ESAF

Escola de Administração Fazendária

Missão: *Desenvolver pessoas para o aperfeiçoamento da gestão das finanças públicas e a promoção da cidadania.*

GOVERNO FEDERAL BRASIL PAÍS RICO É PAÍS SEM POBREZA

Controladoria-Geral da União-CGU

Concurso Público: AFC/CGU-2012
(Edital ESAF n. 07, de 16/4/2012)

Cargo:

Analista de Finanças e Controle

Área:

Tecnologia da Informação / Infraestrutura de TI

Prova 3

Conhecimentos Especializados

Instruções

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

Nome: _____ N. de Inscrição: _____

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:

   "Inspiração vem dos outros. Motivação vem de dentro de nós."
4. **DURAÇÃO DA PROVA: 3 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) fabricada em material transparente, 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 30 (trinta) minutos que antecederem o término da prova, poderão ser copiados os seus assinalamentos feitos no CARTÃO DE RESPOSTAS, conforme subitem 9.2.7 do edital regulador do concurso.
11. A saída da sala só poderá ocorrer depois de decorrida 1 (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.

GESTÃO DE TECNOLOGIA DA INFORMAÇÃO

1 - Segundo o *Cobit 4.1*, as áreas de foco na Governança de TI são:

a) Gestão de Recursos, Entrega de Valor, Mensuração de Desempenho, Alinhamento Estratégico e Gestão de Riscos.
b) Alinhamento Estratégico, Planejamento de TI, Gestão de Infraestrutura, Entrega de Valor e Gestão de Riscos.
c) Alinhamento Estratégico, Gestão de Recursos, Entrega e Suporte, Segurança da Informação e Gestão de Riscos.
d) Gestão do Desenvolvimento de Sistemas, Entrega de Valor, Mensuração de Desempenho, Alinhamento Estratégico e Gestão de Riscos.
e) Gestão Estratégica, Gestão Operacional da TI, Entrega de Valor, Mensuração de Desempenho e Gestão de Riscos.

2 - Qual é a principal atribuição do domínio **Entregar e Suportar** do *Cobit 4.1*?

a) Desenvolver as soluções e as tornar passíveis de uso pelos clientes.
b) Monitorar o desempenho das soluções e as tornar passíveis de uso pelos usuários finais.
c) Receber as soluções e as tornar passíveis de uso pelos usuários finais.
d) Homologar as soluções e as tornar passíveis de teste pelos clientes.
e) Adquirir as soluções e as tornar passíveis de homologação pelos clientes.

3 - No *Cobit 4.1*, são considerados recursos de TI:

a) Sistemas, Informações, Rede e Servidores críticos.
b) Aplicativos, Sistemas de Informação, Rede e Estações de Trabalho.
c) Sistemas, Bancos de Dados, Infraestrutura e Pessoas.
d) Aplicativos, Informações confidenciais, Rede e Estações de Trabalho.
e) Aplicativos, Informações, Infraestrutura e Pessoas.

4 - Um dos Critérios de Informação do *Cobit 4.1* é a integridade, que se relaciona com:

a) a confidencialidade e privacidade da informação bem como sua confiabilidade operacional.
b) a conformidade e estabilidade da informação bem como sua integridade de acordo com os requisitos de negócio.
c) a eficiência e eficácia da entrega da informação bem como sua conformidade de acordo com os parâmetros estabelecidos.
d) a fidedignidade e totalidade da informação bem como sua validade de acordo com os valores de negócios e expectativas.
e) a segurança e totalidade da informação bem como sua estabilidade operacional de acordo com os valores de níveis de serviço acordados.

5 - No *Cobit 4.1*, os níveis de maturidade de um processo podem ser:

a) (0) Vazio, (1) Principiante, (2) Repetível, (3) Integrado, (4) Gerenciado, (5) Otimizado.
b) (1) Inicial, (2) Repetível, (3) Definido, (4) Gerenciado, (5) Classe Mundial.
c) (1) Inicial, (2) Repetível, (3) Integrado, (4) Gerenciado, (5) Perfectivo.
d) (0) inexistente, (1) Inicial, (2) Repetível, (3) Definido, (4) Gerenciado, (5) Otimizado.
e) (1) Indefinido, (2) Padronizado, (3) Definido, (4) Medido, (5) Otimizado.

