Segurança da Informação

01 Confidencialidade, disponibilidade e integridade da informação são princípios básicos que orientam a definição de políticas de uso dos ambientes computacionais. Esses princípios são aplicados exclusivamente às tecnologias de informação, pois não podem ser seguidos por seres humanos.
02 A confidencialidade tem o objetivo de garantir que apenas pessoas autorizadas tenham acesso à informação.
03 Confidencialidade é a propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas pelo proprietário da informação.
04 Integridade é a propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação.
05 Cópias de segurança devem ser testadas periodicamente para verificar o estado do seu meio de suporte e devem ser guardadas em local distinto das instalações onde se encontram os dados nelas gravados
06 A criação de cópias de segurança é um procedimento básico para a continuidade do negócio e recuperação de desastres.
07 A grande novidade do Windows 7, última versão do sistema operacional da Microsoft, é a existência de antivírus capaz de excluir todo tipo de vírus automaticamente.
08 O Windows XP possui um sistema antivírus eficiente, o que garante total segurança aos sistemas computacionais.
09 Instalar e utilizar antivírus em um computador é uma ação preventiva que elimina completamente a possibilidade de ataques a arquivos e pastas.
10 Ao se utilizar firewall é garantido o bloqueio de vírus e worms, pois a sua principal função é identificar e eliminar arquivos corrompidos.
11 Uma das formas de se evitar a infecção por vírus de computador pela Internet é sempre renovar a senha de acesso à caixa postal de e-mail do usuário, já que a senha deve ser secreta, pessoal e intransferível.
12 Firewall é um recurso utilizado para a segurança tanto de estações de trabalho como de servidores ou de toda uma rede de comunicação de dados. Esse recurso possibilita o bloqueio de acessos indevidos a partir de regras preestabelecidas.
13 Antivírus é um software especificamente desenvolvido para detectar, anular e eliminar de um computador vírus e outros tipos de código malicioso.
14 O phishing começa com um email recebido aparentemente de uma fonte confiável, mas que na verdade direciona os destinatários para que forneçam informações a um site fraudulento.
15 Pharming é o termo atribuído ao ataque baseado na técnica DNS cache poisoning (envenenamento de cache DNS) que, consiste em corromper o DNS (Sistema de Nomes de Domínio ou Domain Name System) em uma rede de computadores, fazendo com que a URL (Uniform Resource Locator ou Localizador Uniforme de Recursos) de um site passe a apontar para um servidor diferente do original.
16 O Windows Defender foi projetado para que o usuário remova um spyware ou um software potencialmente indesejado de forma prática.
17 Criptografia é o processo de converter dados em um formato que não é entendido por pessoas não autorizadas.
18Os dados já descriptografados são denominados texto cifrado.
19 Na criptografia, os algoritmos de cifragem e decifragem são públicos, enquanto as chaves são secretas.
20 Em um código de chave pública, cada usuário divulga um conjunto de números que será utilizado para um remetente enviar-lhe uma mensagem criptografada. Esse conjunto é denominado chave de decodificação e é indispensável para a decodificação da mensagem.
21 Um algoritmo de criptografia simétrica requer que uma chave secreta seja usada na criptografia e uma chave pública diferente e complementar da secreta, utilizada no processo anterior, seja utilizada na decriptografia. Devido à sua baixa velocidade, a criptografia simétrica é usada quando o emissor de uma mensagem precisa criptografar pequenas quantidades de dados. A criptografia simétrica também é chamada criptografia de chave pública.
22 A criptografia de chave pública ou criptografia assimétrica é um método de criptografia que utiliza um par de chaves: uma chave pública e uma chave privada. A chave pública é distribuída livremente para todos os correspondentes via e-mail ou outras formas, enquanto a chave privada deve ser conhecida apenas pelo seu dono.
23 Num algoritmo de criptografia assimétrica, uma mensagem cifrada com a chave pública pode somente ser decifrada pela sua chave privada correspondente.
24 Para confidencialidade, a chave pública é usada para cifrar mensagens, com isso apenas o dono da chave privada pode decifrá-la.
25 A infraestrutura de TI, por ser uma tecnologia de alto custo, embora seja importante para uma empresa, deve ser adquirida apenas quando se esgotarem outras formas de armazenamento de informações com mais baixo custo.
26 Para que uma empresa tenha infraestrutura de tecnologia da informação (TI), é necessário que ela esteja cadastrada no Ministério das Comunicações para poder adquirir e oferecer acesso à Internet, e obter um conjunto de software livres.
27 Um IDS refere-se a meios técnicos de descobrir em uma rede quando esta está tendo acessos não autorizados que podem indicar a ação de um hacker ou até mesmo funcionários mal intencionados.
28 No host-based o IDS é instalado em um servidor para alertar e identificar ataques e tentativas de acessos indevidos à própria máquina.
29 Network Based são implementações de um IDS que são instalados em máquinas que serão responsáveis por identificar ataques direcionados a toda a rede, por meio da monitoração do tráfego.

