# CONHECIMENTOS ESPECÍFICOS

Acerca da organização e arquitetura de computadores e dos componentes de um computador, julgue os itens a seguir.

**51** A diminuição do tamanho dos *chips* resulta em ganho de desempenho em *hardware*, uma vez que leva ao aumento da relação entre resistência e capacitância, pois as interconexões de fio se tornam mais finas, aumentando a resistência, e os fios estão mais próximos, aumentando a capacitância.

**52** Arquitetura de computador refere-se aos atributos de um sistema visíveis a um programador, ou seja, atributos que possuem impacto direto sobre a execução lógica de um programa. Nesse contexto, é considerada uma questão arquitetural, por exemplo, se uma instrução de multiplicação será realizada por uma unidade de multiplicação especial ou por um mecanismo que faça uso repetido da unidade de adição do sistema.

A respeito dos princípios de sistemas operacionais, das características dos principais processadores do mercado e dos processadores de múltiplos núcleos, julgue os itens subsequentes.

**53** Por meio da técnica de *pipeline*, a arquitetura MIMD e a MISD podem executar múltiplos *threads* ao mesmo tempo. Na arquitetura MISD, os *threads* executados são independentes e manipulam dados diferentes.

**54** No processamento das interrupções geradas pelos componentes de entrada e saída, é necessário que o processador identifique univocamente qual dispositivo gerou a interrupção. Uma das técnicas utilizadas para essa identificação é a *daisy chain*, que realiza a identificação por *hardware*, usando uma conexão entre os módulos e o processador, na forma de uma cadeia circular.

Julgue o próximo item, no que se refere à paravirtualização.

**55** A substituição da chamada de uma instrução sensível pela chamada de um tratador de interrupção de *software* (*trap*) com uma parametrização adequada de registradores é conhecida como *hypercall*.

Com referência a sistemas de arquivos e a sistemas RAID, julgue o item seguinte.

**56** Em sistemas de arquivos NTFS, a tabela-mestra de arquivos (MTF) é dividida em seis partições de tamanhos variáveis. Para prover tolerância a falhas nessa configuração, é necessário e suficiente organizá-los utilizando-se RAID nível 4, pois, quanto maior o número de discos do arranjo, menor será a possibilidade de falha.

Julgue o item abaixo, referente às técnicas de recuperação de arquivos apagados.

**57** Cópias de segurança físicas armazenam dados, usando uma estrutura de diretório e permitem que os dados de arquivo sejam recuperados por sistemas heterogêneos. Salvar arquivos nesse formato é eficiente, pois não ocorre sobrecarga na tradução entre o formato do arquivo nativo e o formato de arquivamento.

No que se refere a arquitetura, modelos lógicos e representação física de banco de dados e implementação de SGBDs relacionais, julgue os itens que se seguem.

**58** As dependências de dados, que incluem as funcionais e as multivaloradas, são consideradas dependências semânticas da implementação do banco de dados, por serem restrições inerentes embasadas no modelo.

**59** A arquitetura ANSI de três níveis separa o nível externo dos usuários, o nível conceitual do banco de dados e o nível de armazenamento interno no projeto de um banco de dados. O nível interno tem um esquema interno, que descreve a estrutura do armazenamento físico do banco de dados e descreve os detalhes completos do armazenamento de dados e os caminhos de acesso para o banco de dados.

Julgue os itens a seguir, relativos à linguagem de consulta estruturada (SQL).

**60** Em SQL, *triggers* são conhecidas como técnicas de banco de dados ativo, pois especificam ações que são disparadas automaticamente por eventos.

**61** Divergência de impedância é o termo usado para se referir aos problemas que ocorrem devido às diferenças entre o modelo de banco de dados e o modelo da linguagem de programação.

Com relação a características e análise de *logs* em transações de banco de dados, julgue o item subsequente.

**62** Para realizar a auditoria em um banco de dados, a utilização de um sistema gerenciador de *streams* de dados (SGSD) impede que o administrador do banco de dados defina os parâmetros de auditoria e os dados a serem auditados mediante consultas, de tal forma que os resultados sejam obtidos em tempo real, minimizando o volume de registros de *log* que precisam ser armazenados.

Acerca dos conceitos da engenharia reversa, julgue os itens subsecutivos.

