PRESIDÊNCIA DA REPÚBLICA
INSTITUTO DE PESQUISA ECONÔMICA APLICADA – IPEA

CONCURSO PÚBLICO

Aplicação: 14/12/2008

CARGO 002:
ANALISTA DE SISTEMAS
PERFIL:
SUPORTE DE INFRA-ESTRUTURA

CADERNO DE PROVAS – PARTE II
CONHECIMENTOS ESPECÍFICOS
DISCURSIVA

ATENÇÃO!

» Leia atentamente as instruções constantes na capa da Parte I do seu caderno de provas.

» Nesta parte do seu caderno de provas, que contém os itens relativos à prova objetiva de **Conhecimentos Específicos** e a **prova discursiva**, confira o número, o nome e o perfil de seu cargo transcritos acima, no rodapé de cada página numerada desta parte do caderno de provas, na **folha de respostas** e na **folha de texto definitivo da prova discursiva**.

AGENDA (datas prováveis)

I **16/12/2008**, após as 19 h (horário de Brasília) – Gabaritos oficiais preliminares das provas objetivas: Internet — www.cespe.unb.br.

II **17** a **21/12/2008** – Recursos (provas objetivas): exclusivamente no Sistema Eletrônico de Interposição de Recurso, Internet, mediante instruções e formulários que estarão disponíveis nesse sistema.

III **21/1/2009** – Resultados final das provas objetivas e provisório da prova discursiva: Diário Oficial da União e Internet.

IV **23/2/2009** – Resultado final da prova discursiva e convocação para a entrega da documentação para a avaliação de títulos: Diário Oficial da União e Internet.

OBSERVAÇÕES

- Não serão objeto de conhecimento recursos em desacordo com o item 16 do edital n.º 1 – IPEA, de 8 de setembro de 2008.
- Informações adicionais: telefone 0(XX) 61 3448-0100; Internet – www.cespe.unb.br.
-

cespeUnB
Centro de Seleção e de Promoção de Eventos

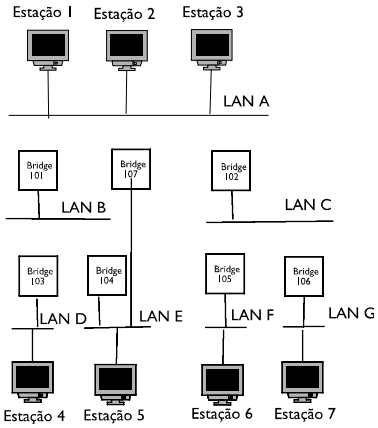
De acordo com o comando a que cada um dos itens de **51** a **120** se refira, marque, na **folha de respostas**, para cada item: o campo designado com o código **C**, caso julgue o item **CERTO**; ou o campo designado com o código **E**, caso julgue o item **ERRADO**. A ausência de marcação ou a marcação de ambos os campos não serão apenadas, ou seja, não receberão pontuação negativa. Para as devidas marcações, use a **folha de respostas**, único documento válido para a correção das suas provas.

CONHECIMENTOS ESPECÍFICOS

Com base nos conceitos de redes, julgue os itens a seguir.

51 As redes *ethernet* utilizam o CSMA/CD (*carrier sense multiple access with collision detect*). Este protocolo foi criado com o objetivo de resolver o problema das colisões que acontecem quando os pacotes são transmitidos simultaneamente a partir de nós diferentes.

52 O protocolo OSPF (*open shortest path first*) é um protocolo de roteamento IP de estado do enlace, em que a largura de banda disponível no enlace é o parâmetro principal para definir o melhor caminho para um nó remoto na rede.



Com base na figura acima, julgue os itens seguintes.

53 Suponha que a estação 1 transmita um quadro na LAN A com destino para a estação 6. Nesse caso, este quadro será lido pelos *bridges* 101, 102 e 107.