30 Um certificado digital é um arquivo de computador que contém um conjunto de informações referentes a entidade para o qual o certificado foi emitido (seja uma empresa, pessoa física ou computador) mais a chave pública referente a chave privada que acredita-se ser de posse unicamente da entidade especificada no certificado
31Cavalo de troia é um programa executável que objetiva realizar a função maliciosa de se autorreplicar, ou seja, criar cópias de si mesmo, de um computador para outro, podendo ocupar totalmente a memória de um computador.
32 A identificação e a eliminação de atividades suspeitas ou indesejadas, tanto no computador pessoal como na rede, pode ser realizada por meio de sistemas de controle de vírus, como malware, spyware e cavalo de troia.
33 Vírus, spywares, worms e trojans são conhecidas ameaças aos ambientes eletrônicos que devem ser monitoradas por meio de software de segurança específicos para cada tipo de ameaça.
34 O worm é um tipo de vírus de computador que utiliza mensagens de e-mail para disseminar pela Internet arquivos infectados.
35 O termo worm é usado na informática para designar programas que combatem tipos específicos de vírus de computador que costumam se disseminar criando cópias de si mesmos em outros sistemas e são transmitidos por conexão de rede ou por anexos de e-mail.
36 Cavalo de troia é um programa executável que objetiva realizar a função maliciosa de se autorreplicar, ou seja, criar cópias de si mesmo, de um computador para outro, podendo ocupar totalmente a memória de um computador.
37 Um programa nocivo que tem a capacidade de se replicar ou se auto-enviar é um exemplo de um hacker.
38 Um programa capaz de se auto-propagar automaticamente através de redes, enviado cópias de si mesmo, de computador para computador, denomina-se
a.trojan b.macros c.backup d.backdoor e.worm
39 Os cookies, também denominados cavalos de troia, são arquivos indesejáveis que se instalam no computador durante um acesso à Internet e coletam informações armazenadas na máquina para posterior envio a destinatário não autorizado.
40 Worm é um vírus que tem a capacidade de auto-replicação, espalhando-se rapidamente de uma rede para outra, mas somente causa danos se for ativado pelo usuário.
41 Os programas de antivírus são indicados para fazer controle e eliminação de pragas virtuais. São exemplos típicos de pragas virtuais: spyware, worm, firewall e boot.
42 Cookie é um vírus que capta as informações digitadas pelo usuário e as encaminha para um servidor.
43 Adware é qualquer programa que, depois de instalado, automaticamente executa, mostra ou baixa publicidade para o computador. Alguns desses programas têm instruções para captar informações pessoais e passá-la para terceiros, sem a autorização ou o conhecimento do usuário, o que caracteriza a prática conhecida como spyware.
44 Keylogger é um programa de computador do tipo spyware cuja finalidade é monitorar tudo o que for digitado, a fim de descobrir senhas de banco, números de cartão de crédito e afins. Alguns casos de phishing e determinados tipos de fraudes virtuais baseiam-se no uso de keylogger.
45 Programa que a partir da execução em determinado computador vítima passa a monitorar informações digitadas e visualizadas e, em seguida, envia e-mail para o seu criador encaminhando informações capturadas denomina-se trojan
46 Os spywares podem vir embutidos em software ou ser baixados quando o internauta visita determinados sítios.
47 Spam é o envio de correio eletrônico solicitado pelo destinatário; é utilizado para distribuir propaganda, notícias e convites.
48 Os keyloggers são aplicativos destinados a capturar o que é digitado no teclado.
49 Os worms podem se propagar rapidamente para outros computadores por meio da Internet e da intranet.
50 (CESPE-SEPLAGEDUC2009) Firewall e anti-spyware são nomes diferentes para software com os mesmos objetivos, ambos implementam o bloqueio a determinadas páginas web.
51 (CESPE-SEPLAGEDUC2009) Hacker é um programa inteligente de computador que, após detectar falhas em um ambiente computacional, causa danos irreparáveis e a proliferação de outros programas maliciosos.
52 (CESPE-SEPLAGEDUC2009) Os programas de antivírus são utilizados para detectar e eliminar vírus de computador que já tenham uma vacina equivalente, assim como manter em quarentena vírus que ainda não possuem vacina.
53 (CESPE-SEPLAGEDUC2009) O controle de acesso físico é uma das formas de se evitar que usuários tenham acesso aos discos, pastas e arquivos de uma máquina conectada em rede, por meio de acesso remoto não autorizado, realizado a partir de outra rede de computador.
54 (CESPE-SEPLAGEDUC2009) A criptografia é um processo de segurança de dados que faz com que eles fiquem inacessíveis, sendo possível acessar o conteúdo apenas a partir de uma chave de criptografia equivalente.
55 (CESPE-SEPLAGEDUC2009) Computadores que não estejam conectados à Internet, ou a qualquer outra rede de comunicação, estão livres do risco de contaminação por vírus.
56 (CESPE-SEPLAGEDUC2009) Apesar de firewalls serem ferramentas que podem ser utilizadas para a proteção de computadores contra ataques de hackers, eles não são suficientes para evitar a contaminação de computadores por vírus.

"O insucesso é apenas uma oportunidade para recomeçar de novo com mais inteligência."

Henry Ford