CONHECIMENTOS ESPECÍFICOS

Com relação à suíte de protocolos TCP/IP, julgue os itens que se seguem.

61 A recepção de três segmentos TCP com o mesmo número de ACK provoca retransmissão de dados, ainda que o temporizador correspondente não tenha expirado.

62 A configuração de endereço IP por meio do DHCP dispensa o ARP gratuito.

63 Um servidor SMTP pode receber e enviar mensagens de correio eletrônico, agindo tanto como cliente quanto como servidor.

64 Os serviços POP e IMAP alocam as mesmas portas para disponibilizar seus servidores.

65 A fim de se obter adequada configuração de segurança em um *firewall*, deve-se configurar o serviço FTP para operar em modo passivo.

A respeito de criptografia, julgue os itens seguintes.

66 Em um sistema assimétrico, garante-se a autenticidade da mensagem quando uma mensagem é cifrada duas vezes: primeiro, com a chave pública do autor e, depois, com a chave pública do destinatário.

67 Nos sistemas simétricos, as partes compartilham uma chave secreta, utilizada tanto na cifração quanto na decifração.

68 Uma assinatura digital consiste na cifração de um arquivo digital e do seu resumo criptográfico com uma chave privada.

69 Um certificado digital consiste na cifração do resumo criptográfico de uma chave privada com a chave pública de uma autoridade certificadora.

70 Se, em um sistema assimétrico, uma mensagem for cifrada duas vezes, primeiro com a chave privada do autor e, depois, com a chave pública do destinatário, garante-se que somente o destinatário conseguirá abrir a mensagem e que só o fará se dispuser da chave pública do autor.

Julgue os itens subsequentes, relativos a ataques e vulnerabilidades.

71 *Firewalls* e IDS são dispositivos eficazes para detectar e evitar ataques de *buffer overflow*.

72 Em decorrência da disponibilização de serviços e aplicações sediados em máquinas virtuais (MVs), que proporciona contenção e rápida recuperação em caso de ataques, uma mesma vulnerabilidade pode estar presente em várias instâncias de um mesmo *snapshot* de uma MV que originalmente apresente tal vulnerabilidade.

73 O ataque conhecido como VLAN *hopping* permite estabelecer tráfego bidirecional entre duas VLANs sem passar por roteamento.

74 Ocorrendo ataque de negação de serviço dirigido a um servidor HTTP, com acesso a uma URL válida, certamente o endereço IP de origem das requisições será forjado (*spoofed*).

75 Um ataque de SQL *injection* explora vulnerabilidades presentes em aplicações *web*, podendo ser evitado com inspeção criteriosa dos dados de entrada.

Acerca de segurança da informação, julgue os itens que se seguem.

76 Em um ambiente bancário, integridade e auditabilidade tem prioridade sobre a confidencialidade.

77 Em um ambiente universitário, a integridade e disponibilidade são os requisitos de segurança prioritários.

78 Uma política de segurança da informação deve atender às necessidades de proteção da informação em uma organização, sendo elaborada por decisão daqueles que vão implantá-la e operá-la.

79 Uma política de segurança da informação eficaz está centrada no controle de acesso à informação, independentemente de formato, mídia ou tecnologia que a suporte.

80 A conformidade pode levar à garantia de atendimento aos requisitos de segurança da informação.

Julgue os próximos itens, relativos a sistema de gestão de segurança da informação (SGSI).

81 No estabelecimento do SGSI, deve-se definir seu escopo e seus limites, junto com uma política específica, a qual deve estar alinhada às metas de negócio.

82 A formulação de um plano de tratamento de riscos é uma das atividades que ocorre após a implementação e operação de um SGSI.

83 O controle dos registros referentes ao SGSI restringe-se aos aspectos referentes aos eventos de natureza técnica.

84 A rastreabilidade de decisões, remetendo a políticas e decisões da direção superior, é um dos requisitos de um SGSI.

85 O SGSI adota o modelo PDCA (*plan-do-check-act*), que estrutura todos os processos, visando proporcionar melhoria contínua.

Com relação aos controles a serem implementados em um SGSI, julgue os itens seguintes.

86 Os usuários devem ser conscientizados e educados no que diz respeito à segurança da informação, uma vez que recai sobre eles a responsabilização pelos eventos em que venham a se envolver, como quebras de segurança e erros de operação.

87 O código fonte de programas é um bem informacional que requer proteção adequada, podendo até conter segredos de negócio; assim, seu acesso deve ser restrito e sujeito a controles de acesso.

88 Acordos de não divulgação que reflitam as necessidades da organização para proteção da informação devem ser revisados sempre que houver vazamento de informação.

