Cartilha de Segurança para Internet
Parte II: Riscos Envolvidos no Uso da Internet e Métodos de Prevenção

NIC BR Security Office
nbso@nic.br

Versão 2.0
11 de março de 2003

Resumo

Esta parte da Cartilha aborda diversos riscos envolvidos no uso da Internet e seus métodos de prevenção. São discutidos os programas que possibilitam aumentar a segurança de um computador, como antivírus e *firewalls*, e apresentados riscos e medidas preventivas no uso de programas de *e-mail*, de troca de mensagens, de distribuição de arquivos, *browsers* e recursos de compartilhamento de arquivos. Também é discutida a importância da realização de cópias de segurança. Algumas seções aqui apresentadas necessitam do entendimento de conceitos discutidos na parte I desta Cartilha (Conceitos de Segurança).

Como Obter este Documento

Este documento pode ser obtido em http://www.nbso.nic.br/docs/cartilha/. Como ele é periodicamente atualizado, certifique-se de ter sempre a versão mais recente.

Caso você tenha alguma sugestão para este documento ou encontre algum erro, entre em contato através do endereço doc@nic.br.

Nota de *Copyright* e Distribuição

Sumário

1 Vírus

1.1 Como posso saber se um computador está infectado?

A melhor maneira de descobrir se um computador está infectado é através dos programas antivírus (vide seção 3).

É importante ressaltar que o antivírus deve ser **sempre atualizado**, caso contrário poderá **não** detectar os vírus mais recentes.

1.2 Existe alguma maneira de proteger um computador de vírus?

Sim. Algumas das medidas de prevenção contra a infecção por vírus são:

- instalar e manter atualizado um bom programa antivírus;
- desabilitar no seu programa de *e-mail* a auto-execução de arquivos anexados às mensagens;
- não executar ou abrir arquivos recebidos por *e-mail*, mesmo que venham de pessoas conhecidas, mas caso seja inevitável, certifique-se que o arquivo foi verificado pelo programa antivírus;
- não abrir arquivos ou executar programas de procedência duvidosa ou desconhecida e mesmo que você conheça a procedência e queira abrí-los ou executá-los, certifique-se que foram verificados pelo programa antivírus;
- procurar utilizar, no caso de arquivos de dados, formatos menos suscetíveis à propagação de vírus, tais como RTF, PDF ou PS;
- procurar não utilizar, no caso de arquivos comprimidos, o formato executável. Utilize o próprio formato compactado, como por exemplo ZIP ou GZ.

2 Cavalos de Tróia

2.1 O que um cavalo de tróia pode fazer em um computador?

O cavalo de tróia, na maioria das vezes, irá instalar programas para possibilitar que um invasor tenha controle total sobre um computador. Estes programas podem permitir que o invasor:

- veja e copie todos os arquivos armazenados no computador;
- descubra todas as senhas digitadas pelo usuário;
- formate o disco rígido do computador, etc.

2.2 Um cavalo de tróia pode instalar programas sem o conhecimento do usuário?

Sim. Normalmente o cavalo de tróia procura instalar programas, para realizar uma série de atividades maliciosas, sem que o usuário perceba.

2.3 É possível saber se um cavalo de tróia instalou algo em um computador?

A utilização de um bom programa antivírus (desde que seja atualizado freqüentemente) normalmente possibilita a detecção de programas instalados pelos cavalos de tróia.

É importante lembrar que nem sempre o antivírus será capaz de detectar ou remover os programas deixados por um cavalo de tróia, principalmente se estes programas forem mais recentes que a sua versão de antivírus.

2.4 Existe alguma maneira de proteger um computador dos cavalos de tróia?

Sim. As principais medidas preventivas contra a instalação de cavalos de tróia são semelhantes às medidas contra a infecção por vírus e estão listadas na seção 1.2.

Uma outra medida preventiva é utilizar um *firewall* pessoal. Alguns *firewalls* podem bloquear o recebimento de cavalos de tróia (vide seção 7).

3 Antivírus

Os antivírus são programas que procuram detectar e, então, anular ou remover os vírus de computador. Atualmente, novas funcionalidades têm sido adicionadas aos programas antivírus, de modo que alguns procuram detectar e remover cavalos de tróia, barrar programas hostis e verificar *e-mails*.

