

## CONHECIMENTOS ESPECÍFICOS

Com relação aos fundamentos dos sistemas UNIX e suas funcionalidades, julgue os itens que se seguem.

- 61 O arquivo `/etc/passwd` contém os dados dos usuários, senhas de acesso, datas de expiração, bem como os caminhos de diretório home dos usuários autorizados no sistema.
- 62 Uma entrada de valor `15 14 1 * * /bin/backup` no Crontab fará com que o comando `/bin/backup` seja executado semanalmente às 15 h 14 min.
- 63 A seqüência de permissões `-rwxr-xr--` indica que o arquivo só pode ser modificado por seu proprietário.
- 64 Para compartilhar diretórios com outros computadores da rede por meio de um servidor NFS, é necessário especificar o caminho e as permissões no arquivo de configuração `/etc/fstab`.
- 65 O comando `init 0` provoca o encerramento do sistema e só pode ser executado por usuários privilegiados.
- 66 O Sendmail atua essencialmente como um cliente para envio de *email*, de modo a requerer um agente de transferência de mensagens para se comunicar com o servidor de correio do destinatário.
- 67 A ferramenta `ifconfig` é utilizada para configurar parâmetros das interfaces de rede, como endereços IP, máscaras de rede e definições de rotas.

Microsoft Windows Server é um sistema operacional robusto que suporta diversos componentes de serviço, como o Exchange Server, que provê serviços de correio eletrônico e colaboração. Considerando esse assunto, julgue os itens a seguir, acerca dos fundamentos do sistema Windows Server 2012 e seus componentes de serviço.

- 68 O WSUS (*windows server update services*) requer a ativação do serviço BITS, cuja função é verificar se há novas atualizações no repositório oficial do Windows Update.
- 69 Caso o nome do domínio do *Active Directory* seja **servidor.empresa.com**, então a zona DNS com autoridade poderá ser **servidor.empresa.com**, **empresa.com** ou apenas **com**.
- 70 O `cmdlet Get-Mailbox` permite exibir objetos e atributos das caixas de correio, e pode também ser combinado com outras tarefas para fornecer informações sobre as caixas.
- 71 A ferramenta Exchange PST Capture possibilita a localização de arquivos PST nos computadores da rede e a importação automática nas caixas de correio do Exchange.
- 72 A opção padrão de instalação do Windows Server 2012 disponibiliza uma interface gráfica do usuário que proporciona melhor administração, desempenho e segurança do ambiente.
- 73 O centro administrativo do *Active Directory* fornece a funcionalidade de lixeira, que permite recuperar arquivos excluídos acidentalmente dos compartilhamentos de rede.

Acerca dos protocolos e aplicações típicas de serviços TCP/IP, julgue os itens subsecutivos.

- 74 ARP é um protocolo da camada de transporte do TCP/IP responsável pela tradução de endereços IP para endereços Ethernet (MAC).
- 75 A arquitetura do NIS é composta por servidor *master*, servidor *slave* e clientes, os quais utilizam serviços RPC para permitir a gestão centralizada de um grupo de servidores UNIX.
- 76 Para que um servidor DHCP ofereça suporte a clientes em outras sub-redes remotas separadas por roteadores, estes roteadores devem ser usados como agentes de retransmissão BOOTP e DHCP a fim de oferecer suporte ao encaminhamento de tráfego DHCP entre sub-redes.
- 77 Enquanto clientes de *email* do tipo POP liberam espaço da caixa de correio remota assim que as mensagens são descarregadas, clientes de *email* do tipo IMAP se limitam à sincronização das mensagens, de modo a requererem intervenção direta no servidor para limpeza das caixas de correio.
- 78 O protocolo SMTP padrão da Internet tem o papel de transportar mensagens e possui capacidades como o controle do roteamento e a entrega de mensagens por meio de comunicação segura.
- 79 Os registros de DNS do tipo SPF (*sender policy framework*) são usados para evitar falsificação de *emails*, uma vez que os endereços dos servidores autorizados a enviar mensagens podem ser delimitados em registros do tipo MX.
- 80 O protocolo FTP faz uso de, no mínimo, duas conexões durante uma sessão de transferência: uma conexão *half-duplex* para controle, tipicamente pela porta TCP 21, e uma conexão *full-duplex* para transferência de dados.

Com referência ao *Active Directory*, do Windows Server 2012, julgue os itens subseqüentes.

