TRIBUNAL DE CONTAS DA UNIÃO

Concurso Público

Aplicação: 30/9/2007

Cargo: Analista de Controle Externo
Área: Controle Externo
Especialidade: Controle Externo
Orientação: Auditoria de Tecnologia da Informação

MANHÃ

Caderno G

Prova Objetiva P_1
Prova Discursiva P_2

LEIA COM ATENÇÃO AS INSTRUÇÕES ABAIXO.

1 **Ao receber este caderno, confira atentamente se o tipo de caderno — Caderno G — coincide com o que está registrado em sua folha de respostas. Em seguida, verifique se ele contém CEM itens, correspondentes à prova objetiva de conhecimentos específicos (P_1), corretamente ordenados de 101 a 200, seguidos da prova discursiva de conhecimentos específicos (P_2) acompanhada de espaços para rascunho.**

2 Os espaços para rascunho são de uso opcional; não contarão, portanto, para efeito de avaliação.

3 Caso o caderno esteja incompleto ou tenha qualquer defeito, solicite ao fiscal de sala mais próximo que tome as providências cabíveis.

4 Não utilize lápis, lapiseira (grafite), borracha e(ou) qualquer material de consulta que não seja fornecido pelo CESPE/UnB.

5 Não se comunique com outros candidatos nem se levante sem autorização do chefe de sala.

6 Não serão distribuídas folhas suplementares para rascunho nem para texto definitivo.

7 Nos itens da prova objetiva, recomenda-se não marcar ao acaso: cada item cuja resposta divirja do gabarito oficial definitivo receberá pontuação negativa, conforme consta em edital.

8 A duração das provas é de **cinco horas**, já incluído o tempo destinado à identificação — que será feita no decorrer das provas —, ao preenchimento da folha de respostas e à transcrição dos textos definitivos da prova discursiva para o CADERNO DE TEXTOS DEFINITIVOS DA PROVA DISCURSIVA P_2 — CONHECIMENTOS ESPECÍFICOS.

9 Você deverá permanecer obrigatoriamente em sala por, no mínimo, uma hora após o início das provas e poderá levar este caderno de provas somente no decurso dos últimos **quinze minutos** anteriores ao horário determinado para o término das provas.

10 Ao terminar as provas, chame o fiscal de sala mais próximo, devolva-lhe a sua folha de respostas e o seu caderno de textos definitivos e deixe o local de provas.

11 A desobediência a qualquer uma das determinações constantes no presente caderno, na folha de respostas ou no caderno de textos definitivos poderá implicar a anulação das suas provas.

AGENDA (datas prováveis)

I **2/10/2007**, após as 19 h (horário de Brasília) – Gabaritos oficiais preliminares das provas objetivas: Internet — www.cespe.unb.br/concursos/tcu2007.

II **3** a **5/10/2007** – Recursos (provas objetivas): exclusivamente no Sistema Eletrônico de Interposição de Recurso, Internet, mediante instruções e formulários que estarão disponíveis nesse sistema.

III **22/10/2007** – Resultados finais das provas objetivas e provisórios das provas discursivas: Diário Oficial da União e Internet.

IV **23** a **25/10/2007** – Recursos (provas discursivas): em locais e horários que serão informados na divulgação dos resultados provisórios.

V **9/11/2007** – Resultados finais das provas discursivas e convocação para a segunda etapa do concurso: Diário Oficial da União e Internet.

OBSERVAÇÕES

- Não serão objeto de conhecimento recursos em desacordo com o item 12 do Edital n.º 1 – TCU – ACE/TCE, de 20/7/2007.
- Informações adicionais: telefone 0(XX)61 3448-0100; Internet — www.cespe.unb.br/concursos/tcu2007.
-

cespe UnB

De acordo com o comando a que cada um dos itens de **101** a **200** se refira, marque, na **folha de respostas**, para cada item: o campo designado com o código **C**, caso julgue o item **CERTO**; ou o campo designado com o código **E**, caso julgue o item **ERRADO**. A ausência de marcação ou a marcação de ambos os campos não serão apenadas, ou seja, não receberão pontuação negativa. Para as devidas marcações, use a **folha de respostas**, único documento válido para a correção da sua prova.

CONHECIMENTOS ESPECÍFICOS (P_2)

Julgue os itens subseqüentes, a respeito da execução do trabalho de auditoria.

101 De acordo com a estrutura conceitual da análise de risco do tipo COSO, é imprescindível a existência de controles internos para o cumprimento das metas e objetivos da entidade. Caso se detecte potencial de risco na obtenção desses objetivos, poderá o controle interno atuar como a auditoria interna.

102 O uso da técnica de amostragem é facultativo para o auditor interno; entretanto, a realização de exames e investigações, como a verificação junto a terceiros sobre operações de grande vulto, as inspeções no capital financeiro e o registro de transações de recursos financeiros, é obrigatória. São esses resultados, denominados achados de auditoria, que irão fundamentar as conclusões do auditor.

103 Em um ambiente de processamento eletrônico de dados, o auditor deve proceder a avaliação dos riscos inerentes de controle nas demonstrações contábeis, dado que erros nessas demonstrações poderão ensejar aumento de fraudes, comprometendo a estrutura da empresa. Portanto, é competência do auditor cuidar para que isso não ocorra.

Acerca da auditoria no setor público federal, bem como à administração da função de auditoria, julgue os itens que se seguem.