6 - No Planejamento da Contratação de Soluções de TI, em que momento deverá ser realizado o processo Estratégia de Contratação?

a) Após a produção da Análise de Riscos.
b) Após a produção da Análise de Riscos e do Termo de Referência.
c) Após a produção do Plano de Sustentação e do Termo de Referência.
d) Após a produção da Análise da Viabilidade e da Análise de Riscos.
e) Após a produção da Análise da Viabilidade e do Plano de Sustentação.

7 - São atores da fase de Seleção do Fornecedor de Soluções TI:

a) Contratada, Área Administrativa, Área de Licitações, Área de Tecnologia da Informação.
b) Área Requisitante da Solução, Área Administrativa, Área de Licitações.
c) Equipe de Planejamento da Contratação, Área de Licitações.
d) Área Administrativa, Área de Licitações, Área de Tecnologia da Informação.
e) Integrante Administrativo, Área de Licitações, Área de Tecnologia da Informação.

8 - São processos da fase de Gerenciamento do Contrato:

a) Encerramento do Contrato, Demandar Ordem de Serviço.
b) Assinatura do Contrato, Alteração Contratual.
c) Iniciação, Transição Contratual.
d) Encaminhar Ordem de Serviço, Publicação do Contrato.
e) Iniciação, Assinatura do Contrato.

9 - São processos da publicação Estratégia de Serviços da *ITIL V3*:

a) Gerenciamento da Capacidade, Gerenciamento de Portfólio de Serviços, Gerenciamento de Fornecedor.
b) Gerenciamento de Problema, Gerenciamento do Catálogo de Serviços, Gerenciamento da Demanda.
c) Gerenciamento de Eventos, Gerenciamento do Catálogo de Serviços, Gerenciamento de Fornecedor.
d) Gerenciamento Financeiro de TI, Gerenciamento de Portfólio de Serviços, Gerenciamento da Demanda.
e) Gerenciamento Financeiro de TI, Gerenciamento de Portfólio de Serviços, Gerenciamento de Fornecedor.

10- Na publicação Operação de Serviço, o processo Cumprimento de Requisição tem como objetivo

a) tratar requisições dos usuários que não foram geradas por um incidente, mas que foram originadas a partir de uma solicitação de serviço ou de uma simples solicitação de informação.
b) tratar requisições dos usuários geradas por um incidente ou que foram originadas a partir de uma solicitação de serviço ou de uma simples solicitação de informação.
c) tratar requisições dos usuários que tenham impacto na disponibilidade e na continuidade do serviço, e que foram originadas a partir de uma solicitação de serviço ou de uma simples solicitação de informação.
d) tratar toda e qualquer requisição de usuário, em especial as relacionadas a problemas que impactam o negócio.
e) tratar apenas as requisições dos usuários que não foram geradas por um incidente e que tenham relação com os requisitos de negócio especificados.

11- São funções da Operação de Serviço:

a) Central de Serviço, Gerenciamento Tático e Operacional, Gerenciamento das Operações de TI, Gerenciamento de Sistemas de Negócio.
b) Central de Serviço, Gerenciamento Técnico, Gerenciamento das Operações de TI, Gerenciamento de Aplicativo.
c) Gerenciamento Técnico-administrativo, Gerenciamento dos processos da TI, Gerenciamento de Sistemas Operacionais.
d) Central de Serviços ao Cliente Comercial, Gerenciamento Técnico-administrativo, Gerenciamento das Operações Básicas de TI, Gerenciamento de Aplicativo.
e) Gerenciamento Técnico, Gerenciamento das Operações Críticas de TI, Gerenciamento de Sistemas de Negócio.

12- São processos da Transição de Serviço:

a) Gerenciamento de Mudança, Gerenciamento de Problema, Avaliação.
b) Gerenciamento da Configuração e de Ativo de Serviço, Gerenciamento do Conhecimento, Avaliação.
c) Gerenciamento da Configuração e de Ativo de Serviço, Gerenciamento de Incidente, Gerenciamento de Mudança.
d) Gerenciamento da Demanda, Gerenciamento do Conhecimento, Validação e Teste de Serviço.
e) Gerenciamento da Configuração, Gerenciamento do Conhecimento, Central de Serviço.

