

De acordo com o comando a que cada um dos itens de 1 a 120 se refira, marque, na **folha de respostas**, para cada item: o campo designado com o código **C**, caso julgue o item **CERTO**; ou o campo designado com o código **E**, caso julgue o item **ERRADO**. A ausência de marcação ou a marcação de ambos os campos não serão apenadas, ou seja, não receberão pontuação negativa. Para as devidas marcações, use a **folha de respostas**, único documento válido para a correção das suas provas.

CONHECIMENTOS BÁSICOS

Entendendo a Internet

1 Imagine um número enorme de computadores interligados, recebendo e enviando informações entre si constantemente... Assim é a Internet.

4 Tecnicamente falando, Internet é o nome dado à organização que se faz em uma rede de computadores. Ela não serve somente como fonte de informações onde o usuário (chamado de internauta) se conecta a fim de obter dados para seu trabalho ou suas pesquisas; ela é útil também por permitir que os internautas se comuniquem uns com os outros, por meio de correio eletrônico ou bate-papo em tempo real (*chat*).

13 Entender a Internet como um todo não é difícil. Ao contrário do que muitos imaginam, a Internet não tem uma sede instalada em algum lugar do mundo com filiais em seus principais países. Envolvida por diversos termos, às vezes complicados, como *http*, *URL*, *sítio*, *canal*, *home-page*, *modem*, *e-mail*, entre outros, a Internet forma-se a partir da possibilidade de conexão de vários computadores ao mesmo tempo. Esses computadores podem ser individuais, como um computador doméstico, ou podem estar organizados em grupos, lembrando uma rede ou uma teia de aranha.

22 Hoje é possível encontrar (quase) tudo na grande rede. Ao conectar-se, o internauta passa a ter acesso a informações diversas, relacionadas a cultura, turismo, educação, lazer, viagem, televisão, cinema, arte, informática, política, religião, enfim, um mundo paralelo ao nosso, onde a informação é compartilhada de diferentes maneiras.

Mozart Fialho Jr. *Novo dicionário de informática*. 2.ª ed., Goiânia: Gráfica Terra, 2002, p. 28-30 (com adaptações).

Com relação às idéias e às estruturas do texto acima, julgue os itens de 1 a 10.

- 1 O verbo empregado no título do texto está no gerúndio. Existem certas formas de emprego do gerúndio, como em **eu vou estar registrando o seu pedido**, que são condenadas pela tradição gramatical.
- 2 O vocábulo “si” (l.2) tem valor reflexivo e o seu emprego, no texto, contribui para o entendimento de que uns computadores recebem e enviam informações para outros, que fazem o mesmo em relação aos primeiros.
- 3 No texto, as palavras “interligados” (l.2), “rede” (l.5) e “conexão” (l.18) possuem estreita relação de sentido.
- 4 A expressão “não serve somente” (l.6) dispensa a informação dada pela oração “ela é útil também por permitir que os internautas se comuniquem uns com os outros” (l.8-10).
- 5 O nome “internauta” é dado às ferramentas de comunicação na Internet, tais como o correio eletrônico e o bate-papo em tempo real (*chat*).
- 6 O itálico foi empregado nas palavras “*chat*”, “*home-page*”, “*modem*” e “*e-mail*” para indicar que se trata de termos de origem estrangeira.
- 7 O emprego dos parênteses no último parágrafo do texto representa uma ressalva à afirmação de que tudo pode ser encontrado na rede.
- 8 As palavras “número” e “doméstico” são acentuadas graficamente porque, nelas, a sílaba tônica recai sobre a antepenúltima sílaba.

- 9 Não foi empregado o acento grave em “relacionadas a cultura” (l.24) porque o termo “cultura” está empregado em sentido geral, sem anteposição de artigo definido, tal como as demais palavras da enumeração — “turismo, educação, lazer, viagem, televisão, cinema, arte, informática, política, religião” (l.24-26).
- 10 O vocábulo “enfim” (l.26) introduz uma informação que pode ser interpretada como uma conseqüência do que se diz na oração anterior.

