ESAF
Escola de Administração Fazendária

Controladoria-Geral da União

Concurso Público - 2006

Cargo: ANALISTA DE FINANÇAS E CONTROLE

Prova P.3

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:

"Quem mal lê, mal ouve, mal fala, mal vê."

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

5- Na prova há **70 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

INFORMÁTICA

01- Analise as seguintes afirmações relacionadas a conceitos básicos de hardware:

I. ADSL (*Assimetric Digital Subscriber Line*) é uma tecnologia de acesso rápido que usa as LANs para permitir acesso à Internet. Em geral, as velocidades variam de 256 kbps a 2 Mbps, dependendo da velocidade do adaptador de rede utilizado no computador. A principal vantagem é usar apenas a LAN, não sendo necessário o uso do sistema telefônico.

II. O *overclock* é uma técnica que permite aumentar a freqüência de operação do processador alterando-se a freqüência de barramento da placa-mãe ou, em alguns casos, o multiplicador.

III. O AGP 8X é uma versão recente do barramento AGP, que apesar de manter a freqüência de operação de 66 MHz passou a ser capaz de realizar 8 transferências por ciclo, atingindo uma taxa de 2133 MB/s. Tem uma característica especial que é a utilização da memória RAM compartilhada como memória de vídeo.

IV. ALU (*Arithmetic Logic Unit* ou Unidade Lógica e Aritmética) é a parte do processador principal, denominada co-processador aritmético, encarregada de controlar os cálculos de números inteiros.

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

02- Analise as seguintes afirmações relacionadas a conceitos básicos de hardware:

I. A fonte ATX tem os mesmos fios de alimentação de 3,3V e *power-on* existentes nas fontes AT. Por conta deste último, o comando de ligar ou desligar a fonte passou a ser enviado pela placa-mãe e não mais por uma chave liga-desliga conectada diretamente à fonte. Da mesma forma que a fonte AT, a fonte de alimentação ATX usa um plug de 20 pinos, sendo que a grande diferença entre os dois tipos de fonte é a inovação do tipo ATX que permite programar o PC a se desligar sozinho. Devido à compatibilidade entre estes dois tipos de fontes, a instalação de uma fonte ATX em uma placa-mãe AT, ou vice-versa, apenas deixa desabilitada a funcionalidade *power-off*.

II. As memórias DDR e DDR2 transferem dois dados por pulso de *clock*. Por conta disso, para obter o *clock* real, deve-se dividir, por dois, o *clock* nominal indicado para estas memórias. Por exemplo, a memória DDR2-667 na realidade trabalha a 333 MHz.

III. Nas memórias DDR a terminação resistiva necessária para a memória funcionar está localizada na placa-mãe. Já na DDR2 este circuito está localizado dentro do *chip* de memória. É por este motivo que não é possível instalar memórias DDR2 em soquetes de memória DDR e vice-versa.

IV. O único componente que pode acessar a memória RAM da máquina é o processador. O recurso DMA impede que outros componentes, exceto adaptadores AGP, também acessem a memória RAM diretamente. Este controle resulta em um aumento do desempenho na transferência de grande quantidade de dados.

Indique a opção que contenha todas as afirmações verdadeiras.

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

03- Dependendo da configuração do computador, algumas pastas compartilhadas especiais são criadas automaticamente pelo Windows 2000 para uso administrativo e do sistema. Com relação a essas pastas é correto afirmar que

a) todos esses compartilhamentos são visíveis no menu “Meu computador” do Windows 2000.
b) o NETLOGON é um recurso que compartilha os *pipes* essenciais para a comunicação entre programas. Ele é utilizado durante a administração remota e a visualização dos recursos compartilhados de um computador.
c) o compartilhamento C$ é um recurso utilizado pelo sistema durante a administração remota de um computador. O caminho deste recurso é sempre o caminho da raiz do sistema Windows 2000.
d) o IPC$ é um recurso também utilizado pelo serviço *Logon* de rede de um computador com o Windows 2000 Server durante o processamento de solicitações de *logon* de domínio.
e) o FAX$ é uma pasta compartilhada em um servidor usado por clientes de fax no processo de envio de um fax. A pasta compartilhada é usada para armazenar arquivos temporariamente em *cache* e acessar folhas de rosto armazenadas no servidor.

04- Analise as seguintes afirmações relacionadas aos conceitos básicos de *clusters*, gerência de recursos e sistema operacional Linux com Kernel 2.4:

I. No Linux, os processos denominados “zumbis” são aqueles cujas execuções foram interrompidas, podendo voltar a atividade através de um comando. Esses processos podem estar “travados”, inativos ou, em alguns casos, executando em segundo plano.

II. Um *cluster* de máquinas Linux é composto por um conjunto de PCs heterogêneos que atuam compartilhando entre si seus recursos computacionais. Por exemplo, se um usuário executar uma aplicação que exige um uso extraordinário de CPU, todas as máquinas envolvidas no *cluster* irão iniciar a aplicação e aquela que terminar primeiro irá avisar às outras máquinas do *cluster* que podem abandonar a execução da tarefa em questão. Todos os procedimentos para o uso do *cluster* são transparentes à aplicação e ao usuário final.

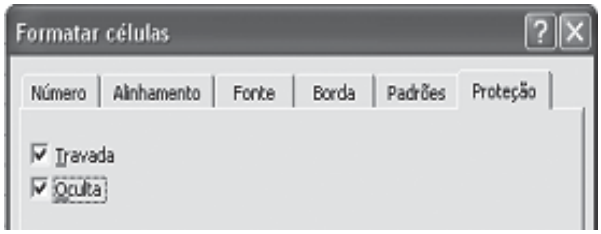
III. O Linux com Kernel 2.4 suporta quase todos os sistemas de arquivos existentes. Uma exceção é o sistema NTFS do Windows 2000, que é suportado apenas em modo de “somente leitura”.

IV. Ao utilizar uma máquina que tenha *dual-boot* entre o Linux com Kernel 2.4 e o Windows XP, uma forma de se manter uma partição que possa ser utilizada para escrita e leitura pelos dois sistemas operacionais é por meio da criação de uma partição FAT 32 que sirva como uma “área de transferência” para troca de arquivos, já que o Windows não é capaz de escrever nas partições Linux.

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- No Microsoft Excel, ao se selecionar uma célula e formatá-la conforme indicado na figura a seguir, é correto afirmar que os itens selecionados “Travada” e “Oculta”



a) impedem que o valor da célula, qualquer que seja seu conteúdo, seja visualizado quando a planilha estiver protegida.
b) impedem que o valor da célula, qualquer que seja seu conteúdo, seja visualizado qualquer que seja a situação de proteção da planilha.
c) impedem que o usuário altere o conteúdo de uma célula desde que este seja uma fórmula.
d) que, respectivamente, se referem a Travar o alinhamento e Ocultar o conteúdo da célula de maneira que ela não apareça na barra de status quando a célula for selecionada, não terão efeito, a menos que a planilha esteja protegida.
e) que, respectivamente, se referem a Travar a célula e Ocultar a fórmula de maneira que ela não apareça na barra de fórmulas quando a célula for selecionada, não terão efeito a menos, que a planilha esteja protegida.

06- Analise as seguintes afirmações relacionadas ao uso da Internet:

I. Ao configurar um aplicativo de gerenciamento de e-mail, o usuário deverá relacionar o servidor POP3 com o envio de e-mail de sua máquina para o servidor de e-mail.

II. Um *cookie* é um arquivo criado por um site da Web que armazena informações no computador do usuário, como suas preferências ao visitar esse site.

