CONHECIMENTOS ESPECÍFICOS

No que se refere aos conceitos de segurança da informação, julgue os itens subsequentes.

51 A capacidade de localização de identidades preexistentes em sistemas conectados é uma funcionalidade de sistemas de gestão de identidades.

52 O repasse de informações institucionais a terceiros viola a política de confidencialidade fixada na política de segurança da informação de uma organização.

53 Escuta, análise de tráfego e falsificação são exemplos de ataques que ameaçam a integridade dos dados.

Acerca de segurança de banco de dados e de desenvolvimento de *software*, julgue os itens subsecutivos.

54 Na metodologia de desenvolvimento seguro de *software* SDL (*Security Development Lifecycle*), a modelagem de ameaças é realizada na fase de requisitos.

55 Os bancos de dados NoSQL são imunes a ataques de injeção SQL.

Julgue os itens a seguir, relativos à criptografia e suas aplicações.

56 Um *hash*, que é resultante de uma função de resumo, pode ser utilizado para gerar assinaturas digitais.

57 A decriptografia de dados por meio do algoritmo RC4 é realizada com sucesso se os dados tiverem sido criptografados mediante o algoritmo AES (*Advanced Encryption Standard*) e a mesma chave simétrica tiver sido utilizada em ambos os algoritmos.

58 A adição de um bite ao tamanho da chave duplica o tempo médio necessário para um ataque de força bruta.

59 RSA, 3DES e SHA-1 são métodos criptográficos que utilizam chave assimétrica.

A propósito de ataques a redes e serviços, julgue os próximos itens.

60 Quando a autenticação e o gerenciamento da sessão de aplicação não são feitos corretamente, ocorre o ataque de referência insegura a objetos, por meio do qual o atacante, ao assumir a identidade da vítima, compromete senhas, chaves e sessões *web*.

61 Diferentemente dos golpes de *phishing*, os ataques de *spear phishing* são realizados mediante o envio aleatório e em massa de *emails* enganosos para múltiplos usuários, para a obtenção de informações bancárias das vítimas ou apropriação da identidade delas.

62 Constituem estratégias para evitar ataques de XSS (*cross-site scripting*): a utilização da *flag* HTTPOnly nos *cookies*, pela qual se evita que estes sejam manipulados por JavaScript; e a ativação da *flag* Secure, que garante que o tráfego seja feito apenas por HTTPS.

63 Ataque de dia zero é um tipo de ataque de *software* projetado para ativar e realizar uma ação destrutiva em hora ou data específica.

64 Em ataques APT (*Advanced Persistent Threat*), são aplicadas técnicas de engenharia social para que se invadam, de forma discreta, os sistemas organizacionais.

Julgue os seguintes itens, relativos à segurança de aplicativos *web*.

65 A técnica de *fuzzing* do OWASP ZAP fornece entradas não válidas para qualquer tipo de mecanismo de entrada.

66 Limitar o tempo de vida dos *cookies* de uma sessão e implementar mecanismos de desafio-resposta, como o *captcha*, são contramedidas para ataques de CSRF (c*ross-site request forgery*).

À luz da NBR ISO/IEC 27005:2011, que dispõe diretrizes para o processo de gestão de riscos de segurança da informação (GRSI), julgue os itens a seguir.

67 Durante o processo de GRSI, é importante que os riscos, bem como a forma com que se pretende tratá-los, sejam comunicados ao pessoal das áreas operacionais e aos devidos gestores.

68 O processo de GRSI é iterativo tanto para o processo de avaliação de riscos quanto para as atividades de tratamento de risco.

Com relação ao que dispõe a NBR ISO 31000:2009 acerca da gestão de riscos, julgue os itens subsecutivos.

69 São consideradas as circunstâncias e as necessidades da organização para se determinar se a análise de riscos será qualitativa, quantitativa ou uma combinação dessas duas formas de análise.

70 A gestão de riscos é uma atividade autônoma e independente de outros processos da organização.

Com base na NBR ISO 22301:2013, que dispõe requisitos para a gestão de continuidade de negócios, julgue os itens que se seguem.

71 O controle dos processos terceirizados é opcional, motivo pelo qual as organizações podem avaliar tais processos apenas quando considerarem isso necessário.

72 Os objetivos da continuidade de negócios devem ser monitorados e, quando necessário, atualizados.

Com base no disposto na NBR ISO/IEC 27001:2013, julgue o item a seguir, relativo à gestão de segurança da informação.

