CONHECIMENTOS ESPECÍFICOS

A respeito dos ambientes Windows e UNIX, julgue os seguintes itens.

61 O Windows Server 2000 possui versões que suportam arquiteturas de 32 e 64 *bits*.

62 O recurso do *Active Directory* foi desenvolvido e distribuído pela primeira vez no Windows Server 2000.

63 No UNIX, uma conta de usuário é classificada como *root* se seu UID (*user identifier*) for igual a 1.

Acerca dos protocolos que compõem o modelo TCP/IP (*transmission control protocol*/*internet protocol*), julgue os itens a seguir. Nesse sentido, considere que a sigla DNS, sempre que utilizada, se refere a *domain name service*.

64 O DHCP (*dynamic host configuration protocol*) não interage com o DNS, portanto, a vinculação entre um nome de *host* e o endereço IP que o DHCP atribui ao *host* deve ser gerenciado de maneira independente.

65 Há duas formas de utilizar o DNS: contratando os servidores de nome, um de cada vez, ou solicitando ao sistema do servidor de nome que execute toda a conversão.

Com relação aos serviços de arquivos e impressão em rede, julgue os próximos itens. Nesse sentido, considere que a sigla CUPS, sempre que utilizada se refere a *common unix printing system*.

66 O Linux define os seguintes tipos de arquivos: arquivo regular, diretório, arquivo de dispositivo de caracteres, arquivo de dispositivo de blocos, *socket* de domínio local, *pipe* identificado e *link* simbólico.

67 Quando mais de uma impressora estiver conectada a uma máquina, o gerenciador de impressão CUPS mantém uma fila única de impressão para todas as impressoras.

68 O HTTPS (*hyper text transfer protocol secure*) é o protocolo subjacente para todas as interações entre os servidores CUPS e seus clientes.

69 O sistema de arquivos de hierarquia única utilizado nos sistemas UNIX difere do sistema utilizado nos sistemas operacionais Windows, que conservam o conceito de espaços e nomes específicos a discos.

No que se refere à instalação e configuração dos serviços e servidores, julgue os itens subsecutivos.

70 Uma das características mais importantes do *proxy* é a restrição de acesso a sítios não autorizados, executada por meio de listas de controle de acesso (*access control lists*).

71 Uma vez que o servidor de correios *Sendmail* não possui modos específicos de entrega, ele não apresenta relação clara de compromisso entre latência e *throughput*.

72 No servidor Apache, caso um provedor de conteúdo de sítio necessite realizar modificações na configuração do servidor por-diretório, mas não tem acesso *root* ao sistema do servidor, devem ser utilizados arquivos `password.file`.

Os sistemas operacionais de rede da Microsoft, Windows Server 2000 e 2003, possuem funcionalidades específicas, como o *Active Directory*, o *Internet Information Services* e o *Terminal Services*. Acerca dessas funcionalidades, julgue os itens subsequentes.

73 No IIS 5.0, os serviços de Internet padrão, como servidores *web* e FTP, residem no processo chamado *Inetinfo*, que não inclui o *pool* compartilhado de discussão, o *cache* e os serviços de registro.

74 A fim de definir diretivas dos serviços de terminal para um domínio, o usuário deve utilizar um computador que possua permissão para acesso ao controlador de domínio, porém, ele não precisa ser administrador desse domínio.

75 Os nomes de domínio do *Active Directory* geralmente são os nomes DNS completos dos domínios. Nesse serviço, é possível agrupar domínios que fazem parte do mesmo espaço de nomes DNS dentro de uma mesma árvore de domínio.

A respeito da integração com ambiente UNIX, julgue os itens que se seguem.

76 Por questões de segurança, as portas NetBIOS 137, 138, 139 e Microsoft-DS 445 do servidor SAMBA devem ser bloqueadas para acesso pela interface externa.

77 O SAMBA, conjunto de ferramentas que permite a comunicação entre máquinas Linux e Windows, utiliza os protocolos SMB (*server message block*) e CIFS (*common internet file system*), sendo o lado servidor do SMB implementado em *hosts* Linux.

78 O SUA (*subsystem for UNIX-based applications*) é um subsistema para compilação e execução de aplicativos fundamentados no UNIX em um computador executando o Windows Server 2003 R2.

