BANCO DA AMAZÔNIA S.A.

CARGO 21
TÉCNICO CIENTÍFICO

ÁREA
TECNOLOGIA DA INFORMAÇÃO
SEGURANÇA DA INFORMAÇÃO

MANHÃ

LEIA COM ATENÇÃO AS INSTRUÇÕES ABAIXO.

1 **Confira atentamente se os seus dados pessoais e os dados identificadores do seu cargo transcritos acima coincidem com o que está registrado em sua folha de respostas. Confira também o seu nome e seu cargo em cada página numerada deste caderno de provas. Em seguida, verifique se ele contém a quantidade de itens indicada em sua folha de respostas, correspondentes às provas objetivas.** Caso o caderno esteja incompleto, tenha qualquer defeito ou apresente divergência quanto aos seus dados pessoais ou quanto aos dados identificadores do seu cargo, solicite ao fiscal de sala mais próximo que tome as providências cabíveis, pois não serão aceitas reclamações posteriores nesse sentido.

2 Quando autorizado pelo chefe de sala, no momento da identificação, escreva, no espaço apropriado da **folha de respostas**, com a sua caligrafia usual, a seguinte frase:

Execute com fé tudo o que decidiu.

3 Não se comunique com outros candidatos nem se levante sem autorização de fiscal de sala.

4 Na duração das provas, está incluído o tempo destinado à identificação — que será feita no decorrer das provas — e ao preenchimento da folha de respostas.

5 Ao terminar as provas, chame o fiscal de sala mais próximo, devolva-lhe a sua folha de respostas e deixe o local de provas.

6 A desobediência a qualquer uma das determinações constantes em edital, no presente caderno ou na folha de respostas poderá implicar a anulação das suas provas.

OBSERVAÇÕES

- Não serão objeto de conhecimento recursos em desacordo com o estabelecido em edital.
- Informações adicionais: telefone 0(XX) 61 3448-0100; Internet – www.cespe.unb.br.
-

cespeUnB
Centro de Seleção e de Promoção de Eventos

De acordo com o comando a que cada um dos itens a seguir 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**. Para as devidas marcações, use a **folha de respostas**, único documento válido para a correção das suas respostas.

CONHECIMENTOS BÁSICOS

Texto para os itens de 1 a 8

A discussão acerca da influência do pensamento econômico na teoria moderna é aparentemente uma discussão metateórica, ou seja, de caráter metodológico. Mas, na ciência econômica, como de resto nas ciências sociais em geral, não há consenso sobre a forma de evolução dos paradigmas. Contrariamente ao que, em regra, acontece no mundo das ciências naturais, há aqui dúvidas a respeito de se o conhecimento mais recente é necessariamente o melhor, o mais verdadeiro, ou seja, aquele que incorporou produtivamente os desenvolvimentos teóricos até então existentes, tendo deixado de lado aqueles que não se mostraram adequados a seu objeto.

O economista Pérsio Arida tratou desse problema em um texto que se tornou clássico muito antes de ser publicado. Afirma ali que o aprendizado da teoria econômica tem sido efetuado de acordo com dois modelos distintos: o que ele chama de *hard science*, que ignora a história do pensamento e segundo o qual o estudante deve familiarizar-se de imediato com o estágio atual da teoria, e o que ele chama de *soft science*, que considera que o estudante deve conhecer bem, e, se possível, dominar, os clássicos do passado, mesmo que em prejuízo de sua familiaridade com os desenvolvimentos mais recentes. Acrescenta a esse enquadramento que, por trás do modelo *hard science*, está a ideia de uma "fronteira do conhecimento": o estudante não precisaria perder tempo com antigos pensadores, porque todas as suas eventuais contribuições já estariam incorporadas ao estado atual da teoria. De outro lado, subjacente à visão do modelo *soft science*, estaria a ideia de que o conhecimento está disperso historicamente, ensejando a necessidade de os estudantes se dedicarem a esses pensadores.

Leda Maria Paulani. Internet: <www.fipe.org.br> (com adaptações).

Acerca do texto, julgue os itens a seguir.

1 O texto constitui uma argumentação em defesa de determinada linha de pesquisa dentro das ciências econômicas.

2 Pela leitura do texto, depreende-se que a *hard science* e a *soft science* correlacionam-se, respectivamente, às ciências naturais e às ciências humanas.

3 Infere-se do texto que o conhecimento recente da área econômica pode não ser, necessariamente, o que incorporou as melhores facetas do conhecimento historicamente desenvolvido.

4 Os pronomes "aqui" (ℓ.7) e "ali" (ℓ.14), que geralmente denotam referência a lugar, são usados no texto para retomar objetos concretos.

