

## CONHECIMENTOS ESPECÍFICOS

Acerca dos sistemas operacionais Windows e Linux, julgue os itens a seguir.

- 51 Em uma rede que possua um servidor controlador de domínio Windows, deve-se, para incluir as estações de trabalho dessa rede nesse domínio, permitir ao menos a um usuário o direito de administração no servidor controlador de domínio.
- 52 No Linux, a execução do comando `du -h` permite visualizar se um ponto de montagem está com suporte à leitura e gravação.
- 53 Para limpar a *cache* de consultas DNS (*Domain Name Server*) em um computador com sistema operacional Windows, deve-se executar o comando `ipconfig/flushdns`.
- 54 Para exibir as últimas 20 linhas de um arquivo, em Linux, com nome teste.txt, é necessário executar o comando `head -20 teste.txt`.

A respeito do banco de dados SQL Server e da linguagem SQL, julgue os itens seguintes.

- 55 O comando `SELECT GETDATE()` recebe como retorno a data e a hora atual do sistema operacional. Para se retornar um usuário qualquer conectado a uma base de dados, deve-se executar o comando `SELECT SYSTEM_ADMIN`.
- 56 Ao se executar o comando `SELECT ROUND(2.1234, 1) AS Valor1`, obtém-se Valor1 2.1000 como resultado.

Julgue os próximos itens, acerca de MPLS (*Multiprotocol Label Switching*), BGP (*Border Gateway Protocol*) e OSPF (*Open Shortest Path First*).

- 57 O encaminhamento de pacotes pelo caminho mais curto e balanceamento do tráfego feito pelo OSPF é chamado de ECMP (*Equal Cost MultiPath*).
- 58 A MPLS encaminha os pacotes de acordo com endereço de destino contido no cabeçalho.

No que concerne a VPN (*Virtual Private Network*), julgue os itens subsequentes.

- 59 Em um filtro de pacotes que atue como *firewall* em uma rede por onde se verifique tráfego VPN IPSEC (*Internet Protocol Security*), é necessário liberar a porta 500 e o protocolo UDP (*User Datagram Protocol*) para o funcionamento da VPN.
- 60 O uso do protocolo AH (*Authentication Header*) no IPSEC (*Internet Protocol Security*) de uma VPN tem a função de garantir a confidencialidade dos dados trafegados.

Em relação a *firewall* e segurança de perímetro, julgue os itens a seguir.

- 61 Para que as estações de trabalho possam acessar a Internet, é desnecessário que um *firewall* de borda que possui a função de roteador e repassa todos os endereços originais da LAN para WAN mascare os endereços para trafegarem na WAN em uma rede com endereços privados de classe C.
- 62 Em um equipamento de *firewall* que utilize filtro de pacotes, para que seja possível bloquear tráfego HTTP que acesse páginas na Internet, é necessário restringir o tráfego no protocolo UDP (*User Datagram Protocol*) na porta 80.

Julgue o item que se segue, relativo a cabeamento estruturado.

- 63 Em uma rede local que utilize cabeamento padrão categoria 6, devem-se utilizar cabos com tamanho máximo de 50 metros para que a velocidade da rede seja mantida em 100 *Mbits* por segundo sem repetidores de sinal.

Com relação ao sistema operacional Windows Server, julgue os itens a seguir.

- 64 O sistema operacional Windows Server tem a capacidade de armazenar dados de usuários e senhas por meio do protocolo *kerberos* e de SSL, (*Secure Socket Layer*) utilizando o protocolo LDAP (*Lightweight Directory Access Protocol*) para criptografar pastas.
- 65 Por meio do comando `nslookup`, é possível executar consultas a servidores DNS e obter informações como o nome e o endereço IP (*Internet Protocol*) do servidor de correio eletrônico do domínio consultado.
- 66 O Windows Server possui um recurso, conhecido como DFS (*Distributed File System*), que consegue prover, entre dois *hosts*, um serviço que replica pastas e arquivos.

Acerca do sistema operacional Linux e do servidor de arquivos Samba, julgue os itens subsequentes.