54 Um quadro que chegar na LAN C será direcionado à LAN F, de tal forma que somente o bridge 105 fará a sua leitura.

55 Existem duas rotas entre a LAN A e a LAN E, de tal forma que um pacote com origem em uma destas LANs poderia ser encaminhado pelo *bridge* 101 ou pelo *bridge* 107.

A respeito do funcionamento dos equipamentos de rede, julgue os itens que se seguem.

56 Existem dois tipos de *switches* de camada 2. O *switch* tipo *cut-through* analisa o endereço destino do quadro no inicio do quadro MAC e repete o quadro em todas as linhas de saída para reconhecer quem é o nó com esse endereço.

57 O *switch* tipo *cut-through*, antes de retransmitir um quadro faz uma avaliação de CRC, de tal forma que evita a retransmissão de quadros com erro.

58 Um conjunto de dispositivos conectados a *switches* camada 2 implica que estes compartilham o mesmo endereço MAC de *broadcast*. Um *switch* de camada 3 implementa a lógica de encaminhamento de pacotes do roteador no *hardware*.

A respeito dos endereços IP, julgue os itens subseqüentes.

59 Suponha que uma rede utiliza a máscara de rede 255.255.255.192. Nesse caso são utilizados 2 *bits* para o endereço de rede e 6 *bits* para o endereço dos *hosts*, para um total de 64 possíveis endereços de *hosts*.

60 Suponha que uma rede utiliza a máscara 255.255.255.252. Nesse caso, são possíveis 62 endereços de rede.

```
% netstat -r
Routing tables
Destination      Gateway           Flags  Refs     Use    Netif Expire
default          outside-gw        UGSc     37     418      ppp0
localhost        localhost         UH        0     181       lo0
test0            0:e0:b5:36:cf:4f  UHLW      5   63288       ed0      77
10.20.30.255     link#1            UHLW      1    2421
exam.com         link#1            UC        0       0
host1            0:e0:a8:37:8:1e   UHLW      3    4601       lo0
host2            0:e0:a8:37:8:1e   UHLW      0       5       lo0 =>
host2.exam.com   link#1            UC        0       0
224              link#1            UC        0       0
```

Com base na saída do comando netstat-r, conforme mostrado acima, julgue os seguintes itens.

61 A saída do comando mostra a tabela de roteamento da interface ppp0 em que se especifica que o uso do localhost é lo0, conhecido também como *loopback device*. Este dispositivo permite que todo o trafégo para o destino localhost seja mantido internamente em vez de enviá-lo na LAN.

62 O host1 corresponde ao *host* no qual foi executado o comando. Esta identificação é possível a partir da verificação de que a interface é lo0.

```
default-lease-time 300;
max-lease-time 1200;
option subnet-mask 255.255.255.0;
option broadcast-address 255.255.255.255;
option routers 192.168.1.1;
option domain-name-servers 164.41.1.5, 164.41.1.3;
option domain-name "teste.cespe.unb.br";

subnet 192.168.1.0 netmask 255.255.255.0 {
          range 192.168.1.10 192.168.1.100;
          range 192.168.1.150 192.168.1.200;
```

Com base nas informações apresentadas acima, que representam o arquivo dhcpd.conf em um sistema operacional Linux, julgue os itens a seguir.

63 O arquivo de configuração mostrado apresenta uma sintaxe totalmente correta e normalmente fica armazenado em /bin/dhcpd.conf.

64 A linha option subnet-mask 255.255.255.0 define a máscara de subrede a ser fornecida aos clientes e option broadcast-address 255.255.255.255 define o endereço de envio para requisições de *broadcast*.

Com base nos conceitos básicos de padrões de Internet (W3C e RFCs), julgue os itens seguintes.

65 O W3C trabalha em áreas denominadas de Actividades W3C. Essas atividades são organizadas em grupos de trabalho (*working groups*), grupos de interesse (*interest groups*) e grupos de coordenação (*coordination groups*). Os grupos que desenvolvem os trabalhos técnicos são os grupos de interesse.