104 Considere que a União tenha repassado vultosa quantia a um estado da Federação, com objetivo de aquisição de maquinário para uma corporação militar daquele estado, e que, após determinação do Ministro do Planejamento, Orçamento e Gestão, foi realizada uma auditoria que constatou irregularidades na aplicação desses recursos federais da ordem de R$ 49 milhões. Foram detectados tanto vícios na dispensa de licitação quanto inadequação dos bens adquiridos. Nessa situação hipotética, a auditoria realizada é classificada como especial, de forma indireta compartilhada.

105 Em cada auditoria realizada, o auditor governamental deverá elaborar relatório que refletirá os resultados dos exames efetuados. Entretanto, nos relatórios de auditorias realizadas com base no processo de tomada e prestação de contas, nas quais se detectar desvio de bens públicos, a autoridade administrativa competente deverá comunicar imediatamente o resultado ao TCU, para que este instaure processo de tomada de contas especiais.

106 É responsabilidade da auditoria interna fazer periodicamente uma avaliação dos controles internos. Nesse sentido, é correto afirmar que a auditoria interna representa um controle interno.

Julgue os próximos itens, relativos a tipos de auditoria.

107 Suponha que uma auditoria, realizada em uma escola agrícola federal subordinada ao Ministério da Educação, tenha constatado falhas e deficiências na área orçamentário-financeira, no sistema escola-fazenda e na área de recursos humanos. Nessa situação hipotética, a auditoria descrita é um exemplo de auditoria de natureza operacional, que abrange, inclusive, avaliação de programas, o que permite à equipe de auditoria pronunciar-se sobre o aumento da evasão escolar em virtude da situação.

108 O julgamento das contas dos gestores públicos em virtude de danos ao erário decorrentes de atos de gestão ilegítima ou antieconômica, ou por desfalques ou desvio de dinheiros, bens e valores públicos, é um meio de detecção de fraudes propiciado pela fiscalização adotada pelo TCU, e a modalidade específica de auditoria que o TCU utiliza para detectar fraudes é a auditoria de conformidade.

Julgue os itens a seguir, que tratam de metodologias empregadas em auditoria governamental e da etapa de monitoramento do trabalho de auditoria.

109 O TCU, nos processos de auditorias operacionais, usa metodologias específicas para análise do objeto auditado e apresentação dos dados coletados. Um dos métodos é o modelo insumo-produto, que objetiva demonstrar como o objeto da auditoria desenvolve as suas atividades, identificando, por exemplo, as informações e os recursos humanos, físicos e financeiros exigidos (insumos), os processos de transformação dos insumos em produtos e os bens e serviços ofertados (produtos).

110 O monitoramento é um instrumento de fiscalização exclusivo da auditoria, cujas finalidades são desenvolver metodologias, corrigir desvios e assegurar os objetivos previstos.

Os princípios orçamentários formam os pilares de uma gestão de recursos públicos. O art. 2.º da Lei n.º 4.320/1964 dispõe que a Lei de Orçamento conterá a discriminação da receita e da despesa, de forma a evidenciar a política econômico-financeira e o programa de trabalho de governo, obedecidos os princípios da unidade, universalidade e anualidade. Com relação à observância ao princípio da universalidade, julgue o item a seguir.

111 O projeto da lei orçamentária deve ser acompanhado do demonstrativo regionalizado dos efeitos sobre as receitas e despesas, decorrentes de isenções, anistias, remissões, subsídios e benefícios de natureza financeira, tributária e creditícia.

O ciclo orçamentário, também denominado processo orçamentário, corresponde ao período de tempo em que se processam as atividades típicas do orçamento público, desde sua concepção até sua apreciação final. Com relação ao período de discussão, votação e aprovação do orçamento público, julgue o item que se segue.

112 As emendas ao projeto de lei do orçamento anual ou aos projetos que o modifiquem somente podem ser aprovadas caso sejam compatíveis com o plano plurianual (PPA) e com a lei das diretrizes orçamentárias (LDO).

No programa do orçamento, é articulado um conjunto de ações que concorrem para um objetivo comum preestabelecido, mensurado por indicadores fixados no PPA, visando à solução de um problema ou ao atendimento de uma necessidade ou demanda da sociedade. De acordo com a sua finalidade, os programas compreendem quatro modalidades: programas finalísticos, programas de gestão de políticas públicas, programas de serviços ao Estado e programas de apoio administrativo. Quanto às características que cercam os programas finalísticos, julgue o item a seguir.

113 Os programas finalísticos abrangem as ações de governo relacionadas à formulação, coordenação, supervisão e avaliação de políticas públicas.

Como função de um setor público, deve-se entender o maior nível de agregação das diversas áreas de despesa que competem ao setor. Cada programa deverá dar solução a um problema ou atender a uma demanda da sociedade, mediante um conjunto articulado de projetos, atividades e de outras ações que assegurem a consecução dos objetivos. Sobre as características que cercam as atividades, julgue o item abaixo.

114 Trata-se de um instrumento de programação para alcançar o objetivo de um programa, envolvendo um conjunto de operações que se realizam de modo contínuo e permanente, das quais resulta um produto necessário à manutenção da ação de governo.

A LDO foi introduzida no direito financeiro brasileiro pela Constituição Federal de 1988, tornando-se, a partir de então, o elo entre o PPA e a Lei Orçamentária Anual. Acerca da LDO, julgue o item seguinte.

115 A LDO é o instrumento que expressa o planejamento dos governos federal, estadual, distrital e municipal para um período de quatro anos, objetivando garantir a continuidade dos planos e programas instituídos pelo governo anterior.

A Lei n.º 4.320/1964, em seu artigo 11, classifica a receita orçamentária em duas categorias econômicas: receitas correntes e receitas de capital. Com a Portaria Interministerial STN/SOF n.º 338/2006, essas categorias econômicas foram detalhadas em receitas correntes intra-orçamentárias e receitas de capital intra-orçamentárias. A respeito da função das receitas intra-orçamentárias, julgue o próximo item.

