ESAF
Escola de Administração Fazendária

CONTROLADORIA-GERAL DA UNIÃO

Concurso Público 2008

Cargo: ANALISTA DE FINANÇAS E CONTROLE

Prova 3

Área: Tecnologia da informação / Infra-Estrutura de TI

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:

"Onde existe uma mente aberta, sempre haverá uma nova fronteira a desbravar".
(Charles Kettering)

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

5 - Na prova há **60 questões** de múltipla escolha, com cinco opções: a, b, c, d e e.

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

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 - A saída da sala só poderá ocorrer depois de decorrida uma hora do início da prova. A não-observância dessa exigência acarretará a sua exclusão do concurso.

12 - Ao sair da sala entregue este CADERNO DE PROVA, juntamente com o CARTÃO DE RESPOSTAS, ao Fiscal de Sala.

Boa prova!

GESTÃO DE TECNOLOGIA DA INFORMAÇÃO

1 - O COBIT - *Control Objectives for Information and related Technology* fornece boas práticas por meio de uma estrutura de domínio e processos e apresenta atividades de forma gerencial e lógica para a Governança de TI. O COBIT contém componentes interrelacionados, provendo suporte para a governança, gerenciamento, controle e atendimento das necessidades de diferentes organizações. O componente Atividades-Chaves do COBIT (versão 4.1) está relacionado com

a) Indicadores de performance.
b) Modelos de Maturidade.
c) Controle de Objetivos.
d) Responsabilidades e Contabilização.
e) Controle de Práticas.

2 - O nível de maturidade é uma maneira de prever o futuro desempenho de uma organização dentro de cada disciplina ou conjunto de disciplinas. Um nível de maturidade é uma etapa evolucionária definida de melhoria de processos. No modelo CMMI com representação em estágios existem os seguintes níveis:

a) inicial, gerenciado, definido, gerenciado quantitativamente e otimizado.
b) inicial, parcialmente gerenciado, executado, gerenciado qualitativamente e otimizado.
c) inicial, parcialmente gerenciado, definido, gerenciado quantitativamente e otimizado.
d) parcialmente gerenciado, gerenciado, definido, gerenciado quantitativamente e otimizado.
e) inicial, incompleto, executado, gerenciado, definido, gerenciado quantitativamente e otimizado.

3 - No MPS.BR são definidos níveis de maturidade que são uma combinação entre processos e sua capacidade. Os níveis de maturidade estabelecem patamares de evolução de processos, caracterizando estágios de melhoria da implementação de processos na organização. Assinale a opção que identifica todos os níveis de maturidade do MPS.BR.

a) A (Otimizado), B (Gerenciado Quantitativamente), C (Definido),
D (Largamente Definido), E (Parcialmente Definido), F (Gerenciado), G (Inicial).
b) A (Otimizado), B (Parcialmente otimizado),
C (Definido), D (Largamente Definido),
E (Parcialmente Definido), F (Gerenciado),
G (Parcialmente Gerenciado).
c) A (Em Otimização), B (Gerenciado Quantitativamente), C (Definido), D (Largamente Definido), E (Parcialmente Definido), F (Gerenciado),
G (Parcialmente Gerenciado).
d) A (Em otimização), B (Parcialmente Otimizado), C (Definido), D (Largamente Definido),
E (Parcialmente Definido), F (Gerenciado),
G (Inicial).
e) A (Otimizado), B (Executado), C (Definido), D (Largamente Definido), E (Parcialmente Definido), F (Gerenciado), G (Parcialmente Gerenciado).

4 - Os componentes de um modelo CMMI são agrupados em três categorias, que refletem como eles serão interpretados: Exigidos – metas específicas e metas genéricas; Esperados – práticas específicas e práticas genéricas; e Informativos – sub-práticas, produtos de trabalho típicos, definições ampliadas de disciplinas, elaborações de práticas genéricas, títulos e metas práticas, notas de metas e práticas de referências.

Em relação aos componentes do Modelo CMMI, é correto afirmar que

a) as práticas específicas são utilizadas nas avaliações para auxiliar na determinação de que a área de processo está sendo satisfeita.
b) as áreas de processo tratam de características únicas que descrevem o que deve ser implementado para satisfazer o modelo.
c) as metas específicas podem ser componentes opcionais no modelo.
d) as definições ampliadas de disciplinas são descrições detalhadas que fornecem um direcionamento para a interpretação de práticas específicas.
e) todas as áreas de processo do CMMI são as mesmas tanto na representação contínua quanto na representação em estágios.