- 67 No Samba, podem-se gerar *logs* customizados, incluindo-se variáveis na opção *log file* do arquivo de configuração (`smb.conf`). Para que seja possível separar os *logs* por nomes de *hosts*, utiliza-se a variável `%T`.
- 68 BASH (*Bourne Again Shell*) é um interpretador de comandos que pode ser utilizado no Linux.
- 69 Durante a instalação do sistema operacional Linux, no sistema de arquivos da partição raiz (`/`), um administrador de redes pode utilizar o sistema de arquivos `ext2`, que possui suporte a *journally*.
- 70 O Linux possui um recurso para agendamento de tarefas denominado Crontab, por meio do qual é possível programar que determinada tarefa seja automaticamente executada em um mesmo horário, em um único dia do mês, durante os doze meses do ano.
- 71 O serviço Samba, que pode ser utilizado como um servidor de arquivos, tem a capacidade de compartilhar arquivos em uma rede com clientes que consigam montar compartilhamentos utilizando CIFS (*Common Internet File System*).

Em relação ao protocolo TCP/IP (*Transfer Control Protocol/Internet Protocol*), julgue os itens a seguir.

- 72 O envio da *flag* SYN de um *host* para outro pode indicar o pedido de início de uma conexão TCP.
- 73 O protocolo ICMP (*Internet Control Message Protocol*), que trabalha na camada de enlace do TCP/IP, é utilizado por administradores de rede por meio do comando `ping`, disponível em sistemas operacionais Windows e Linux.
- 74 O HTTP é um dos protocolos que atuam na camada de transporte.

No que se refere a servidores de correio eletrônico e a *antispam*, julgue os próximos itens.

- 75 O comando RCPT TO especifica o endereço do remetente da mensagem de *email*.
- 76 Ferramentas de *antispam* são capazes de criar bases de conhecimento por meio de aprendizado com mensagens consideradas *spam* e utilizando o algoritmo Bayes.
- 77 Em uma conexão SMTP (*Simple Mail Transfer Protocol*) entre servidores de correio eletrônico, o comando EHLO é enviado para iniciar a conversa entre os servidores, juntamente com o nome do *host*.

Julgue os itens seguintes, que versam sobre RAID (*Redundant Array of Independent Disks*).

- 78 Em um arranjo de discos em RAID tipo 6, são necessários 3 discos para o arranjo, e não há suporte a discos de *spare*.
- 79 Em um arranjo de discos em RAID 5, é suportada a falha de até dois discos sem que sejam comprometidas a integridade e a disponibilidade dos dados armazenados.
- 80 Em um arranjo de RAID tipo 0 que utilize dois discos e tenha outro de *spare*, em caso de problemas com um dos discos do arranjo, é possível manter os dados íntegros e dois discos em funcionamento.

Julgue os itens a seguir, relativos a ataques a redes de computadores, prevenção e tratamento de incidentes.

- 81 *Phishing* é uma forma de ataque em que *crackers* tentam se passar por empresas ou por pessoa confiável, que agem por meio de uma comunicação eletrônica oficial, como um correio ou mensagem instantânea, para conseguir captar, às vezes ardilosamente, senhas e(ou) números de cartões de crédito.
- 82 Os vampiros (*vampires*), formas de ataque aos sistemas computacionais mais populares atualmente, são projetados para tomar ações maliciosas e, após infectar um sistema, excluir arquivos e provocar ataques a outros computadores a partir do computador infectado.
- 83 Uma das formas de barrar ataques às vulnerabilidades de sistemas é aplicar rotineiramente os *patches* disponibilizados pelos fabricantes de *software*.

Em consonância com as normas NBR ISO/IEC 27.001:2006 e 27.002:2005, julgue os itens seguintes quanto a classificação, controle de ativos de informação e gestão de políticas.

- 84 A segurança da informação envolve preservação da confidencialidade, da integridade e da disponibilidade da informação e é caracterizada adicionalmente por outras propriedades, como autenticidade, responsabilidade e confiabilidade.
- 85 No SGSI, devem-se identificar os riscos, buscando-se definir os ativos e seus proprietários, as ameaças, as vulnerabilidades que possam ser exploradas e os impactos que os ataques podem gerar.
- 86 Um evento de segurança da informação constitui uma etapa do ciclo PDCA (*plan-do-check-act*), que é aplicado para divulgar e capacitar todos os processos do sistema de gestão da segurança da informação (SGSI) para os colaboradores da instituição.