13- São Áreas de Conhecimento do *PMBOK*:

a) Gerenciamento dos Custos do Projeto, Gerenciamento do Tempo do Projeto, Gerenciamento da Iniciação do Projeto.
b) Gerenciamento dos Custos do Projeto, Gerenciamento do Tempo do Projeto, Gerenciamento de Aquisições do Projeto.
c) Gerenciamento do Planejamento do Projeto, Gerenciamento do Tempo do Projeto, Gerenciamento de Aquisições do Projeto.
d) Gerenciamento dos Custos do Projeto, Gerenciamento das Contratações de Serviços de TI do Projeto, Gerenciamento de Aquisições do Projeto.
e) Gerenciamento do Controle do Projeto, Gerenciamento do Tempo do Projeto, Gerenciamento de Aquisições do Projeto.

14- No *PMBOK* o processo que agrega os custos estimados de atividades individuais ou pacotes de trabalho para estabelecer uma linha de base dos custos é o de:

a) Estimativa de Custos.
b) Planejamento da Qualidade.
c) Desenvolvimento do Cronograma.
d) Estimativa de Investimento e Custeio.
e) Orçamentação.

15- São processos do Grupo de Processos de Iniciação do *PMBOK*:

a) Desenvolver o termo de abertura do projeto, Planejar o escopo do projeto.
b) Definir o escopo do projeto, Desenvolver a declaração do escopo preliminar do projeto.
c) Desenvolver o termo de abertura do projeto, Desenvolver a declaração do escopo preliminar do projeto.
d) Planejar o escopo do projeto, Criar EAP.
e) Criar EAP, Desenvolver o termo de abertura do projeto.

SISTEMAS DE COMPUTAÇÃO

16- São registradores utilizados em operações com a memória principal

a) *MATR (memory address transfer register). MRR (memory retrieve register).*
b) *MAR (memory address register). MBR (memory buffer register).*
c) *MAR (memory actual record). MBBR (memory buffer branch register).*
d) *MRA (memory register assign). MBAR (memory buffer access register).*
e) *MAR (memory adjust register). MVLR (memory virtual linkage register).*

17- O código executável de um processador CISC

a) é interpretado por microprogramas durante sua compilação, gerando microinstruções, que são interpretadas pelo *hardware*.
b) é armazenado durante sua interpretação, gerando comandos na linguagem fonte, que são executados pelo *hardware*.
c) é interpretado por microprogramas anteriormente à sua execução, gerando instruções compiláveis, que são executadas pelo *software* de execução.
d) é interpretado por microprogramas durante sua execução, gerando microinstruções, que são executadas pelo *hardware*.
e) gera microprogramas após sua execução, decorrentes de peculiaridades operacionais do *hardware*.

18- É vantagem da arquitetura de camadas:

a) vincular as funções do sistema operacional a diferentes níveis de pontos de acesso.
b) isolar as funções do sistema operacional e criar uma hierarquia de níveis de modos de acesso.
c) isolar os meios de armazenamento do sistema operacional e criar uma hierarquia de níveis de modos de compartilhamento.
d) isolar as funções da hierarquia dos modos de compilação e hierarquizar as funções do sistema operacional.
e) isolar as camadas do sistema operacional pertinentes a determinados níveis de modos de verificação.

19- No *Linux*, são categorias em que se enquadram informações contidas na tabela de processos:

a) Parâmetros de estratificação. Camadas de memória. Sinais. Registradores de conteúdo. Estado da espera de sistema.
b) Critérios de escalonamento. Imagem de memória. Registradores de acesso. Registradores de máquina. Versão de sistema.
c) Parâmetros de escalonamento. Imagem de execução. Sinais. Registradores de máquina. Estrutura da chamada de sistema.
d) Parâmetros de direcionamento. Imagem de memória. *Devices*. Registradores de máquina. Estado da chamada do programa.
e) Parâmetros de escalonamento. Imagem de memória. Sinais. Registradores de máquina. Estado da chamada de sistema.

20- Um projeto de banco de dados está na *BCNF*

a) se cada membro do conjunto de esquemas de relação que constituem o projeto estiver na *BCNF*.
b) se todos os membros do conjunto de esquemas de herança que decorrem do projeto estiverem na *BCNF*.
c) se cada membro do conjunto de estruturas de atributos que decorrem dos programas estiver na *BCNF*.
d) se cada relação do conjunto de esquemas de classes que constituem o fluxo de atividades estiver na *BCNF*.
e) se pelo menos um membro do conjunto de estruturas de relação que inicializam o projeto estiver na *BCNF*.

