Questões.

(TCE-SP – Agente de Fiscalização Financeira – Sistemas, Gestão de Projetos e Governança de TI – 2015 – VUNESP)

1. Considerando as definições apresentadas na literatura a respeito da auditoria de sistemas, é correto afirmar que a auditoria de sistemas de informação

a) pode ser feita por profissionais internos à empresa proprietária dos sistemas

b) não abrange os sistemas de bancos de dados da empresa.

c) não pode ser feita por profissionais externos à empresa proprietária dos sistemas

d) não se importa com o tipo de controles existentes nos sistemas de informação.

e) somente deve ser feita uma vez a cada dois anos.

(FIOCRUZ – Analista de Gestão em Saúde – Gestão de Tecnologia da Informação – 2010 – FGV)

2. A Auditoria pode ser considerada como um mecanismo de:

a) controle que deve ser usado em serviços para o negócio.

b) controle de armazenamento de informação.

c) gerenciamento autoritário da informação.

d) gestão de transmissão e armazenamento de informação.

e) recuperação e conferência de processos.

(TCE-RJ – Analista de Controle Externo – Tecnologia da Informação – 2012 – FEMPERJ)

3. Uma auditoria de TI deve estar atenta:

a) aos parâmetros acordados de entrega de serviços, pois a área de TI deve estar estruturada adequadamente para atender aos SLAs (Service Level Agreement) nos contratos;

b) ao processo de gerenciamento de mudanças, para garantir que, depois de um incidente imprevisível, os serviços de TI possam ser restaurados dentro dos limites de tempo preestabelecidos;

c) ao planejamento orçamentário de TI, que deverá acompanhar a execução do planejamento institucional, não podendo haver ajustes em decorrência de variações no suprimento orçamentário ou de mudanças nas demandas;

d) à terceirização de serviços de TI, que não pode ser utilizada em atividades-meio da instituição;

e) ao uso de técnicas de auditoria assistidas por computador, pois essa decisão só pode ser tomada na fase de planejamento e não no decorrer dos exames.

4. Ao final de um processo de auditoria, o relatório fnal deve:

a) conter necessariamente a opinião do auditor sobre as não conformidades encontradas;

b) ser revisado por toda a equipe de auditores, para evitar inconsistências;

c) relatar todas as falhas encontradas, não sendo recomendada a divisão nas sub-áreas auditadas;

d) ser bem detalhado, não devendo conter uma síntese dos resultados obtidos, para evitar possíveis interpretações errôneas por parte da alta direção;

e) ser objetivo e estritamente técnico, não cabendo pareceres da gerência superior sobre os achados e recomendações dos auditores.

5. Se, durante a realização de um processo de auditoria de TI, for encontrada uma evidência considerada incompatível com a auditoria em execução, tal fato:

a) pode servir para indicar a necessidade de realização de outra auditoria;

b) demonstra que a fase de planejamento da auditoria não foi adequada;

c) deve ser considerado irrelevante, se a auditoria for interna;

d) deve ser desconsiderado, por não ser relevante;

e) comprova uma falha na governança corporativa da instituição auditada.

6. O processo de auditoria de TI deve procurar respeitar certas linhas de ação, como, por exemplo, aquela que diz que:

a) o auditor deve ser um funcionário da organização auditada, trabalhando no setor analisado;

b) a auditoria procura primordialmente garantir o processo de aquisição de produtos e serviços de TI;

c) durante a fase de planejamento, o auditor deve reunir a maior quantidade possível de informações sobre a entidade auditada e seu ambiente de TI;

d) todas as falhas e irregularidades encontradas na fase de execução devam ser coletadas para que os devidos controles sejam implantados na fase seguinte da auditoria;

e) ferramentas computacionais de apoio à auditoria devem ser evitadas, em razão da falta de segurança dos softwares nessa área.

7. Entrevistas, questionários e técnicas de análise de dados, entre outros, podem ser usados em uma auditoria de TI:

a) para detecção de falhas e irregularidades nos processos da instituição auditada, descobertas na fase de planejamento;

b) desde que estejam ausentes do relatório fnal apresentado;

c) como técnicas para defnir previamente o escopo da auditoria e o grau de profundidade de sua verifcação;

d) como parte da metodologia utilizada na fase de execução;

e) para determinar os objetivos de controle a serem alcançados ou os efeitos negativos a serem evitados.

8. Ao longo de uma auditoria de TI, o auditor deve aplicar testes de conformidade e testes substantivos. Com relação a esses últimos, o objetivo é verificar se:

a) de fato realmente ocorreu o que está registrado;

b) os controles internos estão sendo executados na forma determinada pela organização;

c) os funcionários estão respeitando as normas internas;

d) os resultados estão sendo devidamente comunicados aos responsáveis;

e) as falhas e irregularidades encontradas poderiam ter sido evitadas.

