



Nome do candidato:

Número do documento de identidade:

Número de inscrição:

Sala:

Sequencial:

CONCURSO PÚBLICO NÍVEL SUPERIOR

Cargo: ANALISTA DE TECNOLOGIA DA INFORMAÇÃO

PERFIL XI

AUDITOR DE SISTEMAS

Aplicação: 21/5/2006



LEIA COM ATENÇÃO AS INSTRUÇÕES ABAIXO.

- 1 Ao receber este caderno, confira inicialmente os seus dados pessoais transcritos acima. Em seguida, verifique se ele contém cento e vinte itens, correspondentes às provas objetivas, corretamente ordenados de 1 a 120, seguidos da prova discursiva.
- 2 Caso os dados pessoais constantes neste caderno não correspondam aos seus, ou, ainda, caso o caderno esteja incompleto ou tenha qualquer defeito, solicite ao fiscal de sala mais próximo que tome as providências cabíveis.
- 3 O espaço para rascunho da prova discursiva é de uso opcional; não contará, portanto, para efeito de avaliação.
- 4 Não utilize lápis, lapiseira, borracha e(ou) qualquer material de consulta que não seja fornecido pelo CESPE/UnB.
- 5 Não serão distribuídas folhas suplementares para rascunho nem para texto definitivo.
- 6 Não se comunique com outros candidatos nem se levante sem autorização do chefe de sala.
- 7 Nas provas objetivas, recomenda-se não marcar ao acaso: em cada item, se a resposta divergir do gabarito oficial definitivo, o candidato receberá pontuação negativa, conforme consta em edital.
- 8 Na prova discursiva, não será avaliado texto escrito a lápis, texto escrito em local indevido ou texto que tenha identificação fora do local apropriado.
- 9 A duração das provas é de **quatro horas e trinta minutos**, já incluído o tempo destinado à identificação — que será feita no decorrer das provas —, ao preenchimento da folha de respostas e à transcrição do texto definitivo da prova discursiva para a folha de texto definitivo.
- 10 Você deverá permanecer obrigatoriamente em sala por, no mínimo, uma hora após o início das provas.
- 11 Ao terminar as provas, chame o fiscal de sala mais próximo, devolva-lhe a sua folha de respostas e a folha de texto definitivo da prova discursiva e deixe o local de provas.
- 12 A desobediência a qualquer uma das determinações constantes no presente caderno, na folha de respostas ou na folha de texto definitivo da prova discursiva poderá implicar a anulação das suas provas.

AGENDA

- I 23/5/2006, após as 19 h (horário de Brasília) – Gabaritos oficiais preliminares das provas objetivas: Internet — www.cespe.unb.br/concursos/dataprev2006.
- II 24 e 25/5/2006 – Recursos (provas objetivas): exclusivamente no Sistema Eletrônico de Interposição de Recurso, Internet — www.cespe.unb.br/concursos/dataprev2006, mediante instruções e formulários que estarão disponíveis nesse endereço.
- III 13/6/2006 – Resultados final das provas objetivas e provisório da prova discursiva: Diário Oficial da União e Internet — www.cespe.unb.br/concursos/dataprev2006.
- IV 14 e 15/6/2006 – Recursos (prova discursiva): em locais e horários que serão informados na divulgação do resultado provisório.
- V 27/6/2006 – Resultados finais da prova discursiva e do concurso: locais mencionados no item III.

OBSERVAÇÕES

- Não serão objeto de conhecimento recursos em desacordo com o item 11 do Edital n.º 1/2006 – DATAPREV, de 13/3/2006.
- Informações adicionais: telefone 0(XX) 61 3448-0100; Internet — www.cespe.unb.br/concursos/dataprev2006.
- É permitida a reprodução deste material apenas para fins didáticos, desde que citada a fonte.

ITEM	RESPOSTA	ITEM	RESPOSTA	ITEM	RESPOSTA	ITEM	RESPOSTA	ITEM	RESPOSTA	ITEM	RESPOSTA	ITEM	RESPOSTA	ITEM	RESPOSTA
1	C E	16	C E	31	C E	46	C E	61	C E	76	C E	91	C E	106	C E
2	C E	17	C E	32	C E	47	C E	62	C E	77	C E	92	C E	107	C E
3	C E	18	C E	33	C E	48	C E	63	C E	78	C E	93	C E	108	C E
4	C E	19	C E	34	C E	49	C E	64	C E	79	C E	94	C E	109	C E
5	C E	20	C E	35	C E	50	C E	65	C E	80	C E	95	C E	110	C E
6	C E	21	C E	36	C E	51	C E	66	C E	81	C E	96	C E	111	C E
7	C E	22	C E	37	C E	52	C E	67	C E	82	C E	97	C E	112	C E
8	C E	23	C E	38	C E	53	C E	68	C E	83	C E	98	C E	113	C E
9	C E	24	C E	39	C E	54	C E	69	C E	84	C E	99	C E	114	C E
10	C E	25	C E	40	C E	55	C E	70	C E	85	C E	100	C E	115	C E
11	C E	26	C E	41	C E	56	C E	71	C E	86	C E	101	C E	116	C E
12	C E	27	C E	42	C E	57	C E	72	C E	87	C E	102	C E	117	C E
13	C E	28	C E	43	C E	58	C E	73	C E	88	C E	103	C E	118	C E
14	C E	29	C E	44	C E	59	C E	74	C E	89	C E	104	C E	119	C E
15	C E	30	C E	45	C E	60	C E	75	C E	90	C E	105	C E	120	C E

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

CONHECIMENTOS BÁSICOS

Texto para os itens de 1 a 7

Em numerosas reportagens de jornais e televisões, temos lido que as emissoras de TV defendem a escolha do padrão japonês de modulação da TV digital (ISDB), porque este seria o único padrão que lhes permitiria fazer transmissão para recepção móvel, usando a banda do espectro eletromagnético reservada para o UHF. No caso do padrão europeu (DVB), por exemplo, a transmissão para recepção móvel teria de usar a banda reservada para a telefonia celular, o que incluiria as empresas de telefonia no núcleo central da operação de TV. Recosas dessa concorrência, as emissoras, então, preferem a modulação japonesa. Antes de prosseguir, algumas ressalvas:

