-- CONHECIMENTOS ESPECÍFICOS --

Acerca de conceitos relativos à segurança da informação, julgue os itens a seguir.

51 A criptografia de dados é um instrumento eficaz para a aplicação dos conceitos de confidencialidade, integridade, disponibilidade e autenticidade.

52 A validação de entrada de dados, quando eles são inseridos na base de dados por fontes e usuários desconhecidos, é uma prática que atende ao conceito de integridade.

53 A criptografia ajuda a determinar se os dados obtidos são provenientes de uma fonte confiável e não foram alterados durante a transmissão, obedecendo, assim, ao princípio da confidencialidade.

Julgue os itens a seguir, que tratam de gestão da segurança da informação.

54 Segundo a NBR ISO/IEC 27002:2022, são dois os tipos de controle nas políticas de segurança da informação: #Preventivo e #Corretivo.

55 Na NBR ISO/IEC 27002:2022, no atributo propriedades de segurança da informação incluem-se as visões de controle #Confidencialidade, #Integridade, #Disponibilidade e #Autenticidade.

56 Conforme a NBR ISO/IEC 27001:2022, as ações para abordar riscos e oportunidades devem conter um planejamento do sistema de gestão da segurança da informação.

Em relação ao *framework* do NIST e aos controles do CIS, julgue os itens que se seguem.

57 Nos controles CIS, empresas que geralmente armazenam e processam informações confidenciais de clientes são classificadas como IG2 ou IG3.

58 No *framework* do NIST, a função proteção desenvolve e implementa as atividades adequadas para manter os planos de resiliência contra um evento de segurança cibernética.

Em relação aos métodos de autenticação e seus principais protocolos, julgue os próximos itens.

59 O OAuth é um protocolo que fornece aos aplicativos a capacidade de acesso designado seguro por transmitir dados de autenticação entre consumidores e provedores de serviços.

60 A especificação do OpenID Connect determina que a autenticação pode ocorrer, entre outras formas, em fluxo implícito, no qual *tokens* são devolvidos diretamente para a parte confiável, em um URI (*Uniform Resource Identifier*) de redirecionamento.

61 O MFA pode utilizar o fator de inerência, conhecido como autenticação por biometria, por ser uma das opções mais seguras disponíveis, considerando a sua dificuldade de ser contornada.

Em relação a ameaças e vulnerabilidades em aplicações, julgue os itens subsequentes.

62 São exemplos de armazenamento criptográfico inseguro: imprudência no armazenamento de chaves e utilização de um *hash* para proteção de senhas sem o *salt.*

63 SQL *injection*, LDAP *injection* e XSS (*cross-site scripting*) são ataques do tipo injeção de código que podem ser explorados por *hackers* ou criminosos.

64 *Cross-site request forgery* é um vetor de ataque que faz que o navegador *web* execute uma ação indesejada na aplicação *web* alvo onde a vítima está logada.

65 Ao contrário do LDAP *injection*, em que o invasor pode inserir ou manipular consultas criadas pela aplicação, no SQL *injection* o invasor pode apenas inserir consultas na aplicação, que são enviadas diretamente para o banco de dados.

66 O SQL *injection* e o *cross-site scripting* utilizam a linguagem JavaScript.

67 A quebra de autenticação é uma falha no mecanismo de controle de acesso, permitindo que usuários acessem recursos ou realizem ações fora de suas permissões; caso ocorra, o limite para o dano pode ser superior, inclusive, aos privilégios concedidos ao perfil de usuário da aplicação que sofreu o ataque.

68 A adulteração de URL é a forma mais simples de ataque de referência insegura a objetos.

Um servidor *web* de uma empresa de *e-commerce* foi alvo de um ataque DDoS. Durante o ataque, o servidor começou a apresentar lentidão extrema, tornando-se incapaz de atender às requisições legítimas dos clientes. A equipe de segurança detectou um tráfego anormal proveniente de diversos endereços IP, todos de dispositivos comprometidos em diferentes partes do mundo, que inundavam o servidor com solicitações massivas e simultâneas, visando interromper ou degradar significativamente a disponibilidade do serviço de *e-commerce*.

Tendo como referência a situação hipotética precedente, julgue os itens a seguir.

69 Envenenamento de *cache* DNS pode ser uma técnica associada a ataques DDoS.

70 A principal consequência de um ataque DDoS é a perda de integralidade dos dados armazenados no servidor atacado.

71 Infere-se da situação que o ataque DDoS afeta a disponibilidade do serviço *web* da empresa de *e-commerce*.

72 A técnica utilizada no ataque descrito envolve a modificação de mensagens para causar um efeito de acesso não autorizado.

Uma grande empresa que recentemente migrou suas operações para um ambiente de nuvem está preocupada com a integridade, confidencialidade e disponibilidade dos seus dados, especialmente devido a incidentes recentes de segurança que ocorreram em outras organizações do mesmo setor de negócios. Essa empresa utiliza serviços de IaaS (*Infrastructure as a Service*) e está sob constante ameaça de ataques como modificação de dados, espionagem na rede, *phishing*, DDoS, *ransomware*, entre outros. Com isso, a área de segurança digital solicitou uma análise detalhada das possíveis vulnerabilidades e das medidas necessárias para mitigá-las.