116 Como se destinam ao registro de receitas provenientes de órgãos pertencentes ao mesmo orçamento do ente público, as contas de receitas intra-orçamentárias não têm a mesma função da receita original, sendo criadas a partir de base própria pela Secretaria do Tesouro Nacional.

Como parte do orçamento, a despesa compreende as autorizações para gastos com as várias atribuições e funções governamentais, tendo a sua classificação complementada pela informação gerencial denominada de modalidade de aplicação. Com relação a modalidade de aplicação, julgue o item a seguir.

117 A modalidade de aplicação tem por finalidade identificar os objetos de gasto de que a administração pública se serve para a consecução dos seus fins.

Os créditos adicionais são autorizações de despesa não computadas ou insuficientemente dotadas na Lei de Orçamento. Sobre as informações que devam constar na abertura do crédito adicional, julgue o seguinte item.

118 O ato que abrir crédito adicional deve indicar a importância, espécie e a classificação da despesa, até o limite em que for possível.

O balanço patrimonial, previsto no art. 105 da Lei 4.320/1964, é o demonstrativo que evidencia a posição das contas que constituem o ativo e o passivo, apresentando a situação estática dos bens, direitos e obrigações da entidade. A respeito da elaboração do balanço patrimonial, julgue o item subseqüente.

119 O resultado patrimonial do exercício é apurado a partir do levantamento do balanço patrimonial e pode apresentar *superavit* (ativo maior que passivo), *deficit* (ativo menor que passivo) ou resultado nulo (ativo igual ao passivo).

A Lei n.º 101/2000, conhecida como Lei de Responsabilidade Fiscal (LRF), estabeleceu normas de finanças públicas voltadas para a responsabilidade na gestão fiscal, estabelecendo, entre outras, normas para execução orçamentária e cumprimento de metas. Considerando que haja limitação de empenho, julgue o item que se segue, quanto ao restabelecimento da receita prevista.

120 A recomposição das dotações cujos empenhos foram limitados dar-se-á de forma proporcional às reduções efetivadas.

Acerca de organização e arquitetura de computadores, seus componentes e sistemas de entrada e saída, julgue os itens a seguir.

121 Um montador é considerado um *software* de sistema, responsável pela tradução de uma linguagem de alto nível para uma linguagem de baixo nível (linguagem simbólica).

122 Na aritmética computacional, a representação de números de ponto flutuante é de grande importância. Com o objetivo de padronizar a representação desses números, o IEEE definiu um padrão para computação de ponto flutuante (IEEE 754), o qual especifica, entre outras coisas, alguns métodos de arredondamento.

Quanto a arquitetura de sistemas operacionais, gerenciadores de arquivos e recursos, bem como no que se refere a conceitos de administração de contas e de segurança, julgue os itens que se seguem.

123 Embora os atributos de arquivo possam variar de um sistema operacional (SO) para outro, alguns atributos são comuns a praticamente todos os sistemas operacionais. Entre esses atributos, incluem-se localização do arquivo, tamanho e nome, além da extensão do arquivo e da versão do aplicativo que será utilizado para abri-lo. Os dois últimos atributos permitem que o SO identifique a aplicação que deve ser chamada no processo de abertura do arquivo.

124 O SO define as operações que podem ser realizadas sobre arquivos, como, por exemplo, a operação de truncar um arquivo.

125 Entre os métodos mais utilizados na definição da estrutura lógica dos diretórios em um SO, incluem-se o método de nível único, o método árvore e o grafo cíclico.

126 Quando ocorre uma interrupção, o SO interrompe a execução do processo corrente e executa uma rotina do kernel. Entretanto, antes da execução dessa rotina, algumas informações sobre o contexto atual do processo devem ser salvas, tais como as referentes a valores dos registradores, estado do processo e gerenciamento de memória.

Considerando os princípios de linguagens de programação, os conceitos de linguagens estruturadas, os aspectos gerais das linguagens de programação C, C++, Java, Natural, Cobol, Delphi, os conceitos gerais sobre montadores, ligadores, compiladores, interpretadores e estruturas de dados, julgue os itens subseqüentes.

127 A linguagem C disponibiliza mecanismos para a criação de tipos de dados definíveis pelo programador.

128 A linguagem C não permite a chamada de uma função por valor, mas, apenas, por referência.

129 Uma das principais tarefas do ligador, programa responsável por unir módulos-objeto em um único módulo, denominado módulo de carga, é resolver referências internas e externas.

130 Um interpretador pode ser considerado como um programa que lê um conjunto de instruções e as executa passo a passo. Programas interpretados são, em geral, menores e mais facilmente mantidos, embora sejam mais lentos que os programas compilados.

131 A análise semântica — responsável por verificar se a estrutura gramatical do programa está correta, ou seja, se essa estrutura foi formada de acordo com as regras gramaticais da linguagem — é uma das tarefas realizadas pelo compilador.

132 A profundidade de uma árvore binária é de ordem O(*log log n*), em que *n* representa o número de nós da árvore.

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

133 De uma forma geral, a principal diferença entre redes comutadas por circuito e por pacotes é o uso da largura de banda. No último caso, a largura de banda é alocada antes e garantida durante a transmissão, ao passo que, no outro caso, a reserva e liberação de banda ocorre dinamicamente.