O Plano Estratégico de Reestruturação do Exército prevê a instalação de sete novas importantes unidades militares na região Norte, com prioridade para a zona de fronteira. Duas delas já estão em construção: São Gabriel da Cachoeira e Barcelos, no Amazonas. O reforço da tropa nessa região faz parte da estratégia dos militares de transferir para a Amazônia unidades hoje localizadas no Rio Grande do Sul, em São Paulo, no Rio de Janeiro e no Nordeste. Os comandantes também estão preocupados com o vazio demográfico nas regiões mais remotas da Amazônia, o que facilita a atuação de traficantes internacionais de cocaína que utilizam os rios e a floresta para transporte e depósito da droga.

Correio Braziliense, 3/12/2007, p. 7 (com adaptações).

Tendo o texto acima como referência inicial e considerando o atual cenário da região, do Brasil e da América do Sul, julgue os itens de 11 a 20.

- 11 O tráfico internacional de drogas ilícitas constitui, na atualidade, uma das mais poderosas e lucrativas atividades que envolvem o chamado crime organizado, cuja atuação também se tornou globalizada.
- 12 Quando se fala em uso de rios e da floresta para o transporte e depósito de drogas, as fronteiras com a Bolívia e a Colômbia aparecem como áreas merecedoras de especial atenção por parte das autoridades brasileiras.
- 13 O vazio demográfico a que o texto se reporta é fato relativamente recente, pois, como se sabe, a Amazônia foi historicamente caracterizada pela alta densidade populacional desde o início da colonização do Brasil.
- 14 Seguindo uma tendência iniciada em princípios do século XIX, a região platina continua sendo a área de fronteira mais estratégica para o Brasil, o que explica o reforço da presença militar brasileira na região.
- 15 Apesar da retórica considerada agressiva, Hugo Chávez não demonstra interesse em fortalecer militarmente a Venezuela, o que tem contribuído para a redução das tensões na América do Sul.
- 16 Na Bolívia, o nacionalismo defendido por Evo Morales, justamente por relevar a crucial questão energética, não chegou a criar atrito ou alguma forma de constrangimento no relacionamento com o Brasil.
- 17 A persistente atuação da guerrilha das Forças Armadas Revolucionárias da Colômbia (FARC), de forças paramilitares e do narcotráfico responde pela existência de uma espécie de guerra civil que, há décadas, cria turbulências na Colômbia.
- 18 Por falta de recursos financeiros, como reiteradamente afirma o governo federal, a Amazônia ainda não dispõe de um sistema de vigilância aérea, o que facilita a ação de criminosos internacionais na região.

- 19 A Amazônia tem se transformado em alvo das atenções mundiais, como se observa no caso de instituições científicas que buscam estudar sua extremamente rica biodiversidade.
- 20 O atual projeto de construção de hidrelétricas no rio Madeira atesta a importância do potencial hidráulico da Amazônia para a geração de energia.

Texto I – para os itens de 21 a 26

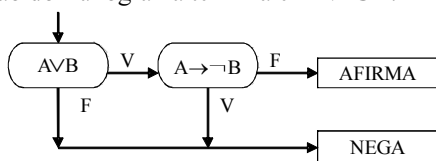
Uma proposição é uma afirmativa que pode ser julgada como verdadeira — V —, ou falsa — F —, mas não como ambas. Considere que A e B representam proposições, e que, a partir delas, proposições compostas são construídas. Expressões da forma $A \vee B$, $\neg A$ e $A \rightarrow B$ são proposições compostas.

Uma proposição da forma $A \vee B$, lida como “A ou B”, é F quando A e B forem F e é V nos demais casos; $\neg A$, lida como “não A”, é V quando A for F e é F quando A for V; $A \rightarrow B$, lida como “se A então B”, é F quando A for V e B for F, e é V nos demais casos.