(TCE-GO – Analista de Controle Externo – Tecnologia da Informação – 2014)

9. [90] Em relação ao processo e organização da função de auditoria de TI, é correto afirmar:

(A) A responsabilidade por aspectos técnicos específicos de TI permanece com os dirigentes da organização e não pode ser delegada. Mas, a responsabilidade pelo uso e entrega aceitável, eficaz e eficiente da TI pela organização pode ser delegada aos gerentes.

(B) Controle externo é uma ferramenta do gestor usada para prover razoável certeza de que os objetivos da Administração estão sendo alcançados.

(C) O gestor e a alta Administração são responsáveis pelos controles da organização, mas os processos de gestão de risco são delegados e controlados pela equipe de TI.

(D) Auditores são parte do modelo governamental de controle interno, mas eles não são responsáveis pela implementação dos procedimentos de controle em uma organização. Este trabalho é do gestor.

(E) As etapas típicas de uma auditoria de TI são: Planejar; Organizar; Adquirir; Implementar; Entregar; Monitorar e Avaliar.

10. [91] Durante um processo de auditoria externa independente, na área financeira contábil de uma entidade, instaurou-se uma auditoria interna para avaliar os sistemas de atestação de acessos aos sistemas de informação. Segundo as recomendações de prática de auditoria, o Auditor Interno da TI deve

(A) estar subordinado ao gerente de TI responsável pelos processos de gestão de acesso, ou gerente responsável pela segurança de informações.

(B) ter autonomia de ação, não estando sujeito a constrangimento profissional ou subordinação que comprometa sua liberdade de ação.

(C) dar publicidade para qualquer interessado sobre todas as informações que obtiver durante o processo de auditoria.

(D) estar vinculado a uma entidade externa e independente da entidade auditada, ou seja, não deve fazer parte do quadro de funcionários da entidade auditada.

(E) controlar os trabalhos do auditor externo independente e monitorar os resultados apresentados por este.

11. [92] Para um Auditor que examinará os controles internos da área de tecnologia da informação, NÃO é fator determinante do escopo da auditoria:

(A) a materialidade.

(B) a natureza de negócio da entidade.

(C) a inexistência de riscos de auditoria.

(D) as exigências legais e regulatórias.

(E) as características de organização da entidade.

12. [93] Uma empresa foi contratada pela primeira vez para prestar serviços de auditoria sobre as atividades da área de TI de uma instituição. Os trabalhos de auditoria foram executados sem observância de trabalhos anteriores que haviam sido realizados por outras empresas de auditoria, os quais são relevantes para o objetivo da auditoria. Na execução da auditoria foi alocado um Auditor que não era especialista em TI. Assim sendo,

(A) a prática de não consultar pareceres de auditorias anteriores foi correta para garantir o princípio da isenção.

(B) a alocação de um Auditor não especializado em TI foi correta para garantir maior nível de investigação, provocando exploração minuciosa através da indagação sobre os assuntos técnicos.

(C) a alocação de um Auditor não especializado em TI foi correta para garantir o princípio de isenção de avaliação e dos pareceres.

(D) a prática de não consultar pareceres de auditorias anteriores foi incorreta, pois o planejamento dos trabalhos de auditoria deve incluir o uso de trabalhos anteriores relevantes.

(E) o Auditor alocado pode não ser especializado na área de auditoria, desde que utilize os trabalhos de auditorias anteriores.

~~13. [94] Após concluir um processo de auditoria interna sobre a proteção de dados e informações armazenadas em meio magnético para backup, o Auditor emitiu um parecer com negativa de opinião. Esse parecer demonstra que~~

~~(A) não foi encontrado qualquer fato que aponte descumprimento de normas estabelecidas na entidade auditada para a proteção de dados.~~

~~(B) a proteção ocorre, praticamente, dentro das normas estabelecidas na entidade auditada, existindo uma ou mais exceções que não~~

comprometem de forma expressiva os compromissos.

(C) a proteção de dados e informações ocorre totalmente fora das normas estabelecidas na entidade auditada.

(D) o Auditor não concluiu os trabalhos, sendo esse parecer um documento preliminar de uma auditoria em andamento.

(E) o Auditor não emitiu opinião por não ter obtido evidência adequada para fundamentar seus argumentos.