89 Os controles relativos a movimentação de equipamentos, informações ou *software* são similares aos controles patrimoniais relativos a outros bens; assim, esses itens só devem ser removidos com autorização prévia e devido registro.

90 As responsabilidades pela segurança da informação devem estar claramente definidas, oferecendo-se, como contrapartida, aos responsáveis os poderes necessários para implementação e operação dos controles, de forma a viabilizar o atendimento aos requisitos de segurança específicos.

Julgue os itens a seguir, relativos à gestão de continuidade de negócio (GCN).

91 A política de GCN define os processos relativos às atividades de preparação para estabelecer a capacidade de continuidade de negócios e o gerenciamento contínuo dessa capacidade.

92 Admite-se que o tempo planejado para a recuperação da normalidade de funcionamento do negócio seja maior que o tempo máximo de interrupção desse funcionamento.

93 Na documentação relativa à GCN, devem estar incluídos, entre outros, documentos relativos à política de GCN, à análise de impacto nos negócios e à avaliação de riscos e ameaças.

94 A GCN não tem relação com o gerenciamento de riscos.

Acerca de um sistema com Windows Server 2003 e seus *services packs* e *patchs* de segurança instalados, julgue os itens subsecutivos.

95 Para se configurar permissão em arquivos ou diretórios, como ponto de partida, uma opção é utilizar o aplicativo Windows Explorer para se configurar direitos de escrita ou leitura.

96 Uma tarefa administrativa de segurança nesse sistema envolve a definição de que tipo de direito os usuários do sistema podem ter. Com base nesse princípio, os usuários que necessitam de direitos administrativos restritivos deverão ser adicionados ao grupo Domain Admins.

97 Membros do grupo de administradores têm permissão para controlar totalmente o servidor, podendo, inclusive, gerenciar as permissões dos usuários e as permissões de controle de acesso, se for necessário.

98 No Windows 2003 Server, por padrão, a conta de convidado é habilitada.

```
C:\>nslookup
Default Server: dns.prova.com.br
Address: 10.1.0.15

> set type=cname
> www.unb.br
Default Server: dns.prova.com.br
Address: 10.1.0.15

Non-authoritative answer:
www.unb.br canonical name = novoportal.unb.br

unb.br nameserver = dns1.unb.br
unb.br nameserver = dns2.unb.br
unb.br nameserver = dns3.unb.br
unb.br nameserver = server1.pop-df.rnp.br
server1.pop-df.rnp.br Internet address = 200.19.119.125
> set type=a
> www.unb.br
Default Server: dns.prova.com.br
Address: 10.1.0.15

Non-authoritative answer:
Name: novoportal.unb.br
Address: 164.41.101.33
Aliases: www.unb.br

>
```

Com base nas consultas DNS contidas no trecho de código apresentado acima, julgue os itens de **99** a **102**.

99 A primeira consulta refere-se a um *alias* cujo registro de DNS aponta para `novoportal.unb.br`.

100 O servidor `dns1.unb.br` respondeu às requisições do cliente.

101 A segunda consulta realizada visou obter um registro do tipo `Address` e, no decorrer dessa consulta, o endereço IP de resposta foi `164.41.101.33`.

102 No trecho de código em questão, todas as respostas obtidas são do tipo autoritativo, o que indica que o servidor responsável pelo domínio `unb.br` é o `dns1.unb.br`.

Considerando que, em um ambiente de rede, exista um servidor de impressão em Windows Server 2003 e outro servidor de impressão em Linux que utilize o sistema CUPS, julgue os itens subsequentes.

103 O CUPS anuncia seu serviço de impressão por meio de *broadcast* e usa por padrão a porta UDP 300. Nesse caso, a configuração padrão do CUPS pode ser alterada para uso apenas de *multicast*.

104 Fazer o controle do acesso físico e lógico às impressoras em uma rede é uma medida de segurança recomendada.

105 No caso do CUPS, recomenda-se utilizar o endereço de *loopback* do servidor para tarefas de administração, a fim de evitar a transmissão da senha de *root* em texto claro com o protocolo HTTP.

106 No caso do serviço de impressão com Windows Server 2003, as portas 139 e 445 com protocolo TCP e as portas 137 e 138 com UDP têm de estar fechadas.

Julgue os próximos itens, a respeito de configuração de *proxy* Squid, serviços de *email* com Sendmail e servidores *web* Apache.

107 Na configuração padrão do Squid, a porta em que o *proxy* aguarda por requisições é a 3128, com protocolo TCP. Se for necessário usar uma outra porta, o parâmetro `http_port` deve ser alterado para a porta de interesse.

108 O Sendmail é um MTA (*mail transfer agent*) que suporta *relay*, cuja configuração necessita, entre outros procedimentos, que a diretiva DS (função de *smart relay*) seja configurada para apontar o nome do servidor para o qual se deseja fazer o *relay*.