3.1 Que funcionalidades um bom antivírus deve possuir?

Um bom antivírus deve:

- identificar e eliminar a maior quantidade possível de vírus;
- analisar os arquivos que estão sendo obtidos pela Internet;
- verificar continuamente os discos rígidos (HDs), flexíveis (disquetes) e CDs de forma transparente ao usuário;
- procurar vírus e cavalos de tróia em arquivos anexados aos *e-mails*;

- criar, sempre que possível, um disquete de verificação (disquete de *boot*) que possa ser utilizado caso o vírus desative o antivírus que está instalado no computador;
- atualizar a lista de vírus conhecidos, pela rede, de preferência diariamente.

Alguns antivírus, além das funcionalidades acima, permitem verificar *e-mails* enviados, podendo detectar e barrar a propagação por *e-mail* de vírus e *worms*.

3.2 Como faço bom uso do meu antivírus?

As dicas para o bom uso do antivírus são simples:

- mantenha-o sempre atualizado;
- configure-o para verificar automaticamente arquivos anexados aos *e-mails* e arquivos obtidos pela Internet;
- configure-o para verificar automaticamente mídias removíveis (CDs, disquetes, discos para Zip, etc);
- configure-o para verificar todo e qualquer formato de arquivo (qualquer tipo de extensão de arquivo);
- se for possível, crie o disquete de verificação e utilize-o esporadicamente, ou quando seu computador estiver apresentando um comportamento anormal (mais lento, gravando ou lendo o disco rígido fora de hora, etc.);

Algumas versões de antivírus são gratuitas para uso pessoal e podem ser obtidas pela Internet. Mas antes de obter um antivírus pela Internet, verifique sua procedência e certifique-se que o fabricante é confiável.

3.3 O que um antivírus não pode fazer?

Um antivírus não é capaz de impedir que um atacante tente explorar alguma vulnerabilidade (seção 4) existente em um computador. Também não é capaz de evitar o acesso não autorizado a um *backdoor* (seção 6) instalado em um computador.

Existem também outros mecanismos de defesa, conhecidos como *firewalls*, que podem prevenir contra tais ameaças (vide seção 7);

4 Vulnerabilidades

4.1 Como posso saber se os *softwares* instalados em meu computador possuem alguma vulnerabilidade?

Existem *sites* na Internet que mantém listas atualizadas de vulnerabilidades em *softwares* e sistemas operacionais. Alguns destes *sites* são http://www.cert.org/ e http://cve.mitre.org/.

Além disso, fabricantes também costumam manter páginas na Internet com considerações a respeito de possíveis vulnerabilidades em seus *softwares*.

Portanto, a idéia é estar sempre atento aos *sites* especializados em acompanhar vulnerabilidades, aos *sites* dos fabricantes, às revistas especializadas e aos cadernos de informática dos jornais, para verificar a existência de vulnerabilidades no sistema operacional e nos *softwares* instalados em seu computador.

4.2 Como posso corrigir as vulnerabilidades dos *softwares* em meu computador?

A melhor forma de evitar que o sistema operacional e os *softwares* instalados em um computador possuam vulnerabilidades é mantê-los **sempre atualizados**.

Entretanto, fabricantes em muitos casos não disponibilizam novas versões de seus *softwares* quando é descoberta alguma vulnerabilidade, mas sim correções específicas (*patches*). Estes *patches*, em alguns casos também chamados de *hot fixes* ou *service packs*, têm por finalidade corrigir os problemas de segurança referentes às vulnerabilidades descobertas.

Portanto, é **extremamente importante** que você, além de manter o sistema operacional e os *softwares* sempre atualizados, instale os *patches* sempre que forem disponibilizados.

5 *Worms*

5.1 Como posso saber se meu computador está sendo utilizado para propagar um *worm*?

Detectar a presença de um *worm* em um computador não é uma tarefa fácil. Muitas vezes os *worms* realizam uma série de atividades, incluindo sua propagação, sem que o usuário tenha conhecimento.

