

• 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 rascunho e, posteriormente, a **folha de respostas**, que é o único documento válido para a correção das suas provas.

• Nos itens que avaliam **Conhecimentos de Informática**, a menos que seja explicitamente informado o contrário, considere que todos os programas mencionados estão em configuração-padrão, em português, que o *mouse* está configurado para pessoas destros e que expressões como clicar, clique simples e clique duplo referem-se a cliques com o botão esquerdo do *mouse*. Considere também que não há restrições de proteção, de funcionamento e de uso em relação aos programas, arquivos, diretórios e equipamentos mencionados.

CONHECIMENTOS BÁSICOS

1 A análise que a sociedade costuma fazer da
violência urbana é fundamentada em fatores emocionais,
quase sempre gerados por um crime chocante, pela falta de
4 segurança nas ruas do bairro, por preconceito social ou por
discriminação. As conclusões dos estudos científicos não são
levadas em conta na definição de políticas públicas. Como
7 reflexo dessa atitude, o tratamento da violência evoluiu
pouco no decorrer do século XX, ao contrário do que
ocorreu com o tratamento das infecções, do câncer ou da
10 AIDS. Nos últimos anos, entretanto, estão sendo
desenvolvidos métodos analíticos mais precisos para
avaliar a influência dos fatores econômicos, epidemiológicos
13 e sociológicos associados às raízes sociais da violência
urbana: pobreza, impunidade, acesso a armamento,
narcotráfico, intolerância social, ruptura de laços familiares,
16 imigração, corrupção de autoridades ou descrédito na justiça.

Dráuzio Varella. Internet: <<http://www.drauziovarella.com.br>> (com adaptações).

Em relação ao texto acima, julgue os itens que se seguem.

- 1 As informações do texto indicam que, além da consideração de “fatores emocionais” (l.2) que geram violência, as políticas públicas voltadas para a segurança dos cidadãos baseiam-se freqüentemente nas “conclusões dos estudos científicos” (l.5) que focalizam esse tema.
- 2 A expressão “Como reflexo dessa atitude” (l.6-7) introduz uma idéia que é uma conseqüência em relação à informação antecedente. Portanto poderia, sem prejuízo da correção e do sentido do texto, ser substituída pela palavra **Conseqüentemente**.
- 3 A substituição do termo “estão sendo desenvolvidos” (l.10-11) por **estavam se desenvolvendo** provoca alterações estruturais sem alterar semanticamente a informação original nem transgredir as normas da escrita culta.
- 4 Na linha 13, o emprego do sinal indicativo de crase em “às raízes” justifica-se pela regência de “associados” e pela presença de artigo; o sinal deveria ser eliminado caso a preposição viesse sem o artigo.

5 Na linha 14, estaria gramaticalmente correta a inserção, entre a palavra “urbana” e o sinal de dois-pontos, de qualquer uma das seguintes expressões, antecedidas de vírgula: **como, tais como, quais sejam, entre as quais se destacam**.

6 É correto inferir do texto que houve evolução no tratamento de certas doenças porque estão sendo desenvolvidos métodos analíticos mais exatos para avaliar seus fatores econômicos, epidemiológicos e sociológicos associados às raízes da violência.

Texto I – itens de 7 a 10

1 Diversos municípios brasileiros, especialmente
aqueles que se urbanizaram de forma muito rápida, não
oferecem à população espaços públicos para a prática de
4 atividades culturais, esportivas e de lazer. A ausência desses
espaços limita a criação e o fortalecimento de redes de
relações sociais. Em um tecido social esgarçado, a violência
7 é cada vez maior, ameaçando a vida e enclausurando
ainda mais as pessoas nos espaços domésticos.

Internet: <<http://www.polis.org.br>> (com adaptações).

Considerando o texto I, julgue os seguintes itens.

- 7 A expressão “tecido social esgarçado” (l.6) está empregada em sentido figurado e representa a idéia de que as estruturas sociais estão fortalecidas em suas instituições oficiais.
- 8 A inserção da palavra **conseqüentemente**, entre vírgulas, antes de “cada vez” (l.7) torna explícita a relação entre idéias desse período e aquelas apresentadas anteriormente no texto.
- 9 A expressão “ainda mais” (l.8) reforça a idéia implícita de que há dois motivos para o enclausuramento das pessoas: a falta de espaços públicos que favoreçam as relações sociais com atividades culturais, esportivas e de lazer e o aumento da ameaça de violência.

Texto II – itens de 10 a 12

1 Entre os primatas, o aumento da densidade populacional não conduz necessariamente à violência desenfreada. Diante da redução do espaço físico, criamos
4 leis mais fortes para controlar os impulsos individuais e impedir a barbárie. Tal estratégia de sobrevivência tem lógica evolucionista: descendemos de ancestrais que tiveram
7 sucesso na defesa da integridade de seus grupos; os incapazes de fazê-lo não deixaram descendentes. Definitivamente, não somos como os ratos.

Dráuzio Varella. Internet: <<http://www.drauziovarella.com.br>> (com adaptações).

Acerca dos textos I e II, julgue os itens a seguir.

- 10 Tanto no texto I como no II, a questão do espaço físico como um dos fatores intervenientes no processo de intensificação da violência é vista sob o prisma da densidade populacional excessiva.
- 11 Como a escolha de estruturas gramaticais pode evidenciar informações pressupostas e significações implícitas, no texto II, o emprego da forma verbal em primeira pessoa — “criamos” (l.3) — autoriza a inferência de que os seres humanos pertencem à ordem dos primatas.
- 12 Por funcionar como um recurso coesivo de substituição de idéias já apresentadas, no texto II, a expressão “Tal estratégia de sobrevivência” (l.5) retoma o termo antecedente “violência desenfreada” (l.2-3).

Os fragmentos contidos nos itens subseqüentes foram adaptados de um texto escrito por Ângela Lacerda para a Agência Estado. Julgue-os quanto à correção gramatical.


- 13 O programa Escola Aberta, que usa as escolas nos fins de semana para atividades culturais, sociais e esportivas de alunos e jovens da comunidade reduziu os índices de violência registrados nos estabelecimentos e melhorou o aproveitamento escolar.
- 14 Em Pernambuco e no Rio de Janeiro, primeiros estados a adotarem o programa recomendado pela UNESCO, o índice de redução de criminalidade para as escolas que implantaram o Escola Aberta desde o ano 2000 foi de 60% em relação às escolas que não o adotaram.
- 15 A maior redução da violência observada nos locais onde o programa tem mais tempo de existência mostram, segundo a UNESCO, que os resultados vão se tornando melhores a longo prazo, ou seja, a proporção que a comunidade se apropriaria do programa.



Considere que um delegado de polícia federal, em uma sessão de uso do Internet Explorer 6 (IE6), obteve a janela ilustrada acima, que mostra uma página *web* do sítio do DPF, cujo endereço eletrônico está indicado no campo **Endereço**. A partir dessas informações, julgue os itens de 16 a 19.


- 16 Considere a seguinte situação hipotética.

O conteúdo da página acessada pelo delegado, por conter dados importantes à ação do DPF, é constantemente atualizado por seu *webmaster*. Após o acesso mencionado acima, o delegado desejou verificar se houve alteração desse conteúdo.

