

**CARGO:****ANALISTA DE TECNOLOGIA DA INFORMAÇÃO – ATIVIDADE TELEMÁTICA**  
**PERFIL II – INFRA-ESTRUTURA TECNOLÓGICA**

Nas questões de 1 a 40, marque, de acordo com o comando de cada uma delas: itens **CERTOS** na coluna **C**; itens **ERRADOS** na coluna **E**. Na Folha de Respostas, a marcação na coluna **SR** é facultativa e não contará para efeito de avaliação; servirá somente para caracterizar que o candidato desconhece a resposta correta. Use a Folha de Rascunho para as devidas marcações e, posteriormente, a **Folha de Respostas**.

**LÍNGUA PORTUGUESA****Texto LP-I – questões de 1 a 3**

1 O primeiro sistema previdenciário do país, criado em 1923, na forma de caixa para os ferroviários, estipulava a draconiana idade mínima de 50 anos para aposentadoria. Só na segunda metade da década de 50 o homem brasileiro atingiria essa expectativa de vida. Ao reordenar o sistema em institutos nacionais, nos anos 30, o presidente Getúlio Vargas manteve a idade mínima. Em 1960, ela foi elevada para 55 anos. Os funcionários públicos, porém, não estavam sujeitos a essa regra. Alegando que a situação era injusta, o Congresso aboliu a idade mínima, em 1962, sem realizar estudo algum sobre o impacto que essa decisão teria nem criar provisões. Desde então, não houve mais idade mínima, até dezembro de 1998.

7 A mesma lei de 1923 também estipulava que, para receber os benefícios, era necessário pagar contribuições ao longo da vida. O sistema apresentava falhas de cálculo atuarial, mas, pelo menos, estava calçado no chamado caráter contributivo. Foi a partir dos anos 60 que mudanças na legislação intensificaram a ruptura na relação entre contribuições e benefícios.

10 Várias categorias passaram a ser incorporadas ao sistema, sem contrapartida de contribuições. A aposentadoria por velhice, concedida aos homens aos 65 anos e às mulheres aos 60, exigia apenas cinco anos de contribuição. Segundo levantamento do ministério, do total de aposentadorias por velhice até 1983, 71% foram concedidas a mulheres inscritas como “domésticas” ou vinculadas a empresas de parentes só para usufruir do benefício. O regime dos autônomos e as aposentadorias especiais por “esforço de guerra” durante a 2.ª Guerra Mundial foram outras formas de drenar a receita.

16 Em 1963, os trabalhadores rurais foram incorporados ao sistema. A contribuição era de 1% sobre o valor de produtos agropecuários, recolhida pelo produtor quando da primeira comercialização. O benefício era metade do salário mínimo vigente e a aposentadoria era por idade, a partir dos 65 anos. A receita era insuficiente e os benefícios rurais foram mantidos com as contribuições dos trabalhadores urbanos.

19 Os trabalhadores temporários das empresas foram incorporados ao sistema em 1974. Os maiores de 70 anos e os inválidos que não tinham cobertura previdenciária passaram a ter direito a renda mensal vitalícia, independentemente de contribuição. Em vez de o Tesouro bancar a assistência, foram usados recursos das contribuições.

22 A Constituição da República de 1988 aumentou o desequilíbrio no setor rural. O salário mínimo passou a ser piso previdenciário e a idade para aposentadoria foi diminuída para 60 anos para homens e 55 para mulheres. A despesa triplicou. A alíquota do tributo sobre os produtos agropecuários passou para 2%, mas não aliviou o déficit. Em 1997, as contribuições representaram 13,9% dos benefícios rurais.

28 Os segurados foram temporariamente dispensados do recolhimento de contribuições e foram facilitadas as formas de comprovação de trabalho rural. Ser filho de fazendeiro passou a ser suficiente para somar tempo de trabalho rural, que depois foi computado para obter aposentadorias mais precoces por tempo de serviço no setor urbano ou nos regimes especiais do serviço público, com benefícios altos e contribuição pequena.

31 A extensão da aposentadoria integral ao meio milhão de celetistas que trabalhavam para o serviço público e a devolução das contribuições que eles tinham pago a fundos de pensão completam o conjunto de generosidades da nova Constituição. Seguindo a tradição brasileira, não foram feitos cálculos do impacto nem provisões de receita.

O Estado de S. Paulo, 1.º/11/1999 (com adaptações).

**QUESTÃO 1**

Em relação às idéias do texto LP-I, julgue os itens a seguir.

- 1 A ausência de cálculos de impacto e a falta de provisões financeiras para a concessão de benefícios têm sido fatores pouco relevantes para o sistema previdenciário.
- 2 Na década iniciada em 1941, a expectativa de vida do brasileiro era de mais de 50 anos.
- 3 Um dos aspectos favoráveis do sistema previdenciário estabelecido em 1923 era sua base de caráter contributivo.
- 4 O sistema previdenciário, desde que foi instituído, tem preservado em sua estrutura o equilíbrio entre o tempo de contribuição e o direito ao benefício previdenciário.
- 5 Com a incorporação dos trabalhadores rurais ao sistema previdenciário, em 1963, procurou-se, pela primeira vez, assegurar que a arrecadação não fosse inferior aos benefícios pagos.

## QUESTÃO 2

Com referência aos elementos constitutivos do texto LP-I e à sua organização, julgue os itens abaixo.

- 1 A palavra “draconiana” (R.1) está associada à idéia de **generosa**.
- 2 O texto organiza as informações agrupando-as e colocando-as de forma que o aspecto cronológico das transformações focalizadas constitua sua matriz estrutural.
- 3 Uma das estratégias para ocultar os agentes das ações apresentadas no texto é o uso das estruturas da voz passiva.
- 4 A preferência pelo discurso estruturado com base na terceira pessoa do singular é uma forma de dar espaço à subjetividade e à posição pessoal do autor.
- 5 Na expressão “conjunto de generosidades” (R.31), há ironia que demonstra que o texto adota um ponto de vista oposto à linha das decisões políticas acerca do sistema previdenciário.

## QUESTÃO 3

Acerca dos elementos do texto LP-I e da sua estrutura, julgue os itens seguintes.

- 1 Em lugar do trecho “a mulheres (...) empresas” (R.12-13), estaria igualmente correta a seguinte estrutura: **às mulheres inscritas como “domésticas” ou vinculadas às empresas**.
- 2 A expressão “drenar a receita” (R.14), empregada no texto em sentido conotativo, está associada à idéia de **consumir os recursos arrecadados**.
- 3 Nas linhas 15 e 19, a expressão “foram incorporados” equivale gramaticalmente a **incorporavam-se**.
- 4 Em “aumentou o desequilíbrio no setor rural” (R.22), a palavra “desequilíbrio” diz respeito à injustiça social refletida nos baixos salários e na avançada idade para a aposentadoria.
- 5 As informações das linhas de 27 a 29, referentes aos filhos de fazendeiros, constituem argumento favorável às decisões tomadas para o sistema previdenciário rural.

## QUESTÃO 4

No texto abaixo, cada fragmento de texto em negrito corresponde a um item que o segue. Julgue os períodos que contêm esses itens quanto ao respeito às exigências da norma culta.