14. [99] Em uma auditoria de contratos firmados pela área de TI, o Auditor registrou achados de auditoria, os quais são

(A) fatos sobre os contratos apontados pelo auditado como aqueles que devem ser considerados na auditoria, com avaliação corroborada entre auditado e Auditor.

(B) padrões de trabalho determinados no manual técnico de auditoria, utilizado por todo Auditor interno operacional e externo operacional.

(C) fatos não relacionados com o escopo da auditoria, que podem ser de interesse da entidade em futuros trabalhos de auditoria interna.

(D) fatos relevantes para sustentar as conclusões da auditoria, os quais devem ser devidamente evidenciados.

(E) pareceres do Auditor, emitidos ao final dos trabalhos de auditoria ou constantes em relatórios intermediários de andamento dos trabalhos.

(CHESF – Analista de Sistemas – 2012 – Cesgranrio)

15. [43] O governo dos EUA promulgou a Lei Sarbanes-Oxley (SOX) que se aplica, inclusive, a empresas internacionais que possuam determinados vínculos com as bolsas de valores americanas. Na seção 404, essa lei determina que um relatório anual da empresa inclua um relatório da administração sobre controles internos que contenha, entre outras informações, a seguinte:

a) declaração identificando os procedimentos (frameworks) usados pela administração para conduzir a avaliação sobre a eficácia dos controles internos da empresa sobre seus relatórios financeiros.

b) declaração anual sobre os controles e procedimentos internos e externos para a emissão de relatórios financeiros, que atribua aos gerentes operacionais a responsabilidade pela avaliação periódica desses controles.

c) análise das avaliações mensais dos controles e procedimentos externos para a emissão de relatórios de conformidade, que seja homologada pelos diretores financeiros da empresa.

d) análise das avaliações trimestrais dos controles e procedimentos internos para a emissão de relatórios financeiros, homologada pelos gerentes operacionais da empresa.

e) relatório dos controles e procedimentos internos e externos adotados pelos stakeholders para emissão de relatórios financeiros.

(TRE SP – Analista Judiciário – Análise de Sistemas – 2012 – FCC)

16. [45] No tocante a auditoria de TI, principalmente aos fundamentos de controles internos, considere:

I. Os principais objetivos de um sistema geral de controle, entre outros, são salvaguardar o ativo de uma organização, manter a integridade, correção e confiabilidade dos registros contábeis.

II. A gerência por objetivos, procedimentos e tomada de decisões deve manter um controle que a capacite a uma supervisão efetiva dentro do ambiente de tecnologia da informação.

III. As responsabilidades e ocupações compatíveis devem estar segregadas de maneira a minimizar as possibilidades de perpetuação de fraudes e até de suprimir erro e irregularidade na operação normal.

Está correto o que consta em

a) III, apenas.
b) I e III, apenas.
c) I e II, apenas.
d) II e III, apenas.
e) I, II e III.

(TCE GO – Analista de Controle Externo - TI– 2009 – FCC)

17. [92] Políticas, procedimentos, práticas e estruturas organizacionais desenvolvidas para dar razoável garantia de que os objetivos do negócio serão alcançados e que os eventos indesejáveis serão prevenidos ou detectados e corrigidos definem o conceito de

a) Controle.
b) objetivo de controle.
c) técnica de auditoria.
d) processo de auditoria.
e) governança de TI ou corporativa.

18. [94] Na relação entre risco de auditoria e relevância,

I. quanto maior o risco, maior será o valor estabelecido como nível de relevância.

II. quanto maior a relevância de um item, menor é a possibilidade de ele não ser selecionado para teste.

III. o auditor deve selecionar o item que será examinado para diminuir o risco.

Está correto o que se afirma em

a) I, II e III.
b) I, apenas.
c) I e II, apenas.
d) I e III, apenas.
e) II e III, apenas.

19. [95] NÃO se trata de uma conformidade normalmente já incluída no arquivo de auditoria, cuja documentação em separado seja desnecessária,

a) o plano de auditoria.
b) o julgamento significativo do auditor.
c) a carta de contratação de auditoria.

d) o parecer do auditor com ressalva.
e) a ata de reunião com a participação do responsável pelo trabalho de auditoria.

20. [96] Quando os procedimentos de controle são adequados e aplicados de forma apropriada e consistente pela organização, os testes de auditoria.
a) de conformidade e substantivos são desnecessários.
b) de conformidade podem ser limitados.
c) de conformidade devem ser significativos.
d) substantivos podem ser limitados.
e) substantivos devem ser significativos.