66 Os grupos de trabalho do IETF estão organizados por áreas e são gerenciadas por ADs (area directors). Cada AD é membro do *Internet Engineering Steering Group* (IESG). As RFCs publicadas pelo IETF inicialmente passam pelo estágio IETF-Draft para, eventualmente, virem a ser aceitas como uma RFC.

Com base na operação de serviços DHCP, WINS, DNS, FTP, servidores WEB, servidores de correio, VPN e operação de servidores *proxy*, julgue os itens que se seguem.

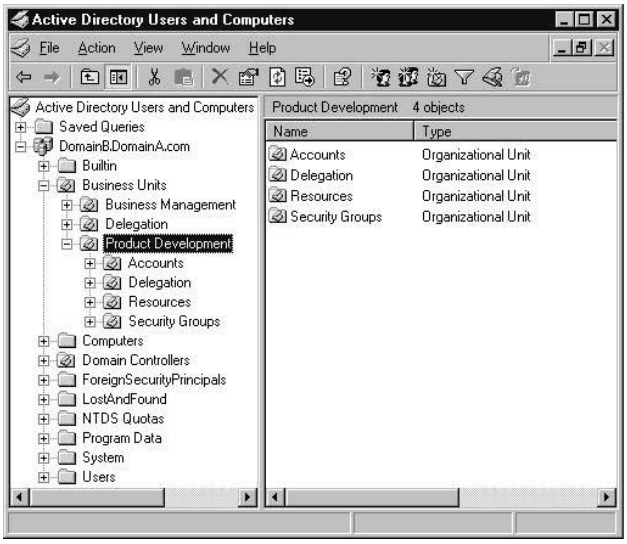
67 Um *proxy* transparente permite que o usuário, ao configurar o *hostname* e a porta do *proxy* no *software* de *browsing*, possa utilizar as vantagens do serviço. Um exemplo de servidor de *proxying* transparente é o Squid.

68 A utilização do comando `iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT --to-port 3128` permite que os pedidos para a interface eth0 sejam encaminhados para a porta 3128. Esse comando, de forma geral faria parte da implementação do serviço de *proxy* transparente em um servidor Linux.

69 A utilização dos comandos no Linux: `openvpn --remote 192.168.1.1 --dev tun0 --ifconfig 10.0.0.1 10.0.0.2` e do comando `openvpn --remote 192.168.1.202 --dev tun0 --ifconfig 10.0.0.2 10.0.0.1` em um cliente e servidor, respectivamente, permitem a criação de um túnel simples e não encriptado quando o cliente e o servidor estiverem ligados em rede e sem *firewall* no meio.

70 Em um servidor Windows, o *gateway* de serviços de terminal permite o acesso remoto a aplicações com o uso de uma VPN para que os usuários possam acessar as aplicações, independentemente de onde se localizem.

71 No Linux a utilização do comando `/usr/sbin/sendmail -q` permite que sejam visualizados os conteúdos das mensagens que estão na fila de correio.



Com base na figura acima que mostra o Active 2 Directory do Windows 2003, julgue os itens seguintes.

72 No topo da estrutura do Active Directory encontra-se a floresta (*forest*) que contém todos os objetos, unidades organizacionais, domínios e atributos na sua hierarquia. Abaixo de uma floresta podem existir uma ou mais árvores que contém três tipos de elementos: unidades organizacionais, objetos e atributos. Na figura, o cursor está em uma unidade organizacional.

73 Os grupos, que se encontram dentro do item System mostrado na figura, têm duas funções principais: segurança e distribuição. Um grupo de segurança contém contas que podem ser usadas para alocar direitos de acesso a um diretório particular em um servidor de arquivos.

Acerca de conectividade de banco de dados, *softwares* aplicativos e plataformas operacionais em redes locais, julgue os itens subseqüentes.