Nessa situação, ao clicar o botão , o delegado terá condições de verificar se houve ou não a alteração mencionada, independentemente da configuração do IE6, mas desde que haja recursos técnicos e que o IE6 esteja em modo *online*.

- 17 O armazenamento de informações em arquivos denominados *cookies* pode constituir uma vulnerabilidade de um sistema de segurança instalado em um computador. Para reduzir essa vulnerabilidade, o IE6 disponibiliza recursos para impedir que *cookies* sejam armazenados no computador. Caso o delegado deseje configurar tratamentos referentes a *cookies*, ele encontrará recursos a partir do uso do *menu* **Ferramentas**.


18 Caso o acesso à Internet descrito tenha sido realizado mediante um provedor de Internet acessível por meio de uma conexão a uma rede LAN, à qual estava conectado o computador do delegado, é correto concluir que as informações obtidas pelo delegado transitaram na LAN de modo criptografado.

19 Por meio do botão , o delegado poderá obter, desde que disponíveis, informações a respeito das páginas previamente acessadas na sessão de uso do IE6 descrita e de outras sessões de uso desse aplicativo, em seu computador. Outro recurso disponibilizado ao se clicar esse botão permite ao delegado realizar pesquisa de conteúdo nas páginas contidas no diretório histórico do IE6.



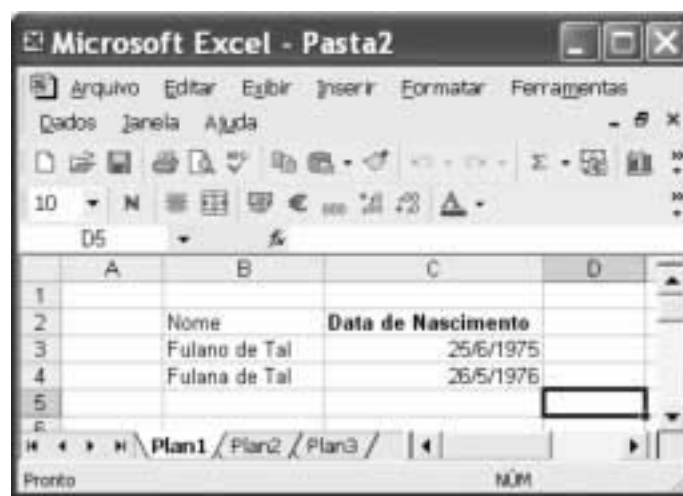
Considerando a figura acima, que ilustra uma janela do Word 2000 contendo parte de um texto extraído e adaptado do sítio <http://www.funai.gov.br>, julgue os itens subsequentes.

20 Considere o seguinte procedimento: selecionar o trecho “Funai, (...) Federal”; clicar a opção Estilo no menu **Exibir**; na janela decorrente dessa ação, marcar o campo Todas em maiúsculas; clicar OK. Esse procedimento fará que todas as letras do referido trecho fiquem com a fonte maiúscula.


21 A correção e as idéias do texto mostrado serão mantidas caso se realize o seguinte procedimento: clicar imediatamente antes de “no final”; pressionar e manter pressionada a tecla **Shift**; clicar imediatamente após “semana,”; liberar a tecla **Shift**; pressionar e manter pressionada a tecla **Ctrl**; teclar **X**; clicar imediatamente após “apreenderam”; teclar **Enter**; clicar o botão .

22 As informações contidas na figura mostrada permitem concluir que o documento em edição contém duas páginas e, caso se disponha de uma impressora devidamente instalada e se deseje imprimir apenas a primeira página do documento, é suficiente realizar as seguintes ações: clicar a opção Imprimir no menu **Arquivo**; na janela aberta em decorrência dessa ação, assinalar, no campo apropriado, que se deseja imprimir a página atual; clicar OK.

23 Para encontrar todas as ocorrências do termo “Ibama” no documento em edição, é suficiente realizar o seguinte procedimento: aplicar um clique duplo sobre o referido termo; clicar sucessivamente o botão **Ir**.



A figura acima mostra uma janela do Excel 2002 com uma planilha em processo de edição. Com relação a essa figura e ao Excel 2002, e considerando que apenas a célula C2 está formatada como negrito, julgue o item abaixo.

24 É possível aplicar negrito às células B2, B3 e B4 por meio da seguinte seqüência de ações, realizada com o mouse: clicar a célula C2; clicar ; posicionar o ponteiro sobre o centro da célula B2; pressionar e manter pressionado o botão esquerdo; posicionar o ponteiro no centro da célula B4; liberar o botão esquerdo.

Nos últimos 13 anos, a América Latina cumpriu grande parte de suas tarefas econômicas. Mesmo assim, a desigualdade e a pobreza aumentaram na região. O diagnóstico é da Comissão Econômica para a América Latina e o Caribe (CEPAL), que propõe para a região uma nova estratégia de desenvolvimento produtivo. Para o secretário executivo do órgão das Nações Unidas, a maior integração da região foi um ganho dos últimos anos. Sua aposta para reduzir a forte desigualdade que ainda existe é a união de crescimento econômico com proteção social. Ele propôs a substituição do conceito de mais mercado e menos Estado por uma visão que aponta para “mercados que funcionem bem e governos de melhor qualidade”.

América Latina cresceu sem dividir. In: Jornal do Brasil, 25/6/2004, p. 19A (com adaptações).

Tendo o texto acima como referência inicial e considerando a amplitude do tema por ele abordado, julgue os itens subseqüentes.

- 25** Ao relatar que os países latino-americanos cumpriram “grande parte de suas tarefas econômicas” nos últimos anos, o texto permite supor a existência de algum tipo de receituário que a região deveria seguir para se modernizar e se desenvolver.
- 26** No período aludido pelo texto, ainda que possa ter ostentado números positivos de crescimento econômico, a América Latina fracassou quanto aos índices sociais, de modo a não conseguir romper com a histórica concentração de renda, matriz da enorme desigualdade existente na região.
- 27** Ao propor uma nova estratégia de desenvolvimento produtivo para a região, a CEPAL implicitamente reconhece os equívocos da política econômica que, de maneira praticamente generalizada, a América Latina adotou especialmente na última década do século passado.
- 28** O Brasil foi uma exceção no cenário latino-americano retratado pelo texto. Particularmente nos dois períodos governamentais de Fernando Henrique Cardoso, o país optou por um modelo autônomo de desenvolvimento que prescindia da inserção internacional de sua economia.
- 29** É provável ter sido o Chile o exemplo mais notório — e dramático — de fracasso da adoção da política econômica preconizada pelo neoliberalismo: além de ter crescimento quase nulo, o país sucumbiu ante a dimensão de uma crise social sem precedentes em sua história.

Mais de 340 pessoas — entre elas 155 crianças — morreram no desfecho trágico da tomada de reféns na escola de Beslan. Funcionários dos hospitais da região indicam que pelo menos 531 pessoas foram hospitalizadas, das quais 336 eram crianças. O presidente russo Vladimir Putin culpou o terror internacional pelo ataque, após visitar o local do massacre e ordenar o fechamento das fronteiras da região da Ossétia do Norte, para evitar a fuga de um número indefinido de terroristas que escapou. Para especialistas ocidentais, a operação das forças de segurança russas foi um fiasco total.

Mortos no massacre passam de 340. In: O Estado de S. Paulo, 5/9/2004, capa (com adaptações).