No resto do mundo, a previdência é entendida como fator de estabilidade social. Se os mais pobres fossem **deixados à própria sorte 1**, só com o que podem poupar ou contribuir para o sistema, não **teriam asseguradas 2** sua sobrevivência na velhice ou invalidez. Por isso, os sistemas nos outros países **pressupõe 3** que as contribuições pagas pelos segurados com maior rendimento **ajudarão a financiar 4** os benefícios pagos aos de renda mais baixa.

No Brasil, é o contrário. As pessoas que recebem os benefícios mais altos são aquelas que **contribuíram 5** com as menores parcelas de seus salários, por menos tempo, e que ficam mais tempo aposentadas. É o que os especialistas chamam de “solidariedade invertida”.

Lourival Sant’anna. O Estado de S. Paulo, 2/11/1999 (com adaptações).

## QUESTÃO 5

- 1 Literalmente, são os que fazem as leis e os que interpretam que recebem os benefícios mais altos: na União, a média de aposentadoria do Poder Legislativo é de 47,4 salários mínimos e a do Poder Judiciário, de 40,5. Nos estados, não há dados públicos consolidados, mas é conhecida a norma segundo a qual quanto mais pobre o estado mais altos os salários na Assembleia Legislativa — que originarão aposentadorias régias e precoces. Em seguida, vêm os benefícios pagos aos aposentados do Poder Executivo. Até 1993, os servidores públicos federais não pagavam contribuições para a aposentadoria. Participavam apenas com 6% para as pensões. A partir daquele ano, foi instituída contribuição de 11% sobre os salários integrais. Já os trabalhadores do setor privado que recebem até três salários mínimos pagam alíquota de 8%, de três a cinco salários mínimos, de 9%, e, na faixa de cinco salários mínimos até o teto de R\$ 1.255,00, de 11%.
- 16 A explicação para a distinção é a de que os servidores se aposentam com salário integral, enquanto os trabalhadores da iniciativa privada estão sujeitos àquele teto.

*Idem, ibidem.*

Quanto às estruturas do texto acima, julgue os itens que se seguem.

- 1 Como recurso de coesão, a expressão “Poder Legislativo” (R.3) substitui a expressão “os que fazem as leis” (R.1) e “Poder Judiciário” (R.4) substitui “os que interpretam” (R.1-2).
- 2 Seria pertinente a substituição da palavra “consolidados” (R.5) por **consistentes** ou **seguros**.
- 3 Na linha 7, o termo “que” pode ser substituído por **cujos**, sem prejuízo para a correção e a coerência do período.
- 4 O período “Já os trabalhadores (...) 9%” (R.12-14) estrutura-se coesivamente com vírgulas que marcam elipses dos trechos “os trabalhadores do setor privado que recebem” e “pagam alíquota de”.
- 5 Na linha 13, a colocação de vírgulas após “privado” e antes de “pagam” manteria inalterado o sentido da informação do período.

## Texto LP-II – questões 6 e 7

1 Embora nessa sua nova ofensiva para reformar a  
previdência do funcionalismo público e criar uma  
contribuição para os inativos o governo tenha ganho o apoio  
4 dos estados e municípios, que acabam de enviar uma “carta”  
ao Poder Legislativo, pedindo regime de urgência nessa  
matéria, o Congresso e o Poder Judiciário já deixaram claro  
7 que, se depender deles, tudo continuará como está. Para os  
parlamentares, que desfrutam da aposentadoria mais rápida do  
país, as medidas são “impopulares”. Para a magistratura,  
10 composta ela própria de funcionários públicos, elas são  
ilegais, pois a Constituição da República veda a cobrança  
retroativa de qualquer tipo de taxa ou imposto. Esses  
13 argumentos, contudo, não resistem um minuto quando  
confrontados com a realidade dos fatos. Na verdade, qualquer  
um que examinar os grandes números do sistema  
16 previdenciário brasileiro chegará, obrigatoriamente, à  
conclusão de que ele é a maior máquina institucionalizada de  
transferência de renda de pobres para ricos e remediados de  
19 que se tem notícia no planeta.

Jornal da Tarde, 13/8/2001 (com adaptações).

### QUESTÃO 6

Considerando a estrutura e as escolhas lexicais do texto LP-II, julgue os itens a seguir.

- 1 O pronome “sua” (R.1) refere-se de forma antecipada a “Poder Legislativo” (R.5).
- 2 A palavra “regime” (R.5) está sendo empregada no sentido de **sistema político que rege o país**.
- 3 A expressão “nessa matéria” (R.5-6) retoma a idéia do trecho “reformar a previdência do funcionalismo público e criar uma contribuição para os inativos” (R.1-3).
- 4 As vírgulas após “parlamentares” (R.8) e “país” (R.9) conferem caráter restritivo à oração por elas isoladas.
- 5 É possível que a palavra “impopulares” (R.9) esteja entre aspas no texto tanto para representar citação quanto para conferir caráter de ironia à informação.

### QUESTÃO 7

Quanto à estrutura e às idéias do texto LP-II, julgue os itens que se seguem.

- 1 A expressão “Esses argumentos” (R.12-13) retoma as idéias de impopularidade e de ilegalidade trazidas ao debate pelos parlamentares e pelos magistrados, respectivamente.
- 2 A conjunção “contudo” (R.13) pode ser substituída por **embora** sem alteração da coerência do texto.
- 3 A expressão “Na verdade” (R.14) reforça a direção argumentativa do texto, que é favorável às reformas do sistema previdenciário.
- 4 A expressão “é a maior máquina institucionalizada” (R.17) pode, sem prejuízo para a coerência do texto, ser substituída por **é o maior mecanismo institucional**.
- 5 Infere-se do texto que os mais beneficiados pelo sistema de previdência não são os mais necessitados.

### QUESTÃO 8

Quanto ao uso dos sinais de pontuação, julgue os itens abaixo.

- 1 Entre 1987 e 1997, a despesa da União com servidores ativos, cresceu 10%. Mas, por causa da explosão do número de inativos, alimentada pelo privilégio das aposentadorias precoces, seus gastos totais com pessoal, aumentaram 45%.
- 2 Com o direito a aposentadorias com salário integral e beneficiados por generosos critérios para a contagem de tempo de serviço, os 925 mil servidores federais, geraram em 1999, uma receita previdenciária de apenas R\$ 2,6 bilhões, o que equivale a menos de 14% do total gasto pela União com o pagamento de seus aposentados.
- 3 A diferença entre as contribuições e as aposentadorias pagas pela União e pelos estados e municípios deverá ficar em R\$ 42 bilhões. A multidão de miseráveis do Brasil será chamada a pagar essa conta.
- 4 Ela equivale a perto de 5% do PIB. Levando-se em conta que o déficit global do setor público é de 7% do PIB, isso mostra que o governo já fez quase tudo o que podia em matéria de corte de gastos em saúde, educação e segurança — suas funções sociais básicas.
- 5 Portanto, se o Poder Legislativo e o Poder Judiciário mais uma vez conseguirem impedir a cobrança da contribuição dos inativos, estarão consolidando um regime de privilégios que não só impede o crescimento da economia, mas também obriga a maioria pobre da sociedade a pagar pelo bem-estar dos marajás do setor público.

Itens adaptados de *Jornal da Tarde*, 13/8/2001.

