# ****INTEGRADO INFORMÁTICA****

**REDES DE COMUNICAÇÃO DE DADOS – 3º ANO**

# **-** INTRODUÇÃO

Sabemos que no mundo real não existem sistemas totalmente seguros e o mundo virtual segue o mesmo preceito. Por maior que seja a proteção adotada, estaremos sempre sujeitos as invasões, roubos e ataques. Então é importante que conheçamos o perigo e saibamos como nos proteger.

Atualmente já utilizamos a Internet para realizar diversos serviços corriqueiros, como compras, serviços bancários, investimentos, além de negócios ou troca de informações confidenciais via e-mail. Grandes partes dos problemas ocorrem por puro desconhecimento dos procedimentos básicos de segurança por parte dos usuários. Saber como agir em caso de problemas, também poderá ajudar, e muito, nas investigações policiais dos crimes virtuais.

# - PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

A segurança da informação busca reduzir os riscos de vazamentos, fraudes, erros, uso indevido, sabotagens, paralisações, roubo de informações ou qualquer outra ameaça que possa prejudicar os sistemas de informação ou equipamentos de um indivíduo ou organização. Uma solução de segurança adequada deve satisfazer os seguinte princípios:

- CONFIABILIDADE: significa proteger informações contra sua revelação para alguém não autorizado - interna ou externamente. Consiste em proteger a informação contra leitura e/ou cópia por alguém que não tenha sido explicitamente autorizado pelo proprietário daquela informação. A informação deve ser protegida qualquer que seja a mídia que a contenha, como por exemplo, mídia impressa ou mídia digital.

- INTEGRIDADE: consiste em proteger a informação contra modificação sem a permissão explícita do proprietário daquela informação. A modificação inclui ações como escrita, alteração de conteúdo, alteração de status, remoção e criação de informações.

- DISPONIBILIDADE: consiste na proteção dos serviços prestados pelo sistema de forma que eles não sejam degradados ou se tornem indisponíveis sem autorização, assegurando ao usuário o acesso aos dados sempre que deles precisar. Isto pode ser chamado também de continuidade dos serviços.

- AUTENTICIDADE: está associado com identificação correta de um usuário ou computador. O serviço de autenticação em um sistema deve assegurar ao receptor que a mensagem é realmente procedente da origem informada em seu conteúdo.

Também podemos contar um termo muito usado na área de segurança: o NÃO-REPÚDIO.

Não-Repúdio é a garantia de que um agente não consiga negar um ato ou documento de sua autoria. Essa garantia é condição necessária para a validade jurídica de documentos e transações digitais. Só se pode garantir o não-repúdio quando houver **AUTENTICIDADE e INTEGRIDADE**.

# AMEAÇAS

Para se garantir a proteção de uma rede ou sistema é importante conhecer as ameaças e técnicas de ataque utilizadas pelos invasores, para então aplicar as medidas e ferramentas necessárias para proteção desses recursos. Sem o conhecimento desses fatores, toda a aplicação de mecanismos de proteção pode ser anulada, pois se existir algum ponto vulnerável ou protegido de maneira incorreta, todo sistema estará comprometido. Dessa maneira, vamos identificar as principais ameaças e técnicas de ataque contra a segurança da informação.

1) VÍRUS: são programas maliciosos, criados para se replicar automaticamente e danificar o sistema. A principal característica de um vírus é sua capacidade de se copiar sozinho e de se anexar a arquivos. Podem ser:

VÍRUS DE BOOT: afetam o setor de boot e o sistema operacional. Normalmente se copiam para o MBR do HD, apagando o seu conteúdo ou permanecendo lá, para serem carregados sempre que o sistema operacional for executado;

VÍRUS DE MACRO: afetam programas da Microsoft. As instruções desses vírus são, na verdade, macros existentes em arquivos .doc ou .xls, que, quando executados, dão origem a várias operações inconvenientes no micro, podendo até apagar arquivos.

2) WORMS: programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador. Diferente do vírus, o worm não necessita ser explicitamente executado para se propagar. Sua propagação se dá através da exploração de vulnerabilidades existentes ou falhas na configuração de softwares instalados em computadores. Worms são notadamente responsáveis por consumir muitos recursos. Degradam sensivelmente o desempenho de redes e podem lotar o disco rígido de computadores, devido à grande quantidade de cópias de si mesmo que costumam propagar. Além disso, podem gerar grandes transtornos para aqueles que estão recebendo tais cópias.