~~**(TRE-SP – Analista Judiciário – Análise de Sistemas – 2012 – FCC)**~~

~~21. [23] São objetivos da auditoria, EXCETO:~~

~~a) Assegurar a adequação do sistema de controles que está implantado e que está sendo utilizado.~~

~~b) Determinar se os recursos estão sendo utilizados em função da análise de custo e benefício.~~

~~c) Gerenciar os riscos da organização e tomar ações para solucionar os problemas porventura identificados.~~

~~d) Checar se os ativos estão salvaguardados apropriadamente~~

~~e) Revisar a integridade, confiabilidade e eficiência do sistema de informação e dos relatórios financeiros nele produzidos.~~

~~**(TRE-RS – Analista Judiciário – Analista de Sistemas – 2010 – FCC)**~~

~~22. [60] Sobre auditoria no sistema de segurança da informação, considere:~~

~~I. Um critério de auditoria pode ser uma norma ou um conjunto de políticas, procedimentos ou requisitos.~~

~~II. O programa de auditoria precisa garantir a melhoria contínua e, para tanto, utilizar o ciclo PDCA.~~

~~III. A utilização de uma metodologia de gestão de projetos associada à etapa de implementação do programa de auditorias gera resultados muito positivos.~~

~~IV. Os procedimentos de auditoria precisam ser definidos mas não devem fazer parte da política de segurança da informação.~~

~~Está correto o que consta em~~

~~a) I, II, III e IV.~~
~~b) I e III, somente.~~
~~c) II e IV, somente.~~
~~d) I, II e III, somente.~~
~~e) II, III e IV, somente.~~

~~**(TRE-SP – Analista Judiciário – Análise de Sistemas – 2012 – FCC)**~~

~~23. [48] Os objetivos globais referentes à auditoria de sistemas aplicativos NÃO incluem~~
~~a) integridade e privacidade~~
~~b) confidencialidade e disponibilidade.~~
~~c) acuidade e auditabilidade.~~
~~d) versatilidade e manutenibilidade.~~
~~e) irreversibilidade e retratabilidade.~~

~~**(TCE-AP – Analista de Controle Externo – Controle Externo – TI – 2012 – FCC)**~~

~~24. [72] A técnica de auditoria denominada test-deck trata-se de~~
~~a) uma tabulação de um arquivo log para verificar a utilização de um recurso computacional.~~
~~b) um rastreamento do processamento para avaliar o caminho de uma transação.~~
~~c) um mapeamento do processamento para identificar rotinas não utilizadas.~~
~~d) uma simulação de dados para testar processos computacionais.~~
~~e) uma análise de dados para avaliar a integridade das informações.~~

~~**(TCE-AP – Analista de Controle Externo – Controle Externo – TI – 2012 – FCC)**~~

~~25. Para assegurar que as medidas de controle estabelecidas estejam funcionando como prescrito de maneira consistente e contínua e para concluir sobre a adequação do ambiente de controle, os passos de auditoria são estabelecidos, em uma guia de auditoria, na etapa~~
~~a) obtendo um entendimento.~~
~~b) avaliando os controles.~~
~~c) elaborando o relatório.~~
~~d) avaliando a conformidade.~~
~~e) evidenciando o risco.~~

~~**(TRE-SP – Analista Judiciário – Análise de Sistemas – 2012 – FCC)**~~

~~26. [21] Sobre Auditoria de TI, analise:~~

~~I. Nos projetos de TI a auditoria tem ênfase na análise do passado e não na avaliação atual dos processos da empresa para definir ações futuras.~~

~~II. Todos os processos de auditoria são reativos, ou seja, buscam culpados por determinadas ocorrências geradas, as quais tenham ou não trazido determinados riscos operacionais ou mesmo de imagem à corporação.~~

~~III. O CobiT pode ampliar a visão da auditoria interna possibilitando uma melhor identificação dos riscos relacionados com a TI e a apresentação de resultados consistentes, com baixo grau de refutação por parte dos auditados.~~

~~IV. Os resultados das auditorias podem provocar discussões internas e a identificação da necessidade de evolução da maturidade dos processos e do modelo de governança de TI, que deve estar sustentada pela Governança Corporativa.~~

Está correto o que consta em

a) III, apenas.
b) II e IV, apenas.
c) III e IV, apenas.
d) I, II e III, apenas.
e) I, II, III e IV.