Considere a forma de raciocínio constituída por uma seqüência de três proposições, em que as duas primeiras são denominadas premissas e a terceira, conclusão. Um raciocínio que tem essa forma é denominado válido quando se consideram as premissas verdadeiras e, com isso, pode-se garantir que a conclusão seja também verdadeira.

Com referência ao texto I, julgue os itens a seguir.

- 21 Considerando-se como premissas as proposições “Nenhum pirata é bondoso” e “Existem piratas que são velhos”, se a conclusão for “Existem velhos que não são bondosos”, então essas três proposições constituem um raciocínio válido.
- 22 Considere como premissas as proposições “Todos os *hobits* são baixinhos” e “Todos os habitantes da Colina são *hobits*”, e, como conclusão, a proposição “Todos os baixinhos são habitantes da Colina”. Nesse caso, essas três proposições constituem um raciocínio válido.
- 23 As proposições $(\neg A) \vee (\neg B)$ e $\neg A \rightarrow \neg B$ têm exatamente as mesmas valorações V ou F, independentemente das valorações V ou F atribuídas às proposições básicas A e B.
- 24 No fluxograma ilustrado abaixo, as instruções devem ser executadas seguindo-se o fluxo das setas de acordo com a avaliação da proposição que ocorre em cada caixa oval. Nesse caso, quando A e B têm valorações contrárias, a execução do fluxograma termina em NEGA.



Texto II – para os itens 25 e 26

Dois proposições são denominadas equivalentes quando têm exatamente as mesmas valorações V e F. Por exemplo, são equivalentes as proposições $(\neg A) \vee B$ e $A \rightarrow B$.

A partir das informações dos textos I e II acima, e supondo que A simboliza a proposição “Alice perseguiu o Coelho Branco” e B simboliza a proposição “O Coelho Branco olhou o relógio”, julgue os itens a seguir.

- 25 A proposição “Se o Coelho Branco não olhou o relógio, então Alice não perseguiu o Coelho Branco” pode ser simbolizada por $(\neg B) \rightarrow (\neg A)$.
- 26 A proposição “Se o Coelho Branco olhou o relógio, então Alice não perseguiu o Coelho Branco” é equivalente à proposição “O Coelho Branco não olhou o relógio ou Alice não perseguiu o Coelho Branco”.

Problemas de contagem surgem naturalmente quando se deseja determinar o número de elementos de um conjunto finito, e os de probabilidades são freqüentemente associados à avaliação da chance em jogos e à freqüência da ocorrência de um evento. Com relação a esses assuntos, julgue os itens a seguir.

- 27 Considere que um painel deva ser montado utilizando-se 4 peças em forma de losangos, 6 em forma de círculos e 2 em forma de triângulos. A quantidade de maneiras que se pode construir esse painel, colocando-se uma peça ao lado da outra, é inferior a 14.000.
- 28 Ao iniciar um *videogame*, o jogador dispõe de uma tela onde pode selecionar de 1 a 4 jogadores, outra tela onde pode selecionar de 1 a 3 níveis de dificuldade e, por último, uma tela onde pode selecionar de 1 a 3 velocidades para o jogo. Nesse caso, a quantidade de formas distintas de se jogar esse *videogame* é superior a 25.
- 29 Considere que, para criar códigos a partir das 5 vogais, sejam usadas seqüências binárias de 4 dígitos. Nesse caso, a quantidade de códigos distintos que podem ser formados é igual a $\frac{16!}{11! \times 5!}$.
- 30 Considere que a prova objetiva de um concurso tenha 5 questões de múltipla escolha, com 4 opções cada uma. Considere também que as questões sejam independentes e que um candidato responda a todas elas aleatoriamente. Nessa situação, a probabilidade de ele acertar todas as questões é inferior a 0,05%.

RASCUNHO

A respeito das funções essenciais à justiça, julgue os itens a seguir.