No que se refere à operacionalização do SGSI com base nas normas NBR ISO/IEC 27.009:2007, 27.001:2006 e 27.002:2005, julgue os itens que se seguem.

- 87 No plano de tratamento de riscos, deverão ser incluídas as considerações de financiamentos e atribuições de papéis e responsabilidades.
- 88 O monitoramento da eficácia dos controles, definido na NBR ISO/IEC 27.009:2007, define a eficácia dos controles ou grupos de controles selecionados e implementa o plano de tratamento de riscos com vistas a alcançar os objetivos de controle identificados.

Acerca da auditoria do SGSI segundo as normas NBR ISO/IEC 27.001:2006 e 27.002:2005, julgue os itens subsecutivos.

- 89 Um sistema de gestão da segurança da informação deverá proceder à condução de auditorias internas a intervalos planejados, para melhoria do processo.
- 90 As auditorias internas do SGSI são conduzidas pela própria organização para analisar os riscos residuais e os níveis de riscos aceitáveis.

No que se refere ao controle de acesso aos ativos com fundamento nas normas NBR ISO/IEC 27.001:2006 e 27.002:2005, julgue os itens seguintes.

- 91 Para a política de SGSI, todos os registros de acesso às informações deverão ser armazenados em meio eletrônico e criptografados para segurança, e os registros de incidentes de segurança da informação deverão ser guardados em sigilo.
- 92 Um dos requisitos de um SGSI é a rastreabilidade de decisões, que remeta a políticas e decisões da direção superior.

A respeito de plano de continuidade de negócios, planejamento do sistema de gestão de riscos, processo de gestão de risco e etapa de identificação de controles, julgue os seguintes itens.

- 93 O escopo de um plano de gerenciamento de riscos, aplicado a métodos e a processos e ligado ao local da declaração que introduz no processo, refere-se à região da empresa em que é utilizável.
- 94 A etapa de identificação de controles envolve a determinação dos responsáveis pelos ativos e o envio dos comandos de controle de incidentes para que sejam tomadas as medidas pertinentes.
- 95 No processo de gestão de riscos, a identificação das consequências pressupõe a análise do risco de uma consequência, que, por sua vez, poderá redundar em perda de eficácia e instabilidade no funcionamento de sistemas e perda de oportunidade de negócios, entre outras.
- 96 A identificação do ativo, que representa elemento com valor para o empreendimento que necessita de proteção, é uma etapa fundamental ao processo de gestão de riscos.
- 97 O plano de continuidade de negócios descreve como a instituição enfrentará situações não previstas pelo controle do risco.

Com fundamento nas definições da gestão de riscos segundo as normas NBR ISO/IEC 15.999-1:2007 (versão corrigida 2008) e 27.005:2005, julgue os itens subsequentes.

- 98 No âmbito da gestão de riscos, a estimativa de riscos atribui valores à probabilidade e às consequências de um risco.
- 99 As consequências de riscos na saúde ou na vida dos envolvidos estão excluídas das referidas normas, já que envolvem processos afetos ao Ministério da Saúde e ao Ministério do Trabalho e Emprego acerca da segurança e do bem-estar no ambiente de trabalho.
- 100 Segundo a gestão de riscos, entende-se que vulnerabilidade é o evento ou incidente, ao passo que ameaça é a fragilidade que será explorada para que a vulnerabilidade se torne concreta.

Julgue os itens a seguir, acerca de sistemas operacionais.

- 101 Um processo é mais fácil de ser descontinuado ou derrubado do que um *thread*, pois este possui recursos associados que devem ser destruídos primeiro.
- 102 No Unix, uma hierarquia de processos ocorre quando um processo pai cria outro processo filho e ambos, conseqüentemente, continuam associados.
- 103 Realiza-se o processo de *boot* quando o chip *bios* inicia as operações da sequência de *booting*, seguida da auto-inicialização (*post*) e passa o controle para o MBR (*master boot record*).
- 104 O gerenciador de *boot* do Windows denominado NTLDR deve ser utilizado em máquinas que tenham um único sistema operacional instalado.
- 105 Cada processo de um sistema operacional está associado a um espaço de endereçamento, que contém uma lista de posições de memória em quantidades mínimas ou máximas que podem ser lidas ou escritas.