III. É possível configurar o Internet Explorer como o navegador padrão da Internet, de tal forma que, após esta configuração, se outro navegador for definido como navegador padrão da Internet e, em seguida, o Internet Explorer for iniciado, este perguntará se o usuário deseja restaurá-lo como navegador padrão.

IV. No Outlook Express, na configuração padrão, quando se envia uma nova mensagem pode-se atribuir uma prioridade a ela, de maneira que o destinatário saiba se deve lê-la imediatamente (Prioridade alta) ou quando tiver tempo (Prioridade baixa). Uma mensagem de prioridade alta é indicada por uma seta para cima, enquanto a de prioridade baixa possui um ponto de exclamação próximo a ela.

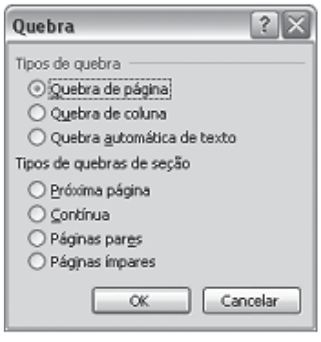
Indique a opção que contenha todas as afirmações verdadeiras.

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

07- A proteção dos sistemas utilizados pelos fornecedores de serviços pela Internet requer a aplicação de ferramentas e conceitos de segurança eficientes. Quanto ao *firewall* que trabalha na filtragem de pacotes, um dos mais importantes itens de segurança para esses casos, é correto afirmar que ele

a) se restringe a trabalhar nas camadas HTTP, decidindo quais pacotes de dados podem passar e quais não. Tais escolhas são regras baseadas nas informações do serviço remoto, endereço IP do destinatário, além da porta UDP usada.
b) é capaz de controlar conexões pelas portas UDP utilizadas, além de ser capaz de analisar informações sobre uma conexão já estabelecida, sem o uso de portas.
c) é instalado geralmente em computadores servidores, também conhecidos como *proxy*.
d) determina que endereços IPs podem estabelecer comunicação e/ou transmitir ou receber dados.
e) além de ter a capacidade de analisar o conteúdo dos pacotes, o que permite um controle ainda maior, pode ou não ser acessível para conexões que usam porta UDP.

08- Considerando-se um texto com vários parágrafos, ao selecionar todo um parágrafo localizado no meio desse texto, incluindo a sua marca de parágrafo, e, em seguida, utilizando-se a opção "Quebra" do menu "Inserir", conforme indicado na figura a seguir, será inserida uma Quebra de página.



Neste caso é correto afirmar que

a) a marca de Quebra de página fica localizada na mesma página na qual se encontra a primeira linha do parágrafo selecionado.
b) a marca de Quebra de página fica localizada no final do último parágrafo do texto em questão.
c) o parágrafo selecionado mudará para a próxima página.
d) o parágrafo selecionado permanecerá na mesma situação e localização que se encontrava antes da inserção da Quebra de Página.
e) o Word apresentará uma mensagem de erro indicando que a seleção da marca de parágrafo é inválida para a tarefa de inserção de Quebra de página.

09- Analise as seguintes afirmações relacionadas a redes de computadores e segurança da informação:

I. Protocolos como POP3 e FTP enviam senhas criptografadas através da rede, tornando essa informação impossível de ser obtida por um invasor que use a detecção de rede.
II. O IPsec pode ser usado para implementar uma verificação de conexão adicional. É possível configurar regras de diretiva que exijam uma negociação de IPsec bem-sucedida a fim de conceder acesso a um conjunto de aplicativos.
III. Na Espionagem na rede (*sniffing*) os invasores tentam capturar o tráfego da rede com diversos objetivos, entre os quais podem ser citados obter cópias de arquivos importantes durante sua transmissão e obter senhas que permitam estender o seu raio de penetração no ambiente invadido.
IV. Ataques de negação de serviço são ataques direcionados a um usuário específico da Internet.

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

10- Analise as seguintes afirmações relacionadas a sistemas de Tolerância a Falhas:

I. Em um espelhamento, os dois volumes envolvidos devem residir no mesmo disco rígido. Se um espelho se tornar indisponível, devido à falha do sistema operacional, pode-se usar o outro espelho para obter acesso aos dados.
II. No RAID 5 as informações de paridade são gravadas e distribuídas dentro dos próprios discos envolvidos, isto é, não existe a necessidade de um disco rígido extra para este fim.
III. O RAID 0, além de distribuir informações de paridade entre seus discos, usa um disco extra para armazenamento em redundância dessas informações de paridade.
IV. O RAID 4 funciona com três ou mais discos iguais. Um dos discos guarda a paridade da informação contida nos demais discos. Se algum dos discos falhar, a paridade pode ser utilizada para recuperar o seu conteúdo.

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

DESENVOLVIMENTO DE SISTEMAS

11- Analise as seguintes afirmações relacionadas a desenvolvimento estruturado.

I. Um DFD é composto por dois elementos gráficos. Um representa o fluxo de dados e os processos e o outro, o dicionário de dados.
II. Um diagrama de fluxo de dados - DFD é uma especificação em rede de um sistema e mostra os componentes ativos do sistema e as interfaces de dados entre eles.
III. Um processo pode transformar dados, modificando a informação contida nos dados.
IV. Um dicionário de dados em um DFD é desenhado como um par de linhas paralelas. A identificação do nome do arquivo encontra-se entre as duas linhas.

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

12- Quanto ao uso de diagramas na UML para a modelagem de objetos é correto afirmar que o Diagrama de Seqüência

a) descreve a funcionalidade do sistema percebida por atores externos.
b) apresenta a interação de seqüência de tempo dos objetos que participam na interação.
c) apresenta a interação de seqüência de atores que participam na interação.
d) descreve a funcionalidade do sistema percebida por atores internos.
e) apresenta a interação de seqüência estática de pacotes, relacionamentos e instâncias.

13- Na UML o diagrama que mostra elementos de configuração de processamento *runtime* e os componentes de software, processos e objetos, que neles se mantêm, é denominado diagrama de

a) Atividades.
b) Casos de Uso.
c) Implantação.
d) Componentes.
e) Estado.

14- Analise as seguintes afirmações relacionadas aos conceitos básicos relacionados a programação e Linguagens de Programação Orientadas a Objetos.

I. Na Programação Orientada a Objetos o *overflow* em operações aritméticas e a divisão por zero não podem ser tratados como exceções.
II. Uma vez que uma exceção é disparada o controle não pode retornar diretamente ao ponto de disparo.
III. Uma exceção termina o bloco no qual ela ocorreu.
IV. O tratamento de exceções é utilizado para tratar erros de sintaxe, isto é, erros que acontecem como resultado da compilação de um programa.

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

15- Analise as seguintes afirmações relacionadas aos conceitos básicos de Programação Orientada a Objetos.

I. Modificações de uma classe base requerem, obrigatoriamente, que as classes derivadas mudem.
II. Uma classe derivada não pode conter atributos adicionais diferentes dos existentes na sua classe base.
III. Criar uma classe derivada não afeta o código-fonte da sua classe base. A integridade de uma classe base é preservada pela herança.
IV. Uma classe derivada contém os atributos e comportamentos de sua classe base.

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

16- Analise as seguintes afirmações relacionadas a conceitos básicos de Programação de Computadores.

I. O escopo de uma variável de programa é a faixa de instruções na qual a variável é visível. Uma variável é visível em uma instrução se puder ser referenciada nessa instrução.