Embora alguns programas antivírus permitam detectar a presença de *worms* e até mesmo evitar que eles se propaguem, isto nem sempre é possível.

Portanto, o melhor é evitar que seu computador seja utilizado para propagá-los (vide seção 5.2).

5.2 Como posso proteger um computador de *worms*?

Além de utilizar um bom antivírus, que permita detectar e até mesmo evitar a propagação de um *worm*, é importante que o sistema operacional e os *softwares* instalados em seu computador não possuam vulnerabilidades.

Normalmente um *worm* procura explorar alguma vulnerabilidade disponível em um computador, para que possa se propagar. Portanto, as medidas preventivas mais importantes são aquelas que procuram evitar a existência de vulnerabilidades, como visto na seção 4.2.

Uma outra medida preventiva é ter instalado em seu computador um *firewall* pessoal (seção 7). Se bem configurado, o *firewall* pessoal pode evitar que um *worm* explore uma possível vulnerabilidade em algum serviço disponível em seu computador ou, em alguns casos, mesmo que o *worm* já esteja instalado em seu computador, pode evitar que explore vulnerabilidades em outros computadores.

6 *Backdoors*

6.1 Existe alguma maneira de proteger um computador de *backdoors*?

Embora os programas antivírus não sejam capazes de descobrir *backdoors* em um computador, as medidas preventivas contra a infecção por vírus (seção 1.2) são válidas para se evitar algumas formas de instalação de *backdoors*.

A idéia é que você **não** execute programas de procedência duvidosa ou desconhecida, sejam eles recebidos por *e-mail*, sejam obtidos na Internet. A execução de tais programas pode resultar na instalação de um *backdoor*.

Caso você utilize algum programa de administração remota, certifique-se de que ele esteja bem configurado, de modo a evitar que seja utilizado como um *backdoor*.

Uma outra medida preventiva consiste na utilização de um *firewall* pessoal (vide seção 7). Apesar de não eliminarem os *backdoors*, se bem configurados, podem ser úteis para amenizar o problema, pois podem barrar as conexões entre os invasores e os *backdoors* instalados em um computador.

Também é importante visitar constantemente os *sites* dos fabricantes de *softwares* e verificar a existência de novas versões ou *patches* para o sistema operacional ou *softwares* instalados em seu computador.

Existem casos onde a disponibilização de uma nova versão ou de um *patch* está associada à descoberta de uma vulnerabilidade em um *software*, que permite a um atacante ter acesso remoto a um computador, de maneira similar ao acesso aos *backdoors*.

7 *Firewalls*

Os *firewalls* são dispositivos constituídos pela combinação de *software* e *hardware*, utilizados para dividir e controlar o acesso entre redes de computadores.

O ***firewall* pessoal** é um *software* ou programa utilizado para proteger **um** computador contra acessos não autorizados vindos da Internet, e constitui um tipo específico de *firewall*.

7.1 Como o *firewall* pessoal funciona?

Se alguém ou algum programa suspeito tentar se conectar ao seu computador, um *firewall* bem configurado entra em ação para bloquear tais tentativas, podendo barrar o acesso a *backdoors*, mesmo se já estiverem instalados em seu computador.

Alguns programas de *firewall* permitem analisar continuamente o conteúdo das conexões, filtrando cavalos de tróia e vírus de *e-mail* antes mesmo que os antivírus entrem em ação.

Também existem pacotes de *firewall* que funcionam em conjunto com os antivírus, provendo um maior nível de segurança para os computadores onde são utilizados.

7.2 Por que devo instalar um *firewall* pessoal em meu computador?

É comum observar relatos de usuários que acreditam ter computadores seguros por utilizarem apenas programas antivírus. O fato é que a segurança de um computador não pode basear-se apenas em **um** mecanismo de defesa.

Um antivírus não é capaz de impedir o acesso a um *backdoor* instalado em um computador. Já um *firewall* bem configurado pode bloquear o acesso a ele.

Além disso, um *firewall* poderá bloquear e permitir que o usuário identifique as tentativas de explorar vulnerabilidades em seu computador e as possíveis origens de tais ataques.