**QUESTÃO 9**

1 Como aponta o próprio nome, a previdência é uma  
instituição que se preocupa com o futuro. Desde a origem  
histórica, na Alemanha do fim do século XIX, seu objetivo é  
4 assegurar um ganho metódico ao beneficiado e a sua família a  
partir de certa idade, a título de aposentadoria por tempo de  
serviço, ou quando sofrer alguma incapacitação para o trabalho  
7 ou, ainda, como pensão após a morte para o cônjuge e os filhos.  
Existe no mundo todo, em graus variados de sucesso e fracasso.

No Brasil, desde as primeiras caixas e institutos para  
10 ferroviários, industriários, comerciários e bancários, nos anos 20  
e 30, sempre foi um sistema que viveu no limite da indigência,  
sob as asas generosas do Estado ou sob o manto protetor de  
13 associações beneficentes ou ordens religiosas. Nos anos 70 e 80,  
houve a experiência desastrosa dos montepios, instituições de  
previdência privada sem fins lucrativos que drenaram a economia  
16 de inúmeras famílias pelo país afora. Em época de inflação  
galopante, os contratos não previam correção monetária, e os  
planos se revelaram uma gigantesca ratoeira. Quem aparecia para  
19 receber os benefícios prometidos encontrava a seu dispor uma  
ninharia, corroída pela inflação ou pela administração pantanosa.  
Isso quando tinha a sorte de localizar os responsáveis pelas  
22 arapucas, que geralmente desapareciam no mundo com o dinheiro  
das contribuições mensais efetuadas no decorrer de anos por  
legiões de pessoas de boa-fé.

Veja, 1.º/8/2001, p. 109 (com adaptações).

Em relação ao texto acima, julgue os seguintes itens.

- 1 A palavra “metódico” (R.4) está sendo utilizada no sentido de **módico**.
- 2 Na linha 14, caso a expressão “a experiência desastrosa” fosse flexionada no plural, a forma verbal “houve” também teria de ser flexionada no plural, para que não ocorresse transgressão às normas da língua culta.
- 3 Para que o texto estivesse de acordo com as exigências da língua escrita padrão, a forma verbal “drenaram” (R.15) deveria estar no singular para concordar com “a experiência” (R.14).
- 4 As expressões “galopante” (R.17), “ratoeira” (R.18), “pantanosa” (R.20) e “arapucas” (R.22) conferem ao texto um tom de informalidade que é impróprio para correspondências oficiais.
- 5 Na linha 20, a palavra “pantanosa” está sendo utilizada em sentido conotativo, podendo conferir à “administração” as características de **corrupta, incorreta, inadequada, imprópria, insegura**.

**QUESTÃO 10**

Os fragmentos a seguir constituem um texto, mas estão ordenados aleatoriamente.

- I A tendência mais singular, entretanto, está no contingente da previdência aberta, com 3,7 milhões de planos de aposentadoria.
- II A primeira é uma espécie de clube cujos sócios só podem ser os empregados de determinada empresa e reúne 2,3 milhões de adesões atualmente no país.
- III Junta-se a eles mais 1,3 milhão de contribuintes da previdência fechada em empresas privadas de grande porte.
- IV Em meados dos anos 70, gestou-se no Brasil um sistema que corre paralelo ao INSS e tenta copiar experiências que deram certo em países do primeiro mundo. É o da previdência complementar, dividida em duas modalidades: a fechada e a aberta.
- V Aí está 1 milhão de funcionários das empresas estatais e autarquias, cujas contribuições mensais são administradas pelos poderosos fundos de pensão, entre os quais figuram como exemplo o PREVI e o PETROS, dos assalariados do Banco do Brasil e da PETROBRAS, respectivamente.

Itens adaptados de Veja, 1.º/8/2001, p. 109.

Considerando que a organização de um texto pressupõe a ordenação lógica e coerente de seus fragmentos, julgue os itens que se seguem.

- 1 No fragmento V, “Aí está” indica uma articulação com “previdência aberta”, no fragmento I.
- 2 O fragmento IV deve ser a introdução do texto, uma vez que não apresenta referências a elementos anteriores.
- 3 O fragmento II vem imediatamente após o fragmento IV porque se refere ao primeiro elemento da divisão em duas modalidades de previdência complementar neste apresentada.
- 4 No fragmento III, o termo “eles” refere-se à expressão “3,7 milhões”, no fragmento I.
- 5 A ordem correta para os fragmentos do texto seria: V-III-II-I-IV.

# LÍNGUA INGLESA

## Text LI-I – questions 11 to 15

1 The explosive growth of information technology has fueled  
an unprecedented demand for new software. Software is needed to  
support new products, to provide fundamental services on the  
4 Internet, and to solve important national problems. At the same  
time, the resources needed to develop this software have not kept  
pace with the demand, producing what might be called a  
7 “software gap”.

An interaction of factors has caused this software gap:  
accelerated demand for software, increased complexity of systems,  
10 labor-intensity of development, variable quality in the labor pool,  
labor shortages, and lack of adequate science technology to support  
robust development. Since cost-effective improvements in hardware  
13 lead to a strong demand for more software, the demand will  
continue to accelerate. Today’s systems and applications software  
are substantially more complex than in the past. Software systems  
16 are now among the most complex of human-engineered structures.

The situation threatens to inhibit the progress of the current  
boom in information technology and may threaten the health and  
19 welfare of the Nation by reducing the rate at which solutions to  
software-intensive problems, like aviation security and crisis  
management, can be solved. The Federal Government must take  
22 steps to address the situation by investing in research on new  
strategies to improve software development productivity and by  
helping to increase the pool of information technology professionals  
25 capable of developing good software.

The Nation needs robust systems, but the software our  
systems depend on is fragile.

Internet: <<http://www.itrd.gov/ac/interim/section-3.html>>  
Access on August 13, 2001 (adapted).

### QUESTÃO 11

From text LI-I, it can be deduced that

- 1 never before has information technology been so much required.
- 2 new information technology demands new software.
- 3 nowadays software is the most important way of providing new products.
- 4 resources have been provided to bridge the “software gap”.
- 5 some new products lack the corresponding software.

### QUESTÃO 12

According to text LI-I,

- 1 software is basic to Internet services.
- 2 software should keep up with technological information demands.
- 3 the software gap has been caused by the independent action of several factors.
- 4 more than a dozen of reasons contribute to the software gap.
- 5 software systems are becoming more complex.

### QUESTÃO 13

Based on text LI-I, it can be gathered that

- 1 more software requires the lack of suitable technology.
- 2 the more improvement in hardware the more the need for software.
- 3 nowadays software systems are considered highly sophisticated human-engineered structures.
- 4 the “software gap” can contribute to increase the present boom in information technology.
- 5 expanding information technology may be harmful to the nation’s health and welfare.

### QUESTÃO 14

Text LI-I conveys the idea that

- 1 the present boom of information technology is threatening aviation safety.
- 2 the Federal Government has made massive investments on strategies to improve software development.
- 3 professionals are no longer needed to develop good software.
- 4 the Federal Government should take steps to deal with the “software gap”.
- 5 demand for software exceeds the Nation’s ability to produce it.

### QUESTÃO 15

In text LI-I,

- 1 “has fueled” (R.1) means **has decreased**.
- 2 “Today’s systems” (R.14) is the same as **The current systems**.
- 3 “Nation” (R.19) refers to **any nation**.
- 4 “capable of developing” (R.25) is synonymous with **able to develop**.
- 5 “but the software our systems depend on is fragile” (R.26-27) can be correctly replaced by **but the software on which our systems depend is fragile**.