- 31** As funções essenciais à justiça incluem o Ministério Público, a Advocacia, a Advocacia Pública e a Defensoria Pública.
- 32** A defesa judicial dos direitos e interesses das populações indígenas é função institucional do Ministério Público.
- 33** Considere que um promotor de justiça do estado do Amazonas tenha se aposentado em 1.º de janeiro de 2007 e que, no dia 2 de fevereiro de 2007, tenha começado a atuar como advogado perante o Tribunal de Justiça do estado do Amazonas. Nessa situação, a conduta do promotor é uma conduta possível, pois ele já estava aposentado quando iniciou suas atividades como advogado perante o referido tribunal.

Acerca dos direitos e das garantias fundamentais, julgue os itens que se seguem.

- 34** A Constituição Federal de 1988 proíbe a pena de morte em qualquer caso.
- 35** Considere que, em determinada cooperativa, um cooperado tenha praticado conduta contrária ao estatuto social, e que, por isso, a diretoria da cooperativa tenha decidido excluí-lo sumariamente, fundamentando essa decisão no caráter punitivo e na conduta contrária ao estatuto. Nessa situação, a diretoria agiu corretamente, pois a decisão foi fundamentada em dispositivo do estatuto.
- 36** São inconstitucionais, por ferirem o princípio da igualdade, cláusulas do estatuto de uma empresa de porte internacional que atribuam a profissionais estrangeiros vantagens que não alcancem profissionais brasileiros.
- 37** Se um governador de estado editasse decreto proibindo todo e qualquer ato de manifestação na via pública que dá acesso à sede do governo, agiria de acordo com os princípios constitucionais, já que estaria visando à proteção tanto do prédio sede do governo quanto das autoridades que nele despacham.
- 38** O uso de algemas em um cidadão pacato, de bons antecedentes, que não oferece nenhum risco para a sociedade, preso em razão de atraso de prestação alimentícia, fere o princípio da proporcionalidade e da razoabilidade.
- 39** A memória contida em um computador está protegida pela garantia da inviolabilidade da intimidade das pessoas.

Em cada um dos itens **40** e **41** a seguir, é apresentada uma situação hipotética, seguida de uma assertiva a ser julgada, a respeito dos servidores públicos.

- 40** Um servidor público do estado do Amazonas que cumpre seu horário normal de trabalho das 8 às 18 horas foi eleito vereador em Manaus. Nesse município, as reuniões da câmara de vereadores ocorrem sempre às quartas-feiras, no horário de 19 a 22 h 30 min. Nessa situação, é possível a cumulação da vereança com as funções normais de servidor público.

- 41** Em determinado município, foram realizadas contratações diretas de médicos, sob a alegação de necessidade do serviço. Decorrido um ano dessas contratações, o prefeito do referido município editou decreto que efetivou os médicos como servidores do município. Nessa situação, o prefeito agiu correta e legalmente, já que existia a necessidade do serviço.

Julgue os itens seguintes, relativos aos princípios básicos da administração pública.

- 42** O princípio da eficiência foi acrescentado à Constituição Federal de 1988 pela Emenda Constitucional n.º 19/1998, chamada de reforma administrativa.
- 43** A administração pode anular seus próprios atos se estes estiverem eivados de vícios que os tornem ilegais.
- 44** Considere que uma empresa privada que presta serviços públicos a um município por delegação tenha suspenso a prestação desse serviço em virtude da interrupção, sem justificativa prévia, dos pagamentos mensais feitos pelo referido município. Nessa situação, a empresa agiu corretamente, pois o município descumpriu o contrato ao não efetuar os pagamentos devidos.
- 45** Em um município que não disponha de imprensa oficial, a fixação de um ato administrativo na sede da prefeitura atende ao princípio da publicidade.
- 46** Uma câmara de vereadores de determinado município pode dispor de 3.000 cargos em comissão e de 300 cargos efetivos, pois cabe ao Poder Legislativo municipal dispor sobre sua estrutura; além disso, esse fato não fere nenhum princípio da administração pública.
- 47** A existência das chamadas cláusulas exorbitantes nos contratos administrativos visa atender ao princípio da supremacia do interesse público.
- 48** Um bem público afetado a uma destinação específica pode ser alienado pela administração pública, já que não existe norma ou princípio que impeça tal ato.
- 49** O princípio da legalidade determina que a administração, além de não poder atuar contra a lei ou além da lei, somente pode agir segundo a lei.
- 50** Fere o princípio da eficiência a atitude praticada pelo prefeito de uma cidade do interior que, com o objetivo de valorizar sua propriedade, abre processo de licitação para asfaltar a estrada que liga a cidade à sua fazenda.

