

CONHECIMENTOS ESPECÍFICOS

A respeito do Windows Server 2012, julgue os itens a seguir.

- 51 O serviço DHCP (*dynamic host configuration protocol*), ao ser disponibilizado no Windows Server, tem a capacidade de atualizar dinamicamente serviços de DNS que estejam configurados para suportar essa atualização.
- 52 O *Active Directory* suporta o uso de controladores de domínio primário e de becape, de modo que um dos controladores lê e grava informações, ao passo que o outro somente lê.
- 53 No *file server*, é possível habilitar cópias de sombra de pastas compartilhadas, o que permite realizar a compressão de pastas e arquivos e mantê-los acessíveis ao usuário final.
- 54 O *print server* é capaz de gerenciar as filas de impressão e determinar permissões de segurança, além de impedir ou liberar o acesso de usuários às impressoras.
- 55 Em uma zona DNS, ao se utilizar o registro de recurso do tipo MX, informa-se o registro reverso de nome para endereço IP.

Julgue os próximos itens, acerca do ambiente Linux.

- 56 Em um *cluster* configurado com *heartbeat*, o arquivo de configurações globais é o *authkeys*.
- 57 Para que o processo de número 3.000 seja reiniciado, deve ser executado o comando `kill -HUP 3000`.
- 58 Ao ser executado o comando `su - oracle`, o usuário corrente será alterado para o usuário *oracle* e o ambiente do usuário corrente será transferido para o usuário *oracle*.
- 59 O EXT4 suporta sistema de arquivos de um *exabyte* e possui *checksum* de jornal.
- 60 Em um *script shell*, se o retorno do último comando obtido pela variável interrogação (?) for igual a 1, então o comando teve sucesso na sua execução.

A respeito de virtualização de servidores, julgue os itens subsequentes.

- 61 O R2 Hyper-V, do Windows Server 2012, suporta NUMA — acesso não uniforme à memória — dentro de uma máquina virtual e é, portanto, compatível com a arquitetura de sistemas de multiprocessadores.
- 62 A versão atualizada do VHD (*virtual hard disk format*) do Windows Server 2012 Hyper-V é o VHDX, que suporta até 64 *terabytes* de armazenamento por disco virtual e tem registro interno que captura atualizações para os metadados do arquivo de disco rígido virtual antes que elas sejam gravadas no seu local final.
- 63 No trabalho com o sistema Xen 4, a necessidade que o Linux tem de armazenar os metadados da memória do sistema é um motivo para se recomendar a reserva de quantidade fixa de memória para Dom0 (*domain zero*).
- 64 No Xen 4, o comando `xentop` exhibe informações sobre o sistema Xen em tempo real e de forma contínua.
- 65 Na paravirtualização, quando uma instrução é executada, são alterados tanto o sistema convidado como as instruções de usuário, as quais são executadas diretamente sobre o processador nativo.

Acerca dos servidores de aplicação e da Web, julgue os itens subsequentes.

- 66 Quanto aos três modelos de serviços de *cloud*, é correto afirmar que o IaaS fornece recursos computacionais (*hardware* ou *software*) para o PaaS, que, por sua vez, fornece recursos e ferramentas para o desenvolvimento e a execução de serviços a serem disponibilizados como SaaS.
- 67 A plataforma Web JBoss Enterprise 5.0 usa *microcontainers* para integrar serviços corporativos, juntamente com *containers* Servlet/JSP e EJB, mas a necessidade de utilização de construtor com argumentos impede que esses *microcontainers* lidem com POJOs (*plain old Java objects*).
- 68 No IIS 7, cada aplicativo deve contar com, no mínimo, um diretório virtual que mapeie o aplicativo para o diretório físico em que o conteúdo do aplicativo esteja contido.
- 69 O `mod_jk` — um módulo Apache projetado para permitir o encaminhamento de pedidos do servidor Apache para recipientes *servlet* — gerencia o balanceamento de carga em chamadas HTTP para um conjunto de recipientes *servlet*, a exemplo do JBoss.
- 70 A computação em GRID, que acopla recursos heterogêneos distribuídos, oferece suporte à execução de aplicações paralelas que podem ser acessadas independentemente de sua posição física.