5 - Um modelo de qualidade define os requisitos que as organizações devem seguir para se capacitarem segundo o mesmo. Entre as opções abaixo, assinale a que se refere exclusivamente a modelos de qualidade de software.

a) CMMI, MPS.BR, COBIT.
b) CMMI, COBIT, ISO9001.
c) CMMI, MPS.BR, ISO9001, COBIT.
d) CMMI, MPS.BR, ISO9000-1.
e) CMMI, ISO12207, ISO15504, ISO20000, ITIL.

6 - Existem diversos modelos CMMI disponíveis, gerados a partir do CMMI Framework. As organizações devem selecionar uma representação, contínua ou em estágios, e determinar as áreas de conhecimento que desejam incluir no modelo que irão utilizar.

Quando uma organização escolhe a representação em estágios do modelo CMMI, espera que o modelo permita

a) selecionar a seqüência de melhorias que mais atendem aos objetivos do negócio.
b) oferecer uma classificação única que resume os resultados de avaliações e realizar comparações entre organizações.
c) reduzir as áreas de riscos da organização.
d) facilidade de comparação de melhoria de processos para a ISO/IEC 15504 - International Organization for Standardization and International Eletrotechnical Commission.
e) oferecer uma migração fácil do Electronic Industries Alleance Interim Standard (EIA/IS) 731 para o CMMI.

7 - No MPS.BR, Guia Geral versão 1.2, para cada um dos níveis de maturidade é atribuído um perfil de processos que indica onde a organização deve colocar o esforço de melhoria. Assinale a opção que representa corretamente todos os processos atribuídos ao nível de maturidade.

a) Nível E – Processos: Gerência de Recursos Humanos - GRH, Definição do Processo Organizacional - DFP, Avaliação e Melhoria do Processo Organizacional - AMP, Gerência de Reutilização - GRU, Gerência de Projetos - GPR(evolução).
b) Nível F – Processos: Garantia da Qualidade - GQA, Gerência de Configuração - GCO, Medição - MED.
c) Nível D – Processos: Gerência de Requisitos - GRE, Desenvolvimento de Requisitos – DRE, Verificação - VER, Validação - VAL, Projeto e Construção do Produto - PCP, Integração do Produto - ITP.
d) Nível D – Processos: Gerência de Recursos Humanos - GRH, Definição do Processo Organizacional - DFP, Avaliação e Melhoria do Processo Organizacional - AMP, Gerência de Reutilização - GRU.
e) Nível E – Processos: Desenvolvimento de Requisitos - DRE, Verificação-VER, Validação - VAL, Projeto e Construção do Produto - PCP, Integração do Produto - ITP.

8 - A ITIL - Information Technology Infrastructure Library é composta por um conjunto das melhores práticas para a definição dos processos necessários ao funcionamento de uma área de TI. Os objetivos da ITIL são:

a) definir os processos a serem implementados na área de TI.
b) fornecer um guia para o planejamento de processos padronizados, funções e atividades para os integrantes da equipe de TI.
c) permitir o máximo alinhamento entre a área de TI e as demais áreas de negócio da organização.
d) tornar-se uma referência para as organizações que necessitam de informações para a melhoria do Gerenciamento de Serviços de TI.
e) aumentar a qualidade e diminuir o custo alocado dos serviços de TI.

9 - Na ITIL, a Central de Serviços (Service Desk) é a principal interface operacional entre a área de TI e os usuários dos seus serviços. Assinale a opção que representa uma tarefa da Central de Serviços.

a) Identificar tendências de problemas.
b) Controlar erros conhecidos.
c) Revisar os principais problemas identificados.
d) Gerenciar o trabalho das diversas equipes de suporte técnico.
e) Produzir informações gerenciais, coletando medidas e calculando indicadores de desempenho.