3) CAVALO DE TRÓIA Também conhecidos como *Trojans*, são códigos maliciosos, geralmente camuflados como programas inofensivos que, uma vez instalados no computador da vítima, podem permitir que o criador da praga obtenha o controle completo sobre a máquina infectada, que passa a ser chamada de "zumbi". Alguns tipos de *Trojans* conhecidos, como o BO e o Netbus, permitem acesso ao computador, deixando vulneráveis arquivos do sistema e senhas gravadas no disco e na memória.

4) EXPLOIT: programa de computador, uma porção de dados ou uma sequência de comandos que se aproveita das vulnerabilidades de um sistema computacional. São geralmente elaborados por hackers como programas de demonstração das vulnerabilidades, a fim de que as falhas sejam corrigidas, ou por crackers a fim de ganhar acesso não autorizado a sistemas.

5) SNIFFERS: Os “farejadores” são programas que espionam a comunicação em uma rede. Eles exploram o fato do tráfego dos pacotes das aplicações TCP/IP não utilizar nenhum tipo de cifragem nos dados. Dessa maneira um sniffer pode obter nomes de usuários, senhas ou qualquer outra informação transmitida que não esteja criptografada. A dificuldade no uso de um sniffer é que o atacante precisa instalar o programa em algum ponto estratégico da rede, como entre duas máquinas.

6) PORT SCANNERS: são programas que vasculham um computador a procura de portas de comunicação abertas. Esses programas ficam enviando vários pacotes seguidos para esse computador, em diferentes portas, apenas para receber a resposta de uma delas e, com isso, constatar a presença de portas abertas.

7) BACKDOOR: ou “porta dos fundos”, é uma brecha, normalmente colocada de forma intencional pelo programador, que permite a invasão do sistema por quem conhece a falha. Versões antigas do ICQ possuem defeito que abre um Backdoor que permite ao hacker derrubar a conexão do programa com o servidor, fazendo que ele pare de funcionar.

8) SPYWARE E ADWARE: O Spyware é basicamente programa, cuja função é a de coletar suas informações pessoais sem que você saiba o que está havendo. Você pode ser o alvo de um spyware se você faz download de músicas de programas de compartilhamento de arquivos, jogos gratuitos de sites, ou outros softwares de origem desconhecida. O Spyware é freqüentemente associado com softwares que exibem propagandas, chamados Adware. O Adware são programas instalados no computador do usuário que realizam constantemente a abertura de janelas de anúncios de propagandas. propagandas. Alguns anunciantes podem instalar software adware em seu sistema e gerar uma série de anúncios não solicitados que podem encher o seu desktop e afetar sua produtividade.

9) DOS: Denial of Service, ou Negação de Serviço, é um ataque onde o acesso a um sistema/aplicação é interrompido ou impedido, deixando de estar disponível; ou uma aplicação, cujo tempo de execução é crítico, é atrasada ou abortada. Esse tipo de ataque é um dos mais fáceis de implementar e mais difíceis de se evitar. O objetivo é incapacitar um servidor, uma estação ou algum sistema de fornecer os seus serviços para os usuários legítimos. Normalmente o ataque DoS não permite o acesso ou modificação de dados. Usualmente o atacante somente quer inabilitar o uso de um serviço, não corrompê-lo.

10) KEYLOGGER: Programa capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado de um computador. Normalmente, a ativação do keylogger é condicionada a uma ação prévia do usuário, como por exemplo, após o acesso a um site de comércio eletrônico ou Internet Banking, para a captura de senhas bancárias ou números de cartões de crédito.

# MECANISMOS DE SEGURANÇA

Uma vez conhecidos as principais ameaças e técnicas utilizadas contra a segurança da Informação, pode-se descrever as principais medidas e ferramentas necessárias para eliminar essas ameaças e garantir a proteção de um ambiente computacional.