21- O *Hypervisor*, ou Monitor de Máquina Virtual (*Virtual Machine Monitor – VMM*), é uma camada de *software* entre

a) o sistema operacional e a máquina virtual.
b) o sistema operacional e o aplicativo.
c) o *hardware* e o sistema operacional.
d) o aplicativo e o *hardware*.
e) o *hardware* e a máquina virtual.

22- A Virtualização pode ser classificada em três tipos na arquitetura x86:

a) Virtualização total, Paravirtualização, Virtualização assistida pelo *hardware*.
b) Virtualização abrangente, Metavirtualização, Virtualização assistida pelo *software*.
c) Virtualização assistida pelo sistema operacional, Metavirtualização, Virtualização assistida pelo *hardware*.
d) Virtualização total, hipervirtualização, Virtualização de translação binária.
e) Virtualização assistida pelo sistema operacional, hipervirtualização, Virtualização assistida pela máquina virtual.

23- A solução de Virtualização da *VMware* é baseada nos *hypervisors ESX* e *ESXi*, que são considerados *hypervisors* do tipo:

a) *Vstorage.*
b) De borda.
c) *Double.*
d) *Baremetal.*
e) *Double sphere*.

24- A distribuição de dados sobre vários discos é chamada de:

a) *Slicing*.
b) *Stretching*.
c) *Striping*.
d) *Scattering*.
e) *Index distributing*.

25- Para prosseguir com a operação normal, o uso do *RAID* pressupõe:

a) Instalar um único disco nas proximidades do computador. Substituir a placa controladora de disco por um controlador *UNIVERSAL*. Mesclar os dados do *RAID*. Controlar a operação.
b) Instalar uma caixa de discos dentro do computador. Manter ativa a placa controladora de disco existente. Copiar os programas para o *RAID*. Executar programas *RAID*.
c) Instalar um dispositivo virtual de armazenagem (*VSD*) nas proximidades do computador. Substituir o interpretador existente por um compilador *RAID*. Copiar os programas tipo *RAID* para o *VSD*. Controlar a operação.
d) Deslocar as unidades de disco existentes para uma unidade externa. Substituir a placa hospedeira de memória por um controlador *RAID*. Retirar os dados incompatíveis com o *RAID*. Depurar as inconsistências.
e) Instalar uma caixa cheia de discos nas proximidades do computador. Substituir a placa controladora de disco por um controlador *RAID*. Copiar os dados para o *RAID*. Prosseguir com a operação normal.

26- O *Active Directory*

a) depende do *DNS* para desencadear geração de nomes *string*.
b) depende do *DPS* para agir como serviço de verificação de nomes e também como serviço de compartilhamento.
c) depende do *DNS* para agir como serviço de resolução de nomes e também como serviço de localização.
d) independe do *DNS* para agir como serviço de resolução de nomes e também como parâmetro de localização *LOC*.
e) é um serviço de diretório que não comporta objetos.

27- Os servidores *DNS (Domain Name System)* contêm

a) o banco de dados do *DNS* com o mapeamento entre os domínios de acesso e o respectivo número *APS*.
b) o banco de dados do *DNS* com o mapeamento entre os nomes *DNS* e o respectivo número *IP*.
c) os programas do *DNS* com a transformação dos nomes *DNS* em números no padrão *IP-S.*
d) o banco de operações do *DNS* com o mapeamento entre os usuários *DNS* e os mecanismos de suporte *Active Device*.
e) o banco de dados do *DNS* com as relações entre *plug-ins DNS* e o respectivo meio de acesso *IP*.

28- Na arquitetura e-PING, o padrão para notação de modelagem de processos é:

a) *BPM 1.7*, conforme definido pelo *BPO*.
b) *NOT 2.0*, conforme definido pelo *BPMM*.
c) *NOTP 2.0*, conforme definido pelo *OBP*.
d) *BPXML 1.2*, conforme definido pelo *BPO*.
e) *BPMN 1.0*, conforme definido pelo *OMG*.