A partir da situação hipotética precedente, julgue os seguintes itens, em relação à segurança da informação.

73 *Phishing* é um ataque que compromete apenas a confidencialidade das informações.

74 O uso de SSL/TLS ajuda a prevenir ataques de negação de serviço.

75 Utilizar funções de *hash* como MD5 ou SHA1 para verificação de integridade é uma ação eficaz contra modificação não autorizada durante a transmissão de arquivos.

Um grande banco brasileiro sofreu um ataque de *ransomware*. Os sistemas ficaram inacessíveis quando os funcionários chegaram ao trabalho na manhã de segunda-feira e os clientes não conseguiram acessar suas informações financeiras. Os sistemas internos do banco exibiam uma mensagem na tela dos computadores na qual se exigia um pagamento em *bitcoins* para a liberação dos dados. A equipe de segurança da referida instituição financeira identificou que o ataque começara durante o fim de semana e que os *backups* estavam criptografados.

Com referência a essa situação hipotética, julgue os próximos itens, a respeito de ações para mitigar os danos causados pelo ataque de *ransomware*, recuperar as operações e prevenir futuros incidentes dessa natureza.

76 O pagamento do resgate representa a garantia da recuperação imediata de todos os dados criptografados.

77 A implantação de uma política de *backup* e restauração robusta, além de um plano de gestão de crises, é medida preventiva e reativa eficaz para minimizar o impacto dos ataques de *ransomware* na referida instituição financeira.

78 A referida instituição financeira pode resolver o problema sem pagar o resgate, utilizando os *backups* de dados.

Julgue os itens que se seguem, relativos a *port scanning*.

79 Todos os *logs* relacionados ao *port scanning* devem ser mantidos por um período longo, com o objetivo de análise futura e conformidade com normas de segurança, bem como para permitir a identificação de ataques de cadeias longas.

80 O *port scanning* não pode ser prevenido, sendo possível apenas a sua detecção, pois é uma técnica muito comum e não há forma de interrompê-la.

81 O *port scanning* é usado, com o processo de *hardening*, para garantir que as portas estejam corretamente configuradas e seguras.

Um usuário recebeu um *email*, aparentemente vindo do departamento de TI da sua empresa, no qual lhe era solicitada a validação urgente de suas credenciais em um *link* incluído na mensagem, sob pena de um possível bloqueio das credenciais caso a solicitação não fosse atendida. Sem desconfiar da mensagem, o usuário clicou no *link* e preencheu um formulário com seu nome de usuário e senha. Posteriormente, descobriu-se que as informações prestadas pelo usuário foram usadas por terceiro para acessar dados confidenciais e realizar atividades não autorizadas, em um ataque de *phishing*.

Considerando essa situação hipotética, julgue os itens seguintes.

82 A melhor contramedida contra o *phishing* seria usar algoritmos de criptografia mais robustos nas comunicações de *email* efetuadas na empresa.

83 A implantação de autenticação multifator (2FA) poderia ajudar a mitigar o ataque de *phishing*.

A respeito de técnicas de proteção de aplicações *web*, julgue os itens subsequentes.

84 A implantação de 2FA aumenta a complexidade para acesso ao sistema, mas não oferece ganhos em relação à segurança.

85 O armazenamento de credenciais em texto puro no banco de dados é uma prática segura, desde que o acesso ao banco de dados seja bem controlado.

86 A utilização de HTTPS para todas as comunicações entre cliente e servidor elimina a necessidade de outras medidas de segurança.

Acerca de criptografia e proteção de dados, julgue os itens a seguir.

87 Determinados algoritmos de *hash* podem sofrer colisões que impedem a correta verificação de integridade.

88 Uma função *hash* permite a transformação de uma grande quantidade de dados (de tamanho variado) em uma pequena quantidade de informações com saída de tamanho fixo.

89 *Salting* é uma medida de segurança adicional que pode ser adicionada ao *hash* de uma senha para aumentar sua resiliência contra ataques.

90 Independentemente do tamanho de dados armazenados, a técnica criptográfica mais eficiente e rápida é a de chave pública.

91 Em criptografia de curva elíptica, para ser considerada uma curva elíptica, a equação $y^2 = x^3 + ax + b$ deve ser satisfeita.

92 A criptografia de curva elíptica é um tipo de sistema criptográfico simétrico embasado na estrutura algébrica de curvas elípticas sobre campos infinitos.

Em relação ao processo de geração e verificação de assinatura digital embasado em certificados digitais, julgue os itens que se seguem.

93 Na verificação da assinatura digital, o destinatário da mensagem deve usar sua própria chave pública para verificar a assinatura.

94 Durante a geração da assinatura digital, o emissor usa a chave pública do destinatário para fazer a assinatura digital, garantindo a confidencialidade.

Tendo em vista as boas práticas de segurança em redes de comunicação, julgue os seguintes itens.

95 A detecção de ataques baseados em filtros com regras YARA permite o reconhecimento de padrões em arquivos de texto ou binários.

