Neste documento constam os gabaritos da 1a. prova presencial (Manhã), na página 1, e o da 1a. prova presencial (Tarde), na página 2, da disciplina de Segurança e Auditoria de Sistemas

1a. Prova Presencial Segurança e Auditoria de Sistemas (Manhã).

Questão 1)
A ISO/IEC 12207 agrupa os processos de ciclo de vida em processos fundamentais, em processos de apoio e em processo organizacionais. Descreva cada um deles e indique em qual processo a auditoria de computadores se enquadra.(9 pontos)
Processos fundamentais abrangem a contratação entre o adquirente e o fornecedor e a execução do desenvolvimento, da operação ou da manutenção de produtos de software durante o ciclo de vida do software. **Processos de apoio** são processos que auxiliam e contribuem para o sucesso e qualidade do projeto de software. Um processo de apoio é empregado e executado, quando necessário, por um dos seguintes processos. **Processos organizacionais** são processos que são empregados por uma organização para estabelecer e implementar uma estrutura constituída pelos processos de ciclo de vida e pelo pessoal envolvido no desenvolvimento de software. O processo de auditoria se enquadra nos processos de apoio.

Questão 2)
O processo de auditoria pode ser dividido em três grandes fases: planejamento, execução e fechamento. Com base nesta afirmativa, descreva o objetivo principal de cada uma destas fases (9 pontos)
A fase de planejamento ou pré-auditoria identifica-se os **instrumentos indispensáveis** à sua realização (recursos, área de verificação, metodologias, objetivos de controle e procedimentos a serem adotados). Ao longo da execução da auditoria, deve **reunir evidências suficientemente confiáveis**, relevantes e úteis para a realização da auditoria. Na finalização, o auditor normalmente apresenta seus achados e conclusões na forma de um relatório escrito.

Questão 3)
Ao longo da execução da auditoria, a equipe deve reunir evidências suficientemente confiáveis, relevantes e úteis para a realização da auditoria. Quais são estas evidências e como são descritas ? (9 pontos)
Evidência física: observações de atividades desenvolvidas pelos funcionários, gerentes, sistemas, equipamentos e etc. **Evidência documentária**: resultados de extração de dados, registros de transações e etc. **Evidência fornecida pelo auditado**: transcrições de entrevistas, cópias de documentos cedidos pelo auditado, fluxogramas, e-mails trocados com a gerência, relatórios e etc. **Evidência analítica**: comparações, cálculos e interpretações de documentos de entidades similares ou da mesma entidade em períodos de tempos diferentes.

Questão 4)
Quanto a forma de abordagem a auditoria pode ser horizontal ou orientada. Explique cada uma delas. (8 pontos)
Auditoria Horizontal: com tema específico realizada em várias entidades paralelamente; **Auditoria Vertical ou Orientada**: focada em uma atividade específica com fortes indícios de erros e fraudes.

1a. Prova Presencial Segurança e Auditoria de Sistemas (Tarde).

Questão 1)
Um sistema de informação pode ser definido como uma combinação organizada de pessoas, hardware, software, redes de computadores e dados que possibilita a coleta, transformação e a disseminação de informações em uma organização. Com base nessa definição, qual a função desempenhada por cada um dos elementos que fazem parte de um sistema de informação ?(9 pontos)
Um sistema de informação pode ser definido como uma combinação organizada de pessoas (especialistas e usuários finais), hardware (computadores e periféricos), software (sistemas operacionais, editores de texto, ferramentas de desenvolvimento, banco de dados e etc), rede de computadores (meios de comunicação, processadores de comunicações e etc) dados (descrição de produtos, banco de dados de estoque e etc) que possibilita a coleta, transformação e disseminação de informações em uma organização.

Questão 2)
Defina auditoria de computadores, campo, âmbito. Além disto, responda como área de verificação se relaciona com campo e âmbito ? (9 pontos)
Tipo de auditoria, essencialmente operacional, por meio da qual os auditores analisam os sistemas de informática, o ambiente computacional, a segurança das informações e o controle interno da entidade fiscalizada, identificando seus pontos fortes e/ou deficiências

Um campo engloba o **objeto** (entidade completa, uma parte selecionada ou uma função dessa entidade) a ser fiscalizado, o **período** a ser fiscalizado e **natureza** da auditoria. O âmbito engloba a **Amplitude** e **exaustão** dos processos de auditoria, incluindo uma limitação racional dos trabalhos a serem executados (**grau de abrangência**).A área de verificação é o conjunto formado pelo **campo** e pelo **âmbito** de auditoria. Delimita de **modo preciso** os temas da auditoria, em função da entidade a ser fiscalizada e da natureza da auditoria.

Questão 3)
Explique e exemplifique controle preventivo, controle detectivo e controle corretivo.(9 pontos)
Controles preventivos: são usados para prevenir erros, omissões ou atos fraudulentos. Exemplo: senhas de acesso a um determinado sistema. **Controles detectivos**: são usados para detectar erros , omissões ou atos fraudulentos, ou ainda relatar a sua ocorrência. Exemplo: softwares de controle de acesso e relatórios de tentativas de acesso não autorizado. **Controles corretivos**: são usados para reduzir impactos ou corrigir erros detectados. Exemplo: plano de contingência.

Questão 4)
Quais as evidências que podem ser encontradas durante uma auditoria ? E em qual fase elas são levantadas ?(8 pontos)
Evidência física: observações de atividades desenvolvidas pelos funcionários, gerentes, sistemas, equipamentos e etc;**Evidência documentária**: resultados de extração de dados, registros de transações e etc;**Evidência fornecida pelo auditado**: transcrições de entrevistas, cópias de documentos cedidos pelo auditado, fluxogramas, e-mails trocados com a gerência, relatórios e etc.**Evidência analítica**: comparações, cálculos e interpretações de documentos de entidades similares ou da mesma entidade em períodos de tempos diferentes. Estas evidências são levantadas na fase de execução.