Tendo o texto acima como referência inicial e considerando algumas características marcantes do mundo contemporâneo, julgue os itens que se seguem.

- 30** A hipotética presença de terroristas árabes — anunciada pelo governo russo — no episódio focalizado no texto indica que, pela primeira vez depois do 11 de setembro de 2001, esses terroristas resolveram atacar no Ocidente, escolhendo um alvo estratégico e de grande visibilidade internacional.
- 31** A maior fragilidade da atual Rússia, claramente percebida por terroristas e pelos que lutam por autonomia em relação a Moscou, é a perda de seu arsenal bélico, sobretudo nuclear, resultante da desintegração da URSS.

- 32** A ação do terrorismo internacional, na atualidade, assusta a opinião pública mundial, eleva consideravelmente os gastos governamentais com segurança e dissemina o temor ante a expectativa de ataques a qualquer tempo e lugar.

Amanda, ocupante de cargo público lotado no Departamento de Polícia Federal (DPF), foi condenada administrativamente à penalidade de advertência por, no recinto da repartição, ter dirigido impróprios a um colega de trabalho.

Com referência à situação hipotética apresentada acima e considerando que o DPF é um órgão do Ministério da Justiça (MJ), julgue os itens a seguir.

- 33** O DPF integra a administração indireta da União.
- 34** Amanda deve ser brasileira nata, pois a legislação administrativa veda a investidura de brasileiros naturalizados em cargos públicos federais.
- 35** O ato que aplicou a referida sanção a Amanda configura exercício de poder disciplinar.
- 36** Para ter direito a impugnar judicialmente o ato que lhe aplicou a referida penalidade, é desnecessário que Amanda esgote previamente os recursos administrativos cabíveis para impugnar essa decisão.

Acerca do processo penal, julgue os itens seguintes.

- 37** A legislação determina que as provas periciais devem prevalecer sobre as provas testemunhais.
- 38** É requisito de validade da nomeação de um perito judicial a aprovação prévia do seu nome pelas partes envolvidas no processo.

Augusto e Luciano são agentes de polícia federal que, no exercício de suas funções, realizaram a prisão em flagrante de um traficante de drogas e apreenderam os vinte pacotes de maconha que ele tinha consigo. Durante a detenção do traficante, um comparsa dele tentou, sem sucesso, impedir a prisão, disparando arma de fogo na direção da viatura em que estavam os policiais. Luciano, porém, revidou e terminou por atingir o braço do agressor, que, apesar de ferido, conseguiu fugir.

Considerando a situação hipotética acima, julgue os itens subseqüentes.

- 39** Ao disparar na direção da viatura, com o objetivo de impedir a prisão, o comparsa do traficante praticou crime de resistência.
- 40** Se o comparsa do traficante houvesse alvejado Augusto, causando-lhe ferimento que o levasse à morte, ele deveria ser condenado pela prática de homicídio doloso, mesmo se restasse comprovado que a sua intenção não era a de matar o policial, mas simplesmente a de permitir a fuga do traficante.
- 41** Se, ao revidar aos disparos, na tentativa de defender-se, Luciano acertasse um tiro na perna do comparsa do traficante, esse ato não configuraria crime porque, apesar de ser penalmente típico, falta-lhe antijuridicidade.
- 42** Se, ao colocar os entorpecentes na viatura, Augusto apropriar-se de um dos pacotes, escondendo-o dentro de sua mochila, ele praticará crime de furto.

Texto para os itens de 43 a 50

10 DOS CRITÉRIOS DE AVALIAÇÃO E DE CLASSIFICAÇÃO NA PRIMEIRA ETAPA

- 10.1 Todos os candidatos serão submetidos a duas provas objetivas — uma de Conhecimentos Básicos (P_1), composta de 50 itens, e outra de Conhecimentos Específicos (P_2), composta de 70 itens — e a uma prova discursiva.
- 10.2 A nota em cada item das provas objetivas, feita com base nas marcações da folha de respostas, será igual a: 1,00 ponto, caso a resposta do candidato esteja em concordância com o gabarito oficial definitivo da prova; -1,00 ponto, caso a resposta do candidato esteja em discordância com o gabarito oficial definitivo da prova; 0,00, caso não haja marcação ou haja marcação dupla (C e E).
- 10.3 O cálculo da nota em cada prova objetiva, comum às provas de todos os candidatos, será igual à soma algébrica das notas obtidas em todos os itens que a compõem.
- 10.4 Será reprovado nas provas objetivas e eliminado do concurso o candidato que se enquadrar em pelo menos um dos itens a seguir:
- obtiver nota inferior a 8,00 pontos na prova de Conhecimentos Básicos (P_1);
 - obtiver nota inferior a 17,00 pontos na prova de Conhecimentos Específicos (P_2);
 - obtiver nota inferior a 36,00 pontos no conjunto das provas objetivas.

10.5 Para cada candidato não eliminado segundo os critérios definidos no subitem 10.4, será calculada a nota final nas provas objetivas (NFPO) pela soma algébrica das notas obtidas nas duas provas objetivas.

11 DA NOTA FINAL NA PRIMEIRA ETAPA

- 11.1 A nota final na primeira etapa (NFIE) do concurso público será a soma da nota final nas provas objetivas (NFPO) e da nota na prova discursiva (NPD).
- 11.2 Os candidatos serão ordenados por cargo/área/localidade de vaga de acordo com os valores decrescentes de NFIE.

12 DOS CRITÉRIOS DE DESEMPATE

- 12.1 Em caso de empate na classificação, terá preferência o candidato que, na seguinte ordem:
- obtiver maior nota na prova discursiva;
 - obtiver maior nota na prova de Conhecimentos Específicos (P_2);
 - obtiver maior número de acertos na prova de Conhecimentos Específicos (P_2);
 - obtiver maior número de acertos na prova de Conhecimentos Básicos (P_1).

Julgue os itens seguintes, de acordo com as normas estabelecidas no texto acima, adaptado do Edital n.º 25/2004 – DGP/DPF – REGIONAL, de 15 de julho de 2004.

- 43 De acordo com o texto acima, se um candidato marcar ao acaso todas as respostas dos 120 itens que compõem as duas provas objetivas, a probabilidade de ele ser reprovado nessas provas será igual a $\frac{8}{50} \times \frac{17}{70} \times \frac{36}{120}$.
- 44 Do ponto de vista lógico, é equivalente ao texto original a seguinte reescritura do subitem 10.4:
- 10.4 Será aprovado nas provas objetivas o candidato que se enquadrar em todos os itens a seguir:
- obtiver nota maior ou igual a 8,00 pontos na prova de Conhecimentos Básicos (P_1);
 - obtiver nota maior ou igual a 17,00 pontos na prova de Conhecimentos Específicos (P_2);
 - obtiver nota maior ou igual a 36,00 pontos no conjunto das provas objetivas.