## CONHECIMENTOS ESPECÍFICOS

### QUESTÃO 16

Em computadores, números, caracteres e outros tipos de informação podem ser representados de diversas formas. Nos itens a seguir, considere que o subscrito de um número indica o sistema de numeração em que ele está representado. Assim, 25<sub>DEZ</sub> e 1001<sub>DOIS</sub> são números representados em base dez e em base dois, respectivamente. Com relação aos sistemas de representação de números e caracteres utilizados em computadores, julgue os itens a seguir.

- 1 A representação no sistema binário do número decimal 115<sub>DEZ</sub> é 1110011<sub>DOIS</sub>.
- 2 A representação no sistema octal do número em notação hexadecimal 3A1D<sub>DEZESSEIS</sub> é 35035<sub>OITO</sub>.
- 3 A notação binária em complemento de dois, em 8 *bits*, para o número decimal negativo !23<sub>DEZ</sub> é 11101001<sub>COMPLEMENTO DE DOIS</sub>.
- 4 O formato IEEE 754 para números em ponto flutuante contém informações acerca do sinal, do expoente e da mantissa do número.
- 5 O código ASCII é um código de 16 *bits* que contém os caracteres de praticamente todas as línguas vivas, e o código Unicode é um código de 8 *bits* que é capaz de representar uma quantidade bem menor de caracteres.

**QUESTÃO 17**

Com relação a arquiteturas e a características de computadores, microcomputadores, microprocessadores e seus diferentes componentes, julgue os itens abaixo.

- 1 Todos os tipos de unidade lógica e aritmética realizam apenas as operações básicas de adição binária e de **E** (*and*) lógico *bit* a *bit*. Para se realizar outras operações, como subtração e **OU** (*or*) *bit* a *bit*, é sempre necessário que elas sejam implementadas por *software* a partir de combinações dessas duas operações básicas.
- 2 Os processadores Pentium utilizam uma arquitetura puramente RISC, enquanto os processadores SPARC utilizam uma arquitetura puramente CISC.
- 3 No modelo von Neumann, a unidade de memória pode armazenar tanto instruções como dados.
- 4 Muitos microprocessadores comerciais utilizam um registrador denominado acumulador, que muitas vezes contém um dos operandos de entrada da unidade lógica e aritmética, e que armazena o resultado da operação dessa mesma unidade lógica e aritmética.
- 5 O disco rígido é um exemplo de memória não-volátil embasada em gravação magnética, que apresenta, em geral, um tempo de acesso maior que aquele das memórias RAM estáticas.

**QUESTÃO 18**

Quanto a conceitos relacionados a arquiteturas de computador, julgue os seguintes itens.

- 1 O surgimento das arquiteturas RISC fez a implementação de microprocessadores por meio de microprogramação crescer exponencialmente, pois esse tipo de procedimento é bem mais rápido e eficiente em arquiteturas mais simples que em implementações do tipo *hardwired*. O surgimento das arquiteturas RISC também fez o conjunto de instruções para acesso a memória crescer em número e complexidade em relação ao conjunto de instruções CISC, pois, nos processadores RISC, esse tipo de instrução é executado mais rapidamente que instruções que utilizam apenas registradores de uso geral. Assim, o uso extensivo de instruções lógicas e aritméticas que utilizam acesso a memória é uma prática recomendável nas arquiteturas RISC.
- 2 Nos microprocessadores CISC, o conjunto de instruções apresenta um número mínimo de instruções em linguagem de máquina, fazendo que a quantidade de memória demandada por programas seja bem menor que a quantidade demandada por máquinas RISC, que utilizam conjuntos de instruções com um número muito maior de instruções.
- 3 Em processadores com caminho de dados com *pipeline*, é possível, em muitas situações, que diferentes estágios de duas ou mais instruções possam ser executados simultaneamente.
- 4 Muitos sistemas de memória modernos podem ter diversos níveis de *cache*. Em muitos casos, o *cache* de nível 1 é implementado dentro do *chip* da CPU.
- 5 Em uma arquitetura do tipo *Harvard*, a seção de *cache* de instruções é a mesma seção de *cache* de dados, enquanto, em arquiteturas tradicionais, as seções de *cache* de instruções e de dados ocupam espaços diferentes da memória.

**QUESTÃO 19**

Parte fundamental no funcionamento dos equipamentos, os programas de computador são muitas vezes classificados em *softwares* de sistema e *softwares* de aplicação. Com relação aos diversos tipos de *software* utilizados em computadores, julgue os itens que se seguem.

- 1 Os programas denominados montadores (*assemblers*) realizam a conversão de programas em linguagem *assembly* para a linguagem de máquina.
- 2 Um editor de ligação, ou ligador (*linker*), permite combinar módulos montados separadamente, muitas vezes chamados de módulos-objeto, em um único programa.
- 3 Os programas denominados compiladores realizam o processo de converter um programa em linguagem de máquina para um código equivalente em linguagem de alto nível.
- 4 A função principal de um programa carregador (*loader*) é permitir a edição de um programa em linguagem de alto nível, de modo que se possa salvá-lo em modo texto.
- 5 Os sistemas operacionais modernos não têm por função auxiliar no controle do acesso a periféricos. Atualmente, essa função é realizada por um programa denominado processador de macros.

**QUESTÃO 20**

O sistema operacional, uma camada de *software* posta entre o *hardware* e os programas que executam tarefas para os usuários, é um conceito central em informática. Acerca de sistemas operacionais e temas correlatos, julgue os itens seguintes.

- 1 Em todo sistema multiprogramado, diversos programas podem ser mantidos na memória ao mesmo tempo, mas um programa só pode ser iniciado quando outro já tiver sido completamente finalizado.
- 2 Em diversos sistemas multiprogramados, é possível que um mesmo programa seja executado por diferentes processos.
- 3 Devido a suas características específicas, nenhum sistema multiprogramado permite que se utilize o mecanismo da interrupção, pois não existe forma de desabilitar esse mecanismo; assim, caso ele seja utilizado, sempre ocorrerá perda de informação essencial quando o sistema operacional realizar a troca de um processo para outro.
- 4 Programa concorrente é a denominação dada a um grupo de processos que têm, necessariamente, objetivos diferentes e independentes uns dos outros, e que competem entre si pelo uso dos recursos computacionais de uma determinada máquina e de seus periféricos.
- 5 Quando, em um conjunto de  $N$  processos, cada um dos  $N$  processos está bloqueado à espera de um evento que somente pode ser causado por um dos  $N$  processos desse conjunto, esse conjunto está em *deadlock*.

