ESAF
Escola de Administração Fazendária

Superintendência de Seguros Privados
SUSEP

Concurso Público 2006

Cargo: Analista Técnico

Prova 2

Área: Tecnologia da Informação

Nome: _____ N. de Inscrição _____

Instruções

1 - Escreva seu nome e número de inscrição, de forma legível, nos locais indicados.

2 - O CARTÃO DE RESPOSTAS tem, obrigatoriamente, de ser assinado. Esse CARTÃO DE RESPOSTAS não poderá ser substituído, portanto, não o rasure nem o amasse.

3 - Transcreva a frase abaixo para o local indicado no seu CARTÃO DE RESPOSTAS em letra *cursiva*, para posterior exame grafológico:

"Sonhar é preciso, agir na direção da realização de um sonho é fundamental".

4 - DURAÇÃO DA PROVA: **5 horas**, incluído o tempo para o preenchimento do CARTÃO DE RESPOSTAS.

5 - Na prova há **75 questões** de múltipla escolha, com cinco opções: a, b, c, d e e.

6 - No CARTÃO DE RESPOSTAS, as questões estão representadas por seus respectivos números. Preencha, FORTEMENTE, com caneta esferográfica (tinta azul ou preta), toda a área correspondente à opção de sua escolha, sem ultrapassar seus limites.

7 - Será anulada a questão cuja resposta contiver emenda ou rasura, ou para a qual for assinalada mais de uma opção. Evite deixar questão sem resposta.

8 - Ao receber a ordem do Fiscal de Sala, confira este CADERNO com muita atenção, pois nenhuma reclamação sobre o total de questões e/ou falhas na impressão será aceita depois de iniciada a prova.

9 - Durante a prova, não será admitida qualquer espécie de consulta ou comunicação entre os candidatos, tampouco será permitido o uso de qualquer tipo de equipamento (calculadora, tel. celular etc.).

10- Por motivo de segurança, somente durante os trinta minutos que antecedem o término da prova, poderão ser copiados os seus assinalamentos feitos no CARTÃO DE RESPOSTAS, conforme subitem 6.5 do edital regulador do concurso.

11- Entregue este CADERNO DE PROVA, juntamente com o CARTÃO DE RESPOSTAS, ao Fiscal de Sala, quando de sua saída, que não poderá ocorrer antes de decorrida uma hora do início da prova. A não-observância dessa exigência acarretará a sua exclusão do concurso.

Boa prova!

Escola de Administração Fazendária
Rodovia BR 251 Km 04 - Brasília-DF
www.esaf.fazenda.gov.br

TECNOLOGIA DA INFORMAÇÃO

01- A metodologia publicada pelo COSO define o Controle Interno como um processo que se torna efetivo através das pessoas, as quais devem

a) garantir a mitigação e contingenciamento dos riscos organizacionais.
b) garantir uma avaliação ao longo de todo o tempo, evitando que se realize uma avaliação em um ponto específico.
c) assegurar com razoável grau de segurança os seguintes objetivos: economia e eficiência das operações, veracidade das demonstrações financeiras e conformidade com as normas e legislação locais.
d) assegurar a integridade do ambiente operacional na gestão e disposição de tolerar riscos.
e) garantir uma avaliação ao longo de todo o tempo para a formação de um Ambiente de Controle de Riscos.

02- Segundo os componentes do ERM (*Enterprise Risk Management*) do COSO, a avaliação de riscos e a busca dos controles apropriados devem ser precedidos

a) de capturas e identificação de conteúdo apropriado para permitir um fluxo adequado de informações dos níveis estratégicos aos operacionais.
b) da identificação e comunicação, ao supervisor responsável, de não conformidades (deficiências do sistema de controles).
c) da Monitoração.
d) da formação de um Ambiente de Controle.
e) por atividades contínuas de gestão, por auditorias internas ou externas (periódicas ou especiais), ou por ambas.

03- Analise as seguintes afirmações relacionadas aos Processos de Controle Internos, segundo o COSO.

I. A Análise de Riscos visa identificar vulnerabilidades, ameaças e suas probabilidades, estimar o risco e estabelecer controles, de forma que estes minimizem os riscos identificados.
II. Uma vez implementados, os controles irão reduzir ou transferir riscos, sendo necessário avaliar sua eficácia em relação aos seus objetivos. A avaliação é de responsabilidade das Auditorias de Controles, processos investigativos que visam gerar indicadores de conformidade com as políticas internas e normativas externas.
III. Não existe ponto de equilíbrio entre riscos e controles. Os riscos devem ser tratados e eliminados, independentemente dos custos necessários para se realizar os controles adequados, evidenciando o objetivo do alcance do risco “zero”.
IV. As Análises de Riscos são instrumentos de monitoração do desempenho do Sistema de Controles Internos.

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

04- Analise as seguintes afirmações relacionadas a Gerenciamento de Riscos.

I. Um Risco Residual está diretamente relacionado ao risco gerado pela decisão de não se envolver com uma situação de riscos.
II. O compartilhamento, com um terceiro, do prejuízo da perda em relação a um determinado risco é um exemplo de Transferência do Risco.
III. A Otimização do Risco é o processo de se retirar benefício financeiro da ocorrência de um risco.
IV. O Tratamento do Risco é o processo de seleção e implementação de medidas para modificar o risco.

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

05- Analise as seguintes afirmações relacionadas à Análise de Riscos.

I. Ameaça é a expectativa de acontecimento acidental ou proposital, causado por um agente que pode afetar o ambiente analisado.
II. Vulnerabilidade é um evento decorrente da exploração de um ataque ou alvo por uma ameaça.
III. Impacto é o efeito ou conseqüência de um ataque ou incidente para a organização.
IV. Probabilidade Incidental é a fragilidade que poderia ser explorada por uma ameaça para concretizar um ataque.

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

06- Considerando a metodologia COSO, analise as seguintes afirmações relacionadas aos componentes do *ERM* (*Enterprise Risk Management*).

I. No Tratamento dos Riscos a Administração seleciona a opção adequada - evitar, aceitar, reduzir ou compartilhar riscos - desenvolvendo uma série de ações (controles) para alinhar os riscos com a tolerância e o apetite de risco.

II. Nas Atividades de Controle as políticas e procedimentos são definidos e implementados para ajudar a garantir que o tratamento de risco foi corretamente realizado, de forma que os objetivos estratégicos possam ser alcançados.

III. Na Definição de Objetivos devem ser identificados todos os tipos de riscos internos e externos que podem afetar o alcance dos objetivos da instituição, devendo ser distinguidos os riscos das oportunidades.

IV. Na Identificação de Eventos os riscos internos e externos à instituição são analisados considerando a probabilidade e a severidade das ameaças como base para determinar os riscos relevantes e como estes devem ser gerenciados.

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

07- Segundo o COSO, na Gestão de Riscos, deve-se buscar uma estrutura ou *framework* com uma comunicação adequada, objetivando um entendimento entre as camadas envolvidas. Desta forma, todas essas funções irão desempenhar o seu papel efetivo nesse processo. Assim, a área de Administração irá exercer a responsabilidade de

a) assegurar a adequação, o fortalecimento e o funcionamento do Sistema de Controles Internos, procurando contingenciar os Riscos de acordo com a complexidade de seus negócios.
b) buscar a adequação, o fortalecimento e o funcionamento do Sistema de Controles Internos, procurando mitigar os Riscos de acordo com a complexidade de seus negócios.
c) buscar um Sistema de Controles Internos apropriado ao risco de seus negócios, a fim de proporcionar segurança operacional e maior confiabilidade aos seus investidores e clientes.
d) estabelecer e disseminar a cultura de controles para garantir o cumprimento de leis e regulamentos existentes.
e) estabelecer os parâmetros e controles que a área necessita para verificar a conformidade, o uso prático e a adequação dos controles para as respectivas atividades operacionais.