74 A linguagem Java dispõe da Java DataBase Connectivity ou JDBC para acessar os repositórios de dados. O JDBC implementa em Java a funcionalidade definida pelo padrão SQL. Um outro exemplo de API que implementa o SQL é o ODBC. A vantagem do JDBC é a portabilidade da aplicação cliente, inerente da linguagem Java.

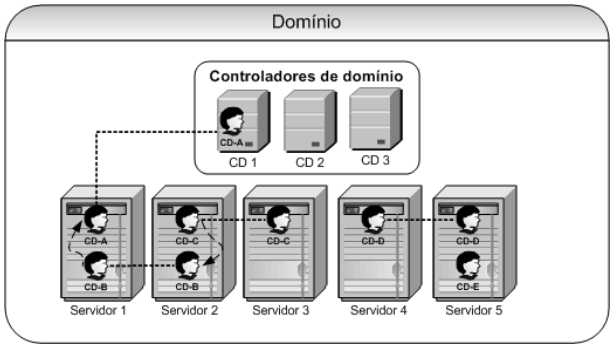
75 No Linux, ao utilizar o comando `service smb start` nas configurações padrão, são lidas as configurações do arquivo `etc/smb.conf` e o servidor samba é inicializado. Para conferir se o serviço está funcionando normalmente deve-se conferir se a porta `149/tcp netbios-ssn` está ativa.

Acerca de recuperação de bancos de dados e de tecnologias de bancos de dados, julgue os itens a seguir.

76 O PL/SQL é uma extensão da Oracle para o padrão SQL. Com o uso do PL/SQL podem-se criar funções, *triggers*, objetos, *strored procedures* e as funcionalidades da linguagem podem ser extendidas com *procedures* externos.

77 O PostgresSQL utiliza o modelo cliente/servidor. Uma sessão *postgress* consiste dos seguintes processos: um *postmaster* ou *daemon* supervisor, uma aplicação *frontend* do usuário e o processo de coleta do banco de dados do servidor.

78 A Oracle permite que sejam definidas marcas, denominadas *savepoints*, a fim de possibilitar um *rollback* de apenas partes da transação. Essas marcas são especificadas com a utilização do comando *savepoint*. O *rollback* desfaz a transação até o útlimo *savepoint* criado.



Internet:<www.microsoft.com/brasil/security/guidance/servaccount/sspgch02.mspx>.

Com base na figura acima, que exemplifica um domínio de servidores Windows e considerando que: a conta A tem privilégios equivalentes a administrador em mais de um controlador de domínio; as contas A, B, C e D têm privilégios equivalentes a administrador em mais de um servidor membro e; a conta E tem privilégios equivalente a administrador em apenas um único servidor membro, julgue os itens seguintes.

79 É considerarada uma situação de vulnerabilidade do domínio quando a conta A estiver executando um serviço no Servidor 1 e depois que a senha da Conta A for descoberta no Servidor 1, o usuário tiver acesso ao CD 1. Isso acontece pois a conta A tem privilégios equivalentes a administrador em um controlador de domínio para executar serviços em um servidor membro.

80 É considerada uma vulnerabilidade do domínio quando a conta E estiver executando um serviço no Servidor 5 e, depois que a senha da conta E for descoberta no servidor, o usuário tiver acesso a todos os servidores membros nos quais a conta E possuir privilégios.

Acerca de segurança em redes, controle de *logs* e políticas de *backup* de ativos de rede, julgue os itens seguintes.

81 Um ataque comum para os usuários que se conectam em servidores de IRC e que possuem um *firewall* pessoal é que alguns servidores maliciosos enviam para a máquina do cliente conexões que checam a existência de *proxies*, de forma a invadir os diretórios pessoais do usuário. O uso do *firewall* permite que essas conexões sejam apontadas como possíveis ataques.