**63** A depuração de programas utiliza métodos de teste e análise para tentar entender o *software*. Esses métodos são classificados como caixa-branca (*white box*) e caixa-preta (*black box*). Para se conhecer o código e seu comportamento, o teste caixa-branca é menos eficiente que o teste caixa-preta, embora seja mais fácil de ser implementado.

**64** *Red pointing* é o método mais rápido para se realizar engenharia reversa em um código. Para criar um *red pointing* em um código alvo, é suficiente identificar no programa os locais potencialmente vulneráveis, que fazem chamada ao sistema operacional, e detectar os dados fornecidos pelo usuário, que são processados nesse local.

**65** A engenharia reversa permite conhecer a estrutura do programa e sua lógica e, com base nessas informações, alterar a estrutura do programa, afetando diretamente o fluxo lógico. Essa atividade é conhecida como *patching*.

Com relação à ofuscação de código, a programas maliciosos e a compactadores de código executável, julgue os itens seguintes.

**66** Programas maliciosos do tipo RootKits são os mais perigosos, principalmente para usuários de *Internet Banking*, pois esses programas têm a função de capturar as teclas digitadas no computador.

**67** Um arquivo compactado do Linux cujo nome é `prova.tar.gz` poderá ser descompactado para a saída padrão, alterando-se o nome original, por meio do comando `gzip -dc prova.tar.gz tar xvf -`.

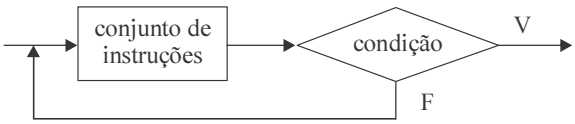
No que se refere às linguagens de programação, julgue os itens subsecutivos.

**68** A execução da função `x` descrita abaixo para o valor `n` igual a 8 fornecerá 21 como resultado.

```
long x(int n){
    if (n<0) return -1;
    if (n==0) return 0;
    if (n==1) return 1;
    return x(n-1) + x(n-2);
}
```

**69** Coesão e acoplamento são dois critérios úteis para se analisar a qualidade da interface pública de uma classe. A interface pública será considerada coesa se todos os seus recursos estiverem relacionados ao conceito que a classe representa, enquanto, no acoplamento, uma classe é dependente de outra.

**70** O diagrama de blocos apresentado abaixo se refere à instrução `faça <conjunto de instruções> enquanto <condição>`.




**71** No *servlet* e *Jsp*, o tratamento de caracteres especiais como caractere comum, recebidos em páginas HTML, pode ser feito por meio do método estático `encode` da classe `java.net.URLEncoder`.

**72** A propriedade `readyState` do objeto `XMLHttpRequest` em Ajax no Internet Explorer possui 3 estágios, sendo 0 correspondente a não inicializado, 1 correspondente a carregado e 2 correspondente a completo.

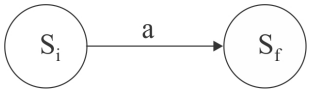
Com relação aos conceitos e características de compiladores, julgue os itens que se seguem.

**73** Interpretador é um tradutor de linguagem que executa o programa fonte de imediato, em vez de gerar um código objeto a ser executado após o término da tradução, enquanto o compilador recebe um programa fonte e produz programa equivalente na linguagem alvo. No caso da linguagem Java, os processadores combinam compilação e interpretação.

**74** Considere a gramática `string → string + string | string - string |0|1|2|3|4|5|6|7|8|9` e a `string` como um único nó não terminal, que pode ser um dígito ou uma sentença. Nessa situação, a expressão 10 – 4 + 3 possibilita criar duas árvores de derivação distintas.

Acerca dos conceitos e características de estrutura de dados e autômatos, julgue os itens a seguir.

**75** Autômatos finitos são usualmente apresentados na forma de um grafo dirigido. A figura abaixo representa uma transição que pode ocorrer se o autômato estiver em um estado $S_i$ e se o símbolo da *string* de entrada for a. Caso a entrada para o autômato seja a *string* `prova`, é correto afirmar que ocorrerá a transição de $S_i$ para $S_f$.