## Texto CE-I – questões 21 e 22

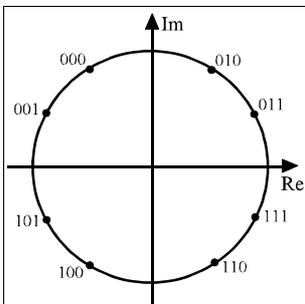
O objetivo principal de um *data modem* é realizar a interface entre computadores, redes de computadores ou qualquer outro equipamento terminal digital e os meios de comunicação analógicos ou os canais de rádio. Um *modem* pode ser visto como um repetidor que converte sinais elétricos em diversos formatos analógicos e digitais. Muitos são os padrões e as técnicas de comunicação utilizadas em um *modem*, estando alguns dados referentes a esses padrões representados na tabela abaixo.

padrão	taxa de transmissão máxima	modo de operação	meio de transmissão	modulação
208 (Bell System)	4,8 kbps	<i>full-duplex</i> <i>half-duplex</i>	dois fios quatro fios	8-PSK
209 (Bell System)	9,6 kbps	<i>full-duplex</i> <i>half-duplex</i>	dois fios quatro fios	16-QAM
V.29 (CCITT)	9,6 kbps	<i>half-duplex</i>	quatro fios	16-QAM
V.32 (CCITT)	9,6 kbps	<i>full-duplex</i>	dois fios quatro fios	16-QAM com codificação de <i>trellis</i>

### QUESTÃO 21

Com base nas informações apresentadas no texto CE-I e em relação às técnicas de modulação utilizadas em sistemas de comunicação, julgue os itens a seguir.

- 1 A técnica de modulação utilizada no *modem* padrão 208 da Bell System realiza um chaveamento na fase do sinal portador em função do sinal modulante. Assim, a informação é transmitida por meio de variações na fase do sinal portador, apresentando um diagrama de estado-espço teórico típico da envoltória complexa do sinal modulado da forma ao lado.
- 2 Para uma filtragem de Nyquist ideal e nas mesmas condições de operação, os padrões 209 da Bell System e V.29 do CCITT apresentam, teoricamente, a mesma eficiência de banda em bps/Hz.
- 3 Para uma taxa de transmissão de 9,6 kbps na entrada de um *modem* V.29 do CCITT, é gerado um sinal modulado na saída do *modem* com uma taxa de transmissão de 38.400 *bauds*.
- 4 Para as mesmas condições de operação, de ocupação de banda de frequências e de potências de sinal e de ruído, caso o parâmetro de escolha de técnica de modulação para um sistema seja uma melhor BER, é preferível o uso de um *modem* que opere com a técnica do tipo 16-QAM em lugar de um *modem* que opere com a técnica 16-PSK.
- 5 Para oferecer uma determinada qualidade de transmissão em termos de BER, um sistema que utilize o padrão V.32 do CCITT deverá apresentar uma relação entre a potência do sinal e a potência de ruído (S/N) maior que a relação S/N que deveria ser oferecida caso o sistema operasse com um *modem* no padrão V.29, nas mesmas condições de operação.



### QUESTÃO 22

A partir das informações apresentadas no texto CE-I, julgue os itens a seguir, relativos aos modos de operação e às técnicas de comunicação e de modulação utilizadas em sistemas de comunicação.

- 1 No caso de uma transmissão *full-duplex* a dois fios em uma banda de frequências disponível fixa, um sistema de comunicação digital deverá alocar bandas de frequências distintas para a transmissão e para a recepção, o que faz que esse sistema apresente, comparativamente ao sistema de quatro fios, uma menor capacidade de transmissão em ambas as direções, necessitando, dessa forma, mais tempo para a transmissão e a recepção de uma determinada quantidade de informação.
- 2 Um sistema *half-duplex* permite o uso de uma menor banda de frequências alocada, quando comparado ao sistema *full-duplex*; porém, nesse caso, para um sistema *half-duplex* balanceado e simétrico, o tempo necessário para a troca de uma determinada quantidade de informação entre dois pontos quaisquer do sistema é maior que aquele que seria utilizado no caso do sistema *full-duplex*, dadas as mesmas condições de modulação e de transmissão.
- 3 Para que um sistema *full-duplex* em um esquema a quatro fios possa funcionar corretamente, é necessário que a técnica TDM seja utilizada.
- 4 Em um processo de transmissão *simplex* que utilize um esquema a dois fios, a banda ocupada por um sistema 8-PSK é igual à banda ocupada por um sistema 16-QAM, dadas as mesmas condições de operação.
- 5 Caso o sinal modulante de um sistema 16-QAM seja obtido por um processo TDM de dez sinais de informação e supondo um esquema *full-duplex* com uma banda hipotética alocada em cada direção de transmissão de 0,1 MHz, a taxa de transmissão individual máxima que cada um dos dez sinais poderá ter em um sistema FDMA é superior a 30 kbps.

### RASCUNHO

**QUESTÃO 23**

A arquitetura TCP/IP tornou-se o padrão de fato para a interconexão de redes. Acerca da arquitetura TCP/IP e de seus principais protocolos, julgue os itens que se seguem.

- 1 Entre as funções associadas ao protocolo IP (*Internet Protocol*), encontram-se o roteamento e o endereçamento da inter-rede. Em redes que podem ser endereçadas diretamente a partir da Internet, são utilizados endereços IP válidos e roteadores convencionais. Em redes isoladas da Internet, são utilizados endereços IP inválidos e roteadores especiais, projetados para operar com esse tipo de endereçamento.
- 2 As adaptações recentes para o protocolo de transporte TCP incluem a definição de uma *option* para estender o tamanho da janela de transmissão TCP, o que permite a utilização do protocolo em redes com grandes larguras de banda.
- 3 UDP é um protocolo de transporte simples que implementa pouco mais do que a função de multiplexação por meio dos endereços de transporte ou portas.
- 4 RIP e OSPF são protocolos de roteamento do tipo IGP. O RIP tem como característica a utilização de um algoritmo do tipo vetor de distância e apresenta uma convergência considerada lenta. O OSPF baseia-se em um algoritmo do tipo estado de enlace e possui uma convergência mais rápida que o RIP.
- 5 O protocolo de roteamento BGP é um protocolo do tipo EGP e não pode ser utilizado para a troca de informações de roteamento entre dois roteadores de um mesmo sistema autônomo.

**QUESTÃO 24**

A arquitetura TCP/IP, pilar da estrutura da Internet, inclui dois protocolos na camada de transporte. Um deles é o *Transmission Control Protocol* (TCP), que é orientado a conexão. Acerca desse protocolo, julgue os seguintes itens.

- 1 O TCP utiliza o conceito de porta para permitir que vários processos em um único sistema possam transmitir simultaneamente cadeias de dados, ou seja, para que possam usar os serviços TCP.
- 2 O TCP é capaz de transferir uma cadeia contínua de octetos unidirecional entre os usuários. Assim, é necessário que dois usuários, cada um em um sistema, abram duas conexões TCP, uma em cada direção, para que esses usuários possam comunicar-se de forma bidirecional.
- 3 O procedimento de *three-way handshake* do TCP consiste no emprego em seqüência das primitivas para abrir (*open*) uma conexão, enviar (*send*) ou receber (*receive*) dados e fechar (*close*) a conexão aberta.
- 4 Cada entidade TCP trata independentemente a associação de portas a processos. Entretanto, os processos servidores mais usados são associados a portas fixas notórias, que são divulgadas para os usuários.
- 5 O TCP provê um mecanismo de informação da janela de recepção que permite a um transmissor especificar a quantidade de dados que será enviada ao receptor na próxima mensagem.

**QUESTÃO 25**

O protocolo IP foi projetado para permitir a interconexão de redes de computadores que utilizam a tecnologia de comutação de pacotes. Associada com a técnica de roteamento de pacotes, essa característica é apontada como a principal causa da flexibilidade do IP na formação de grandes redes, como a Internet, a partir da interconexão de redes heterogêneas. Acerca desse protocolo, na sua versão 4, julgue os itens abaixo.