(TRE SP – Analista Judiciário – Análise de Sistemas – 2012 – FCC)

27. [22] Sobre as etapas do processo de auditoria interna de TI é correto afirmar:

a) Possui 6 etapas: Planejamento, Análise, Projeto, Execução, Relatório e Plano de Ação.
b) A identificação e apresentação dos Pontos de Auditoria ocorrem apenas em duas fases do processo de auditoria: no Planejamento da Auditoria e no Relatório de Auditoria.
c) Os documentos resultantes da Auditoria de TI são apresentados apenas à área de TI, pois mostra a direção a ser tomada e os investimentos prioritários e necessários apenas nessa área.
d) Tem como resultado alguns documentos que geralmente contêm informações sobre os riscos encontrados e a avaliação desses riscos, os controles em conformidade ou não com normas, e recomendações de melhoria.
e) Apesar do relatório de auditoria funcionar como um mapa que mostra a direção a ser tomada pela área de TI, ele não serve como um guia para auxiliar a administração no planejamento estratégico e na priorização de investimentos, pois apresenta informações técnicas de interesse exclusivo da área de TI.

(TCE SE – Analista de Controle Externo – Coordenadoria de Informática – 2011 – FCC)

28. [72] Em uma auditoria, se os controles se apresentam estabelecidos

a) adequadamente e forem aplicados consistentemente, nos testes de conformidade, determinarão as necessidades de testes substantivos de abrangência limitada.

b) inadequadamente e forem aplicados consistentemente, nos testes de conformidade, determinarão as necessidades de testes substantivos de abrangência significativa.

c) adequadamente e forem aplicados consistentemente, nos testes substantivos, determinarão as necessidades de testes de conformidade de abrangência limitada.

d) inadequadamente e forem aplicados consistentemente, nos testes substantivos, determinarão as necessidades de testes de conformidade de abrangência significativa.

e) inadequadamente ou forem aplicados inconsistentemente, nos testes substantivos, determinarão as necessidades de testes de conformidade de abrangência significativa.

29. [73] Sobre a documentação de auditoria, considere:

I. O conteúdo da documentação deve ser registrado apenas em papel para facilitar a apresentação de evidências.

II. Resumos ou cópias de registros da entidade podem ser incluídos na documentação.

III. Versões superadas de papéis de trabalho e de demonstrações financeiras não precisam ser incluídas na documentação.

IV. A existência de plano de auditoria demonstra que o auditor planejou a auditoria.

Está correto o que se afirma em

a) I, II, III e IV.

b) II, III e IV, apenas.

c) I e III, apenas.

d) II e IV, apenas.

e) II, apenas.

30. [74] No processo de Avaliação de Riscos, no qual são executadas as análises da relevância dos riscos identificados nas entidades do setor público, NÃO se inclui

a) a forma de como serão gerenciados.

b) a avaliação das probabilidades de suas ocorrências.

c) a resposta aos riscos, indicando a decisão gerencial para mitigá-los, considerando as hipóteses de eliminação, redução, aceitação ou compartilhamento.

d) a definição das ações para prevenir ocorrências ou para minimizar os seus efeitos.

e) o acompanhamento dos pressupostos do controle interno.

31. [75] O controle interno exercido em todos os níveis das entidades do setor público é classificado nas seguintes categorias:

a) operacional, contábil e normativo.

b) operacional, contábil e gerencial.

c) operacional, tático e estratégico.

d) contábil, gerencial e estratégico.

e) normativo, gerencial e estratégico.

(ABIN – Agente Técnico de Inteligência – TI – 2010 – Cespe)

Acerca de auditoria na área de tecnologia da informação (TI), julgue o item abaixo.

32. [108] A auditoria realizada em TI engloba a verificação de operações, processos, sistemas e responsabilidades.

(SEBRAE II – AN07 – Analista Técnico II – 2010 - Cespe)

A respeito das ferramentas de extração de dados, julgue os seguintes itens.

33. [57] A utilização de software generalista de auditoria de tecnologia de informação envolve o uso de programa específico, o que inibe a extração de dados de vários ambientes distintos para a realização da auditoria.

(SEF SC – Tecnologia da Informação – 2010 – CESPE)

34. [56] Com relação à auditoria de segurança de sistemas, assinale a alternativa correta.

a) Em um processo de auditoria de sistema, o auditor deve necessariamente ser um colaborador da organização auditada, preferencialmente, deve pertencer ao setor analisado na auditoria.

b) Achados de auditoria são fatos significativos observados pelo auditor durante a execução da auditoria. Geralmente, são associados a falhas e irregularidades, porém podem também indicar pontos fortes da instituição auditada. O achado deve ser relevante e baseado em fatos e evidências irrefutáveis.

c) A auditoria da segurança de informação tem como principal objetivo implantar a política de segurança e o plano de continuidade de negócios (PCN) de uma organização.

d) O processo de auditoria está divido em três fases: planejamento, execução e relatório. Na fase de planejamento, todas as evidências das falhas e irregularidades encontradas devem ser coletadas para que durante a fase de execução as devidas correções nos controles sejam realizadas.

e) Devido à falta de confiabilidade dos dados processados por computador, ferramentas computacionais de apoio, tais como mapping, tracing e snapshot, não podem ser empregadas em auditorias de segurança.