96 Técnicas de ofuscação de binários bem executadas são capazes de burlar o processo de verificação do antivírus.

Um administrador de rede precisa fazer configurações de permissão ou negação de tráfego para os protocolos na pilha TCP/IP entre redes com um *firewall* como elemento de controle de fluxo.

A partir dessa situação hipotética, julgue os próximos itens.

97 Para que o IMAP e o IMAPS sejam negados em suas portas padrão, o administrador deve bloquear as portas 143 e 993, ambas com o TCP.

98 Para que o HTTPS seja admitido em sua porta padrão, o administrador precisa permitir o UDP na porta 443.

Julgue os itens a seguir, a respeito de segurança de redes sem fio e de segurança de ativos de redes.

99 O SNMPv3 suporta autenticação e criptografia, permitindo três níveis de segurança diferentes: NoAuthNoPriv, AuthNoPriv e AuthPriv.

100 Conforme o padrão IEEE 802.11ax, é irrelevante o uso de MFP (*Management Frame Protection*) para manter a resiliência de redes de missão crítica, já que o MFP usa tecnologia insegura.

101 WPA3 evita o uso da tecnologia SAE (*Simultaneous Authentication of Equals*), que permite ataques para a quebra de senha de usuários por falhas no vetor de inicialização.

102 Um roteador e um *switch* podem fazer uso da funcionalidade do Engine ID Identifier no SNMPv3, que agrega uma dupla identidade a um pacote SNMPv3 para fins de redução do tamanho do fluxo de dados entre elemento controlador e elemento controlado.

103 O SNMPv3 garante a integridade da mensagem: se um pacote for alterado durante o trânsito, ele pode ser facilmente detectado e descartado.

Julgue os próximos itens, relativos a continuidade do negócio e resposta a incidentes de segurança da informação.

104 Os *backups* ou cópias dos dados contidos em um sistema de informação compõem estratégias de recuperação em caso de desastres, mas não garantem a recuperação da infraestrutura de TI.

105 Três elementos devem ser considerados em um plano de recuperação de desastres de um sistema de TI: a prevenção, a detecção e a recuperação.

106 O plano de recuperação de desastres é um conjunto de procedimentos documentados que visa recuperar dados e serviços de tecnologia da informação após a ocorrência de um incidente de segurança.

107 As siglas RTO e RPO referem-se, respectivamente, ao tempo necessário para a recuperação dos dados e ao estado pontual que se deve recuperar em um sistema afetado por um incidente de segurança.

108 Mediante um plano de recuperação de desastres, deve-se buscar eliminar qualquer possibilidade de desastre ou perda de dados provocados por incidentes de segurança nos serviços de TI de uma instituição.

109 Quando ocorre um incidente de segurança que impacta o correto funcionamento de um sistema de TI, pode-se recorrer ao plano de contingência para a manutenção da continuidade do negócio.

110 Um plano de contingência pode descrever, por exemplo, que certos processos automatizados em um sistema de informação comprometido devem ser executados manualmente, enquanto se busca a recuperação do sistema.

111 Os desastres relacionados a sistemas de TI restringem-se aos causados por falhas em equipamentos e *softwares* e aos provocados por ataques maliciosos ou falhas humanas.

Em relação ao gerenciamento de crises e à gestão de incidentes de segurança da informação, julgue os itens seguintes.

112 A legislação brasileira recomenda que as empresas que manipulam ou armazenam dados pessoais de terceiros possuam um processo formal de gestão de incidentes de segurança da informação.

113 A adoção de um plano de gestão de incidentes de segurança da informação não reduz a probabilidade de ocorrência de desastres, mas ajuda na solução do problema quando da sua ocorrência.

114 O gerenciamento de crise no setor de TI envolve exclusivamente os incidentes de violação de dados e interrupção de serviços ocasionados por fatores internos ou externos à instituição.

115 O monitoramento de mídias sociais e de notícias veiculadas nos meios de comunicação em busca de informações que afetam a imagem de uma organização constitui uma forma proativa de prevenção de crise.

116 Um plano de gestão de incidentes de segurança da informação deve garantir, entre outras coisas, o sigilo absoluto dos fatos ocorridos após a detecção e contenção do incidente.

Julgue os próximos itens, a respeito da norma NBR ISO/IEC 15999.

117 A norma em questão foi publicada em 2008 e posteriormente alterada por outra NBR no que tange às terminologias da gestão da continuidade de negócios.

118 A referida norma, baseada em norma britânica, trata da gestão de continuidade do negócio nas organizações.

Acerca da Lei n.º 13.709/2018 (Lei Geral de Proteção de Dados Pessoais — LGPD), julgue os itens subsequentes.

119 A LGPD criou a Autoridade Nacional de Proteção de Dados (ANPD), órgão responsável, entre outras atribuições, por fiscalizar e aplicar sanções administrativas em casos de descumprimento das normas de tratamento de dados previstas na LGPD.

120 Entre as sanções administrativas aplicáveis pela autoridade nacional a agente de tratamento de dados que cometa infração às normas da LGPD, inclui-se multa diária, limitada a R$ 50 milhões.