08- Analise as seguintes afirmações relacionadas à Análise de Riscos.

I. Avaliação do risco é o processo relacionado a um risco para minimizar as conseqüências positivas e maximizar as conseqüências negativas e suas respectivas probabilidades.

II. Identificação do risco é a maneira pela qual um *stakeholder* decide se envolver ou não com a definição da probabilidade e impacto gerado pelo risco.

III. Estimativa de risco é o processo usado para atribuir valores à probabilidade e às conseqüências de um risco. A estimativa do risco pode considerar custo, benefício, preocupações de *stakeholders* e outras variáveis apropriadas para a avaliação do risco.

IV. Controle do risco envolve ações para a implementação das decisões de gestão do risco. O controle do risco pode envolver monitoração, reavaliação e conformidade com decisões.

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

09- Quanto à classificação para as medidas de proteção, é correto afirmar que Medidas Corretivas

a) reduzem o impacto de um ataque e devem ser tomadas durante ou após a ocorrência do evento.
b) detectam os ataques ou incidentes e devem disparar e controlar mitigações para evitar que o evento se repita.
c) detectam os ataques ou incidentes e devem disparar e controlar mitigações para reduzir a probabilidade de uma ameaça se concretizar.
d) são controles que reduzem a probabilidade de uma ameaça se concretizar.
e) são controles que controlam o grau de vulnerabilidade do ambiente buscando reduzir a probabilidade de um ataque se concretizar.

10- A categoria de riscos a que uma atividade está exposta depende da natureza dessa atividade. Entre os riscos aos quais as organizações empresariais podem estar sujeitas, as fraudes, erros de sistemas de informações, extrapolação de autoridade dos empregados, desempenho insatisfatório e incêndios devem ser caracterizados como

a) Risco Legal.
b) Risco de Variabilidade.
c) Risco Operacional.
d) Risco de Correlação Imperfeita.
e) Risco de Relacionamento Econômico e Social.

11- Para estar em um determinado nível de maturidade

a) a empresa deverá produzir software de excelente qualidade e atender as ACP´s deste nível, mesmo que não atenda aos níveis inferiores.
b) a empresa não deve adotar ACP´s de níveis mais adiantados.
c) a empresa deve satisfazer pelo menos a uma ACP de cada nível.
d) o processo de software deverá satisfazer a todas as Áreas-Chave do Processo(ACP) deste nível e dos níveis inferiores.
e) o processo de software deverá alcançar todas as atividades e infra-estruturas das ACP´s.

12- O CMM – *Capability Maturity Model* é

a) um modelo de processo de software para garantir a qualidade do desenvolvimento.
b) uma estrutura (*framework*) que descreve os principais elementos de um processo de software efetivo.
c) um processo de software contendo as etapas Inicial, Repetitivo, Definido, Gerenciado e Otimizado.
d) um método que estabelece ações específicas a serem seguidas para a maturidade da capacitação das organizações.
e) uma técnica para definir, implementar, medir, controlar e melhorar os processos de software.

13- No esquema da estrutura do CMM, compromisso, habilitação, atividade, medição e verificação são considerados

a) seções.
b) áreas-chave do processo.
c) práticas-chaves.
d) metas.
e) características comuns.

14- Na estrutura do Modelo CMM

a) cada área-chave agrupa as correspondentes práticas-chave de acordo com as Características Comuns.
b) cada um dos cinco níveis é composto por várias Áreas-Chave de Processo (ACP).
c) existem 5 níveis de maturidade que tratam de planos de projeto, documentos de especificação, documentos de *design*, código e casos de teste respectivamente.
d) as Características Comuns conduzem ao alcance de metas de melhoria de processo para um determinado nível.
e) as práticas-chave institucionalizam ou implementam as Características Comuns do modelo.

15- As Áreas-Chave de Processo: definição do processo da organização, revisão por parceiros e programa de treinamento, são encontradas, entre outras, no nível

a) 1 - Inicial.
b) 2 - Repetitivo.
c) 3 - Definido.
d) 4 - Gerenciado.
e) 5 - Otimizado.

16- Entre os 34 processos que compõem os quatro domínios do COBIT, aquele responsável por prover auditorias independentes está presente

a) apenas nos domínios de “Planejamento e Organização” e de “Aquisição e Implementação”.
b) apenas nos domínios de “Planejamento e Organização” e de “Monitoramento”.
c) apenas no domínio de “Entrega e Suporte”.
d) apenas no domínio de “Monitoramento”.
e) em todos os domínios.

17- Analise as seguintes afirmações relacionadas a conceitos básicos, domínios e terminologias do COBIT (*Control Objectives for Information and related Technology*).

I. O domínio “Planejamento e Organização” cobre estratégia e tática, e diz respeito à identificação da maneira como TI e Segurança podem melhor contribuir para o atendimento dos objetivos do negócio.
II. O domínio “Aquisição e Implementação” cobre a identificação, o desenvolvimento ou aquisição, a implementação e a integração dos processos do negócio.
III. O domínio “Entrega e Suporte” cobre a avaliação ao longo do tempo com relação à sua qualidade e conformidade.
IV. O domínio “Monitoramento” abrange as operações tradicionais sobre aspectos de segurança, continuidade e treinamento.

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

18- Os domínios do COBIT cobrem um conjunto de processos de forma a completar a gestão de TI. Entre aqueles que cobrem o domínio "Planejamento e Organização (PO)" estão os processos que

a) identificam as soluções de automação, gerenciam os recursos humanos e identificam e alocam custos.
b) gerenciam os investimentos de TI, a comunicação das direções de TI e os recursos humanos.
c) avaliam os riscos, asseguram a continuidade dos serviços e gerenciam as mudanças.
d) avaliam os riscos, garantem a segurança dos serviços e gerenciam a configuração.
e) identificam as soluções de automação, garantem a segurança dos serviços e gerenciam a configuração.

19- O relacionamento entre o COBIT e a ISO/IEC 17799 permite que se faça um mapeamento entre as estratégias de negócios do COBIT e a aplicação das práticas da ISO/IEC 17799. Com relação a esse relacionamento, é correto afirmar que o processo

a) "DS1 define e mantém os acordos de níveis de serviço" do COBIT está relacionado à prática "Segurança de arquivos do sistema" da ISO/IEC 17799:2000.
b) "DS5 assegura segurança dos dados" do COBIT está relacionado à prática "Gerenciamento da Rede" da ISO/IEC 17799:2000.
c) "DS11 gerencia os dados" do COBIT está relacionado à prática "Requisitos do negócio para controle de acesso" da ISO/IEC 17799:2000.
d) "AI5 instala e Certifica Software" do COBIT está relacionado à prática "Treinamento dos usuários" da ISO/IEC 17799:2000.
e) "AI3 adquire e mantém a infra-estrutura Tecnológica" do COBIT está relacionado à prática "Responsabilidades do usuário" da ISO/IEC 17799:2000.

20- A prática "Conformidade com requisitos legais" da ISO/IEC 17799 está relacionada, no COBIT, com os processos

a) "Gerencia a comunicação das direções de TI"; "Assegura o alinhamento de TI com os requisitos externos"; "Gerencia Dados"; "Monitora processos" e "Provê Auditorias independentes".
b) "Identifica as soluções de automação" e "Provê Auditorias independentes".
c) "Identifica as soluções de automação"; "Monitora processos" e "Gerencia Mudanças".
d) "Adquire e mantém os softwares"; "Assegura segurança dos serviços"; "Monitora processos" e "Gerencia Mudanças".
e) "Adquire e mantém os softwares"; "Assegura segurança dos serviços" e "Provê Auditorias independentes".