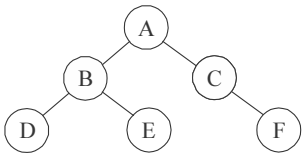

**76** Considere `tnode` um nó de uma lista encadeada e a função `monta_lista` listados abaixo. Nesse caso, a utilização da função `monta_lista` criará uma lista encadeada com as informações ordenadas em ordem decrescente alfabeticamente e o ponteiro topo apontará para o nó com a maior informação alfabética.

```
struct tnode {
   char info[100];
   struct tnode *prox;
};
monta_lista(struct tnode **topo, struct tnode
*p)) {
   struct tnode *atual, *ant;
   if (*topo == NULL) {
      *topo = p;
       return;
   }
   if (strcmp((*topo)->info, p->info) >= 0) {
      p->prox = *topo;
      *topo = p;
      return;
   }
   ant = *topo;
   atual = ant->prox;
   while (atual != NULL) {
      if (strcmp(atual->info,p->info) > 0){
         p->prox = atual;
         ant->prox = p;
         return;
      }
      ant = atual;
      atual = atual->prox;
   }
   ant->prox = p;
}
```

**77** As árvores apresentadas abaixo são ditas equivalentes.


**78** Considere um vetor C com valores entre 0 e 999, em que cada elemento do vetor é dividido em três partes (unidade, dezena e centena). Nesse caso, o método de classificação por distribuição de chave, aplicado sobre C, realizará a ordenação dos valores pela execução de sucessivos passos, tomando-se em cada passo apenas uma parte do elemento.

**79** Na árvore binária representada abaixo, o caminhamento pós-fixado produzirá a seguinte sequência de nós visitados: D, B, E, A, C, F.



Julgue os itens que se seguem, referentes a técnicas de comunicação, topologias, arquiteturas e protocolos relacionados às redes de computadores.

**80** Para assegurar uma topologia livre da ocorrência de *loops*, o que é fundamental para que redes IEEE 802.5 funcionem adequadamente, os equipamentos de interconexão, como *switches* e pontes, trocam informações com a utilização do protocolo STP (*Spanning Tree Protocol*).

**81** Com relação à qualidade de serviço (QoS) na camada de rede IP, os serviços diferenciados (DiffServ) são embasados no conceito de classes de serviços. Os serviços integrados (IntServ), por sua vez, utilizam uma abordagem de parametrização na qual é necessária a reserva prévia de recursos nos roteadores com o uso do protocolo de sinalização RSVP (*Resource Reservation Protocol*).

**82** Utilizado em dispositivos de acesso a redes sem fio, o padrão IEEE 802.1x provê um mecanismo de autenticação para dispositivos que se conectam a uma porta em uma LAN. Esse padrão envolve três partes: o cliente (também conhecido como suplicante), um dispositivo autenticador e o servidor de autenticação (por exemplo, o Radius).

**83** Em uma rede P2P (*peer-to-peer*), cada computador pode atuar como cliente e como servidor de outros computadores, possibilitando, por exemplo, o compartilhamento de arquivos. O BitTorrent é um dos protocolos para redes P2P e caracteriza-se pela existência de um mapeamento das taxas de *download* e *upload* entre os *peers*, de forma que um cliente pode transferir um arquivo a partir do *peer* com maior taxa de transferência.

**84** Considerando-se o endereçamento IPv4 das redes com arquitetura TCP/IP e sabendo-se que o endereço de um *host* em uma sub-rede é 182.44.82.16/27, é correto afirmar que os endereços 182.44.82.158 e 182.44.82.159 representam *hosts* em uma mesma sub-rede.

**85** Com base nas características inerentes a um equipamento de interconexão de ponto de acesso sem fio (*wireless access point*), é correto afirmar que ele funciona como uma ponte (*bridge*).

---

Acerca de computação em nuvem, julgue os itens subsequentes.

**86** O GAE (*Google App Engine*) pertence à categoria de computação em nuvem conhecida como IaaS *(Infrastructure as a Service*) e caracteriza-se por prover máquinas virtuais, infraestrutura de armazenamento, *firewalls*, balanceamento de carga, entre outros recursos, de forma a hospedar aplicações *web* nos *datacenters* da Google.

**87** Com o ambiente de computação em nuvem Azure, da Microsoft, é possível a criação de máquinas virtuais com sistemas operacionais distintos, desde o Windows Server até máquinas com distribuição Linux, como, por exemplo, CentOS, Suse e Ubuntu.