(TCU – Analista de Controle Externo – TI – 2007 – CESPE)

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.

35. [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.

36. [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 [julgue itens]

37. [189] se há política de segurança de informação no órgão auditado e avaliar o seu conteúdo e efetividade, por meio de testes de auditoria.

38. [190] a localização de sítio backup, assegurando que ele fique perto da base original de dados, para facilitar o acesso em caso de emergência.

39. [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.

40. [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.

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

41. [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.

42. [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

43. [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.

44. [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.

(INMETRO – Analista em Métricas e Qualidade – Ciências da Computação – 2007 – CESPE)

Julgue os próximos itens, relativos a conceitos de auditoria e controle de riscos em tecnologia da informação (TI).

~~45. [113] Uma das principais funções de um auditor de TI é avaliar se as configurações dos sistemas computacionais implantadas pelos técnicos de TI dessa organização estão aderentes aos padrões de segurança estabelecidos pelo mercado.~~

~~46. [114] O modelo COBIT propõe, para fins de auditoria, que os processos de gestão de TI de uma organização sejam classificados em quatro domínios: planejamento e organização do desenvolvimento de software; aquisição e desenvolvimento de sistemas; entrega e suporte de serviços de software; e monitoramento de redes.~~

47. [115] O uso de ferramentas de teste de penetração de rede, como o nmap, não deve ser realizado durante uma atividade de auditoria, pois o teste de aderência a controles e políticas de segurança em redes está fora do escopo do trabalho do auditor.

48. [116] Considere que, durante a auditoria de planos de contingência e recuperação de desastres, tenha sido identificado que a última revisão do plano havia sido efetuada há três meses. Nessa situação, mesmo que a organização não tenha sofrido no último ano nenhuma mudança significativa nas áreas administrativas no ambiente competitivo externo nem em seu ambiente de TI, uma das recomendações da auditoria seria a imediata revisão do plano.

~~49. [117] A emissão de um relatório definitivo de uma auditoria de sistemas de informações não precisa ser precedida de uma validação dos achados junto aos representantes da organização auditada, a fim de que não haja distorção ou pressão sobre os resultados da auditoria.~~

~~50. [118] Após uma auditoria, as recomendações para a separação de técnicos de uma organização de desenvolvimento de sistemas em duas equipes: de desenvolvimento e de teste, podem ser diretamente embasadas no princípio da segregação de responsabilidades.~~

51. [119] Ao encontrar, em uma área pública de um servidor, um arquivo contendo a lista de logins e senhas criptografadas usadas no controle de acesso a um sistema, o auditor deverá aumentar a classificação de risco de que esse sistema seja invadido por meio de um ataque de dicionário.

52. [120] Ao atuar na avaliação das funções de um help desk, o auditor estará mais focado na adequação dos aspectos operacionais de uma organização que nos aspectos de desenvolvimento de projetos dessa organização.

~~**(TJ-PE – Analista Judiciário – Analista de Suporte – 2007 – FCC)**~~

~~53. [29] Em auditoria de sistemas, para verificar se os controles estão funcionando conforme prescrito, consistentemente e continuamente, utiliza-se:~~

~~a) documentação dos requisitos de negócio.~~

~~b) documentação das evidências.~~

~~c) teste de conformidade.~~

~~d) teste substantivo.~~

~~e) identificação dos pontos de controle.~~

~~54. [30] Para uma avaliação de auditoria nas funcionalidades das transações de negócio realizadas por um sistema em operação normal, deve-se utilizar a técnica~~

~~a) test-deck.~~

~~b) teste beta.~~

~~c) teste de desempenho.~~

~~d) análise de dados.~~

~~e) verificação in-loco.~~

(TSE – Analista Judiciário – Análise de Sistemas – 2007 – CESPE)

55. [76] Julgue os seguintes itens acerca da formalização, controle e auditoria de sistemas.

I Os controles incluem políticas, procedimentos e práticas estabelecidas visando prover uma garantia que determinados objetivos serão atingidos. Os controles internos procuram reduzir a exposição a riscos.

II A análise de riscos pode ser parte de um plano de auditoria e visa auxiliar a identificação de riscos e vulnerabilidades de modo que o auditor possa determinar os controles necessários para reduzir esses riscos.

