



## **Curso Tecnológico de Redes de Computadores**

**Disciplina: Segurança da Informação**

**Professor: José Maurício S. Pinheiro**

**V. 01/08**

### **Aula 1 – Introdução a Segurança da Informação**

**“Informação é o conjunto de dados utilizados para a transferência de uma mensagem entre pessoas ou máquinas em processos de troca de mensagens (processos comunicativos) ou transacionais (transferência de arquivos)”.**

#### **1. Conceitos de Segurança da Informação**

Na gestão empresarial moderna, a informação é tratada como um importante ativo da empresa. Essa informação pode ser impressa, manuscrita, gravada em meios magnéticos, ou simplesmente ser do conhecimento dos funcionários (falada). Essas informações (ou ativos), também podem ser classificadas de acordo com o eventual impacto negativo gerado decorrente de acesso, divulgação ou conhecimento não autorizado. Podem, por exemplo, ser classificadas como confidenciais ou restritas, internas ou públicas.

A divulgação ou o conhecimento não autorizado desses ativos pode gerar impactos dos mais variados, dentre os quais cita-se: problemas financeiros, queda na produtividade, riscos para o negócio, perda de credibilidade, desgaste da imagem, etc. A Segurança da Informação, mais que um problema de utilização de tecnologias, deve ser encarada como a gestão inteligente da informação em qualquer ambiente.

#### **2. Definição**

A Segurança da Informação é a área do conhecimento dedicada à proteção dos ativos de informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade.

Para atender essas expectativas de uma corporação, um sistema de segurança da informação deve atender aos objetivos básicos destacados a seguir:

- 1. Confidencialidade ou privacidade** – proteger as informações contra acesso de qualquer pessoa não autorizada pelo gestor da informação. Este objetivo envolve medidas como controle de acesso e criptografia;
- 2. Integridade dos dados** – evitar que dados sejam apagados ou alterados sem a permissão do gestor da informação;

3. **Disponibilidade** – garantir o funcionamento do serviço de informação e acesso aos usuários autorizados. As medidas relacionadas a esse objetivo podem ser duplicação de equipamentos e sistemas e política de backup;
4. **Consistência** – certificar-se de que o sistema atua de acordo com a expectativa dos usuários;
5. **Isolamento ou uso legítimo** – controlar o acesso ao sistema. Garantir que somente usuários autorizados possuam acesso ao sistema;
6. **Auditoria** – proteger os sistemas contra erros e atos cometidos por usuários autorizados. Para identificar autores e ações, são utilizadas trilhas de auditorias e logs, que registram o que foi executado no sistema, por quem e quando;
7. **Confiabilidade** – garantir que, mesmo em condições adversas, o sistema atuará conforme esperado;
8. **Legalidade** – a informação deve estar em conformidade com os preceitos da legislação em vigor.

### 3. Objetivos

As políticas de segurança da informação devem fornecer meios para garantir que as informações de uso restrito não serão acessadas, copiadas ou codificadas por pessoas não autorizadas. Uma das maneiras de se evitar o acesso indevido a informações confidenciais é através da codificação ou cifragem da informação, conhecida como criptografia, fazendo com que apenas as pessoas às quais estas informações são destinadas, consigam compreendê-las.

A Figura 1 representa um fluxo de informações e quatro ameaças possíveis para a segurança de um sistema de informação:

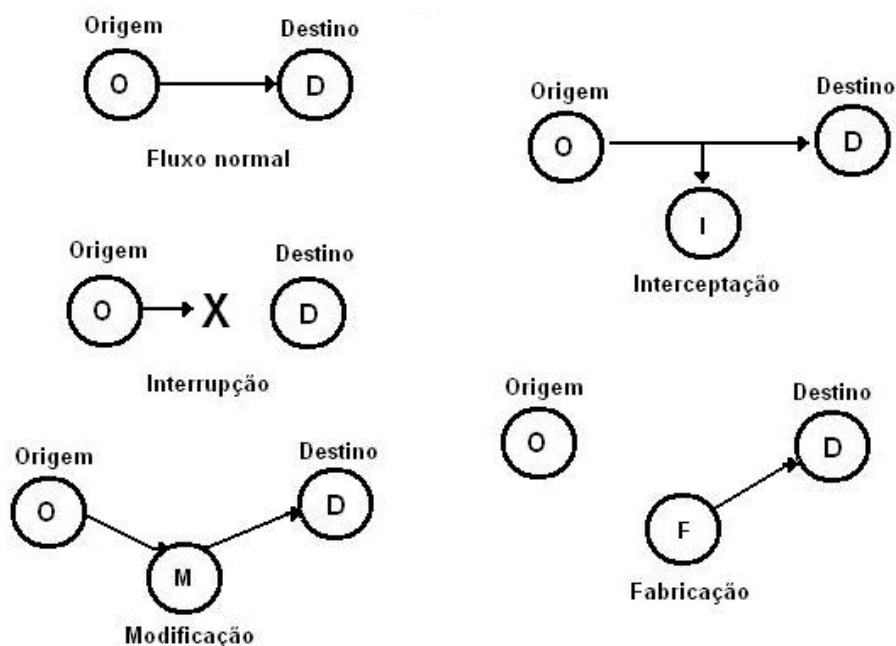


Figura 1 - Exemplos de ataques contra um sistema de informação

- **Interrupção:** Ataque na transmissão da mensagem, onde o fluxo de dados é interrompido. Um exemplo pode ser a danificação de componentes de hardware ou a queda do sistema de comunicação por sabotagem.
- **Interceptação:** Este é um ataque sobre a confidencialidade. Ocorre quando uma pessoa não autorizada tem acesso às informações confidenciais de outra. Um exemplo seria a captura de dados na rede, ou a cópia ilegal de um arquivo.
- **Modificação:** Este é um ataque à integridade da mensagem. Ocorre quando uma pessoa não autorizada, além de interceptar as mensagens, altera o conteúdo da mensagem e envia o conteúdo alterado para o destinatário.
- **Fabricação:** Este é um ataque sobre a autenticidade. Uma pessoa não autorizada insere mensagens no sistema assumindo o perfil de um usuário autorizado.

#### **4. Classificação das informações**

A classificação das informações é o processo de identificar e definir níveis e critérios de proteção adequada para as informações, objetivando garantir a segurança das mesmas. Uma organização precisa ser capaz de identificar os valores de suas informações para garantir sua confidencialidade, integridade e disponibilidades.

O objetivo principal dessa classificação está em priorizar recursos, focando os investimentos nas informações mais importantes para a organização. São exemplos de informações:

- **Dados:** base de dados e arquivos, documentação de sistema, informações armazenadas, procedimentos de suporte ou operação;
- **Software:** aplicativos, sistemas, ferramentas de desenvolvimento e utilitários;
- **Ativos físicos:** equipamentos computacionais(processadores, monitores), equipamentos de comunicação(roteadores, hubs), mídia magnética(fitas, discos), mesas, cadeiras;
- **Serviços:** serviço de operadoras de telecomunicação, serviço de energia elétrica, água, etc;

#### **5. Desclassificação e reclassificação das informações**

Uma informação pode ter seu nível de classificação alterado ou rebaixado, dependendo do nível de confidencialidade, integridade e disponibilidade que a informação tiver no momento. Por exemplo, a informação sobre um novo produto de uma empresa que ainda será lançado comercialmente. Esta informação no momento anterior ao lançamento é considerada confidencial, mas no momento em que este produto é divulgado publicamente, esta informação passa a ser pública.

## 6. Critérios de classificação das informações

Os critérios de classificação definem qual o tratamento de segurança que uma informação receberá, ou seja, quanto será preciso investir em segurança para garantir a confidencialidade, integridade e disponibilidade dessa informação, objetivando sempre priorizar recursos. Para tanto, podemos classificar as informações quanto a:

- **Confidencialidade** – Classificar a informação levando em consideração a gravidade do impacto ou prejuízo que a revelação não autorizada da mesma trará para a organização. Podem-se definir três níveis de classificação quanto a confidencialidade:
  - Confidencial - é toda informação considerada de alto risco para a empresa, pois sua revelação não autorizada pode trazer graves prejuízos. Geralmente estas informações são acessadas pela alta administração da empresa (presidência, diretoria, superintendência);
  - Restrita – é toda informação considerada de médio e baixo risco para a empresa, pois sua revelação não autorizada pode trazer prejuízos a uma determinada área da empresa. Geralmente estas informações são acessadas pelas áreas envolvidas na geração e uso destas informações, pelos gestores da área e pela alta administração;
  - Pública – é toda informação considerada de nenhum risco para a empresa e sua revelação não autorizada não traz nenhum prejuízo. Estas informações são acessadas por todos os funcionários e pessoas externas à empresa.
- **Integridade** - Classificar a informação levando em consideração a gravidade do impacto ou dos prejuízos que a modificação não autorizada da informação trará. Podem-se definir dois níveis de classificação quanto à integridade:
  - Crítica – é toda informação de alto risco para a empresa. Esta informação não pode ser alterada sem prévia autorização;
  - Não Crítica – é toda informação que, se alterada sem prévia autorização, não representa nenhum risco para a empresa.
- **Disponibilidade** - Classificar as informações levando em consideração a gravidade do impacto ou dos prejuízos que a indisponibilidade da informação trará. Podem-se definir dois níveis de classificação quanto à disponibilidade:
  - Vital - é toda informação de alto risco para a empresa. Esta informação precisa estar sempre disponível;
  - Não Vital - é toda informação que em caso de indisponibilidade não representa nenhum risco para a empresa.
- **Classificação Padrão** - Todas as informações que não forem classificadas deverão entrar no nível padrão de classificação.