29- A arquitetura e-PING – Padrões de Interoperabilidade de Governo Eletrônico – define um conjunto mínimo de premissas, políticas e especificações técnicas que regulamentam a utilização da Tecnologia de Informação e Comunicação (TIC) na interoperabilidade de serviços de Governo Eletrônico, estabelecendo as condições de interação com os demais Poderes e esferas de governo e com a sociedade em geral. As áreas cobertas pela e-PING estão segmentadas em:

a) Redes *WAN* e *LAN*, Tecnologia da Informação, Controle de Acesso, Intercâmbio de Informações, Áreas de Governo Eletrônico.
b) Conexão Banda Larga, Segurança física, Mecanismos de Acesso à informação, Armazenamento de Informações, Áreas de Integração para Governo Eletrônico.
c) Telecomunicações, Padronização, Mecanismos de Acesso ao e-Gov, Proteção à informação, Áreas de Integração para Governo Eletrônico.
d) Interconexão, Segurança, Meios de Acesso, Organização e Intercâmbio de Informações, Áreas de Integração para Governo Eletrônico.
e) Redes sem-fio, Padronização, Meios de Acesso Web, Organização de Informações em Bancos de Dados, Coordenação para Governo Eletrônico.

30- A análise dos padrões candidatos a integrar a arquitetura e-PING abrange a seleção, a homologação e a classificação das especificações selecionadas em cinco níveis de situações que caracterizam o grau de aderência às políticas técnicas gerais e específicas de cada segmento. Os cinco níveis são:

a) adotado, recomendado, em transição, em estudo, estudo futuro.
b) homologado, sugerido, em testes, em avaliação, avaliação futura.
c) aprovado, analisado, em análise, em estudos preliminares, no aguardo.
d) aceito, validado, em validação, aceito para validação, para futuro.
e) acatado, estudado, em estudos, aceito para avaliação, avaliação de entrada.

REDES DE COMPUTADORES

31- No modelo de referência *ISO OSI*, as camadas que formam a sub-rede de comunicação são

a) Enlace de Dados, Rede, Física.
b) Enlace de Dados, Rede, Transporte.
c) Transporte, Sessão, Física.
d) Sessão, Transporte, Rede.
e) Sessão, Rede, Física.

32- São camadas do modelo de referência *TCP/IP:*

a) Apresentação, Transporte.
b) Rede, Enlace de Dados.
c) *Host*/rede, Inter-redes.
d) Transporte, Física.
e) Aplicação, Sessão.

33- Os serviços de controle de diálogo, gerenciamento de *token* e sincronização pertencem à camada de

a) Rede.
b) Enlace de Dados.
c) Sessão.
d) Apresentação.
e) Transporte.

34- O protocolo sem conexão e não-confiável, destinado a aplicações que não querem controle de fluxo nem manutenção da sequência das mensagens enviadas é o

a) *SMTP*.
b) *OSPF*.
c) *FTP*.
d) *TCP*.
e) *UDP*.

35- O protocolo de roteamento que funciona transformando o conjunto de redes, roteadores e linhas reais em um grafo orientado, no qual se atribui um custo (distância, retardo etc.) a cada arco, para, em seguida, calcular o caminho mais curto com base nos pesos dos arcos é o

a) *IP*.
b) *OSPF*.
c) *AODV*.
d) *IPX*.
e) *RIP*.

36- A camada do modelo de referência *ATM* que permite aos usuários enviarem pacotes maiores que uma célula é denominada

a) Camada de Conversão.
b) Camada de Controle.
c) Camada de Tradução *ATM*.
d) Camada de Adaptação *ATM*.
e) Camada *ATM*.

37- É um dispositivo utilizado em redes de computadores para reencaminhar módulos (*frames*) entre os diversos nós. Além disso, segmenta a rede internamente, sendo que a cada porta corresponde um domínio de colisão diferente, o que significa que não haverá colisões entre os pacotes de segmentos diferentes. Este dispositivo é o

a) Roteador.
b) *Hub*.
c) *Switch*.
d) Concentrador.
e) Ponte.