CONHECIMENTOS ESPECÍFICOS

Com relação às redes de computadores, julgue os seguintes itens.

- 51** Uma rede de computadores é uma coleção de computadores e outros dispositivos que usam um protocolo de rede comum para compartilhar recursos por meio da rede.
- 52** Do ponto de vista da abrangência geográfica, as redes de computadores podem ser classificadas em redes por difusão, ponto-a-ponto e multi-entrega.
- 53** Segundo o critério da topologia, as redes de computadores podem ser classificadas em LANs, MANs e WANs.
- 54** Tomando como critérios o caminho de comunicação usado e a forma como os dados são transmitidos, uma rede por comutação por circuito é aquela em que um circuito físico é estabelecido entre os nós terminais antes de ocorrer a comunicação.
- 55** As redes por comutação por pacotes assemelham-se às redes por comutação por circuito no que diz respeito ao estabelecimento de circuito físico antes do início da comunicação. Entretanto, as mensagens são subdivididas em unidades menores, transmitidas independentemente.

Quanto aos protocolos de roteamento, julgue os itens subsequentes.

- 56** Os protocolos de roteamento podem ser de *gateway* interior ou exterior, que operam, respectivamente, inter e intradomínio.
- 57** Protocolos *distance vector* mantêm, durante a operação, uma tabela com informações da menor distância para determinado destino e o caminho que deve ser utilizado. As informações dessa tabela são atualizadas por meio de troca de mensagens sobre o estado dos enlaces de comunicação.
- 58** A operação de protocolos *link-state* obedece às seguintes fases: descoberta dos roteadores vizinhos e de suas redes; cálculo do custo do envio de mensagens para cada vizinho; formatação e envio das informações coletadas para os vizinhos; cálculo do menor caminho para os outros roteadores.
- 59** RIP é um protocolo embasado no algoritmo *distance vector* que utiliza a porta 520 UDP.
- 60** OSPF é um protocolo embasado no algoritmo *link-state* que roda diretamente sobre o IP e que utiliza a designação 89 para protocolo nos datagramas IP.

Julgue os itens a seguir referentes aos protocolos de redes.

- 61** O *asynchronous transfer mode* (ATM) define ambiente de rede de múltipla velocidade que provê grande variedade de serviços complexos para aplicações como transmissão de dados, voz e vídeo — separada ou simultaneamente — sobre o mesmo caminho de rede. Esse protocolo tem sido usado tanto em redes públicas quanto em redes privadas.
- 62** O *Frame Relay* é um protocolo público de chaveamento por pacotes para redes de longa distância. A partir desse protocolo, que provê conectividade entre redes locais, originou-se parte do padrão das redes digitais de serviços integrados (ISDN-RDSI).
- 63** O *Data-Link Switching* (DLSw) provê um meio de transportar tráfego SNA e NetBIOS sobre uma rede IP, e constitui uma alternativa ao *Source-Route Bridge* (SRB), que transporta o mesmo tipo de tráfego em redes *Token Ring*.
- 64** A arquitetura SNA é composta pelas seguintes entidades: controle de enlace de dados, controle de caminho, controle de transmissão, controle de fluxo de dados, serviços de apresentação e serviços de transação.
- 65** O IPX tem como base o *Internet Datagram Protocol* (IDP), e é um protocolo não orientado à conexão, que não oferece garantia ou verificação do sucesso na comunicação e mecanismos que garantam a segurança na troca de pacotes.

