-- CONHECIMENTOS ESPECÍFICOS --

A respeito de configuração de rede de computadores, compartilhamento de recursos e arquitetura TCP/IP, julgue os itens a seguir.

51 O compartilhamento de recursos de rede está relacionado aos dados, às informações ou aos dispositivos de *hardware* de um computador, os quais podem ser acessados por meio de qualquer outro computador que esteja conectado à Internet.

52 A arquitetura TCP/IP prevê a segurança no processo de troca de dados entre *hosts*, apresentando ainda a vantagem de ser uma tecnologia que possibilita a conexão entre sistemas não compatíveis.

53 Uma rede local configurada, em IPv4, com endereço de rede 172.27.10.0 e máscara de rede 255.255.255.0 tem a capacidade de distribuir endereços lógicos para até 254 *hosts*.

Julgue os próximos itens, em relação a *malwares* e *spywares*.

54 O *cookie* de rastreamento é um tipo de *spyware* que monitora as atividades de um usuário em um computador e as envia ao invasor.

55 *Malware* é um termo genérico para qualquer tipo de *software* malicioso projetado para prejudicar ou mesmo explorar quaisquer dispositivos, serviços ou rede de computadores.

Acerca do *Active Directory* da Microsoft e dos serviços de *help desk*, julgue os itens que se seguem.

56 O *help desk* pode ser voltado para o público interno, quando auxilia os colaboradores internos da empresa em relação a algum problema técnico, ou pode ser voltado para o público externo, quando um cliente, por exemplo, necessita de algum tipo de suporte sobre um produto ou serviço adquirido na empresa.

57 O *help desk* é a área do setor de TI que atua quando há problemas de alta complexidade.

58 O *Active Directory* possui um serviço de replicação que distribui todos os dados do diretório por meio de uma rede de computadores, de modo que todos os controladores de um domínio contenham uma cópia completa de todas as informações desse domínio.

Julgue os itens seguintes, que tratam do sistema operacional Windows Server e do pacote Microsoft Office.

59 O DHCP permite que um servidor distribua dinamicamente informações de configuração e endereçamento IP às máquinas clientes de uma rede, fornecendo, em geral, pelo menos, o endereço IP, a máscara de sub-rede e o *gateway* padrão.

60 O Microsoft Word não é capaz de fazer a conversão de um arquivo `PDF` para um arquivo com formato editável do tipo `.docx`, sendo necessário, para isso, o uso de *software* de terceiros.

61 O Windows Server não oferece nativamente serviços como DNS e DHCP, que devem ser instalados pelo próprio usuário, se necessário.

A respeito do uso de *software* de correio eletrônico e dos serviços FTP, julgue os itens subsequentes.

62 Há três maneiras de estabelecer uma conexão FTP: por meio de linha de comando, de navegadores e de um cliente FTP; a conexão por meio de navegadores é a que oferece mais recursos aos usuários.

63 As versões mais atuais do Microsoft Outlook permitem armazenar informações de contatos e gerenciar calendário e tarefas.

Julgue os itens seguintes, que tratam de banco de dados.

64 No contexto de arquitetura de dados, o modelo de dados lógicos, também conhecido como modelo de domínio, oferece uma visualização geral do conteúdo do sistema, como ele será organizado e quais regras de negócios estão envolvidas.

65 Os bancos de dados orientados a objetos são aqueles cujas informações são representadas como objetos e organizadas como um conjunto de tabelas com colunas e linhas.

Julgue os itens a seguir, relacionados aos meios de transmissão utilizados em redes de comunicação.

66 O meio de transmissão não guiado pode ser utilizado em comunicação do tipo *multicast* na faixa de micro-ondas.

67 Em comunicação via fibra óptica, uma das vantagens do uso de *laser* é sua potência luminosa altamente direcionada, que permite a transmissão de dados em altas taxas e entre grandes distâncias.

68 Na faixa do infravermelho em meio não guiado, a velocidade de transmissão de dados pode atingir 4.000 Mbps.

69 Nas redes de comunicação atuais, os cabos metálicos trançados da categoria 7 (Cat7) estão sendo adotados em substituição aos cabos metálicos trançados da categoria 6 (Cat6).