Alguns fabricantes de *firewalls* oferecem versões gratuitas de seus produtos para uso pessoal. Mas antes de obter um *firewall*, verifique sua procedência e certifique-se que o fabricante é confiável.

7.3 Como posso saber se estão tentando invadir meu computador?

Normalmente os *firewalls* criam arquivos em seu computador, denominados arquivos de registro de eventos (*logs*). Nestes arquivos são armazenadas as tentativas de acesso não autorizado ao seu computador, para serviços que podem ou não estar habilitados.

A parte VII desta cartilha (Incidentes de Segurança e Uso Abusivo da Rede) apresenta um guia para que você não só identifique tais tentativas, mas também reporte-as para os responsáveis pela rede ou computador de onde a tentativa de ataque se originou.

8 Programas de *E-Mail*

8.1 Quais são os riscos associados ao uso de um programa de *e-mail*?

Grande parte dos problemas de segurança envolvendo *e-mails* estão relacionados aos conteúdos das mensagens, que normalmente abusam das técnicas de engenharia social (partes I e IV desta cartilha) ou de características de determinados programas de *e-mail*, que permitem abrir arquivos ou executar programas anexados às mensagens automaticamente.

8.2 É possível configurar um programa de *e-mail* de forma mais segura?

Sim. Algumas dicas de configuração para melhorar a segurança do seu programa de *e-mail* são:

1. desligar as opções que permitem abrir ou executar automaticamente arquivos ou programas anexados às mensagens;
2. desligar as opções de execução do *JavaScript* e de programas *Java* (seção 9.2);
3. desligar, se possível, o modo de visualização de *e-mails* no formato HTML.

Estas configurações podem evitar que o seu programa de *e-mail* propague automaticamente vírus e cavalos de tróia. Existem programas de *e-mail* que não implementam tais funções e, portanto, não possuem estas opções.

É importante ressaltar que se o usuário seguir as recomendações dos itens 1 e 2, mas ainda assim abrir os arquivos ou executar manualmente os programas que vêm anexados aos *e-mails*, poderá ter algum problema que resulte na violação da segurança do seu computador.

8.3 Que medidas preventivas devo adotar no uso dos programas de *e-mail*?

Algumas medidas preventivas que minimizam os problemas trazidos com os *e-mails* são:

- manter sempre a versão mais atualizada do seu programa de *e-mail*;
- evitar abrir arquivos ou executar programas anexados aos *e-mails*, sem antes verificá-los com um antivírus;
- desconfiar sempre dos arquivos anexados à mensagem, mesmo que tenham sido enviados por pessoas ou instituições conhecidas. O endereço do remetente pode ter sido forjado[1] e o arquivo anexo pode ser, por exemplo, um vírus ou um cavalo de tróia;
- fazer o *download* de programas diretamente do *site* do fabricante;

[1] Existem vírus que utilizam o *e-mail* como meio para sua replicação e quase sempre forjam o endereço do remetente.

- desconfiar de *e-mails* pedindo urgência na instalação de algum aplicativo ou correções de determinados defeitos dos *softwares* que você utilize. Caso isto ocorra, entre em contato com os distribuidores destes *softwares* para certificar-se sobre a veracidade do fato.

9 *Browsers*

9.1 Quais são os riscos associados ao uso de um *browser*?

Existem diversos riscos envolvidos na utilização de um *browser*. Dentre eles, podem-se citar:

- execução de *Javascript* ou de programas *Java* hostis;
- execução de programas ou controles *ActiveX* hostis;
- obtenção e execução de programas hostis em *sites* não confiáveis;
- realização de transações comerciais ou bancárias via *Web*, sem qualquer mecanismo de segurança.

Nos dois primeiros casos o *browser* executa os programas automaticamente, ou seja, sem a interferência do usuário.

9.2 Quais são os riscos associados à execução de *Javascripts* e de programas *Java*?

Normalmente os *browsers* contém módulos específicos para processar programas *Java*. Apesar destes módulos fornecerem mecanismos de segurança, podem conter falhas de implementação e, neste caso, permitir que um programa *Java* hostil cause alguma violação de segurança em um computador.