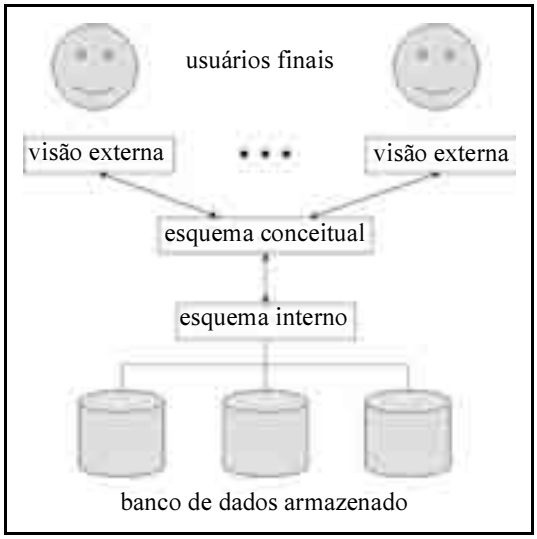
134 A arquitetura cliente-servidor tem por motivação sincronizar a execução de dois processos que devem cooperar um com outro. Assim, dadas duas entidades que queiram comunicar-se, uma deve iniciar a comunicação enquanto a outra aguarda pela requisição da entidade que inicia a comunicação.

135 O modelo de referência OSI é organizado em camadas, e foi concebido segundo os seguintes princípios: uma camada deve ser criada onde uma nova abstração seja necessária; cada camada deve ter uma função bem definida; as fronteiras entre as camadas devem ser escolhidas de forma a minimizar o fluxo de informações entre elas; o número de camadas deve ser tal que não force o grupamento de funções não-relacionadas.

136 A arquitetura TCP/IP difere do modelo OSI no número de camadas, entretanto suas camadas de rede, transporte e aplicação correspondem às de mesmo nome no modelo OSI.

137 Os roteadores tomam suas decisões de encaminhamento com base nos endereços físicos, enquanto as *bridges* se baseiam nos endereços lógicos.

138 Em VoIP, é possível a injeção de tráfego, bem como forjar e interceptar conexões.



Elmasri. **Sistemas de banco de dados** (com adaptações).

Considerando a figura acima, que apresenta um esquema da arquitetura ANSI/SPARC, utilizada para representar características de sistemas de gerenciamento de bancos de dados (SGBDs), julgue os itens a seguir, acerca de conceitos de bancos de dados.

139 Em uma aplicação de banco de dados, *scripts* escritos na linguagem SQL nativa de um SGBD podem representar: o esquema conceitual dessa aplicação; a visão externa dos usuários finais; e as características físicas de armazenamento do esquema interno.

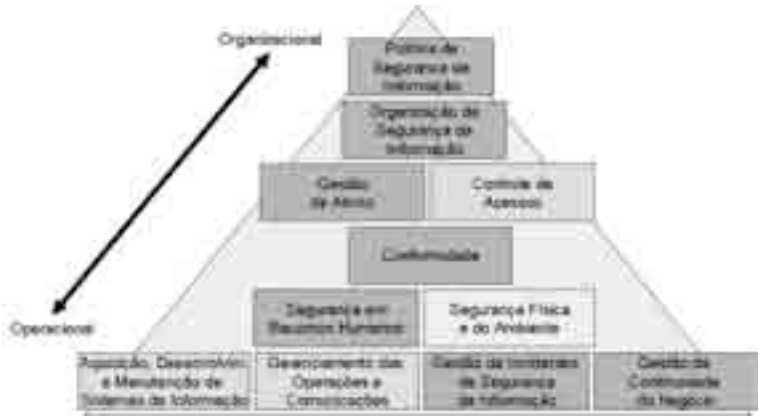
140 Considere a situação na qual uma mesma aplicação de banco de dados tenha sido implementada utilizando-se quatro diferentes técnicas de modelagem: relacional, rede, hierárquica, e orientada a objetos. Nesse caso, espera-se que o uso de polimorfismo seja mais intenso junto à aplicação que empregou a técnica orientada a objetos; o armazenamento de ponteiros em disco que representam registros em listas circulares duplamente encadeadas seja mais comum junto à aplicação que empregou a técnica em rede; dificuldades para representar relacionamentos *m*:*n* sejam mais comuns junto à aplicação que empregou a técnica de modelagem hierárquica; e maiores facilidades para alcance da terceira forma normal estejam presentes na aplicação que empregou a modelagem relacional.

141 Durante o projeto de um esquema de dados relacional, a partir de um modelo entidade-relacionamento de uma aplicação, espera-se que as seguintes operações sejam realizadas: para cada tipo de entidade forte do modelo, será criada uma relação que conterá a mesma quantidade de atributos dessa entidade; para cada relacionamento binário *m*:*n*, será criada uma nova relação que inclua como atributos de chave estrangeira as chaves primárias das duas relações já mapeadas a partir das entidades que fazem parte desse relacionamento binário.

142 Considere um cenário no qual há necessidade de desenvolvimento de uma aplicação transacional empregando bancos de dados federados. Nesse caso, uma das técnicas indicadas para assegurar a atomicidade de transações seria o emprego de coordenadores de transação embasados em protocolos de *commit* em duas fases: *rollback* e *commit*.

143 Considere uma situação na qual um administrador de banco de dados de uma organização execute atividades rotineiras de manutenção de um SGBD. Nessa situação, é razoável supor que esse profissional proverá maior suporte aos usuários finais por meio da realização de mudanças junto à visão externa da aplicação do que por meio de mudanças no esquema conceitual da aplicação.

144 São características de uma aplicação de banco de dados aderente ao paradigma de modelagem multidimensional: visões internas que usam uma menor quantidade de operações de junção de tabelas, menor latência durante a execução de consultas que trabalham com valores agregados e esquema em baixos níveis de normalização.



Adaptado de BSI.ORG.