III Alguns controles são preventivos, pois tentam identificar problemas e evitar erros antes que ocorram. Como exemplo de controles preventivos, têm-se o emprego de pessoal qualificado e o controle do acesso às instalações físicas.

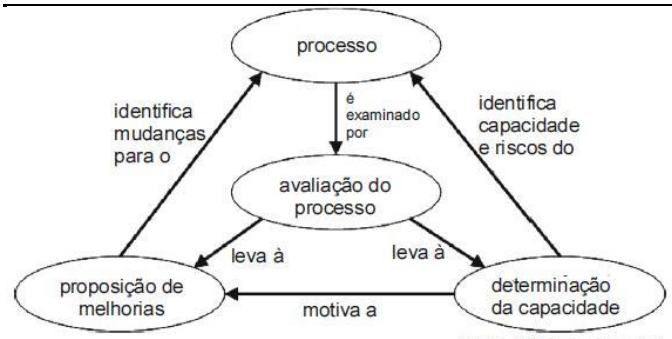
IV Em uma auditoria, há procedimentos que visam identificar a área a ser auditada, os objetivos da auditoria e os sistemas a serem auditados; planejar a auditoria; testar a aderência aos controles e elaborar relatório.

V Em qualquer auditoria, para evitar a ocorrência de erros, todas as transações e eventos são verificados. Nenhuma auditoria pode se basear em amostragens coletadas usando-se métodos estatísticos.

A quantidade de itens certos é igual a

a) 1.
b) 2.
c) 3.
d) 4.

(DATAPREV – Analista de TI – Auditor de Sistemas – 2006 – CESPE)



SPICE, 1995 (com adaptações).

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.

56. [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.

57. [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.

58. [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.

59. [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.

60. [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.

~~61. [49] Não é papel central do auditor prover auxílio ao auditado.~~

~~62. [50] Não é atitude adequada do auditado receber elogiosamente o auditor.~~

~~63. [51] A atitude do auditor perante o auditado deve ser imparcial, inflexível, impessoal e independente.~~

~~64. [52] Durante o relacionamento com o auditado, a subjetividade, a capacidade de argumentação e a atitude crítica não são atributos desejáveis de um auditor.~~

~~65. [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.~~

~~66. [54] Os objetivos do controle externo, conforme definidos no âmbito da legislação federal sobre controle e auditoria, são idênticos aos da auditoria interna.~~

~~67. [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.~~

68. [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.

69. [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.

70. [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.

71. [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.

72. [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.

73. [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.

74. [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.

(CGU – Analista de Finanças e Controle – TI – 2006 – ESAF)

75. [61] Analise as seguintes afirmações relacionadas a Auditoria de Sistemas.

I. O auditor de Tecnologia da Informação deve ser ligado diretamente à área sob auditoria, devendo ser, preferencialmente, um funcionário ou ter um cargo nessa área.

II. O colaborador a ser auditado deve planejar as tarefas de auditoria para direcionar os objetivos da auditoria e seguir os padrões profissionais aplicáveis.

III. O auditor de Tecnologia da Informação deve requisitar e avaliar informações apropriadas sobre pontos, conclusões e recomendações anteriores e relevantes para determinar se ações apropriadas foram implementadas em tempo hábil.

IV. De acordo com o código de ética profissional da Associação de Auditores de Sistemas e Controles, seus membros devem manter privacidade e confidencialidade das informações obtidas no decurso de suas funções, exceto quando exigido legalmente. Indique a opção que contenha todas as afirmações verdadeiras.

a) I e II
b) II e III
c) III e IV
d) I e III
e) II e IV

76. [62] Analise as seguintes afirmações relacionadas a Auditoria de Sistemas.

I.A gerência da empresa deve estabelecer critérios para a criação, processamento e disseminação de informações de dados, por meio de autorização e registro de responsabilidade.

II. A gerência deve implementar um plano adequado, bem como procedimentos de implantação para prevenir-se contra falhas de controle que podem surgir durante especificações de sistemas, desenho, programação, testes e documentação de sistemas.

III. A gerência deve ter acesso restrito de "somente leitura" ao sistema, ficando o controle sob a responsabilidade dos colaboradores auditados.