70 Por serem imunes aos ruídos eletromagnéticos, as fibras ópticas monomodo são mais utilizadas que as fibras ópticas multimodo em redes de comunicação.

Acerca dos tipos de serviço e qualidade de serviço em redes de comunicação de dados, julgue os seguintes itens.

71 Nos serviços do tipo integrado, a qualidade do serviço é baseada em fluxos projetados para o IP (Internet *protocol*).

72 Nas reservas de recursos realizadas com o RSVP (*resource reservation protocol*), o remetente faz a reserva do recurso e cabe ao destinatário aceitar ou não essa reserva.

73 Na qualidade de serviço (QoS) de granularidade fina, o provedor do serviço permite que o cliente indique os requisitos específicos de QoS para uma determinada instância de comunicação.

74 Na categoria de serviços com taxa de *bits* disponível (ABR – *available bit rate*), devem ser especificadas a taxa de *bits* sustentada (SBR – *sustained bit rate*) e a taxa de *bits* de pico (PBR – *peak bit rate*).

75 Na técnica de conformação do tipo fluxo balde furado (*leaky bucket*), o número máximo de pacotes (n) é $n = r \cdot t + c$, em que r é a taxa de entrada de fichas no balde por segundo, t é o tempo da transmissão e c é a capacidade de fichas do balde.

Julgue os próximos itens, com relação aos protocolos de comunicação utilizados em redes de comunicação.

76 A base do funcionamento do protocolo OSPF (*open short path first*) é o algoritmo de Djikstra.

77 No SNMP (*simple network management protocol*), as variáveis monitoradas são restritas às disponíveis no protocolo base.

78 O UDP (*user datagram protocol*) é um protocolo da camada de transporte que apresenta verificação de integridade dos segmentos recebidos.

79 A finalização de uma conexão TCP (*transmission control protocol*) ocorre com a realização de dois processos *two-way handshake* do tipo `FIN` e `ACK`.

80 Com o advento dos protocolos de roteamento dinâmico, o roteamento estático perdeu sua significância e praticamente está em desuso.

Com base na NBR ISO/IEC 27001, julgue os próximos itens, a respeito de gestão de segurança da informação.

81 As organizações devem realizar avaliações *ad hoc* sobre os riscos de segurança da informação, independentemente da proposição ou da ocorrência de mudanças significativas.

82 Em uma instituição produtiva, a alta direção pode atribuir responsabilidades e autoridades para relatar o desempenho de seu sistema de gestão da segurança da informação.

Julgue os itens seguintes, relativos a métodos e protocolos de autenticação.

83 O programa ICP-Brasil é um método de autenticação baseada em certificados e, entre seus principais componentes de infraestrutura de chaves públicas, se encontra a CA (autoridade de certificação), que é um servidor que mantém uma lista dos certificados que foram revogados ou cancelados.

84 JSON Web Tokens é um padrão para autenticação e troca de informações que pode ser assinado usando-se um segredo ou par de chaves privadas/públicas em um cenário de autorização no qual, depois que o usuário estiver conectado, será possível observar cada solicitação e verificar se esta inclui o JWT, permitindo que o usuário acesse rotas, serviços e outros recursos.

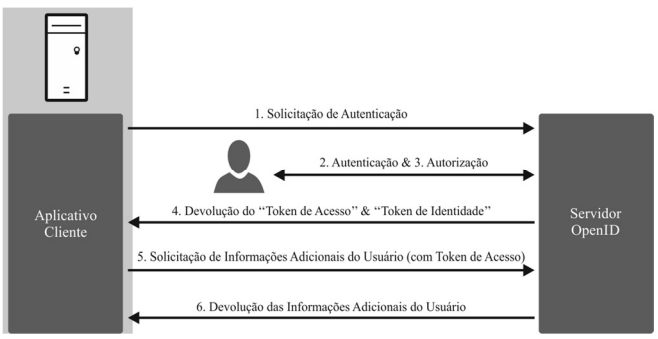
85 As notificações por *push* são um formato de autenticação de dois fatores (2FA) no qual os usuários, em vez de receberem um código em seu dispositivo móvel, via SMS ou mensagem de voz, recebem uma notificação por *push* em um aplicativo seguro no dispositivo registrado no sistema de autenticação, o que reduz a possibilidade de riscos de segurança como *phishing*, ataques *man-in-the-middle* e tentativas de acesso não autorizado.