21- Analise as seguintes afirmações relacionadas às auditorias da metodologia COBIT para a avaliação dos níveis de maturidade.

I. No Nível 1 - Inicial: O processo é realizado, documentado e comunicado na organização.
II. No Nível 2 - Repetível: O processo é realizado sem organização, de modo não planejado.
III. No Nível 4 - Gerenciado: Existem métricas de desempenho das atividades, o processo é monitorado e constantemente avaliado.
IV. No Nível 5 - Otimizado: As melhores práticas de mercado e automação são utilizadas para a melhoria contínua dos processos.

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

22- Quanto aos Indicadores de Metas KGIs (*Key Goal Indicators*) utilizados no COBIT é correto afirmar que eles

a) determinam "como" a monitoração de performance dos fatores medidos viabilizam os processos de TI.
b) determinam o quanto um processo de TI está sendo monitorado.
c) determinam quando um processo de TI está atingindo os requisitos do negócio.
d) fornecem um guia para implementar controles sobre TI e seus processos.
e) representam uma medida do "que" tem de ser realizado. Indicam se o processo atingiu seus objetivos, definidos como uma meta.

23- As auditorias internas, consideradas um processo sistemático, documentado e independente,

a) são denominadas auditorias de primeira parte, podendo ser realizadas em nome da organização.
b) são aquelas realizadas diretamente pelo comprador.
c) são aquelas realizadas por entidades certificadoras.
d) dizem respeito à avaliação/certificação de fornecedores.
e) são também denominadas auditorias de segunda parte, conduzidas pela própria organização.

24- As auditorias internas são realizadas com o objetivo de

a) prover certificados e registros de acordo com uma norma de referência.
b) fornecer evidência da qualificação dos fornecedores da organização.
c) inspecionar os produtos recebidos e fornecidos.
d) validar a capacidade profissional dos auditores do sistema da qualidade.
e) servir de base para análise crítica pela direção.

25- Um plano de auditoria deve envolver

a) procedimentos administrativos e organizacionais.
b) itens que estão sendo produzidos.
c) estruturas organizacionais.
d) documentação, relatórios e registros.
e) indicação do pessoal qualificado para conduzir as auditorias.

26- Entrevistas, observações de atividades e análise crítica de documentos são

a) evidências objetivas da execução dos processos.
b) métodos para coletar informações durante as auditorias internas.
c) sistemáticas adotadas para a programação de auditorias.
d) critérios de auditoria para gerar constatações.
e) formas de analisar criticamente os resultados da auditoria.

27- Uma equipe de auditoria interna

a) é composta sem a designação de um auditor líder.
b) não permite a presença de auditores de outras organizações.
c) não deve ser treinada por instrutores da própria organização.
d) poderá incluir auditores em treinamento, isto é, que estão sendo treinados.
e) deve incluir pessoas do setor/processo auditado.

28- A implementação de um programa de auditoria deve

a) planejar e programar auditorias internas.
b) assegurar a análise crítica e a aprovação de relatórios de auditoria e garantir sua distribuição ao cliente da auditoria e a outras partes especificadas.
c) gerar registros do programa de auditoria.
d) monitorar o desempenho e a eficácia do programa de auditoria.
e) manter registros da formação dos auditores.

29- O propósito de uma reunião de abertura de auditoria é

a) elaborar listas de verificação de auditoria.
b) fornecer oportunidade para o auditado fazer perguntas.
c) estabelecer planos de amostragem de auditoria.
d) preparar documentos de trabalho para referência e para registros.
e) designar responsabilidade a cada membro da equipe para auditar processos específicos.

30-O método de relatar, incluindo classificação de não-conformidades, deve ser comunicado ao auditado

a) durante a análise crítica dos documentos.
b) no conteúdo do plano de auditoria.
c) na preparação dos documentos de trabalho.
d) na reunião de abertura.
e) na apresentação do relatório de auditoria.

31- Recomendações para melhorias, caso citadas no relatório de auditoria,

a) devem ser implementadas pela área auditada.
b) são evidências de que os processos não estão sendo executados em conformidade com os documentos analisados.
c) constituem não-conformidades, consideradas não críticas ou leves.
d) não são ações obrigatórias.
e) são resultados de opiniões divergentes relativas às conclusões e/ou constatações da auditoria.

32- O relatório de auditoria

a) é de propriedade do cliente da auditoria.
b) é o documento que delimita a conclusão da auditoria.
c) estabelece as ações a serem tomadas para eliminar as não-conformidades identificadas.
d) deverá conter ações corretivas, preventivas e de melhoria a serem tomadas pela área auditada.
e) é uma forma especificada de gerenciar um programa de auditoria interna.

33- Faz parte das habilidades de um auditor

a) a capacidade de convencer o auditado em relação a um processo que aparentemente esteja não-conforme.
b) realizar a auditoria, mesmo divergindo da programação acordada.
c) manter-se dentro dos questionamentos estabelecidos nos planos de auditoria.
d) priorizar e enfocar detalhes dos processos, mesmo que aparentemente triviais.
e) entender a conveniência e as conseqüências de usar técnicas de amostragem para auditar.

34- Em um programa de auditoria interna

a) deve-se incluir apenas um tipo de auditoria.
b) é permitido conter uma variedade de objetivos.
c) não se deve incluir auditorias combinadas ou auditorias em conjunto.
d) não se deve incluir necessidade de avaliação de fornecedor.
e) deve-se excluir requisitos para certificação em uma norma de sistema de gestão.

35- Um programa de auditoria interna tem como um de seus objetivos

a) estabelecer mudanças significativas para uma organização ou suas operações.
b) especificar requisitos normativos, estatutários, regulamentares e contratuais.
c) levantar necessidades para credenciamento ou registro/certificação.
d) registrar evidências objetivas da execução dos processos organizacionais.
e) obter e manter confiança na capacidade de um fornecedor.

36- Durante a execução da auditoria interna, o auditor

a) deve se restringir ao conteúdo das listas de verificação de auditoria.
b) fica impedido de alterar os planos de amostragem definidos.
c) deve avaliar resumos de dados, análises e indicadores de desempenho como fontes de informação, mesmo que não estejam contidos nas listas de verificação de auditoria.
d) deve coletar registros e anexá-los ao relatório de auditoria como evidências das constatações.
e) não deve solicitar e analisar registros com informações confidenciais.

37- Analise as seguintes afirmações relacionadas a conceitos básicos sobre Banco de Dados.

I. O comando SQL responsável por fechar uma transação confirmando as operações feitas é o INSERT.
II. O comando SQL responsável por fechar uma transação e desfazer todas as operações é o COMMIT.
III. Quando uma transação ainda está aberta para um usuário, enquanto não é executado um comando COMMIT, o próprio usuário pode ver as suas alterações, mas outros usuários não podem vê-las.
IV. Uma transação assegura um espaço de trabalho que contém várias alterações, inclusões e exclusões de dados em uma ou mais tabelas, com a possibilidade de confirmação ou cancelamento das operações sem comprometimento dos dados.