Considerando a figura acima, que apresenta uma proposta de organização da norma NBR ISO/IEC 17799:2005, julgue os próximos itens, acerca dos conceitos de segurança da informação.

145 A NBR 17799 prescreve o uso de gerenciamento quantitativo de riscos.

146 A NBR 17799 define como aplicar seus controles em processos de gestão e auditoria.

147 A NBR 17799 prescreve vários atributos de classificação da informação, entre os quais se encontram os que indicam graus de sensibilidade e criticidade. O grau de sensibilidade de um ativo de informação está mais associado a aspectos de privacidade que o grau de criticidade, este mais relacionado a aspectos negociais.

148 A NBR 17799 prescreve explicitamente que as instalações de processamento da informação gerenciadas por uma organização devem estar fisicamente separadas daquelas que são gerenciadas por terceiros. Esse controle está descrito no capítulo 9 da referida NBR, juntamente com outros relacionados a ameaças externas como explosões e perturbações sociais, e controle de acesso com múltiplos fatores de autenticação, como senhas, *smart cards* e biometria.

149 Conforme os controles da NBR 17799, os processos de gestão de segurança de recursos humanos de uma organização envolvem o retorno dos ativos à organização após o encerramento do contrato de trabalho, bem como conscientização, educação e treinamento em segurança da informação, inclusive para terceiros.

150 Um plano de continuidade de negócios distingue-se de um plano de recuperação de desastres por vários aspectos, entre os quais a maior ênfase no gerenciamento de riscos.

151 Acerca do gerenciamento das operações e comunicações segundo a NBR 17799, considere o uso combinado de três tipos de *backups*: pleno (*full*), incremental e diferencial. Nesse caso, é correto afirmar que, no evento de um desastre, uma estratégia embasada em *backup* pleno mais incremental atenderá a uma métrica RPO (*recovery point objective*) de melhor qualidade que uma estratégia embasada em *backup* pleno mais diferencial.

152 Diferentemente do tratamento de incidentes de segurança em tecnologia da informação (TI) em geral, o tratamento de incidentes de segurança da informação por meio da abordagem de times de resposta a incidentes de segurança busca encontrar a causa raiz de vários outros incidentes similares antes da realização das ações de contenção.

153 São características típicas dos *malwares*: cavalos de tróia aparentam realizar atividades úteis; *adwares* obtêm e transmitem informações privadas do usuário; *backdoors* estabelecem conexões para fora da rede onde se encontram; *worms* modificam o código de uma aplicação para propagar-se em uma rede; e *botnets* realizam ataques articulados por meio de um controle remoto.

154 *Rootkits* apresentam portabilidade entre plataformas e devem ser manuseados conforme os controles estabelecidos no capítulo relativo à aquisição, desenvolvimento e manutenção de sistemas de informação da NBR 17799.

155 Acerca das técnicas gerais de ataques e vulnerabilidades de aplicações, é correto afirmar que vulnerabilidades de SQL *injection* são minimizadas por meio do uso de *prepared statements*; ataques de *heap overflow* ocorrem com maior freqüência em linguagens com tipos de dados fracos que em linguagens com tipos de dados fortes; ataques de dicionário são tecnicamente mais complexos de empreender quando são empregados *hashes* criptográficos embasados no algoritmo MD5 que no caso do algoritmo SHA1.

156 O emprego de mecanismos de controle de acesso obrigatório ou mandatório possibilita o alcance de segurança multinível em bancos de dados, algo que é bem mais difícil de ser alcançado com mecanismos de controle de acesso flexíveis ou discricionários. No primeiro caso, são empregados esquemas de classificação da informação. No último, em geral, empregam-se listas de controle de acesso.

157 A detecção, por um *sniffer* de rede, de uma longa série de segmentos TCP SYN enviados de um *host* local para um *host* remoto, sem o correspondente envio de segmentos TCP ACK, sugere que a rede sob análise pode estar sofrendo um ataque de negação de serviço.

158 Acerca das vulnerabilidades e ataques comuns aos sistemas de rede *wireless*, é correto afirmar que o protocolo WEP, independentemente do uso de TKIP, utiliza vetores de inicialização dinâmicos e não cíclicos, que auxiliam na randomização das chaves de criptografia simétricas do tipo RC4 usadas durante a transmissão de pacotes.

159 O uso de uma ferramenta como `tcpdump` ou `windump`, para análise de tráfego de rede, oferece uma saída de dados mais amigável que `Ethereal`, principalmente pela sua capacidade de apresentar estatísticas de conversação entre *hosts* e hierarquias de protocolos empregadas.

160 Como regra geral, quanto menor for a MTU de um enlace de rede, maior tenderá a ser a fragmentação de segmentos que trafegam nessa rede. Devido à fragmentação, assinaturas de ataques com o protocolo ICMP poderão ser mais difíceis de detectar, especialmente no caso de o *firewall* em uso ser do tipo de filtragem de pacotes.

161 Sistemas criptográficos simétricos AES, DES e RC4 são mais adequados ao estabelecimento de protocolos de não repúdio, quando comparados com algoritmos assimétricos, como RSA.

Internet: <www.isaca.org>.

A figura acima apresenta um conjunto de elementos relacionados ao modelo COBIT 4.0, alguns dos quais estão numerados de #1 a #11. Considerando essa figura, julgue os itens seguintes com relação à governança de TI.

162 O conceito de governança de TI está mais associado à melhoria do relacionamento entre os elementos #5 e #6 que ao relacionamento entre os elementos #9 e #11.