10- Para que as atividades de Tecnologia da Informação sejam efetivamente governadas, é importante considerar as atividades e riscos da área de TI a serem gerenciadas. As atividades são classificadas em domínios de responsabilidade. No COBIT, estes domínios são denominados

a) Planejar e Organizar; Adquirir e Implementar, Entregar e dar Suporte, Monitorar e Avaliar.
b) Planejar e Organizar; Adquirir e Executar, Entregar e dar Suporte, Monitorar e Medir.
c) Planejar e Organizar; Implementar, Entregar e dar Suporte, Medir e Avaliar.
d) Planejar e Organizar; Adquirir e Desenvolver, Entregar e dar Suporte, Monitorar e Melhorar.
e) Planejar e Organizar; Adquirir e Implementar, Entregar e dar Suporte, Medir e Melhorar.

SISTEMAS DE COMPUTAÇÃO

11- O registrador que especifica o endereço de memória a ser usado pela próxima instrução na unidade central de processamento é o registrador

a) de endereçamento à memória.
b) de instruções.
c) temporário de dados.
d) de endereçamento de entrada/saída.
e) temporário de dados de entrada/saída.

12- São características consideradas específicas de um computador com um conjunto reduzido de instruções ou RISC (*Reduced Instruction Set Computer*).

I . Tamanho de instrução único.
II. Apenas 1 operando endereçado na memória por instrução.
III. Uso de endereçamento indireto.

Assinale a opção verdadeira.

a) Apenas I e II são verdadeiras.
b) Apenas I e III são verdadeiras.
c) Apenas II e III são verdadeiras.
d) I, II e III são verdadeiras.
e) I, II e III são falsas.

13- Na memória de acesso não-aleatório, considerando T o tempo médio de acesso e R a taxa de transferência em bits por segundo, o tempo médio de transferência de N bits é obtido pela expressão

a) T + N x R.
b) T + N/R.
c) T – N x R.
d) T – N/R.
e) T x N x R.

14- A decisão de adicionar um novo processo ao conjunto de processos a serem executados é função do escalonamento

a) de entrada/saída.
b) a curto prazo.
c) a médio prazo.
d) a longo prazo.
e) de entrada/saída a curto prazo.

15- Analise as seguintes afirmações relacionadas a segmentos no sistema de memória virtual e assinale a opção verdadeira.

I. Um segmento é composto por uma seqüência aleatória de endereços, de zero até um valor máximo.
II. O tamanho de um segmento é um valor variável de zero até um valor máximo.
III. Um segmento compreende um espaço de endereçamento separado, com isso, segmentos distintos crescem/diminuem de modo independente.

a) Apenas I e II são verdadeiras.
b) Apenas I e III são verdadeiras.
c) Apenas II e III são verdadeiras.
d) I, II e III são verdadeiras.
e) I, II e III são falsas.

16- Analise as seguintes afirmações, levando em conta as chamadas de sistemas usadas com semáforos, e assinale a opção verdadeira.

I. A chamada de sistema *UP* adiciona uma unidade ao valor corrente de um semáforo.
II. Se o valor do semáforo é zero, uma chamada de sistema *DOWN* não será completada e o processo será suspenso.
III. Quando um processo inicia a execução de uma chamada de sistema *UP* ou *DOWN*, nenhum outro processo terá acesso ao semáforo até que o processo complete a execução ou seja suspenso.

a) Apenas I e II são verdadeiras.
b) Apenas I e III são verdadeiras.
c) Apenas II e III são verdadeiras.
d) I, II e III são verdadeiras.
e) I, II e III são falsas.

17- O diretório no sistema operacional Linux usado para armazenar arquivos temporários de dados tais como filas de impressão é o

a) */urs*
b) */home*
c) */root*
d) */opt*
e) */var*

18- As relações existentes entre processos, no Linux, são visualizadas usando o comando

a) ps.
b) pstree.
c) df.
d) last.
e) tail.

19- O binário do SAMBA que facilita a execução de aplicativos em *hosts* SMB é o

a) *smbclient.*
b) *smbprint.*
c) *smbprint.sysv.*
d) *smbstatus.*
e) *smbrun.*

20- Acesso ao código-fonte é uma premissa para o seguinte tipo de liberdade em programas considerados livres:

a) liberdade de executar o programa.
b) liberdade de alterar o programa.
c) liberdade de redistribuir cópias do programa.
d) liberdade de remover cópias do programa.
e) liberdade de executar cópias do programa.