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

38- Em um Banco de Dados Relacional

a) uma relação está na 1FN (primeira forma normal) se nenhum domínio contiver valores atômicos.
b) uma Chave Primária corresponde ao identificador único de uma determinada relação. Em uma relação pode haver mais que uma coluna candidata a chave primária.
c) as colunas que irão compor as Chaves Primárias devem ser inicializadas com valores nulos.
d) em uma tabela existirão tantas Chaves Primárias quantas forem as colunas nela existentes.
e) uma Chave Externa é formada por uma coluna de uma tabela que se referencia a uma Coluna qualquer de outra tabela. Essas colunas, na tabela destino, não aceitam valores nulos. Uma tabela destino pode ter apenas uma Chave Externa.

39-Analise as seguintes afirmações relacionadas a segurança, concorrência, integridade e recuperação de Banco de Dados.

I. Em um mesmo Banco de Dados é possível ter uma *stored procedure* para atualizar dados, outra para retornar valores de uma consulta e uma terceira para excluir determinado conjunto de dados de uma tabela.
II. As *stored procedures* podem ser usadas em mecanismos de segurança. Um usuário poderá possuir direitos de execução de uma *stored procedure* mesmo que não possua permissões sobre as tabelas que ela referencia.
III. A cópia do banco de dados ou *backup* diferencial é caracterizada pela existência de dois bancos de dados com as mesmas informações trabalhando juntos, mas em máquinas diferentes. Dessa forma, quando uma máquina fica impossibilitada de trabalhar, a outra assume automaticamente seu lugar.
IV. A JUNÇÃO entre tabelas somente será possível se existir um relacionamento **N:N** entre as tabelas envolvidas.

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

40- Analise as seguintes afirmações relacionadas a gatilhos e procedimentos em Banco de Dados.

I. Fazer auditoria das informações em uma tabela registrando as alterações ocorridas e o responsável por essas alterações é um exemplo da utilidade e uso de um *trigger*.

II. Quando uma *stored procedure* é chamada, o SGBD executa automaticamente um *trigger* padrão que irá incrementar um contador em todas as outras tabelas que possuírem um relacionamento **N:N** com a tabela que recebeu ação da referida *stored procedure*.

III. Uma *View* pode ser usada para restringir o acesso aos dados de uma tabela original e pode conter apenas algumas colunas da referida tabela.

IV. Quando o comando DROP VIEW é executado, as estruturas das tabelas referenciadas pela *view* e os dados são excluídos.

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

41- Analise as seguintes afirmações relacionadas a banco de dados distribuídos, relacionais e orientados a objetos.

I. Em um Banco de Dados Relacional um objeto está encapsulado quando seu estado é visível ao usuário e ele pode ser consultado e modificado exclusivamente por meio das operações a ele associadas.

II. A linguagem de manipulação de dados (DML) permite a uma aplicação acessar ou manipular as informações contidas num banco de dados. A manipulação de dados engloba incluir, recuperar, excluir e modificar a informação armazenada.

III. Os dados manipulados por um banco de dados orientado a objeto são sempre transientes e são armazenados fora do contexto de um programa, e assim podem ser usados em várias instâncias de programas.

IV. Todo dado de um Banco de Dados Relacional deve ter a garantia de ser logicamente acessível, recorrendo-se a uma combinação de Nome da Tabela, um Valor de Chave e o Nome da Coluna.

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

42- Entre os benefícios advindos da adoção de boas práticas de Governança Corporativa é correto afirmar que

a) ela cria, por si só, valor para a empresa.
b) proporciona uma administração ainda melhor, em benefício dos acionistas majoritários como prioridade.
c) proporciona aos proprietários (acionistas ou cotistas) a gestão estratégica de sua empresa, sem a necessidade da efetiva monitoração da direção executiva.
d) disponibiliza ferramentas que asseguram ao Conselho de Administração o controle da propriedade sobre a gestão, descartando a necessidade de Auditoria Independente e de Conselho Fiscal.
e) os investidores tendem a pagar mais por ações de empresas que adotam melhores práticas de administração e transparência.

43- Segundo o IBGC (Instituto Brasileiro de Governança Corporativa), Governança Corporativa é o sistema

a) que define o papel e a operação dos conselhos das organizações da sociedade civil, no contexto empresarial.
b) que define processos para garantir a regulamentação do acesso à informação digital nas corporações, criando assim uma gestão segura, confiável e eficaz dos processos automatizados que garantem o funcionamento e a comunicação das redes e dos dispositivos conectados à rede corporativa.
c) que define como criar, melhorar ou adaptar mecanismos globais que permitam tratar dos temas centrais derivados da presença cada vez mais abrangente da Internet na economia, política, sociedade e cultura de todas as corporações.
d) pelo qual as sociedades são dirigidas e monitoradas, envolvendo os relacionamentos entre Acionistas/ Cotistas, Conselho de Administração, Diretoria, Auditoria Independente e Conselho Fiscal.
e) que define o conjunto de diretrizes e procedimentos que sistematiza a gestão de conteúdo de uma intranet/ portal corporativo.

44- Entre as finalidades das boas práticas de governança corporativa <u>não</u> se inclui

a) aumentar o valor da sociedade.
b) fortalecer o poder de decisão dos acionistas sobre os rumos do negócio.
c) facilitar o acesso ao capital.
d) contribuir para a perenidade da organização.
e) a busca da transparência na administração.

45- Acerca de planejamento de capacidade é incorreto afirmar que

a) planejamento de capacidade é importante para estender negócios de uma organização, considerando adições ou modificações nas linhas de produtos e introduzindo novas técnicas, equipamentos e materiais.

b) na área de negócios, capacidade é a taxa máxima de saída para um processo, ou seja, pode ser expressa em termos de (número de máquinas) x (utilização) x (eficiência).

c) adicionar capacidade antecipadamente a um aumento da demanda é uma estratégia agressiva e como possível desvantagem pode-se destacar possibilidades de custos excessivos e disperdícios.

d) adicionar capacidade apenas após uma organização estar trabalhando com sua capacidade máxima ou além desta, é uma estratégia conservadora que diminui os riscos, mas pode ocasionar possíveis perdas de clientes.

e) o planejamento de requisitos de capacidade refere-se ao processo de determinar a quantidade de trabalho e recursos necessários à execução das tarefas.

46- A respeito de administração, monitoramento, virtualização e armazenamento em ambientes distribuídos, é incorreto afirmar que

a) uma recomendação para administradores de rede é automatizar o maior número possível de tarefas, como por exemplo, verificação e relatório do espaço livre em disco, coleta de dados sobre o desempenho do sistema e *backups*.

b) o monitoramento de desempenho é normalmente feito em etapas, a saber: identificar a natureza e escopo da redução de recursos que causam o problema de desempenho, analisar os dados obtidos no monitoramento e aplicar uma seqüência de ações para resolver o problema e, por fim, monitorar para garantir que o problema de desempenho foi resolvido.

c) o monitoramento da capacidade do sistema com o propósito de planejamento tem as mesmas características do monitoramento de desempenho, ou seja, deve ser feito quase continuamente e não é tão detalhado, uma vez que o planejamento de capacidade requer um ponto de vista macro.

d) RAID (*Redundant Array of Independent Disks*) é uma tecnologia de armazenamento que permite *drives* de múltiplos discos atuarem como se fossem um único *drive* de disco. Neste contexto, RAID nível 5 consiste em, no mínimo, 3 *drives* de disco de tamanho idêntico e, cada um, dividido em pedaços; todavia, nem todo pedaço é dedicado ao armazenamento como no RAID nível 0.

e) a virtualização de sistemas permite que haja vários sistemas operacionais trabalhando em paralelo, cada um com vários programas em execução. Sendo assim, cada sistema operacional executa em um processador virtual ou máquina virtual.