Com relação à norma ISO/IEC 27001:2006, julgue os itens a seguir.

**88** De acordo com a norma ISO/IEC 27001:2006, a formulação de um plano de tratamento de riscos que identifique a ação apropriada, os recursos, as responsabilidades e as prioridades para a gestão de riscos está relacionada à etapa *Do* do ciclo PDCA.

**89** Segundo a norma ISO/IEC 27001:2006, a organização deve elaborar uma declaração de aplicabilidade, detalhando os ativos dentro do escopo do SGSI e os seus proprietários, bem como as possíveis ameaças aplicadas a tais ativos e as vulnerabilidades por elas exploradas.

**90** Segundo a norma ISO/IEC 27001:2006, no estabelecimento do Sistema de Gestão da Segurança da Informação (SGSI), devem-se identificar e avaliar as opções para o tratamento de riscos, cujas ações englobam a aceitação consciente dos riscos (desde que satisfaçam às políticas estabelecidas dentro da organização), bem como a possibilidade de transferência dos riscos para outras partes, como seguradoras e fornecedores.

---

A respeito de segurança da informação, julgue os próximos itens.

**91** O ser humano possui traços psicológicos e comportamentais que o tornam vulneráveis a ataques de engenharia social, como a vontade de ser útil, a busca por novas amizades, esteganografia e autoconfiança.

**92** Um aplicativo que utiliza recursos biométricos para a criptografia de arquivos, como a impressão digital de um indivíduo tanto para encriptar quanto decriptar, assemelha-se a um sistema criptográfico simétrico.

---

No que se refere a processos de desenvolvimento seguro de aplicações, julgue os itens subsecutivos.

**93** O processo SDL (*Secure Development Lifecycle*) tem sido adotado pela Microsoft no desenvolvimento de alguns de seus produtos, como Windows Server, SQL Server e Exchange Server, reduzindo o número de vulnerabilidades encontradas nesses produtos em versões desenvolvidas sem o uso do SDL. Uma das características desse processo é que ele provê dois roteiros, sendo um com foco no suporte a desenvolvimento de novos sistemas com base em um processo iterativo, e outro que enfoca a manutenção de sistemas já existentes.

**94** O CLASP (*Comprehensive, Lightweight Application Security Process*) fornece uma taxonomia de vulnerabilidades que podem ocorrer no código-fonte e que podem ser verificadas com o uso de ferramentas automatizadas para análise estática de código.

Julgue os seguintes itens, relativos à segurança em redes de computadores.

**95** O termo APT (*Advanced Persistent Threat*) refere-se a ataques que são altamente focados em uma empresa ou em um governo particular. Geralmente, o ataque é conduzido de forma lenta e gradativa, podendo levar meses ou anos para atingir seu objetivo. O vírus Stuxnet, que recentemente atingiu o programa nuclear iraniano, é considerado um exemplo de APT.

**96** O uso de criptografia SSL (*Secure Socket Layer*) como item de segurança nas transmissões de dados via Internet dificulta o monitoramento realizado por sistemas de detecção de intrusos (IDS) de redes. Uma solução para esse problema é o uso de *proxies* reversos, que permite retirar o processo de criptografia do servidor *web* e, consequentemente, possibilita ao IDS o monitoramento do tráfego.

**97** A captura de quadros de redes *wireless* IEEE 802.11 geralmente não é alcançada com o uso do modo promíscuo da interface de rede, sendo necessário configurar a interface de rede para o modo de monitoramento (*monitor mode*). Além disso, pode haver restrições por parte do sistema operacional, como ocorre no Windows, o que impede a captura de quadros desse tipo.

**98** O WIPS *(Wireless Intrusion Prevention System*) é um dispositivo que monitora o espectro de ondas de rádio, buscando identificar a presença de pontos de acesso não autorizados. Ao detectar a presença de sinais de rádio não autorizados, o WIPS pode enviar alerta ao administrador ou ao *firewall* da rede para prevenir possíveis ataques.

**99** O *ARP Spoofing* é um tipo de ataque no qual o computador do atacante gera quadros com endereços MAC falsos, para que a tabela de endereços MAC do *switch* da rede seja preenchida totalmente com endereços forjados. Com isso, muitos *switches* não conseguem armazenar os endereços MAC verdadeiros e acabam trabalhando como um *hub*, repassando os quadros a todas as portas e permitindo que o atacante possa capturar o tráfego da rede.