A autora defende que, na economia e nas ciências sociais em geral, não há consenso sobre a verdadeira qualidade da informação teórica incorporada ao conhecimento recente na área. Tal afirmação pode ser inferida da leitura do primeiro parágrafo. Cada um dos itens de **5** a **8** apresenta uma proposta de reescrita dessa asserção, devendo ser julgado certo se mantiver, com correção gramatical, o sentido dessa assertiva, ou errado, em caso contrário.

5 Não existem, segundo a autora, uniformidade de opiniões, nas ciências sociais, às quais se englobariam a ciência econômica, quanto à verdadeira qualidade da informação teórica incorporada ao conhecimento recente na área.

6 A autora defende não haver consenso na ciência econômica, a exemplo do que ocorre nas demais ciências sociais, a respeito da verdadeira qualidade da informação incorporada ao conhecimento recente na área.

7 Quanto ao consenso nas ciências sociais sobre a verdadeira qualidade da informação teórica incorporada para o conhecimento recente em ciência econômica, a autora defende que não há.

8 A respeito da qualidade real da informação teórica juntada ao conhecimento recente na área, a autora defende não haver consenso seja na ciência econômica, seja nas demais ciências sociais.

Texto para os itens de 9 a 17

Frederick August von Hayek concebe o indivíduo como uma singularidade e o conhecimento como algo subjetivamente determinado, particular e intransferível. Esse conhecimento, portanto, não está, para Hayek, fundamentado nem em fatos objetivos, que a teoria pudesse captar, nem em uma sorte qualquer de razão transcendental. Mas, além de seus propósitos particulares e do conhecimento subjetivo que cada um possui do mundo, a ação humana é, para Hayek, constituída também por regras, que os homens seguem meio inquestionadamente, por um processo de imitação. Essas regras, por sua vez, não são postuladas, não são produtos de um suposto contrato original resultante da ação intencional de indivíduos autocentrados, não podendo, pois, ser reduzidas às ações de indivíduos racionais, como rezam os preceitos metodológicos por trás da *rational choice* (escolha racional). Ora, o que Hayek está então sugerindo é que nem toda ação humana é produto de indivíduos racionais, autônomos e independentes, autodeterminados e soberanos, tal como requer a teoria econômica moderna. Ao contrário, as ações humanas são fortemente dependentes de um processo que é social e socialmente determinado. Afirma, por isso, que, em uma sociedade complexa como a nossa, o homem não tem outra escolha a não ser se adaptar às forças cegas do processo social. E, em função de tudo isso, afirma que, palavras dele, "a desgraça do mecanismo de mercado é dupla, porque, por um lado, ele não é produto do desígnio humano e, por outro, as pessoas que são guiadas por ele normalmente não sabem por que são levadas a fazer o que fazem".

Idem, ibidem.

Com referência às ideias e à tipologia do texto, julgue os itens subsequentes.

9 O texto, por apresentar a síntese do pensamento de von Hayek, é predominantemente descritivo.

10 Embora esteja empregada de modo correto, a palavra "rezam" (ℓ.14) poderia ser substituída, sem prejuízo para o sentido e a correção gramatical do texto, por **ditam** ou por **estabelecem**.

11 Ao afirmar que as pessoas guiadas pelo mercado 'normalmente não sabem por que são levadas a fazer o que fazem' (ℓ.27-28), von Hayek retoma a ideia de que as ações humanas dependem de um processo social socialmente determinado.

Acerca dos elementos gramaticais presentes no texto, julgue os itens que se seguem.

12 No texto, a palavra "Ora" (ℓ.16) tem sentido diferente daquele empregado na seguinte frase: Ora essa ação é voluntária, ora ela é socialmente determinada.

13 No último período do texto, caso se retirem o trecho "palavras dele" e as vírgulas que o isolam, não se perde a informação sobre a autoria da citação feita, e o trecho continua gramaticalmente correto.

14 A correção gramatical do texto seria prejudicada caso se colocasse uma vírgula logo após a forma verbal "é" (ℓ.16).

15 No trecho "às forças cegas do processo social" (ℓ.23), caso se substitua "forças cegas" por **mecanismos cegos**, será necessário trocar "às" por **aos** para se manter a correção gramatical.

16 As palavras "intransferível", "inquestionadamente" e "indivíduos" possuem em sua estrutura elementos que indicam negação.

17 O trecho em que ocorre a palavra 'desígnio' (ℓ.26) teria sua coerência prejudicada caso tal palavra fosse substituída por **destino**.

Cada um dos itens abaixo apresenta um fragmento hipotético de correspondência oficial, seguido de uma proposta de classificação desse fragmento (entre parênteses) quanto à parte e ao padrão de correspondência. Julgue-os quanto ao aspecto gramatical, quanto à classificação proposta e quanto à observância das recomendações previstas para o padrão de correspondência indicado.