Considerando-se o modelo de referência OSI, julgue os próximos itens.

- 66** O modelo *Open Systems Interconnection* (OSI) foi proposto pela International Standards Organization (ISO), com objetivo de padronizar os protocolos usados para a conexão de sistemas que estão abertos para a comunicação com outros sistemas.
- 67** O modelo OSI compreende sete camadas: física, de enlace, de rede, de transporte, de sessão, de apresentação de dados e de aplicação.
- 68** Os princípios que levaram às camadas do modelo OSI podem ser resumidos nas seguintes premissas: cada camada corresponde a uma abstração e deve ter suas funcionalidades bem definidas; as interfaces entre as camadas devem minimizar o fluxo de informações entre elas; funcionalidades idênticas e correlatas devem ser agrupadas em uma mesma camada para evitar o excesso de complexidade do modelo.
- 69** O modelo OSI é hierárquico, de modo que uma camada superior consome serviços das camadas inferiores.
- 70** Tradução sintática e semântica, controle de fluxo de diálogo e transmissão livre de erros são, respectivamente, funções associadas às camadas de apresentação de dados, de transporte e de enlace de dados.

No referente ao protocolo IP, julgue os seguintes itens.

- 71** O protocolo IP baseia-se em uma estratégia de melhor esforço e provê um serviço de entrega de datagramas não confiável e orientado à conexão.
- 72** O tratamento de erros no IP consiste no descarte de datagramas e, se for o caso, no envio de uma mensagem ICMP.
- 73** Apesar de o IP manter informações de estado sobre a transmissão de sucessivos datagramas, cada datagrama é enviado independentemente e pode, inclusive, ser entregue fora da ordem original de envio.

```
sun % netstat -in
```

Name	Mtu	Net/Dest	Address	lpkts	lerrs	Opkts	Oerrs	Collis	Queue
le0	1500	140.252.13.32	140.252.13.33	67719	0	92133	0	1	0
s10	552	140.252.1.183	140.252.1.29	48035	0	54963	0	0	0
lo0	1536	127.0.0.0	127.0.0.1	15548	0	15548	0	0	0

R. W. Stevens. TCP/IP Illustrated, v. 1, c.3.

Considerando as informações acima, obtidas a partir da captura de tela de um computador, julgue os itens subsequentes.

- 74** De acordo com as informações mostradas, caso o *host* esteja com o roteamento habilitado, deve ocorrer fragmentação quando um datagrama recebido pela interface `le0` for roteado pela interface `s10`.
- 75** Ocorrerá fragmentação se o *host* associado às informações acima mandar um `ping` (ICMP *echo request*) com 1024 bytes para o endereço 140.252.1.183. Entretanto, se um datagrama de mesmo tamanho for enviado para 140.252.13.34, a fragmentação não ocorrerá.

Acerca do protocolo TCP, julgue os itens a seguir.

- 76** O protocolo TCP provê serviço de *byte stream*, confiável e orientado à conexão.
- 77** O uso de números seqüenciais e de *acknowledgement*, juntamente com o janelamento, são mecanismos básicos para a confiabilidade de entrega dos segmentos TCP.
- 78** Se dois *hosts* enviam simultaneamente, um para o outro, segmentos TCP com o *flag* SYN setado (*flag* ACK resetado), serão iniciadas duas conexões distintas.
- 79** O algoritmo de Nagle do TCP tem por finalidade evitar que segmentos pequenos venham a colaborar para o congestionamento em redes lentas. Esse algoritmo determina que, se houver segmentos pequenos enviados para os quais ainda não chegou o respectivo ACK, apenas mais um segmento poderá ser enviado.
- 80** O tamanho da janela deslizante é negociado entre os *hosts* no processo do *three-way handshake*.