- ▶ o padrão de modulação brasileiro, desenvolvido pela PUC-RS, conhecido como SORCER, também permite a transmissão para recepção móvel. Portanto, mesmo aceitando o argumento das emissoras, poderíamos adotar uma modulação com tecnologia brasileira;
- ▶ todos os padrões de modulação (japonês, europeu, norte-americano e brasileiro, além do chinês, que está em desenvolvimento) permitem transmitir em SDTV, EDTV e HDTV, ou seja, para essa questão específica, a escolha da modulação é indiferente;
- ▶ igualmente, todos os padrões permitem que se desenvolva uma série de serviços interativos, como governo eletrônico, *e-learning*, *e-bank*, telemedicina etc. Novamente, nessa questão específica, a escolha da modulação é indiferente.

Gustavo Gindre, coordenador-geral do Instituto de Estudos e Projetos em Comunicação e Cultura (INDECS). Internet: <www.oppi.org.br> (com adaptações).

Julgue os itens a seguir, a respeito das idéias e das estruturas lingüísticas do texto.

- 1 De acordo com o texto, é indiferente a escolha de um padrão de modulação para TV digital, porque todos permitem a transmissão para recepção móvel.
- 2 Preservam-se o sentido e a correção gramatical, se for empregada a preposição **em** antes de “que” (l.4).
- 3 A forma verbal “usando” (l.5) se refere à expressão “o único padrão” (l.4).
- 4 Na expressão “o que” (l.9), o termo sublinhado retoma coesivamente o trecho “No caso do padrão europeu (...) telefonia celular” (l.6-9).
- 5 Com o emprego do termo “também” (l.14) soma-se mais um argumento à idéia de que a transmissão para recepção móvel não é exclusividade do padrão japonês de modulação.
- 6 Nas linhas de 13 a 27, a primeira palavra de cada ressalva pode ser reescrita com letra inicial maiúscula sem prejuízo da correção gramatical.
- 7 Seria sintaticamente correto substituir-se o trecho “que se desenvolva uma série de serviços interativos” (l.23-24) por: que uma série de serviços interativos seja desenvolvida.

1 Inclusão digital é, entre outras coisas, alfabetização
digital, ou seja, é a aprendizagem necessária ao indivíduo
para circular e interagir no mundo das mídias digitais como
4 consumidor e produtor de seus conteúdos e processos. Para
isso, computadores conectados em rede e *software* são
instrumentos técnicos imprescindíveis. Mas são apenas isso,
7 suportes técnicos às atividades a serem realizadas a partir
deles no universo da educação, no mundo do trabalho, nos
novos cenários de circulação das informações e nos
10 processos comunicativos.

Dizer que inclusão digital é somente oferecer
computadores seria análogo a afirmar que as salas de aula,
13 cadeiras e quadro-negro garantiriam a escolarização e o
aprendizado dos alunos. Sem a inteligência profissional dos
professores e sem a sabedoria de uma instituição escolar que
16 estabelecesse diretrizes de conhecimento e trabalho nesses
espaços, as salas seriam inúteis. Portanto, a oferta de
computadores conectados em rede é o primeiro passo, mas
19 não é o suficiente para se realizar a pretensa inclusão digital.

Elizabeth Rondelli. *Revista I-Coletiva*, 24/6/2003 (com adaptações).

Acerca da organização das idéias e das estruturas lingüísticas no
texto acima, julgue os itens subseqüentes.

- 8 Do ponto de vista da construção textual, a expressão
“alfabetização digital” (l.1-2) e o segmento “a aprendizagem
necessária ao indivíduo (...) processos” (l.2-4) estabelecem
uma relação semântica de identificação com “Inclusão
digital” (l.1).
- 9 A expressão “ou seja” (l.2) introduz uma idéia retificadora
do que foi dito na oração anterior.
- 10 As palavras “conteúdos” e “inúteis” são acentuadas com
base na mesma regra de acentuação gráfica.
- 11 A conjunção “Mas” (l.6) inicia um período cujo sentido
aponta para a insuficiência dos suportes técnicos como
recursos capazes de promover o aprendizado na educação,
no trabalho e nos meios de circulação das informações.
- 12 Mantêm-se a correção gramatical e o sentido original do
texto, se o vocábulo “às” (l.7) for substituído por a.
- 13 Na linha 15, o vocábulo “que” tem como referente semântico
o termo “sabedoria”.

1 Sendo a informação um bem que agrega valor a uma
empresa ou a um indivíduo, é preciso fazer uso de recursos
de tecnologia da informação de maneira apropriada, ou seja,
4 é preciso utilizar ferramentas, sistemas ou outros meios que
façam das informações um diferencial competitivo.

Além disso, é necessário buscar soluções que
7 tragam bons resultados, mas que tenham o menor custo
possível. A questão é que não existe fórmula mágica para se
determinar como utilizar da melhor maneira as informações.
10 Tudo depende da cultura, do mercado, do segmento e de
outros aspectos de uma empresa. As escolhas precisam ser
bem feitas. Do contrário, gastos desnecessários ou, ainda,
13 perda de desempenho podem ocorrer. Por exemplo, se uma
empresa renova sua base de computadores comprando
máquinas com processadores velozes, muita memória e placa
de vídeo 3D para serem utilizadas por empregados que
16 apenas precisam acessar a Internet ou trabalhar com pacotes
de escritório, a companhia faz gastos desnecessários.