- 1 Ao contrário do X.25, que também é um protocolo embasado na comutação de pacotes, o IP é um protocolo que opera sem conexões.
- 2 Os endereços IP são números com 32 *bits*, normalmente designados por quatro valores decimais separados por pontos.
- 3 O cabeçalho do datagrama IP possui um campo para indicar qual é o protocolo utilizado no nível superior, ou seja, no nível de aplicação da arquitetura TCP/IP.
- 4 Para efeito de roteamento, cada datagrama IP é tratado como uma unidade independente, não possuindo nenhuma relação com qualquer outro datagrama anterior ou posterior.
- 5 Antes de transmitir um datagrama, o IP verifica a integridade do cabeçalho e dos dados transportados, pois não faz sentido rotear datagramas errados.

**QUESTÃO 26**

O padrão IEEE 802.3, referente ao *ethernet* CSMA/CD e seus sucessores *fast-ethernet* e *gigabit-ethernet*, é certamente aquele de maior sucesso da série IEEE 802. Acerca desse padrão e das tecnologias a ele associadas, julgue os itens seguintes.

- 1 Para redes locais em banda-base a 10 Mbps, o padrão 802.3 estabelece quatro principais especificações de meio físico: 10base5, 10base2, 10baseT e 10baseF.
- 2 No nível físico, a subcamada PLS (*physical signaling*) fornece um serviço que inclui informações a serem usadas para a entidade MAC (*medium access control*) executar a função de controle de acesso ao meio, o que compreende, por exemplo, a detecção de portadora e a detecção de colisão.
- 3 O quadro MAC possui um campo de preâmbulo de sete octetos, com *bits* alternados 10101010, usados para a sincronização do transmissor e do receptor, e para garantir o tamanho mínimo do quadro.
- 4 O primeiro *bit* do campo do endereço de destino do quadro MAC identifica o endereço como sendo individual (*bit* = 0) ou de grupo (*bit* = 1).
- 5 O quadro MAC é terminado por um campo de 8 *bits* que contém um verificador de redundância cíclica calculado a partir dos campos de endereço, de comprimento, de dados e de extensão (PAD) do quadro MAC.

**QUESTÃO 27**

O modo de transferência assíncrono (ATM) é uma tecnologia com base na transmissão de pequenas unidades de informação de tamanho fixo e formato padronizado, denominadas células. Associada com outros mecanismos de conexão e de controle de serviços, essa tecnologia é capaz de suportar diferentes serviços, para responder a requisitos de diferentes tipos de tráfegos a altas velocidades de transmissão. Acerca do ATM, julgue os itens a seguir.

- 1 Um canal ATM é identificado por um rótulo, no cabeçalho da célula, que indica o endereço de destino da célula, de modo semelhante ao endereço de destino do IP.
- 2 O tamanho fixo e reduzido das células permite diminuir o tempo de empacotamento de informações, o que é importante para não deteriorar sinais de áudio e vídeo em aplicações com interatividade em tempo real entre os usuários, tal como em uma conversação telefônica.
- 3 Um dos pontos negativos do pequeno tamanho das células é o grande *overhead* que o cabeçalho representa, o que diminui a capacidade de transmissão efetiva da rede.
- 4 No contexto do Modelo de Referência para Protocolos (PRM) da recomendação I.321 do ITU aplicado à RDSI-FL, a camada ATM tem as funções de controle genérico de fluxo, inserção e remoção do cabeçalho das células, interpretação dos campos VPI/VCI e multiplexação/demultiplexação de células.
- 5 As células ATM contêm, no cabeçalho, um campo com informações de redundância para a detecção de erros no cabeçalho. Células com erros irreparáveis no cabeçalho são simplesmente descartadas.

**QUESTÃO 28**

A estruturação de redes corporativas, concebidas para a realização de serviços integrados de comunicação, vem-se consolidando como requisito fundamental no processo de projeto e formação de redes. Como consequência, as tecnologias utilizadas em tais projetos incorporam, cada vez mais, recursos voltados para a diferenciação e a integração de serviços de comunicação, em geral sob uma perspectiva de qualidade (QoS). Acerca das modalidades de serviços de comunicação em redes e dos recursos de QoS disponíveis para a realização de redes de serviços integrados, julgue os itens que se seguem.

- 1 Serviços de comunicação interativa são sensíveis a variações na latência e a níveis elevados de atrasos.
- 2 Serviços de comunicação não-interativa não são bem-acomodados a redes que operam segundo a política de *best effort*.
- 3 Serviços síncronos, chamados, em alguns contextos, de serviços de tempo real, exigem banda passante constante e garantida.
- 4 Tecnologias como ATM e *frame-relay* oferecem serviços com QoS garantido, realizando classificação e priorização de tráfego nos comutadores da rede.
- 5 Não se pode falar em rede IP com garantia de QoS pois esse tipo de rede opera apenas no modo *best effort*, não suportando categorias de serviço diferentes desta.

**QUESTÃO 29**

Os principais ambientes de rede da atualidade experimentam uma diversificação e uma disseminação dos serviços de interação e colaboração via rede, em especial com a utilização em larga escala de recursos multimídia. Assim, os serviços de mensagem não-interativos, como o correio eletrônico, possuem agora versões interativas, representadas pelos serviços de conversação via rede (*chats*) e pelas tecnologias de teleconferência e telecolaboração, nos quais a interatividade extrapola o limite das mensagens textuais e passa a utilizar recursos multimídia que incluem interatividade com voz e vídeo e compartilhamento de recursos computacionais avançados. Acerca do planejamento de serviços e aplicações de mensagem e colaboração via rede, julgue os itens seguintes.

- 1 A implantação de serviços de mensagem eletrônica a partir do padrão TCP/IP inclui a configuração de um MTA (SMTP), que atua como *gateway* de saída das mensagens, e de um servidor de caixas de correio (POP3), o qual realiza a função de *gateway* de entrada das mensagens.
- 2 Sistemas de correio eletrônico via *Web (webmail)* utilizam os mesmos protocolos para transmitir, receber e distribuir mensagens que os sistemas convencionais de correio eletrônico.
- 3 Soluções de colaboração visual, que incluem recursos para a realização de videoconferência, podem ser projetadas e implementadas a partir de *softwares* disponíveis a baixo custo e periféricos multimídia básicos para plataforma baixa.
- 4 A ambientação de salas de videoconferência costuma incluir tratamento sonoro (isolamento acústico), recursos especiais de iluminação e utilização adequada de cores no cenário.
- 5 Recursos avançados de apresentação podem ser incorporados nos ambientes de colaboração via rede, permitindo a captura e o transporte de documentos ou a disponibilização de apresentações multimídia entre os participantes da sessão de colaboração.

**QUESTÃO 30**

O padrão de videoconferência em redes que utiliza o protocolo IP é o ITU-T H.323, que define um modelo de videoconferência em redes por comutação de pacotes *best effort*, sem garantia de QoS. Acerca dos ambientes H.323, julgue os itens abaixo.