REDES DE COMPUTADORES

21- O esquema de multiplexação em que cada fonte transmissora obtém acesso ao meio de transmissão por um dado período, no qual cada intervalo de tempo é do mesmo tamanho, é denominado multiplexação

a) por divisão de freqüência.
b) por divisão de comprimento de onda.
c) por divisão de comprimento de onda densa.
d) codificada por pulsos.
e) síncrona por divisão de tempo.

22- Usando a técnica de janela deslizante com o tamanho de 6 pacotes, o tempo gasto para envio é 2T, onde T é o tempo de transmissão em uma direção. Sendo assim, o tempo gasto para o envio de 600s pacotes, considerando T = 2 milissegundos será de

a) 600 milissegundos.
b) 2400 milissegundos.
c) 3600 milissegundos.
d) 7200 milissegundos.
e) 14400 milissegundos.

23- O mapeamento correto entre protocolo e respectiva camada no modelo de referência OSI é o

a) SMTP – camada física.
b) TCP – camada de aplicação.
c) SSL – camada de rede.
d) UDP – camada de enlace.
e) AAL 5 – camada de transporte.

24- O serviço Internet TCP/IP que usa o serviço não-orientado a conexão na camada de transporte é o

a) SMTP
b) HTTP
c) SNMP
d) FTP
e) HTTPs

25- Considerando a necessidade de endereçar 7 sub-redes na rede cujo IP (*Internet Protocol*) é 199.10.0.0, a máscara aplicável é

a) 199.10.0.0/24
b) 199.10.0.0/25
c) 199.10.0.0/26
d) 199.10.0.0/27
e) 199.10.0.0/32

26- Considerando a política de geração de ACKs do TCP (*Transmission Control Protocol*), em um dado *host* destino, a chegada de um segmento na ordem e com o número de seqüência esperado, seguida de um outro segmento na ordem esperando por transmissão de ACK, resulta em

a) envio imediato de um ACK duplicado.
b) envio imediato de um ACK.
c) envio imediato de um único ACK cumulativo.
d) retardo de 100 milissegundos para envio de um ACK.
e) retardo de 500 milissegundos para envio de um ACK.

27- O equipamento de interconexão caracterizado por formar redes restritas a uma árvore de cobertura (*spanning tree*) e por necessitar da geração e processamento considerável de tráfego do protocolo de resolução de endereços ou ARP (*Address Resolution Protocol*) é o

a) repetidor.
b) concentrador.
c) comutador.
d) roteador.
e) agente de gerência SNMP.

28- Na modalidade de comutação por memória, em um roteador cuja largura de banda da memória é de N pacotes por segundo para escritas ou leituras, a velocidade total de repasse de pacotes a portas de entrada para portas de saída deve ser menor que

a) 2N
b) N/2
c) 2N - 2
d) 2N + 2
e) N/2 + 2

29- O comando LINUX para inicializar o serviço de nomes ou DNS (*Domain Name Service*) é o

a) *named*
b) *dns*
c) *bind*
d) *resolv*
e) *search*

30- São exemplos de campos opção aceitos no arquivo de configuração */etc/dhcpd.conf* do protocolo de configuração de host dinâmica ou DHCP (*Dynamic Host Configuration Protocol*), exceto

a) *subnet-mask*
b) *broadcast-address*
c) *routers*
d) *domain-name*
e) *range*

31- Em termos da estrutura de gerenciamento de redes, o componente que possibilita um gerente investigar os estados dos dispositivos gerenciados é

a) a base de informação de gerência ou MIB.
b) o objeto gerenciado.
c) o agente de gerenciamento de rede.
d) o protocolo de gerenciamento de rede.
e) a estrutura de informação de gerenciamento ou SMI.

32- O tipo de dado da estrutura de informações de gerenciamento ou SMI (*Structure of Management Information*) do padrão Internet TCP/IP de gerenciamento, que define uma cadeia de bytes no formato ASN.1 (*Abstract Syntax Notation One*) para a representação de dados binários ou texto de até 65.535 bytes, é o

a) *INTEGER*
b) *OCTET STRING*
c) *Counter32*
d) *Counter64*
e) *TimeTicks*

33- A unidade de dados do protocolo ou PDU (*Protocol Data Unit*) da versão 2 do SNMP que informa a um gerente remoto os valores da base de informação de gerência ou MIB (*Management Information Base*) que são remotos ao seu acesso é denominada

a) *InformationRequest*
b) *SetRequest*
c) *GetRequest*
d) *GetNextRequest*
e) *GetBulkRequest*

34- Considerando a arquitetura de redes ATM (*Asynchronous Transfer Mode*), a camada que possui funções similares às da camada de transporte Internet TCP/IP, permitindo a comunicação entre sistemas finais, é a camada

a) física ATM.
b) ATM.
c) de adaptação ATM.
d) de sessão ATM.
e) de aplicação ATM.