19 Comprar máquinas de boa qualidade não significa
comprar as mais caras, mas aquelas que possuam os recursos
necessários. Por outro lado, imagine que uma empresa tenha
22 compre computadores com vídeo integrado à placa-mãe e
monitor de 15 polegadas para profissionais que trabalham
com Autocad. Para estes, o ideal é comprar computadores
25 que suportem aplicações pesadas e um monitor de, pelo
menos, 17 polegadas. Máquinas mais baratas certamente
conseguiriam rodar o Autocad, porém com lentidão, e o
28 monitor com área de visão menor daria mais trabalho aos
profissionais. Nesse caso, a aquisição das máquinas tem
reflexo direto no desempenho dos empregados. Por isso, é
31 preciso saber quais as necessidades de cada usuário.

Emerson Alecrim. Internet: <www.infowester.com> (com adaptações).

De acordo com as idéias e os aspectos sintático-semânticos do
texto acima, julgue os próximos itens.

- 14 Nas linhas 1 e 2, a conjunção “ou” liga dois termos que se
alternam e não se excluem: “a uma empresa” e “a um
indivíduo”.
- 15 Segundo o texto, as empresas, na busca de soluções para
seus problemas, precisam em primeiro lugar usar recursos
de tecnologia da informação que tenham o menor custo.
- 16 Se determinada empresa adquirir equipamentos e
suprimentos de informática sem levar em consideração o
melhor aproveitamento desses recursos por seus
empregados, ela, necessariamente, terá gastos e,
conseqüentemente, haverá perda de desempenho.
- 17 As expressões “de boa qualidade” (l.19) e “que possuam os
recursos necessários” (l.20-21) se referem a “máquinas”
(l.19).
- 18 Com o emprego das formas verbais “conseguiriam” (l.27) e
“daria” (l.28), sugere-se, no texto, que certamente há
problemas no uso de equipamentos de informática mais
baratos que não atendam às necessidades de trabalho dos
usuários.

Julgue os itens seguintes, referentes a redação de
correspondências oficiais.

- 19 O memorando é a comunicação feita apenas entre unidades
administrativas de mesmo órgão que estejam
hierarquicamente no mesmo nível.
- 20 O vocativo a ser empregado em comunicações dirigidas aos
chefes dos poderes da República é Ilustríssimo Senhor.

This text refers to items 21 through 30

1 When we think of the people who make our lives
miserable by hacking into computers, or spreading malicious
viruses, most of us imagine an unpopular teenage boy,
4 brilliant but geeky, venting his frustrations* from the safety
of a suburban bedroom.

Actually, these stereotypes are just that —
7 stereotypes — according to Sarah Gordon, an expert in
computer viruses and security technology, and a Senior
Research Fellow with Symantec Security Response. Since
10 1992, Gordon has studied the psychology of virus writers.
“A hacker or a virus writer is just as likely to be the guy next
door to you,” she says, “or the kid at the checkout line
13 bagging your groceries. Your average hacker is not
necessarily some Goth type dressed entirely in black and
sporting a nose ring: she may very well be a 50-year-old
16 female”.

The virus writers Gordon has come to know have
varied backgrounds; while predominately male, some are
19 female. Some are solidly academic, while others are athletic.
Many have friendship with members of the opposite sex,
good relationships with their parents and families; most are
22 popular with their peers. They don’t spend all their time in
the basement. One virus writer volunteers in his local library,
working with elderly people. One of them is a poet and a
25 musician, another is an electrical engineer, and others work
for a university quantum physics department.

Hackers and virus writers are actually very different,
28 distinct populations. “Hackers tend to have a more thorough
knowledge of systems and a more highly developed skill
set,” Gordon says, “whereas virus writers generally take a
shallower approach to what they’re doing.” Hackers tend to
31 have a much deeper knowledge of individual applications
and are still regarded as being somewhat “sexy” in today’s
34 counterculture, while virus writing is looked down upon,
mostly for its random damage and lack of required skill.

* **venting his frustrations** – getting rid of feelings of anger or resentment.

Neil Anderson. *Active skills for reading: Book 4*.
Thomson/Heinle, 2002, p. 17 (with adaptations).

Based on the text above, judge the following items.

- 21 Research confirms common belief: most hackers are teenage boys.
- 22 Sarah Gordon’s research main focus was on stereotypes.
- 23 Sarah Gordon has been studying virus writers’ behavior for more than a decade.
- 24 Your neighbor could very well be a hacker.
- 25 An average hacker would never be a female in her fifties.
- 26 There seems to be nothing in particular that could easily identify a virus writer.
- 27 The virus writers may spend some time in the basement.
- 28 Virus writers know more about computers than hackers.

In the text,

- 29 “parents” (l.21) refers to **mother and father**.
- 30 “volunteers” (l.23) is a **noun**.

Risk identification is a systematic attempt to specify threats to a project plan (estimates, schedule, resource loading, etc.). By identifying known and predictable risks, the project manager takes a first step toward avoiding them when possible and controlling them when necessary.

There are two distinct types of risks for each of the categories: generic risks and product-specific risks. Generic risks are a potential threat to every software project. Product-specific risks can only be identified by those with a clear understanding of the technology, the people, and the environment that is specific to the project at hand. To identify product-specific risks, the project plan and the software statement of scope are examined and an answer to the following question is developed: what special characteristics of this product may threaten our project plan?

R. S. Pressman. *Software engineering – A practitioner’s approach*.
4th Edition, The McGraw-Hill Companies, Inc., 1997 (with adaptations).

From the text above, it can be concluded that

- 31 the identification of risks is a hazardous attempt to prevent menaces to the project plan.
- 32 systematic identification helps to avoid foreseen risks.
- 33 the project manager is in charge of controlling and forestalling risks.
- 34 generic risks and product-specific risks both refer to software projects.
- 35 the project plan and the software statement of scope are product-specific risks.

In a small software development project a single person can analyze requirements, perform design, generate code, and conduct tests. As the size of a project increases, more people must become involved — we can rarely afford the luxury of approaching a ten person-year effort with one person working for ten years!