79 Para compartilhar impressoras locais com o SAMBA, deve-se adicionar uma seção `[printers]` ao arquivo `smb.conf`.

Acerca de infraestrutura de *hardware*, julgue os itens a seguir.

80 A arquitetura *Fibre Channel* forma a base da infraestrutura de SAN (*storage area networks*) e foi criada para satisfazer à demanda de velocidades maiores de transferência de dados entre computadores, servidores e subsistemas de armazenamento maciço.

81 Em processadores com tecnologia RISC, o compilador deve converter comandos simples em poucas instruções mais complexas, gerando o resultado de operação padronizado.

82 O NAS (*network attached storage*) utiliza protocolos de rede e de compartilhamento de arquivos para executar funções de arquivamento e armazenamento. Estes protocolos incluem IPX (*internetwork packet exchange*) e SPX (*sequenced packet exchange*) para transferência de dados e CIFS e NFS (*network file system*) para *file serving* remotos.

83 Os processadores Intel de 6.ª geração utilizam uma arquitetura híbrida CISC / RISC, enquanto os processadores das gerações anteriores usavam apenas a arquitetura CISC.

Acerca da segurança da informação, julgue os itens seguintes.

84 Quanto à segurança física e ambiental das informações, o ambiente de alta disponibilidade para *data centers*, denominado de sala-cofre, provê proteção contra fogo, vazamentos de líquidos e poeira.

85 A classificação da informação consiste na categorização e na indexação da informação, a fim de facilitar a sua recuperação.

Julgue os itens subsequentes a respeito das tecnologias de *firewalls*, IDS (*intrusion detection system*) e virtualização.

86 *Firewalls* SPI (*stateful packet inspection*) implementam nativamente VPN (*virtual private network*) para comunicação *site-to-site*, sendo utilizados para interligar, de forma segura, filiais das empresas a matrizes.

87 Por meio de análise de protocolos e aplicações de redes, os sistemas de IDS, cuja função é a de identificar e bloquear ataques avançados, podem mitigar, por exemplo, ataques do tipo SQL *injetion*.

88 Em sistemas virtualizados, *escape to host* ou *guest-to-host virtual machine escape* são ataques em que o atacante explora vulnerabilidades normalmente associadas ao virtualizador, rompendo o isolamento das máquinas virtuais e acessando o *host*.

89 Os NFGW (*next generation firewalls*) se diferenciam dos *firewalls* UTM (*unified threat management*), entre outras características, pelo uso da tecnologia DPI (*deep packet inspection*), que analisa pacotes de dados até a camada de aplicação, e por trazer inteligência externa aos *firewalls*.

Julgue os itens seguintes, relativos ao risco de segurança da informação.

90 São critérios de impactos à segurança da informação o dano à reputação, os níveis de classificação de ativo de informação afetado e o não cumprimento de prazos.

91 Critérios de avaliação de risco, de impacto, de auditoria e de aceitação do risco incluem-se entre os critérios básicos para gestão de risco à informação.

92 O processo de gestão de riscos de segurança da informação consiste na definição de contexto, processo de avaliação, tratamento, aceitação, comunicação e consulta, monitoramento e análise crítica de risco.

Em relação à criptografia e às funções criptográficas, julgue os itens subsecutivos.

93 AES, Twofish e 3DES são exemplos de cifras utilizadas na criptografia simétrica.

94 Para implementar um sistema de ECM (*enterprise content management*), do ponto de vista da criptografia, é necessário utilizar infraestrutura interna de chaves públicas, na qual *tokens* ou *smartcards* podem ser utilizados para armazenagem e proteção das chaves públicas de cada colaborador.

95 A função criptográfica *hash* pode ser utilizada para ofuscar senhas em aplicações. O algoritmo md5 é considerado seguro, quando comparado ao SHA-2, devido a sua baixa taxa de colisões e à baixa quantidade de *rainbow tables* associadas.

96 Na comunicação de um usuário com um servidor *web* de certificado SSL (*secure socket layer*) autoassinado, não é possível a confirmação da autenticidade do certificado, de modo que esse tipo de comunicação é considerado inseguro.