Com relação às redes de comunicação, julgue os itens que se seguem.

- 106 O padrão 802.11 é destinado para uso em redes de longa distância.
- 107 O IPV6 é um endereçamento de IP<sub>s</sub> que utiliza 32 *bits*.
- 108 O uso do TTL( tempo de vida do pacote) permite a detecção de erros em pacotes que trafegam na Internet, estando os endereços IP de origem e de destino no cabeçalho do pacote IP.
- 109 O serviço de DNS (*Domain Name Server*) utiliza a porta 53 no protocolo UDP.

Com relação a correio eletrônico e navegação na Internet, julgue os itens subsequentes.

- 110 O Mozilla Thunderbird é um programa livre, gratuito e que possui as mesmas funcionalidades dos programas de *email* comerciais. Ele funciona de maneira independente e não permite importar configurações de contas de outros sistemas, como as do Outlook Express.
- 111 No Thunderbird, o VCard é um cartão de visitas que contém informações como nome, *email* e endereço e que pode ser anexado às mensagens.
- 112 Uma mensagem de *phishing* pode ser bloqueada por meio de filtros configuráveis em *softwares* de navegação como o Internet Explorer.
- 113 Na opção Ferramentas do menu Opções da Internet do Internet Explorer, é possível configurar o histórico de navegação para que arquivos temporários, *cookies* e senhas salvas sejam configurados segundo a preferência do usuário.
- 114 O assistente de localização de *Feeds* RSS do Internet Explorer permite bloquear *popups*.
- 115 No Outlook Express, o comando Identidades permite criar diversos usuários para uso do programa, com nomes e senhas específicos.
- 116 Uma das vantagens de segurança do uso do Outlook Express é sua imunidade a vírus que afetam o sistema operacional Windows.

Acerca de segurança da informação, julgue os itens subsecutivos.

- 117 *Pharming* é um ataque que possui como estratégia corromper o DNS e direcionar o endereço de um sítio para um servidor diferente do original.
- 118 *Failover* é a capacidade que um sistema possui de continuar, automaticamente, um serviço em caso de falhas, sem a necessidade de um comando humano.
- 119 Token é um *software* de autenticidade capaz de gerenciar chaves criptográficas e autenticar certificados digitais.
- 120 Os *rootkits* são um conjunto de programas que oferecem mecanismos para esconder o invasor, assegurando a sua presença em um computador invadido.

## PROVA DISCURSIVA

- Na prova a seguir, 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 texto que tenha qualquer assinatura ou marca identificadora fora do local apropriado. Ao texto que contenha qualquer outra forma de identificação será atribuída nota zero, correspondente a identificação do candidato em local indevido.
- Ao domínio do conteúdo serão atribuídos até **10,00 pontos**, dos quais até **0,50 ponto** será atribuído ao quesito apresentação e estrutura textual (legibilidade, respeito às margens e indicação de parágrafos).

---

Atualmente os responsáveis pela gestão de tecnologia da informação (TI) possuem uma diversidade de soluções disponíveis no mercado, que são capazes de fornecer recursos que auxiliam no gerenciamento da infraestrutura de TI. Independente dos fornecedores e da solução que seja disponibilizada, um fator determinante é a capacidade de interoperar e se integrar ao que já existe na estrutura de TI da instituição.

---

Considere que em uma instituição seja identificada a necessidade de implementar um servidor de arquivos, e que o responsável por TI decida, após uma série de avaliações, utilizar o sistema operacional Linux. A partir dessas informações, redija um texto dissertativo descrevendo o que deve ser feito para implementar o servidor de arquivos na instituição. Em seu texto, aborde, necessariamente, os seguintes aspectos:

- ▶ descrição do serviço utilizado para compartilhamento de arquivos para estações de trabalho Linux e Windows; **[valor: 3,00 pontos]**
  - ▶ configurações para montagem de compartilhamentos em estações Windows e Linux; **[valor: 3,00 pontos]**
  - ▶ escolha de um arranjo de disco que seja capaz de proporcionar redundância em caso de falha em pelo menos um dos discos e flexibilidade para disponibilizar aumento do espaço de armazenamento para o servidor. **[valor: 3,50 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	



**cespeUnB**

Centro de Seleção e de Promoção de Eventos