1) ANTI-VÍRUS: Os antivírus são programas que detectam, anulam e eliminam os vírus de computador. Atualmente, os programas antivírus foram ganhando novas funcionalidades e conseguem eliminar Cavalos de Tróia, barram programas hostis e verificam e-mails. Alguns antivírus ainda verificam o funcionamento dos programas de seu computador, avisando ao usuário, caso algum programa comece a apresentar algum comportamento suspeito. Algumas versões de antivírus são gratuitas para uso pessoal e podem ser baixadas pela Internet.

2) FIREWALL: Os firewalls são sistemas ou programas que barram conexões indesejadas na Internet. Assim, se algum hacker ou programa suspeito tenta fazer uma conexão ao seu computador o firewall irá bloquear. Com um firewall instalado em seu computador, grande parte dos Cavalos de Tróia serão barrados mesmo se já estiverem instalados em seu computador. Alguns programas de Firewall chegam ao requinte de analisar continuamente o conteúdo das conexões, filtrando os Cavalos de Tróia e os Vírus de e-mail antes mesmo que os antivírus entrem em ação. Existem, ainda, pacotes de Firewall que funcionam em conjunto com os antivírus possibilitando ainda um nível maior de segurança nos computadores que são utilizados em conexões com a Internet. Assim como certos antivírus, alguns fabricantes de Firewalls oferecem versões gratuitas de seus produtos para uso pessoal.

3) IDS: Intrusion Detection Systems, ou Sistemas de Detecção de Intrusão, são, basicamente, como uma ferramenta inteligente capaz de detectar tentativas de invasão e tempo real. Esses sistemas podem atuar de forma a somente alertar as tentativas de invasão, como também em forma reativa, aplicando ações necessárias contra o ataque.

4) CRIPTOGRAFIA: Criptografia é arte ou ciência de escrever em cifra ou em códigos. É então um conjunto de técnicas que tornam uma mensagem incompreensível permitindo apenas que o destinatário que conheça a chave de encriptação possa decriptar e ler a mensagem com clareza. Sobre criptografia, precisamos falar um pouco mais...

5) BACKUP: O backup é uma ferramenta que permite a cópia de mais de um diretório ou todo o conteúdo do computador para unidades externas de armazenamento. Como um disco rígido possui maior capacidade de armazenamento do que um disquete, a ferramenta Backup permite a divisão das informações em mais disquetes, em ordem seqüencial que a mesma ferramenta backup é capaz de copiar de volta para o disco rígido....

### 5.1 - TIPOS DE BACKUP

- COMPLETO OU NORMAL - Para entendermos os tipos de backup, vamos, antes, esclarecer um ponto. Quando nos referimos a um backup completo, estamos nos referindo a um intervalo limitado de dados completo. Por exemplo, podemos fazer um backup completo de nossas fotos digitais, um backup completo de nossas planilhas eletrônicas etc. Fazemos backup de arquivos de dados e não de programas ou arquivos do sistema. Quando fazemos um backup completo, o sistema operacional sinaliza os arquivos que foram copiados. No Windows, os arquivos possuem um atributo chamado Arquivo morto que indica que o arquivo está pronto para ser copiado para backup. É importante notar que, no Windows, se um arquivo possui o atributo Arquivar (ou Arquivo morto em versões mais antigas) marcado, ele ainda não foi copiado para um backup. Verifique isso clicando em um arquivo com o botão direito do mouse e selecionando Propriedades.

– INCREMENTAL **-** Backup incremental é aquele que copia os arquivos que foram criados ou alterados desde o último backup normal ou completo. No exemplo das fotos digitais, um backup incremental copiaria as fotos que foram alteradas desde o último backup, além das novas fotos que porventura houvesse.

Em outras palavras, o backup incremental copia os arquivos que não possuem marca de backup. Depois de copiá-los, marca-os para que não sejam copiados novamente.

5.1.3 – DIFERENCIAL **-** O backup diferencial é similar ao incremental no que se refere ao que ele vai copiar, ou seja, copia todos os arquivos que não estejam marcados. Todavia, o backup diferencial, ao contrário do incremental, não marca os arquivos que copia. Assim, os arquivos copiados pelo backup diferencial continuarão sem marca de que passaram por backup. Parece estranho, mas, mais à frente, vamos poder entender qual a utilidade disso.