II. Um registro é um agregado, possivelmente heterogêneo de elementos, cujos elementos individuais são identificados por nomes.

III. Um *array* é um agregado heterogêneo de elementos de dados, cujo elemento individual é identificado por sua posição em relação ao primeiro.

IV. Um tipo **Ponteiro** é aquele em que as variáveis têm uma faixa de valores que consiste em uma *string* ou coleção de caracteres e um valor especial denominado Null.

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

17- Analise as seguintes afirmações relacionadas a conceitos básicos de Programação de Computadores.

I. Uma instrução iterativa faz com que uma instrução ou uma coleção de instruções seja executada zero, uma ou mais vezes.

II. Cada subprograma tem um único ponto de entrada e o controle sempre retorna ao chamador quando a execução do subprograma é concluída.

III. Quando um parâmetro é passado por referência, o valor do parâmetro real é usado para inicializar o parâmetro formal correspondente, que, então, age como uma variável local no subprograma.

IV. O encapsulamento é uma estrutura de dados que consiste em um número inteiro e uma fila que armazena descritores de tarefas. O conceito de encapsulamento consiste na colocação de proteções em torno do código que acessa a estrutura para oferecer acesso limitado a uma estrutura de 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

18- As unidades concorrentes em Java são objetos que incluem um método chamado *run*, cujo código pode estar em execução concorrente. Uma das maneiras de se definir uma classe cujos objetos podem ter métodos concorrentes é definir uma

a) classe abstrata *run* e, em seguida, definir subclasses *run*.
b) subclasse da classe predefinida thread, que fornece suporte para o método *run*.
c) exceção para o método *run*.
d) exceção para o método *main*.
e) exceção com interrupção para o método *run* ativo, sempre que um novo método *run* for instanciado.

19- Analise as seguintes afirmações relacionadas a conceitos básicos de estruturas de dados.

I. Em uma árvore genérica, não binária, cada nó pode ter qualquer quantidade de nós filhos.

II. Em uma árvore binária de pesquisa, a busca é feita de tal forma que se o dado procurado está na raiz a pesquisa será encerrada. Caso contrário, a busca continua e deve ser feita em apenas uma das duas sub-árvores.

III. Uma árvore binária é considerada balanceada quando, para cada nó, a altura das duas sub-árvores diferem, no máximo, da somatória da quantidade de nós existentes nos níveis pares, dividido pela quantidade de níveis considerados.

IV. Um circuito em um grafo é um caminho único que tem origem no primeiro nó e se encerra no último nó.

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

20- Em algumas linguagens de Programação Orientadas a Objetos, como por exemplo o C++, ao se derivar uma classe a partir de uma classe base, a classe base pode ser herdada como *public*, *protected* ou *private*. Quando a derivação é do tipo *public*, os membros

a) *public e protected* da classe base tornam-se, respectivamente, membros *public* e *protected* da classe derivada.
b) *private* da classe base serão acessados e utilizados diretamente a partir da classe derivada.
c) *public* e *protected* da classe base tornam-se membros *public* da classe derivada.
d) *public* e *protected* da classe base tornam-se membros *protected* da classe derivada.

e) *public*, *protected* e *private* da classe base tornam-se, todos, membros *private* na classe derivada, independentemente do tipo de herança utilizada.

21- Um procedimento armazenado (*stored procedure)* é uma coleção de comandos em SQL que

a) provoca um aumento no tráfego na rede e reduz a performance do sistema, mas continua sendo largamente utilizado para criar mecanismos de segurança em bancos de dados relacionais.
b) encapsula tarefas repetitivas, aceita parâmetros de entrada e pode retornar um valor de *status* para indicar sucesso ou falha na execução.
c) estão armazenados no banco de dados e que são executadas diretamente na máquina do usuário.
d) estão armazenados na máquina do usuário e que são executadas diretamente no servidor do banco de dados.
e) são utilizados unicamente para autenticar um usuário, dando a ele direitos de acesso a escrita/alteração em tabelas do banco de dados.

22-Analise as seguintes afirmações relacionadas a conceitos básicos de banco de dados e linguagem SQL.

I. Na linguagem SQL um INNER JOIN retorna todas as tuplas comuns às duas tabelas.
II. Em uma Junção entre duas tabelas a cláusula USING só poderá ser usada quando o nome do atributo for igual nas duas tabelas.
III. Na linguagem SQL um RIGHT OUTER JOIN retorna todas as tuplas que não são comuns às duas tabelas.
IV. Uma Junção é usada para compor informações complexas a partir de tabelas sem nenhum tipo de relacionamento.

Indique a opção que contenha todas as afirmações verdadeiras.

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

23-Analise as seguintes afirmações relacionadas a conceitos de Sistemas de Gerenciamento de Banco de Dados.

I. O LOCK é um mecanismo usado para controlar o acesso aos dados em um sistema multiusuário. Ele previne que o mesmo dado seja alterado por dois usuários simultaneamente ou que a tabela seja alterada em sua estrutura enquanto os dados estão sendo modificados.
II. Os bloqueios de registros gastam mais memória que bloqueios em páginas ou tabelas, mas permitem bloquear um único registro por um longo tempo.
III. O LOCK de tabela ocorre quando o sistema entra em estado de *DeadLock* e, em seguida, executa um COMMIT para sair do referido estado.
IV. O comando SQL responsável por fechar uma transação confirmando as operações feitas é o INSERT. Para desfazer todas as operações o comando a ser utilizado é o DROP.

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

24- Analise as seguintes afirmações relacionadas aos conceitos de Sistemas de Gerenciamento de Banco de Dados.

I. A visão (*View*) é uma construção de uma projeção de uma ou mais tabelas a partir do comando SELECT que, em alguns casos, pode ser manipulada como uma tabela, mas não existe fisicamente como uma tabela.
II. As *Views* são usadas para garantir o acesso aos dados da tabela original. Esse mecanismo permite que se desconsiderem os sofisticados sistemas de privilégios dos SGBDs modernos.
III. Um SGBD deve dispor de recursos que possibilitem selecionar a autoridade de cada usuário.
IV. A linguagem SQL naturalmente controla a concorrência ao acesso dos dados, garantindo em qualquer tipo de situação a escrita/leitura de dados sem erros.

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

25-Analise as seguintes afirmações relacionadas aos sistemas de qualidade no desenvolvimento de software.

I. No CMMI nível 2, a área de processo Garantia da Qualidade do Processo e Produto (PPQA) deve fornecer uma gestão com visibilidade apropriada sobre os processos utilizados e produtos desenvolvidos pelo projeto de software.

II. No CMMI nível 3, a área de processo Validação (VAL) deve demonstrar que o produto ou seus componentes funcionam como esperado no ambiente pretendido.

III. No CMMI nível 3, a área de processo Foco do Processo na Organização (OPF) deve estabelecer e manter um conjunto de processos que pode ser utilizado por toda organização.

IV. No CMMI nível 3, a área de processo Desenvolvimento e Inovação Organizacional (OID) deve planejar e implementar melhorias de processos na organização baseadas nas suas fragilidades e forças.