18 Aos dez dias do mês de novembro do ano de dois mil e nove, às dez horas, na sala de reuniões do Departamento de Biologia Celular da Universidade de Brasília, teve início a... (**cabeçalho de uma ata**)

19 De ordem do senhor ministro da Educação, estamos informando a todos os chefes do Poder Executivo de todos os entes federados que, nos termos da Lei de Responsabilidade Fiscal, a data limite para apresentação das prestações de contas e respectivos relatórios a que se refere a citada lei... (**corpo de um relatório**)

20 Certos da atenção e da observância de V. S.ª para com as recomendações que ora lhe enviamos, antecipamos agradecimentos.

Atenciosamente,

(**fecho de um memorando**)

A Apple, dirigida pelo carismático Steve Jobs, tornou-se a mais fulgurante empresa da era digital. Jobs apresentou ao mundo sua nova aposta, o iPad, um aparelho maior que um telefone celular e menor que um computador portátil. Se não convenceu inteiramente os comentaristas tecnológicos, é unânime a previsão de que o iPad "fará dinheiro".

A expressão "fazer dinheiro", como sinônimo de criação de riqueza, nasceu com a transformação dos Estados Unidos da América (EUA) em potência tecno-militar-industrial. Antes disso, vigorava a noção mercantilista de que a riqueza apenas mudava de dono, sendo herdada ou tomada de alguém mais fraco ou menos hábil, pelo comércio, pela trapaça e pela guerra de conquista. O que libertou as forças econômicas desse jogo de soma zero, em que o ganho de alguns não aumentava o bolo geral de riqueza, foi a inovação, aliada a sua irmã gêmea, a produtividade.

Veja, 3/2/2010, p. 12-3 (com adaptações).

Tendo o texto acima como referência inicial e considerando aspectos marcantes do atual estágio da economia mundial, fortemente marcado pelo papel nele desempenhado pelo conhecimento, julgue os itens de **21** a **25**.

21 O texto remete à ideia de que, nos dias atuais, diferentemente do que ocorria no passado, a produção da riqueza — o "fazer dinheiro", para usar a expressão por ele utilizada — está essencialmente vinculada ao domínio do conhecimento.

22 O domínio norte-americano nos mercados mundiais, citado no texto, foi possível graças ao fim dos subsídios e das práticas protecionistas assegurado pela firme atuação da Organização Mundial do Comércio.

23 Países emergentes, como o Brasil, ressentem-se dos baixos investimentos em ciência e tecnologia, além dos índices educacionais insatisfatórios, razões suficientes para praticamente inviabilizar a exportação de seus produtos industriais e agrícolas.

24 O atual estágio da economia mundial, comumente identificado como globalização, tem nas inovações tecnológicas que se processam no campo das comunicações um de seus instrumentos fundamentais, pois elas permitem, entre outros importantes aspectos, a rápida circulação de informações e de capitais.

25 A recente crise econômica e financeira que abalou o mundo teve seu epicentro nos EUA. A timidez das medidas tomadas pelo governo de Barak Obama para enfrentá-la foi, para a maioria dos analistas, a principal razão para a perda da supremacia mundial do país para a emergente China.

Em um planeta aquecido, mantenha o refrigerador ligado. A floresta amazônica há muito deixou de ser tratada como o pulmão do mundo, mas ganhou *status* ainda mais importante, o de ar-condicionado da Terra. A preservação da mata é fundamental no combate ao aquecimento global, apontam especialistas.

O Globo. "Planeta Terra", nov./2009, p. 20 (com adaptações).

Tendo o texto acima como referência inicial e considerando a inserção da Amazônia no quadro de desenvolvimento sustentável, julgue os itens que se seguem.

26 Embora relativamente pouco extensa quanto à dimensão geográfica, a Amazônia é o ecossistema integralmente brasileiro mais conhecido no mundo, graças à formidável quantidade de água e de espécies que possui, e à sua importância para o clima global, como afirma expressamente o texto.

27 A ideia de desenvolvimento sustentável na Amazônia, a maior floresta tropical úmida do planeta, deve pressupor, entre diversas outras considerações, a substituição do uso desordenado de motosserras pelo exercício de aprender a extrair riqueza da floresta enquanto se garante sua preservação.

28 A cobiça internacional sobre a Amazônia passa ao largo de seu importante peso nos processos naturais que regulam os padrões climáticos globais, como afirmado no texto, mas deriva do extraordinário patrimônio mineral da região, hoje plenamente conhecido e devidamente mensurado.