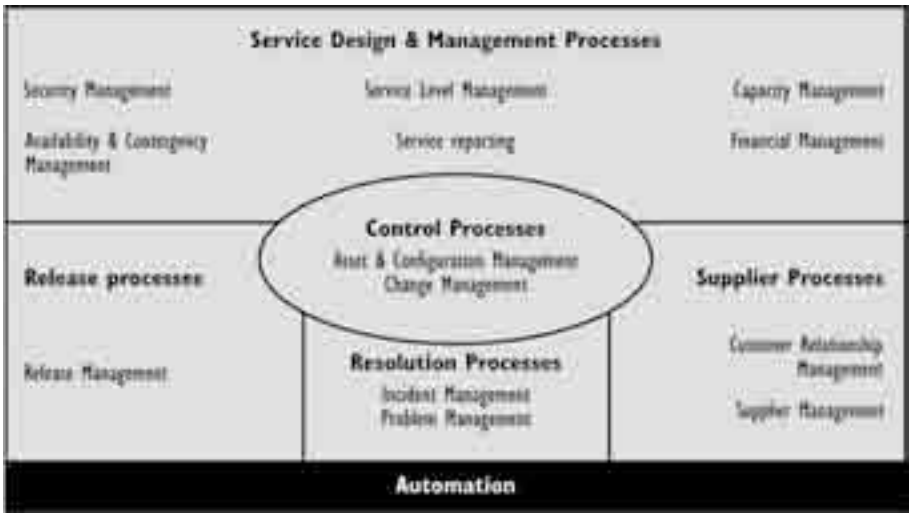
163 Assumindo-se a implantação de um planejamento estratégico de TI embasado no método de *balanced scorecard* (BSC) em uma organização que faz prestação de serviços de TI, uma métrica que indica o tempo necessário para desenvolvimento e implantação de novos serviços de TI é mais adequadamente localizada na perspectiva de aprendizagem e crescimento que na perspectiva de processos de negócios internos.

164 Em uma organização que faz prestação de serviços de TI, uma métrica que indica o grau de adesão a um treinamento básico e voluntário sobre segurança da informação seria mais adequadamente enquadrada como um indicador chave de desempenho (KPI) que como um indicador chave de metas (KGI).

165 A implantação de um planejamento estratégico organizacional embasado no BSC definirá fluxos de informações que produzirão maior volume de dados entre os níveis #1 e #2 que entre os níveis #2 e #3.

166 Os processos genéricos de auditoria presentes no modelo COBIT 4.0 são descritos em #4.

167 O modelo COSO é adotado pelo modelo COBIT para definição dos elementos centrais que fazem parte da implementação de controle interno em uma organização, entre as quais se destacam: a criação de um ambiente de controle interno baseado na ética, no compromisso com a competência e no provimento para auditoria independente; a ação fundamentada no gerenciamento de riscos, seja no âmbito organizacional seja no de atividades; a adoção de políticas e procedimentos, entre outras atividades de controle; a efetividade e tempestividade da comunicação e informação entre os vários elementos organizacionais; o monitoramento contínuo das atividades e o relato das deficiências encontradas pelo controle interno.



Internet: <tso.co.uk>.

Considerando a figura acima, que apresenta os elementos principais de gestão de serviços de TI embasados no modelo ITIL, julgue os itens seguintes, acerca dos conceitos de gerenciamento de serviços de TI.

168 O processo de gerenciamento de acordos de níveis de serviço pode produzir requisitos usados diretamente pelo processo de resolução de incidente. Ambos os processos devem ser realizados por diferentes unidades da estrutura organizacional, inclusive para atender a demandas de segregação de funções.

169 Os processos de controle, apresentados no centro do diagrama, abrangem auditorias periódicas de primeira parte, às quais tais processos também estão sujeitos.

170 Apresenta maior risco de segurança, em decorrência da não segregação de funções, um gerente de sistemas que elabora um projeto básico para aquisição de um serviço de TI e posteriormente aprova o recebimento do serviço, quando comparado a um gerente de segurança de rede que desabilita temporariamente uma regra de um *firewall* visando acesso a um serviço na Internet para solução de problemas de natureza pessoal.

171 A fim de possuir eficácia, a política de gerenciamento de riscos de segurança da informação de uma organização tem de ser necessariamente subordinada a uma política de segurança da informação de mais amplo escopo.

172 Uma política organizacional de segurança da informação orientada a um tema específico apresenta maior estruturação operacional que um guia de ação recomendada.

173 O modelo COBIT 4.0 considera os recursos humanos de TI de uma organização como uma classe de recursos de TI, do mesmo modo que o são as aplicações, as informações e a infra-estrutura de TI.

174 Conforme o modelo ITIL 2.0, o registro de um erro conhecido ocorrerá antes da liberação da mudança que corrige esse erro, mas após a escrita do pedido de mudança correspondente.

175 Conforme o modelo ITIL 2.0, a produção de relatórios analíticos da carga média de tempo necessária para solução de incidentes por grupo de suporte é uma atividade mais pertinente à gerência de incidentes que à gerência de acordos de níveis de serviço.