- 81 Os dados armazenados no *Active Directory* são apresentados ao usuário de forma hierárquica semelhante à forma como os dados são armazenados em um sistema de arquivos, sendo cada entrada referenciada como um objeto.
- 82 Entre os componentes lógicos dos serviços de domínio do *Active Directory*, as unidades organizacionais são contêineres que oferecem uma estrutura para que sejam delegados direitos administrativos e sejam vinculados objetos de política de grupo.
- 83 A floresta dos serviços de domínio do *Active Directory* representa um limite de segurança; portanto, por padrão, nenhum usuário de fora da floresta pode acessar recursos dentro da floresta e apenas usuários administradores de fora da floresta têm acesso administrativo dentro da floresta.
- 84 Embora o *Active Directory* seja um repositório de informações sobre os objetos que residem em uma rede, as listas de controle de acesso são tratadas em um módulo à parte do Windows Server.

Com base nos conceitos dos serviços de domínio do *Active Directory*, do Windows Server 2012, julgue os itens a seguir.

- 85 O domínio dos serviços do *Active Directory* fornece um centro de autenticação de modo que todas as contas de usuário e de computador sejam armazenadas no banco de dados do domínio, permitindo que usuários e computadores possam se autenticar a uma rede sem se conectar ao controlador de domínio para autenticação.
- 86 As informações dos serviços de domínio do *Active Directory* são armazenadas no banco de dados do diretório, no qual cada partição, também conhecida como contexto de nomenclatura, contém objetos de um escopo de replicação e finalidade específica.
- 87 Dentro dos limites de domínio e floresta em uma estrutura dos serviços de domínio do *Active Directory*, embora seja possível conceber políticas de senhas específicas para configurações de políticas diferentes para usuários em particular em um domínio, não é possível aplicar as políticas de conta e senha além do escopo de um único domínio.

Julgue os próximos itens, relativos ao IIS (*Internet Information Server*) 7.0.

- 88 No IIS 7.0, é possível melhorar, por meio do WAS (*Windows Process Activation Service*), a segurança da aplicação *web* eliminando-se a possibilidade de essa aplicação acessar recursos de outras aplicações ao colocar todos os sítios, por exemplo, no mesmo *application pool*.
- 89 O IIS 7.0, que faz parte do pacote de *roles* do *Application Server*, é um componente opcional do Windows Server 2008 e, por padrão, não é instalado após o término de uma instalação básica do sistema operacional.
- 90 O IIS 7.0 é um servidor *web* que garante compatibilidade limitada para aplicações, tais como ADSI (*Active Directory Service Interfaces*) existentes e *scripts* WMI.
- 91 O IIS 7.0 é composto por módulos que podem ser adicionados e removidos do servidor *web* e que permitem a customização de seu servidor, com adição e remoção de características específicas.

Com relação aos serviços de terminal fornecidos no Windows Server 2008, julgue os itens subsecutivos.

- 92 Os usuários podem acessar programas *RemoteApp* em um sítio da Internet ou em uma *intranet*, usando um servidor *web*, após a instalação, com base no Windows Server 2008, do *TS Web Access*, que é um serviço na função de serviços de terminal.
- 93 O *Terminal Service Gateway* usa o protocolo de área de trabalho remota (*remote desktop protocol*) sobre HTTP formando uma conexão simples entre usuários remotos e computadores remotos nos quais as aplicações de produtividade desses usuários são executadas.
- 94 Entre as funcionalidades básicas dos serviços de terminal está aquela que permite que usuários com uma conta de domínio efetuem o *login* uma vez, usando uma senha ou *smart card*, e obtenham acesso a um servidor de terminal sem a necessidade de apresentarem as credenciais novamente.

Os processadores Intel utilizam dois princípios básicos de construção: CISC (*Complex Instruction Set Computing*) e RISC (*Reduced Instruction Set Computing*). Considerando esse assunto, julgue os itens que se seguem.

- 95 Embora os processadores CISC apresentem um grande conjunto de instruções, apenas 20% destas são usadas por programas e sistemas operacionais durante 80% do tempo de operação do processador, fato que motivou o surgimento de microprocessadores com um conjunto reduzido de instruções, denominados RISC.
- 96 Devido à ausência do decodificador de instruções, os processadores CISC são mais rápidos que os processadores RISC.
- 97 Em um processador RISC, todas as instruções têm o mesmo tamanho. Ao entrar no processador, cada *bit* da instrução é responsável por ativar ou desativar algum dos circuitos lógicos internos desse processador.