No que se refere aos ataques de negação de serviço, julgue os itens que se seguem. Nesse sentido, considere que a sigla DDoS, sempre que utilizada, se refere ao ataque *Distributed Denial of Service*.

97 Ataques Xmas-DDoS (*christmas tree packets*) são caracterizados pela inundação de pacotes ICMP tipo 8 em uma rede de dados.

98 Ataques DDoS de fragmentação de pacotes, tanto em TCP quanto em UDP, são um desafio a qualquer sistema de proteção de rede, pelo fato de os pacotes não chegarem ordenados e as informações relativas às portas de origem e destino serem disponibilizadas apenas no último pacote.

99 Ataques refletivos de DDoS de NTP têm como objetivo indisponibilizar os serviços de NTP pelo mundo, atrasando-os em uma hora, o que gera inconsistências nos horários registrados pelos *logs* e nas trocas de mensagens.

100 Ataques de DDoS fundamentados em `HTTP_GET` e `HTTP_POST` estão cada vez mais complexos, devido à utilização de técnicas de randomização e encodificação. As ferramentas convencionais, como IPS (*intrusion prevention systems*), não são efetivos para mitigação desses ataques.

101 Ataques de negação de serviço SYN *floods*, fundamentados no protocolo UDP, são caracterizados pelo envio de diversos pacotes com a *flag* SYN ativa, o que faz com que o dispositivo vítima aloque recursos desnecessariamente.

102 Ataques de DDoS fundamentados em UDP *flood fragment* podem ocorrer como consequência de ataques de DDoS de NTP (*network time protocol*) ou SNMP (*simple network management protocol*), a partir do momento em que os pacotes gerados ultrapassem o MTU (*maximum transmission unit*) definido na rede local.

Julgue os próximos itens, a respeito de métodos de mitigação de ataques e vulnerabilidades.

103 A restrição de endereços IPs de origem, a utilização de chaves criptográfica para autenticação e a mudança da porta padrão, são consideradas boas práticas de segurança quanto ao uso do serviço de SSH.

104 Como método de segurança contra ataques aos serviços de DNS (*domain name system*), recomenda-se segmentar os servidores em autorativos e recursivos, bloqueando o acesso oriundo dos servidores recursivos à Internet.

105 *The heartbleed bug* é uma vulnerabilidade grave encontrada no OpenSSL, e pode ser mitigada pela atualização do OpenSSL, pela revogação das chaves que tenham indicação de estarem comprometidas e pela emissão e distribuição de novas chaves.

Em relação à política de segurança da informação e à gestão de continuidade do negócio, julgue os itens a seguir.

106 Política de segurança pode ser definida como um documento que estabelece princípios, valores, compromissos, requisitos, orientações e responsabilidades sobre o que deve ser feito para se alcançar um padrão desejável de proteção das informações.

107 A política de informação deve ser escrita e assinada pelo chefe da SOC (*security operation center*), responsável máximo pela informação organizacional, que, durante a escrita desse documento, deverá ouvir as demais áreas institucionais, de modo a incrementar a audiência e o entendimento do funcionamento da organização.

108 As normas relativas ao controle de acesso aos sistemas corporativos das instituições são definidas dentro da política de segurança da informação.

Acerca da NBR ISO/IEC 27001:2013 e de sua aplicabilidade no sistema de gestão da segurança da informação (SGSI), julgue os itens que se seguem.

109 As decisões táticas e operacionais para avaliação de risco devem ser descritas como processos relacionados a integridade e confidencialidade. A disponibilidade não possui risco operacional, logo não são descritas por esse processo.

110 A referida norma exige, por sua própria natureza, formalidade, documentação e organização da área de segurança da informação.

111 A adoção de um SGSI prescinde do cunho estratégico, pois é vista como uma decisão tática e operacional da organização.

Julgue os próximos itens, de acordo com a norma NBR ISO/IEC 27002:2013, que estabelece diretrizes para práticas de gestão de segurança da informação.

112 As fontes principais de requisitos de segurança da informação são avaliação de riscos para a organização, legislação vigente e conjuntos particulares de princípios, objetivos e requisitos do negócio.