38- Os 3 componentes chave de uma rede gerenciada *SNMP* são:

a) O equipamento gerenciador, Agente comutador, *Software* de gerenciamento de Rede.
b) O equipamento gerenciado, Agente, *Software* de gerenciamento de Rede.
c) O equipamento gerenciador, Agente concentrador, *Software* de roteamento de Rede.
d) O equipamento concentrador, Agente, *Software* de roteamento de Rede.
e) O equipamento de comutação, Agente roteador, *Software* de bloqueio de Rede.

39- O protocolo *SNMP* opera na seguinte camada do modelo *OSI*:

a) Aplicação.
b) Enlace de Dados.
c) Sessão.
d) Transporte.
e) Apresentação.

40- São requisitos de Qualidade de Serviço (*QoS – Quality of Service*):

a) Capacidade, *Jitter*, Sincronização, Banda estável.
b) Confiabilidade, Retardo, Flutuação no *Jitter*, Largura de Banda.
c) Capacidade do enlace, *Jitter*, Sincronização, Banda variável.
d) Confiabilidade, Retardo, Flutuação do tempo de transmissão, Largura de Banda.
e) Capacidade, Retardo, Flutuação no *Jitter*, Banda estável.

41- O algoritmo em que cada *host* está conectado à rede por uma interface que contém uma fila interna finita e, se um pacote chegar à fila quando ela estiver cheia, o pacote será descartado, é o:

a) Algoritmo de balde cheio (*Full bucket*).
b) Algoritmo de roteamento finito (*Finite routing*).
c) Algoritmo de fila finita (*Finite Queue*).
d) Algoritmo de balde de símbolos (*Token bucket*).
e) Algoritmo de balde furado (*Leaky bucket*).

42- Fazem parte da pilha de protocolos *H.323*:

a) *TCP, G723, RTP, H.229*.
b) Protocolo de enlace, *IP, RTP, H.248*.
c) *TCP*, Protocolo de Aplicação, *RPP, H.245*.
d) *UDP, IP, G724, H.328.*
e) *UDP, IP, RTCP, H.225*.

43- Comparando o *H.323* com o *SIP*, observa-se que

a) o primeiro tem arquitetura modular, enquanto o segundo tem arquitetura monolítica.
b) o primeiro tem endereçamento pelo número de *host* ou telefone, enquanto o segundo tem endereçamento pela *URL*.
c) o primeiro não tem conferência de multimídia, enquanto o segundo tem.
d) o primeiro tem formato de mensagens *ASCII*, enquanto o segundo tem formato de mensagens binário.
e) o primeiro não tem compatibilidade com *PSTN*, enquanto o segundo tem compatibilidade restrita.

44- Em videoconferência, no modelo centralizado, quando existem três ou mais pontos para se conectarem entre si, a comunicação é possível utilizando-se uma Unidade de Controle Multiponto (*MCU - Multipoint Control Unit*), que mescla os vários fluxos de áudio, seleciona o fluxo de vídeo correspondente e retransmite o resultado para todos os outros participantes. Um *MCU* é a combinação de

a) um Controlador Multiponto e de dois Processadores Multiponto.
b) dois Controladores Multiponto e de um Processador Multiponto.
c) dois Controladores Multiponto e de dois ou mais Processadores Multiponto.
d) um Controlador Multiponto e de zero ou mais Processadores Multiponto.
e) três Controladores Multiponto e de vários Processadores Multiponto.

45- São variantes do protocolo *PIM (Protocol-Independent Multicast*):

a) *PIM Sparse Mode, PIM Dense Mode, Birectional PIM, PIM source-specific multicast.*
b) *Shortest path PIM, PIM Dense Mode, Birectional PIM, Unidirectionsl PIM.*
c) *PIM Sparse Mode, PIM Source Discovery, One-way PIM, PIM wide multicast.*
d) *Shortest path PIM, PIM Source Discovery, One-way PIM, PIM source-specific multicast.*
e) *Shortest path PIM, PIM Source Discovery, Birectional PIM, Unidirectional PIM*.

SEGURANÇA DA INFORMAÇÃO

46- Comparando a criptografia simétrica com a assimétrica, observa-se que

a) a primeira possui o problema do gerenciamento de chaves, ao passo que a segunda possui o problema da complexidade binária.
b) a primeira possui o problema da privacidade da chave universal, ao passo que a segunda possui o problema da criação e distribuição de chaves.
c) a primeira possui o problema da distribuição e gerenciamento de chaves, ao passo que a segunda possui o problema do desempenho.
d) a primeira possui o problema do desempenho em redes sem fio, ao passo que a segunda possui o problema do desempenho em ambientes corporativos.
e) a primeira possui o problema do desempenho, ao passo que a segunda possui o problema da geração de chaves.