47- Acerca dos conceitos fundamentais de lógica de programação e algoritmos, é incorreto afirmar que

a) os denonimados fluxos seqüenciais em algoritmos determinam explicitamente os passos a serem seguidos, com a respectiva execução seqüencial.

b) compreender o problema, selecionar um método de solução, descrever a solução passo a passo, validar o algoritmo, programá-lo e testá-lo, nesta seqüência, é uma proposta viável para analisar um problema.

c) o controle de fluxo de programas corresponde à lógica do algoritmo que, por sua vez, canaliza a ação entre os procedimentos, na ordem necessária à realização da execução.

d) rotinas de biblioteca, em linguagens de programação estruturada, correspondem a programas independentes (subprogramas externos), compilados e testados separadamente.

e) por meio do desenvolvimento de algoritmos que tornem mais eficiente o uso de repetições (ou de fluxo repetitivo), consegue-se desenvolver programas que realizem atividades em escalas mais amplas.

48- A respeito dos fundamentos da Engenharia de Software, é correto afirmar que

a) os requisitos normativos são aqueles descritos em um documento que engloba a especificação dos requisitos de um produto.

b) o modelo de ciclo de vida de entrega evolutiva aplicado aos processos de software compreende exclusivamente os seguintes sub-processos: requisitos, análise, desenho, implementação e testes.

c) testes são indicadores da qualidade do produto e, em particular, os testes de integração têm por objetivo verificar as interfaces entre os módulos constituintes de uma arquitetura de produto.

d) gestão de configurações e a gestão da manutenção são atividades que compreendem o escopo da bateria de testes aplicados aos produtos de software.

e) o valor de um produto é proveniente de suas características. Neste sentido, características não-funcionais representam os comportamentos que um programa ou sistema deve apresentar diante de certas ações de seus usuários.

49- Praticamente todos os projetos de computadores atuais são fundamentados nos conceitos desenvolvidos por John von Neumman. A respeito de arquiteturas de computadores e seus fundamentos, portanto, é incorreto afirmar que

a) a principal vantagem do modo de endereçamento indireto via registrador é o fato dele poder referenciar a memória sem ter que expressar, na instrução, um endereço de memória completo.

b) no esquema de E/S (Entrada e Saída) programada há uma única instrução de entrada e uma única instrução de saída e, em geral, um único caracter é transferido entre um registrador fixo do processador e o dispositivo de E/S selecionado na instrução.

c) uma interrupção de relógio é gerada por um controlador de E/S (Entrada/Saída), sinalizando a conclusão de uma operação ou ocorrência de uma situação de erro.

d) quando um dispositivo externo estiver pronto para ser utilizado, um sinal de requisição de interrupção é enviado para o processador através do módulo de E/S (Entrada/Saída) desse dispositivo. O processador, então, suspende a execução do programa atual.

e) em termos de linguagem de montagem, a tradução de um programa não é efetuada diretamente. O programa é convertido para um programa-objeto que será executado, após a tradução.

50- A respeito do gerenciamento de memória realizado pelo sistema operacional, é correto afirmar que

a) páginas são espaços de endereçamento independentes e compostos, cada um, de uma seqüência linear de endereços (de 0 a até um valor máximo), podendo ser variável neste intervalo, durante a execução de um programa.

b) o algoritmo LRU (*Least Recently Used*) remove a página que está há mais tempo na memória principal, independente da última referência feita a essa página, associando um contador a cada moldura de página.

c) a segmentação implementada por *swapping* baseia-se na divisão de cada segmento em um conjunto de páginas e passa a trabalhar como no esquema da paginação sob demanda e, algumas páginas podem estar na memória, enquanto as demais, no disco.

d) todo processador que tem o suporte ao conceito de memória virtual tem o dispositivo MMU (*Memory Management Unit*) que, por sua vez, pode estar em um *chip* separado (porém, ligado ao *chip* do processador) ou integrado diretamente ao processador.

e) se o tamanho de uma página for *n bytes*, a quantidade média de espaço de endereçamento desperdiçado na última página pela fragmentação interna será de *n*/8 *bytes*, em média.

51- Em relação à estrutura, fundamentos e armazenamento em massa em ambientes operacionais é correto afirmar que

a) as VMs (*Virtual Machines*) estruturam o sistema operacional, removendo todos os componentes não-essenciais do *kernel* e implementando-os como programas em nível de sistema e usuário.

b) as informações em arquivos podem ser acessadas de várias maneiras. O acesso seqüencial baseia-se num modelo de disco de arquivos, já que os discos permitem acesso aleatório a qualquer bloco do arquivo. Neste caso, o arquivo é visto como uma seqüência numerada de blocos ou registros.

c) uma desvantagem do SAN (*Storage Area Network*) é que em sua implementação, as operações de E/S para armazenamento consomem largura de banda, aumentando assim, a latência da comunicação na rede.

d) um NAS (*Network-Attached Storage*) é uma solução flexível, pois vários *hosts* e *arrays* de armazenamento podem estar conectados ao mesmo NAS, e o armazenamento pode ser alocado aos *hosts*, de modo dinâmico.

e) no escalonamento de processos por prioridade em um sistema operacional, a CPU (*Central Processing Unit*) é alocada ao processo com maior prioridade – considerando que a cada processo está associada uma prioridade. Processos com mesma prioridade são escalonados na ordem FCFS (*First Come First Serve*).

52- Um sistema distribuído é uma coleção de processadores pouco acoplados, interconectados por uma rede de comunicação. A respeito de seus fundamentos, é correto afirmar que

a) na estratégia preemptiva de transferência de tarefas para escalonamento em ambientes distribuídos, têm-se a transferência de tarefas parcialmente executadas e, com isso, o estado da tarefa também deve ser transferido.

b) protocolos de bloqueio em duas fases podem ser usados em ambientes distribuídos. Nesse contexto, o esquema de protocolo parcial requer apenas duas transferências de mensagem para tratar de requisições de bloqueio e uma para tratar de desbloqueios.

c) em uma estratégia de prevenção de *deadlocks* para ambientes distribuídos, requer-se que a quantidade máxima de recursos requisitados por um processo seja conhecida antes de sua execução.

d) a técnica totalmente distribuída para implementar exclusão mútua em arquiteturas distribuídas faz circular um *token* entre os processos do sistema. A posse do *token* dá direto a seu possuidor, entrar na sessão crítica.

e) RMI (*Remote Method Invocation*) é uma das estratégias para a comunicação em sistemas cliente/servidor em 2 e 3 camadas. Baseia-se na troca de mensagens bem estruturadas e endereçadas a um *daemon* RMI associado a uma porta no sistema remoto, e os parâmetros são estruturas de dados comuns em RMI.

53- A organização de computadores compreende as unidades operacionais e as interconexões que implementam a especificação de sua arquitetura. Em relação a tal contexto, afirma-se que:

a) As portas lógicas são a base da construção de *chips* que, por sua vez, são circuitos com várias entradas e várias saídas, nos quais as saídas são determinadas exclusivamente pelo valor presente nas entradas.

b) Em termos de álgebra booleana, o Teorema de DeMorgan diz que A * (B + C) = (A * B) + (A * C), assim como A + (B *C) = (A + B) * (A + C), para os operandos A, B e C.

c) A regra para converter uma representação em complemento de 2 em outra com maior número de bits, consiste em mover o bit de sinal para a posição mais à esquerda e as demais posições com valor 1 para números positivos e valor 0 para números negativos.

d) A CPU *(Central Processing Unit)* se interconecta aos outros módulos de um computador através de barramentos. No barramento de controle, os sinais de controle são usados para transmitir comandos e informação de temporização entre os módulos do computador.

e) São características comuns a CISC (*Complex Instrutions Set Computer*): uma instrução por ciclo de máquina e operações de registrador para registrador, contribuindo para a simplificação de compiladores, uma vez que estes geram uma seqüência de instruções de máquina para cada comando.