O *JavaScript* é bem mais utilizado em páginas *Web* do que os programas *Java* e, de modo geral, constitui uma versão bem "enxuta" do *Java*. É importante ressaltar que isto não quer dizer que não existam riscos associados à sua execução. Um *Javascript* hostil também pode acarretar a violação da segurança de um computador.

9.3 Quais são os riscos associados à execução de programas *ActiveX*?

Antes de receber um programa *ActiveX*, o seu *browser* verifica sua procedência através de um esquema de certificados digitais (vide partes I e IV desta cartilha). Se você optar por aceitar o certificado, o programa é executado em seu computador.

Ao serem executados, os programas *ActiveX* podem fazer de tudo, desde enviar um arquivo qualquer pela Internet, até instalar programas (que podem ter fins maliciosos) em seu computador.

9.4 Quais são os riscos associados ao uso de *cookies*?

Muitos *sites*, ao serem acessados, utilizam *cookies* para manter informações, como por exemplo, as preferências de um usuário. Estas informações, muitas vezes, são compartilhadas entre diversas entidades na Internet e podem afetar a privacidade do usuário.

Maiores detalhes sobre os riscos envolvidos no uso de *cookies* bem como formas de se ter maior controle sobre eles pode ser vistos na parte III desta cartilha (Privacidade).

9.5 Quais são os cuidados necessários para realizar transações via *Web*?

Normalmente as transações, sejam comerciais ou bancárias, envolvem informações sensíveis, como senhas ou números de cartões de crédito.

Portanto, é muito importante que você, ao realizar transações via *Web*, certifique-se da procedência dos *sites*, se estes *sites* são realmente das instituições que dizem ser e se eles fornecem mecanismos de segurança para evitar que alguém conectado à Internet possa obter informações sensíveis de suas transações, no momento em que estiverem sendo realizadas.

Maiores detalhes sobre estes cuidados, bem como formas de prevenção na realização de transações via *Web* podem ser vistos na parte IV desta cartilha (Fraudes na Internet).

9.6 Que medidas preventivas devo adotar no uso de *browsers*?

Algumas medidas preventivas para o uso de *browsers* são:

- manter o seu *browser* sempre atualizado;
- desativar a execução de programas *Java* na configuração de seu *browser*[2]. Se for absolutamente necessário o *Java* estar ativado para que as páginas de um *site* possam ser vistas, basta ativá-lo antes de entrar no *site* e, então, desativá-lo ao sair;
- desativar a execução de *Javascripts* antes de entrar em uma página desconhecida e, então, ativá-la ao sair. Caso você opte por desativar a execução de *Javascripts* na configuração de seu *browser*, é provável que muitas páginas *Web* não possam ser visualizadas;
- permitir que programas *ActiveX* sejam executados em seu computador apenas quando vierem de *sites* conhecidos e confiáveis.
- manter maior controle sobre o uso de *cookies*, caso você queira ter maior privacidade ao navegar na Internet (vide parte III desta cartilha);
- certificar-se da procedência do *site* e da utilização de conexões seguras ao realizar transações via *Web* (vide parte IV desta cartilha).

[2] Os programas *Java* não são utilizados na maiora das páginas *Web* e, quando utilizados, a desativação de sua execução não costuma comprometer a visualização da página.

10 Programas de Troca de Mensagens

10.1 Quais são os riscos associados ao uso de salas de bate-papo e de programas como o ICQ ou IRC?

Os maiores riscos associados ao uso destes programas estão no conteúdo dos próprios diálogos. Alguém pode utilizar técnicas de engenharia social (vide partes I e IV desta cartilha) para obter informações (muitas vezes sensíveis) dos usuários destes porgramas.

Você pode ser persuadido a entregar seu *e-mail*, telefone, endereço, senhas (como a de acesso ao seu provedor), número do cartão de crédito, em uma conversa "amigável". As conseqüências podem ser desde o recebimento de mensagens com conteúdo falso/alarmante ou mensagens não solicitadas contendo propagandas (vide parte V desta cartilha), até a utilização da sua conta para realizar atividades ilícitas ou a utilização de seu número de cartão de crédito para fazer compras em seu nome.

