



Escola de Administração Fazendária



SECRETARIA DO TESOURO
NACIONAL - STN

Cargo: ANALISTA DE FINANÇAS E CONTROLE

Concurso Público 2008

Área:

Prova 2

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:
“Obstáculos são aquilo que vemos quando afastamos nossos olhos do objetivo”.
(Henry Ford)
4. DURAÇÃO DAS PROVAS: **5 horas**, incluído o tempo para a elaboração da Prova Discursiva e para o preenchimento do CARTÃO DE RESPOSTAS.
5. Na prova objetiva há **30 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 iniciadas as provas.
9. Durante as provas, 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 das provas, 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 das provas. A não-observância dessa exigência acarretará a sua exclusão do concurso.
12. Ao sair da sala entregue este CADERNO DE PROVAS, juntamente com o CARTÃO DE RESPOSTAS, ao Fiscal de Sala.

Boa prova!

INFORMÁTICA

- 1 - A habilidade para uso de uma mesma mensagem para invocar comportamentos distintos de um determinado objeto é denominada
- Interface.
 - Polimorfismo.
 - Herança.
 - Encapsulamento.
 - Abstração.
- 2- O diagrama UML que apresenta objetos e suas ligações mútuas, evidenciando a seqüência das mensagens trocadas por meio de números de seqüência, é o
- Diagrama de seqüência.
 - Diagrama de estado.
 - Diagrama de colaboração.
 - Diagrama de caso de uso.
 - Diagrama de atividade.
- 3 - Considere o seguinte contexto: "Um cliente pode comprar vários livros". Em um diagrama de classes, este é um exemplo de relacionamento do tipo
- Agregação.
 - Generalização.
 - Especialização.
 - Associação.
 - Dependência.
- 4 - O componente da arquitetura orientada a serviços (SOA) que consiste em um contrato, uma ou mais interfaces e uma implementação é denominado
- Serviço.
 - Aplicação *front-end*.
 - Repositório de serviços.
 - Barramento de serviços.
 - Lógica de negócio.
- 5 - Na validação de software, o estágio do processo de testes no qual se recomenda o foco na detecção de erros de interfaces de módulos é o teste de
- unidade.
 - módulo.
 - subsistema.
 - sistema.
 - aceitação.
- 6 - Quanto a métricas de software, assinale a opção que corresponde a um exemplo de métrica de controle.
- Complexidade ciclomática de um componente.
 - Número de operações associadas a um objeto.
 - Número de atributos associados a um objeto.
 - Tempo médio para o reparo de defeitos previamente relatados.
 - Tamanho médio de identificadores de um programa.
- 7 - Em relação ao nível lógico de abstração de dados nos sistemas de bancos de dados, é correto afirmar que
- descreve estruturas de dados complexas de baixo nível.
 - descreve quais dados estão armazenados no banco de dados e as relações existentes entre eles.
 - simplifica a interação entre o sistema e os usuários.
 - disponibiliza um conjunto de programas de aplicação que ocultam detalhes dos tipos de dados.
 - descreve um registro como um bloco de armazenamento, composto por palavras ou bytes.
- 8 - No gerenciamento de transações em bancos de dados, a propriedade que deve ser garantida para dar suporte à idéia de execução simultânea de um par de transações é denominada
- Atomicidade.
 - Durabilidade.
 - Sincronismo.
 - Consistência.
 - Isolamento.
- 9 - É uma função da linguagem de manipulação de dados (DML), em um sistema gerenciador de bancos de dados (SGBD):
- permitir a especificação do esquema conceitual do banco de dados.
 - permitir a especificação do esquema interno do banco de dados.
 - especificar visões dos usuários e seus respectivos mapeamentos para o esquema conceitual.
 - especificar e recuperar vários registros em uma única declaração.
 - descrever os componentes dos esquemas: conceitual e interno.