54-Em relação aos ambientes operacionais de grande porte, família Microsoft Windows, Unix e Linux é correto afirmar que

a) sob o Linux, o gerenciador de memória virtual mantém 2 visões separadas do espaço de endereçamento de um processo. Nesse contexto, na visão de um conjunto de regiões separadas, o espaço de endereços consiste em regiões não-sobrepostas, no qual, cada região representa um subconjunto contínuo, alinhado por páginas.

b) em sistemas operacionais Unix e Linux, as APCs (*Asynchronous Procedure Call)* são usadas para iniciar a execução de uma nova *thread*, terminar processos e oferecer notificação de que uma operação de E/S (Entrada/Saída) assíncrona foi concluída.

c) o princípio de gerência de processos nos sistemas operacionais da família Microsoft Windows é separar 2 operações: criação de processos (função da chamada de sistema *fork*) e a execução de um novo programa (função da chamada de sistema *execve*).

d) sistemas de grande porte evoluíram dos sistemas em *batch* aos de tempo compartilhado, sendo que o primeiro apresenta a característica de multiprogramação, permitindo o uso eficiente de CPU, uma vez que efetua o escalonamento de atividades à CPU, de modo organizado.

e) o *kernel* do Linux não é implementado como um *kernel* monolítico tradicional por motivos de desempenho. Ao invés disto, seu projeto é modular, permitindo que a maioria dos *drivers* seja carregada/descarregada dinamicamente.

55-Analise as seguintes afirmações relacionadas à terminologia e conceitos básicos do ITIL (*Information Technology Infrastructure Library*).

I. Um incidente é um evento que faz parte da operação normal de um serviço e causa, ou pode causar uma interrupção ou redução na qualidade deste serviço.

II. O Gerenciamento de Configuração é o processo de identificar e definir os itens de configuração em um sistema, de gravar e reportar o *status* destes itens e de controlar as solicitações de mudanças, garantindo assim a sua integridade.

III. A implantação do ITIL aumenta a transparência perante usuários e clientes.

IV. É considerado ponto fraco do ITIL o aumento do tempo médio para a resolução de incidentes e a queda na velocidade de implementação de mudanças.

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

56-Em relação ao Gerenciamento reativo de problemas no Gerenciamento de problemas do ITIL é correto afirmar que fazem parte de suas tarefas:

a) Disponibilizar informações e treinamento antes do *delivery*; Instalar ou modificar o hardware; Armazenar a *release* de hardware no hardware de armazenamento definitivo; *Release*, distribuição e instalação de software; e Armazenar a *release* de software na biblioteca de software definitiva.

b) Estabelecer o fluxo de trabalho dos processos operacionais; especificar a tabela de tempo e processos para implementar as atividades de identificação da configuração, checagem, documentação do status das mudanças e auditoria; e analisar os requisitos de integração usando produtos de terceiros.

c) As medidas de preparação de relatórios de qualidade.

d) As medidas de prevenção de erros, que são análise de tendências, ações e medidas.

e) A identificação, documentação, classificação e análise de problemas; a identificação, documentação e avaliação de erros, planejamento e início do *troubleshooting* (*Request for Change*); e o Suporte para a administração de mais incidentes envolvidos.

57- Com relação ao ITIL é correto afirmar que

a) é formado por todos os processos utilizados no CMMI nível 5.
b) é formado por um conjunto de melhores práticas para operações e gerenciamento de serviços de TI.
c) rastreia problemas exclusivamente em áreas de serviço de *help desk* e suporte.
d) é voltado para processos de desenvolvimento de software.
e) aborda o desenvolvimento de sistemas de gerenciamento de qualidade.

58- Considere as tarefas relacionadas a seguir.

I. Realizar a análise inicial do incidente e iniciar o suporte de 1º nível.
II. Disponibilizar informações para melhoria da qualidade dos serviços.
III. Transferir para o suporte de 2º e 3º níveis caso o problema não tenha sido resolvido nos níveis anteriores e adicionar os recursos necessários se o perigo de falha comprometer os níveis de serviço.
IV. Realizar o filtro inicial das requisições dos usuários e iniciar o processamento baseado nos níveis de serviço.

Indique a opção que contenha apenas as tarefas relacionadas à Gerência de Incidentes no ITIL.

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

59- Analise os benefícios relacionados a seguir.

I. Melhor foco no usuário e pró-atividade na disponibilidade dos serviços.
II. Redução dos efeitos negativos para a companhia em virtude da análise de problemas.
III. Redução dos custos de suporte e dos custos ocultos de TI (duplicação de recursos).
IV. Melhoria da disponibilidade do negócio, relacionando informações concernentes à performance no contexto do acordo de níveis de serviço (SLA).

Indique a opção que contenha apenas os benefícios relacionados à Gerência de Incidentes no ITIL.

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

60- Para as organizações, é cada vez mais crucial manter as informações seguras, assim como confiáveis suas fontes. Sendo assim, é relevante estabelecer controles que garantam a qualidade no contexto de Segurança da Informação. Nesse contexto, a Norma NBR ISO/ABNT 17799 é aplicada. A respeito de tal norma, é <u>incorreto</u> afirmar que

a) ela compreende recomendações para a gestão da segurança da informação visando ser aplicada àqueles departamentos responsáveis pela introdução, implementação ou manutenção da segurança em suas organizações.
b) convém que a direção da organização estabeleça uma política clara e demonstre apoio e comprometimento com a segurança da informação, através da emissão e manutenção de uma política de segurança da informação para toda a organização.
c) ela abrange, ao todo, 9 (nove) domínios: política de segurança; segurança organizacional; controle dos ativos de informação; segurança de pessoas; segurança física; controle de acesso; desenvolvimento e manutenção de sistemas; gestão da continuidade do negócio; e conformidade.
d) ela aconselha efetuar referências à documentação que possam apoiar a política de segurança de uma organização. Um exemplo de documentação compreende políticas e procedimentos de segurança de sistemas de informação específicos que devem ser conhecidos pelos usuários.
e) para os controles criptográficos também é necessário estabelecer uma política para o uso, na qual se determina que seja feita uma avaliação de riscos do ambiente, visando determinar o nível de proteção a ser dado à informação. O resultado pode ser usado para determinar se um controle é adequado ou qual o tipo de controle pode ser aplicado.

61- O acesso aos sistemas de informação deve ser controlado com base nos requisitos de segurança e de negócio, levando-se em conta as políticas para disseminação e autorização da informação. Em relação a controle de acesso, é correto afirmar que

a) não há necessidade, para o controle de acesso, de se ter conhecimento a respeito dos princípios e níveis de segurança e classificação da informação na organização.
b) o gerenciamento de acessos físicos deve compreender o registro de usuários, gerenciamento de privilégios, gerenciamento das senhas de usuários e revisão dos direitos de acesso dos usuários – preocupações que não se aplicam aos acessos lógicos.
c) fazem parte do controle de acesso ao sistema operacional, preocupações tais como restrição de acesso a aplicações e isolamento de sistemas sensíveis.
d) na especificação das regras para controle de acesso, não se deve utilizar a premissa: "tudo deve ser permitido, a menos que expressamente proibido".
e) o controle, na auditoria, consiste em fiscalizar as atividades, com relação às normas pré-estabelecidas. Com isso, a identificação e autenticação de usuários formam um exemplo de controle de detecção.

