelo de rede MPLS, é denominado de LSP definido.
- 68 Com relação ao formato do datagrama, o MPLS define a *shim header*, que é uma rotulação denominada encapsulamento genérico para tecnologias de enlace que empregam identificadores de conexão.
- 69 O padrão de encriptação WEP possui muitas vulnerabilidades e falhas, o que facilita ataques à rede, como a captura de mensagens e a autenticação indesejada na rede.
- 70 Em regra, o protocolo WPA (Wi-Fi Protected Access) usa o método de criptografia TKIP, o qual permite implementar criptografia nas mensagens sem uso de assinatura.

Acerca de *routing* e *switching*, julgue os itens seguintes.

- 71 Por meio da técnica de *switching*, que permite a comunicação de sistemas em redes heterogêneas, sistemas em redes X.25 podem se comunicar com sistemas em redes locais.
- 72 A estratégia *switching* pode ser aplicada para melhorar o desempenho de uma rede.
- 73 Os roteadores são equipamentos capazes de descobrir o melhor caminho para um *host* de destino e de prover mecanismos para controle de fluxo.
- 74 Roteadores não são capazes de filtrar mensagens *broadcast*, o que representa a principal desvantagem deles em relação aos *switches*.
- 75 Os roteadores, por meio das redes lógicas e dos grupos de trabalho, permitem direcionar mensagens para apenas um grupo determinado.

Com relação à segurança em redes de computadores, julgue os itens subsequentes.

- 76 O IDS (Intrusion Detection System) é um dispositivo físico que, instalado antes do servidor, restringe o acesso entre as redes para prevenir uma invasão.
- 77 O *firewall* é um equipamento de *hardware* ou *software* que identifica anomalias no tráfego e aciona o IDS (Intrusion Detection System) para bloquear o tráfego na rede.
- 78 VPN (Virtual Private Network) é uma rede privada virtual restrita que usa a Internet como infraestrutura para estabelecer tráfego seguro sobre uma rede pública.
- 79 Entre as finalidades do IPS (Intrusion Prevention System) inclui-se a proteção do protocolo de redes a partir da identificação de anomalias.
- 80 Em segurança da informação, o conceito de disponibilidade refere-se à preservação da integridade dos dados disponibilizados aos usuários, a fim de evitar alterações indevidas.

Acerca dos tipos de ataques a redes de computadores, julgue os itens subsecutivos.

- 81 É maliciosa a varredura de rede (*scan*) realizada com o objetivo de fazer uma análise de riscos preventiva ou corretiva.
- 82 O ataque de negação de serviço DOS (*denial of service*) afeta a integridade dos dados, tornando-os indisponíveis aos usuários.
- 83 No ataque de *spoofing*, é feita uma verificação do fluxo da rede por meio da análise do envio e recebimento de pacotes de dados, de forma que se obtém um mapa dos dispositivos existentes na rede.
- 84 Chama-se *spoofing* o tipo de ataque em que se tenta autenticar uma máquina externa desconhecida como sendo uma máquina da rede interna.
- 85 Os ataques de *flood* podem afetar a disponibilidade da rede por meio de requisições simultâneas de grandes grupos de pacotes para diversas portas aleatórias de um servidor.
- 86 O uso de *firewall UTM (unified threat management)* é uma das principais soluções para evitar ataques de *flood* e de vírus.
- 87 Habilitar filtro *antispoofing* e desabilitar serviços desnecessários são técnicas de prevenção contra ataques de DDoS.

Com relação aos tipos de *malwares*, julgue os itens que se seguem.

- 88 O *phishing* é uma técnica explorada por um invasor que tenta obter o endereço IP do usuário para enviar uma quantidade volumosa de requisições e aumentar o consumo da banda.
- 89 *Keylogger* é um tipo de *spyware* que copia o que está sendo digitado na tela do usuário, como *logins* e senhas inseridas mediante teclados virtuais de aplicações de *internet banking*.
- 90 *Ransomware* é uma técnica utilizada para coletar dados de usuários por meio de mensagens de *email*, geralmente na forma de *spam*.
- 91 Os vírus possuem a capacidade de se duplicarem, enquanto os *worms* exploram vulnerabilidades em programas, mas não se propagam automaticamente.
- 92 Cavalo de Troia é um tipo de vírus que infecta computadores a partir de programas aparentemente úteis ou por meio de um *link* de uma página na Web.

Acerca de criptografia, julgue os itens que se seguem.