29 Na Amazônia, exemplo de desenvolvimento sustentável verifica-se no aumento do número de empresas e cooperativas extrativistas que exploram a madeira legalmente, isto é, recebem o selo que certifica a extração embasada na preservação dos recursos florestais.

30 A produção de madeira certificada precisa ser socialmente justa e estar adaptada plenamente a padrões aceitáveis por parte de crescente parcela do mercado consumidor, sobretudo de países que apresentam uma consciência ambiental mais avançada e onde organizações não governamentais tendem a atuar com bastante vigor.

Julgue os itens seguintes a respeito de permutação e lógica sentencial.

31 Considerando que o anagrama da palavra ALARME seja uma permutação de letras dessa palavra, tendo ou não significado na linguagem comum, a quantidade de anagramas distintos dessa palavra que começam por vogal é 360.

32 A sentença "como hoje o alarme não foi acionado, então José não foi ao banco e os sensores não estavam ligados" é logicamente equivalente a "se José foi ao banco ou os sensores estavam ligados, então hoje o alarme foi acionado".

Suponha que um banco tenha um cartão especial para estudantes, que já venha com senha de 4 algarismos escolhidos de 0 a 9 e atribuídos ao acaso. Com relação a essa situação, julgue os itens subsequentes.

33 Ao se realizar todas as combinações possíveis, com os algarismos 2 e 1 juntos, nessa ordem, obtêm-se, no máximo, 192 senhas diferentes.

34 Podem-se obter 2.016 senhas em que o 0 é, necessariamente, um, e somente um, dos algarismos e os outros 3 algarismos são distintos.

35 Ao se utilizar somente os algarismos 1, 3, 4 e 7, podem-se obter 12 senhas de algarismos distintos e que não sejam maiores que 4.173.

36 Dizer que "todas as senhas são números ímpares" é falsa, do ponto de vista lógico, equivale a dizer que "pelo menos uma das senhas não é um número ímpar".

Considerando que, dos 100 candidatos aprovados em um concurso, 30 sejam mulheres, sendo que apenas 20% delas têm idade acima de 30 anos; e, entre os homens, 40% têm idade acima de 30 anos, jugue os itens que se seguem.

37 Selecionando-se, entre os referidos candidatos, somente homens com idade acima de 30 anos, é possível formar mais de 20.000 grupos, não ordenáveis, de quatro candidatos.

38 Se forem separadas somente as mulheres acima de 30 anos e 10% dos homens, então será possível formar 525 grupos diferentes de 5 pessoas, compostos por 3 homens e 2 mulheres.

39 Se um candidato tiver de escolher, em ordem de preferência, 7 cidades para trabalhar, entre 10 apresentadas pelo banco, então haverá mais de 144 opções de escolha para esse candidato.

40 A negação da proposição "se Paulo está entre os 40% dos homens com mais de 30 anos, então Luísa tem mais de 30 anos" é "se Paulo não está entre os 40% dos homens com mais de 30 anos, então Luísa não tem mais de 30 anos".

RASCUNHO

The Gordon and Betty Moore Foundation, the largest private funder of Amazon rainforest conservation, is playing an unheralded but integral role in the development of the Earth Engine platform, a system that combines the computing power of Google with advanced monitoring and analysis technologies developed by leading environmental scientists. The platform, which was officially unveiled at climate talks in Copenhagen, promises to enable near real-time monitoring of the world's forests and carbon at high resolution at selected sites before COP-16 in Mexico.

The Earth Engine builds upon decades of research by scientists at a range of institutions, including NASA, the Woods Hole Research Center, Brazil's Imazon, and the Carnegie Institute. While it is so far only available for the Amazon and the Andes region in South America, the model is highly scalable and could eventually be applied virtually anywhere on Earth, enabling three-dimensional mapping of ecosystems and rapid reporting of land cover change, including alerting of deforestation and incidence of fire. The tool could play a critical role in helping countries win compensation under REDD, a mechanism that rewards countries for reducing emissions from deforestation and forest degradation. REDD is seen by many as perhaps the best way to generate funds for protection and sustainable use of forests.

Internet: <news.mongabay.com> (adapted).

According to the text above, judge the following items.

41 The biggest private funder of Amazon conservation has teamed up with Google and scientists to develop an earth monitoring platform.

42 The word "unheralded" (ℓ.3) means **expected**.

43 A new prototype that enables advanced monitoring and analysis of the world's forests was presented at the International Climate Change Conference (COP-15) in Copenhagen.

44 New technology can help stop the destruction of the world's rapidly-disappearing forests.

45 A scheme — known as REDD — provides financial incentives to rainforest nations for reducing emissions from deforestation and degradation.