62- Ameaças programadas são aquelas que compreendem a execução de códigos, gerados com o intuito de adulterar o comportamento considerado normal, dos softwares. Em relação a tais ameaças e suas conseqüências, é correto afirmar que

a) *bombs* (ou bombas lógicas) é uma ameaça programada, cujo intuito é sua replicação (exponencial) em sistemas computacionais, assumindo, eventualmente, a capacidade completa do processador, memória ou espaço em disco.
b) *worms* (ou vermes) são uma ameaça programada camuflada em programas, que são ativados sob determinada condição, executando funções que alteram o comportamento do software hospedeiro.
c) vírus é uma espécie de entrada para um programa que permite acesso não-autorizado, violando procedimentos de segurança do sistema computacional.
d) *trapdoors*, cavalos de tróia, bombas lógicas, *adwares* e spywares são exemplos de ameaças independentes, isto é, não precisam de um programa hospedeiro.
e) *trojans* (ou cavalos de tróia) normalmente são utilizados como veículos para vírus, vermes e bombas lógicas.

63- A segurança em redes de computadores possui algumas propriedades desejáveis, a saber: confidencialidade, autenticidade e integridade das mensagens em tráfego. É correto, portanto, afirmar acerca de tal contexto que

a) DoS/DDoS (*Denial of Service/Distributed Denial of Service*), mesmo sob a forma de *flooding* simples são considerados ataques passivos.
b) a detecção de intrusão baseada em regras engloba a coleta de dados e sua análise, tendo como base o comportamento legítimo de usuários, num dado intervalo de tempo.
c) *firewalls* são soluções que auxiliam a detecção de intrusos, nos quais a DMZ (*De-Militarized Zone*) é construída sobre *hosts dual-homed*, que agem como roteadores entre as redes interna-externa.
d) uma contramedida aceitável para o IP (*Internet Protocol*) *spoofing* é descartar pacotes com um endereço IP interno à rede, mas que chega a partir de uma interface externa.
e) o *firewall* de nível de aplicação aplica um conjunto de regras aos pacotes, liberando-os na rede ou bloqueando-os, com base nos campos do cabeçalho IP (*Internet Protocol*) e de transporte.

64- Sobre política de segurança é <u>incorreto</u> afirmar que

a) é comum encontrar nesta política orientações sobre a análise e a gerência de riscos, princípios de conformidades dos sistemas com a política de segurança da informação e padrões mínimos de qualidade a serem incorporados aos sistemas de informação.
b) uma das primeiras atividades para a definição da política de segurança é classificar as informações em quatro níveis: públicas, secretas, internas e confidenciais.
c) a análise de riscos engloba tanto a análise de ameaças e vulnerabilidades quanto a análise de impactos, sendo considerada ponto-chave da política de segurança.
d) é recomendável que a política de segurança contenha os passos a serem seguidos para violações, de acordo com o grau de criticidade, visando aplicar ações corretivas sobre as vulnerabilidades e punição dos envolvidos.
e) é uma proposta viável para a implantação desta política: identificar recursos críticos, definir os objetivos de segurança a atingir, elaborar a proposta da política, analisar os riscos, discutir entre os envolvidos, aprovar e implementar.

65- A segurança de informações, em função de sua importância para a sociedade, originou diversos grupos de pesquisa, cujos trabalhos são traduzidos em padrões de segurança. Acerca de tal contexto, é correto afirmar que

a) a política de segurança define um padrão de segurança nas instituições, englobando o estabelecimento de princípios institucionais de como a organização irá proteger, controlar e monitorar seus recursos e as informações por eles manipulados.
b) a norma NBR/ABNT 17799 tem como objetivo a classificação de sistemas computacionais, de acordo com suas características de projeto.
c) o NCSC (*National Computer Security Center*) avalia os aspectos de segurança internos de sistemas computacionais e ainda publicou o conhecido "*Orange Book*" (ou Livro Laranja) que interpreta os princípios e critérios do "*Red Book*" (ou Livro Vermelho) para o ambiente cliente/servidor.
d) a classe D1 do "*Orange Book*" (ou Livro Laranja) compreende a mais alta categoria de segurança, englobando processos rígidos de projeto, controle e verificação.
e) a política de segurança de informações é independente, não gerando impactos ao plano de contingência, planejamento de capacidade e plano de continuidade de negócios.

66- Devido às vulnerabilidades do ambiente computacional, planejar a continuidade dos negócios e de recuperação após desastres, tornam-se atividades cada vez mais relevantes para a segurança da informação. Em relação a tal contexto, é incorreto afirmar que

a) a análise de impacto faz parte do planejamento de contingências da organização, identificando os impactos diretos e indiretos causados por interrupção de sistemas computacionais para a continuidade dos negócios da organização.
b) são fases do planejamento de contingências, nesta ordem: análise das alternativas de recuperação, análise de impacto, desenvolvimento do plano de contingência e treinamentos.
c) a política de *backup* é um dos itens importantes em um plano de contingências e compreende os procedimentos e a infra-estrutura necessários à proteção das informações de uma organização.
d) um plano de contingência efetivo deve compreender resposta imediata a desastres e processo de restauração, englobando assim, decisões gerenciais e passos para retornar à normalidade na organização.
e) enquanto na análise de riscos, identificam-se os aplicativos críticos, ao desenvolver um plano de contingências, deve-se estabelecer uma lista de prioridades para recuperação.

67-A respeito da análise de riscos e vulnerabilidades de segurança, é correto afirmar que

a) ameaça é uma fraqueza ou deficiência que pode ser explorada.
b) ataque é um evento ou atitude indesejável que potencialmente remove, desabilita, danifica ou destrói um recurso.
c) risco depende da probabilidade de uma ameaça atingir um sistema e do impacto resultante deste ataque.
d) ameaças que envolvem invasão e/ou monitoramento, sem alterações de informações, são denominadas ativas.
e) a análise de riscos despreza vulnerabilidades, concentrando-se em medir ameaças e impactos em um dado ambiente.

68-Sobre assinaturas e certificados digitais é correto afirmar que

a) a assinatura digital gerada pelo uso da chave privada de A aplicada a uma mensagem para o destino B, garante a autenticidade da origem e a integridade da mensagem.
b) um certificado digital é atribuído por uma CA (Certificate Authority) a um usuário, associando a este, uma chave pública e garantindo comunicações autênticas e confidenciais sempre que o certificado for utilizado pelo usuário.
c) o campo assinatura (*signature*) dos certificados digitais baseados no formato X.509 contém apenas o código *hash* dos outros campos do certificado, encriptados com a chave privada da autoridade certificadora.
d) a revogação de certificados acontece antes da expiração, caso ocorra, em caráter de exclusividade, o comprometimento da chave privada do usuário.
e) para qualquer número de usuários envolvidos, o esquema de efetuar autenticação usando criptografia convencional será viável para garantir autenticidade e confidencialidade no processo.

69-Técnicas criptográficas são essenciais à segurança da informação, nas organizações. A respeito de tal contexto, é correto afirmar que

a) no modo CBC (*Cipher Block Chaining*) do DES (*Data Encryption Standard*), se houver um erro em um bloco do criptograma transmitido, apenas aquele bloco da mensagem original será afetado, ou seja, o erro não se propaga aos demais blocos.
b) para A enviar uma mensagem M confidencial para B, uma possibilidade é encriptar M com uma chave secreta ECB-DES (*Encoding Code Book – Data Encryption Standard*) e encriptar a chave secreta com a chave pública RSA (*Rivest-Shamir-Adleman*) de B, garantindo melhor performance ao processo.

c) o DES (*Data Encryption Standard*) é um algoritmo simétrico com chaves de tamanho 64 bits, baseando-se em operações XOR (OU-exclusivo) e S-boxes (caixas-S) variáveis.

d) o RSA (*Rivest-Shamir-Adleman*) é um algoritmo de criptografia simétrica que limita o tamanho das chaves em 1024 por questões de desempenho, já que se baseia em operações com números primos de grande magnitude.

e) para um grupo de N usuários, haveria 1 chave pública e N chaves privadas para provar uma comunicação confidencial para quaisquer usuários, i e j, ao considerar a criptografia assimétrica.