5.1.4 - DE CÓPIA **-** O backup de cópia é utilizado quando se quer fazer cópias de arquivos emergencialmente, mas não se quer alterar os atributos dos arquivos. Ele copia todos os arquivos selecionados, mas não altera nenhuma marca. Assim, a situação das marcas dos arquivos permanece inalterada.

5.1.5 – DIÁRIO **-** Um backup diário copia os arquivos que foram criados ou alterados em uma determinada data. Não altera as marcas dos arquivos. Esse é o principal backup em empresas com grande volume de dados que são alterados com freqüência e cujo histórico seja importante, como arquivos de instituições financeiras, por exemplo.

Normalmente nessas empresas a solicitação de restauração de um arquivo é relativa a uma data específica. Se, por exemplo, há uma planilha que foi sofrendo alterações durante todos os dias de uma semana e, na segunda-feira seguinte descobriu-se que os dados da planilha de quarta-feira estavam inconsistentes, pode-se solicitar a restauração do arquivo de terça-feira.

#### 5.1.6 - COMBINAÇÃO DE BACKUPS

Há uma diferença importante entre a realização de uma política de backup que combine um backup normal seguido de backups incrementais para uma que combine um backup normal seguido de backups diferenciais. Para entender isso, vamos supor um backup que é feito semanalmente, no decorrer de um mês. Vamos utilizar o exemplo das fotos digitais.

#### 5.1.6.1 - NORMAL + INCREMENTAL:

* Primeira semana: backup normal copia todas as fotos e as marca.
* Segunda semana: surgiram mais 50 fotos; backup incremental copia essas 50 fotos e as marca, indicando que foram copiadas.
* Terceira semana: surgiram mais 100 fotos; backup incremental copia somente as 100 fotos novas e as marca, indicando que foram copiadas.
* Quarta semana: foram alteradas 10 fotos; backup incremental copia as 10 fotos alteradas e as marca, indicando que foram copiadas.

Há um detalhe importante aqui. Normalmente os backups são feitos em fitas magnéticas devido à boa relação de custo e benefícios desses dispositivos de memória. Entretanto, como sabemos, fitas são dispositivos de acesso seqüencial. Isso quer dizer que toda vez que forem utilizadas para backup, o conteúdo anterior será perdido.

Assim, na combinação de backup normal com backups incrementais sucessivos, se forem utilizadas fitas magnéticas, teremos que ter fitas diferentes para cada backup diferencial realizado. Isso acontece porque cada backup diferencial só copia os arquivos não marcados.

Vamos pegar o nosso exemplo para entender isso melhor. Na segunda semana 50 fotos foram copiadas em uma fita. Na terceira semana temos 100 novas fotos para armazenar. Se utilizarmos a mesma fita, as 50 fotos da segunda semana serão perdidas. Por isso, temos que guardar cada backup incremental em um volume diferente.

#### 5.1.6.2 - NORMAL + DIFERENCIAL

* Primeira semana: backup normal copia todas as fotos e as marca.
* Segunda semana: surgiram mais 50 fotos; backup diferencial copia todas as fotos não marcadas, ou seja, copia essas 50 novas fotos e não as marca.
* Terceira semana: surgiram mais 100 fotos; backup diferencial copia todas as fotos não marcadas, ou seja, as 100 fotos da terceira semana mais as 50 fotos da segunda semana. Ao final da operação, não as marca.
* Quarta semana: foram alteradas 10 fotos; backup diferencial copia todas as fotos não marcadas, ou seja, as 100 fotos da terceira semana, mais as 50 fotos da segunda semana, mais as 10 fotos da terceira semana. Serão copiadas 160 fotos. Ao final da operação, não as marca.

Aqui devemos notar que o backup feito na terceira semana contém os arquivos criados ou alterados na segunda e na terceira semanas. Da mesma forma, o backup feito na quarta semana contém os arquivos criados ou alterados na segunda, terceira e quarta semanas.

Acho que vocês já imaginam a conseqüência disso: podemos fazer os backups diferenciais em uma única fita magnética sem o risco de perdermos as fotos das semanas anteriores.

# CRIPTOGRAFIA

Como já comentamos, a criptografia é um conjunto de técnicas, um processo matemático usado para embaralhar os dados de uma mensagem que deve ser secreta.