Considerando-se a gerência de redes TCP/IP, julgue os próximos itens.

- 81** A gerência de redes TCP/IP consiste de estações de gerenciamento, gerentes, que se comunicam com elementos da rede. Estes podem ser quaisquer dispositivos capazes de usar suíte TCP/IP, juntamente com um agente de gerência.
- 82** A comunicação entre gerentes e agentes pode ocorrer de duas formas: periodicamente, o gerente interroga os agentes para obter alguma informação específica, que é enviada de volta pelos agentes; ou os agentes enviam, a qualquer momento e por sua iniciativa, informações sobre eventos significativos que venham a demandar ação por parte do gerente.
- 83** A gerência TCP/IP envolve três componentes básicos: a base de informações de gerenciamento (MIB), que especifica as variáveis que os elementos de rede têm que manter; um conjunto de estruturas comuns e um esquema de identificação usados para referenciar as variáveis na MIB; e um protocolo de comunicação entre gerentes e agentes, o SNMP.
- 84** O SNMP utiliza as portas UDP 161 e 162, sendo a primeira utilizada pelos agentes para envio de informações sobre as condições do sistema e eventos importantes ao gerente.
- 85** Em todas as suas versões, o protocolo SNMP utiliza mecanismos fortes de autenticação e sigilo na comunicação.

Julgue os seguintes itens relativos a VPNs.

- 86** Uma VPN é uma conexão estabelecida sobre uma infraestrutura pública ou compartilhada, que utiliza tecnologias de cifração e autenticação para garantir a segurança dos dados trafegados.
- 87** A segurança dos dados em uma VPN pode ser assegurada em diferentes camadas: ao nível da aplicação (por exemplo, com túneis SSH), do transporte (por exemplo, com SSL), da rede (por exemplo, com IPSec) ou no enlace (por exemplo, com L2TP).
- 88** Um componente básico de uma VPN é o tunelamento, definido como o encapsulamento dos dados de um protocolo de uma camada mais alta em um protocolo de camada mais baixa.
- 89** Algumas vantagens do uso de uma VPN são segurança, melhor eficiência em custo e menor complexidade.
- 90** As VPNs implementadas no nível de aplicação são mais eficientes e mais facilmente portáveis que as implementadas em *kernel*.

Acerca de algoritmos criptográficos, julgue os itens subsequentes.

- 91** Os algoritmos de chave simétrica ou compartilhada utilizam o mesmo valor de chave tanto para cifração quanto para decifração.
- 92** Uma premissa básica para a segurança dos algoritmos simétricos é a existência de uma forma segura de distribuição e guarda da chave compartilhada entre as partes que vão se comunicar.
- 93** Os algoritmos de chave assimétrica utilizam dois valores de chave: um público, usado para a cifração, e outro mantido privado, que é usado na decifração.
- 94** Em algoritmos de chave assimétrica, é factível a obtenção da chave privada a partir da pública com o uso de técnicas de engenharia reversa.
- 95** Se duas cópias de um mesmo arquivo forem cifradas independentemente, uma com um algoritmo simétrico e a outra com um assimétrico, a primeira operação, normalmente, demorará menos que a segunda.

Com relação à segurança de perímetro, julgue os itens a seguir.

- 96** O perímetro de segurança da rede pode ser composto de: roteadores de borda, *firewalls*, IDSs, IPSs, terminadores de VPN, DMZs e redes com tráfego filtrado.
- 97** O roteador de borda é o último roteador sobre o qual se pode ter controle antes de entrar, de fato, na Internet. Geralmente, sua operação segue as políticas de roteamento e de acesso, neste caso implementadas por listas de acesso que controlam os tráfegos ingresso e egresso.
- 98** *Firewalls* são pontos de concentração de tráfego que controlam o tráfego de entrada e de saída da rede. Entretanto, as regras e as características de implementação e operação lhes conferem menor especificidade e granularidade que as listas de acesso dos roteadores.
- 99** Os IDS podem ser embasados em rede ou em *host*. No primeiro caso, inspecionam o tráfego de rede para detectar atividade maliciosa; no outro, residem no *host* e, tipicamente, atuam com o objetivo de deter ataques, sem que seja necessária a intervenção do administrador.
- 100** Os IPS detectam anomalias na operação da rede e reportam-nas aos administradores para análise e ação posterior.