86 A forma automática de autenticação biométrica por impressão digital é realizada por peritos que, mediante inspeção visual, cotejam impressões digitais para determinar se são ou não iguais.

87 A autenticação baseada em *token* consiste no processo de verificar a identidade por meio de um *token* físico que envolve a inserção de um código secreto ou mensagem enviada a um dispositivo para provar a posse desse dispositivo.

88 O protocolo OAuth 2, adotado por instituições de governo para autenticação e controle dos acessos às suas APIs, permite que aplicativos obtenham acesso limitado a contas de usuários em um serviço HTTP, sem a necessidade de envio do nome de usuário e da senha.

89 Um aplicativo cliente que realiza a autenticação de um usuário mediante um servidor de autorização que adota o OpenID Connect recebe de volta um *token* de acesso e um *token* de identidade com algumas informações adicionais do usuário, seguindo o fluxo de autenticação representado a seguir.



Acerca de ameaças e vulnerabilidades em aplicações, julgue os itens subsequentes.

90 Para que um ataque de *cross-site request forgery* funcione em aplicações *web*, basta que a vítima tenha conectado, em algum momento, sua conta original ao disparar a requisição maliciosa.

91 Uma aplicação torna-se vulnerável pelo armazenamento inseguro de dados criptografados quando, por exemplo: dados sensíveis não são cifrados; a criptografia é usada de forma incorreta; o armazenamento das chaves é feito de forma imprudente; ou utiliza-se um *hash* sem *salt* para proteger senhas.

92 Em função de muitos *sites* e aplicativos da Web dependerem de bancos de dados SQL, um ataque SQL *injection* pode gerar sérias consequências, porque boa parte dos formulários da Web não consegue impedir a entrada de informações adicionais, o que propicia a exploração desse ponto fraco e o uso das caixas de entrada no formulário para envio de solicitações maliciosas ao banco de dados.

93 A injeção de LDAP é um vetor de ciberataque sofisticado que visa às vulnerabilidades da camada de aplicação dos sistemas que utilizam o protocolo LDAP. Particularmente, aplicações Web com *backends* LDAP estão imunes a esse tipo de ataque, e os riscos associados à injeção de LDAP se limitam à exposição de dados.

94 Um ataque de XSS (*cross-site scripting*) não tem como alvo direto o próprio aplicativo, mas sim os usuários do aplicativo da Web.

No que se refere à segurança da informação, julgue os itens subsecutivos.

95 Uma das formas de prevenção à vulnerabilidade SQL *injection* consiste em realizar a validação dos dados digitados pelo usuário mediante a aceitação de somente dados que sejam conhecidamente válidos.

96 No *cross-site scripting* refletido (não persistente), a carga útil do invasor deve fazer parte da solicitação enviada ao servidor da Web. Em seguida, é refletida de volta, de maneira que a resposta HTTP inclua a carga útil da solicitação HTTP. Os invasores usam técnicas de engenharia social para induzir a vítima a fazer uma solicitação ao servidor. A carga útil XSS refletida é, então, executada no navegador do usuário.

97 Ocorre quebra de autenticação e gerenciamento de sessões quando, por exemplo, um atacante obtém acesso a uma conta bancária, modifica ou exclui informações do sistema ou altera as configurações de segurança, podendo causar perdas financeiras significativas e até mesmo a quebra de confiança da entidade no cliente dono da conta.

98 Referências diretas inseguras a objetos, ou IDOR (*insecure direct object reference*), são vulnerabilidades resultantes de controle de acesso interrompido em aplicativos da Web. Um tipo de ataque é a passagem de diretório, que é a maneira mais simples de explorar uma vulnerabilidade IDOR, bastando simplesmente alterar o valor de um parâmetro na barra de endereço do navegador.