A principal finalidade é reescrever uma mensagem original de uma forma que seja incompreensível, para que ela não seja lida por pessoas não autorizadas. A idéia só funciona se a pessoa (autorizada, lógico!) que receber a mensagem, conseguir transformar a mensagem embaralhada em legível.

Para isso, precisamos primeiro conhecer alguns conceitos:

- ALGORITMOS CRIPTOGRÁFICOS: São funções matemáticas usadas para codificar os dados, garantindo segredo e autenticação. Os algoritmos devem ser conhecidos e testados, a segurança deve basear-se totalmente na chave secreta, sendo que essa chave deve ter um tamanho suficiente para evitar sua descoberta por força-bruta.

- CHAVE CRIPTOGRÁFICA: é o número que será usado, em conjunto com o algoritmo, que alterará a mensagem original.

# - TIPOS DE CRIPTOGRAFIA

## 1) CRIPTOGRAFIA SIMÉTRICA

Também denominado algoritmo simétrico, criptografia de chave simétrica ou criptografia convencional, é um sistema que utiliza apenas uma chave para encriptar e decriptar a informação.

|  |  |
| --- | --- |
|  |  |
| Para encriptar | Para decriptar |

Uma informação é encriptada através de um polinômio utilizando-se de uma chave (Chave A) que também serve para decriptar novamente a informação. As principais vantagens dos algoritmos simétricos são:

* Rapidez: Um polinômio simétrico encripta um texto longo em milésimos de segundos.
* Chaves pequenas: uma chave de criptografia de 128 bits torna um algoritmo simétrico praticamente impossível de ser quebrado.

A maior desvantagem da criptografia simétrica é que a chave utilizada para encriptar é igual à chave que decripta. Quando um grande número de pessoas tem conhecimento da chave, a informação deixa de ser um segredo.

## 2) CRIPTOGRAFIA ASSIMÉTRICA

Também conhecido como algoritmo assimétrico, ou criptografia de chave-pública, é um sistema que utiliza duas chaves diferentes, uma chave denominada secreta e outra denominada pública. O par de chaves pertence a uma entidade ou pessoa e é calculado a partir de um número aleatório.

|  |  |
| --- | --- |
|  |  |
| Para encriptar | Para decriptar |

Podemos considerar algumas desvantagens no uso de algoritmos assimétricos:

* São lentos: Um polinômio assimétrico leva mais tempo para encriptar uma informação do que um simétrico.
* Utilizam chaves grandes: uma chave de criptografia de 3078 bits torna um polinômio assimétrico equivalente a um polinômio simétrico com chave de 128 bits.

A grande vantagem do uso de criptografia assimétrica é que a chave que encripta é diferente da que decripta, garantindo uma segurança muito maior no processo.

## 

## 3) COMPARATIVO

|  |  |
| --- | --- |
| **Criptografia Simétrica** | **Criptografia Assimétrica** |
| Uma única chave para cifrar e decifrar | Usa chaves diferentes para cifrar e decifrar |
| A chave tem que ser compartilhada entre os usuários | A chave para criptografar é compartilhada (pública), mas a chave de decriptografar é mantida em segredo (privada). |
| Processos simples de criptografia e decriptografia (exigem pouco processamento), ideal para grandes quantidades de dados. | Os processos são mais lentos,viável apenas em pequenas quantidades de dados. |
| É mais suscetível a quebras de chave | É praticamente impossível quebrar as chaves. |
| **Principais Algoritmos**:   * DES * 3DES * AES | **Principal algoritmo:**   * RSA |

# - ASSINATURA DIGITAL

A assinatura digital busca resolver dois problemas não garantidos apenas com uso da criptografia para codificar as informações: a Autenticidade e a Integridade.

Autenticidade porque, com a assinatura digital, garante que quem enviou a mensagem é quem diz ser. E Integridade, porque também garante que quem enviou mandou exatamente aquela mensagem.