Julgue os seguintes itens, referentes a *storages* e suas tecnologias.

- 98 Discos físicos de um *storage* ou grupos de unidades RAID podem ser divididos logicamente em volumes conhecidos como volumes lógicos, comumente referenciados como LUN (*logical unit numbers*).
- 99 O foco da configuração RAID 0 é o desempenho, uma vez que ele não tem tolerância a falhas.
- 100 Na configuração RAID 4, a paridade é distribuída em todos os discos, ao passo que, na RAID 5, a paridade é escrita em um disco dedicado a essa finalidade.

Considerando que SAN (*Storage Area Network*) e NAS (*Network Attached Storage*) são tecnologias para acesso a dispositivos de armazenamento de dados por meio de uma rede corporativa, julgue os itens a seguir.

- 101 O NAS utiliza o acesso de nível de arquivo para todas as suas operações de entrada e saída, sendo essas operações entendidas como pedidos de alto nível que especificam o arquivo a ser acessado, mas não especificam seu endereço de bloco lógico.
- 102 A arquitetura *Fibre Channel* (FC), que forma a construção fundamental da infraestrutura SAN, é uma tecnologia de rede de alta velocidade que funciona em cabos de fibra óptica (preferidos para conectividade *front-end* da SAN) e cabos seriais de cobre (preferenciais em conectividade *back-end* de disco).
- 103 A tecnologia SAN permite que haja consolidação de armazenamento e que este seja compartilhado por diversos servidores, mas não permite que as organizações conectem servidores e armazenamento geograficamente dispersos.
- 104 Na ativação do compartilhamento de dados, o NAS geralmente usa o NFS para sistemas UNIX, o CIFS para sistemas Windows, e o protocolo FTP (*File Transfer Protocol*) para ambos os ambientes.
- 105 A eficiência do NAS pode ser melhorada por meio da compatibilidade entre os clientes das plataformas UNIX e Windows, obtida pelo uso de protocolos padrão do mercado.

Acerca de gestão da segurança da informação, julgue os itens a seguir.

- 106** Um dos objetivos da política de segurança da informação é prover orientação da direção da organização para a segurança da informação, de acordo com os requisitos do negócio, as leis e as regulamentações pertinentes.
- 107** Para realizar análises críticas da eficácia do sistema de gestão de segurança da informação a intervalos planejados, a organização deve ter em conta os incidentes de segurança da informação mais graves do período, e desconsiderar eventuais sugestões dos atores envolvidos que não estejam relacionadas aos incidentes observados.
- 108** A classificação de informações quanto ao grau de proteção contra destruição é importante para a continuidade operacional dos negócios da organização, ao passo que a classificação quanto ao grau de sigilo é importante para a estratégia de negócios da organização.
- 109** A gerência da auditoria de segurança engloba, entre outros aspectos, a administração da política de segurança e os procedimentos de recuperação após desastres; além disso, é de responsabilidade dessa gerência a constante atualização com respeito a problemas e riscos de segurança.

Julgue os itens subsecutivos, a respeito da segurança física.

- 110** Alguns controles de segurança física podem conflitar com a segurança de pessoas. Por isso, em um ambiente corporativo, esses aspectos precisam ser identificados e tratados, de modo a se priorizar a preservação da vida humana em relação a uma instalação ou aos ativos que ela possa conter.
- 111** A instalação de piso elevado é recomendada para atender necessidades específicas de um ambiente corporativo de processamento de dados, entre elas a de climatização em sistema com *plenum* de insuflação. Por outro lado, o uso de piso elevado apresenta baixa flexibilidade para alterações de leiaute e expansões.
- 112** Os gases Halon e FM-200 são muito eficientes no combate a incêndios, pois interferem na reação química do fogo, extinguindo-o; entretanto o FM-200 não é mais utilizado em ambientes corporativos de processamento de dados já que contribui para a destruição da camada de ozônio do planeta.

Com relação à segurança lógica, julgue os próximos itens.

- 113** O controle de acesso lógico não discricionário habilita os proprietários dos dados a determinarem quem pode ter acesso a arquivos e a recursos que lhes pertencem.
- 114** No contexto da segurança da informação, o mecanismo de assinaturas digitais pode suportar serviços para prover a integridade, como autenticação da origem dos dados e não repúdio.
- 115** Controle de acesso lógico é um mecanismo de segurança usado para prover confidencialidade no contexto da segurança da informação, assim como protocolos de transmissão e visões em bancos de dados.