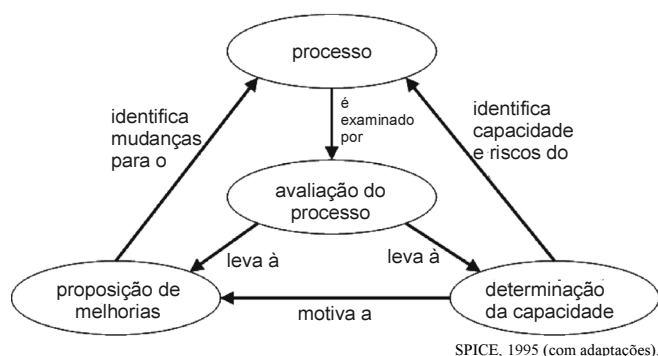
There is a common myth that is still believed by many managers who are responsible for software development effort: “if we fall behind schedule, we can always add more programmers and catch up later in the project”.

Idem, ibidem (with adaptations).

Based on the text above, judge the following items.

- 36 Small software projects usually require just one person to perform different tasks.
- 37 The bigger the project, the fewer people are demanded.
- 38 We can often afford to have a ten person-year effort or one person working for ten years when developing a software project.
- 39 A lot of project managers tend to believe in the same myth.
- 40 To update a software project is just a matter of hiring more people.

CONHECIMENTOS ESPECÍFICOS



A figura acima apresenta um modelo conceitual aplicável à melhoria de processos de *software*. Julgue os itens a seguir acerca das informações apresentadas, dos conceitos de análise de processos e de auditoria de sistemas de informação.

- 41 O foco da aplicação dos elementos do modelo conceitual acima apresentado tem como cenário a avaliação de capacidade de processos de produção de *software*, não sendo de aplicação genérica.
- 42 Mesmo consideradas as restrições decorrentes do princípio da segregação de responsabilidades, a execução do conjunto das três atividades apresentadas nas elipses da parte inferior da figura poderia ser atribuída, sem conflito de escopo, procedimentos, normas e regras de auditoria, a uma mesma equipe de auditoria de processos.
- 43 A avaliação de processos de TI torna-se mais objetiva quando se adota um modelo de referência para comparação, o que está ficando cada vez mais difícil de conseguir-se, devido ao aperfeiçoamento cada vez mais intenso dos processos nas organizações.
- 44 Durante a avaliação do processo no cenário acima, o auditor deve coletar evidências exaustivas de que todas as atividades pertinentes foram executadas de acordo com os controles prescritos, sob pena de tornar a auditoria ineficaz.
- 45 A proposição de melhorias para um processo ou sistema deve ser acatada unilateralmente pelo auditado, dadas a autoridade e a competência incontestáveis do auditor.
- 46 Modelos correntes de auditoria de processos de produção de *software* indicam que a determinação da capacidade de processos deve produzir valores em uma escala graduada formada por níveis contíguos, sendo comum o emprego de uma escala de capacidade que varie de 0 a 5.
- 47 O conceito de risco apresentado na figura relaciona-se mais diretamente aos processos de negócios da organização auditada e menos aos processos da auditoria.
- 48 Uma auditoria, mesmo que realizada de forma satisfatória, nunca consegue eliminar a materialização de riscos nos processos e sistemas auditados.



Cerqueira e Martins. Auditoria de sistemas de gestão.

A figura acima, cujo título é **Dois Grandes Mentirosos?**, apresenta um cenário para discussão acerca dos conceitos, normas e técnicas de auditoria. Acerca desse tema, julgue os itens a seguir.

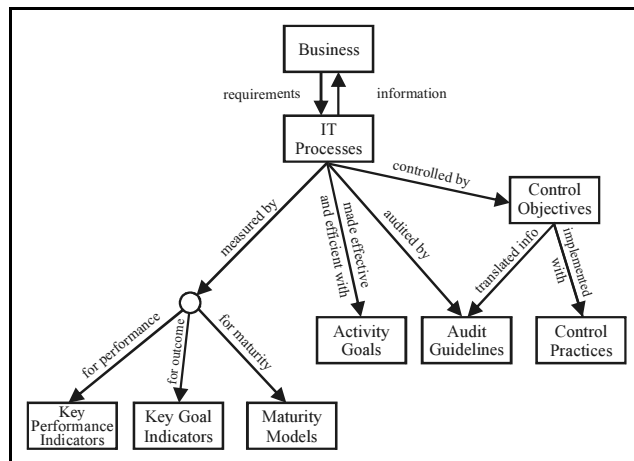
- 49 Não é papel central do auditor prover auxílio ao auditado.
- 50 Não é atitude adequada do auditado receber elogiosamente o auditor.
- 51 A atitude do auditor perante o auditado deve ser imparcial, inflexível, impessoal e independente.
- 52 Durante o relacionamento com o auditado, a subjetividade, a capacidade de argumentação e a atitude crítica não são atributos desejáveis de um auditor.
- 53 A imediata suspensão da auditoria deve ser feita quando o auditado demonstra comportamento negativo, como pânico por associação à sindicância, fornecimento, em manuscrito, de evidências objetivas que não estavam originalmente vinculadas aos documentos solicitados e adoção de postura agressiva em relação aos métodos de auditoria.
- 54 Os objetivos do controle externo, conforme definidos no âmbito da legislação federal sobre controle e auditoria, são idênticos aos da auditoria interna.
- 55 Antes do preparo do relatório final sobre a atividade de auditoria, o auditado sempre deve receber uma versão preliminar do relatório com vistas à confirmação, esclarecimentos e mesmo retificações, a fim de se dirimirem todas as dúvidas ou falhas que tenham ocorrido durante a auditoria.
- 56 Tem de constar no relatório final sobre a atividade de auditoria pública, as seguintes informações, entre outras: declaração de escopo e objetivo da auditoria, identificação da equipe, descrição das não-conformidades encontradas, julgamento acerca da importância e do impacto das não-conformidades detectadas, assinatura de concordância plena do auditado com os resultados da auditoria e assinatura do auditor líder.



Internet: <http://www.21tb.com> (com adaptações).