46 Concerns remain that REDD could fail to deliver benefits to forest dwellers.

Creative, convergent, and social: prospects for mobile computing

The mobile computing industry, more than most, suffers a constant obsession with the future. Commoditization, market saturation, and technology and service convergence render the mobile communications business one of the most volatile and precarious in terms of cycle time, customer churn, and obsolete investments. At the core of the industry's preoccupation with prospective market trends is the question of what technologies and services users will demand in the future — a question that has proven to be notoriously difficult to answer.

The first thing to notice about the current state of the mobile industry is that it is becoming increasingly commoditized. It is growing difficult to sustain competitive edge on handset differentiation alone. Mobile phones, like toasters and microwave ovens, are all now stylishly designed and contain similar chipsets and functionality. Although it would be wrong to suggest that consumers see all handsets as equally attractive — aesthetic qualities will surely continue to matter for such personal and visible devices, just as they do for, say, wrist watches — the large handset manufactures anticipate difficulty relying on high-margin luxury production models. As an alternative, they turn toward the idea that services can help differentiate their offerings. Recent movements in related industries to define a revitalized science of services (IBM, 2008) have emphasized that interaction with the physical device is to a large extent governed or defined by the service or application layer that resides on top of the physical artifact (Spohrer *et al.*, 2007). The appeal of a device depends, therefore, on the way in which it integrates into a larger system of services (Austin and Beyersdorfer, 2007); the locus of competition, whether through functionality or aesthetics, thus moves to a more diffuse realm where appeal depends on nuances of interaction between service components. The industry's perceptive but imperfect comprehension of this shift has led to a sometimes comic frenzy, a quest for the next perfect service or killer application that can be successfully monetized — a service or application users will actually pay for.

Internet: <www.palgrave-journals.com> (adapted).

Judge the following items according to the text above.

47 The text highlights themes salient in the rapidly converging mobile computing industry.

48 For consumers, mobile phones would be as attractive as all handsets.

49 The word "current" (ℓ.11) can be correctly substituted by **obsolete**.

50 Mobile vendors seeking to foster the consumption of mobile devices are increasingly viewing the challenge as a well-defined technology problem.

CONHECIMENTOS ESPECÍFICOS

A segurança da informação procura garantir a preservação da confidencialidade, a integridade e a disponibilidade da informação. Relativamente às normas ISO 27001, ISO 27002, ISO 27005 e ISO 15999, julgue os itens seguintes.

51 Um incidente de segurança da informação refere-se a um ou mais riscos não desejados ou esperados que possuem significativa probabilidade de comprometer os ativos de informação e ameaçam a segurança da informação.

52 São exemplos de ativos de uma organização a informação e os processos de apoio, sistemas e redes. Os requisitos de segurança, em uma organização, são identificados por meio de análise sistemática dos riscos de segurança.

53 Entre os ativos associados a sistemas de informação em uma organização, incluem-se as bases de dados e arquivos, os aplicativos e os equipamentos de comunicação (roteadores, secretárias eletrônicas etc.).

54 Uma organização deve ser capaz de inventariar seus ativos, identificar seus respectivos valores e importâncias e indicar um proprietário responsável por eles. A informação deve ser classificada em termos de sua utilidade, adequabilidade e nível de segurança.

55 É conveniente que, na classificação das informações e seu respectivo controle de proteção, considerem-se as necessidades de compartilhamento ou restrição de informações. Ao se tornar pública, uma informação frequentemente deixa de ser sensível ou crítica.

No que se refere às normas ISO 27001, ISO 27002, ISO 27005 e ISO 15999 e aos assuntos correlatos, julgue os itens de **56** a **76**.

56 O acesso físico e lógico de terceiros aos recursos de processamento da informação da organização devem ser controlados. Um exemplo de acesso lógico é o acesso aos bancos de dados da organização.

57 A necessidade de conexão com terceiros deve considerar o tipo de acesso requerido, o valor da informação, os controles empregados por terceiros e as implicações desse acesso à segurança da informação da organização.

58 Recomenda-se que as responsabilidades de segurança sejam atribuídas nas fases de seleção de pessoal, incluídas em acordos informais de trabalho e monitoradas durante a vigência de cada contrato de trabalho.

59 Acordos de confidencialidade fazem parte de uma política de pessoal cujo objetivo é assegurar que não haja acesso a sistemas sensíveis por pessoas não autorizadas.

60 O documento da política de controle de acesso contém as políticas para autorização e distribuição de controle de acesso. É recomendável a existência de um procedimento formal de registro e cancelamento de usuário para obtenção de acesso a todos os sistemas de informação e serviços, com exceção dos sistemas multiusuários.