A assinatura digital se baseia em criptografia assimétrica. A diferença entre a assinatura digital e a criptografia assimétrica. é a forma como as chaves são usadas. Na assinatura digital, o remetente usará a chave privada para encriptar a mensagem. Por outro lado, o destinatário usará a chave pública do remetente para confirmar que ela foi enviada por aquela pessoa. Garantiremos, assim, que o remetente não vá dizer: “Ei, não fui eu que mandei essa mensagem!”.

Mas, e se ele disser: “Fui eu, mas não era isso que estava escrito!”.

Aí, entra um recurso incluso na assinatura digital: o Hash. HASH é um método matemático que garante a integridade dos dados durante uma transferência qualquer. Quando o e-mail é enviado, é calculado o hash (através de um programa) e enviado junto com a mensagem. Quando a mensagem chega ao destinatário, ele calcula o hash e compara com o hash enviado pelo remetente. Se os resultados forem iguais, garante-se a integridade dos dados enviados.

# - CERTIFICAÇÃO DIGITAL

A Certificação Digital, também conhecida como Certificado de Identidade Digital, associa a identidade de um titular a um par de chaves eletrônicas (uma pública e outra privada) que, usadas em conjunto, fornecem a comprovação da identidade. É uma versão eletrônica (digital) de algo parecido a uma Cédula de Identidade - serve como prova de identidade, reconhecida diante de qualquer situação onde seja necessária a comprovação de identidade.

Dessa forma, um cliente que compre em um shopping virtual, utilizando um Servidor Seguro, solicitará o Certificado de Identidade Digital deste Servidor para verificar: a identidade do vendedor e o conteúdo do Certificado por ele apresentado. Da mesma forma, o servidor poderá solicitar ao comprador seu Certificado de Identidade Digital, para identificá-lo com segurança e precisão.

Caso qualquer um dos dois apresente um Certificado de Identidade Digital adulterado, ele será avisado do fato, e a comunicação com segurança não será estabelecida.

O Certificado de Identidade Digital é emitido e assinado por uma Autoridade Certificadora Digital (Certificate Authority).

# EXERCÍCIOS PROPOSTOS

1. O backup que copia somente os arquivos criados ou alterados desde o último backup normal ou incremental e os marca como arquivos que passaram por backup, desmarcando o atributo de arquivo, é o backup:

(A) normal.

(B) diferencial.

(C) incremental.

(D) estratégico.

(E) full.

2. NÃO é considerado um programa malicioso:

(A) KeyLogger

(B) Worm

(C) Firewall

(D) Trojan

(E) Spyware

3. Observe as seguintes afirmativas sobre segurança em senhas de acesso.

I - Todo vírus com extensão EXE instala um programa espião para roubo de senhas.

II - Quanto menor o tamanho de uma senha, maior sua segurança.

III - Quanto maior a aleatoriedade de uma senha, maior sua segurança.

Está(ão) correta(s), somente, a(s) afirmativa(s):

(A) I

(B) II

(C) III

(D) I eIII

(E) II e III

4. Que técnica é utilizada em programas de antivírus para detecção de vírus desconhecidos?

(A) Heurística.

(B) md5.

(C) Imunização.

(D) Quarentena.

(E) Backdoor.

5. Uma empresa faz backup completo (full, com duração de 2h) de seus arquivos, semanalmente, sempre aos domingos às 18h. Diariamente, um backup incremental é realizado às 21h. Em uma determinada quinta-feira, houve uma pane às 15h, ocasionando a perda total dos arquivos.

Com base nestas informações, assinale a afirmativa correta.

(A) Arquivos gravados na quinta-feira às 14h serão recuperados a partir dos backups de domingo e quarta-feira.

(B) Todos os arquivos gravados na quinta-feira serão perdidos, exceto os menores que 1 MB.

(C) A recuperação poderá ser feita a partir dos backups de segunda a quarta-feira, sem a necessidade do backup de domingo.

(D) Para recuperação dos arquivos até a última posição possível, serão necessários somente os backups de domingo e quarta-feira.

(E) Para recuperação dos arquivos até a última posição possível, serão necessários os backups de domingo a quarta-feira, indispensavelmente.

6. Para executar tarefas comuns, que não exijam privilégios de administrador, é uma boa prática de segurança não utilizar um usuário que possua tais privilégios, uma vez que

(A) cavalos de tróia só atacam máquinas autenticadas com administrador do sistema.