Considerando a figura acima, que apresenta um cenário pictórico de aplicação de uma regra de auditoria chamada 5W+1H+*Show Me*, julgue os itens abaixo acerca dos conceitos, normas e técnicas de auditoria.

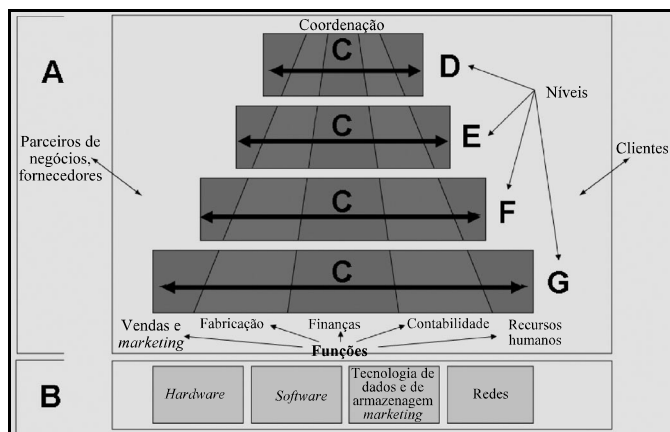
- 57** É objetivo fundamental da auditoria a busca de impropriedades e irregularidades, e a regra de auditoria mencionada deve ser aplicada primariamente para provar a existência dessas condições.
- 58** A opinião do auditor líder é um aspecto abordado explicitamente em normas e técnicas de auditoria, e uma delas se refere à seleção das áreas a serem investigadas, bem como à indicação da equipe de auditoria mais adequada à realização da atividade.
- 59** Em uma atividade de auditoria em equipe, espera-se que o responsável por assinar o relatório final, o auditor líder, não seja o único responsável pela produção das evidências de não-conformidades junto à organização auditada.
- 60** As impropriedades e irregularidades relatadas ao final da auditoria devem decorrer do alcance da decisão unânime entre os que compõem a equipe de auditoria.
- 61** Todos os fatos e evidências materiais coletados para dar suporte à elaboração do relatório de auditoria precisam ser fornecidos antes do início da fase de estudo e avaliação de controles, sendo inadequado o fornecimento de novas informações e documentos após o início dos trabalhos de campo.
- 62** A teoria da agência provê justificativa conceitual ou filosófica para a realização de auditorias, ao definir que uma organização é representada pelo conjunto de seus contratos entre agentes com interesses próprios, o que exige supervisão.



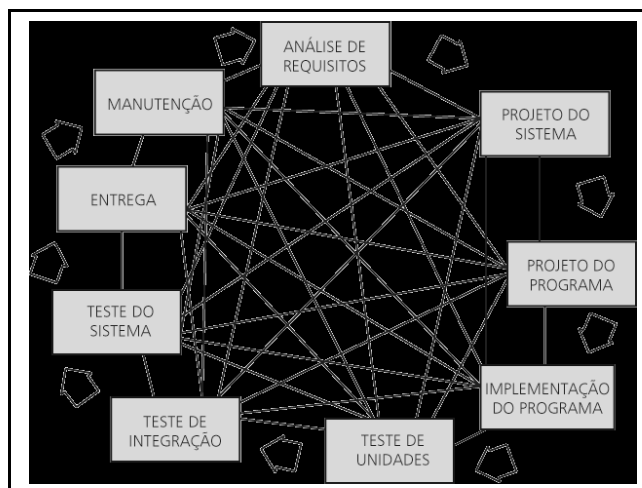
ITGI, COBIT 4.0.

A figura acima apresenta um esquema para definição de guias de auditoria de TI. Julgue os itens seguintes, acerca dos conceitos apresentados no âmbito da auditoria de sistemas e seu papel nas organizações.

- 63** São exemplos de áreas de processos de TI: o planejamento e a organização da área; a aquisição e a implementação de soluções; a entrega de serviços; o suporte ao usuário; o monitoramento e a avaliação da aderência aos controles.
- 64** As organizações estão, contínua e inevitavelmente, aperfeiçoando seus processos de negócios e de TI. Justifica-se, nesse cenário, uma abordagem evolutiva de processos, que, no modelo acima, apresenta-se por meio de: adoção de modelos de maturidade; orientação a projetos suportados pela existência de indicadores de metas; orientação a operações suportadas pela existência de indicadores de desempenho.
- 65** No modelo apresentado, os objetivos de controle são mais específicos que as práticas de controle.
- 66** Os processos de negócio, por princípio, precisam adequar-se às restrições ou requisitos dos processos de TI existentes em uma organização.



Laudon e Laudon. *Gerência de sistemas de informação*.



Pfleeger. *Engenharia de software*.

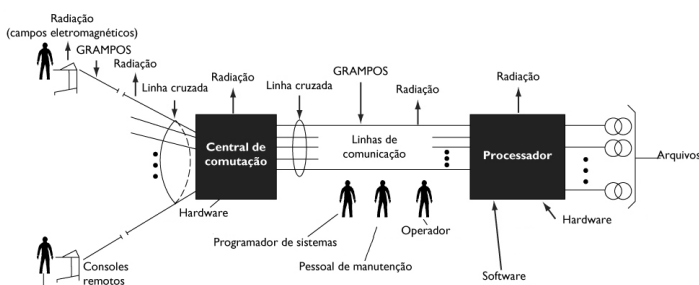
A figura acima apresenta um esquema de organização de empresas, em que existem elementos numerados de A a G, denotando níveis ou focos de análise. O papel dos elementos C é prover um fluxo de integração entre atividades desempenhadas por trabalhadores da empresa. Acerca dos elementos apresentados, julgue os itens seguintes.