47- Com relação ao processo de verificação de assinatura digital, tem-se que o algoritmo de assinatura digital é aplicado sobre a assinatura digital recebida, usando a chave pública do remetente, o que resulta no resumo criptográfico da mensagem; em seguida, o algoritmo de *hash* é aplicado na mensagem recebida. A assinatura digital é válida se

a) os dois resumos obtidos forem simétricos.
b) os dois certificados digitais forem iguais.
c) o resumo obtido na recepção for o *hash* do resumo original.
d) os dois resumos obtidos forem iguais.
e) as chaves públicas forem diferentes.

48- Infraestrutura de Chave Pública é o conjunto de *hardware*, *software*, pessoas, políticas e procedimentos necessários para

a) instanciar, transmitir, apagar, publicar e revogar certificados digitais.
b) montar, validar perante a Polícia Federal, distribuir e apagar certificados digitais.
c) criar, gerenciar, armazenar, distribuir e revogar certificados digitais.
d) criar, instanciar, armazenar, restaurar e publicar certificados digitais.
e) montar, gerenciar, armazenar, restaurar e publicar certificados digitais.

49- Quanto à rede desmilitarizada, DMZ, pode-se afirmar que ela permite que serviços sejam providos para os usuários

a) Internos (por meio de servidor de detecção - *bastion hosts*) ao mesmo tempo em que protege a rede interna dos acessos externos.
b) Externos (por meio de servidor de prevenção - *bastion hosts*) ao mesmo tempo em que protege a rede externa dos acessos internos.
c) Internos (por meio de servidor de detecção - *bastion hosts*) ao mesmo tempo em que protege a rede interna dos acessos internos indevidos.
d) Externos (por meio de servidor de tradução de protocolo - *honeypot*) ao mesmo tempo em que protege a rede externa dos acessos externos maliciosos.
e) Externos (por meio de servidor fortificado - *bastion hosts*) ao mesmo tempo em que protege a rede interna dos acessos externos.

50- Os tipos de *IDS* – Sistema de Detecção de Intrusão são

a) *IDS* baseado em *Honeypot (HIDS), IDS* baseado em Rede *(NIDS), IDS* Híbrido.
b) *IDS* baseado em Serviço *(SIDS), IDS* baseado em Rede *(NIDS).*
c) *IDS* baseado em *Host (HIDS), IDS* baseado em *Scanning (SIDS).*
d) *IDS* baseado em Host *(HIDS), IDS* baseado em Rede *(NIDS), IDS* Híbrido.
e) *IDS* baseado em Bloqueio *(BIDS), IDS* baseado em *Prevenção (PIDS), IDS* Híbrido.

51- As arquiteturas clássicas de *Firewall* são

a) *Dual-homed host, Screened host, Global prevention.*
b) *Single host, Screened detection, Screened subnet.*
c) *Dual-homed blocking, Screened detection, Screened subnet.*
d) *Single host, Screened host, Screened prevention.*
e) *Dual-homed host, Hybrid host, Screened subnet.*

52- É um mecanismo de *Hardening* do Servidor *Linux*:

a) minimizar *software* instalado.
b) instalar apenas *softwares* padronizados internacionalmente.
c) instalar versões antigas do sistema operacional e fazer logo em seguida o *upgrade* do sistema.
d) não fazer *upgrades* frequentes, o que pode comprometer a segurança do sistema.
e) manter instalados todos os serviços, mesmo os que sejam aparentemente desnecessários.

53- Qual a diferença entre os protocolos *SPF* e *DKIM*?

a) O primeiro verifica o endereço *IP* do destinatário, enquanto o segundo verifica a estrutura do conteúdo do cabeçalho do e-mail.
b) O primeiro verifica o conteúdo do e-mail, enquanto o segundo verifica a sintaxe do conteúdo do e-mail.
c) O primeiro verifica o endereço *IP* do remetente, enquanto o segundo verifica a estrutura do conteúdo do e-mail.
d) O primeiro verifica a existência de palavras classificadas no e-mail, enquanto o segundo verifica a validade dos endereços de *IP*.
e) O primeiro verifica o conteúdo e o endereço *IP* do remetente, enquanto o segundo verifica a existência de palavras classificadas no e-mail.