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

26-Quanto às Metas e Áreas de Processos do CMMI é correto afirmar que

a) a meta “Mitigar Riscos”, da área de processo Gerência de Projeto Integrada (IPM), é exigida em todos os níveis do CMMI.
b) “Desenvolver Melhorias”, com o objetivo de inovar e desenvolver melhorias de forma incremental de acordo com os objetivos da organização e que permitam medir o desempenho dos seus processos e tecnologias, é meta da Área de Processo “Análise e Resolução de Causa” (CAR) do CMMI nível 2.
c) verificar se os componentes do produto podem ser integrados, montar o produto, verificar, validar e entregar o produto são metas da Área de Processo Solução Técnica(TS) do CMMI nível 2.
d) a meta “Estabelecer os Recursos para os Processos da Organização”, da área de processo Gerência de Projeto Integrada (IPM), é exigida apenas no CMMI nível 2.
e) “Prevenir as Causas dos Defeitos”, tomando-se decisões para prevenir que os defeitos e problemas já ocorridos voltem a acontecer, é meta da Área de Processo “Análise e Resolução de Causa” (CAR) do CMMI nível 5.

27- Na Análise de Ponto por Função, para que uma determinada função seja contada como um Arquivo Lógico Interno (ALI), algumas regras devem ser atendidas. Uma dessas regras visa a garantir que o grupo de dados

a) é referenciado pela aplicação contada, porém é mantido fora da sua fronteira.
b) não é referenciado pela aplicação contada e deve ser mantido fora da sua fronteira.
c) não participa de nenhum tipo de relacionamento com o usuário.
d) é mantido por outra aplicação, porém é considerado um ALI nesta outra aplicação.
e) ou informações de controle é logicamente relacionado e identificável pelo usuário.

28-Na Análise de Ponto por Função, o fator de ajuste é baseado em 14 características gerais de sistema. Com relação a essas características, é correto afirmar que a

a) Performance descreve o nível em que a aplicação comunica-se diretamente com o processador.
b) Facilidade de Operação descreve em que nível considerações sobre fatores humanos e facilidade de uso pelo usuário final influenciam o desenvolvimento da aplicação.
c) Comunicação de dados descreve o nível em que considerações sobre tempo de resposta e taxa de transações influenciam o desenvolvimento da aplicação.
d) Reusabilidade descreve o quanto a aplicação e seu código foram especificamente projetados, desenvolvidos e suportados para serem utilizados em outras aplicações.
e) Modificação facilitada descreve em que nível o processamento lógico ou matemático influencia o desenvolvimento da aplicação.

29- Com relação à arquitetura em camadas no desenvolvimento Orientado a Objetos é correto afirmar que

a) uma camada é diretamente dependente de todas as outras camadas existentes na aplicação.
b) as camadas se comunicam da base para o topo.
c) na camada de apresentação a lógica de interface do usuário é o ponto mais forte.
d) nenhuma camada pode ser desativada de qualquer outra camada, exceto da camada imediatamente inferior a ela.
e) a camada de negócio é responsável pelo armazenamento e recuperação dos dados.

30- Analise as seguintes afirmações relacionadas ao Guia do Conjunto de Conhecimentos em Gerenciamento de Projetos - PMBOK.

I. O Gerenciamento das comunicações do projeto descreve os processos envolvidos na verificação de que o projeto inclui todo o trabalho necessário, e apenas o trabalho necessário, para que seja concluído com sucesso.

II. Segundo o PMBOK, os objetivos dos projetos e das operações são fundamentalmente diferentes. A finalidade de um projeto é atingir seu objetivo e, em seguida, terminar. Por outro lado, o objetivo de uma operação contínua é manter o negócio.

III. O gerenciamento de projetos é realizado através da aplicação e da integração dos seguintes processos de gerenciamento de projetos: Gerenciamento de risco, Desenvolvimento e Teste.

IV. Segundo o PMBOK, o gerenciamento de projetos é a aplicação de conhecimento, habilidades, ferramentas e técnicas às atividades do projeto a fim de atender aos seus requisitos.

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

ADMINISTRAÇÃO DE REDES

31- Analise as seguintes afirmações relacionadas à topologia de redes:

I. Uma rede em anel consiste de estações conectadas através de um caminho fechado. O anel não interliga diretamente às estações. Neste caso, uma série de repetidores interligados fisicamente são encarregados de conectarem estações à rede.

II. Em algumas configurações em anel a transmissão é unidirecional, permitindo que os repetidores sejam projetados de forma a transmitir e receber dados simultaneamente, diminuindo assim o retardo da transmissão.

III. Em redes em anel com transmissão unidirecional, quando uma mensagem é enviada por um nó ela entra no anel e fica circulando na rede até que complete um número de voltas igual ao número de nós existentes. Após isso, recebe a marcação indicativa de “a ser descartada” e, no próximo ciclo, será descartada pelo nó que colocou a referida marcação.

IV. A maior vantagem do uso de redes com topologia em anel é que a quebra ou falha em qualquer dos repetidores não compromete o funcionamento da rede. Essa característica torna a rede com topologia em anel uma das mais confiáveis e seguras.

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

32- Analise as seguintes afirmações relacionadas à topologia e elementos de interconexão de redes de computadores:

I. O poder de crescimento, no que diz respeito à distância máxima entre dois nós, em uma rede com topologia em barra dependerá exclusivamente da taxa de transmissão utilizada.

II. A topologia em barra apresenta uma configuração multiponto onde todas as estações ou nós conectam-se ao meio físico de transmissão, permitindo que cada um desses nós possam “ouvir” as informações transmitidas.

III. Os transceptores utilizados para conectar os nós ao meio de transmissão em redes com topologia em barra geram descontinuidade de impedância, causando reflexões e limitando em 16 a quantidade de nós que podem fazer parte do mesmo segmento físico.

IV. Na topologia em barra a ligação das estações ao meio de comunicação é realizada através de um transceptor, que tem como funções básicas transmitir e receber sinais, bem como reconhecer a presença destes sinais no meio.

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

33- No nível de aplicação da arquitetura TCP/IP para a Internet, os usuários usam programas para acessar os serviços disponíveis, que interagem com o nível de transporte para enviar e receber dados. As aplicações podem utilizar serviços orientados à conexão fornecidos pelo

a) HTTP.
b) TCP.
c) UDP.
d) TCP e pelo UDP.
e) HTTP, pelo TCP e pelo UDP.

34- Um *Firewall* pode ser definido como uma coleção de componentes, colocada entre duas redes, que coletivamente possua propriedades que

a) independentemente da política de segurança adotada, tem como objetivo principal impedir a entrada de vírus em um computador, via arquivos anexados a e-mails.

b) garantem que todo o tráfego de dentro para fora da rede, e vice-versa, deve ser bloqueado, independentemente da política de segurança adotada. Todo *firewall* deve ser à prova de violação.

c) garantem que todo o tráfego de dentro para fora da rede, e vice-versa, passe por ele. Somente o tráfego autorizado pela política de segurança pode atravessar o *firewall* e, finalmente, ele deve ser à prova de violação.

d) garantem que apenas o tráfego de dentro para fora da rede deve passar por ele. Somente o tráfego autorizado pela política de segurança pode atravessar o *firewall* e, finalmente, ele deve ser à prova de violação.

e) garantem que apenas o tráfego de fora para dentro da rede deve passar por ele. Somente o tráfego autorizado pela política de segurança pode atravessar o *firewall* e, finalmente, ele deve ser à prova de violação.

35- Em algumas topologias de rede, onde as estações estão ligadas a um elemento concentrador, com implementação interna desconhecida e com interface compatível com as estações, é possível que estes implementem arquiteturas que possibilitem a troca de mensagens entre várias estações simultaneamente. Assim, duas estações podem obter taxas efetivas de transmissão bem maiores que aquelas obtidas quando a taxa de transmissão nominal do elemento concentrador é compartilhada entre todas as estações. O elemento concentrador que permite esse tipo de configuração é denominado

a) *switch*.

b) ponte.

c) repetidor.

d) roteador.

e) *hub*.