- 10- O modelo de dados, no qual itens de dados individuais do mesmo tipo podem ter diferentes conjuntos de atributos, é conhecido como modelo
- de dados baseado em objeto.
 - entidade-relacionamento.
 - de dados semi-estruturado.
 - relacional.
 - de dados relacional de objeto.
- 11- Uma restrição caracterizada por expressar uma condição que o banco de dados deve atender, de modo que após tal condição ser validada qualquer modificação posterior, somente será aceita se não causar a sua violação, é denominada
- metadado.
 - assertiva.
 - autorização de exclusão.
 - restrição de consistência.
 - autorização de atualização.
- 12- Em ambientes nos quais máquinas, clientes e servidores são comparáveis quanto ao poder de processamento, sendo conectados por uma rede de alta velocidade e, ainda, nos quais as tarefas exigem uma considerável quantidade de computações, o tipo de arquitetura de sistema de banco de dados mais adequado é baseado em sistemas
- orientados a objetos.
 - cliente-servidor.
 - servidores de transação.
 - centralizados.
 - servidores de dados.
- 13- Com respeito à mineração de dados, assinale a opção correta, após avaliar as seguintes afirmações:
- A mineração de dados pode ser usada em conjunto com um *datawarehouse*, para auxiliar tomada de decisão.
 - A mineração de dados permite a descoberta de regras de associação entre hierarquias.
 - A mineração de dados compreende todo o processo de descoberta de conhecimento em bancos de dados.
- Apenas as afirmações I e II são corretas.
 - Apenas as afirmações I e III são corretas.
 - Apenas as afirmações II e III são corretas.
 - As afirmações I, II e III são corretas.
 - As afirmações I, II e III são incorretas.
- 14- Considere uma implementação de *arrays* redundantes de discos independentes (RAID) nível 5, para armazenamento de dados, na qual um bloco de paridade armazena a paridade para blocos no mesmo disco. Se ocorrer uma falha no disco, haverá
- perda de dados e da paridade, impossibilitando a recuperação.
 - perda de dados, porém o bloco de paridade pode ser usado com os blocos correspondentes de outros discos, para a recuperação.
 - perda de dados e de paridade, porém os bits de correção de erros associados ao disco podem ser lidos a partir de outros discos, para a recuperação.
 - perda de dados, porém o bloco de paridade e os bits de correção de erros precisam ser lidos em conjunto, a partir de outros discos, possibilitando a recuperação.
 - perda de dados, porém podem ser utilizados códigos de correção de erros, para a recuperação.
- 15- A mensagem SNMP que permite a busca do valor de uma instância de um objeto MIB (*Management Information Base*) específica é denominada
- Set-request.
 - Get-response.
 - Trap.
 - Get-next-request.
 - Get-request.
- 16- Os equipamentos de interconexão que delimitam domínios de difusão são os
- roteadores.
 - comutadores.
 - concentradores.
 - pontes.
 - repetidores.
- 17- O administrador de uma rede deve selecionar um meio de transmissão para uma distância de longo alcance, de modo que interferências eletromagnéticas não são permitidas. A solução mais adequada deve utilizar
- cabo coaxial.
 - cabo par trançado não-blindado.
 - cabo par trançado blindado.
 - infra-vermelho.
 - fibra ótica.