Julgue os itens que se seguem, tendo em vista a NBR ISO/IEC 27002.

99 Convém que os incidentes de segurança da informação de uma organização sejam reportados e, assim que eles tenham sido tratados, seu registro seja mantido, mesmo que informalmente.

100 No gerenciamento de mídias removíveis, quando houver a necessidade de seu uso, convém que a transferência da informação contida na mídia (incluídos documentos em papel) seja monitorada pela organização.

Com base na NBR ISO/IEC 27005, julgue os itens a seguir, a respeito de gestão de riscos e continuidade de negócio.

101 No processo de avaliação de ameaças, as ameaças intencionais indicam ações de origem humana que podem comprometer os ativos de informação.

102 Ferramentas automatizadas de procura por vulnerabilidades são utilizadas, em computador ou em rede de computadores, para a busca de serviços reconhecidamente vulneráveis que possam gerar falsos positivos.

103 Para estabelecer o valor dos seus ativos, a organização deve primeiramente identificá-los, distinguindo-os em dois tipos: primários ou secundários.

104 Convém que a alta direção da organização avalie os riscos e aceite uma parcela dos riscos de forma consciente e calculada, para evitar custos excessivos em segurança.

Julgue os seguintes itens, a respeito de segurança de aplicativos *web*.

105 A análise de vulnerabilidades em aplicações *web* deve ser realizada apenas durante a fase de desenvolvimento do aplicativo.

106 A implementação de HTTPS em uma aplicação *web* é suficiente para protegê-la contra todos os tipos de ataques cibernéticos.

107 A OWASP recomenda que as empresas implementem o OWASP Top 10 como um padrão obrigatório para garantir a segurança de seus aplicativos *web*.

Com base na Lei n.º 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), julgue os itens que se seguem.

108 O controlador poderá implementar programa de governança em privacidade que preveja, no mínimo, planos de resposta a incidentes e remediação.

109 Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança.

110 O controlador deverá realizar o tratamento de dados pessoais segundo as instruções fornecidas pelo operador, que deverá verificar a observância das próprias instruções e das normas sobre a matéria.

111 O Conselho Nacional de Proteção de Dados Pessoais e da Privacidade compõe-se, entre outros titulares e suplentes, de três membros de instituições científicas, tecnológicas e de inovação, os quais não poderão ser membros do Comitê Gestor da Internet no Brasil.

A respeito de prevenção e combate a ataques a redes de computadores, julgue os itens subsecutivos.

112 Uma forma de se prevenir e combater o ataque *port scanning* é manter protegidas ou bloqueadas as portas dos computadores da rede.

113 Os ataques de DoS e DDoS utilizam apenas um único computador para sobrecarregar um servidor de rede, tornando-o indisponível, sendo necessário apenas um *software* antivírus para prevenir e combater esses ataques.

114 Uma forma de se prevenir o ataque cibernético do tipo *eavesdropping* é utilizar criptografia de ponta a ponta tanto em redes de computadores quanto em sistemas de comunicação sem fio.

115 O *port scanning* pode ser utilizado tanto por administradores de rede quanto por *hackers* para identificar vulnerabilidades em sistemas de rede de computadores.

Julgue os próximos itens, a respeito de criptografia, proteção de dados, sistemas criptográficos simétricos e assimétricos e principais protocolos.

116 Os sistemas criptográficos assimétricos utilizam um par de chaves, uma pública e uma privada, para criptografar e descriptografar dados.

117 RSA e ECC são os principais protocolos utilizados na criptografia simétrica.

118 A criptografia é uma técnica utilizada para proteger dados tanto em trânsito quanto em repouso, garantindo a confidencialidade e a integridade das informações contra acessos não autorizados.

Julgue os itens que se seguem, relativos a assinatura e certificação digital.

119 O protocolo de certificação digital é um conjunto de regras e procedimentos que garantem a emissão, validação e revogação de certificados digitais, assegurando a autenticidade e a integridade das transações eletrônicas.

120 A assinatura digital e o certificado digital têm o mesmo objetivo: apenas autenticar a identidade de uma pessoa em documentos eletrônicos.

Espaço livre