36- Analise as seguintes afirmações relacionadas a redes de comunicação de dados e ao modelo OSI:

I. No modelo OSI, durante a transmissão no modo "não-orientado à conexão" o fornecedor do serviço relaciona um pedido com todos os outros feitos antes, mas não permite seu relacionamento com os outros feitos depois.

II. No modelo OSI, o serviço fornecido por uma camada pode ser "orientado à conexão" ou "não-orientado à conexão". No modo de transmissão "orientado à conexão" o serviço é dividido em três fases de operação: estabelecimento da conexão; transferência de dados e liberação da conexão.

III. No modelo OSI, durante a recepção no modo "orientado à conexão" o fornecedor do serviço não relaciona um pedido com os outros ocorridos antes dele e nem permite seu relacionamento com os que ocorrerem depois dele.

IV. No modelo OSI, durante a transmissão no modo "não-orientado à conexão básica", cada unidade de dados é roteada de forma independente das demais e não ocorre seqüenciamento nem controle de fluxo.

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

37- O modelo OSI possui sete níveis de protocolos, cada um tem seus objetivos e implementam serviços específicos. O objetivo do nível de enlace é

a) detectar e, opcionalmente, corrigir erros que porventura ocorram no nível físico, convertendo um canal de transmissão não-confiável em um canal de transmissão confiável para uso do nível de rede.

b) a multiplexação de conexões.

c) fornecer ao nível de transporte uma independência quanto a considerações de chaveamento e roteamento associadas ao estabelecimento e à operação de uma conexão de rede.

d) fornecer os serviços de controle de diálogo e o gerenciamento de *token* e de atividades.

e) fornecer as características mecânicas, elétricas, funcionais e de procedimento para ativar, manter e desativar conexões físicas para a transmissão de dados.

38- Analise as seguintes afirmações relacionadas a servidores, protocolos e elementos de interconexão em redes de comunicação de dados:

I. O FTP permite que um usuário de um computador transfira, renomeie ou remova arquivos remotos. O FTP só permite a transferência de arquivos completos.

II. Os repetidores são usualmente classificados em conversores de meio e em tradutores de protocolos. Como conversores de meio são capazes de receber um pacote do nível inferior, tratar o cabeçalho inter-redes do pacote, identificar os dados que necessita, construir novo pacote e enviá-lo ao destino.

III. O sistema de gerenciamento de redes da arquitetura Internet TCP/IP opera na camada de aplicação e baseia-se no protocolo SNMP.

IV. O HTTP é um esquema de gerenciamento de nomes, hierárquico e distribuído, capaz de definir a sintaxe dos nomes usados na Internet, as regras para a delegação de autoridade na definição desses nomes, um banco de dados distribuído que associa nomes a atributos e um algoritmo distribuído para mapear nomes em endereços.

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

39- A comunicação via comutação de circuitos envolve as fases de

a) autenticação do usuário, estabelecimento dos direitos de acesso desse usuário e transferência dos dados. Após a autenticação do usuário, um canal não dedicado é alocado, permitindo a transferência dos dados até que o usuário abandone a conexão.
b) identificação e autenticação do usuário, transferência dos dados e encerramento do processo. Após a autenticação do usuário, um canal é alocado e permanece dedicado a essa transmissão até o momento do encerramento do processo.
c) estabelecimento do circuito, transferência de informação e desconexão do circuito. No caso da fase de estabelecimento do circuito, uma rota entre as estações é determinada e alocada e, para cada enlace, um canal é alocado e permanece dedicado a essa conexão até o momento da desconexão do circuito.
d) estabelecimento do circuito e transferência de informação. No caso da fase de estabelecimento do circuito, uma rota entre as estações é determinada e alocada e, para cada enlace, um canal não dedicado é alocado, permitindo a transferência dos dados até que o usuário abandone a conexão.
e) estabelecimento do circuito, transferência de informação e desconexão do circuito. No caso da fase de estabelecimento do circuito, uma rota entre as estações é determinada e alocada e, para cada enlace, um canal não dedicado é alocado, permitindo a transferência dos dados até o momento da desconexão do circuito ou até que o usuário abandone a conexão.

40- O Modo de Transferência Assíncrono (ATM) é uma tecnologia baseada na transmissão de

a) unidades de informação de tamanho variável e de formato padronizado, denominadas pacotes, sendo seu encaminhamento baseado em informação de um cabeçalho contido apenas no primeiro e no último pacote da conexão.
b) unidades de informação de tamanho variável e de formato padronizado, denominadas pacotes, sendo seu encaminhamento baseado em informação de um cabeçalho contido em cada um deles.
c) pequenas unidades de informação de tamanho fixo e formato padronizado, denominadas células, sendo seu encaminhamento baseado em informação de um cabeçalho contido em cada uma delas.
d) pequenas unidades de informação de tamanho fixo e formato padronizado, denominadas células, sendo seu encaminhamento baseado em informação de um cabeçalho contido apenas no primeiro e no último pacote da conexão.
e) pequenas unidades de informação de tamanho fixo e formato padronizado, denominadas células, sendo seu encaminhamento baseado em informações contidas apenas em um pacote inicial para sincronização e estabelecimento da conexão e, adicionalmente, em um pacote final de encerramento ou fechamento da conexão.

41- Analise as seguintes afirmações relacionadas a protocolos, tipos e meios de transmissão, modos de operação e gerenciamento em redes de computadores:

I. O protocolo *Frame Relay* provê um serviço orientado a conexão através de circuitos que permitem definir velocidades diferentes de transmissão em cada direção.
II. Em uma rede *Frame Relay* o roteador do usuário é responsável por construir os quadros, inserir os identificadores necessários e entregar os quadros para transmissão.
III. No tráfego de pacotes TCP/IP em redes *Frame Relay* os identificadores DLCIs e o roteamento *Frame Relay* são substituídos, no início da transmissão, pelas características TCP/IP que passam a se responsabilizar pelo comportamento da rede.
IV. Em uma rede *Frame Relay* o roteamento dos quadros é de responsabilidade do protocolo IP da família de protocolos TCP/IP.

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- Analise as seguintes afirmações relacionadas a protocolos, tipos e meios de transmissão, modos de operação e gerenciamento em redes de computadores:

I. Uma rede *Frame Relay* provê diversos mecanismos para definição da prioridade de um quadro, resultando, com isso, em uma previsão confiável e constante dos tempos de latência. Isso permite que o *Frame Relay* seja utilizado em redes com aplicações sensíveis a variações dos tempos de latência.

II. O *Frame Relay* implementa mecanismos que notificam a ocorrência de congestionamento em uma rede, embora não se responsabilize pelo controle de fluxo.

III. Quando uma rede *Frame Relay* está congestionada, o bit FECN (*Forward Explicit Congestion Notification*) é ativado. Isso possibilita que o destino saiba que a rede estava congestionada durante a transmissão do quadro.

IV. Em uma rede *Frame Relay* congestionada, um segundo bit BECN (*Backward Explicit Congestion Notification*) é ativado no cabeçalho dos dados que não conseguiram, na primeira tentativa, trafegar no sentido do congestionamento.

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

43- Analise as seguintes afirmações relacionadas a protocolos, tipos e meios de transmissão, modos de operação e gerenciamento em redes de computadores:

I. Em uma rede de computadores, os endereços 255 são usados quando é necessário enviar uma mensagem para mais de um destino simultaneamente. Com esse recurso, denominado *Broadcast*, quando se envia uma mensagem para o endereço 192.168.255.255 ela é entregue a todas as placas na rede 192.168.0.0.