IV. Para um bom andamento e independência das auditorias, nenhum investimento em treinamentos em tecnologia da informação deve ser realizado ou planejado para a equipe de auditores do quadro de colaboradores da organização. Indique a opção que contenha todas as afirmações verdadeiras.

a) I e II
b) II e III
c) III e IV
d) I e III
e) II e IV

77. [63] De acordo com o Código de Ética Profissional, os membros e detentores de certificações da ISACA devem

a) repassar ou transferir conhecimento aos acionistas evitando, assim, que tenham um aumento de sua compreensão dos controles dos sistemas de informação.

b) evitar repassar qualquer tipo de informação dos resultados obtidos no trabalho às partes competentes.

c) evitar qualquer tipo de conhecimento no campo de atuação a ser auditado e concordar em atuar apenas com as atividades onde não tenham envolvimento profissional.

d) servir aos interesses dos acionistas de forma honesta e legal, mantendo altos padrões de conduta e caráter, não se envolvendo em atos desonrosos à profissão.

e) manter as informações obtidas no curso de suas atividades disponíveis para a consulta de terceiros.

78. [65] As ferramentas utilizadas nas auditorias de Tecnologia da Informação normalmente auxiliam na extração e seleção de dados e podem fornecer relatórios com indicativos de desvios. Essas ferramentas e as técnicas por elas utilizadas proporcionam ao usuário vantagens como: ganho na produtividade, redução de custo e qualidade. Quanto a essas técnicas e ferramentas utilizadas nas auditorias de TI é correto afirmar que a técnica denominada "Rastreamento e Mapeamento" envolve

a) a verificação da lógica de programação para certificar que as instruções dadas ao computador são as mesmas já identificadas nas documentações do sistema.

b) a inclusão de lógicas de auditoria nos sistemas quando são desenvolvidos.

c) o uso de um programa especialmente desenvolvido para processar transações e dados anteriormente executados numa rotina normal e operacional com o objetivo de verificar se os resultados são idênticos.

d) a simulação de operações normais com o objetivo de estimular a verificação de resultados recorrentes que são inconsistentes.

e) o desenvolvimento e implementação de uma trilha de auditoria para acompanhar certos pontos da lógica do processamento de algumas transações.

79. [68] Os objetivos da auditoria de redes de computadores são certificar-se da

a) existência do controle de versões.

b) possibilidade de geração de relatórios gerenciais.

c) eficácia na identificação da existência de problemas com fornecedores e se os mesmos são significativos ou repetitivos.

d) eficácia na avaliação da plataforma adotada, verificando se está de acordo com os padrões e necessidades da empresa.

e) confidenciabilidade da rede quanto à segurança de enlace, assegurando que as linhas e canais de transmissão entre unidades e localidades remotas obedecendo aos limites estabelecidos.

80. [69] Os objetivos da auditoria de plano de contingência e de recuperação de desastres de uma empresa são certificar-se de que

a) a equipe de contingência está preparada para realizar um treinamento no momento de ocorrência de um desastre.
b) esses planos são testados periodicamente.
c) o sistema de qualidade executa suas tarefas periodicamente.
d) existe a possibilidade de se desenvolver planos que contemplem todas as necessidades de contingências.
e) o sistema de recuperação de backups é lento e não satisfaz plenamente ao desejado pela organização.

81. [70] Analise as seguintes afirmações relacionadas à emissão de relatórios de auditoria de sistemas de informação.

I. Um relatório de auditoria deverá ser emitido exclusivamente nos padrões da empresa realizadora da auditoria.

II. Um relatório de auditoria deverá apontar riscos em que a empresa incorre em decorrência das fraquezas apontadas.

III. Um relatório de auditoria deverá responsabilizar a alta administração da empresa quanto à elaboração de sugestões ou medidas de correção.

IV. Um relatório de auditoria deverá fazer um apontamento de prazos para implementações de medidas ou plano de ações. Indique a opção que contenha todas as afirmações verdadeiras.

a) I e II
b) II e III
c) III e IV
d) I e III
e) II e IV

Gabarito.

1. A.
2. A.
3. A.
4. B.
5. A.
6. C.
7. D.
8. A.
9. D.
10. B
11. C.
12. D.
13. E.
14. D.
15. A.
16. C.
17. A.
18. E.
19. B.
20. D.
21. C.
22. D.
23. E.
24. D.
25. D.
26. C.
27. D.
28. A.
29. B.
30. E.
31. A.
32. C.
33. E.
34. B.
35. E.
36. C.
37. C.
38. E.
39. C.
40. C.
41. E.
42. E.
43. X.
44. E.
45. E.
46. E.
47. E.
48. E.
49. E.
50. C.
51. C.
52. C.
53. C.
54. A.
55. D.
56. E.
57. E.
58. C.
59. C.
60. C.
61. C.
62. C.
63. E.
64. C.
65. E.
66. E.
67. C.
68. E.
69. E.
70. C.
71. C.
72. C.
73. E.
74. C.
75. C.
76. A.
77. D.
78. E.
79. E.
80. B.
81. E.