1 - Programa de computador de encriptação e descriptografia de dados que fornece autenticação e privacidade criptográfica para comunicação de dados. Frequentemente utilizado, por exemplo, para assinatura digital, criptografia de textos, e-mails, arquivos, diretórios e partições inteiras de disco para incrementar a segurança de comunicações. Este programa é conhecido por:

a) ICP
b) Cookie.
c) Cifra de César
d) Crypt.
e) PGP

2 - É um programa que registra tudo o que é digitado em um determinado computador e envia o conteúdo para e-mails preestabelecidos. Seu principal objetivo é capturar senhas e tecnicamente denomina-se:

a) Adware.
b) Backdoor.
c) Hoax
d) Vírus.
e) Keylogger

3 - Relacionado à Segurança da Informação, o conjunto de programas que tem como fim esconder e assegurar a presença de um invasor em um computador comprometido é conhecido como:

a) Adware
b) Rootkit.
c) Worm.
d) Backdoors
e) Spyware.

4 - É um método de autenticação que tenta medir algo intrínseco ao usuário podendo ser, por exemplo, uma impressão digital, a palma da mão, a imagem da face, a retina ou íris dos olhos. Esse método se chama:

a) Audiometria
b) Criptografia
c) Biometria.
d) Radius.
e) Caligrafia.

5 - No processo de verificação de assinatura digital, o destinatário recebe a mensagem assinada e utiliza, para verificar a assinatura,

a) sua chave pública.
b) a chave pública do remetente.
c) a chave privada do remetente.
d) sua chave privada.
e) a chave privada do remetente e a sua chave pública.

6 - Um dos esquemas criptográficos mais utilizados atualmente é o esquema conhecido como criptografia de chave pública. Neste esquema,
a) o emissor codifica a mensagem utilizando a chave privada e o receptor decodifica a mensagem utilizando a chave pública.
b) o emissor codifica a mensagem utilizando a chave pública e o receptor decodifica a mensagem utilizando a chave privada.
c) uma mesma chave pode fazer simultaneamente o papel de chave pública e de chave privada na comunicação, mediante prévio acordo entre emissor e receptor.
d) caso o sigilo da chave privada seja comprometido, é possível substituí-la, sem ser necessário substituir a chave pública.
e) não é possível implementar assinaturas ou certificados digitais.

7 - Na virada do mês de janeiro para fevereiro de 2012, os sites de diversos bancos comerciais brasileiros foram alvos de ataques através da Internet com o objetivo de deixá-los inacessíveis. O tipo de ataque de que foram vítimas estes bancos é conhecido genericamente pelo nome de

a) port scanning.
b) backdoor.
c) cookie hijacking.
d) denial of service.
e) phishing.

8 - Marque a opção que é definida como uma característica ou falha no projeto, implementação ou configuração de um software ou sistema operacional que, quando explorada por um atacante, resulta na violação da segurança de um computador.

a) Autenticidade.
b) Confidencialidade.
c) Integridade.
d) Não-repúdio.
e) Vulnerabilidade

9 - Quanto a Segurança da Informação precisamos agir continuamente para combater aos constantes ataques de hackers e crackers que podem causar vários danos aos computadores. Dentre os meios técnicos que auxiliam na proteção de uma rede de computadores à ação de hackers e crackers, inclui-se o:

a) ATM.
b) RIP
c) IDS
d) RSS.
e) IRC

10 - Quanto à criptografia, as mensagens a serem criptografadas, conhecidas como texto simples, são transformadas por uma função que é parametrizada por uma chave. Em seguida, a saída do processo de criptografia, é conhecida como texto cifrado, e transmitida. Neste contexto, criptografia simétrica é um método de codificação que utiliza:

a) Duas chaves privadas para codificar e decodificar a mensagem
b) Uma chave simples e uma chave composta para codificar e decodificar a mensagem.
c) A mesma chave para codificar e decodificar a mensagem
d) Duas chaves públicas para codificar e decodificar a mensagem
e) Uma chave pública e uma chave privada para codificar e decodificar a mensagem.

11 - Uma forma de se evitar fraudes através de ataques conhecidos por man-in-the-middle é certificar-se que, quando acessar um site seguro (Exemplo: Bancos, Lojas de compras, etc) o navegador:

a) apresente a identificação http.
b) apresente a identificação https
c) apresente a identificação do fabricante do Sistema Operacional como Site Confiável
d) esteja indicando o nome correto do site acessado.
e) apresente o cadeado fechado (obtenção da aprovação da certificadora digital).