II Quando um *datagrama multicast* é enviado para uma rede, todas as máquinas, independentemente de seu endereço IP, devem receber, tratar e responder, acusando o recebimento e, quando for o caso, o atendimento da solicitação.

III. O protocolo IP usa endereços IP para identificar as placas, enquanto os protocolos MAC usam endereços MAC. Em alguns casos os protocolos ARP (*Address Resolution Protocol*) e RARP (*Reverse Address Resolution Protocol*) são utilizados para traduzir endereços IP em endereços MAC ou vice-versa.

IV. O uso dos protocolos ARP e RARP é necessário quando, em um mesmo segmento de rede, um mesmo endereço IP é utilizado simultaneamente por mais de uma placa de rede ativa. Nesses casos, a identificação correta da máquina na rede é feita com a união dos endereços MAC e IP.

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

44- O DHCP possibilita a distribuição de endereços IP para máquinas na rede. Com relação aos tipos de distribuição possíveis com o uso do DHCP é correto afirmar que

a) na distribuição automática é definido um tempo de validade, possibilitando o reaproveitamento de endereços IP. Nesses casos, os endereços IP são desvinculados dos respectivos endereços MAC.
b) na distribuição manual, um endereço IP é associado de forma estática a um endereço MAC.
c) na distribuição dinâmica, os endereços são distribuídos à medida que novas máquinas são inseridas na rede. Neste caso, os endereços IP são associados de forma estática a endereços MAC, não permitindo o reaproveitamento de endereços IP.
d) para impedir a alta rotatividade dos endereços IP quando se utiliza a distribuição automática, faixas de endereços MAC e IP são especificados no servidor DHCP.
e) para gerenciar a alta rotatividade dos endereços IP quando se utiliza a distribuição dinâmica, faixas de endereços MAC e IP são especificadas e vinculadas manualmente no servidor DHCP.

45- Analise as seguintes afirmações relacionadas a QoS, configuração e gerenciamento de redes de computadores:

I. Os bits usados no endereço IP para o endereço de rede e das sub-redes são identificados por uma máscara de mesmo tamanho de um endereço IP. Em uma máscara, os bits com valor 0 (zero) identificam os bits usados para reconhecer a rede e as sub-redes no endereço IP.

II. Tanto no roteamento estático quanto no roteamento dinâmico, as tabelas de roteamento são atualizadas a partir de informações trocadas entre os roteadores. O ponto que difere as duas tecnologias está na possibilidade de escolha da melhor rota disponível no momento, existente apenas no roteamento dinâmico.

III. A interface *loopback* é um tipo especial que permite fazer conexões com a própria máquina local. Computadores que usam o protocolo TCP/IP utilizam esta interface e, por convenção, o endereço IP 127.0.0.1 é o escolhido especificamente para a *loopback*. Com esse tipo de interface, uma conexão *Telnet*, por exemplo, para 127.0.0.1, abrirá uma conexão para o computador local.

IV. No TCP/IP, cada serviço é associado a um número chamado porta, onde o servidor espera pelas conexões dos computadores clientes. Uma porta de rede pode ser referenciada tanto pelo número como pelo nome do serviço. Algumas portas padrões, como por exemplo, as portas 21, 23, 25, 80 e 110 associadas, respectivamente, ao FTP, Telnet, SMTP, HTTP e POP3 são usadas em serviços TCP/IP.

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

SEGURANÇA DA INFORMAÇÃO

46- Segurança compreende a proteção de informações, sistemas, recursos e serviços contra desastres, erros e manipulação não-autorizada, reduzindo assim, a probabilidade e o impacto de incidentes de segurança. Em termos de Segurança da Informação, é correto afirmar que:

a) são classificadas como informações confidenciais aquelas cujo acesso interno ou externo de pessoas não autorizadas é crítico para a empresa, sendo imprescindível um número restrito de pessoas autorizadas e o controle total sobre o uso das informações.
b) a segurança de acesso físico tem por objetivo proteger informações contra usuários não autorizados, protegendo o acesso aos recursos, de modo explícito ou implícito (áreas de acesso restrito), englobando ainda, a prevenção de dados provocados por desastres naturais.
c) os elementos fundamentais do controle de acesso lógico podem ser visualizados sob dois aspectos distintos: a partir do recurso computacional que se pretende proteger e a partir do usuário a quem se pretende dar certos privilégios e acessos aos recursos. Tais elementos, em essência, podem ser considerados como a identificação e a autenticação de usuários.
d) A envia uma mensagem encriptada com sua chave privada para B (e que B já possui uma cópia da chave pública de A). Ao receber o criptograma, B usa uma cópia da chave pública de A para decriptar a mensagem. Sendo assim, a mensagem encriptadada servirá como assinatura digital, garantindo autenticidade em termos da origem e integridade da mensagem.
e) considerando que A deseja se comunicar com B, uma possibilidade para resolver a distribuição de chaves convencionais a garantir a autenticidade das partes envolvidas é A gerar um par de chaves públicas e transmitir uma cópia de sua chave pública para B que, por sua vez, gera uma chave secreta e a transmite para A, encriptada com a chave pública de A.

47- A respeito da segurança de serviços Internet TCP/IP (*Transmission Control Protocol / Internet Protocol*) é correto afirmar que

a) uma conexão SSL (*Secure Socket Layer*) é uma associação entre um cliente e um servidor, criada pelo *Handshake Protocol* SSL, definindo os parâmetros de criptografia.
b) para controlar o serviço SMTP, usa-se filtragem de pacotes restringindo conexões de *hosts* externos para o *bastion host*, e do *bastion host* para um servidor (ou conjunto destes) específico.
c) POP3 (*Post Office Protocol* 3) é um protocolo cliente/servidor cujo serviço se baseia em UDP, e para o qual é possível fazer *proxy*, uma vez que é um protocolo que opera em duas conexões ao prover seu serviço.
d) a conversão RADIX-64 e o DSS/SHA são algoritmos utilizados no projeto do PGP (*Pretty Good Privacy*) para correio eletrônico, provendo especificamente o serviço de encriptação de mensagens.
e) no ataque de inundação ACK, o servidor é inundado por pacotes TCP ACK, cada um contendo um endereço IP falsificado, caracterizando assim, um ataque de fonte DoS (*Denial of Service*) ao servidor atingido.

48-Portas são identificadores de processos na camada de transporte Internet TCP/IP (*Transmission Control Protocol / Internet Protocol*), isto é, a porta origem identifica o processo que enviou dados e a porta destino identifica o processo que recebe os dados – informações indicadas no cabeçalho de cada segmento TCP e pacote UDP (*User Datagram Protocol*). Sendo assim, em termos das questões relacionadas ao contexto das portas, é incorreto afirmar que

a) regras de filtragem de pacotes são baseadas em campos do cabeçalho IP e de transporte, incluindo endereços IP origem e destino, campo *Protocol* e o número das portas TCP ou UDP.

b) a camada SSL (*Secure Socket Layer*), no lado remetente, recebe os dados, criptografa-os e direciona-os a uma porta TCP e, no lado receptor, a porta TCP é lida, os dados são decriptados e direcionados à aplicação.

c) em uma configuração cujo *bastion host* é também um servidor secundário DNS, deve-se permitir pedidos de transferência de zonas DNS de um *bastion host* ao servidor interno, ou seja, de pacotes TCP com portas acima de 1023 para a porta 53 no servidor interno.

d) portas denominadas bem-conhecidas (*well-known ports*) são atribuídas pelo IANA (*Internet Assigned Numbers Authority*) e usadas por processos que operam em um nível privilegiado do sistema operacional.

e) uma estratégia aplicável ao serviço FTP (*File Transfer Protocol*) é bloquear portas específicas, por *default*, ao invés de bloquear todas as portas e então liberar portas específicas, considerando uma arquitetura de *firewall screened subnet*.