Além disso, estes programas podem fornecer o seu endereço na Internet (endereço IP[3]). Um atacante pode usar esta informação para, por exemplo, tentar explorar uma possível vulnerabilidade em seu computador.

10.2 Existem problemas de segurança específicos no uso de programas de troca instantânea de mensagens?

Sim. Programas, tais como o ICQ, AOL Instant Messenger e Yahoo! Messenger ficam constantemente conectados a um servidor (senão não teriam como saber quem está no ar) e, como estão conectados, podem ser alvos de ataques.

Lembre-se que qualquer programa que utilize a Internet para prestar algum serviço (como neste caso troca de mensagens) pode possuir alguma vulnerabilidade e ficar sujeito a ataques externos.

10.3 Que medidas preventivas devo adotar no uso de programas de troca de mensagens?

Algumas medidas preventivas para o uso de programas de troca de mensagens são:

- manter seu programa de troca de mensagens sempre atualizado, para evitar que possua alguma vulnerabilidade (vide seção 4);
- não aceitar arquivos de pessoas desconhecidas, principalmente programas de computadores;
- evitar fornecer muita informação, principalmente a pessoas que você acabou de conhecer;
- não fornecer, em hipótese alguma, informações sensíveis, tais como senhas ou números de cartões de crédito;

[3] O significado de endereço IP pode ser encontrado no Glossário desta cartilha.

- configurar o programa para ocultar o seu endereço IP.

11 Programas de Distribuição de Arquivos

11.1 Quais são os riscos associados ao uso de programas de distribuição de arquivos?

Existem diversos riscos envolvidos na utilização de programas de distribuição de arquivos, tais como o Kaaza, Morpheus, Edonkey e Gnutella. Dentre estes riscos, podem-se citar:

Acesso não-autorizado: o programa de distribuição de arquivos pode permitir o acesso não autorizado ao computador, caso esteja mal configurado ou possua alguma vulnerabilidade;

***Softwares* ou arquivos maliciosos:** os *softwares* ou arquivos distribuídos podem ter finalidades maliciosas. Podem, por exemplo, conter vírus, ser um cavalo de tróia, ou instalar *backdoors* em um computador;

Violação de direitos autorais (*Copyright*): a distribuição não autorizada de arquivos de música, filmes, textos ou programas protegidos pela lei de direitos autorais constitui a violação desta lei.

11.2 Que medidas preventivas devo adotar no uso de programas de distribuição de arquivos?

Algumas medidas preventivas para o uso de programas de distribuição de arquivos são:

- manter seu programa de distribuição de arquivos sempre atualizado e bem configurado;
- ter um bom antivírus instalado em seu computador, mantê-lo atualizado e utilizá-lo para verificar qualquer arquivo obtido, pois eles podem conter vírus ou cavalos de tróia;
- certificar-se que os arquivos obtidos ou distribuídos são **livres**, ou seja, não violam as leis de direitos autorais.

12 Compartilhamento de Recursos do Windows

12.1 Quais são os riscos associados ao uso do compartilhamento de recursos?

Um recurso compartilhado aparece no Explorer do Windows como uma “mãozinha” segurando a parte de baixo do ícone (pasta, impressora ou disco), como mostra a figura 1.

Alguns dos riscos envolvidos na utilização de recursos compartilhados por terceiros são:

Figura 1: Exemplos de ícones para recursos compartilhados.

- abrir arquivos ou executar programas que contenham vírus;
- executar programas que sejam cavalos de tróia.

Já alguns dos riscos envolvidos em compartilhar recursos do seu computador são:

- permitir o acesso não autorizado a recursos ou informações sensíveis;
- permitir que um atacante possa utilizar tais recursos, sem quaisquer restrições, para fins maliciosos. Isto pode ocorrer se não forem definidas senhas para os compartilhamentos.

12.2 Que medidas preventivas devo adotar no uso do compartilhamento de recursos?

Algumas medidas preventivas para o uso do compartilhamento de recursos do Windows são:

- ter um bom antivírus instalado em seu computador, mantê-lo atualizado e utilizá-lo para verificar qualquer arquivo ou programa compartilhado, pois eles podem conter vírus ou cavalos de tróia;
- estabelecer senhas para os compartilhamentos, caso seja estritamente necessário compartilhar recursos do seu computador. Procure elaborar senhas fáceis de lembrar e difíceis de serem descobertas (vide parte I desta cartilha).