- 45 Se um candidato é considerado “reprovado nas provas objetivas” por não atender o disposto na alínea “a)” do subitem 10.4 do texto, também não atenderá o disposto na alínea “c)” do mesmo subitem.
- 46 De acordo com o subitem 10.5 do texto, após a aplicação do concurso, se um candidato não teve a sua nota final nas provas objetivas (NFPO) calculada pela soma algébrica das notas obtidas nas duas provas objetivas, então esse candidato foi eliminado do concurso segundo os critérios definidos no subitem 10.4.
- 47 Considere que um candidato obteve x acertos na prova P_1 e que a sua nota nessa prova tenha sido a mínima necessária para que ele não fosse reprovado de acordo com o disposto na alínea “a)” do subitem 10.4 do texto. Nessas condições, existem mais de 20 valores possíveis para o número de acertos x desse candidato.
- 48 De acordo com os critérios de desempate apresentados no item 12 do texto acima, a probabilidade de que dois candidatos fiquem empatados no concurso é igual a zero.
- 49 Mantém-se a correção lógica e semântica do texto substituindo-se o critério “c)” do subitem 12.1 por: **obtiver menor número de erros na prova de Conhecimentos Específicos (P_2)**.
- 50 O seguinte critério, inserido como alínea e) do subitem 12.1, seria redundante com os já existentes e não traria qualquer alteração na classificação estabelecida pelos critérios de “a)” a “d)”: **obtiver maior nota na prova de Conhecimentos Básicos (P_1)**.

RASCUNHO

CONHECIMENTOS ESPECÍFICOS

```
C:\temp>debug arq1.txt
-d
0006:0100 45 50 46 00 00 20 44 65-70 2E 00 0A 50 6F 6C 20 EPF.. Dep...Pol-
0006:0110 00 00 46 45 44 2E 00 0A-0B 10 2A E4 34 00 F5 0C ..Fed....*.4...
0006:0120 00 45 10 03 45 02 50 0A-45 11 2A E4 03 45 04 50 .E..E.P.E.*.E.P
0006:0130 00 4E FE 00 44 03 51 50-0E C1 26 FF 34 E8 02 16 .H..0.QP..8.4...
0006:0140 09 46 F0 01 2C 40 33 02-E0 F7 06 57 E8 00 F4 E0 .F...K3...N...
0006:0150 40 09 76 F0 00 1E 2C 40-0E 00 07 30 40 40 09 46 K.w.k.,K...0KH.F
0006:0160 09 C3 F7 00 31 00 09 08-0B 10 2A E4 0A 47 04 50 ....1.....*.G.P
0006:0170 00 45 10 03 45 02 03 C6-50 FF 36 2C 40 56 E8 45 .E..E...P.6,KU.E
-e 100
0006:0100 45.44 50.50 46.46 00.2d 0A.0d 20.0a 44.44 65.65
0006:0108 70.70 2E.74 00.6f 0A.2e 50.
-r cx
CX 0010
:16
-w
Gravando 00016 bytes
-r ax
AX 0000
:abcd
-a 160
0006:0160 MOV BX, AX
0006:0162 NEG BX
0006:0164 XOR AX, BX
0006:0166 MOV AX, BX
0006:0168
-r ip
IP 0100
:160
-r
AX=ABCD BX=0000 CX=0016 DX=0000 SP=FFEE BP=0000 SI=0000 DI=0000
DS=0006 ES=0006 SS=0006 CS=0006 IP=0160 HU UP EI PL NZ NA PO NC
0006:0160 89C3 MOV BX,AX
-p
AX=ABCD BX=ABCD CX=0016 DX=0000 SP=FFEE BP=0000 SI=0000 DI=0000
DS=0006 ES=0006 SS=0006 CS=0006 IP=0162 HU UP EI PL NZ NA PO NC
0006:0162 F700 NEG BX
-p
AX=ABCD BX=5433 CX=0016 DX=0000 SP=FFEE BP=0000 SI=0000 DI=0000
DS=0006 ES=0006 SS=0006 CS=0006 IP=0164 HU UP EI PL NZ AC PE CY
0006:0164 3100 XOR AX,AX
-p
AX=FFFE BX=5433 CX=0016 DX=0000 SP=FFEE BP=0000 SI=0000 DI=0000
DS=0006 ES=0006 SS=0006 CS=0006 IP=0166 HU UP EI NG NZ NA PO NC
0006:0166 8900 MOV AX,BX
-q
```

A figura acima apresenta uma sessão de uso da ferramenta de *debug* do MS Windows, sendo executada em um computador com arquitetura Intel IA-32. A sessão foi encerrada após a

digitação do comando “q” seguido de . A partir da análise dos comandos efetuados na sessão e acerca do uso de *debug*, julgue os itens a seguir.

- 51 O tamanho original do arquivo “arq1.txt” era de 18 (decimal) *bytes* e ele foi alterado para 16 (decimal) *bytes*.
- 52 O arquivo de nome “arq1.txt” possuía, antes do início da sessão, 5 linhas de texto.
- 53 O arquivo de nome “arq1.txt” ficou com 4 linhas de texto, após o fim da sessão.
- 54 O conteúdo do arquivo “arq1.txt”, ao final da sessão de trabalho, foi modificado para conter a seqüência de caracteres “DPF-”.
- 55 Em momentos distintos dessa sessão de trabalho, o registrador AX armazenou os valores 0 e 125715 (em notação octal).
- 56 A sessão de trabalho envolveu a digitação de três instruções em formato de montador que foram gravadas no arquivo “arq1.txt”.
- 57 Quatro instruções de montador foram executadas ao comando do usuário durante a sessão.
- 58 O *flag* de *carry* foi setado para 1 após a execução da instrução de montador NEG BX.

- 59 Imediatamente antes do término da sessão, o registrador AX, de 16 *bits*, continha um valor considerado negativo na notação de complemento a dois.
- 60 A seqüência de *bits* 10001001 (binário) é utilizada para representar o código de operador (*opcode*) da instrução MOV.
- 61 Todos os registradores da CPU, no total de 13, são apresentados por meio do aplicativo de *debug*.
- 62 O programa *debug* pode ser usado para invocação de sub-rotinas básicas de entrada e saída de dados, como gravação de blocos de *bytes* em setores de disco.

RASCUNHO

```

#include<stdio.h>
struct stack {
    int top;
    char item[10];
};
int isfull(struct stack *ps) {
    if(ps->top==9) { return(1); }
    else { return(0); }
}
int isempty(struct stack *ps) {
    if(ps->top==-1) { return(1); }
    else { return(0); }
}
void push(struct stack *ps,char a) {
    ps->top++;
    ps->item[ps->top]=a;
}
void pop(struct stack *ps) {
    ps->top--;
}
char peek(struct stack *ps) {
    return ps->item[ps->top];
}
void display(struct stack *ps)
{
    int i;
    printf("\nthe stack contains:\n");
    for (i=ps->top;!--1;--i) {
        printf("%c",ps->item[i]);
    }
}
void main() {
    struct stack s;
    s.top = -1;
    push(&s,65);
    printf("%c\n",peek(&s));
    printf("%d\n",isfull(&s));
    printf("%d\n",isempty(&s));
    display(&s);
    pop(&s);
    printf("%d\n",isfull(&s));
    printf("%d\n",isempty(&s));
}

```

```

class Stack {
    private final int MAX = 100;
    private Etr top = null;
    private int size = 0;
    public Stack () { }
    public void push (Object element) {
        Etr Etr = new Etr (element, top);
        top = Etr;
        size++;
    }
    public Object pop () {
        Etr entry = top;
        top = top.getN();
        size--;
        return entry.getE();
    }
    public Object peek () {
        return top.getE();
    }
    public boolean empty () {
        return top == null;
    }
    public boolean full () {
        return size == MAX;
    }
}
class Etr {
    private Object e;
    private Etr n;
    public Etr (Object e_, Etr n_) {
        this.e = e_;
        this.n = n_;
    }
    public Object getE() {
        return e;
    }
    public Etr getN() {
        return n;
    }
    public void setN(Etr newN){
        n = newN;
    }
}
public class Main {
    public static void main(String[] args) {
        Stack s = new Stack();
        s.push("A");
        System.out.println(s.peek());
        System.out.println(s.full());
        System.out.println(s.empty());
        s.pop();
        System.out.println(s.full());
        System.out.println(s.empty());
    }
}

```

A tabela acima mostra os códigos de dois programas, escritos nas linguagens C e Java, que realizam implementações de uma estrutura de dados do tipo pilha (*stack*). Considerando as características desses programas e das linguagens nas quais eles foram escritos, julgue os itens de 63 a 73 a seguir.