Com relação a colaboração e mensageria, julgue os itens que se seguem.

- 71 A unificação de mensagens do Microsoft Exchange Server 2010 combina mensagem de voz e *email* em uma caixa de entrada que pode ser acessada a partir do telefone e do computador.
- 72 O SharePoint Server 2010 oferece suporte a dois tipos de modos de autenticação: o clássico e o embasado em declarações. No primeiro caso, o SharePoint Server 2010 trata todas as contas de usuário como contas do ADDS (serviços de domínio do Active Directory). O segundo tem como base o WIF (*Windows identity foundation*), que é um conjunto de classes do .NET Framework usadas para implementar a identidade com base em declarações.
- 73 O Postfix 2.8 pode ser configurado para ser utilizado juntamente com o SGBD MySQL em servidores que utilizam Linux Debian. Os recursos com essa configuração incluem a implantação de múltiplos servidores de banco de dados MySQL, o que resultaria em maior disponibilidade de acesso em caso de falha em algum desses servidores.
- 74 O Postscreen — recurso presente no Postfix 2.8 — destina-se a proteger o usuário contra uma sobrecarga de processamento do servidor de *email*, bloqueando conexões provenientes de *zumbis* e outros *spambots*.
- 75 Apesar de o Postfix 2.8 não suportar exames de cabeçalho e de corpo da mensagem antes de esta ser armazenada na fila Postfix, é possível filtrar e controlar a entrada de *spam* com a análise de conteúdo e de cabeçalho após a mensagem ser inserida em sua fila.
- 76 No Microsoft Exchange Server 2010, federação é uma tecnologia usada para a gestão de grupos de usuários, que são integrados a serviços de LDAP, o que permite que as contas de usuários sejam administradas e organizadas por meio de uma estrutura de árvores.
- 77 O Microsoft Exchange Server 2010 suporta o IPv6 mesmo quando o IPv4 não é usado, uma vez que há suporte a um ambiente de IPv6 puro.

A respeito de banco de dados, julgue os itens que se seguem.

78 Considere que haja necessidade de se criar uma tabela T1 com uma coluna do tipo ENUM que armazene uma lista permitida de dados em formato *string*. Suponha ainda que essa operação deva ser feita no Mysql 5.7. Nesse caso, o comando a ser dado seria o seguinte:

```
CREATE TABLE T1 ( COL1 ENUM('1', '2', '3') );
```

79 A conexão com o PostgreSQL 9.3 é realizada, por padrão, na porta TCP 5432. Uma das configurações de segurança permitida é o acesso por meio de SSL que é `true`, por padrão, e é aceito, neste caso, com o uso dos protocolos TCP, IP ou NTP.

80 É válida para o PostgreSQL 9.3, mas não para o SQL Server 2012, a criação da SEQUENCE `seqa` por meio do seguinte comando:

```
CREATE SEQUENCE seqa START WITH 1;
```

81 Os índices do tipo B-tree são suportados tanto pelo PostgreSQL 9.3 quanto pelo MySQL 5.7, com exceção, nesse último caso, para tabelas do tipo MyISAM, que aceitam os tipos `Fulltext` e `hash`, mas não suportam B-tree.

82 O PostgreSQL 9.3, ao gerenciar o controle de concorrência, permite o acesso simultâneo aos dados. Internamente, a consistência dos dados é mantida por meio do MVCC (*multiversion concurrency control*), que impede que as transações visualizem dados inconsistentes.

83 No processo de *Data Mining* (mineração de dados), é indispensável o uso de técnica conhecida como *Data Warehousing*, uma vez que a mineração de dados deve ocorrer necessariamente em estruturas não normalizadas (FN0).