Com respeito a serviços e aplicações de rede, julgue os próximos itens.

- 101** O protocolo SMTP utiliza a porta 25 UDP.
- 102** O IMAP tem, em comparação ao POP3, a vantagem de permitir o acesso e manter as caixas de correio dos usuários no servidor.
- 103** O POP3 roda sobre o TCP na porta 109.
- 104** O IMAP suporta o compartilhamento de caixas postais entre usuários membros de um grupo de trabalho.
- 105** O DNS utiliza a portas 53 UDP nas consultas e a 53 TCP nas transferências de zona em servidores primários e secundários.

No que se refere ao sistema operacional Unix, julgue os seguintes itens.

- 106** Os *inodes* armazenam informações sobre objetos no sistema de arquivo. Entre essas, incluem-se o tipo de objeto, a localização do conteúdo do objeto no disco, seu tamanho (se for o caso), a modificação mais recente feita no *inode*, a modificação mais recente no conteúdo do objeto, o último acesso ao objeto, o proprietário, o grupo e os privilégios de acesso.
- 107** O sistema de permissões e privilégios de arquivos permite que um arquivo seja executável, porém sem privilégios de leitura e escrita.
- 108** Em alguns casos, *scripts* executáveis necessitam de privilégios de leitura e execução para que possam ser executados.

109 O superusuário (*su*) pode alterar um arquivo que está localizado em um sistema de arquivos montado apenas para leitura.

110 O superusuário pode desmontar um sistema de arquivos que contém arquivos abertos.

Quanto ao NAT, julgue os itens subsequentes.

- 111** Em sua configuração mais simples, o NAT opera em um roteador que conecta duas redes, sendo que uma, a interna, utiliza endereços privativos ou obsoletos que precisam ser traduzidos para endereços válidos, antes de serem enviados para a rede externa.
- 112** O NAT, em geral, opera em conjunto com o roteamento, mas também é comum encontrá-lo em *firewalls* e *proxies*.
- 113** As técnicas de NAT permitem apenas o mapeamento um para um entre endereços.
- 114** Os mapeamentos efetuados pelo NAT são exclusivamente estáticos.
- 115** No PAT, uma forma de implementar o NAT, os endereços internos são combinados com as portas internas, para que se possa cobrir toda a faixa endereçável internamente. Essa abordagem permite o *overload* da faixa de endereçamento de saída, o que torna necessário manter inalterada a porta interna.

Com relação às *proxies* e aos filtros de acesso, julgue os itens a seguir.

- 116** A filtragem de pacotes sem estado baseia-se na inspeção das informações de cabeçalho para determinar se um pacote pode ou não ser aceito ou transmitido.
- 117** A filtragem com informação de estado leva em consideração o estado das conexões para aceitar ou não pacotes, o que reduz o esforço computacional da inspeção em si e aumenta a granularidade da filtragem.
- 118** Uma *proxy* media a conexão de um cliente ou usuário para prover acesso a um serviço de rede, o que evita a conexão direta *peer-to-peer*.
- 119** Um *firewall* embasado em *proxy* tem melhor desempenho (retardo e *throughput*, por exemplo) quando comparado a um *firewall* que opera em camadas mais baixas, visto que, como atua no nível da aplicação, pode inspecionar não só as informações de cabeçalho, como também as dos protocolos de aplicação.
- 120** Uma desvantagem do uso de um *firewall* baseado em *proxy* é que ele pode ser mais difícil de configurar e operar. Entretanto, o uso de VPNs pode reverter essa situação.