- 63 Ambas implementações aplicam a técnica de *design* chamada *information hiding*.
- 64 No programa em linguagem C, os valores booleanos são internamente armazenados como inteiros de valor 0 e 1, correspondentes a verdadeiro e falso, respectivamente. O mesmo ocorre na linguagem Java.
- 65 Diferentemente da implementação em C, a implementação de *stack* em Java é capaz de armazenar diretamente valores de qualquer tipo, como objetos, inteiros (int) e caracteres (char) primitivos.
- 66 A implementação do *stack* em C declara 8 funções em uma única unidade de compilação, enquanto a implementação em Java declara 8 métodos de instância, 2 construtores e um método estático em 3 classes diferentes.
- 67 Para cada execução dos métodos *push(struct stack *,char)* em C ou *push(Object)* em Java, é feita uma alocação de memória para armazenar um novo objeto.
- 68 As duas implementações do método *push* não tratam adequadamente do estouro do limite de armazenamento que é predefinido em *stack* (em C) e *Stack* (em Java).

- 69 O espaço de memória alocado por um *stack*, como implementado em C, é fixo, enquanto o espaço de memória alocado pelo *stack*, como implementado em Java, cresce ou reduz dinamicamente à medida que as operações são realizadas.
- 70 A classe *Etr* no código em Java pode ser reutilizada na implementação de uma lista dinâmica com encadeamento simples.
- 71 Se o compilador usado para gerar o executável do programa em C é um compilador de 16 *bits*, então pelo menos 12 *bytes* são alocados no *frame* de invocação do método *main*, para armazenar a estrutura *stack*.
- 72 A implementação em C apresenta uma maior capacidade de reutilização, relativa à implementação em Java.
- 73 O uso de métodos construtores em Java permite a declaração de blocos de código para inicialização automática dos valores das variáveis de um objeto alocado, algo que não pode ser feito em C quando se usa apenas a declaração de estruturas (*struct*).

	composto		lista	lista	lista				
código médico	nome médico	idade médico	código especialidade	nome especialidade	experiência especialidade	número logradouro residência	cidade residência	UF	CEP
21	Maria Quitéria	32	113	clínica geral	3	rua X, 52	Brasília	DF	01.001-001
35	Joaquim Xavier	55	113	clínica geral	5	rua Y, 44	Rio de Janeiro	RJ	02.002-002
			179	obstetrícia	1				
			204	pediatria	6				
50	Carlos Gomes	40	179	obstetrícia	2	rua Z, 44	Salvador	BA	03.003-003
77	Tomé Souza	52	148	oftalmologia	3	rua W, 60	Rio de Janeiro	RJ	04.004-004
			179	obstetrícia	6				

Internet: <http://www2.bus.orst.edu/faculty/brownc/lectures/db_tutor/Normal_Forms.htm> (com adaptações).

Na tabela acima, encontra-se um conjunto de informações tabuladas relativas a médicos, suas especialidades, grau de experiência no exercício destas especialidades e endereço residencial. As colunas “código especialidade”, “nome especialidade” e “experiência especialidade” possuem múltiplos valores para um mesmo médico, enquanto a coluna “nome médico” é composta por nome e sobrenome. Tendo em vista os conceitos do modelo relacional e as informações tabuladas, julgue os itens subseqüentes.

- 74 Para que seja criado um modelo relacional normalizado para as informações acima, na primeira forma normal, é suficiente o uso de apenas uma tabela com sete tuplas, o que vai gerar uma maior redundância de informações.
- 75 Um modelo relacional normalizado para as informações acima, na terceira forma normal, conterà pelo menos cinco tabelas.
- 76 A tabela que contém código, nome e idade dos médicos, em um modelo na terceira forma normal, possuirá pelo menos duas chaves estrangeiras.

Julgue os itens seguintes, relativos à linguagem SQL e ao modelo relacional.

- 77 A linguagem SQL permite conceitualmente o uso de operadores de seleção, projeção, união, interseção, diferença entre conjuntos, sincronização, produto cartesiano e junção, que estão presentes no modelo relacional.
- 78 A linguagem SQL padrão apresenta comandos de DDL e DML, entre os quais destacam-se INSERT e CREATE como comandos DDL e SELECT e JOIN como comandos DML.

RASCUNHO

Diversas tecnologias e topologias são empregadas na construção de redes de comunicação, permitindo flexibilidade e robustez na transmissão das informações. Acerca das principais técnicas de comunicação usadas em redes, julgue os itens que se seguem.

- 79** Topologias de rede em anel foram muito usadas na década de 80 do século passado, quando foram definidos os padrões Token Ring (IEEE 802.5) e FDDI (ANSI X3T9.5 e ANSI X3T12). Entretanto, a adoção desse tipo de topologia em redes de comunicação de dados vem sendo abandonada nos últimos anos, pois os padrões citados estão sendo descontinuados pelos fabricantes de equipamentos.
- 80** Em redes de comutação de pacotes não há qualquer tipo de modulação do sinal transmitido, uma vez que toda a comunicação ocorre digitalmente.
- 81** A provisão de qualidade de serviço ocorre de maneira diferenciada para redes por comutação de circuitos e por comutação de pacotes. Em redes por comutação de circuitos, a qualidade do serviço é implicitamente garantida pela própria natureza do serviço de comutação, que reserva e garante o uso dos recursos de comunicação alocados em cada circuito. No caso da comutação por pacotes, a reserva de recursos deve ser explicitamente realizada para cada sessão ou circuito virtual. Assim, não se pratica a especificação de SLA (*service level agreement*) para serviços de redes comutadas por circuitos. Entretanto, SLA precisos devem ser especificados para a provisão de serviços de rede por comutação de pacotes com QoS.

```
(linha de comando: [localhost]#tcpdump -i eth0 -n -nn -v -e > teste)
pacote 1 01:35:09.352730 0:22:35:71:98:2d ff:ff:ff:ff:ff:ff 0806 42:
arp who-has 10.0.0.5 (ff:ff:ff:ff:ff:ff) tell 10.0.0.207
pacote 2 01:35:09.356743 0:62:94:19:57:4a 0:22:35:71:98:2d 0806 60:
arp reply 10.0.0.5 is-at 0:62:94:19:57:4a
pacote 3 01:35:12.721002 0:22:da:8e:a2:23 1:80:c2:0:0:0 0026 60:
802.1d config 8000.00:22:da:6e:ad:e0.8022 root
8000.00:22:da:6e:ad:e0 pathcost 0 age 0 max 20 hello 10
fdelay 15
pacote 4 01:35:19.905572 0:22:35:71:98:2d 0:80:5f:31:d9:7c 0800 74:
10.0.0.207.32769 > 10.0.0.254.53: [udp sum ok] 14021+ A?
www.google.com. (32) (DF) (ttl 64, id 0, len 60)
pacote 5 01:35:20.161082 0:80:5f:31:d9:7c 0:22:35:71:98:2d 0800 406:
10.0.0.254.53 > 10.0.0.207.32769: 14021 2/11/4
www.google.com. CNAME[|domain] (DF) (ttl 63, id 0, len 392)
pacote 6 01:35:22.722020 0:22:da:8e:a2:23 1:80:c2:0:0:0 0026 60:
802.1d config 8000.00:22:da:6e:ad:e0.8022 root
8000.00:22:da:6e:ad:e0 pathcost 0 age 0 max 20 hello 10
fdelay 15
pacote 7 01:35:24.901985 0:22:35:71:98:2d 0:80:5f:31:d9:7c 0806 42:
arp who-has 10.0.0.1 tell 10.0.0.207
pacote 8 01:35:24.902360 0:80:5f:31:d9:7c 0:22:35:71:98:2d 0806 64:
arp reply 10.0.0.1 is-at 0:80:5f:31:d9:7c
pacote 9 01:35:27.694535 0:22:35:71:98:2d 0:80:5f:31:d9:7c 0800 624:
10.0.0.207.33056 > 64.233.171.104.80: P
1475455923:1475456493(570) ack 1188980042 win 8034 (DF)
(ttl 64, id 62171, len 610)
```