**100** *Phishing* é a técnica empregada por vírus e cavalos de troia para obter informações confidenciais do usuário, como, por exemplo, dados bancários.

**101** *Traffic shaping* é uma prática que tem sido adotada por empresas de telefonia e provedoras de acesso à Internet que, apesar de ser considerada abusiva por parte de órgãos de defesa do consumidor, geralmente é utilizada para otimizar o uso da largura de banda disponível, restringindo a banda para serviços que demandam a transferência de grande volume de dados, como P2P e FTP.

A respeito de criptografia, julgue os itens subsequentes.

**102** Modos de operação de cifra de bloco permitem cifrar mensagens de tamanhos arbitrários com a utilização de algoritmos de cifragem de blocos, que trabalham com blocos de tamanho fixo. Os modos de operação existentes asseguram a confidencialidade e a integridade da mensagem cifrada, embora nem todos possam ser utilizados para autenticação.

**103** A confidencialidade e a integridade de uma comunicação são garantidas com o uso de criptografia tanto simétrica quanto assimétrica. No entanto, para garantir autenticidade e irretratabilidade, é necessário o uso combinado desses dois tipos de criptografia.

Julgue os itens a seguir, a respeito de certificação digital e algoritmos RSA, AES e RC4.

**104** Ao acessar um sítio seguro na Internet e receber o certificado digital do servidor, o navegador do cliente faz uma consulta à autoridade certificadora que assinou aquele certificado para verificar, por exemplo, se o certificado é válido ou não está revogado. Essa verificação é feita com o uso do protocolo OCSP (*Online Certificate Status Protocol*).

**105** AES é uma cifra de bloco, enquanto o RC4 é uma cifra de fluxo. Apesar dessa diferença, ambos têm em comum a utilização de um tamanho de chave de 128, 192 ou 256 *bits*.

**106** Embora o algoritmo RSA satisfaça aos requisitos necessários para prover assinatura digital, ele é utilizado, por questões de desempenho, em conjunto com funções de *hashes* criptográficos, como SHA-1.

A respeito de *hashes* criptográficos, julgue os itens que se seguem.

**107** SHA-1 e MD-5 são exemplos de *hashes* criptográficos largamente utilizados na Internet. O MD-5 tem sido substituído pelo SHA-1 pelo fato de este gerar um *hash* maior e ser o único à prova de colisões.

**108** O SHA-1, comumente usado em protocolos de segurança, como TLS, SSH e IPSec, também é utilizado por alguns sistemas de controle de versão como Git e Mercurial para garantir a integridade das revisões.

Julgue os itens a seguir, acerca do sistema operacional Windows.

**109** Administradores de redes com Windows 7, em comparação a administradores de rede com Windows Vista, precisam conceder maior número de privilégios a recursos de rede que exigem acesso de super usuário. Isso se deve, entre outros fatores, ao maior número de aplicativos do Windows 7 que exigem acesso com privilégios administrativos.

**110** Aplicativo, Segurança, Sistema, Instalação e ForwardedEvents são categorias de *logs* do Windows cuja finalidade é organizar os eventos de aplicativos que são monitorados pelo sistema operacional, permitindo aos administradores decidirem quais eventos serão gravados no *log*.

**111** BitLocker é um recurso presente no Windows 7 que fornece criptografia de todos os volumes de inicialização para um computador e para dispositivos móveis, como unidades *flash* USB.

**112** AppLocker é um recurso do Windows 7 que permite especificar quais aplicativos podem ser executados em um *desktop* ou *notebook*, ajudando, assim, a diminuir a probabilidade de execução de *malwares* nessas máquinas.

**113** Registro do Windows é um banco de dados que contém informações sobre os programas instalados, configurações, perfis das contas de usuários e sobre o *hardware* do sistema.

Julgue os itens seguintes, com relação ao Linux.

**114** Squid é uma aplicação nativa do Linux que provê serviços de correio eletrônico compatíveis com o SMTP (*Simple Mail Transfer Protocol*), IMAP (*Internet Message Access Protocol*) e POP3 (*Post Office Protocol*).