61 Privilégio é qualquer característica ou facilidade de um sistema de informação multiusuário que permita ao usuário sobrepor controles do sistema ou aplicação. A concessão e uso de privilégios deve ser restrito e controlado, e sua utilização inadequada é considerada fator de vulnerabilidade de sistemas.

62 As senhas fornecem um meio de validação da autoridade do usuário e o estabelecimento dos direitos de acesso para os recursos ou serviços de leitura da informação.

63 O controle de acesso à rede busca assegurar o uso de interfaces apropriadas entre a rede da organização e as redes de outras organizações ou redes públicas e controlar o acesso dos usuários aos serviços de informação. Também busca utilizar mecanismos de autenticação apropriados para usuários e equipamentos.

64 Conexões externas que utilizam métodos *dial-up* devem ser validados conforme o nível estabelecido por avaliações de risco. Controles e procedimentos de discagem reversa, conhecidos por *call forwarding,* expõem e fragilizam a organização, uma vez que utilizam dispositivos roteadores com discagem reversa e levam o usuário a manter a linha aberta com a pretensão de que a verificação da chamada reversa tenha ocorrido.

65 Os controles baseiam-se nos requisitos de segurança selecionados considerando-se as restrições de implementação, sua eficácia em relação aos riscos que serão reduzidos e às perdas potenciais, caso as falhas na segurança ocorram. Pode-se, ainda, considerar fatores financeiros, como prejuízos à reputação da organização.

66 O documento da política de segurança da informação estabelece as suas linhas mestras, expressa as preocupações da administração e é por ela aprovado e comunicado a todos os funcionários.

67 São exemplos de conteúdos que constam no documento de política da informação: conformidade com a legislação e cláusulas contratuais, requisitos na educação de segurança, gestão da continuidade do negócio e regras para controle de acesso.

68 Convém que a política de segurança da informação tenha um patrocinador responsável por sua manutenção e análise crítica e que esteja de acordo com um processo de submissão definido.

69 Alguns controles deverão salvaguardar sistemas operacionais e ferramentas de auditoria durante as auditorias de sistema. O escopo de verificação deve ser acordado e controlado.

70 Na revisão periódica da conformidade dos sistemas com as políticas e normas organizacionais de segurança, devem-se incluir sistemas de informação, provedores de sistemas, proprietários da informação, ativos de informação, usuários e administração.

71 Controles de ambiente e *software* devem se corretamente implementados para que a validação da conformidade técnica e científica assegure que os sistemas de informação sejam verificados em conformidade com as normas de segurança implementadas.

72 Quando o processo envolver a lei, civil ou criminal, as evidências apresentadas devem se conformar às regras para evidências estabelecidas pela lei, independemente do tribunal de justiça específico onde o caso será julgado. Para obter admissibilidade da evidência, recomenda-se que as organizações garantam que seus procedimentos operacionais estejam em conformidade com qualquer norma ou código de conduta publicado para produção de evidência admissível.

73 Gerenciamento de risco refere-se à análise das ameaças, impactos e vulnerabilidades da informação e das instalações de processamento da informação e da probabilidade de sua ocorrência. Análise de risco é o processo de identificação, controle e maximização ou eliminação dos riscos de segurança que possam, a um custo aceitável, afetar os sistemas de informação.

74 A análise crítica periódica dos riscos de segurança e dos controles implementados deve, entre outros, confirmar que os controles permanecem eficientes e adequados.

75 Análises críticas devem ser executadas em níveis de profundidade distintos e se apóiam nas análises de riscos anteriormente realizadas. As probabilidades de falhas são embasadas, entre outros, nas ameaças e vulnerabilidades mais frequentes e nos controles implementados.

76 A relevância de qualquer controle é determinada pelos riscos específicos a que os patrocinadores estão expostos.

A continuidade do negócio objetiva não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos. Com base nas normas ISO 27001, ISO 27002, ISO 27005 e ISO 15999, julgue os itens seguintes.

77 Pela combinação entre ações de prevenção e de recuperação, trata-se a interrupção causada por inconsistências e falhas da segurança que podem ser resultantes de controles de acesso, desastres naturais, acidentes, falhas de equipamentos e ações intencionais.

78 O desenvolvimento e a manutenção da continuidade do negócio deve ser sustentado por um processo de gestão que permeie toda a organização. A gestão da continuidade do negócio deve estar incorporada aos processos e à estrutura da organização.

79 A análise do risco é realizada sobre os eventos que possam causar interrupções nos processos do negócio e auxiliam na determinação de seus impactos em termos de escala de dano e em relação ao período de recuperação. Nessa análise, devem-se considerar os processos de negócio impactados, limitando-se aos recursos, sem considerar as instalações de processamento de dados.