82 Nos servidores Windows, o log de eventos permite monitorar informações sobre segurança e identificar problemas de *software*, *hardware* e sistema. Existem 3 tipos de *logs*: o *log* de sistema, que armazena os eventos registrados por componentes do Windows, por exemplo carregamento de um *driver*; o *log* de aplicativo, que armazena os eventos registrados por aplicativos ou programas, e o *log* de administração, que registra eventos de uso do servidor, tais como tentativas de *logon* válidas e inválidas, entre outros.

83 Um *backup* incremental captura todos os dados que foram alterados desde o *backup* total ou incremental mais recente. Deve-se usar uma fita de *backup* total e todos os conjuntos de *backups* incrementais subseqüentes para restaurar um servidor sem importar com o tempo de criação desses *backups*.

84 Atualmente, a maioria dos vírus ainda é detectada por meio de assinaturas. A pesquisa por assinatura é variável conforme o antivírus. Dá-se o nome de falso positivo a um alarme falso gerado pelo antivírus, isto é, quando um erro na lista de definição faz que o programa marque arquivos limpos e seguros como infectados.

85 O *DocBook* é um DTD (*document type definition* — definição de tipo de documento) que se baseia em uma linguagem de marcação definida em SGML/XML e é recomentada pela TLDP (*the* Linux *documentation project*), entidade que padroniza a documentação em sistemas Linux.

Acerca do Dynamic Host Configuration Protocol (DHCP), que provê parâmetros de configuração para hospedeiros (*hosts*) da Internet, julgue os itens seguintes.

86 O formato das mensagens DHCP tem base no formato das mensagens BOOTP, o que permite a interoperabilidade dos clientes BOOTP com os servidores DHCP.

87 O DHCP é um protocolo sem a noção de estado (*stateless*), tendo uma operação com base em um par único de mensagens pergunta-resposta, para cada parâmetro a ser configurado.

88 Um administrador de rede pode escolher como configurar os servidores DHCP para responder somente a clientes que tenham sido previamente registrados por meio de algum mecanismo externo ao protocolo.

89 O protocolo DHCP usa o *user datagram protocol* (UDP) como seu protocolo de transporte, com as mensagens DHCP de um cliente sendo enviadas para a porta DHCP Server (67) de um servidor e as mensagens DHCP de um servidor para a porta DHCP client (68) de um cliente.

90 O servidor DHCP tem a funcionalidade opcional de, ao configurar um cliente, registrar o endereço deste junto ao *domain name system* (DNS).

O Windows Internet Naming Service (WINS) é a implementação da Microsoft de um NetBIOS Name Server (NBNS). Acerca dos protocolos subjacentes a essa implementação e das funcionalidades que ela provê, julgue os itens seguintes.

91 Cada nodo NetBIOS deve possuir apenas um nome que é adquirido dinamicamente através de procedimentos de registro.

92 Os nomes mantidos por um NBNS recebem uma duração de vida durante o registro de nome, de modo que o NBNS vai considerar que um nome foi liberado silenciosamente caso o nodo proprietário falte com o envio de uma mensagem relembrando (*refresh*) ao NBNS antes que a duração de vida expire.

93 Um identificador de escopo, que é aposto a cada nome NetBIOS, emprega o conjunto de caracteres restrito do DNS e possui um ponto como primeiro caractere, o que faz o nome NetBIOS, junto com o identificador de escopo, ser um nome válido no DNS.

Acerca do protocolo de roteamento open shortestpPath first (OSPF) para redes TCP/IP, julgue os itens a seguir.

94 Em um sistema autônomo OSPF, cada roteador tem a possibilidade de executar seu próprio algoritmo de roteamento, podendo o resultado obtido por um roteador servir em série para entrada no algoritmo de outro roteador.

95 Quando várias rotas de igual custo existem para uma destinação, o tráfego é distribuído igualmente entre tais rotas pelo OSPF.

96 Para proteger a rede contra a disseminação de falsas rotas, os roteadores OSPF bloqueiam o anúncio de dados de roteamento derivados do ambiente externo ao sistema autônomo, o que inclui rotas aprendidas de um protocolo do tipo *exterior gateway protocol*.