84 O *Data Warehouse* tem como principal objetivo armazenar dados históricos por meio dos esquemas *snow flake* ou *star schema*. O primeiro armazena os dados em dimensões que podem não estar ligadas diretamente à tabela fato; o segundo é voltado para armazenamento de dados não estruturados ou textuais.

85 Para a alteração do nome da coluna do tipo INTEGER de X para Y sem se alterar seu tipo, deve ser dado o seguinte comando do Mysql 5.7:

```
ALTER TABLE T CHANGE X Y INTEGER;
```

Julgue os itens de 86 a 90 a respeito das normas ISO/IEC 27001 e ISO/IEC 27002 e do sistema de gestão de segurança da informação (SGSI).

86 Estabelecer o plano de metas, os prazos para execução e os custos estimados é atividade da fase de planejamento do ciclo da metodologia do SGSI e comunicações proposta pela Norma Complementar n.º 02/IN01/DSIC/GSIPR.

87 A norma ISO 27002 recomenda que as chaves criptográficas usadas para as assinaturas digitais de documentos eletrônicos sejam idênticas àquelas usadas para a criptografia desses documentos: a padronização das chaves garante maior segurança aos documentos.

88 Na norma ISO 27001, recomenda-se que, no contexto da ação preventiva, a organização identifique tanto alterações nos riscos quanto os consequentes requisitos de ações preventivas, especialmente no que diz respeito aos riscos que tenham sofrido alterações significativas.

89 Segundo a Norma Complementar n.º 08/IN01/DSIC/GSIPR, além do serviço de tratamento de incidentes de segurança em redes de computadores, a equipe de tratamento e respostas a incidentes de segurança em redes computacionais pode oferecer à sua comunidade outros serviços, como tratamento de artefatos maliciosos, emissão de alertas e advertências e monitoração de novas tecnologias.

90 De acordo com a Norma Complementar n.º 06/IN01/DSIC/GSIPR, o programa de gestão de continuidade de negócios de órgão ou entidade da administração pública federal deve ser composto, no mínimo, pelos planos de gerenciamento de incidentes, de continuidade de negócios e de recuperação de negócios.

Acerca das tecnologias de segurança e dos ataques eletrônicos, julgue os itens a seguir.

91 Os ataques de SQL Injection do tipo *code injection* se caracterizam por tentar modificar um comando SQL já existente mediante a adição de elementos à cláusula WHERE ou a extensão do comando SQL com operadores como UNION, INTERSECT ou MINUS.

92 O ataque de *spear phishing*, que é uma tentativa de fraude por falsificação de *email*, tem como alvo uma organização específica e objetiva, normalmente, conseguir acesso não autorizado a dados sigilosos.

93 O controle de acesso embasado em portas permite ao administrador restringir o uso da rede local a tráfego seguro entre dispositivos autenticados e autorizados. O padrão IEEE 802.1x especifica a arquitetura, os elementos funcionais e os protocolos que suportam a autenticação mútua entre os clientes da mesma rede local e a comunicação segura entre as portas a que se conectam os dispositivos.

94 O algoritmo de criptografia AES (*advanced encryption standard*) opera em quatro estágios: um de permutação e três de substituição. O estágio de permutação *ShiftRows* é reversível e os estágios de substituição *SubBytes*, *MixColumns* e *AddRoundKey* são não-reversíveis.

95 Para que a criptografia de chave pública seja considerada segura, uma das premissas é que o conhecimento do algoritmo, o conhecimento de uma das chaves e a disponibilidade de amostras de texto cifrado sejam, em conjunto, insuficientes para determinar a outra chave.

96 Uma das propriedades de uma função de *hash*, conhecida como resistência à primeira inversão ou propriedade unidirecional, garante que, dada uma mensagem, não é possível encontrar uma mensagem alternativa que gere o mesmo valor de *hash* da mensagem original.

Com relação a políticas de segurança da informação, julgue o próximo item.