É importante ressaltar que você deve sempre utilizar senhas para os recursos que deseje compartilhar, principalmente os que estão habilitados para leitura e escrita. E, quando possível, não compartilhe recursos ou não deixe-os compartilhados por muito tempo.

13 Realização de Cópias de Segurança (*Backups*)

13.1 Qual é a importância de fazer cópias de segurança?

Cópias de segurança dos dados armazenados em um computador são importantes, não só para se recuperar de eventuais falhas, mas também das conseqüências de uma possível infecção por vírus, ou de uma invasão.

13.2 Quais são as formas de realizar cópias de segurança?

Cópias de segurança podem ser simples como o armazenamento de arquivos em CDs, ou mais complexas como o espelhamento de um disco rígido inteiro em um outro disco de um computador.

Atualmente, uma unidade gravadora de CDs e um *software* que possibilite copiar dados para um CD são suficientes para que a maior parte dos usuários de computadores realizem suas cópias de segurança.

Também existem equipamentos e *softwares* mais sofisticados e específicos que, dentre outras atividades, automatizam todo o processo de realização de cópias de segurança, praticamente sem intervenção do usuário. A utilização de tais equipamentos e *softwares* envolve custos mais elevados e depende de necessidades particulares de cada usuário.

13.3 Com que freqüência devo fazer cópias de segurança?

A freqüência com que é realizada uma cópia de segurança e a quantidade de dados armazenados neste processo depende da periodicidade com que o usuário cria ou modifica arquivos. Cada usuário deve criar sua própria política para a realização de cópias de segurança.

13.4 Que cuidados devo ter com as cópias de segurança?

Os cuidados com cópias de segurança dependem das necessidades do usuário. O usuário deve procurar responder algumas perguntas antes de adotar um ou mais cuidados com suas cópias de segurança:

- Que informações realmente importantes precisam estar armazenadas em minhas cópias de segurança?
- Quais seriam as conseqüências/prejuízos, caso minhas cópias de segurança fossem destruídas ou danificadas?
- O que aconteceria se minhas cópias de segurança fossem furtadas?

Baseado nas respostas para as perguntas anteriores, um usuário deve atribuir maior ou menor importância a cada um dos cuidados discutidos abaixo:

Escolha dos dados: cópias de segurança devem conter apenas arquivos confiáveis do usuário, ou seja, que não contenham vírus ou sejam cavalos de tróia. Arquivos do sistema operacional e que façam parte da instalação dos *softwares* de um computador não devem fazer parte das cópias de segurança. Eles pode ter sido modificados ou substituídos por versões maliciosas, que quando restauradas podem trazer uma série de problemas de segurança para um computador. O sistema operacional e os *softwares* de um computador podem ser reinstalados de mídias confiáveis, fornecidas por fabricantes confiáveis.

Mídia utilizada: a escolha da mídia para a realização da cópia de segurança é extremamente importante e depende da importância e da vida útil que a cópia deve ter. A utilização de alguns disquetes para armazenar um pequeno volume de dados que estão sendo modificados constantemente é perfeitamente viável. Mas um grande volume de dados, de maior importância, que deve perdurar por longos períodos, deve ser armazenado em mídias mais confiáveis, como por exemplo os CDs;

Local de armazenamento: cópias de segurança devem ser guardadas em um local condicionado (longe de muito frio ou muito calor) e restrito, de modo que apenas pessoas autorizadas tenham acesso a este local (segurança física);

Cópia em outro local: cópias de segurança podem ser guardadas em locais diferentes. Um exemplo seria manter uma cópia em casa e outra no escritório. Também existem empresas especializadas em manter áreas de armazenamento com cópias de segurança de seus clientes. Nestes casos é muito importante considerar a segurança física de suas cópias, como discutido no item anterior;

Criptografia dos dados: os dados armazenados em uma cópia de segurança podem conter informações sigilosas. Neste caso, os dados que contenham informações sigilosas devem ser armazenados em algum formato criptografado;