97 O protocolo Hello é a parte do OSPF usada para estabelecer e manter relacionamentos de vizinhança, podendo inclusive prover a descoberta dinâmica de roteadores vizinhos caso a rede permita a difusão de mensagens (*broadcast*).

98 Embora o cabeçalho básico do pacote OSPF careça de um campo de autenticação, esse cabeçalho tem um mecanismo de extensão que possibilita apor ao pacote dados contendo um campo de tipo de autenticação e um campo associado para dados do esquema de autenticação escolhido.

99 O anúncio de estados de enlaces — *link state advertisement* LSA — é uma unidade de dados que armazena os dados de todos os roteadores coletados por um roteador OSPF, permitindo assim o cálculo das rotas mais curtas.

Os protocolos IP, TCP e UDP são os pilares da interconexão de redes Internet e do transporte fim-a-fim de dados nessas redes. Acerca desses protocolos e de outros protocolos associados que formam a arquitetura TCP/IP, julgue os itens seguintes.

100 O campo de carga útil do IP pode carregar dados que não serão passados à camada de transporte.

101 Um endereço IP v4 está tecnicamente associado com um hospedeiro ou roteador e serve como identificador único para tal hospedeiro ou roteador.

102 Para evitar uma grande quantidade de repasses de fragmentos de datagramas, um roteador IP v4, se possuir uma interface de sub-rede adequada para o repasse, procura recompor o pacote IP a partir de fragmentos recebidos para, então, repassar o pacote adiante com apenas uma nova transmissão.

103 O mecanismo de controle de congestionamento do protocolo TCP tem base no uso de realimentação proveniente da camada de rede, especificamente aquela composta por informações da mensagem de redução de fonte do Internet Control Message Protocol (ICMP).

104 O procedimento denominado apresentação de três vias (*three way handshake*) consiste do envio de três mensagens idênticas de um hospedeiro para outro usando o protocolo TCP, de modo que o receptor pode verificar a taxa de chegada e a taxa de erros das mensagens, antes de iniciar uma conexão com o emissor.

105 Quando um hospedeiro TCP recebe uma solicitação de conexão para uma porta, mas não está aceitando conexões para tal porta, então o hospedeiro responde enviando um segmento TCP com o *bit* RST ajustado para 1.

106 O campo de janela de recepção do TCP é usado para indicar o número de *bytes* que um destinatário está disposto a aceitar.

107 A ausência de procedimento de estabelecimento de conexão é uma das razões que explicam a utilização do UDP para várias aplicações, inclusive as atividades de monitoramento da gerência de redes pelo Simple Network Management Protocol (SNMP).

108 Um acordo de segurança (*security association*) do protocolo de segurança IP (IPsec) consiste de uma relação bidirecional entre dois roteadores IP, necessária para estabelecer conexões TCP através desses roteadores, de modo a oferecer serviços de autenticação e confidencialidade das conexões TCP, necessários à formação de redes privadas virtuais (*virtual private networks* (VPN) fim-a-fim.

109 O protocolo de encapsulamento de carga útil — *encapsulation security payload* (ESP) — fornece os serviços de autenticação, integridade de dados e confidencialidade que, no contexto de IPsec, permitem a formação de redes privadas virtuais entre entidades operando na camada de rede IP.

Acerca dos serviços providos pelas aplicações em redes TCP/IP e dos protocolos a elas associados, julgue os itens subseqüentes.

110 Quando um usuário inicia uma transferência de arquivo pelo *file tranfer protocol* (FTP) o lado cliente estabelece uma conexão de dados TCP para o lado servidor e solicita por essa conexão a transferência de exatamente um arquivo, de modo que o cliente fecha tal conexão assim que a transferência terminar.