(B) um código malicioso pode ganhar os privilégios do usuário autenticado.

(C) programas antivírus só podem ser atualizados por usuários sem privilégios de administrador.

(D) usuários sem privilégio de administrador são imunes a código malicioso.

(E) usuários sem privilégios de administrador, apenas, possuem permissão para executar o navegador html.

7. Considerando-se backups completos e incrementais, julgue as afirmações a seguir.

I - A realização de backups (completos ou incrementais) objetiva minimizar a probabilidade de perda de dados, enquanto a realização de restauração visa a recuperar dados previamente armazenados.

II - O procedimento de geração de backups incrementais compara a data da última escrita de um arquivo com a data de realização do último backup para decidir se deve copiar o arquivo.

III - A restauração de arquivos gravados em backups incrementais é mais trabalhosa do que a restauração de um arquivo em um backup completo.

É(São) verdadeira(s) a(s) afirmação(ões)

(A) I, apenas.

(B) I e II, apenas.

(C) I e III, apenas.

(D) II e III, apenas.

(E) I, II e III.

**8. Vírus de computador é um programa escrito por programadores mal intencionados. É como um vírus biológico, vive para se reproduzir. Para proteger seu micro, é necessário saber como eles agem, possibilitando sua detecção e eliminação com um programa anti-vírus. Sobre vírus de computador, é incorreto afirmar que:**

**a) infectam arquivos executáveis, como processadores de texto, planilhas, jogos ou programas do sistema operacional.**

**b) se anexam a programas especiais em áreas do disco rígido chamadas de registros de inicialização e registros mestres de inicialização.**

**c) alguns são programados para apagar arquivos, deteriorar programas e reformatar o disco rígido.**

**d) alguns não têm a finalidade de fazer estragos no computador, apenas duplicam-se ou exibem mensagens.**

**e) infectam ou danificam o teclado, o monitor, o disco rígido e todos os demais periféricos.**

**9. Observe abaixo o quadro que trata de tipos de vírus de computador, que representam uma grave ameaça à segurança na Internet, sendo uma preocupação constante dos administradores de redes de computadores.**

|  |  |
| --- | --- |
| **TIPO** | **DESCRIÇÃO** |
| **I** | **são programas ou scripts que “seqüestram” navegadores de Internet, principalmente o Internet Explorer. Quando isso ocorre, os vírus alteram a página inicial do browser e impedem o usuário de mudá-la, exibem propagandas em pop-ups ou janelas novas, instalam barras de ferramentas no navegador e podem impedir acesso a determinados sites, como os de software antivírus, por exemplo.** |
| **II** | **são tipos de pragas digitais que, basicamente, permitem acesso remoto ao computador após a infecção. Esses vírus podem ter outras funcionalidades, como captura de dados do usuário e execução de instruções presentes em scripts. Entre tais instruções, pode haver ordens para apagar arquivos, destruir aplicativos, entre outras.** |
| **III** | **são pequenos aplicativos que podem vir embutidos em vírus ou softwares suspeitos, destinados a capturar tudo o que é digitado no teclado. O objetivo principal, nesses casos, é capturar senhas.** |

**Os vírus dos tipos I, II e III são denominados, respectivamente, de:**

**a) hijacker, trojan e keylogger**

**b) keylogger, spyware e macro**

**c) trojan, keylooger e sniffer**

**d) macro, worm e hijacker**

**e) spyware, sniffer e worm**

**10. O que são Spywares?**

**a) São programas automáticos de computadores que recolhem informações sobre o usuário e as enviam a uma entidade externa na Internet, sem o conhecimento ou consentimento do usuário.**

**b) É um programa que, ao se instalar no computador, libera uma porta para um possível invasor.**

**c) É uma modalidade de distribuição de software em que é permitido tirar cópias, distribuí-los sem restrições e usá-lo experimentalmente por um determinado período.**

**d) É um programa auto-replicante, que tenta se espalhar para outros computadores, utilizando-se de diversos meios.**

**e) É um programa de computador da Microsoft destinado a combater os Spans.**

**11. Nos sistemas de Segurança da Informação, existe um método que \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_. Este método visa garantir a integridade da informação. Escolha a opção que preenche corretamente a lacuna acima.**