109 No caso do Apache, quando se necessita configurar um servidor virtual HTTP para que vários nomes diferentes respondam em um mesmo endereço IP, as diretivas de `VirtualHost`, `DocumentRoot` e `ServerName` devem ser utilizadas e configuradas.

110 No Apache, como o suporte ao SSL é nativo nas versões 1.3.x, o uso do `mod_ssl` se restringe às versões 2.2.x e posteriores. Além disso, a configuração para gestão de certificados autoassinados requer geração randômica de números primos, o que, no caso do Apache, em sistemas Unix, é feito por meio do `/dev/random`.

Julgue os itens que se seguem, relativos a Active Directory e *terminal services*.

111 Para funcionar adequadamente, o Active Directory precisa de um serviço DNS configurado.

112 O Remote Desktop Connection é o servidor padrão para o *terminal services* no Windows 2003.

113 No caso do *terminal services*, a conexão remota é feita por meio do protocolo VNC sobre o protocolo TCP.

114 Para o funcionamento do Active Directory, é necessário que, no ambiente Windows em que ele esteja instalado, exista um *firewall* de contexto, configurado e ativado.

Julgue os itens subsecutivos, a respeito da tecnologia SFU (Services for Unix) da Microsoft, que permite a integração, até certo ponto, entre ambientes Unix e Microsoft Windows Server.

115 O Linux, por padrão, tem o sistema SAMBA integrado com a tecnologia SFU da Microsoft.

116 O serviço de compartilhamento de arquivos via NFS (*Network File System*) é uma tecnologia padrão da Microsoft. No caso de redes Unix, o cliente NFS se conecta nativamente a um compartilhamento de rede Microsoft e apresenta suas credenciais de acesso.

117 Um sistema com o SFU em funcionamento suporta as funcionalidades de *pipes* e *links* simbólicos.

118 A tecnologia SFU usa o subsistema Interix, que, entre outras características, suporta o Shell Korn e o Shell C.

Com relação a sistema de *storage* embasado em SAN e às técnicas que podem ser utilizadas para aumentar a segurança desse sistema, julgue os itens de **119** a **122**.

119 A criação de zonas (*zoning*) em uma SAN permite isolar determinados dispositivos e sistemas em uma rede com *fibre channel*. Por exemplo, para sistemas Unix, por meio de configurações de *zoning*, é possível isolar o acesso a dados em sistemas Windows em um *storage*.

120 Por meio da tecnologia VSAN (*virtual* SAN), é possível criar, em um mesmo *switch fibre channel*, vários *switches* lógicos, fazendo a segmentação entre os mesmos, o que permite o isolamento de tráfego.

121 IPSEC é o principal protocolo que garante a segurança em camada de rede em *fibre channel* com suporte a IP.

122 O *zoning* pode ser implementado em *hardware* ou em *software*. Na implementação em *software*, acontece o mascaramento do LUN (*logical unit number*), o que a torna mais segura e eficiente que o *zoning* implementado em *hardware*.

No que se refere à segurança da informação, bem como às técnicas, às tecnologias e aos conceitos a ela relacionados, julgue os próximos itens.

123 Em um processo de gestão de riscos de TI, é importante avaliar os riscos e estimar os seus impactos nos negócios da organização.

124 Um IDS (*intrusion detection system*) é capaz de procurar e detectar padrões de ataques em pacotes trafegados em uma rede local por meio de assinaturas de ataques conhecidos.

125 Um *firewall* do tipo *stateful* não depende do *three-way handshake* do protocolo TCP.

126 Em uma VPN do tipo *site-to-site*, a criptografia assimétrica envolve uma chave única para o processo de cifrar e decifrar os dados da conexão.

Julgue os itens que se seguem, acerca de máquinas virtuais, intrusão em sistemas e técnicas de invasão de sistemas.

127 O ataque mediante a utilização da técnica de *cross-site script* consiste em explorar falhas de aplicações *web* para inserir nessas aplicações determinados tipos de códigos que serão executados no lado cliente.

128 Ataques do tipo SQL *injection* exploram erros em aplicativos *web* que lhes permitam inserir, remover ou alterar dados em um banco de dados.

129 Em uma máquina virtual que esteja comprometida devido a um ataque, o atacante pode obter o controle da estação que gerencia a máquina virtual (*hipervisor*). Essa técnica utiliza despejo de memória e acessa os registros de controle da máquina virtual.

De acordo com as normas complementares, julgue o item abaixo.

130 A Norma Complementar GSI/PR n.º 3 estabelece as diretrizes para a elaboração de políticas de segurança da informação e comunicações nos órgãos e entidades da administração pública federal.