73 Devido a seu conteúdo confidencial e estratégico, a política de segurança da informação de uma organização deve estar disponível, como informação documentada, exclusivamente para a alta gerência.

Acerca da análise de *malwares* executáveis em ambiente Windows, julgue os itens a seguir.

74 Por meio da análise estática, é possível descrever o comportamento de um *malware* como se ele estivesse sendo executado em tempo real.

75 Pela técnica de engenharia reversa, é possível obter o código-fonte de um *malware* e o nome real de suas funções, desde que utilizado um leitor hexadecimal.

76 Informações a respeito das funções que um *malware* executa podem ser obtidas pela extração de *strings* desse *malware*.

No que diz respeito à segurança em redes, julgue os próximos itens.

77 Para bloquear um ataque de XSS (*cross-site script*) a uma aplicação *web*, é suficiente desativar o suporte a XML no navegador do usuário.

78 Por padrão, um WAF (*web application firewall*) é capaz de utilizar as camadas de rede, de transporte e de aplicação da pilha TCP/IP.

79 Um ataque SQL *Injection* possibilita o envio de comandos SQL por meio de campos de entrada de aplicações *web*.

Acerca da ação de *softwares* maliciosos, julgue os itens subsequentes.

80 Um *rootkit* é uma ferramenta que manipula recursos do sistema operacional para manter suas atividades indetectáveis por mecanismos tradicionais, podendo, ainda, operar no nível de *kernel* do sistema operacional.

81 A atuação de um *adware* ocorre de maneira que o usuário não esteja ciente de que seu computador está sendo monitorado e de que suas informações estão sendo enviadas a um servidor de terceiros.

No que se refere a algoritmos e protocolos de segurança em redes *wireless*, julgue os itens que se seguem.

82 O padrão WPA2 não tem seu uso restrito ao modo de funcionamento para redes sem fio com padrões 802.11b.

83 O protocolo WEP (*wired equivalent privacy*) não é considerado seguro, uma vez que por meio de uso dos vetores de inicialização é possível quebrá-lo.

84 O padrão WPA2 é inseguro contra ataques de força bruta.

A respeito de configurações de segurança em servidores Linux e em servidores Windows 2012 R2, julgue os itens a seguir.

85 O Windows 2012 R2 possui uma ferramenta de segurança denominada ISA KMP (*Internet Security Association and Key Management Protocol*), que permite ao administrador do sistema configurar a segurança de um usuário no Windows.

86 Por padrão, após a instalação de um servidor Windows, qualquer usuário criado em uma estação Windows 2012 R2 será administrador do domínio.

87 No Linux, os *drivers* relacionados à implementação do *firewall* Iptables estão na camada de *kernel*, ligados ao conceito de *netfilter*.

Julgue os itens subsecutivos, acerca de ataques comuns realizados em testes de invasão (*pentests*).

88 Ferramentas automatizadas para ataques MITM (*man-in-the-middle*) na camada de enlace provocam muito ruído na rede e, consequentemente, ocasionam sobrecarga desnecessária e mau funcionamento dos *switches*.

89 *Phishing*, técnica pela qual é possível capturar senhas de usuários, pode utilizar mecanismos de engenharia social para tentar enganar as vítimas.

90 Um ataque de negação de serviço é dificilmente detectado em ambientes de rede.

Com relação aos protocolos NAC (*network access control*) e NAP (*network access protection*), julgue os seguintes itens.

91 Em redes Windows, o NAP não funciona com o protocolo RADIUS.

92 O padrão 802.1 X, que é uma forma de NAC, define formas de encapsulamento do EAP (*extensible authentication protocol*) sobre IEEE 802.

93 O NAP funciona em redes Windows e permite aos administradores de sistemas definirem políticas que permitam ou neguem acesso a uma estação na rede.

Julgue os próximos itens, acerca dos protocolos Syslog e Microsoft Event Viewer.

94 O nível de severidade das mensagens do Syslog varia entre 0 e 7.

95 As ferramentas de visualização de *logs* da Microsoft utilizam a tecnologia Azure com Elasticsearch para o processamento distribuído dos registros de segurança do sistema operacional. Nesse caso, o *plugin* AZEL é adicionado ao Event Viewer.

96 O mecanismo de geração de *logs* do Linux utiliza o Syslog por padrão, sendo algumas mensagens do sistema direcionadas para o arquivo `/var/log/messages`.

No que se refere a ferramentas e recursos de segurança nos sistemas operacionais Debian e Windows Server, julgue os itens a seguir.