113 A definição de uma política de segurança da informação e o estabelecimento da abordagem para gerenciar os objetivos de segurança da informação devem ser aprovados no mais alto nível da organização.

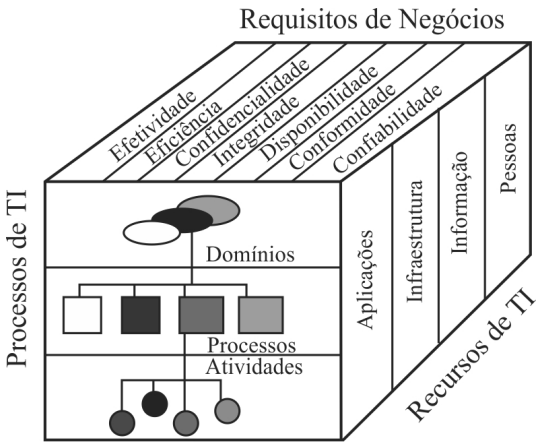
114 A estrutura organizacional e as funções de *software* e *hardware* não figuram como objetos da referida norma.

A respeito do ITIL, que define melhores práticas de serviços, julgue os itens subsequentes.

115 Na estratégia de serviços, é defendida a definição de um único ponto de contato e não, necessariamente, do primeiro ponto de contato na visão de um *service desk*.

116 O projeto de serviços enfoca o desenho da tecnologia utilizada pelo serviço, ao passo que a estratégia de serviços enfoca exclusiva e permanentemente a função de tecnologia ligada à entrega do serviço.

117 Gestão de mudanças é objeto de atuação definido pela transição de serviços.



Considerando que a figura apresentada mostra a inter-relação dos componentes do COBIT, julgue os itens seguintes.

118 O COBIT 5, atual versão do *framework*, embora atualizado, é independente e não possui integração com outros conjuntos de boas práticas e metodologias.

119 A integridade, relacionada aos requisitos de negócio, refere-se à propriedade de proteção das informações sensíveis, cuja finalidade é a de evitar a divulgação indevida dessas informações.

Com base no Decreto n.º 3.505/2000, que instituiu a política de segurança da informação nos órgãos e nas entidades da administração pública federal, julgue os itens a seguir.

120 A Agência Brasileira de Inteligência, por meio do Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações, é responsável por atividades de assessoramento do Conselho de Defesa Nacional.

121 A realização de auditorias nos órgãos e nas entidades da administração pública federal envolvidas com a política de segurança da informação compete à Secretaria-Executiva do Conselho de Defesa Nacional.

Acerca das etapas e dos processos do PMBOK (versão 5), julgue os itens subsecutivos.

122 Na versão 5 do PMBOK, o escopo do projeto é definido na fase de iniciação do projeto.

123 A identificação e o gerenciamento de riscos são atividades definidas na fase de execução do projeto.

124 Iniciação, planejamento, execução, monitoração e controle e, ainda, encerramento integram as fases da versão 5 do PMBOK.

Julgue os próximos itens, que tratam da Instrução Normativa do Gabinete de Segurança Institucional da Presidência da República (IN-GSIPR) n.º 1/2009 e de normas complementares (NC), estabelecidas na mesma norma IN.

125 A NC n.º 21 estabelece as diretrizes para elaboração de política de segurança da informação e comunicações nos órgãos e nas entidades da administração pública federal.

126 A criação de equipes de tratamento e respostas a incidentes em redes computacionais nos órgãos e nas entidades da administração pública federal figura em norma complementar.

127 A NC n.º 8 cuida das diretrizes para gerenciamento de incidentes em redes computacionais nos órgãos e nas entidades da administração pública federal.

Acerca do acesso à informação, no âmbito da administração pública, julgue os itens seguintes.

128 É garantido, por qualquer ente federal, o acesso irrestrito à informação referente a projetos de pesquisa e de desenvolvimento científicos ou tecnológicos.

129 Os órgãos e as entidades do poder público devem assegurar a gestão transparente da informação, propiciando amplo acesso a ela e sua divulgação, com observância das normas e dos procedimentos específicos aplicáveis.

130 A identificação do requerente não pode conter exigências que inviabilizem a solicitação, quando se tratar de acesso a informações de interesse público.

Espaço livre