- 18- A tecnologia de redes baseada em um protocolo de acesso múltiplo, no qual, em caso de colisão, um adaptador aguarda um período de tempo aleatório antes de tentar retransmissão de quadros, é denominada
- ATM.
 - FDDI.
 - Token Ring.
 - Ethernet.
 - Ponto-a-ponto.
- 19- No RUP (*Rational Unified Process*), a descrição de critérios de aceitação para o projeto ocorre na fase de
- Concepção.
 - Elaboração.
 - Construção.
 - Transição.
 - Testes.
- 20- O administrador da rede de uma Universidade, cujo endereço IP é 200.0.0.0, precisa endereçar 15 sub-redes. A máscara mais adequada para o contexto é
- 200.0.0.0/16
 - 200.0.0.0/28
 - 200.0.0.0/26
 - 200.0.0.0/24
 - 200.0.0.0/27
- 21- A área de gerenciamento de rede que permite registrar e controlar o acesso de usuários aos recursos em função de quotas de utilização definidas é denominada gerenciamento de
- falhas.
 - segurança.
 - desempenho.
 - configuração.
 - contabilização.
- 22- A saída do comando Linux: `cat /etc/passwd | wc -l` é a
- listagem, em linhas, dos usuários do sistema.
 - quantidade de usuários online no sistema.
 - listagem do identificador de cada usuário do sistema.
 - listagem dos grupos de usuários do sistema.
 - quantidade de usuários do sistema.
- 23- Considerando a seqüência de segmentos trocados entre duas máquinas para o *handshake* (negociação) em três vias do protocolo de transmissão de controle (TCP), o comando que o destino envia à origem, ao receber um segmento SYN (seq = x) inicial, é
- ACK (x + 1).
 - SYN (seq = y), ACK (x + 1).
 - SYN (seq = y), ACK (y + 1).
 - SYN (seq = x), ACK (x + 1).
 - SYN (seq = x + 1).
- 24- A chave de criptografia utilizada para verificar a autenticidade de um usuário destinatário de mensagens é denominada chave
- secreta.
 - privada.
 - pública.
 - aleatória.
 - one-time-pad*.
- 25- Em uma dada empresa, a política de segurança pode ser definida e modificada por um conjunto pequeno de funcionários em função de níveis de segurança. Este é um cenário relacionado ao serviço de segurança denominado
- Confidencialidade.
 - Integridade.
 - Disponibilidade.
 - Controle de acesso.
 - Assinatura digital.
- 26- Considere o seguinte cenário: Em certa empresa, há máquinas que podem acessar exclusivamente o serviço Web, outras que acessam a Web e o serviço de transferência de arquivos (FTP), enquanto outras podem apenas acessar recursos locais à rede. A solução de segurança mais adequada para o controle de acesso nesta rede deve utilizar
- Firewall de gateway de aplicação.
 - Filtragem de pacotes.
 - Rede privada virtual.
 - Sistema de detecção de intrusos.
 - IPSec.

27- Ao efetuar uma compra em um site de comércio eletrônico, o elemento que garante a autenticidade do servidor (site) e do cliente (usuário) na transação, é denominado

- a) certificado digital.
- b) assinatura digital.
- c) chave pública.
- d) resumo de mensagem.
- e) protocolo de autenticação.

28- Segundo a norma ISO BS 17799, a definição das responsabilidades gerais e específicas no que se refere à gestão da segurança da informação, compreendendo inclusive o registro dos incidentes de segurança, deve ser estabelecida no(a)

- a) Processo de restauração.
- b) Política de segurança.
- c) Análise de riscos.
- d) Acordo de confidencialidade.
- e) Auditoria de segurança.

29- Considere os usuários A e B, cujas chaves públicas são conhecidas por ambos. O usuário A gera o *hash* $H(M)$ de uma mensagem M, assina-a digitalmente e envia para o usuário B. Assinale a opção que representa o que este esquema visa garantir.

- a) A mensagem M está livre de ataques de negação de serviço (DoS).
- b) A mensagem M é confidencial.
- c) A mensagem M não foi modificada durante a transmissão.
- d) A mensagem não pode ser verificada por B.
- e) Não é possível garantir nenhum dos serviços de segurança para o contexto.

30- Considere um grupo de N usuários e um esquema de criptografia combinada – baseada em criptografia simétrica e assimétrica. Suponha que um usuário deste grupo deseja enviar uma mensagem M, de forma confidencial e eficiente, aos demais usuários no mesmo grupo. O número total de encriptações necessárias para o envio da mensagem M é

- a) 1.
- b) $2N + 1$.
- c) $2N$.
- d) N.
- e) $N - 1$.