12 - Uma das maneiras de promover a segurança em conexões na World Wide Web é a utilização do Hypertext Transfer Protocol Secure (HTTPS) em lugar do Hypertext Transfer Protocol (HTTP). A seu respeito é correto afirmar que

a) para estabelecer uma conexão HTTPS, o servidor deve ser capaz de criptografar e decriptografar o conteúdo transmitido; a mesma capacidade não é necessária da parte do cliente (navegador).
b) para o uso do protocolo HTTPS é necessário que o cliente (navegador) esteja habilitado a processar e armazenar pacotes de informação conhecidos como cookies.
c) o port reservado pela Internet Assigned Numbers Authority (IANA) para conexões HTTPS é o de número 22.
d) estritamente falando, HTTPS não é um protocolo diferente do protocolo HTTP mas, simplesmente, um nome para o uso do protocolo HTTP através de uma conexão criptografada.
e) o protocolo HTTPS permite a transmissão segura entre cliente e servidor sem a necessidade de certificados digitais emitidos por terceiros.

13 - Com relação a ataques DoS (Denial of Service) e DDoS (Distributed Denial of Service), analise:

I. O ataque DoS (Denial of Service), é também denominado ataque de negação de serviço.
II. No ataque DoS o atacante tenta tornar os recursos de um sistema indisponíveis para seus usuários.
III. DDoS, constitui um ataque de negação de serviço distribuído, ou seja, um conjunto de computadores é utilizado para tirar de operação um ou mais serviços ou computadores conectados à Internet.

Marque a opção que apresenta apenas as afirmativas corretas:

a) Somente a I.
b) Somente II e III
c) Somente a III.
d) Somente I e II
e) I, II e III.

14 - Um site oficial do governo foi vítima de um ataque. Este ataque foi promovido por um programa semelhante ao vírus, mas se diferenciam por se espalharem sem a intervenção do usuário e se distribuem através de replicação automática, algumas vezes com mutações para dificultar sua identificação. Eles são conhecidos como:

a) Adwares.
b) Hoaxs
c) Trojans
d) Worms
e) Backdoors.

15 - É conhecido como um arquivo eletrônico que contém dados de uma pessoa ou instituição, utilizados para comprovar sua identidade. Este arquivo pode estar armazenado em um computador ou em outra mídia, como um token ou smart card. Estamos falando em:

a) Mídia digital.
b) Certificado digital.
c) Token Smart.
d) Certificado inteligente.
e) Token digital

16 - O antivírus é um programa desenvolvido com o propósito de detectar, prevenir, eliminar vírus e outros tipos de softwares nocivos aos sistemas digitais. Qual das alternativas abaixo NÃO representa um software danoso que pode ser eliminado por um antívirus?

a) Trojan
b) Backdoor
c) Spyware
d) Ransomware
e) Shareware

17 - No contexto da segurança em redes de computadores, o termo firewall pode ser considerado uma espécie de:

a) mecanismo de autenticação;
b) programa de transferência de arquivos seguro;
c) mecanismo que verifica e bloqueia spam de correio eletrônico;
d) antivírus, que pesquisa os arquivos em busca de programas malignos;
e) filtro, que restringe o tráfego de mensagens com sites e outros recursos.

18 - É correto afirmar que ransonware:
a) é uma técnica maliciosa que consiste em uma varredura dos computadores de uma rede com o objetivo de coletar informações sobre os usuários.
b) tem como exemplo os e-mails enviados com campos falsificados.
c) é um programa que se propaga no computador de forma a incluir cópias de si mesmo em softwares e arquivos.
d) monitora as atividades de um sistema e envia as informações para terceiros.
e) é um tipo de código malicioso que torna inacessíveis os dados de um computador.

19 - Assinale a alternativa que corresponde à definição do princípio da Autenticidade, relacionado à segurança da informação:

a) Princípio que garante que a informação seja aberta apenas por pessoas autorizadas.
b) Princípio que assegura a precisão e a integridade da informação.
c) Princípio que garante que a informação ou o usuário é autêntico.
d) Princípio que assegura que a informação e os sistemas de informação estão acessíveis e podem ser acessados a qualquer tempo.