35- A localização correta de um cabeçalho de comutação de rótulos multi-protocolo ou MPLS (*Multi Protocol Label Switching*) em um quadro da camada de enlace é

a) entre o cabeçalho da camada de enlace e o cabeçalho da camada de rede.
b) antes do cabeçalho da camada de enlace.
c) antes dos dados da camada de enlace.
d) após o cabeçalho da camada de rede.
e) ao final dos dados da camada de enlace.

36- Cada participante de uma sessão do protocolo de transporte em tempo real ou RTP (*Real Time Transport Protocol*) usa um número fixo de endereços de transporte, em uma comunicação *unicast*, sendo distribuídos da seguinte forma:

a) 2 para o fluxo RTP.
b) 1 para o fluxo RTP e 1 para mensagens do protocolo de controle em tempo real ou RTCP (*Real Time Control Protocol*).
c) 1 para o fluxo RTP e 2 para mensagens RTCP (*Real Time Control Protocol*).
d) 2 para o fluxo RTP e 1 para mensagens RTCP (*Real Time Control Protocol*).
e) 2 para fluxos de mensagens RTCP (*Real Time Control Protocol*).

37- Analise as seguintes afirmações a respeito do protocolo de inicialização de sessão ou SIP (*Session Initiation Protocol*) e assinale a opção correta.

I. O SIP utiliza o protocolo simples de controle de conferência ou SCCP (*Simple Conference Control Protocol*) para efetuar o controle de servidores de dados de tempo real.
II. Uma resposta 301 de um servidor de redirecionamento a uma requisição *Invite* de um cliente indica que a URL SIP não pode mais ser contactada em tal localização.
III. As requisições e respostas SIP são autenticadas por meio de assinatura digital, utilizando o campo *Authorization* do cabeçalho SIP.

a) Apenas as afirmações I e II são verdadeiras.
b) Apenas as afirmações I e III são verdadeiras.
c) Apenas as afirmações II e III são verdadeiras.
d) As afirmações I, II e III são verdadeiras.
e) As afirmações I, II e III são falsas.

38- O comando do protocolo controlador de *gateways* de mídia ou MGCP (*Media Gateway Controller Protocol*), usado para que um *gateway* de mídia envie de volta eventos que foram requisitados por um controlador de *gateway* de mídia, é o

a) Modify Connection
b) Notification Request
c) Create Connection
d) Notification
e) Delete Connection

39- No padrão IEEE 802.11b, os pontos de acesso ou APs (*Access Points*) enviam quadros de sinalização para

a) informar seu identificador de conjunto de serviços ou SSID (*Service Set Identifier*) e o seu endereço MAC.
b) efetuar a varredura dos 11 canais de freqüência.
c) negociar com as estações sem fio o protocolo de associação a ser usado na comunicação.
d) enviar uma mensagem de descoberta DHCP (*Dynamic Host Configuration Protocol*) às estações sem fio.
e) efetuar a autenticação das estações sem fio.

40- O mecanismo de segurança para redes sem fio IEEE 802.1i que define os formatos de mensagens fim-a-fim utilizadas nas interações entre clientes e servidor de autenticação é denominado

a) protocolo de aplicação sem fio ou WAP (*Wireless Application Protocol*).
b) privacidade equivalente sem fio ou WEP (*Wired Equivalent Privacy*).
c) vetor de inicialização.
d) protocolo extensível de autenticação ou EAP (*Extensible Authentication Protocol*).
e) WAP2.

SEGURANÇA DA INFORMAÇÃO

41- Considerando uma comunicação segura entre os usuários A e B, garantir confidencialidade indica que

a) cada usuário deve confirmar a identidade da outra parte envolvida na comunicação.
b) apenas A e B podem modificar, intencionalmente ou não, o conteúdo da comunicação.
c) apenas A e B devem compreender o conteúdo da comunicação.
d) cada usuário deve provar que uma dada mensagem foi enviada pela outra parte envolvida na comunicação.
e) os recursos necessários à comunicação devem estar disponíveis e acessíveis aos usuários.