97 A política de segurança da informação deve conter diretivas da alta gerência da organização e propor a criação de um programa de segurança da informação para a organização.

Acerca da infraestrutura de chaves públicas ICP-Brasil, julgue o item abaixo.

98 A assinatura eletrônica vinculada a um certificado emitido no âmbito da ICP-Brasil tem função específica e restrita de determinar a não violação do conteúdo de um documento assinado eletronicamente, e não conduz à presunção de autenticidade do emissor do documento subscrito.

No tocante a protocolos, serviços, padrões e topologias de redes, julgue os itens subsequentes.

- 99 No protocolo IPv6, não existe endereço *broadcast*, normalmente responsável por direcionar um pacote para todos os nós de um mesmo domínio. Nesse protocolo, essa função é atribuída a tipos específicos de endereços *multicast*.
- 100 Na estrutura hierárquica de funcionamento do serviço DNS, ao receber uma requisição para resolução de nome, o servidor local de nomes DNS verifica se o nome está no *cache* DNS local ou se consta do seu banco de dados. Se o encontrar, retorna o endereço IP correspondente ao solicitante; caso contrário, o servidor DNS local repassa a consulta a um servidor DNS de nível mais alto.
- 101 A topologia lógica de interconexão de uma rede corporativa complexa precisa refletir a topologia física dessa rede, de modo que os requisitos de segurança lógica da rede sejam de implementação direta a partir dos aspectos da segurança física das instalações de TI da organização.
- 102 Em redes padrão Gigabit Ethernet, é possível implementar níveis de classes de serviços (CoS) e qualidade de serviço (QoS) por meio da combinação de padrões auxiliares como IEEE 802.1p (manipulação de prioridades dos dados em um dispositivo da subcamada MAC), IEEE 802.3x (controle de fluxo duplex completo), IEEE 802.1q (graus de prioridade) e IETF RSVP (reserva de largura de banda).
- 103 A versão 2 do protocolo de gerência de rede SNMP (SNMPv2) é incompatível com a versão 1 (SNMPv1). Os formatos das mensagens são diferentes e há dois novos tipos de mensagens na SNMPv2 que não existem na SNMPv1: GetBulk e Inform.
- 104 Os pacotes da camada IP não seguem circuitos virtuais nem qualquer outro tipo de orientação sinalizada ou direcionamento predefinido para o fluxo dos pacotes, como acontece em outras tecnologias de redes em camadas.

A respeito do analisador de protocolos Wireshark, julgue o item abaixo.

- 105 O administrador de rede pode configurar o analisador de protocolos Wireshark no modo IDS de detecção de tráfego malicioso para incluir regras e configurar assinaturas de ataques específicos de rede que devem ser monitorados.

No que diz respeito à telefonia e aos serviços multimídia, julgue os itens que se seguem.

- 106 Nas redes VoIP, o padrão H.323 codifica as mensagens em um formato ASCII, sendo este adequado para conexões de banda larga.
- 107 Vazão — parâmetro que indica a taxa de transmissão efetiva dos dados em *bits* — é um requisito básico para aplicações multimídia distribuídas.
- 108 No modelo de referência OSI, assim como no IP, o protocolo SIP (*session initiation protocol*) se situa na camada de rede e pode funcionar sobre o UDP ou o TCP.
- 109 A recomendação POLQA (*perceptual objective listening quality assessment*), definida pelo ITU-T, pode ser aplicada para a análise da qualidade da voz em comunicações que utilizam a tecnologia VoLTE (*voice over LTE*).

Com relação aos sistemas de armazenamento de redes de comunicação, julgue os próximos itens.