- 67 Tecnologia da informação é melhor associada ao elemento B, em detrimento de A.
- 68 A arquitetura da informação corporativa é melhor associada ao conjunto dos elementos C, em detrimento de B.
- 69 O conjunto dos sistemas de informação da organização é mais bem associado ao elemento C que ao elemento B.
- 70 C representa os processos de TI da organização.
- 71 Em alguns casos, visando a economicidade e desburocratização, o auditor pode sugerir que as atividades em C sejam divididas entre trabalhadores pertencentes a níveis e funções distintas.
- 72 Em alguns casos, visando a melhor segregação de responsabilidades, o auditor pode sugerir que as atividades em C sejam agrupadas para realização com uma quantidade menor de trabalhadores.
- 73 Entre as funções apresentadas na base da pirâmide, a mais fortemente relacionada com a auditoria, em geral, é a de contabilidade, em detrimento à das finanças.
- 74 As atividades de controle interno, na organização representada, são mais adequadamente realizadas pelos recursos humanos da própria organização sob análise que pelos recursos humanos dos parceiros.
- 75 O emprego de amostragem será maior quando a auditoria for realizada no nível G que quando realizada no nível D.
- 76 A auditoria de controles gerenciais e operacionais de TI será maior no nível B que no nível A.
- 77 O emprego de testes de controles de operação de *mainframes* será maior no nível G que no nível B.
- 78 Durante a auditoria no uso de aplicativos de escritório, como editores de texto e planilhas, será dado maior foco aos trabalhadores do nível E que aos no nível G.
- 79 A auditoria no uso de ferramentas de *datawarehouse* e OLAP será mais intensa junto aos trabalhadores do nível D que aos do nível F.

A figura acima apresenta um ciclo de desenvolvimento comum em engenharia de sistemas de *software*, no qual o encadeamento entre as fases do desenvolvimento desses sistemas é representada por setas e linhas. Acerca dos conceitos apresentados na figura, julgue os itens que se seguem.

- 80 Quanto maior o número de linhas que interligam as diversas fases representadas, mais caótico torna-se o processo de desenvolvimento de *software*, e mais fácil se torna a sua rastreabilidade.
- 81 Em uma auditoria sobre análise, projeto, desenvolvimento e implementação de *software* e sistemas, a organização auditada deverá receber uma cópia prévia do plano de auditoria ao qual aquela será submetida, no qual estão informados as datas, os horários e as pessoas responsáveis pelo fornecimento de informações que devem estar disponíveis para a visita dos auditores.
- 82 O emprego do termo manutenção, no cenário demonstrado na figura, refere-se à manutenção integrada de sistemas de *hardware* e *software*.
- 83 No âmbito do desenvolvimento de sistemas de informação organizacionais, a análise de requisitos, no cenário apresentado, deve conter referência aos requisitos dos processos de negócios da organização.
- 84 A etapa “Projeto do Sistema” compreende o desenvolvimento completo de Sistema de informação.
- 85 O “Teste do Sistema” compreende o teste de controles de segurança da informação durante a realização de uma auditoria.
- 86 Entre as fases que consomem o maior recurso de tempo e pessoal da organização, a fase de “Manutenção” deverá ser mais custosa que a fase de “Implementação do Programa”.
- 87 O auditor deve encontrar maior número de fatos que indicam a realização de diagramas detalhados que descrevem o fluxo de troca de mensagens entre objetos computacionais junto aos trabalhadores que atuam na fase “Projeto do Programa” que na fase “Implementação do Programa”.

- 88** O auditor deve encontrar maior número de fatos que indicam a realização de testes de bancada sobre classes de um programa orientado a objetos junto aos trabalhadores envolvidos na fase de “Teste de Integração” que na fase de “Teste de Unidades”.
- 89** O auditor deve encontrar maior número de fatos que indicam a interação entre o cliente de sistemas de informação e a equipe de desenvolvimento junto aos trabalhadores envolvidos na fase de “Projeto do Sistema” que na fase de “Entrega”.
- 90** Evidências da não-implantação de controles de segurança de *software*, como ausência de documentação de modelagem de ameaças, vulnerabilidades, ataques e contra-medidas devem ser encontradas com maior frequência junto aos trabalhadores que atuam em “Teste do Sistema” que na fase de “Entrega”.
- 91** Fatos, achados e evidências da autoria de artefatos escritos em linguagens como COBOL, Java, Delphi, SQL e outras devem ser encontrados, com maior frequência, junto aos trabalhadores que atuam na fase de “Projeto do Programa” que na fase de “Implementação do Programa”.



Laudon & Laudon. Gerência de sistemas de informação.