42- Um mecanismo de segurança considerado adequado para garantir controle de acesso é

a) o *firewall*.
b) a criptografia.
c) a função de *hash*.
d) a assinatura digital.
e) o certificado digital.

43- Um plano de contingência não compreende

a) respostas imediatas a desastres.
b) identificação e compreensão do problema (desastre).
c) processo de restauração.
d) contenção de danos e a eliminação das causas.
e) análise crítica dos direitos de acesso dos usuários.

44- Segundo a Norma ABNT NBR ISO/IEC 17799: 2005, é correto considerar a seguinte recomendação a fim de garantir uma adequada segurança em Recursos Humanos:

a) documentar procedimentos operacionais.
b) monitorar e analisar criticamente os serviços terceirizados.
c) analisar criticamente os registros (*logs*) de falhas.
d) autenticar adequadamente os usuários em conexões externas.
e) estabelecer um processo formal disciplinar para funcionários em casos de violação da segurança da informação.

45- Considerando uma adequada gestão de riscos para a segurança da informação, analise as afirmações a seguir e assinale a opção correta.

I. É recomendável estabelecer regras para o uso aceitável de ativos associados aos recursos de processamento da informação.
II. É recomendável efetuar, criticamente, a análise de riscos de segurança, uma vez que esta considera ameaças, vulnerabilidades e impactos em função dos negócios da organização.
III. É recomendável estabelecer responsabilidades e procedimentos de gestão para assegurar respostas rápidas e efetivas a incidentes de segurança.

a) Apenas I e II são verdadeiras.
b) Apenas II e III são verdadeiras.
c) Apenas I e III são verdadeiras.
d) I, II e III são verdadeiras.
e) I, II e III são falsas.

46- De acordo com a ISO/IEC 17799:2005, a fim de evitar a interrupção de serviços e das atividades do negócio e proteger os processos críticos de desastres, em tempo hábil, recomenda-se implantar

a) acordo de termos e condições de contratação de funcionários.
b) política de uso de controles criptográficos.
c) plano de continuidade do negócio.
d) acordo de confidencialidade.
e) política para a troca de informações com partes externas.

47- A respeito do documento da Política de Segurança da Informação de uma dada Organização, é <u>incorreto</u> afirmar que

a) deve ser aprovado pela direção antes de ser publicado e divulgado.
b) deve ser analisado regularmente ou na ocorrência de mudanças significativas.
c) gestores devem garantir que os procedimentos de segurança são executados em conformidade com tal documento.
d) deve incluir informações quanto à tecnologia a ser empregada para a segurança da informação.
e) no caso de mudanças, deve-se assegurar a sua contínua pertinência e adequação.

48- Analise as seguintes afirmações em relação à auditoria de segurança da informação e assinale a opção correta.

I. Registros (*logs*) de auditoria devem ser mantidos por um período de tempo adequado para futuras investigações.
II. Para fins de auditoria, é necessário que os relógios dos sistemas de processamento da informação estejam sincronizados de acordo com uma hora oficial.
III. Registros de falhas são aqueles que mantêm as atividades dos administradores e operadores dos sistemas de processamento da informação.

a) Apenas I e II são verdadeiras.
b) Apenas II e III são verdadeiras.
c) Apenas I e III são verdadeiras.
d) I, II e III são verdadeiras.
e) I, II e III são falsas.

49- Analise as seguintes afirmações a respeito de cópias de segurança (*backups)* e assinale a opção correta.

I. Em uma política de *backup*, deve-se declarar a abordagem empregada (completa ou incremental) e periodicidade das cópias, assim como os recursos, infra-estrutura e demais procedimentos necessários.
II. Registrar o conteúdo e data de atualização, cuidar do local de armazenamento de cópias e manter cópias remotas como medida preventiva são recomendados para a continuidade dos negócios.
III. Políticas de *backup* devem ser testadas regularmente para garantir respostas adequadas a incidentes.

a) Apenas I e II são verdadeiras.
b) Apenas II e III são verdadeiras.
c) Apenas I e III são verdadeiras.
d) I, II e III são verdadeiras.
e) I, II e III são falsas.