- 1 Terminais H.323 são entidades capazes de transmitir e receber, obrigatoriamente, áudio e vídeo (videoconferência) e, opcionalmente, dados (T.120).
- 2 Um ambiente H.323 mais completo envolve entidades para controle de registro, admissão e estado (RAS) e controle de recursos de rede, inclusive largura de banda, denominados *gatekeepers*.
- 3 A teleconferência multiponto em ambientes H.323, que tem aplicação típica na realização de reuniões a distância, necessita de uma unidade concentradora dos fluxos de informação, denominada MCU (*multipoint controller unit*).
- 4 Do ponto de vista da sinalização, o MCU realiza o estabelecimento de conexões individuais entre cada um dos terminais H.323 participantes. Do ponto de vista dos fluxos de informação, o MCU processa os fluxos de áudio, vídeo e dados originados em cada terminal que participa da conferência, retransmitindo os fluxos processados para os terminais.
- 5 *Gateways* são conversores de protocolo que permitem a interoperação entre ambientes H.323 e outros ambientes de colaboração via rede.

**QUESTÃO 31**

A estrutura das grandes redes de telecomunicações é, normalmente, dividida em redes de acesso e redes de transporte (*backbone*). Acerca das principais tecnologias utilizadas nos segmentos de acesso e de transporte, julgue os itens a seguir.

- 1 ADSL é uma tecnologia de rede de acesso e seu uso está, normalmente, restrito ao laço de assinante.
- 2 *Frame-relay* e ATM são tecnologias usadas tanto no segmento de acesso quanto no de transporte. Tais tecnologias operam no modo orientado a conexão e estão embasadas em comutação rápida de pacotes.
- 3 No que diz respeito a redes ATM, a sinalização NNI pública está completamente padronizada pelo ITU-T para interconexão de *backbones* ATM com administração distinta e permite a definição e a sinalização de políticas de tráfego entre duas redes.
- 4 A transmissão de tráfego IP constitui um serviço de comunicação de dados. Otimizações de roteamento e comutação desse tipo de tráfego em múltiplos enlaces de um mesmo *backbone* podem ser obtidas pela utilização do protocolo MPLS.
- 5 Redes ATM e *frame-relay* possuem os mesmos mecanismos e padrões de endereçamento, o que facilita a integração desses dois tipos de redes.

**QUESTÃO 32**

Estão disponíveis via Internet ferramentas voltadas para a segurança de redes, distribuídas gratuitamente e, em geral, com código fonte-aberto. Acerca das ferramentas de segurança e suas aplicações, julgue os itens que se seguem.

- 1 Escâneres, como o SAINT e o NESSUS, são úteis para a auditoria de segurança, em especial na realização de inventários de serviços e na identificação de vulnerabilidades a eles associadas.
- 2 *Sniffers*, tais como o TCPDUMP, são ferramentas passivas e difíceis de serem detectadas. Estão normalmente associadas a módulos analisadores de protocolo que permitem realizar análise de tráfego.
- 3 Sistemas *firewall*, como o TIS e o IPCHAINS, nada mais são que filtros que controlam o fluxo de pacotes entre duas redes.
- 4 Sistemas de detecção de intrusão, como o SNORT, consistem normalmente em uma proteção reativa a incidentes de segurança e podem ser utilizados na auditoria *a posteriori* de incidentes.
- 5 Implementações de redes virtuais privadas podem ser feitas para múltiplas conexões de transporte entre duas redes pela utilização de um túnel SSL, com implementação aberta disponível na biblioteca OPENSLL.

**QUESTÃO 33**

Acerca de infra-estruturas de chaves públicas (ICP), suas características tecnológicas e aplicações, julgue os itens abaixo.

- 1 Uma autoridade certificadora (AC) é uma entidade responsável por gerar, assinar e distribuir certificados digitais.
- 2 Certificados digitais são gerados e assinados em um formato padronizado, tal como o X.509v3, e podem ter sua validade completamente verificada sem a necessidade de interação com a autoridade certificadora que os assinou.
- 3 A segurança de um certificado digital, em uma ICP, depende da segurança da chave privada da autoridade certificadora que assinou esse certificado e independe da segurança da chave privada de outras autoridades certificadoras de níveis hierárquicos superiores.
- 4 Uma ICP baseia-se em técnicas e algoritmos de criptografia assimétrica e seus respectivos mecanismos de gerenciamento de chaves.
- 5 Assinaturas são realizadas com a utilização de chaves públicas e verificadas com a utilização de chaves privadas.

**QUESTÃO 34**

A estruturação da arquitetura de segurança de informações de uma organização necessita da definição e da aplicação de uma política de segurança que englobe aspectos tecnológicos e humanos. Acerca da definição e da aplicação de uma política de segurança, julgue os itens a seguir.

- 1 Uma política de segurança deve nortear a definição dos parâmetros para a configuração das principais ferramentas de proteção, tais como sistemas *firewall*, antivírus e detectores de intrusão.
- 2 Considerações acerca da segurança física das pessoas e das instalações estão fora do escopo de uma política global de segurança da informação.
- 3 A definição e a implantação de uma política de segurança da informação, no que diz respeito aos indivíduos, limita-se à especificação e à aplicação de perfis de acesso aos usuários ou grupos de usuários.
- 4 A sistemática de auditoria faz parte da política de segurança e deve ser definida em termos de periodicidade e escopo.
- 5 Uma política de segurança da informação, para ser efetiva, deve ser rígida e pouco flexível no que diz respeito aos procedimentos de acesso aos recursos, pois somente assim é possível evitar falhas de segurança associadas a vulnerabilidades inerentes a concessões desnecessárias.

**QUESTÃO 35**

O governo federal brasileiro vem tomando uma série de medidas que pouco a pouco estão definindo o arcabouço de uma legislação relativa à segurança dos sistemas de informação. Entre tais medidas, citam-se o Decreto n.º 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da administração pública federal, o Decreto n.º 3.587, de 5 de setembro de 2000, que estabelece normas para a Infra-Estrutura de Chaves Públicas do Poder Executivo Federal – ICP-Gov, e a Medida Provisória n.º 2.200, de 28 de junho de 2001, que institui a Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil. Acerca dessa legislação, julgue os seguintes itens.

- 1 A ICP-Brasil, tal como proposta, estabelece que as empresas do governo DATAPREV, DATASUS e SERPRO devem, cada uma, implantar sua própria AC e que as três ACs, assim estruturadas, devem ter uma certificação cruzada, de modo a, conjuntamente, constituir a AC-raiz da Infra-Estrutura de Chaves Públicas Brasileira.
- 2 O Decreto n.º 3.505/2000, entre outras providências, determina que não mais seja utilizado, em aplicações do governo federal, o protocolo de criptografia DES (*data encryption standard*), considerado obsoleto.
- 3 Como parte das determinações do Decreto n.º 3.587/2000, verifica-se que a tecnologia da ICP-Gov deverá utilizar criptografia simétrica.
- 4 Para efeito da ICP-Gov, uma autoridade registradora (AR) é uma entidade de registro, devendo, obrigatoriamente, estar fisicamente localizada fora de qualquer das ACs, de modo a garantir sua independência e sua autonomia com relação às ACs.
- 5 Para efeito da ICP-Gov, a disponibilização de certificados emitidos e de Lista de Certificados Revogados (LCR) atualizada será proporcionada mediante o uso de diretório seguro e de fácil acesso.