49-Ao passo que as informações são consideradas o principal patrimônio de uma organização, hoje em dia, estas estão sob constante risco, fazendo com que a segurança da informação tenha se tornado crucial para a sobrevivência das organizações. Sendo assim, é correto afirmar que

a) a legislação brasileira possui dispositivos legais relacionados à segurança da informação, tais como o Decreto n. 79.099, de 1997, que se aplica à interceptação do fluxo de comunicação em sistemas de informática e telemática.

b) a definição técnica de ameaça é a conseqüência de uma vulnerabilidade do sistema ter sido explorada.

c) a análise de riscos engloba tanto a análise de ameaças e vulnerabilidades quanto a análise de impactos, a qual identifica os componentes críticos e o custo potencial ao usuário do sistema.

d) a observação e conhecimento de informações armazenadas em sistemas ou a análise do tráfego de uma rede são considerados ataques ativos.

e) a gerência de segurança engloba o gerenciamento de riscos, e estabelece processos de revisão e verificação de registros e atividades, com o intuito de testar a adequação dos controles do sistema, garantindo sua adequação à política de segurança.

50- No que se refere às estratégias para *backup* em ambientes de rede é correto afirmar que

a) geralmente são uma combinação de métodos, desde o *backup* completo, passando por um ou mais níveis de *backup* incrementais, até o *backup* de arquivos dos usuários.

b) em redes Windows, é aconselhável desenvolver e implementar um plano de testes de prevenção de desastres para garantir a integridade de seus dados de *backup*.

c) um plano de prevenção de desastres prepara uma organização para se recuperar de desastres e de faltas de energia que não podem ser evitados.

d) não é prática recomendável para ambientes Windows, efetuar backup do estado do sistema de cada servidor e assegurar que o serviço de diretório Microsoft *Active Directory* esteja incluído em cada controlador de domínio.

e) os *backups* protegem as instituições exclusivamente contra falhas de hardware e software.

51- A respeito dos sistemas de *backup* das organizações é incorreto afirmar que

a) a política de *backup* compreende os procedimentos e a infra-estrutura necessários à proteção de informações com o objetivo de possibilitar a continuidade de suas atividades.

b) é recomendável que cada sistema crítico para uma organização tenha pelo menos duas cópias: uma em local próximo, para recuperação imediata e outra em local distante, para permitir a recuperação em caso de desastres com maiores dimensões.

c) a estratégia de *backup* precisa estar focada em objetivos distintos e que não abrangem os requisitos de negócio e ambiente operacional da empresa.

d) uma arquitetura de *backup* e recuperação deve incluir um plano de prevenção de desastres, procedimentos e ferramentas que ajudem na recuperação de um desastre ou falha de energia, além de procedimentos e padrões para realizar a recuperação.

e) a recuperação dos dados define os procedimentos necessários ao retorno da operação normal dos sistemas. Se esta recuperação não funcionar, o *backup* não terá utilidade.

52-*Firewall* é um componente de soluções para a segurança de redes. Em relação a este componente é correto afirmar que

a) um *host dual-homed* deve ser protegido com cautela porque é vulnerável a ataques, uma vez que está exposto à Internet, além de ser o principal ponto de conexão para os usuários de redes internas.

b) um servidor *proxy*, para um protocolo particular ou conjunto de protocolos, executa sob um *host dual-homed* ou *Bastion host*, tendo como função avaliar e decidir sobre a aceitação dos pedidos enviados por clientes.

c) NAT (*Network Address Translation*) é um recurso que permite que uma rede interna tenha endereços IP (*Internet Protocol*) não roteáveis na Internet. Com NAT é possível conseguir *proxy* transparente, exceto quando o *proxy* está em uma máquina diferente da qual está o *firewall*.

d) a filtragem de pacotes baseada no valor do bit TCP ACK é útil quando a organização quer permitir que usuários externos se conectem a servidores internos e impedir que usuários internos se conectem a servidores externos.

e) são considerados soluções completas de segurança, de tal forma que outros controles e verificações de segurança podem falhar sem causar danos à organização.

53- Em termos da aplicação de *firewall* e da sua atuação em ambientes de rede é incorreto afirmar que

a) o ICF (*Internet Connection Firewall*) da Microsoft é um *firewall stateful* para ambiente Windows capaz de efetuar filtragem de pacotes e permitir tráfego a aplicações ou portas específicas (este último sob condição de exceção). Sob configuração *default*, em redes corporativas, o *firewall* Windows pode causar falhas em aplicações críticas para o negócio – em particular, aquelas que requerem portas TCP ou UDP específicas.

b) *iptables* é um *firewall* para filtragem de pacotes em ambientes LINUX que pode também ser usado para monitorar o tráfego da rede, fazer NAT (*Network Address Translation*), redirecionamento de pacotes, entre outras funcionalidades.

c) sendo o *firewall* o ponto de conexão com a Internet, ele tem como responsabilidades aplicar regras de segurança e manter regras de tráfego para auditoria de acordo com as determinações da política de segurança da organização.

d) no Linux, o *ipchains* gerencia regras, por si só, não necessitando de funções específicas do *kernel* do sistema operacional para efetuar seu trabalho.

e) a DMZ (*De-Militarized Zone*) compreende o segmento (ou segmentos) de rede, parcialmente protegido, que se localiza entre redes protegidas e as desprotegidas.

54- A respeito da detecção de intrusão é incorreto afirmar que

a) a detecção de intrusos baseia-se na suposição de que o comportamento de intrusos difere do comportamento de usuários legítimos.

b) a detecção baseada em regras compreende a definição de um conjunto de regras usadas para decidir a respeito de um dado comportamento.

c) SDIs (Sistemas de Detecção de Intrusos) de rede utilizam fontes de informação tais como auditoria do sistema operacional e *logs* do sistema.

d) ataques de DoS (*Denial of Service*) consistem em sobrecarregar um servidor com uma quantidade excessiva de solicitação e são considerados possíveis de detectar por parte de SDIs.

e) um falso negativo ocorre quando uma ação maléfica é classificada como normal, aumentando as vulnerabilidades.

55- É crescente o número de incidentes de segurança causados por vírus de computador e suas variações. Com isso, as organizações estão enfrentando o problema com o rigor e cuidados merecidos. Nesse contexto, é correto afirmar que

a) cavalos de tróia são variações de vírus que se propagam e possuem um mecanismo de ativação (evento ou data) e uma missão.

b) vírus polimórficos suprimem as mensagens de erro que normalmente aparecem nas tentativas de execução da atividade não-autorizada, utilizando, muitas vezes, criptografia para não serem detectados por anti-vírus.

c) os vírus de macro utilizam arquivos executáveis como hospedeiros, inserindo macros com as mesmas funções de um vírus em tais arquivos.

d) softwares anti-vírus controlam a integridade dos sistemas e compreendem três etapas: prevenção, detecção e reação, nesta ordem.

e) vírus geram cópias de si mesmo a fim de sobrecarregarem um sistema, podendo consumir toda a capacidade do processador, memória ou espaço em disco, eventualmente.