No que concerne a tecnologias de *firewall*, julgue os itens subseqüentes.

- 116** As ferramentas de *firewall* convencionais não são capazes de proteger uma rede contra o uso indevido de autorizações válidas de usuários internos; porém, elas são capazes de prevenir ataques em que o conteúdo de uma mensagem válida e autorizada faz ativar a exploração de uma vulnerabilidade de serviço executado na rede destino.
- 117** Os *firewalls* do tipo filtro de pacotes caracterizam-se pela utilização de informações dos protocolos e dos serviços de comunicação das camadas mais altas e implementam controles baseados em políticas mais complexas e personalizadas da organização.

A respeito da criptografia, julgue o item a seguir.

- 118** A cada rodada completa, o algoritmo AES executa quatro funções distintas: substituição de *bytes*, permutação, operações aritméticas sobre um corpo finito e operação XOR com uma chave.

Acerca das tecnologias de VPN, julgue o seguinte item.

- 119** Por questões de segurança, quando um servidor de VPN está à frente de um *firewall* e conectado à Internet, filtros de pacotes devem ser configurados na interface Internet do servidor de VPN para permitir somente tráfego VPN de e para o endereço IP daquela interface.

Com relação a tecnologias de IDS, julgue os itens que se seguem.

- 120** Os IDS estatísticos podem detectar novas e imprevistas vulnerabilidades, além de sinalizar a ocorrência de eventuais ataques por anomalias comportamentais de tráfego; esses IDS são, ainda, muito menos suscetíveis à indicação de falsos positivos do que os IDS baseados em assinaturas.
- 121** Sistemas IDS baseados em redes monitoram o tráfego de rede dos servidores e são usados para garantir que arquivos de sistema desses servidores não serão removidos intencionalmente ou acidentalmente, nem reconfigurados indevidamente, ou, ainda, que seus sistemas não serão colocados, de alguma maneira, em risco.

A respeito da gestão de riscos, julgue os itens subsecutivos.

- 122** Para assegurar que a gestão de riscos seja eficaz, a organização deve analisar, criticamente e de forma periódica, se a política, o plano e a estrutura da gestão de riscos permanecem apropriados, dados os contextos externo e interno da organização.
- 123** A gestão de riscos faz parte das responsabilidades da administração e é parte integrante de todos os processos organizacionais, nos quais se incluem planejamento estratégico e todos os processos de gestão de projetos e de gestão de mudanças.

Em relação às máquinas virtuais, julgue o próximo item.

- 124** Ao manter os ambientes virtuais isolados do sistema real subjacente e entre si, a camada de virtualização provê, em algum grau, confidencialidade de dados entre os sistemas convidados.

Com a relação a IN GSIPR n.º 1 e normas complementares, julgue os itens que se seguem.

Espaço livre

**125** De acordo com a Norma Complementar 08/IN01/DSIC/GSIPR, a prospecção ou a monitoração de novas tecnologias e o desenvolvimento de ferramentas de segurança são serviços adicionais que uma ETIR poderá oferecer à sua comunidade.

**126** A Norma Complementar 02/IN01/DSIC/GSIPR prevê que, na fase Planejar do Ciclo de Gestão de Segurança da Informação, a atividade de análise de riscos deverá identificar a probabilidade real de ocorrência de falhas de segurança; para isso devem-se considerar as vulnerabilidades prevaletentes, os impactos associados a esses ativos e, por fim, as ações de segurança da informação e comunicações atualmente implementadas em determinado órgão ou entidade.

**127** De acordo com a IN GSIPR n.º 1, a atribuição de acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança em um órgão da administração pública federal é responsabilidade do Comitê de Segurança da Informação e Comunicações do órgão.

---

No que diz respeito ao gerenciamento de projetos, julgue os itens a seguir, de acordo com o PMBOK 5.ª edição.

**128** Influenciar os fatores que poderiam impedir o controle integrado de mudanças ou de gerenciamento de configurações para que somente as mudanças aprovadas sejam implementadas está entre as atribuições do grupo de processos de monitoramento e controle.

**129** Os projetos são normalmente autorizados como resultado de uma ou mais considerações estratégicas, entre as quais estão a competitividade concorrencial e a consideração ambiental.

**130** A maior parte do esforço despendido no controle de custos envolve a análise da relação entre o consumo dos fundos do projeto e o trabalho físico que é realizado.