**QUESTÃO 36**

As técnicas, os protocolos e os sistemas de criptografia são um dos pilares para a organização de proteções contra ataques à segurança dos sistemas de informática e comunicação. Por melhor que seja a técnica de criptografia e a robustez do algoritmo, um sistema não pode ser considerado seguro sem os meios, os procedimentos e a política para gerenciar as chaves criptográficas empregadas. Acerca das técnicas, dos protocolos e dos sistemas de gerência de chaves de criptografia existentes, julgue os itens seguintes.

- 1 A dimensão da faixa de valores possíveis para as chaves (*key space*) é um sério problema no processo de geração de chaves criptográficas. Em DES, por exemplo, a faixa de valores pode reduzir-se radicalmente, caso, para facilitar a interação com o usuário, seja permitido empregar apenas chaves com caracteres ASCII ou caso as letras sejam sempre convertidas de minúsculas para maiúsculas.
- 2 Quando as pessoas escolhem suas próprias chaves, constata-se que, em geral, são escolhidas chaves inadequadas, que empregam nomes próprios, iniciais e outras informações facilmente deduzíveis, por exemplo, por meio de ataques de dicionário.
- 3 Alguns algoritmos de criptografia possuem chaves fracas, ou seja, algumas chaves específicas menos seguras que as outras chaves.
- 4 Em sistemas que exigem trocas frequentes das chaves de criptografia, para evitar a repetição dos processos de distribuição de chaves, pode-se empregar um procedimento de atualização que gera uma nova chave a partir da chave antiga, com o auxílio de uma função de embaralhamento unidirecional (*one-way function*).
- 5 Se a chave privada de um usuário de um sistema de criptografia assimétrico (sistema de chave pública) ficar comprometida, então, para retornar a uma situação de segurança, é suficiente que esse usuário regenere um par de chaves privada e pública, divulgando esta última para todos os seus correspondentes.

**QUESTÃO 37**

A complexidade sempre crescente das redes de comunicação vem exigindo cada vez mais o emprego de ferramentas automatizadas de gerência de redes. Isso motivou esforços para a padronização de arquiteturas de gerência, incluindo a definição de protocolos e bancos de dados específicos de gerência de redes e sistemas. O protocolo padronizado de gerência de redes mais popular da atualidade é o SNMP (*simple network management protocol*), que tem três versões oficialmente publicadas em RFC (SNMPv1, SNMPv2 e SNMPv3), todas conservando alguns princípios básicos comuns, mas com diferenças no que se refere ao comportamento do protocolo, tipos de mensagens e mecanismos de segurança. Acerca do protocolo SNMP nas versões v1 e v2, julgue os itens a seguir.

- 1 Em SNMPv1, a mensagem *get-request* possibilita que um gerente obtenha o conteúdo de uma variável ou de um conjunto de variáveis da base de informações de gerência (*management information base – MIB*) de um agente.
- 2 Em SNMPv2, a mensagem *get-bulk-request* é especificada para que um gerente possa solicitar de uma só vez um grande volume de dados da MIB de um outro gerente.
- 3 Os mecanismos de segurança em SNMPv2 incluem uma MIB de segurança que contém informações para identificar e definir autorizações acerca de cada relacionamento entre um gerente e um agente.
- 4 Para efeito de troca das mensagens em SNMPv1, é requerido apenas um serviço de transporte com base em datagramas não-confiáveis.
- 5 A mensagem de *trap* presente em SNMPv1 foi suprimida da padronização de SNMPv2, em função da dificuldade de verificar a fonte das mensagens, o que acarreta potenciais riscos à segurança.

**QUESTÃO 38**

No contexto dos padrões relativos ao protocolo SNMP, a definição da base de informações de gerência MIB-II inclui um grupo de variáveis com informações básicas dos sistemas gerenciados (*MIB-II system group*). Essas informações são consideradas de grande valor, pois uma estação de gerência pode consultar os sistemas gerenciados e automaticamente gerar uma base de dados de configuração da rede. Acerca dessas informações, julgue os itens abaixo.

- 1 Entre as sete informações do grupo-sistema, as variáveis *sysContact*, *sysName* e *sysLocation* apresentam característica de acesso do tipo *read-write*, enquanto as demais variáveis têm acesso do tipo *read-only*.
- 2 A variável *sysObjectID* corresponde a um identificador atribuído pela ISO ao produto que constitui o objeto gerenciado.
- 3 A variável *sysUpTime*, cuja unidade é o décimo de segundo, mede o tempo decorrido desde a última inicialização do sistema de gerência de rede.
- 4 A variável *sysServices* contém um número inteiro codificado que indica os níveis de protocolo para os quais o sistema gerenciado presta serviços, usando os níveis do modelo OSI como referência.
- 5 As variáveis *sysContact* e *sysLocation* permitem que os registros de problemas sejam direcionados às pessoas apropriadas para a correção e o reparo, mostrando ainda a localização do sistema que está apresentando o problema.

**QUESTÃO 39**

Acerca do emprego do SNMP e de suas MIB como infra-estrutura tecnológica de gerenciamento de ambientes de tecnologia da informação, julgue os itens subseqüentes.

- 1 SNMP define uma maneira confiável e segura de transferência de informações de gerência.
- 2 Aplicações SNMP são estruturadas a partir de uma arquitetura gerente-agente, na qual o gerente centraliza e processa as informações de gerenciamento, e os agentes, distribuídos por todos os elementos gerenciados do ambiente, fazem a coleta dessas informações.
- 3 A comunicação entre o gerente e o agente pode ser feita de modo síncrono ou assíncrono, dependendo do evento de gerência que esteja ocorrendo.
- 4 Existem MIB padronizadas para equipamentos típicos de rede, como *hubs*, comutadores e roteadores, e que definem quais informações de gerência podem ser coletadas ou configuradas por meio do SNMP.
- 5 Por se tratar de um padrão internacionalmente reconhecido e respeitado, não existem MIB proprietárias.

**QUESTÃO 40**

Como parte da padronização da arquitetura de gerência de redes OSI, além da definição do protocolo CMIP e do banco de dados específico de gerência de redes e sistemas OSI, foram propostas áreas funcionais de gerência para responder aos requisitos de sistemas de gerência. Acerca dessas áreas e atividades de gerência de redes, julgue os itens seguintes.

- 1 A distribuição e a atualização de *software* em uma rede é considerada uma atribuição da área de gerência de contabilização, em função dos custos e da necessidade de divisão do orçamento entre os diversos participantes da rede.
- 2 A gerência de falhas faz uma distinção básica entre falhas e erros, estes últimos sendo eventos que ocorrem ocasionalmente e podem ser detectados, tratados e recuperados por meio de mecanismos de controle dos protocolos, enquanto as falhas são condições de anormalidade que exigem ações específicas de gerência.
- 3 A área de gerência de desempenho correlaciona-se com a atividade de planejamento de crescimento de uma rede, pelo fato de tratar dos níveis de serviço que estão sendo obtidos e das tendências de funcionamento das redes.
- 4 O estabelecimento, a manutenção e a atualização dos relacionamentos entre os componentes da rede, bem como a identificação e o acompanhamento dos estados administrativos e operacionais desses componentes, são atividades inerentes à área de gerência de segurança, em função das necessidades de garantir a disponibilidade dos componentes e a autenticidade das identificações na rede.
- 5 O acompanhamento do uso de recursos da rede, para evitar, por exemplo, que um usuário ou um grupo de usuários abuse de seus privilégios e provoque impactos na disponibilidade da rede para outros usuários, é uma atividade da área de gerência de segurança.