111 Ao receber uma mensagem de correio eletrônico, o servidor Simple Mail Tranfer Protocol (SMTP) destinatário acrescenta uma linha de cabeçalho *received:* ao topo da mensagem, indicando nessa linha o nome do servidor que enviou a mensagem, o do que recebeu a mensagem e o horário em que recebeu a mensagem.

112 O Post Office Protocol versão 3 (POP3) é um protocolo de acesso de correio eletrônico que permite a um agente de correio eletrônico, não apenas recuperar mensagens em um servidor, como também criar pastas e designar mensagens a pastas desse servidor.

113 Um *cache web*, ou servidor *proxy web*, é uma entidade que atende requisições *hypertext transfer protocol* (HTTP) em nome de um servidor de correio eletrônico SMTP, de modo que um agente de usuário do correio consegue acessar o servidor via um navegador *web*.

114 Em uma cadeia de consultas, quando um servidor de nomes recebe uma resposta DNS, tal servidor pode fazer cópia das informações dessa resposta em sua memória local (*cache*), de modo que se outra consulta chegar a esse servidor e for referente a informações nele armazenadas, então esse servidor poderá enviar ele mesmo a resposta mesmo que não tenha autoridade para o nome consultado.

115 Em um registro de recurso armazenado por um servidor DNS, o campo de tipo A indica que os correspondentes campos de nome e valor contém respectivamente um nome de hospedeiro e o endereço IP para esse hospedeiro.

Acerca dos aspectos de segurança em sistemas de informação e redes TCP/IP, julgue os próximos itens.

116 Uma das proteções clássicas para senhas de usuários em sistemas da família Unix consiste em cifrar as senhas acrescidas de um parâmetro *salt*, embora isso possa gerar senhas duplicadas visíveis no arquivo de senhas.

117 Um vírus metamórfico faz mutação a cada infecção, podendo tanto mudar de comportamento quanto de aparência.

118 Em um ataque negação de serviço por refletor — *reflector distributed denial of service* (*DdoS*) — entidades escravas do atacante constroem pacotes que requerem respostas e contém o endereço IP do alvo como endereço fonte no cabeçalho, de modo que ao serem enviados a computadores não infectados, os refletores, tais pacotes provocam respostas direcionadas ao endereço alvo do ataque.

119 A abordagem de detecção de anomalias por contagem de eventos em intervalos de tempo, com indicação de alarme em caso de ultrapassagem de um limiar, é uma abordagem com baixo índice de falsos positivos e de falsos negativos na detecção de intrusão.

120 Um *firewall* é considerado uma boa proteção para ataques que envolvem colusões entre usuários internos da rede protegida e atacantes externos, pois o *firewall* tem a possibilidade de bloquear as comunicações entre eles.

PROVA DISCURSIVA

- Nesta prova, que vale **dez** pontos, faça o que se pede, usando o espaço para rascunho indicado no presente caderno. Em seguida, transcreva o texto para a **FOLHA DE TEXTO DEFINITIVO DA PROVA DISCURSIVA**, nos locais apropriados, pois **não será avaliado fragmento de texto escrito em local indevido**.
- Qualquer fragmento de texto além da extensão máxima de **trinta** linhas será desconsiderado.
- Na **folha de texto definitivo**, identifique-se apenas no cabeçalho da primeira página, pois **não será avaliado** texto que tenha qualquer assinatura ou marca identificadora fora do local apropriado.

Em um centro de informática, uma das ferramentas que podem ser ser utilizadas para documentar e elaborar tutorias, guias, *how-tos* e páginas de manual dos diferentes sistemas utilizados é o DocBook.

Tendo o fragmento de texto acima como referência inicial, redija um texto dissertativo acerca do seguinte tema.

O DocBook COMO FERRAMENTA PARA DOCUMENTAÇÃO

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

- fundamentos dos elementos/linguagens que compõem o DOCBOOK e suas características principais;
- formatos de documentos que podem ser criados/convertidos;
- vantagens da utilização do DocBook como ferramenta para documentação.

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	