56- Em termos das questões relacionadas à política de segurança e auditoria é correto afirmar que

a) o âmbito da auditoria compreende aspectos tais como o objeto a ser fiscalizado, período e natureza da auditoria, por exemplo, operacional e financeira.

b) a norma NBR ISO IEC 17799 não define regras para a gestão da continuidade do negócio, com a finalidade de evitar interrupções e proteger processos críticos nas organizações.

c) o Decreto n. 3.505, de 13.06.2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal, tem como um de seus pressupostos garantir ao Estado o direito de acesso a qualquer informação que for de seu interesse.

d) a política de segurança deve ser flexível e viável a longo prazo. Todavia, não pode ser definida de modo independente de software e hardware específicos.

e) a auditoria da Segurança da Informação faz parte da auditoria da Tecnologia da Informação e engloba a avaliação da política de segurança, de controles de aspectos de segurança institucional globais (lógico, físico e ambiental) e de planos de contingência e continuidade dos serviços.

57- Em relação à segurança no comércio eletrônico é correto afirmar que

a) ameaças à Web, em termos de integridade, confidencialidade, negação de serviço e autenticação, são exemplos de problemas de segurança que afetam sistemas de comércio eletrônico. Por outro lado, há soluções tais como *firewalls*, sistemas de detecção de intrusos e critptografia que são aplicáveis diretamente a tal contexto de problemas.

b) o SSL (*Secure Socket Layer*) foi projetado para usar UDP (*User Datagram Protocol*), de modo a prover um serviço fim-a-fim confiável e seguro na camada de transporte.

c) o protocolo de registro SSL (*Record Protocol*) é utilizado para negociar e configurar os parâmetros tais como chaves de sessão e algoritmos de criptografia para o estabelecimento da comunicação entre as partes.

d) sendo a segurança na Web crucial para o comércio eletrônico, IPSec (*Internet Protocol Security*) é uma solução complementar para tal, provendo ainda transparência aos usuários finais e aplicações.

e) a obtenção da informação a respeito da configuração da rede é um exemplo de ameaça à integridade na Web, e pode ser solucionada pelo uso de soluções baseadas em criptografia.

58- Em relação às questões que envolvem a segurança na Internet é <u>incorreto</u> afirmar que

a) confidencialidade ou privacidade corresponde a um dos serviços de segurança cujo objetivo é a proteção dos dados transmitidos contra ataques passivos, assim como a proteção do tráfego contra análise.

b) em casos de *spoofing* de endereço IP (*Internet Protocol*), o intruso externo transmite pacotes com o campo de endereço IP origem contendo um endereço de um *host* interno.

c) o ataque DDoS (*Distributed Denial of Service*) é uma variação de ataques DoS. Ambos resultam em perdas ou redução de disponibilidade e são amenizados, em alguns casos, com a utilização de autenticação e criptografia.

d) o software VPN (*Virtual Private Network*) atua como um filtro porque permite que os dados trafeguem apenas entre dispositivos para os quais o software VPN foi configurado, garantindo conexões seguras usando uma infra-estrutura pública de comunicação.

e) na Internet, é aconselhável utilizar soluções baseadas em criptografia com vistas a proporcionar a confidencialidade de dados. Em particular, o SSL (*Secure Socket Layer*) é baseado, em sua completude, na criptografia de chaves assimétricas.

59- Em termos de autenticação de usuários em redes é correto afirmar que

a) na versão 5 do Kerberos, cada *ticket* inclui uma chave de sessão que é usada pelo cliente para encriptar o autenticador enviado ao serviço associado àquele *ticket*, sendo possível a negociação, entre cliente e servidor, de chaves de subsessão a serem usadas na conexão.

b) uma maneira de efetuar a autenticação de usuários é identificá-los no ambiente e associar a cada um, uma senha. A denominada senha *one-time* é um tipo de senha *time-based*, na qual a senha varia a cada minuto, utilizando para tanto, um algoritmo conhecido pelo sistema e pelo dispositivo de autenticação do usuário.

c) Kerberos 5 é especificado na RFC 1510 e requer o uso de algoritmos de criptografia RSA e DES, exclusivamente.

d) X.509 corresponde a um *framework* para prover serviços de autenticação aos usuários, associando, a cada um deles, um certificado de chaves públicas. Tal *framework* é parte do serviço de diretórios X.500 que, por sua vez, é responsável pela criação das chaves públicas e pela certificação.

e) Autoridades certificadoras emitem certificados digitais para autenticação de usuários, vinculando à identidade de um usuário um par de chaves públicas – a chave pública e a chave privada.

60- Em relação às vulnerabilidades de protocolos/aplicações de acesso remotos é correto afirmar que

a) o Telnet é um padrão para acesso a terminais na Internet, que provê segurança por meio da autenticação de usuários, além de manter uma conexão com tráfego criptografado.

b) utilizando ferramentas específicas, é possível explorar a possibilidade de enviar mensagens anônimas a partir do IRC, gerando uma espécie de *spoofing* de mensagens, se o endereço IP e a porta IRC da vítima forem conhecidos.

c) é aconselhável colocar servidores de Terminal (*Terminal Servers*) fora da DMZ (*De-Militarized Zone*) para proteger a rede interna da organização.

d) *Bots* são softwares maliciosos e autônomos que se conectam por meio de um componente ICQ. Normalmente, o software usado para gerenciamento destes canais é modificado de forma que sirvam a mais *bots* e que não revelem a quantidade de *bots* associados.

e) Kerberos e SSH (*Secure Shell*) são soluções para autenticação remota com uso de criptografia, eliminando os problemas de soluções tais como o Telnet.

AUDITORIA DE SISTEMAS

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

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

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.

64- Analise as seguintes afirmações sobre os processos relacionados aos quatro domínios do COBIT.

I. A Avaliação dos riscos e a Gerência da qualidade são definidos no domínio Gerenciamento da Garantia da Qualidade.

II. A definição e manutenção de acordos de níveis de serviços (SLA) e a Gerência dos serviços de terceiros são processos do domínio Aquisição e Implementação.

III. O Desenvolvimento e manutenção dos procedimentos, instalação e certificação de software e gerenciamento de mudanças são processos do domínio Aquisição e Implementação.

IV. O plano estratégico de TI e a arquitetura da informação são definidos no domínio Planejamento e 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

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.

66- Analise as seguintes afirmações relacionadas às responsabilidades da gerência quanto à manipulação e salvaguarda dos ativos da organização do ponto de vista de um processo de Auditoria de Controles de hardware, acesso, suporte técnico e operação de computadores.

I. A gerência é responsável por planejar e executar os *backups* dos servidores de banco de dados da organização.
II. A gerência é responsável por desenvolver os procedimentos de conscientização em todos os níveis da organização.
III. A gerência é responsável por implementar sistemas seguros para atender às políticas de Tecnologia da Informação.
IV. A gerência é responsável por realizar suporte técnico aos usuários do ambiente.

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

67-Os controles de segurança de dados em sistemas de informação estão relacionados principalmente à proteção da informação quanto a destruição, sabotagem, roubo e acidentes. Quanto à propriedade desses controles é correto afirmar que a disponibilidade visa

a) a fornecer um requisito de informação completa, correta e válida.
b) a permitir a rastreabilidade do sistema.
c) ao registro de todas as transações ocorridas no sistema.
d) ao retorno dos dados disponíveis a quem quer que esteja autorizado a usar tais dados.
e) à possibilidade de auditoria dos dados.

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.

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.

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

Escola de Administração Fazendária
www.esaf.fazenda.gov.br