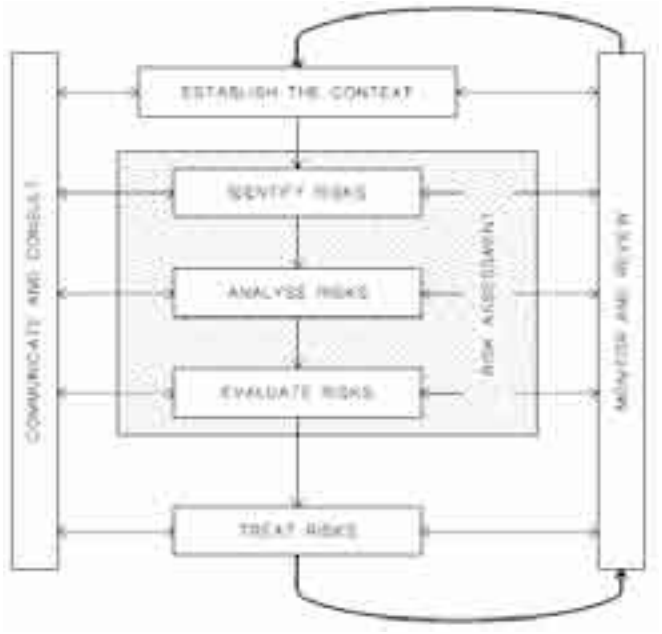
176 Conforme o modelo ITIL 2.0, o registro de mudanças efetuadas em uma base de dados de configuração seria uma atribuição mais pertinente à gerência de liberação que à gerência de mudanças.

177 O modelo COBIT define uma seqüência de níveis de maturidade para guiar a mudança e melhoria da governança de TI de uma organização. O alcance desses níveis é avaliado globalmente para a organização, da mesma forma como ocorre no modelo CMMI. Alguns desses níveis, ordenados do menor para o maior, são: não existente, definido e otimizado.

178 A técnica de *benchmarking* é mais adequadamente apoiada pela comparação entre os níveis de maturidade alcançados por organizações que pela comparação entre os indicadores de desempenho alcançados por organizações.

179 O estabelecimento de uma política organizacional de segurança da informação é uma atividade que depende em maior escala do apoio obtido pelo estafe de nível inferior na hierarquia organizacional que do apoio explícito provido pela alta administração.

180 Fatores críticos de sucesso são, quando comparados a indicadores de meta, instrumentos mais aptos a auxiliar a implantação de controles gerenciais de TI durante mudanças organizacionais.



Standards Australia.

Considerando a figura acima, que apresenta um diagrama de um processo de gerenciamento de riscos, julgue os itens subseqüentes, acerca dos conceitos de governança de TI e gestão de riscos.

181 Modelos correntes de gestão de risco, como o apresentado no diagrama, pressupõem uma abordagem especializada para o tratamento de riscos em diferentes áreas temáticas, buscando uma separação entre os diferentes métodos empregados para a gestão de riscos de segurança da informação, de projetos e organizacionais em geral.

182 A contratação de um seguro é uma técnica de tratamento de riscos que transfere integralmente um risco para outra organização.

183 A identificação dos controles existentes em uma organização é uma atividade de apreciação de riscos, mais precisamente uma atividade de análise de riscos.

184 Critérios previamente desenvolvidos para identificar ações a serem tomadas relativamente ao risco são mais utilizados na fase de avaliação que na fase de tratamento de riscos.

Qual seria sua reação se avistasse um *pendrive* no caminho do estacionamento? Possivelmente, a tentação de abaixar para pegá-lo seria grande. Afinal, os *pendrives* são mídias com capacidade de centenas de disquetes, bem mais rápidos e funcionais. Além disso, é mais fácil hoje em dia encontrar um computador com a interface USB para acoplar o *pendrive* do que unidades para disquetes.

O problema é que um *pendrive* perdido também oferece riscos. Sim, ele pode ter sido deixado ali justamente na expectativa de que alguém o pegasse, plugasse no seu computador corporativo e infectasse toda a rede. O pior é que, ao contrário das unidades de disquetes atuais, as interfaces USB ainda vêm ativadas com recurso de execução automática (*autorun*). Ou seja, basta plugar o *pendrive* no micro para que se dispare a execução de um programa: plataforma mais que perfeita para lançamento de *worms*.

Nos primórdios da microcomputação, as unidades de disquetes possuíam recurso semelhante, o que permitia a propagação dos vírus de disquetes. Bastava o usuário introduzir o disquete na unidade, que micro e vírus se encarregavam da sua reprodução. Infelizmente, a situação com os *pendrives* hoje repete tragicamente esse erro de *design* do passado.

O pior é que tal cenário desolador não é apenas paranóia. O risco é real.

Matt Hines. **Infoworld**. Internet: <www.computerworld.uol.com.br> (com adaptações).

Considere que, corroborando a situação de risco apresentada no texto acima, um usuário de uma rede de computadores de um órgão público, tendo encontrado o referido *pendrive*, tenha conectado tal dispositivo a um dos computadores dessa rede e, em decorrência, tenha infectado toda a rede com *worms*. Nessa situação e sabendo que uma auditoria específica ao problema será realizada no ambiente da rede infectada, julgue os seguintes itens, acerca das verificações e ações que caberão ao auditor encarregado, segundo as boas práticas de auditoria, assim como os padrões normativos desse domínio de atividade.

185 Deve ser verificado se a opção de *autorun* para USB do sistema operacional estava desabilitada ou habilitada no momento da conexão do *pendrive* ao computador, o que acarretou infecção de toda a rede.

186 Deve ser avaliado se existe escaneamento por antivírus das unidades de armazenamento removíveis e se o programa antivírus utilizado no ambiente está atualizado e é capaz de atualizar os padrões e assinaturas para identificar vírus e *worms*, entre outros.

187 Caso constate a inexistência de monitoramento da rede por meio de trilha de auditoria para registro de acesso a portas USB, o auditor deverá implementar esse controle.

188 O auditor deve avaliar se os controles implementados possuem mecanismos de evolução que busquem o objetivo de eliminar ao máximo os diversos tipos de *malware*.