O quadro acima apresenta um conjunto de pacotes capturados pelo analisador de protocolo (*sniffer*) tcpdump, executado em um *host* pertencente a uma rede de comunicação que utiliza TCP/IP e possui uma única interface de rede com endereço IP 10.0.0.207. Com base nessas informações e admitindo que todos os números de porta e serviços TCP/IP utilizados correspondem aos números notórios (*well-known*) definidos pelo IANA, julgue os itens a seguir.

- 82** Nos pacotes acima listados, há mensagens de apenas um dos seguintes protocolos: ARP, DNS, http ou IEEE 802.11d (*spanning tree*).
- 83** Nos pacotes de 1 a 9 acima, são usados, alternativamente, os protocolos de transporte UDP ou TCP.
- 84** O *host* 10.0.0.207 encaminhou o pacote 9 através do *host*/roteador com endereço IP 10.0.0.1. Entretanto, este não era o destinatário final do pacote.
- 85** O *host* 10.0.0.254 é provavelmente um servidor de DNS.

característica	comutador 1	comutador 2	comutador 3
interfaces suportadas	Gigabit Ethernet, 10Gigabit Ethernet, Fast-Ethernet, ATM	Gigabit Ethernet, 10Gigabit Ethernet, Fast-Ethernet, FDDI, Frame-Relay	Gigabit Ethernet, 10Gigabit Ethernet, Fast-Ethernet
capacidade de comutação	384 Gbps	256 Gbps	128 Gbps
capacidade de roteamento	96 Mpps	256 Mpps	80 Mpps
<i>spanning tree</i> (802.1d)	sim	sim	sim
suporte a VLAN (802.1q)	sim	sim	sim
<i>rapid spanning tree</i> (802.1w)	sim	sim	sim
agregação de portas (802.3ad)	sim	sim	sim
suporte a MPLS	sim	sim	-
IGMP <i>snooping</i>	sim	sim	sim
controle de <i>broadcast e multicast</i>	sim	sim	sim
protocolos de roteamento	RIP/RIP2/OSPF2/BGP4	RIP/RIP2/OSPF2/IS-IS/BGP4	RIP/RIP2/OSPF2/BGP4
redundância de <i>default gateway</i> (VRRP/HSRP)	sim	sim	sim
roteamento <i>multicast</i>	PIM/DVMRP	PIM/DVMRP	PIM/DVMRP
filtragem de pacotes	sim	sim	sim
<i>diffserv</i> (QoS)	sim	sim	sim
IEEE802.1p (QoS)	sim	sim	sim
autenticação (802.1x)	sim	sim	sim
autenticação administradores (TACACS)	sim	sim	sim
gerenciamento (RMON 1 e 2)	sim (4 grps.)	sim (4 grps.)	sim (7 grps.)

A tabela acima apresenta um comparativo de especificação entre três modelos de comutador (*core*) para uso em uma rede corporativa. Com base nessa especificação, julgue os itens a seguir, relativos a esses comutadores.

- 86 O comutador 3 é o único que utiliza apenas interfaces da família Ethernet. Assim, este comutador possui um único *backplane* para comutação por pacotes. Os comutadores 1 e 2, por suportarem outras tecnologias, devem possuir um *backplane* para comutação por pacotes e um *backplane* para comutação por células.
- 87 O comutador 1 apresenta o melhor desempenho na operação como *bridge*, mas o comutador 2 é o que tem o melhor desempenho de roteamento.
- 88 Todos os comutadores podem ser considerados como de camada 3.

Existe uma coexistência cada vez mais proeminente de sistemas operacionais distintos nas plataformas computacionais dos ambientes corporativos, dos quais o Windows 2000 e o Linux são representantes importantes. Acerca dos mecanismos para administração e auditoria dos sistemas operacionais Windows 2000 e Linux, julgue os seguintes itens.

- 89 O sistema de *log* do Windows 2000 possui uma interface gráfica denominada visualizador de eventos. Do mesmo modo, o Linux possui uma interface gráfica para o seu sistema de *log*, denominada *syslog*.
- 90 A configuração de sistemas Windows 2000 é controlada por um único arquivo de registro, que pode ser acessado e modificado por meio do aplicativo editor do registro (regedit). Entretanto, esse aplicativo está disponível apenas no modo somente leitura a usuários sem privilégios administrativos, que não podem realizar alterações no registro que comprometam o funcionamento do sistema.
- 91 A configuração de sistemas Linux é, em grande parte, realizada mediante arquivos de configuração localizados tipicamente no caminho */etc/* ou em subdiretórios desse caminho. Para controlar o acesso, utilizam-se as permissões do sistema de arquivos. Assim, para uma permissão anotada como *drwxr-xr-x* para */etc/*, em que o proprietário do diretório é o usuário *root*, apenas este usuário pode criar novos arquivos nesse caminho, sendo que os demais usuários do sistema podem navegar por esse diretório e, eventualmente, modificar alguns arquivos aí existentes, desde que autorizados pelas permissões associadas aos arquivos modificados.

- 92 Os *logs* em sistemas Windows 2000 são divididos em 3 categorias: *log* de sistema (gerado pelo sistema operacional), *log* de segurança (gerado pelo sistema de auditoria configurável) e *log* de aplicativos (gerado pelos aplicativos em execução).

Acerca das principais diferenças e semelhanças existentes entre os sistemas operacionais de gerenciamento de memória e de arquivo das famílias Windows 2000 e Linux, julgue os itens que se seguem.