20 - Sobre Firewall, analise os itens a seguir:

É uma barreira de proteção que ajuda a bloquear o acesso de conteúdo malicioso, mas sem impedir que os dados que precisam transitar continuem fluindo;
É o conjunto de componentes lógicos de um computador ou sistema de processamento de dados; programa, rotina ou conjunto de instruções que controlam o funcionamento de um computador; suporte lógico;
Trabalham usando regras de segurança, fazendo com que pacotes de dados que estejam dentro das regras sejam aprovados, enquanto todos os outros nunca chegam ao destino final;
Em um computador, os firewalls possuem como função fornecer instruções para o hardware.
A partir da leitura dos itens, podemos afirmar que:

a) Apenas os itens I e II estão corretos.
b) Apenas os itens I e III estão corretos.
c) Apenas os itens II e IV estão corretos.
d) Apenas os itens II, III e IV estão corretos.
e) Todos os itens estão corretos.

21 - O trecho apresentado refere-se a um(a):

> Em essência, usa criptografia e autenticação em protocolos de camadas baixas para fornecer uma conexão segura por meio de uma rede insegura, tipicamente a internet.
>
> STALLINGS, W. *Cryptography and network security*: principles and practice. Londres: Pearson, 2017. Tradução livre, com adaptações.

a) proxy.
b) VPN (do inglês, Virtual Private Network).
c) IP (do inglês, Internet Protocol).
d) LAN (do inglês, Local Area Network).
e) firewall.

22 - Qual é o intervalo válido de hosts a que o IP 172.16.10.22/28 pertence?

a) 172.16.10.20 a 172.16.10.22
b) 172.16.10.20 a 172.16.10.255
c) 172.16.10.17 a 172.16.10.30
d) 172.16.10. 16 a 172.16.10.23
e) 172.16.10.17 a 172.16.10.31

23 – Analise as afirmativas abaixo com relação a endereçamento IP (Internet Protocol):

I – Todos os endereços Ipv4 possuem 64 bits.
II – Os endereços da classse B vão de 128 a 193.
III – Se um host estiver em duas redes, precisará de dois endereços IP.
IV – Os endereços da rede 127.0.0.0 são reservados para teste de loopback.
V – O endereço IP 0.0.0.0 é usado pelos hosts quando estão sendo inicializados.

Assinale a opção correta.

a) Apenas as afirmativa III e V são verdadeiras.
b) Apenas as afirmativas II, IV e V são verdadeiras.
c) Apenas as afirmativas III, IV, V são verdadeiras.
d) Apenas as afirmativas II, IV são verdadeiras.
e) Apenas as afirmativas II, III, IV são verdadeiras.

24 – Que máscara de sub-rede deve ser utilizada para dividir um endereço classe B em exatamente 512 sub-redes?

a) 255.255.0.0
b) 255.255.255.192
c) 255.255.255.252
d) 255.255.255.255
e) 255.255.255.128

25 – Se atribuirmos o prefixo CIDR 128.211.0.16/28, qual o menor endereço de host que poderá ser utilizado?

a) 128.211.0.16
b) 128.211.0.15
c) 128.211.0.20
d) 128.211.0.17
e) 128.211.0.30

26 - Com relação às redes de computadores IP na versão 4, assinale a opção correta.

a) O endereçamento IP 10.20.10.0/24 permite o endereçamento de 256 redes e 1024 hosts.
b) O endereçamento IP 194.24.0.0/21 é equivalente ao endereçamento IP 194.24.0.0, com máscara 255.255.248.0, e permite endereçar 2048 hosts.
c) O endereçamento IP 194.24.8.0/22 é equivalente ao endereçamento IP 194.24.8.0, com máscara 255.255.248.0, e permite endereçar 1022 hosts.
d) O endereçamento IP 194.24.18.0, com máscara 255.255.240.0, e permite endereçar 4092 hosts.
e) O endereçamento IP 194.24.12.0/22 é equivalente ao endereçamento IP 194.24.12.0/20, com máscara 255.255.252.0, e permite endereçar 1022 hosts.

27 - A função de comutação em uma rede de comunicação refere-se à alocação dos recursos da rede para a transmissão pelos diversos dispositivos conectados. Sobre comutação, classifique cada uma das afirmações abaixo como verdadeira (V) ou falsa (F).