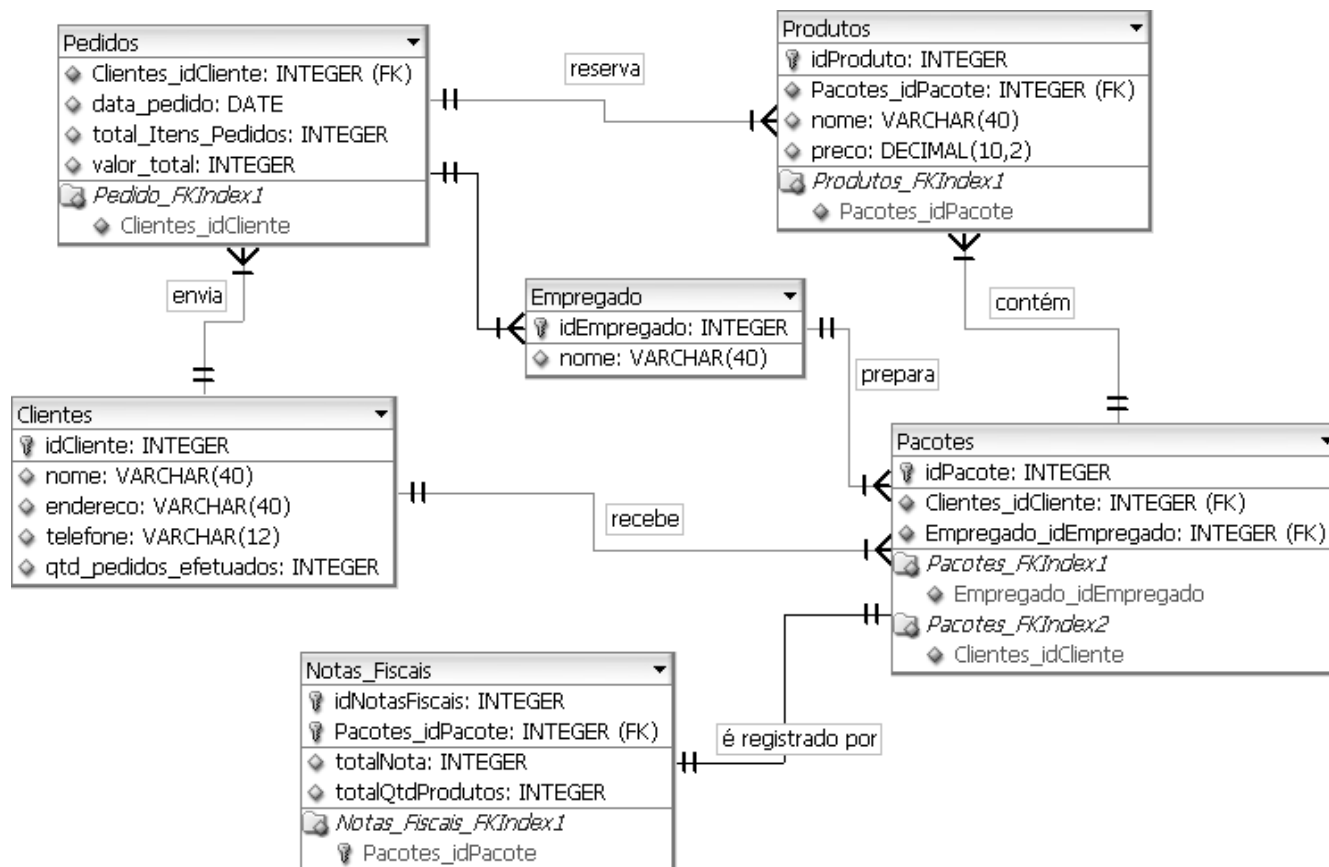
Considerando a figura acima, que apresenta um cenário para análise das vulnerabilidades em ambiente de tecnologia da informação, julgue os próximos itens.

- 92** O sistema acima descrito emprega uma arquitetura do tipo cliente-servidor, característica de sistemas de processamento distribuído.
- 93** O cenário acima apresentado aplica-se mais adequadamente a uma auditoria de controles organizacionais e operacionais que à auditoria de aquisição, desenvolvimento e manutenção de *software*.
- 94** Entre os agentes com maiores oportunidades para introduzir modificações que comprometam a segurança do sistema operacional, identifica-se o usuário, mais que o programador de sistemas.
- 95** Uma falha no elemento *hardware* da figura acima pode ser consequência bem como causa de um ataque.
- 96** A exposição das linhas de comunicação às radiações é um exemplo de vulnerabilidade do sistema.

- 97** A implantação de grampos nas linhas de comunicação entre a central de comutação e os consoles remotos é um exemplo de contra-medida.
- 98** A ausência de procedimentos de investigação sobre a conduta e o histórico prévio dos responsáveis pela manutenção e operação de sistemas como o acima é mais adequadamente chamada de ameaça que de vulnerabilidade.
- 99** A rede de telecomunicações mostrada na figura apresenta uma topologia lógica em barra e não, em estrela.
- 100** O protocolo de rede adotado na comunicação entre os usuários e os aplicativos de *software* é, provavelmente, o protocolo TCP/IP, adotando o sistema uma arquitetura de *intranet*.

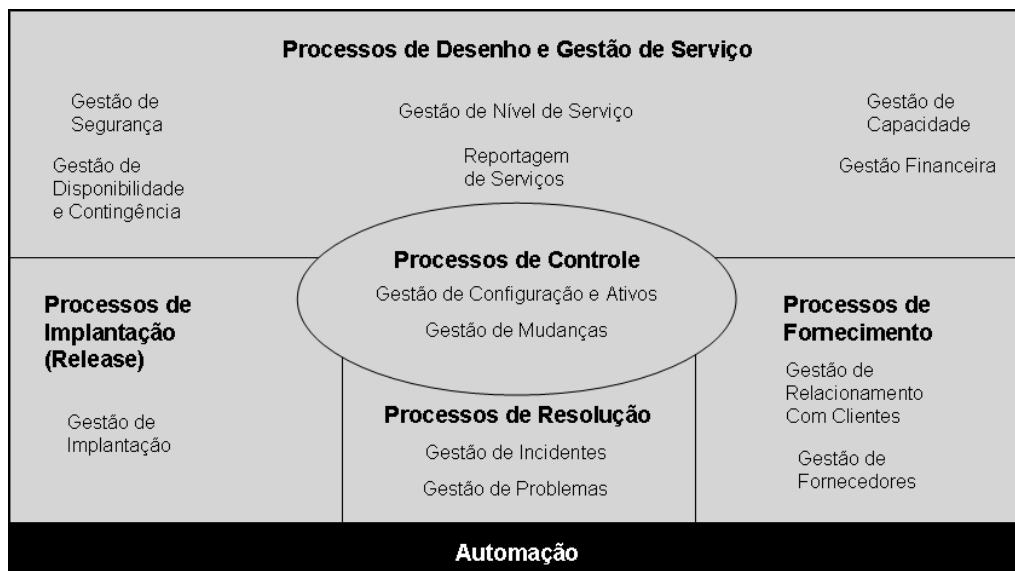
Julgue os itens seguintes, acerca de controles internos em sistemas de informação.