- 93 A memória virtual no Windows 2000 tem tamanho variável, pois é alocada em um arquivo que pode ter seu tamanho aumentado ou diminuído dinamicamente. No entanto, no Linux, a memória virtual tem tamanho fixo, já que é alocada em uma partição do disco rígido especialmente formatada para essa finalidade.
- 94 O controle de acesso a arquivos e diretórios em partições NTFS utiliza uma estrutura de objetos que possibilita atribuições de níveis complexos de permissão a cada arquivo ou parte da árvore de arquivos no sistema. Já o controle de acesso a arquivos e diretórios em partições EXT2 e EXT3 utiliza uma estrutura hierárquica, na qual, para cada objeto, apenas três níveis de permissões podem ser atribuídos: usuário proprietário, grupo e todos os usuários.

- 95 Recursos em uma partição NTFS têm atributos associados às permissões de compartilhamento, para uso em compartilhamento de arquivos por meio dos serviços de compartilhamento proprietários do Windows®. EXT2 e EXT3 também possuem um serviço de compartilhamento nativo baseado em NFS e denominado samba.
- 96 Como os sistemas Linux e Windows 2000 possuem uma arquitetura de *microkernel*, o gerenciamento de memória em ambos os sistemas reside fora do *kernel*, nas formas de um subsistema do executivo, no caso do Windows 2000, e de um serviço que executa em modo privilegiado, no caso do Linux.
- 97 O tamanho das páginas de memória em Linux e em Windows 2000 independe da plataforma de processamento para a qual o sistema foi compilado. Desse modo, por motivos de ajuste fino de desempenho, os dois sistemas operacionais utilizam páginas de tamanhos diferentes, sendo as páginas do Windows maiores que as páginas usadas no Linux.

Considere um sistema Linux típico, no qual as configurações e os *scripts* de iniciação estejam localizados em um diretório */etc/rc.d/* (iniciação no estilo Unix System V). Acerca desse tipo de iniciação, julgue os itens subseqüentes.

- 98 A iniciação pode ser realizada nos níveis de execução (*runlevel*), entre os quais o *runlevel* 0 e o *runlevel* 6 caracterizam-se por serem monousuários, utilizados para a manutenção do sistema.
- 99 Em algumas distribuições, dentro do diretório */etc/rc.d/* são encontrados os diretórios *rc.sysinit* e *init.d*. No primeiro, são disponibilizados *scripts* executados durante a iniciação do sistema. No segundo, há *scripts* para iniciação de serviços do sistema, tais como o gerenciador *pcmcia* e o servidor *http*. Estes *scripts* podem ser executados mesmo depois de o sistema estar completamente iniciado, sob demanda de um usuário com privilégios suficientes.
- 100 Uma vez iniciado em um *runlevel*, o sistema não pode mudar de *runlevel* enquanto estiver no ar (*on-the-fly*), podendo fazê-lo apenas após reiniciação completa do sistema e nova recarga do *kernel* na memória.

As redes de computadores são ferramentas importantes para viabilizar a interconexão entre diversos computadores, posicionados em um mesmo local ou geograficamente distribuídos. Tendo em vista que essas redes, em grande parte, utilizam meios de transmissão pouco seguros para o tráfego de dados, há a necessidade de que sejam fornecidos mecanismos lógicos de segurança a fim de evitar ou diminuir os perigos aos quais essas transmissões de dados estão submetidas. Acerca da segurança fornecida em ambientes de redes, julgue os itens a seguir.

- 101 O protocolo IKE (*Internet key exchange*), método padrão para utilização no IPSec, trabalha com o objetivo de ser um protocolo geral de troca de chaves e é executado na camada de aplicação da arquitetura TCP/IP.
- 102 O PGP (*pretty good privacy*) é um sistema de segurança utilizado na transmissão de mensagens eletrônicas (correio eletrônico). Sua versão mais atual oferece suporte a vários algoritmos criptográficos, simétricos e assimétricos, tais como o AES, o 3-DES e o RSA, que trabalham em conjunto e permitem que, em uma mesma transmissão, sejam fornecidos serviços de confidencialidade, autenticação e integridade de dados.

- 103 Uma das desvantagens de uma rede sem fio em relação a uma rede com fio é a utilização de um meio menos seguro e menos controlável para a transmissão de dados, requerendo a implementação de protocolos de segurança mais sofisticados. Entre esses protocolos, um dos mais utilizados atualmente é o WEP (*wired equivalent protocol*), que utiliza o AES como algoritmo simétrico para a transmissão de dados criptografados.
- 104 Entre os diversos equipamentos que podem ser utilizados para aumentar o nível de segurança de uma rede de computadores corporativa, os *firewalls* exercem um papel fundamental. Para que sua ação possa ser eficaz, eles devem ser instalados entre a rede interna da organização e as redes do mundo externo e têm por objetivo filtrar o conteúdo que chega até a rede interna impedindo que ataques conhecidos sejam realizados.
- 105 Um dos mais conhecidos ataques a um computador conectado a uma rede é o de negação de serviço (DoS – *denial of service*), que ocorre quando um determinado recurso torna-se indisponível devido à ação de um agente que tem por finalidade, em muitos casos, diminuir a capacidade de processamento ou de armazenagem de dados.
- 106 Um IDS (*intrusion detection system*) ou sistema de detecção de intrusão pode estar fundamentado em computador (IDS de *host*) ou em rede de computadores (IDS de rede). Em ambos os casos, esse sistema procura por ataques que ainda não estejam registrados e catalogados, deixando os problemas conhecidos para serem solucionados por outros mecanismos de segurança, tais como *firewalls*.

Nos últimos anos, a segurança da informação vem se tornando área de importância crescente para entidades tais como empresas, universidades e órgãos governamentais, levando à necessidade de tais entidades dedicarem atenção aos processos de definição, implantação e gestão de políticas de segurança da informação. Acerca de segurança da informação, julgue os itens seguintes.

- 107 Segurança da informação é caracterizada, basicamente, pelo fornecimento de três serviços de segurança: a preservação do sigilo ou da confidencialidade das informações, a garantia da integridade dos dados e a manutenção da disponibilidade.
- 108 A avaliação de um risco é a consideração sistemática da probabilidade de uma falha de segurança ocorrer à luz das ameaças e vulnerabilidades mais freqüentes e nos controles atualmente implementados.
- 109 Em relação à segurança física e do ambiente de uma organização, a definição de áreas de segurança contribui para prevenir o acesso não-autorizado, o dano e a interferência nas informações e instalações físicas da organização.
- 110 O objetivo da gestão de continuidade do negócio de uma organização deve ser impedir que ocorra a interrupção das atividades ligadas ao negócio e proteger os processos críticos da organização contra efeitos danosos causados por falhas ou até mesmo desastres significativos.

O emprego sistemático de diversas técnicas de segurança da informação resolve, ou pelo menos atenua, boa parte das vulnerabilidades existentes nesse contexto. Entre as técnicas mais efetivas utilizadas para fornecer segurança da informação, incluem-se a criptografia, a esteganografia e as funções *hash*. A respeito de tais técnicas e do seu emprego adequado, julgue os itens de 111 a 117 a seguir.