- 110 A função zoneamento (*zoning*) em SAN pode ser classificada em três tipos: *WWN zoning*, *soft zoning* e *hard zoning*. Em uma *soft zoning*, a informação da zona deve ser atualizada sempre que o administrador realizar qualquer mudança nas portas de um *switch*.
- 111 Uma SAN pode ter sua capacidade de armazenamento aumentada de maneira quase ilimitada. Entretanto, o comprimento dos cabos de fibra óptica deve ser limitado a, no máximo, 100 metros, para que não haja comprometimento do *throughput*.
- 112 A tecnologia Fibre Channel (FC), utilizada em armazenamento de dados em rede, define uma estrutura de cinco camadas para o transporte de dados, as quais são codificadas em uma sequência numérica de 0 a 4, na forma FC-0 a FC-4. O Fibre Channel Protocol é implementado na camada FC-4.
- 113 O Fibre Channel over Ethernet (FCoE) foi desenvolvido para permitir que o tráfego FC seja transmitido através da rede Ethernet. O fato de os tráfegos do protocolo FC nunca serem segmentados é uma característica importante do encapsulamento.
- 114 SAN (*storage area network*) é uma rede de armazenamento de dados de alto desempenho que se comporta como se fosse uma única unidade de armazenamento, mesmo que possua um *array* com centenas de discos iSCSI.

Acerca da tecnologia de redes, protocolos e serviços IP, julgue os itens a seguir.

- 115 O padrão IEEE 802.11ac, que pertence à nova geração da tecnologia de redes sem fio, especifica a faixa de 2,4 GHz para operação e permite a transferência de dados com velocidade de até 1 Gbps.
- 116 Em VPNs, PPTP, L2TP e IPsec são exemplos de protocolos usados em um tunelamento em nível 2.
- 117 Um dos avanços significativos do protocolo IPv6 com relação ao IPv4 é o suporte à autoconfiguração automática de endereços IP, o que torna o uso de servidor DHCP totalmente desnecessário.

Julgue os itens seguintes, com relação às políticas de backup e recuperação de dados.

- 118 O uso de *snapshot* é ideal como complemento aos backups granulares de arquivos, sendo possível voltar a imagem inteira de um sistema para um ponto anterior no tempo caso o sistema necessite ser restaurado.
- 119 Uma das características da solução de backup Symantec NetBackup é a tecnologia de recuperação granular para máquinas virtuais, que permite que o conteúdo dos arquivos seja indexado e restaurado sem que haja necessidade de recuperar toda a máquina virtual.
- 120 A técnica de deduplicação de dados na origem, ou seja, quando o backup está sendo realizado, é mais indicada para grandes volumes de dados.

PROVA DISCURSIVA

- Nesta prova, tanto na dissertação como nas questões, faça o que se pede, usando os espaços para rascunho indicados no presente caderno. Em seguida, transcreva os textos para o **CADERNO DE TEXTOS DEFINITIVOS DA PROVA DISCURSIVA**, nos locais apropriados, pois **não serão avaliados fragmentos de texto escritos em locais indevidos**.
- Tanto na dissertação como nas questões, qualquer fragmento de texto além da extensão máxima de linhas disponibilizadas será desconsiderado.
- No **caderno de textos definitivos**, 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 cada parte dessa prova, ao domínio do conteúdo serão atribuídos até **10,00 pontos**, dos quais até **0,50 ponto** será atribuído ao quesito apresentação (legibilidade, respeito às margens e indicação de parágrafos) e estrutura textual (organização das ideias em texto estruturado).

DISSERTAÇÃO

No mercado atual, as empresas devem atender a um público global em curto prazo de tempo. Essa disponibilidade constante para clientes e funcionários impõe ainda mais pressão sobre a plataforma de dados da empresa. As empresas não apenas precisam da disponibilidade próxima de 100% para proteger seus negócios, mas também de suporte para garantir a confiança e a segurança. Ademais, cada vez mais as organizações precisam de uma plataforma de *business intelligence* (BI) flexível e segura para oferecer autoatendimento aos usuários finais e ferramentas de tecnologia da informação poderosas, para lidar rapidamente com dados e necessidades comerciais dinâmicas.

Internet: <www.microsoft.com> (com adaptações).