Considerando os princípios de metodologia de auditoria de TI, assim como as boas práticas de auditoria e os referenciais normativos da área, é correto afirmar que a auditoria de TI deve verificar

189 se há política de segurança de informação no órgão auditado e avaliar o seu conteúdo e efetividade, por meio de testes de auditoria.

190 a localização de sítio *backup*, assegurando que ele fique perto da base original de dados, para facilitar o acesso em caso de emergência.

191 se, na ocorrência de problemas com tecnologia de informação (TI), há tempestividade na identificação desses problemas, rapidez na adoção de providências, efetividade nessa ação e registro de todo o processo.

192 se a manutenção dos sistemas e de seus aplicativos, assim como de toda a estrutura de TI, ocorre com periodicidade adequada, se são considerados os registros de ocorrências para respaldarem esse processo, e quais problemas são identificados e corrigidos.

193 a existência de *firewall*, recurso de TI capaz de dividir e controlar o acesso entre redes de computadores, bloquear tentativas de invasão e impedir o acesso de *backdoors*.

194 a existência de plano de continuidade de negócios testado e eficaz, considerando-se as características dinâmicas dos ambientes, em relação aos requisitos de disponibilidade, capacidade e desempenho.

195 se foi definido o nível necessário de cópias de segurança das informações e, em situações em que a confidencialidade seja importante, se as cópias de segurança foram protegidas por meio de encriptação, armazenadas sem vírus, em mídia confiável, em lugar climatizado e restrito.

196 se são observadas, para cada recurso ou arquivo existentes em um sistema, as diretrizes que especificam o que cada usuário pode fazer, diretrizes estas que devem dar privilégio de acesso a dados aos servidores que trabalham na área de TI.

Acerca da comunicação dos resultados da auditoria de TI e das ações gerenciais decorrentes, julgue os próximos itens.

197 Ao final do trabalho de auditoria, o auditor de TI deve elaborar relatório consignando sua opinião acerca dos controles avaliados, dos riscos aos quais a área de TI se sujeita, das evidências dos problemas que foram solucionados pela auditoria, das razões que os originaram e dos controles que foram implementados pela auditoria para reduzir o risco da área auditada.

198 Para assegurar a implantação dos controles necessários, a auditoria deve ser realizada de forma sistemática e permanente na área até que as ações determinadas pela auditoria sejam implementadas.

Acerca da auditoria de aquisições de bens e serviços de TI, considerada a legislação aplicável, julgue os itens a seguir.

199 O auditor deve analisar a legalidade do processo de contratação de bens e serviços de informática e automação, a saber: programas para computadores, máquinas, equipamentos e dispositivos de tratamento da informação e respectiva documentação técnica associada.

200 Em órgãos públicos, com o objetivo de melhor proteger códigos de criptografia utilizados, o auditor deve verificar se é priorizada a aquisição de criptografia de fornecedores estrangeiros certificados, caso contrário, ele deve recomendar que essa determinação seja observada.

PROVA DISCURSIVA P_4

- Nesta prova — que vale **sessenta** pontos, sendo **vinte** pontos para a questão e **quarenta** pontos para a redação —, faça o que se pede, usando os espaços indicados no presente caderno para rascunho. Em seguida, transcreva os textos para o **CADERNO DE TEXTOS DEFINITIVOS DA PROVA DISCURSIVA P_4**, nos locais apropriados, pois **não será avaliado fragmento de texto escrito em local indevido**.
- Nesta prova, respeite os limites máximos de **vinte** linhas para a questão e de **cinqüenta** linhas para a redação, pois quaisquer fragmentos de texto além desses limites serão desconsiderados.
- No **caderno de textos definitivos**, identifique-se apenas no cabeçalho da página correspondente à capa, pois **não será avaliado** texto que tenha qualquer assinatura ou marca identificadora fora do local apropriado.

QUESTÃO 3

A um grupo de trabalho foi atribuída a tarefa de montar um programa para aprimoramento da fiscalização e do controle externo da arrecadação e da aplicação de recursos da União, com cronograma de atividades para os próximos quatro anos. Entre as atividades do grupo de trabalho, inclui-se a de produzir esboço e justificativa preliminar dos tópicos que compõem o programa no que concerne à área de auditoria de tecnologia da informação (TI).

A partir das informações acima, redija um texto dissertativo relativo ao esboço e à justificativa dos tópicos do mencionado programa. No seu texto, devem ser contemplados, necessariamente, os seguintes tópicos:

- desafios ao alcance da governança de TI na administração pública da União;
- estado atual e prognósticos de avanço na prática de auditoria de TI na administração pública da União;
- métodos e processos para aumento da eficiência e eficácia da auditoria de TI na administração pública da União;
- auditoria de segurança da informação no âmbito da auditoria de TI na administração pública da União.

RASCUNHO – QUESTÃO 3

1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	
16	
17	
18	
19	
20	

REDAÇÃO

No trânsito de informações, deve-se utilizar criptografia compatível com o grau de sigilo do documento.

Considerando a afirmação acima, e na qualidade de auditor de tecnologia da informação (TI), redija um texto dissertativo acerca da adequada avaliação da segurança da informação. No seu texto, aborde, necessariamente, os seguintes aspectos:

- relação custo-benefício da implantação do controle em relação ao risco de acesso indevido à informação;
- acesso do próprio auditor de TI aos dados somente para consultá-los, sem possibilidade de editá-los;
- cumprimento das normas de segurança em tecnologia da informação;
- trânsito de equipamentos computacionais como objeto de controle específico;
- processos de governança;
- partes interessadas.

RASCUNHO – REDAÇÃO – 1/2

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	
31	
32	
33	
34	
35	
36	
37	
38	
39	
40	
41	
42	
43	
44	
45	
46	
47	
48	
49	
50	