97 A ferramenta de avaliação Microsoft Baseline Security Analyzer, suportada tanto no Windows Server 2008 R2 quanto no Windows Server 2012 R2, fornece uma metodologia simples e rápida para a identificação das atualizações de segurança ausentes.

98 *Nessus* é a mais completa e atualizada ferramenta de segurança disponibilizada no Debian para verificação remota de vulnerabilidades.

99 As ferramentas *tiger* e *flawfinder* são utilizadas na execução de auditorias internas de *hosts* no Debian para verificar se o sistema de arquivos está configurado de forma correta.

No que se refere à tipologia de ambientes com alta disponibilidade e escalabilidade para a estruturação de ambientes computacionais, julgue os itens subsequentes.

100 Denomina-se *failover* o processo, transparente ou não, em que um nó assume o funcionamento de outro nó em razão de este ter apresentado alguma falha.

101 Balanceamento de carga é um tipo de *cluster* cuja função é manter o sistema em plena condição de funcionamento por longo período de tempo.

102 *Cluster* é um ambiente composto de dois ou mais nós que trabalham em conjunto, como se fossem um único sistema, para a execução de aplicações e realização de tarefas.

103 Durante a operação correta do recurso de *clustering* de *failover*, ocorre um grande número de interrupções nos serviços oferecidos aos usuários.

Acerca dos diretórios de serviços LDAP e AD (*Active Directory*), julgue os itens que se seguem.

104 O servidor controlador de domínio (*domain controller*) é o único tipo de servidor aplicável em domínios que se baseiam no AD.

105 O AD, além de armazenar, em seu banco de dados, objetos como usuários, membros de grupos e relações de confiança, disponibiliza alguns serviços, como, por exemplo, a autenticação de usuários.

106 LDAP é um padrão aberto que facilita a manutenção e o compartilhamento do gerenciamento de grandes volumes de informação, definindo um padrão de acesso em um diretório.

Julgue os itens a seguir acerca do emprego da ferramenta *shell* no desenvolvimento de *scripts*.

107 A principal ferramenta do Unix utilizada para a realização de buscas no conteúdo dos arquivos é o `grep`, cujas variantes são `grep`, `egrep` e `fgrep`.

108 A expressão `teste.?` lista todos os arquivos de um diretório que contenha os arquivos `teste.c`, `teste.o` e `teste.log`.

109 Por utilizar uma linguagem padronizada conforme o padrão POSIX, o Script Bash apresenta simplicidade e portabilidade.

Julgue os itens seguintes, relativos à segurança em Linux.

110 No modo de operação *enforcing*, as regras do SELinux são desativadas e todas as operações geram *logs*.

111 A ferramenta IPTables controla o módulo Netfilter do *kernel* Linux, módulo que, por sua vez, controla as funções NAT, *firewall* e *log* do sistema.

112 O módulo ModSecurity do servidor *web* Apache oferece proteção contra ataques direcionados a aplicações *web* e permite o monitoramento e a análise do tráfego HTTP em tempo real, com reduzida ou nenhuma alteração de infraestrutura.

113 A técnica *hardening* é utilizada para mapear ameaças e executar, em nível lógico, possíveis correções nos sistemas, preparando-os para impedir tentativas de ataques ou de violação da segurança da informação.

Julgue os itens subsecutivos, referentes à gestão do ciclo de vida da informação — ILM (*Information Lifecycle Management*).

114 Classificação, implementação e gerenciamento são as três atividades envolvidas no processo de desenvolvimento de uma estratégia de ILM.

115 Em comparação aos dados não estruturados, os dados estruturados demandam mais espaço de armazenamento e um gerenciamento mais cauteloso, uma vez que constituem a maior parte dos dados corporativos.

116 DAS (*direct-attached storage*) é uma tecnologia de armazenamento de dados criada para que sejam direcionados os requisitos relativos ao custo, ao desempenho e à disponibilidade dos dados.

Julgue os itens a seguir, relativos às tecnologias e às arquiteturas de *data center*.

117 Em um *data center*, não deve haver janelas voltadas para ambiente externo.

118 É imprescindível a execução de aterramento na infraestrutura de qualquer *data center*.

119 A redundância 2N de um *data center* adiciona um módulo, caminho ou sistema ao mínimo necessário para satisfazer o requisito básico.

120 Se a classificação da parte elétrica de um *data center* for TIER 3 e a da parte mecânica for TIER 2, a classificação global desse *data center* será TIER 3.

Espaço livre