- 111** Em um processo de assinatura digital, comumente é gerado um valor condensado (*hash*) do documento que se deseja assinar e, após isso, esse valor é criptografado utilizando-se chave privada (assimétrica) que somente as partes envolvidas na comunicação desse documento devem conhecer. Dessa forma, ao enviar o documento original e o respectivo valor condensado criptografado, o destinatário poderá validar a assinatura do documento e verificar a sua integridade.
- 112** O algoritmo DES (*data encryption standard*) efetua exatamente as mesmas operações durante o processo de cifração e o de decifração. A única diferença percebida entre os dois processos está na ordem de aplicação das chaves parciais (chaves de *round*).
- 113** O AES (*advanced encryption standard*) surgiu com o objetivo de substituir o DES. Um dos principais motivos dessa necessidade de modificação de padrões está no fato de o tamanho do espaço de chaves utilizadas pelo DES (2^{64} possíveis chaves) não ser grande o suficiente, atualmente, para garantir proteção contra ataques do tipo busca por exaustão. O AES, com suas chaves de, no mínimo, 112 *bits*, aumentou tremendamente a resistência a esse tipo de ataque.

114 O algoritmo de criptografia assimétrica RSA (Rivest, Shamir e Adleman) tem sua segurança fundamentada na dificuldade de se fatorar números inteiros muito grandes. Além de ser utilizado para criptografar mensagens a serem enviadas por canais inseguros de comunicação, o RSA também pode ser aplicado na criptografia de chaves simétricas que são utilizadas na criptografia simétrica de mensagens.

115 Para a utilização do modo de operação CBC (*cipher block chaining mode*), é necessário que seja criado o que se denomina vetor de inicialização (*initialization vector*), que evita que mensagens que comecem idênticas gerem criptogramas com começos idênticos. Um inconveniente desse modo de operação reside na questão da propagação de erros, pois, caso haja um *bit* errado em um bloco de criptograma a ser decifrado, todos os blocos a partir dali serão decifrados de forma errada.

116 A esteganografia pode ser utilizada com o objetivo de disfarçar a existência de determinadas informações. Atualmente, a esteganografia utiliza o BMS (*bit* mais significativo) para embutir informações, o que degrada, contudo, a informação hospedeira, pois modifica seu conteúdo.

117 Entre os algoritmos especificados pelo padrão SHS (*secure hash signature standard*), o SHA-1 é o que possui menor tamanho do valor condensado (*message digest*), que é de 160 *bits*.

```
03:17:13.913622 host1.org.23 > host2.org.23: ack 499410217 win 1028 (ttl 30, id 39426)
03:17:13.915481 host2.org.23 > host1.org.23:R 499410217:499410217(0) win 0 (ttl 254, id 34512)
03:17:13.954076 host1.org.23 > host3.org.23: ack 499410217 win 1028 (ttl 0, id 39426)
03:17:13.955461 host3.org.23 > host1.org.23:R 499410217:499410217(0) win 0 (ttl 254, id 5962)
03:17:13.982753 host1.org.143 > host2.org.143: ack 499410217 win 1028 (ttl 30, id 39426)
03:17:13.983904 host2.org.143 > host1.org.143:R 499410217:499410217(0) win 0 (ttl 254, id 34514)
03:17:14.061121 host1.org.143 > host3.org.143: ack 499410217 win 1028 (ttl 30, id 39426)
03:17:14.064069 host3.org.143 > host1.org.143:R 499410217:499410217(0) win 0 (ttl 254, id 5967)
03:17:19.161874 host1.org.1146 > host3.org.23:S 2585837477:2585837477(0) win 16324 <mss 1484,sackOK,timestamp 50637 0,nop,wscale 0 > (DF) (ttl 52, id 770)
03:17:19.170887 host1.org.1147 > host3.org.143:S 2585589580:2585589580(0) win 16324 < mss 1484,sackOK,timestamp 50637 0,nop,wscale 0 > (DF) (ttl 52, id 771)
```

Considerando o extrato de um arquivo de *log* apresentado acima, julgue os itens subsequentes.

- 118** O extrato apresentado indica ocorrência de ataque, partindo da máquina *host1.org* e sendo direcionado para as máquinas *host2.org* e *host3.org*.
- 119** As portas TCP de números 23 (*telnet*) e 143 (*imap*) são alvos de varredura.
- 120** As portas de onde partem os pacotes são diferentes das portas-alvo; isso pode ter o objetivo de mascarar parcialmente o ataque, protegendo-o em relação a certos sistemas de detecção de intrusão.

PROVA DISCURSIVA

- Nesta prova — que vale **cinco** pontos —, faça o que se pede, usando a página correspondente do presente caderno para rascunho. Em seguida, transcreva o texto para a folha de **TEXTO DEFINITIVO**, nos locais apropriados, pois **não serão avaliados fragmentos de texto escritos em locais indevidos**.
- Qualquer fragmento de texto além da extensão máxima de **trinta** linhas será desconsiderado.

ATENÇÃO! Na folha de **texto definitivo**, identifique-se apenas no cabeçalho, pois **não será avaliado** texto que tenha qualquer assinatura ou marca identificadora fora do local apropriado.

As portas foram abertas e as invasões, os roubos e as agressões diminuíram. Pelo menos em educação, essa afirmação não soa contraditória. Números do governo do estado de São Paulo mostram que um programa que permite a utilização das escolas aos fins de semana pela comunidade fez cair os índices de violência.

As mais significativas reduções foram registradas nos meses de janeiro e fevereiro, período das férias escolares. Este ano, mesmo nessa época, havia atividades nos fins de semana em escolas estaduais. A diminuição nos casos de violência foi de 56% e de 33%, em cada mês. "Uma escola com pouco diálogo com a comunidade vira um símbolo de dominação. As depredações e invasões muitas vezes são motivadas por essa rejeição", diz a educadora da Universidade de São Paulo, Sílvia Colello.

Internet: <<http://www.jcsol.com.br>> (com adaptações).

Os aterradores números da violência no Rio entre 1983 e 1994, em pesquisa do ISER, são apontados como sendo resultantes de diversos fatores, tais como as perdas econômicas da década de 80, o agravamento das diferenças sociais no ambiente urbano (com a expansão das favelas), a crise dos serviços públicos e o início do aumento da população jovem que forma, justamente, o grupo mais exposto aos riscos da violência.

No entanto, houve uma queda de 35% nos últimos 6 anos. A partir da segunda metade dos anos noventa, a taxa de homicídios por 100.000 habitantes declina ininterruptamente.

A pesquisa aponta, entre os fatores importantes que contribuíram na diminuição dessa taxa: o surgimento de movimentos sociais pró-ativos, de grande escala, como a Campanha contra a Fome e o Viva Rio, que mobilizaram a cidade para o enfrentamento dos seus problemas; a multiplicação de projetos sociais nos bairros pobres, por ações governamentais e não-governamentais, sobretudo para crianças e jovens, na área educacional; e a organização das comunidades por meio de associações de moradores, ONGs, entidades religiosas, beneficentes, culturais e recreativas.

Internet: <<http://www.fgvsp.br>> (com adaptações).

Considerando que as idéias apresentadas nos textos acima têm caráter unicamente motivador, redija um texto dissertativo, posicionando-se acerca do tema a seguir.

O FORTALECIMENTO DAS REDES DE RELAÇÕES SOCIAIS COMO FORMA DE REDUÇÃO DA VIOLÊNCIA URBANA

RASCUNHO

1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	
21	
22	
23	
24	
25	
26	
27	
28	
29	
30	