70- A autenticação de usuários e mensagens é importante para garantir segurança de informações e de comunicação. Sendo assim, é correto afirmar que

a) considerando que A e B compartilham uma chave secreta e, se A calcula o MAC (*Message Authentication Code*) de uma mensagem M, e anexa-o à mensagem, enviando tudo para B, o processo como um todo garante integridade, autenticidade e confidencialidade.

b) uma função *hash* aceita uma mensagem como entrada e gera um MD (*Message Digest*) fixo como saída, baseando-se numa chave assimétrica de criptografia, para garantir a integridade.

c) no *Kerberos*, versões 4 e 5, os algoritmos de criptografia DES (*Data Encryption Standard*) e o RSA (*Rivest-Shamir-Adleman*) são exclusivamente utilizados.

d) se A envia para B, o conjunto (C = mensagem encriptada com a chave de sessão DES, Kc = chave K de sessão encriptada com a chave pública RSA de B), para B, este por sua vez, terá garantias de autenticidade e confidencialidade da mensagem.

e) no *Kerberos*, versão 5, é possível dispor de credenciais que permitam um cliente requisitar serviço a um servidor de impressão, por exemplo, que por sua vez, acessa o arquivo do cliente em um servidor de arquivos, usando as credenciais de acesso do cliente.

71- Analise as seguintes afirmações relacionadas às especificações que definem as características funcionais, mecânicas e elétricas para rede local Ethernet.

I. Uma rede local 10Base2 e uma 10Base5 utilizam, respectivamente, cabo coaxial grosso e fino.

II. Uma rede local 10Base-T utiliza cabo coaxial fino com conector BNC, ou cabo coaxial grosso.

III. Uma rede local 10Base-T utiliza cabos categorias 3, 4 e 5 com conectores RJ-45.

IV. Uma rede local 100Base-TX utiliza cabo trançado, categoria 5, e conectores RJ-45.

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

72- Considere as seguintes afirmações relacionadas ao protocolo OSPF (*Open Shortest Path First*) e RIP (*Routing Information Protocol*).

I. O RIP consegue lidar com no máximo 16 saltos e o RIP2 consegue lidar com máscaras de sub-rede.

II. O RIP é um protocolo que se utiliza do algoritmo de vetor de distâncias e o OSPF utiliza um algoritmo de estado de enlace.

III. O RIP é um protocolo de passagem interior, também denominado IGP (*Interior Gateway Protocol*), e o OSPF é um protocolo de passagem exterior, também denominado EGP (*Exterior Gateway Protocol*).

IV. O RIP efetua atualizações periódicas de suas tabelas enquanto o OSPF efetua atualizações quando ocorre uma mudança no estado das ligações.

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

73- A rede 172.18.0.0 foi dividida em sub-redes segundo a técnica CIDR (*Classless Interdomain Routing*) tornando-se 172.18.0.0/21. Neste caso, a quantidade de sub-redes obtidas com a divisão, a quantidade máxima de computadores por sub-rede e o endereço de sub-rede à qual pertence o IP 172.18.20.32/21 são, respectivamente,

a) 21, 2048, 172.18.20.0

b) 32, 2048, 172.18.16.0

c) 8, 1024, 172.18.20.0

d) 32, 2046, 172.18.16.0

e) 21, 1024, 172.18.20.0

74-Considerando os conceitos associados à transmissão de dados/voz em uma linha telefônica é incorreto afirmar que

a) a multiplexação por divisão de freqüência consiste na transmissão seqüencial de canais telefônicos, efetuando com isso um melhor aproveitamento do espectro de freqüência disponibilizado.

b) a multiplexação por divisão de freqüência permite o agrupamento de diferentes canais em um super grupo, o qual consiste na multiplexação por freqüência de canais arranjados em grupos, seguido da multiplexação destes grupos, permitindo um melhor aproveitamento do canal.

c) para transmissão de vários bits por *baud*, o modem padrão V.32bis de 14400bps efetua uma transmissão de 6 bits por amostra com uma velocidade de 2400 *bauds*.

d) na multiplexação por divisão do tempo os dados analógicos são convertidos ao formato digital por meio de codec (codificador/decodificador) efetuando-se uma amostragem do sinal milhares de vezes por segundo.

e) conforme o teorema de Nyquist, a taxa máxima de dados em um canal sem ruído é o dobro da taxa de amostras, ou seja, em um canal de 4000Hz (com transmissão de sinais binários) a capacidade é de 8000 bps (bits por segundo).

75-Qualidade de Serviço (QoS) refere-se à habilidade de prover um serviço melhor para redes baseadas em tecnologias diversas, tais como: Ethernet, Frame-Relay, ATM (*Asynchronous Transfer Mode*), entre outras. Neste contexto, é incorreto afirmar que

a) as aplicações que se utilizam da rede demandam dois tipos de tráfego: o elástico e o inelástico. No primeiro, as informações, inclusive vídeo, são codificadas como dados e transmitidas em modo assíncrono, sendo admitidos atrasos e oscilações. No segundo, o dado, geralmente decorrente de uma comunicação interativa, necessita de uma explícita largura de banda para que o atraso (também denominado *delay*) e a variação do atraso (também denominada *jitter*) permaneçam dentro dos padrões aceitáveis por parte de aplicações e usuários.

b) um dos algoritmos utilizados para o controle de banda é denominado de balde furado (ou *leaky bucket*), o qual, através de um fluxo constante de *tokens*, limita o volume de tráfego na rede, não admitindo oscilações no tráfego acima do que foi especificado.

c) na especificação do controle de banda é utilizado um algoritmo denominado balde de *tokens* (ou *token bucket*). É baseado em dois parâmetros: a taxa de *tokens* e a profundidade do balde. A profundidade do balde regula a velocidade do fluxo de pacotes, enquanto a taxa de *tokens* especifica a variação permitida no fluxo.

d) o IntServ é uma arquitetura que define que cada aplicação deve solicitar sua reserva de recursos. Utiliza RSVP (*Resource Reservation Protocol*), que se baseia em duas mensagens: PATH e RESV. Uma mensagem PATH percorre a rede através de caminhos definidos pelos mecanismos de encaminhamento até chegar aos receptores, armazenando os nós por onde passa. Uma mensagem RESV informa os parâmetros a serem aceitos por cada receptor. Os roteadores situados entre o transmissor e o receptor é que decidirão se podem suportar os recursos solicitados.

e) o MPLS (*Multiprotocol Label Switching*) é um protocolo que pode ser considerado uma alternativa ao ATM (*Asynchronous Transfer Mode*). Ele vem sendo amplamente utilizado em redes com alto volume de tráfego e que podem estar sujeitas a acordos de nível de serviço. O pacote entra na nuvem pelo roteador de borda que lhe atribui uma etiqueta de identificação. O roteamento, ao invés de utilizar-se de tabelas IP, é baseado em etiquetas que identificam o trajeto a ser percorrido pelo pacote. O pacote tem sua etiqueta removida quando estiver saindo da nuvem. Esta etiqueta pode ser removida pelo roteador de borda da saída ou por seu antecessor, conforme as configurações efetuadas.