**Exercícios Para Prova Final**

01- Quais são os seis controles gerais que devem ser considerados em auditorias de sistemas?

R.: Controles organizacionais, programa de segurança, continuidade do serviço, controles de software de sistema, controle de acesso e controle de desenvolvimento e alteração de softwares.

Ou

Controle organizacionais, Controle de mudanças, Controle de operação dos sistemas, Controle sobre Banco de Dados, Controle sobre microcomputadores, Controle sobre ambiente cliente/servidor,

02- Descreva o novo papel da auditoria e o novo papel da área de informática nesses tempos dentro das organizações.

R.: **Novo papel da auditoria:** Assessoria, emissão de opiniões e proposta de ações de otimização

**Papel da área de informática**: Consultoria quanto à tecnologia de PED, buscando melhoria em processos e resultados

03- Quando a segurança lógica e física são os focos da auditoria, existem vários controles que podem ser observados. Cite três de cada foco.

R.: físico: formas de identificação; controles de e/s de eqptos, controles de pessoas, vigilância 24 hs; devolução de equipamentos; proteger linhas telefônicas; proteger os backups; etc.

Lógica: acessos aos usuários; criptografia; fornecer contas as pessoas autorizadas somente; cuidado com as senhas; desabilitar contas inativas; limite de números de acessos, etc.

04- 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 x

e) evidenciando os riscos

05- Acerca de auditoria na área de tecnologia da informação (TI), julgue o item abaixo.  
a auditoria realizada em TI engloba a verificação de operações, processos, sistemas e responsabilidades.

A) Certo x B) Errado

06- 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 x E) II e IV

07- 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.

A) Certo B) Errado x

08- 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.

A) Certo B) Errado b

09- Uma auditoria operacional de segurança da informação deve avaliar os controles por meio da análise, entre outros elementos, de sua robustez diante das vulnerabilidades e ameaças identificadas na análise de riscos.

A) Certo x B) Errado

10- 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 x

e) II, III e IV, somente

11- Qual das opções abaixo descreve melhor conceito de ¿Risco¿ quando relacionado com a Segurança da

Informação:

A) Probabilidade de um ativo explorar uma vulnerabilidade.

B) Probabilidade de uma ameaça explorar um incidente.

C) Probabilidade de uma ameaça explorar uma vulnerabilidade. x

D) Probabilidade de um incidente ocorrer mais vezes.

E) Probabilidade de um ativo explorar uma ameaça.

12- Existe uma série de fatores que impactam na segurança de uma organização. A ausência de um mecanismo de proteção ou falhas em um mecanismo de proteção existente está relacionada com o conceito de:

A) Risco B) Vulnerabilidade x C) Valor D) Ameaça E) Impacto.

13- Corrigir pontos vulneráveis ou pontos fracos que circulam em um setor que trabalha com a informação, não acabará, mas reduzirá em muito os riscos em que ela estará envolvida. Logo estará evitando como também prevenindo a concretização de possíveis ameaças. Baseado neste fato podemos denominar como Vulnerabilidade Física:

A) Possibilidade de desastres naturais (incêndios, enchentes, terremotos, tempestades, falta de energia).

B) Acessos não autorizados ou perda de comunicação e a ausência de sistemas de criptografia nas comunicações.

C) Terrorismo ou vandalismo (ameaça de bomba, sabotagem, distúrbios civis, greves, roubo, furto, assalto, destruição de propriedades ou de dados, invasões, guerras, etc.).

D) Instalações prediais fora dos padrões de engenharia e salas de servidores mal planejadas. x

E) Problemas nos equipamentos de apoio (acúmulo de poeira, aumento de umidade e de temperatura).

14- Quanto a auditoria dos Controles organizacionais (ambiente de TI), quais os principais tópicos a serem abordados?

R.: Responsabilidades organizacionais (estrutura de TI bem definida e documentada); Políticas, padrões e procedimentos; Estratégia da Informática; políticas sobre documentação; Gerencia de Recursos Humanos; Gerencia de recursos computacionais.

15- Cite alguns aspectos importantes a serem vistos na auditoria dos Controles de mudanças.

R.: Documentação detalhada de todas as mudanças aprovadas; Avaliação do impacto das mudanças; definição de custos para implementar as mudanças e também na sua manutenção; testar programas antes de colocá-los em produção; comunicar os usuários com antecedência sobre a programação das mudanças.

16- Cite características que devem ser encontradas nas auditorias em Ambiente de Operação de sistemas.

R.: Distribuição adequada de carga de trabalho entre os operadores; evidencias de supervisão total das operações dos sistemas e redes; analise diária do desempenho dos sistemas; implementação de uma gerencia de resolução de problemas (helpdesk); manter histórico dos problemas; estabelecer procedimentos de controles de acessos físicos e lógicos; rotinas de Backup; atualização de manuais e documentação diversas;

17- Na auditoria de ambiente de banco de dados, lembre e cite os principais pontos de controles a serem observados.

R.: Definição clara e documentação das responsabilidades relacionadas ao SGBD; segurança total nos dispositivos de segurança e procedimentos de autorização de acesso ao SGBD; controle de mudanças de versões; monitorar o sistema e registrar os logs; manter o SGBD atualizado.

18- No ambiente de microcomputadores, quais as principais evidencias a serem vistas em uma auditoria?

R: Inventario dos equipamentos; controles de E/S de pecas e equipamentos; padronização de hardware e software; uso de softwares contratados; uso de estabilizadores e no-breaks; manter organizado os registros de licenças; atualização de antivírus; esquema seguro de backup; utilização de senha seguras, etc.

19- Em ambiente cliente/servidor (redes), quais os aspectos importantes a serem auditados?

R.: Softwares e patches sempre atualizados; uso de criptografia; controle total de contas dos usuários e senhas; auditar sempre contas e arquivos; cuidados especiais com senha do administrador; monitorar o ambiente 24 hs por dia (IDS); monitorar os logs, políticas de backup; estudo de necessidade de redundância; limitação dos acessos físicos e lógicos; obrigatoriedade de firewall e Proxy bem configurado; etc.