80 No caso de ocorrerem interrupções ou falhas em processos críticos, devem-se executar planos de continuidade para recuperar as operações do negócio, em conformidade com os requisitos de segurança da informação.

A respeito de ataques a redes de computadores e de incidentes de segurança, julgue os itens de **81** a **85**.

81 O incidente denominado DDoS deve ser tratado de maneira diferente de outros tipos de incidente de segurança, pois dificilmente um *firewall* ou IDS gerará *log.* Sua notificação de incidente deve informar o cabeçalho e o conteúdo completos da mensagem recebida pelo usuário.

82 Um ataque de negação de serviço (DoS) não é uma invasão do sistema e objetiva tornar os recursos de um sistema indisponíveis para seus utilizadores. O ataque tenta indisponibilizar páginas hospedadas em servidores *web* e produz como efeito uma invalidação por sobrecarga.

83 No *phishing*, diversas máquinas zumbis comandadas por um mestre fazem requisições ao mesmo tempo, gerando sobrecarga do recurso atacado, o que pode levar a máquina servidora a reiniciar ou a travar.

84 No *ping flood*, o atacante sobrecarrega o sistema vítima com pactos ICMP *echo request* (pacotes ping). Para o ataque ser bem sucedido, o atacante deve possuir maior largura de banda que a vítima, que, ao tentar responder aos pedidos, irá consumir a sua própria largura de banda, impossibilitando-a de responder a pedidos de outros utilizadores. Uma das formas de prevenir esse tipo de ataque é limitar o tráfego de pacotes ICMP *echo request.*

85 No *syn flood* ou ataque *syn*, o atacante envia uma sequência de requisições *syn* para um sistema-alvo visando uma sobrecarga direta na camada de transporte e indireta na camada de aplicação do modelo OSI.

Com relação a *malwares*, julgue os próximos itens.

86 Um *adware* difere de um *spyware* pela intenção. O primeiro é projetado para monitorar atividades de um sistema e enviar informações coletadas para terceiros, e o segundo é projetado especificamente para apresentar propagandas.

87 O cavalo de troia (*trojan horse*) não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser executado para se propagar. Sua propagação se dá por meio da exploração de vulnerabilidades existentes ou de falhas na configuração de *software* instalados em computadores.

88 Ao se executar um programa previamente infectado — como, por exemplo, ao se abrir arquivo anexado a *e-mail* ou ao se instalar programas de procedência duvidosa ou desconhecida —, um vírus pode infectar o computador. Um vírus de macro é parte de um arquivo normalmente manipulado por algum aplicativo que utiliza macros e que, para ser executado, necessita que o arquivo que o contém esteja aberto para que ele execute uma série de comandos automaticamente e infecte outros arquivos no computador.

89 Um *worm* pode realizar diversas funções maliciosas, como a instalação de *keyloggers* ou *screenloggers*, o furto de senhas e outras informações sensíveis, como números de cartões de crédito, a inclusão de *backdoors*, para permitir que um atacante tenha total controle sobre o computador, e a alteração ou destruição de arquivos.

90 O *worm* costuma ser apenas um único arquivo que necessita ser executado para que infecte o computador destinatário e, de modo distinto do vírus ou do cavalo de troia, não costuma infectar outros arquivos e nem propagar, automaticamente, cópias de si mesmo.

Com relação a segurança de redes de computadores, julgue os itens a seguir.

91 A política de segurança define o que deve ser feito para proteger a informação, seja ela armazenada ou esteja em trânsito.

92 É recomendável que a política de segurança determine medidas específicas a serem implementadas e a forma de implementá-las.

93 A defesa em profundidade é uma arquitetura de defesa que estratifica as medidas de proteção, obtendo níveis de contenção entre a rede externa e a rede interna que se deseja proteger.

94 O estabelecimento de um perímetro da rede visa à separação entre a rede externa e a rede interna que se deseja proteger.

95 A defesa em profundidade recomenda que o perímetro da rede tenha múltiplos pontos de interface entre a rede externa e a interna.

Acerca dos dispositivos de segurança de redes de computadores, julgue os itens subsequentes.

96 Um *proxy*, ao agir no lugar do cliente ou do usuário para prover acesso a um serviço de rede, protege tanto o cliente quanto o servidor de uma conexão direta.

97 IDS e IPS são sistemas que protegem a rede de intrusões, diferindo no tratamento dado quando uma intrusão é detectada. Especificamente, o IPS limita-se a gerar alertas e ativar alarmes, e o IDS executa contramedidas, como interromper o fluxo de dados referente à intrusão detectada.

98 A ocorrência de falsospositivos normalmente acarreta consequências mais graves para as redes que utilizam IDS do que para aquelas que usam IPS.