**115** O escalonador de tarefas do Linux presente na versão 2.6 fornece afinidade de processador, balanceamento de carga e suporte para multiprocessamento simétrico por meio de algoritmo preemptivo embasado em prioridades. Dessa forma, quanto maior for a prioridade, maior será a quota de tempo fornecida.

**116** No Linux, os usuários são cadastrados no sistema no arquivo `/home`, que guarda uma entrada para cada usuário, incluindo-se o diretório e o *shell*.

No que se refere aos sistemas Android e iOS, julgue os próximos itens.

**117** O sistema Android 4.0 foi desenvolvido com base no *kernel* Linux versão 2.6 e é voltado para dispositivos móveis, controlando os serviços do sistema, como gerenciamento de memória e de tarefas, diretivas de segurança e *drivers*.

**118** A arquitetura do iOS possui quatro camadas (*layers*) que funcionam como interface entre a aplicação e o *hardware*. Essas camadas, listadas da mais baixa para a mais alta, são: Core OS, Core Services, Media e CoCoa Touch.

Com relação à governança de tecnologia da informação (TI), julgue os itens subsequentes.

**119** O COBIT abrange controles acerca de gerência de central de serviços especificamente no domínio Entregar e Suportar. No ITIL v3, a central de serviços é tipificada como uma função do estágio Operação de Serviços.

**120** Com base na SLTI MP IN n.º 4/2010, em uma contratação de solução de TI, a fase de planejamento da contratação prescinde a fase de seleção do fornecedor.

# PROVA DISCURSIVA

- Nesta prova, faça o que se pede, usando, caso deseje, o espaço para rascunho indicado no presente caderno. Em seguida, transcreva o texto para a **FOLHA DE TEXTO DEFINITIVO DA PROVA DISCURSIVA**, no local apropriado, pois não serão avaliados fragmentos de texto escritos em locais indevidos.
- Qualquer fragmento de texto que ultrapassar a extensão máxima de linhas disponibilizadas será desconsiderado.
- Na **folha de texto definitivo**, identifique-se apenas na primeira página, pois não será avaliado o texto que apresentar qualquer assinatura ou marca identificadora fora do local apropriado.
- Ao domínio do conteúdo serão atribuídos até **13,00 pontos**, dos quais até **0,60 ponto** será atribuído ao quesito apresentação e estrutura textual (legibilidade, respeito às margens e indicação de parágrafos).

---

> Se uma intrusão em um sistema computacional for detectada com rapidez suficiente, o intruso poderá ser identificado e expulso do sistema antes que qualquer dado seja comprometido. Mesmo que a detecção não seja suficiente para impedir o intruso, quanto mais cedo for detectada a intrusão, menores serão os danos e mais rapidamente a recuperação poderá ser obtida.
>
> William Stallings. **Criptografia e segurança de redes**: **princípios e práticas**. 4.ª ed. São Paulo: Pearson Prentice Hall, 2008, p. 408 (com adaptações).

Considerando que o fragmento de texto acima tem caráter unicamente motivador, redija um texto dissertativo acerca do seguinte tema.

**SISTEMAS DE DETECÇÃO DE INTRUSÃO (IDS: *INTRUSION DETECTION SYSTEMS*)**

Ao elaborar seu texto, aborde, necessariamente, os seguintes aspectos:

- definição de IDS; [**valor: 3,00 pontos**]
- diferenças entre IDS e *firewall*; [**valor: 3,00 pontos**]
- tipos de IDS, em especial aqueles embasados em rede e em *host*; [**valor: 3,00 pontos**]
- principais técnicas de detecção de intrusos e suas limitações. [**valor: 3,40 pontos**]

---

## RASCUNHO

| | |
|---|---|
| 1 | |
| 2 | |
| 3 | |
| 4 | |
| 5 | |
| 6 | |
| 7 | |
| 8 | |
| 9 | |
| 10 | |
| 11 | |
| 12 | |
| 13 | |
| 14 | |
| 15 | |
| 16 | |
| 17 | |
| 18 | |
| 19 | |
| 20 | |
| 21 | |
| 22 | |
| 23 | |
| 24 | |
| 25 | |
| 26 | |
| 27 | |
| 28 | |
| 29 | |
| 30 | |