50- Assinale a opção que <u>não</u> compreende uma informação relevante a decisões em filtragem de pacotes.

a) Porta UDP (*User Datagram Protocol*) destino.
b) Tipo de mensagem ICMP (*Internet Control Message Protocol*).
c) Endereço IP do *gateway* de aplicação.
d) Datagramas de inicialização de conexão usando bits TCP SYN.
e) Linha de requisição de uma mensagem de pedido HTTP (*HyperText Transfer Protocol*).

51- A informação de que um dado *host* respondeu a um datagrama ICMP (*Internet Control Message Protocol*) de eco, com endereço correto no nível IP (*Internet Protocol*), porém com o endereço MAC (*Media Access Control*) incorreto, é útil para

a) varredura de portas.
b) analisador de pacotes (*sniffers*).
c) falsificação de IP.
d) negação de serviço.
e) inundação TCP (*Transmission Control Protocol*) SYN.

52- Considere uma Organização que deseja disponibilizar o serviço FTP (*File Transfer Protocol*) a um conjunto restrito de usuários internos, de modo que estes sejam autenticados antes de iniciarem as sessões FTP. Neste contexto, é correto aplicar

a) *gateway* de aplicação FTP.
b) sistema de detecção de intrusos.
c) filtragem de pacotes.
d) criptografia assimétrica.
e) serviço NAT (*Network Address Translation*).

53- Uma máquina isolada devido a um ataque DNS (*Domain Name System*) representa

a) ação de *spywares*.
b) negação de serviço.
c) varredura de portas.
d) ação de um vírus.
e) falsificação DNS.

54- Assinale a opção que constitui um mecanismo de segurança para redes de computadores.

a) Redes privadas virtuais ou VPN (*Virtual Private Networks*).
b) *Adwares*.
c) *Keyloggers*.
d) *Trapdoors*.
e) Inundação (*flooding*).

55- Ao considerar a camada de soquete segura ou SSL (*Secure Socket Layer*), o responsável por negociar os algoritmos e chaves de criptografia a serem aplicados na comunicação é o protocolo de

a) registro (*Record Protocol*).
b) mudança de especificação de cifra (*Change Cipher Spec Protocol*).
c) negociação (*Handshake Protocol*).
d) alerta (*Alert Protocol*).
e) controle de transmissão (*Transmission Control Protocol*).

56- A respeito de software PGP (*Pretty Good Privacy*), para fins de segurança em correio eletrônico, é correto afirmar que

a) não utiliza o algoritmo SHA-1 (*Secure Hash Algorithm*) para o processamento de resumo de mensagem.
b) a compressão ZIP é aplicada após a assinatura e antes da encriptação de mensagens.
c) para compatibilidade de *e-mails*, usa-se o *Radix*-64, que mapeia cada grupo de 4 octetos para 3 caracteres ASC II.
d) a autenticação baseia-se nos algoritmos CAST-128 e RSA.
e) a confidencialidade de mensagens baseia-se, exclusivamente, em criptografia assimétrica.

57- A operação completa do protocolo de registro SSL para uma mensagem a ser transmitida é representada pela seqüência:

a) fragmentação – compressão – adição de MAC (*Message Authentication Code*) – encriptação – anexação de cabeçalho de registro SSL.
b) fragmentação – adição de MAC – compressão – encriptação – anexação de cabeçalho de registro SSL.
c) compressão – fragmentação – adição de MAC – encriptação – anexação de cabeçalho de registro SSL.
d) compressão – fragmentação – adição de MAC – anexação de cabeçalho de registro SSL – encriptação.
e) fragmentação – compressão – adição de MAC – anexação de cabeçalho de registro SSL – encriptação.

58- Considerando que N usuários utilizam criptografia assimétrica, o número total de chaves é

a) N
b) 2N
c) 1
d) 2N + 1
e) N +1

59- Em assinaturas digitais, a chave criptográfica usada para a verificação da autenticidade de um dado emissor por um receptor é a chave

a) privada do emissor.
b) pública do emissor.
c) pública do receptor.
d) privada do receptor.
e) simétrica compartilhada entre emissor e receptor.

60- Assinale a opção que <u>não</u> contempla um campo existente nos certificados digitais baseados na recomendação X.509.

a) Versão.
b) Número de série.
c) Período de validade.
d) Soma de verificação.
e) Chave pública do sujeito.