( ) A comunicação via comutação por circuitos pressupõe a existência de um caminho dedicado de comunicação entre duas estações.
( ) A comunicação via comutação por pacotes envolve três fases: estabelecimento da conexão, transferência da informação e encerramento da conexão.
( ) Na comutação por circuitos, o caminho alocado durante a fase de estabelecimento da conexão permanece dedicado àquelas estações até que uma delas (ou ambas) decida desfazer o circuito. Isso significa que, caso o trafego entre as estações não seja constante e contínuo, a capacidade do meio físico será desperdiçada.
( ) Na comutação de pacotes não é necessário o estabelecimento de um caminho dedicado entre as estações. Ao invés disso, se uma estação deseja transmitir um pacote, ela adiciona o endereço de destino ao mesmo, que será então transmitido pela rede de nó em nó.
( ) Na comutação de pacotes, o aproveitamento das linhas de comunicação é maior, já que os canais podem ser compartilhados por vários pacotes ao longo do tempo.

A sequência correta é:

a) V – F – V – V – V
b) V – V – V – V – V
c) F – V – F – V – V
d) V – V – V – F – V
e) V – V – V – V –F

28 - No referente a conceitos de comutação de circuitos, mensagens e pacotes, assinale a opção correta.

a) Para se enviar um pacote em uma rede de circuitos, é necessário que o pacote esteja marcado corretamente como prioritário para envio.
b) Em comutação de circuitos, é necessário que ambas as entidades tenham reserva de recursos para que a mesma seja estabelecida.
c) Na comutação de mensagens, é necessário o estabelecimento de um caminho para o envio do dado.
d) Na comutação de circuito, existem somente duas fases bem definidas: o estabelecimento e a transmissão.

29 - Em relação às redes de comutação de circuitos e de comutação de pacotes, qual das afirmativas abaixo está ERRADA?

a) Na rede de comutação de pacotes uma comunicação entre dois pontos podem ocorrer atrasos na transmissão, mas suas taxas são constantes.
b) Em uma rede de comutação de circuito, os recursos necessários à comunicação ao longo do caminho são reservados. Em uma rede de comutação de pacotes os recursos para comunicação não são reservados e sim, são sob demanda.
c) As redes de telefonia, na sua maioria, são redes baseadas em comutação de circuitos.
d) A Internet é baseada em uma rede de comutação de pacotes, faz-se o melhor esforço para entregar os dados, contudo, não existe garantia.
e) Uma comunicação entre dois pontos, usando rede de comutação de circuito, além de uma conexão contínua, também é reservada uma largura de banda constante entre os enlaces.

30 - Sobre roteadores são corretas as afirmações abaixo, exceto:
Não roteiam pacotes para o próprio endereço de origem.

a) Não propagam colisões.
b) A cada uma de suas portas está conectada uma rede diferente.
c) Propagam Broadcasts.
d) Não filtram a camada de aplicação.

31 - Uma das características do Quality of Service (QoS) em redes de computadores é que:

a) em caso de queda de desempenho da rede abaixo de um certo limiar, um alarme é acionado para que outros servidores de rede possam ajudar no roteamento dos pacotes.
b) servidores de rede garantem atender toda a demanda de comunicação sem perda de pacotes nem atrasos.
c) aplicações que necessitam de maior confiabilidade na transmissão usam um canal reservado nos servidores que tem QoS.
d) conexões de rede têm banda suficiente para atender a demanda de comunicação, evitando que os servidores de rede fiquem sobrecarregados.
e) aplicações que necessitam de maior confiabilidade na transmissão marcam seus pacotes para que os servidores de rede possam dar tratamento diferenciado.

32 - Sobre redes de computadores, assinale a alternativa CORRETA.

a) O protocolo IPv4 trabalha com o tamanho de endereços de 32 bits e o IPv6 trabalha com endereços de 128 bits.
b) O protocolo UDPé um protocolo orientado à conexão, garantindo, portanto, a entrega de dados sem erro.
c) O padrão de endereçamento IPv6 utiliza 4 conjuntos de 8 bits (4 octetos) para expressar cada endereço IP
d) O protocolo TCPé um protocolo não orientado à conexão, não garantindo, portanto, a entrega de dados sem erro.
e) O protocolo HTTP é responsável pela comunicação junto ao servidor de e-mails, para entrega destes, ao programa cliente que recebe as mensagens.