- 93 O RSA é um algoritmo de criptografia assimétrica que utiliza chaves com 1.024 bits.
- 94 No método de criptografia simétrica, utiliza-se uma mesma chave tanto para criptografar quanto para descriptografar uma mensagem.
- 95 O DES é um algoritmo de chave pública.
- 96 A criptografia de chave pública envolve uma chave pública, criada para gerar a mensagem, e uma chave privada, usada pelo destinatário para abrir a mensagem.

A respeito de sistemas operacionais e de serviços de diretórios, julgue os itens a seguir.

- 97 No Windows Server, a tecnologia de virtualização que permite criar e executar uma máquina virtual é o Hyper-V.
- 98 DN (*distinguished name*), CN (*common name*) e OU (*organizational unit*) são atributos dos objetos do LDAP.
- 99 No Active Directory, uma árvore é um agrupamento lógico de objetos, enquanto um domínio é um agrupamento lógico de árvores.
- 100 A arquitetura lógica do Active Directory é composta por objetos, domínios, relações de confiança, *namespaces* e distribuição de dados.

Julgue os itens seguintes, relativos a *cloud computing*.

- 101 Computação elástica diz respeito à capacidade de alocar dinamicamente recursos de computação e suportar cargas de trabalho variáveis.
- 102 Nuvem pública é aquela operada por um ente público, federal, estadual ou municipal, para atender às instituições de governo.
- 103 A infraestrutura de nuvem SaaS (Software as a Service) executa apenas aplicativos disponibilizados pelo provedor de serviços.
- 104 Um dos riscos da computação em nuvem é o processo de desperimetriação, no qual os sistemas hospedados na nuvem podem ultrapassar os limites de várias organizações e cruzar as fronteiras de segurança.
- 105 O *hypervisor*, também chamado de supervisor de máquina virtual, controla o disco rígido para que seja possível acessá-lo exclusivamente pela máquina virtual.

Em relação a contêineres em aplicações, julgue os itens a seguir.

- 106 Um contêiner deve fornecer um ambiente de hospedagem do lado do servidor gerenciado e um *middleware* que intercepte as chamadas recebidas e, em seguida, execute as ações apropriadas para garantir que as propriedades desejadas do aplicativo distribuído sejam mantidas.
- 107 O Kubernetes faz o escalonamento e a recuperação no caso de falha de uma aplicação.
- 108 *Deployment descriptors* (em português, descritores de implantação) são escritos em JSON e fornecem informações sobre API e *drives* necessários para o funcionamento do serviço de Internet.

Julgue os itens que se seguem, acerca de DevOps.

- 109 Cada vez que uma alteração na base de código é detectada, é iniciada uma compilação que testa a qualidade do código recém-enviado, alcançando-se, assim, a integração contínua.
- 110 O repositório de artefatos armazena artefatos de construção produzidos por integração contínua e os disponibiliza para implantação automatizada em ambientes de teste, preparação e produção.
- 111 Os processos envolvidos no DevOps são denominados, respectivamente, de planejar, construir, testar, codificar, operar, avaliar e relatar.

A respeito de tecnologias, arquitetura e gestão de *data center* e de ambientes de missão crítica, julgue os itens subsequentes.

- 112 O NAS (Network Attached Storage) fornece uma interface de sistema de arquivos a partir de protocolos de sistema de arquivos em rede, como NFS ou CIFS.
- 113 Na arquitetura de SAN (Storage Area Network), um grande número de discos é conectado, por uma rede de alta velocidade, a vários computadores servidores.
- 114 RAID nível 1 refere-se à paridade distribuída intercalada por blocos, em que os dados e a paridade são particionados entre todos os N + 1 discos.
- 115 O processo de deduplicação é capaz de acelerar bastante as operações de leitura de dados, pois sua velocidade de leitura é muito maior que a de acesso nativo ao disco rígido.
- 116 A redundância dos dados exige que os dados sejam precisos, o que significa que a entrada de dados deve estar correta, as alterações nos dados devem ser registradas e os dados devem ser armazenados de forma segura e confiável para que não possam ser alterados sem autorização.
- 117 Os discos do tipo ATA necessitam de um sistema de terminação, que normalmente é ativado no último dispositivo conectado ao cabo.

Julgue os itens a seguir, a respeito de otimização de desempenho em servidores e de política de *backup*.

- 118 O *backup* incremental é a cópia de todo o conteúdo do espaço de armazenamento e das alterações realizadas nos processos de atualização.
- 119 Um servidor *proxy* armazena conteúdo da Web recuperado ou acessado recentemente e, dentro de uma organização, pode ser usado para o compartilhamento desse conteúdo entre todos os clientes na rede.
- 120 Um componente é redundante quando fornece criptografia e segurança adequadas ao banco de dados de *back-end* ou quando armazena o sistema operacional por meio do armazenamento dos dados.
-

Espaço livre