- 101** O princípio denominado custo-efetividade prescreve que apenas os sistemas de informação organizacionais que manipulam bens tangíveis para a organização necessitam de controles internos.
- 102** A adoção de um SGBD com acesso gerenciado por senhas é um exemplo de controle mais diretamente associado à segurança e privacidade e menos à preparação e captação de dados.
- 103** A adoção de níveis de permissão de acesso para emissão de relatórios de fechamento de operações diárias e mensais é um exemplo de controle mais diretamente associado ao processamento e menos associado à entrada de dados.
- 104** O registro formal e assinado acusando o recebimento para digitação no computador e referente a um lote de registros manualmente emitidos, como notas fiscais, é um exemplo de controle mais associado ao aspecto administrativo e gerencial e menos associado à preparação e captação de dados.
- 105** A definição formal e explícita do organograma de uma unidade de segurança da informação em uma organização, bem como das atribuições de cada subunidade organizacional e de seus respectivos responsáveis e níveis de acesso é um exemplo de controle administrativo e gerencial, mas não, de controle associado à segurança e privacidade.
- 106** Sistemas operacionais como o Windows 2000 e Windows 2003, independentemente do tipo de sistema de arquivos adotado em suas unidades de disco, possibilitam de forma nativa a implantação de controles que registram o sucesso ou falha no acesso, leitura, gravação de arquivos, os quais podem ser diretamente associados a controles de gravação e recuperação de dados.



A figura acima apresenta um modelo de dados parcial de um sistema de atendimento a pedidos de clientes. Acerca das informações apresentadas e dos conceitos e técnicas envolvidos, julgue os itens a seguir.

- 107 O modelo de dados, no que se refere ao relacionamento entre as tabelas clientes e pedidos, está na terceira forma normal.
- 108 A rastreabilidade entre pedidos e notas fiscais não está assegurada nas informações apresentadas no modelo.
- 109 A identificação dos clientes que receberam pacotes de um empregado está garantida nas informações contidas no modelo.
- 110 No que concerne à alteração de preços na tabela dos produtos, o modelo garante a integridade das informações das notas fiscais.
- 111 O comando `Select idCliente, nome, idPacote from Clientes, Pacotes where Clientes_idCliente = idCliente` é um comando SQL válido, que realiza um JOIN que retorna uma lista de todos os pacotes recebidos por cada um dos clientes cadastrados na base de dados.
- 112 Na detecção de possíveis falhas em controles internos de sistemas, quanto mais normalizado for um modelo de dados, menos complexas se tornam as consultas SQL efetuadas pela auditoria.



BSI (British Standards Institute) Code of practice for IT service management (PD0005), (com adaptações).

Com base na figura acima, que apresenta um conjunto de áreas de processos relacionadas com gerenciamento de tecnologia da informação, julgue os itens que se seguem.

- 113** A fim de coletar informações iniciais sobre a condição dos dispositivos e módulos de *software*, *hardware* e bases de dados em um ambiente de TI, o auditor de TI deve solicitar dados aos trabalhadores responsáveis pelos processos de gestão de capacidade.
- 114** Com o objetivo de coletar informações iniciais sobre a natureza técnica dos serviços e produtos de infra-estrutura adquiridos, como dispositivos e linhas de telecomunicações, *software* para gerenciamento de redes, manutenção de impressoras e computadores, o auditor de TI deve solicitar dados aos trabalhadores responsáveis pelos processos de gestão de fornecedores.
- 115** Para coletar informações iniciais sobre o fluxo de recebimento, análise e eventual aprovação de solicitações de melhorias encaminhadas pelos clientes, usuários e técnicos de suporte, o auditor de TI deve solicitar dados aos trabalhadores responsáveis pelos processos de gestão de mudanças.
- 116** Objetivando coletar informações iniciais sobre a análise e soluções técnicas para os erros crônicos que afetam o desempenho dos serviços de TI, o auditor de TI deve solicitar dados aos trabalhadores responsáveis pelos processos de gestão de problemas.
- 117** A fim de coletar informações iniciais sobre o grau de cumprimento dos contratos formais de prestação de serviços estabelecidos entre a organização de TI e a área de negócios, o auditor de TI deve solicitar dados aos trabalhadores responsáveis pelos processos de gestão de fornecedores.
- 118** Na coleta de informações sobre planos para expansão de negócios da organização e sobre o conseqüente provimento de serviços de TI que atendam a tais expansões, o auditor de TI deve solicitar dados aos trabalhadores responsáveis pelos processos de gestão de implantação.
- 119** Para coletar informações iniciais sobre o volume de atendimento aos usuários de TI, bem como sobre o tipo de evento que mais prejudica as atividades destes usuários, o auditor de TI deve solicitar dados aos trabalhadores responsáveis pelos processos de gestão de incidentes.
- 120** A visita do auditor, em uma auditoria de planos de contingência e recuperação de desastres, é uma das únicas que devem ser feitas sem comunicação prévia, a fim de que não haja tempo para que o auditado se prepare para mascarar evidências.

PROVA DISCURSIVA

- Nesta prova — que vale **trinta** pontos —, faça o que se pede, usando o espaço indicado no presente caderno para rascunho. Em seguida, transcreva o texto para a **FOLHA DE TEXTO DEFINITIVO DA PROVA DISCURSIVA**, no local apropriado, pois **não serão avaliados fragmentos de texto escritos em locais indevidos**.
- Qualquer fragmento de texto além da extensão máxima de **trinta** linhas será desconsiderado.
- Na **folha de texto definitivo**, identifique-se apenas no cabeçalho da primeira página, pois **não será avaliado** texto que tenha qualquer assinatura ou marca identificadora fora do local apropriado.

Redija um texto dissertativo que discuta a importância do estabelecimento de um plano de projeto para melhoria da auditoria de *software* e de sistemas em organizações públicas federais de tecnologia da informação. O seu texto deve explorar necessariamente os seguintes aspectos:

- ▶ importância de diagnóstico da segurança da informação na organização;
- ▶ necessidades de divulgação da auditoria dentro da organização;
- ▶ importância da adoção de modelos para o processo de auditoria de sistemas e seleção de controles;
- ▶ uso de tecnologias para aperfeiçoamento ou automação do processo de auditoria;
- ▶ priorização das áreas de auditoria.

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