Considerando que o fragmento de texto acima tem caráter unicamente motivador, redija um texto dissertativo acerca das soluções e ferramentas agregadas ao Microsoft Sql Server 2012 e voltadas para alta disponibilidade e BI. Ao elaborar seu texto, aborde, necessariamente, os seguintes tópicos:

- ▶ *analysis services*: objetivos e abordagens de BI (tabular, multidimensional e PowerPivot); [valor: 2,50 pontos]
- ▶ *Data Mining* (SSAS): objetivos e recursos integrados; [valor: 2,00 pontos]
- ▶ *AlwaysOn availability groups*: objetivos e componentes; [valor: 2,50 pontos]
- ▶ *log shipping* e *failover cluster instances*: objetivos e principais características. [valor: 2,50 pontos]

RASCUNHO – DISSERTAÇÃO

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	

QUESTÃO 1

Discorra sobre o gerenciamento de processos no ambiente do sistema operacional Linux, atendendo, necessariamente, ao que se pede a seguir:

- ▶ conceitue o processo e o mecanismo de envio de sinais para o comando `kill`; [valor: 3,00 pontos]
- ▶ cite três estados do processo ativos no sistema operacional Linux; [valor: 2,50 pontos]
- ▶ indique as funções de cada um dos comandos `ps`, `nice` e `renice`. [valor: 4,00 pontos]

RASCUNHO – QUESTÃO 1

1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	

QUESTÃO 2

Discorra sobre os ataques DDoS, abordando, necessariamente,

- ▶ as características dos principais tipos de ataques DDoS, seus modos de operação e tendências; [valor: 4,00 pontos]
- ▶ as ações de governança, as medidas, os procedimentos e as soluções técnicas que reduzem o impacto de tentativas de ataques DDoS e evitam a indisponibilidade dos serviços da organização na Internet. [valor: 5,50 pontos]

RASCUNHO – QUESTÃO 2

1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	

QUESTÃO 3**ANATEL multa Telexfree por operar sem autorização**

A empresa TelexFree pagou multa à ANATEL por prestação não autorizada de serviços de telecomunicações. Segundo a ANATEL, para comercializar planos de minutos de voz sobre protocolo de Internet (VoIP), a Telexfree precisa de autorização de prestação e exploração do Serviço de Comunicação Multimídia (SCM). O descumprimento resultou na abertura de processo administrativo. A empresa foi notificada no dia 13 deste mês e já pagou a multa. A Telexfree não tem nenhum tipo de autorização da ANATEL e aguarda o processo de anuência prévia para a compra da empresa Simtinternet, que já tem uma autorização de SCM na agência.

Internet: <www.economia.terra.com.br> (com adaptações).

É hora de rever a regulamentação da oferta de VoIP

Ao participar do Mobile World Congress, em Barcelona, o ministro das Comunicações sustentou que a oferta de serviços de voz por empresas como a Viber, Twitter e Facebook, por meio do WhatsApp, exige que o Brasil repense e reformule a sua própria legislação. Hoje, as concessionárias não podem prestar VoIP, por conta das metas de qualidade impostas ao STFC. "A tecnologia andou e muito rápido. Precisamos repensar", disse o ministro.

Ana Paula Lobo. **Convergência Digital**. In: Internet: <www.convergenciadigital.uol.com.br> (com adaptações).

Considerando que os fragmentos de textos acima têm caráter unicamente motivador, discorra acerca da tecnologia VoIP. Ao elaborar seu texto, aborde, necessariamente,

- ▶ a regulamentação, pela ANATEL, da tecnologia VoIP; [valor: 5,00 pontos]
- ▶ as ameaças e vulnerabilidades em VoIP (exposição de dois exemplos). [valor: 4,50 pontos]

RASCUNHO – QUESTÃO 3

1	
2	
3	
4	
5	
6	
7	
8	
9	
10	
11	
12	
13	
14	
15	



 **cespeUnB**

 **Cebraspe**
Centro Brasileiro de Pesquisa em
Avaliação e Seleção e de Fomento de Eventos