99 A inspeção de estados visa determinar se um pacote pode entrar ou sair de uma rede, tendo por base a verificação de informações localizadas no cabeçalho do pacote.

100 Tanto na filtragem quanto na inspeção que se baseiam em estado, a informação de estado é mantida em uma tabela até que a conexão se encerre (como no tráfego TCP) ou ao atingir um limite de tempo (como no caso de tráfego TCP, UDP e ICMP).

Conjunto I

```
allow tcp from any to any
deny tcp from any to any 80
deny tcp from any to any 21
```

Conjunto II

```
permit tcp any any eq 22
permit tcp any any eq 25
permit tcp any any eq 53
permit tcp any any eq 80
permit tcp any any eq 110
permit tcp any any eq 443
permit udp any any eq 53
permit icmp any any
```

A respeito de *firewalls*, e considerando os conjuntos de regras acima e que os serviços estejam utilizando as suas portas *default*, julgue os itens que seguem.

101 As regras do conjunto I permitem todo o tráfego TCP, exceto para as portas 21 e 80.

102 O conjunto II implementa uma política para DNS que permite consultas, mas bloqueia transferências de zona.

103 Os tráfegos http e HTTPS são permitidos pelas regras dos conjuntos I e II.

104 Os dois conjuntos apresentados permitem correio eletrônico.

105 Apenas o conjunto II permite o tráfego ICMP.

Acerca dos sistemas criptográficos, julgue os itens de **106** a **109**.

106 Enquanto uma cifra de bloco atua em um *bit* ou *byte* do fluxo de dados por vez, uma cifra de fluxo atua sobre um conjunto de caracteres de texto em claro, que são tratados como um todo e usados para produzir um criptograma de igual comprimento.

107 Nos sistemas simétricos, os usuários usam a mesma chave para cifrar e decifrar mensagens, enquanto nos sistemas assimétricos mais de uma chave é usada.

108 Em um sistema de chaves assimétricas, cada usuário tem um par de chaves, sendo que uma delas é mantida secreta e a outra é pública.

109 Nos sistemas assimétricos, as chaves são escolhidas de forma que se uma mensagem é cifrada usando uma das chaves, o criptograma correspondente é decifrado utilizando a outra chave do par.

Com relação às cifras criptográficas, julgue os itens seguintes.

110 O padrão DES, que utiliza chave de 64 *bits*, não é mais recomendado, considerando a sua vulnerabilidade a ataques de força bruta.

111 O padrão 2DES consiste em duas rodadas consecutivas do DES, com duas chaves distintas de 56 *bits*, tendo assim uma chave equivalente a 112 *bits*.

112 O padrão 3DES com duas chaves consiste em três rodadas consecutivas do DES, com chaves distintas de 56 *bits*, sendo que a primeira e a última usam a mesma chave, tendo assim uma chave equivalente a 112 *bits*.

113 O padrão AES define uma cifra na qual os comprimentos do bloco e da chave podem ser especificados independentemente para 128 *bits*, 192 *bits* ou 256 *bits*. Os três tamanhos de chave determinam vários parâmetros da cifra, como número de rodadas, e podem ser usados limitando o bloco a 128 *bits*.

No que concerne a sistemas de chave pública, assinatura e certificação digital, julgue os itens subsequentes.

114 Sejam A e B usuários de um sistema de chaves públicas, cada um conhecendo as próprias chaves e a chave pública do outro. Se A cifra uma mensagem com a chave pública de B e cifra o resultado com a própria chave privada, somente B consegue decifrar a mensagem cifrada por A.

115 Na assinatura digital RSA, calcula-se um *hash* da mensagem a ser assinada, que é cifrado usando a chave pública de quem assina, gerando a assinatura que é concatenada com a mensagem original. Na verificação, decifra-se a assinatura usando a chave pública de quem assinou e calcula-se o *hash* da mensagem, sendo a mensagem considerada válida se tanto a chave quanto o *hash* coincidirem.

116 Um certificado digital é a chave pública de um usuário assinada por uma autoridade certificadora confiável.

117 Com o uso de sistemas de chave pública, juntamente com assinatura e certificação digital, consegue-se obter confidencialidade, integridade, autenticidade, não repúdio e disponibilidade.

Com relação a VPN, julgue os itens que se seguem.

118 Uma VPN é uma conexão estabelecida sobre uma infraestrutura pública ou compartilhada, usando tecnologias de tunelamento e criptografia para manter seguros os dados trafegados.

119 Apesar de ser uma opção disponível, não se recomenda o uso de autenticação junto com cifração em VPNs, considerando a diminuição de desempenho.

120 Preferencialmente, as VPNs são implementadas sobre protocolos de rede orientados à conexão como o TCP.