33 - Julgue os itens em verdadeiro (V) ou falso (F) e em seguida assinale a alternativa que apresenta a sequência, de cima para baixo, correta:

( ) Tudo que é disponível na web tem seu próprio endereço, chamado URL, é o endereço de algo que você procura na internet, é formada por um protocolo de administração.
( ) HTTP é um protocolo ou língua específica da internet, responsável pela comunicação entre computadores. A sigla HTTP é encontrada nos endereços de páginas web seguida de ://. Ela informa ao servidor de que forma deve ser atendido o pedido do cliente.
( ) Os endereços que começam com www são servidores de Web e contém principalmente páginas de hipertexto. Já os que começam com ftp, referem-se a lugares onde pode-se copiar arquivos.
( ) Link é uma ligação que é feita apenas em palavras indicando um caminho para você acessar outro endereço com a informação que esta procurando.

a) F - V - V - F
b) V - F - F - V
c) V - V - V - F
d) F - V - F - V

34 - Sobre as noções básicas de conhecimento de internet, analise as seguintes afirmativas.

I - A URL é um endereço virtual que indica onde está o que o usuário procura.
II - HTTP é um protocolo de comunicação que permite a transferência de informação entre redes.
III - WWW é a sigla para World Wide Web, que significa rede de alcance local.
Estão corretas as afirmativas

a) I e II, apenas.
b) I e III, apenas.
c) II e III, apenas.
d) I, II e III.

35 - Analise as seguintes afirmativas sobre as redes de computadores.

I - A topologia física de uma rede de computadores representa o layout físico e o meio de conexão dos dispositivos de redes.
II - A topologia estrela utiliza um concentrador como ponto central da rede e seu gerenciamento é centralizado.
III - Na topologia estrela, a falha em um dos cabos não implica na paralização da rede como um todo.

Estão corretas as afirmativas

a) I e II, apenas.
b) I e III, apenas.
c) II e III, apenas.
d) I, II e III.

36 - Com relação aos computadores de mesa (desktops), assinale a alternativa correta.

a) Uma desvantagem do desktop é que não é possível se conectar a uma rede sem-fio (wireless).
b) Em uma falta de energia, o desktop sempre salva os dados antes de ser desligado.
c) É possível instalar mais do que um sistema operacional em um computador, por exemplo, Windows e Linux.
d) Ao colocar dois monitores em um computador, devem-se instalar dois gabinetes e dois mouses, um para cada monitor.
e) Não é possível conectar dois monitores que tenham conexões diferentes, por exemplo, um HDMI e outro VGA, em um mesmo computador.

37 - Além da integração das informações propriamente ditas, por meio do funcionamento harmônico das funções empresariais, é preciso estabelecer a integração dos recursos computacionais disponíveis na organização. Como resposta a essa necessidade, surgiram várias opções de comunicação e compartilhamento de dados. Um grupo de computadores interligados por meio de cabos, localizados em determinada área geográfica, permitindo que um computador use recursos de todos os outros, na presença de um software gerenciador, está associado com maior intensidade à ideia de:

a) rede local de microcomputadores.
b) internet e intranet.
c) rede cliente/servidor.
d) rede local não hierárquica.
e) multimídia.

38 - Com relação ao modelo de referência TCP/IP, marque a alternativa ERRADA:

a) a camada de inter-rede é responsável pelo envio dos datagramas de um computador qualquer para outro computador.
b) a camada de transporte é responsável por prover suporte à camada de aplicação de maneira confiável ou não.
c) a camada de apresentação é responsável pela definição elétrica e mecânica da interface.
d) a camada de aplicação possui os protocolos que dão suporte às aplicações dos usuários.
e) a camada de interface de rede é responsável por funções de acesso físico e lógico ao meio físico.

39 - As redes IP utilizam o protocolo de roteamento OSPF − Open Shortest Path First, que

a) distribui informações de roteamento somente entre roteadores pertencentes a sistemas autônomos diferentes.
b) usa um algoritmo de menor distância e é considerado um protocolo de estado de enlace.
c) envia todos os pacotes pela menor rota, não suportando balanceamento de carga.
d) implementa mecanismos para que os roteadores sejam obrigados a conhecer toda a topologia da rede.
e) possui compatibilidade somente com conexões de redes de multiacesso com ou sem difusão.

40 - Com relação aos mecanismos de comunicação utilizados nas redes de computadores, considere as siglas de protocolos a seguir.

I - SMTP
II - POP3
III - IMAP
IV - FTP
Os protocolos diretamente associados às configurações de e-mails são somente:

a) I e II;
b) II e III;
c) III e IV;
d) I, II e III;
e) II, III e IV.