**a) valida a autoria da mensagem**

**b) verifica se uma mensagem em trânsito foi alterada**

**c) verifica se uma mensagem em trânsito foi lida por pessoas não autorizadas**

**d) cria um backup diferencial da mensagem a ser transmitida**

**e) passa um antivírus na mensagem a ser transmitida**

**12**

**13. Os investimentos na área de segurança da informação têm crescido em paralelo com o crescimento do comércio eletrônico na Internet. Com relação aos conceitos de segurança da informação é correto afirmar que a:**

**a) confiabilidade é a habilidade de cada usuário saber que os outros são quem dizem ser.**

**b) integridade de mensagens é a habilidade de se ter certeza de que a mensagem remetida chegará ao destino sem ser modificada.**

**c) autenticidade é a garantia de que os sistemas estarão disponíveis quando necessário.**

**d) integridade é a garantia de que os sistemas desempenharão seu papel com eficácia em um nível de qualidade aceitável.**

**e) confiabilidade é a capacidade de controlar quem vê as informações e sob quais condições.**

**14. No que diz respeito à proteção e à segurança em informática, analise as definições abaixo:**

|  |  |
| --- | --- |
| **I** | **Procedimento para salvaguarda física de informações.** |
| **II** | **Palavra secreta que visa a restringir o acesso a determinadas informações.** |
| **III** | **Método de codificação de dados que visa a garantir o sigilo de informações.** |

**Essas definições correspondem, respectivamente, a**

**a) layout, criptograma e restore.**

**b) backup, password e criptografia.**

**c) lookup, password e login.**

**d) criptografia, login e backup.**

**e) backup, plugin e reprografia.**

**15. Analise as seguintes afirmações relacionadas à criptografia.**

**I. A criptografia de chave simétrica pode manter os dados seguros, mas se for necessário compartilhar informações secretas com outras pessoas, também deve-se compartilhar a chave utilizada para criptografar os dados.**

**II. Com algoritmos de chave simétrica, os dados assinados pela chave pública podem ser verificados pela chave privada.**

**III. Com algoritmos RSA, os dados encriptados pela chave pública devem ser decriptados pela chave privada.**

**IV. Com algoritmos RSA, os dados assinados pela chave privada são verificados apenas pela mesma chave privada**

**Indique a opção que contenha todas as afirmações verdadeiras.**

**a) I e II**

**b) II e III**

**c) III e IV**

**d) I e III**

**e) II e IV**

**16. (Auditor Receita Federal) O processo de cifragem e decifragem são realizados com o uso de algoritmos com funções matemáticas que protegem a informação quanto à sua integdade, autenticidade e sigilo. Quanto aos algoritmos utilizados nos processos de cifragem, decifragem e assinatura digital é correto afirmar que:**

**a) o uso da assinatura digital garante o sigilo da mensagem independentemente do tipo de chave utilizada.**

**b) os algoritmos RSA para assinatura digital fazem o uso de chave simétrica.**

**c) os algoritmos de chave simétrica têm como principal característica a possibilidade de utilização de assinatura digital e de certificação digital, sem alteração da chave.**

**d) a criptografia de chave simétrica tem como característica a utilização de uma mesma chave secreta para a codificação e decodificação dos dados.**

**e) a assinatura digital é obtida com a aplicação do algoritmo de Hash sobre a chave pública do usuário que deseja assinar digitalmente uma mensagem.**

**17. Criptografia simétrica é um método de codificação que utiliza**

**(A) uma chave pública e uma chave privada para encriptar e decodificar a mesma mensagem.**

**(B) duas chaves públicas para encriptar e decodificar a mesma mensagem.**

**(C) uma só chave para encriptar e decodificar a mesma mensagem.**

**(D) duas chaves privadas para encriptar e decodificar a mesma mensagem.**

**(E) uma chave pública e duas chaves privadas para encriptar e decodificar a mesma mensagem.**

**Gabarito**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 01 | 02 | 03 | 04 | 05 | 06 | 07 | 08 |
| c | c | c | c | e | b | b | e |
| 09 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| a | a | e | c | b | b | b | d |
| 17 |  |  |  |  |  |  |  |
| c |  |  |  |  |  |  |  |