54- Em um ataque em que o *Cracker* injeta códigos *JavaScript* em um campo texto de uma página *Web* já existente e este *JavaScript* é apresentado para outros usuários, este *JavaScript* poderia, por exemplo, simular a página de *login* do site, capturar os valores digitados e enviá-los a um site que os armazene. Este ataque é denominado

a) *XSS*.
b) *Spyware de Web*.
c) *Backdoor JavaScript*.
d) *Cross-site Request Forgery*.
e) *CSRF de Java*.

55- A ameaça de segurança em que o atacante consegue inserir uma série de instruções *SQL* dentro de uma consulta (*query*) através da manipulação da entrada de dados de uma aplicação é conhecida como

a) *SQL Mixing.*
b) *SQL False Query.*
c) *SQL Fake Query.*
d) *SQL Query Attack.*
e) *SQL Injection.*

56- Segundo a ISO/IEC 17.799 de 2005, a Gestão de Continuidade de Negócios tem por objetivo não permitir a interrupção das atividades do negócio e proteger os

a) processos de manutenção de sistemas críticos contra efeitos de falhas ou desastres significativos, e assegurar a sua retomada no menor tempo possível.
b) serviços táticos de TI contra efeitos de falhas ou desastres significativos, e assegurar a sua retomada no menor tempo possível.
c) processos de *log* e de auditoria contra efeitos de falhas ou desastres significativos, e assegurar a sua retomada imediatamente.
d) processos críticos contra efeitos de falhas ou desastres significativos, e assegurar a sua retomada em tempo hábil, se for o caso.
e) proteger os processos da cadeia de valor da TI contra efeitos de falhas ou desastres significativos, e assegurar a sua retomada em até uma hora após o incidente.

57- É necessário que os Planos de Recuperação de Desastres sejam

a) aplicados integralmente com frequência e flexíveis com relação a plataformas.
b) adaptáveis, e testados e atualizados com frequência.
c) testados de 3 em 3 anos e atualizados com frequência.
d) atualizados apenas quando houver *upgrade* dos sistemas operacionais.
e) atualizados com frequência e testados apenas quando houver alteração de mais de 30% da infraestrutura de TI.

58- A Instrução Normativa GSI/PR n. 1 define Política de Segurança da Informação e Comunicações como o documento aprovado pela autoridade responsável pelo órgão ou entidade da Administração Pública Federal, direta e indireta, com o objetivo de

a) fornecer diretrizes e suporte administrativo suficientes à elaboração das políticas e das normas da segurança da informação e comunicações.
b) fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações.
c) fornecer planos e procedimentos suficientes à definição de todas as políticas da governança de segurança da informação e comunicações.
d) fornecer sugestões e orientações suficientes para a implementação da governança de segurança da informação e comunicações.
e) fornecer suporte técnico à implementação das normas e procedimentos da segurança da informação e comunicações nas áreas de negócios.

59- A Norma Complementar GSI/PR n. 4 recomenda manter os riscos monitorados e analisados criticamente, a fim de verificar regularmente, no mínimo, as seguintes mudanças: nos critérios de avaliação e aceitação dos riscos, no ambiente, nos ativos de informação, nas ações de Segurança da Informação e Comunicações – SIC, e nos fatores de risco, que são:

a) ataque, vulnerabilidade, risco operacional e impacto.
b) ameaça, vulnerabilidade, probabilidade e impacto.
c) ataque, susceptibilidade, probabilidade e impacto na receita.
d) ameaça, susceptibilidade, risco de mercado e impacto.
e) ataque, vulnerabilidade, probabilidade e impacto no resultado.

60- O serviço das Equipes de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais – ETIR, que consiste em divulgar, de forma proativa, alertas sobre vulnerabilidades e problemas de incidentes de segurança em redes de computadores em geral, cujos impactos sejam de médio e longo prazo, possibilitando que a comunidade se prepare contra novas ameaças é chamado de

a) Anúncios.
b) Emissão de Alertas e Advertências.
c) Disseminação de informações relacionadas à segurança.
d) Avaliação de segurança.
e) Prospecção de segurança.