## 7. Funções e Responsabilidades

Em um processo de classificação das informações devemos definir as funções e os responsáveis por cada etapa desta classificação, ou seja, devemos definir quem classifica, quem armazena, quem atualiza, etc.

- **Proprietários** - são considerados proprietários da informação os gestores das áreas geradoras das informações, sendo os proprietários responsáveis por classificar, desclassificar, redefinir os níveis de classificação das informações;
- **Custodiante** - é considerada custodiante das informações a área de informática, sendo responsável por guardar e recuperar as informações classificadas e responsáveis por prover e administrar os acessos às informações devidamente solicitados pelos proprietários.

## **8. Controles para as informações**

Devemos definir controles para as informações classificadas como confidenciais, críticas e vitais, estes controles são definidos quanto ao armazenamento, envio e descarte.

### **1. Armazenamento**

- **Armazenamento de informações eletrônicas** – As informações eletrônicas classificadas como confidenciais e/ou críticas e/ou vitais deverão ser armazenadas em locais específicos para tal finalidade, onde o mesmo será protegido com controle de acesso e procedimento de backup;
- **Armazenamento de informações impressas** – As informações impressas classificadas como confidenciais e/ou críticas e/ou vitais deverão ser armazenadas em locais protegidos do acesso por pessoas não autorizadas pelo proprietário da informação.

### **2. Envio**

- **Envio de informações eletrônicas** – O envio por correio eletrônico de informações eletrônicas classificadas como confidenciais e/ou críticas e/ou vitais deverá ser feito utilizando software de criptografia e assinatura digital, para garantir a confidencialidade, integridade e autenticidade das informações trafegadas;
- **Envio de informações impressas** – O envio de informações impressas classificadas como confidenciais e/ou críticas e/ou vitais deverá ser feito através de envelopes lacrados, contendo o nome do destinatário e um carimbo de “CONFIDENCIAL”.

### **3. Descarte**

- **Descarte de informações eletrônicas** – O descarte de mídias com informações eletrônicas classificadas como confidenciais e/ou críticas e/ou vitais deverá ser feito pela área de informática. As mídias eletrônicas contendo informações a serem descartadas deverão ser encaminhadas à área de informática pelo proprietário da informação;
- **Descarte de informações impressas** – O descarte de informações impressas classificadas como confidenciais e/ou críticas e/ou vitais deverá ser feito através de trituradores de papéis.

### **9. Etapas para o processo de classificação das informações**

As etapas que devem ser cumpridas para a correta classificação das informações são as seguintes:

- Elaboração de uma política de classificação;
- Levantamento das informações;
- Classificação das informações levantadas;
- Implementação da política;
- Revisão periódica da classificação

### **10.A política da segurança da informação**

A política da segurança da informação é um mecanismo preventivo de proteção dos dados e processos de uma organização e que define também um padrão de segurança a ser seguido pelo pessoal técnico, gerência e pelos demais usuários (internos e externos) do sistema de informação. Pode ser usada ainda para definir as interfaces entre usuários, fornecedores e parceiros e para medir a qualidade e a segurança dos sistemas atuais. Uma de suas preocupações é estabelecer os métodos de proteção, controle e monitoramento dos recursos de informação. É importante que a política de segurança defina as responsabilidades das funções relacionadas à segurança e discrimine as principais ameaças, riscos e impactos envolvidos.

A política de segurança deve integrar-se às metas de negócio da organização e ao plano das políticas de informatização, influenciando todos os projetos de informatização da empresa tais como o desenvolvimento de novos sistemas, planos de contingências, planejamento de capacidade, dentre outros. É importante lembrar que a política não envolve apenas a área de tecnologia da informação (TI), mas a organização como um todo.

Como toda política institucional, deve ser aprovada pela alta gerência e divulgada a todos os funcionários e usuários de serviços de informática. A partir de então, todos os controles devem ser baseados nessa política de segurança.



## **11. Gerenciamento de Recursos de Informação**

A segurança de uma rede de computadores é parte integrante do Gerenciamento de Recursos de Informação de uma empresa e deve preocupar-se com a aplicação das proteções (técnicas e administrativas) para minimizar as vulnerabilidades e anular falhas potenciais como:

- **Vulnerabilidades:** pontos suscetíveis a ataques, causados por uma brecha do software ou hardware, má configuração e administração ou ambos. Podemos citar como exemplo a análise do ambiente de uma sala de servidores de conectividade e Internet com a seguinte descrição: A Sala dos Servidores não possui controle de acesso físico;
- **Ameaças:** problemas que podem atacar as vulnerabilidades. Normalmente são agrupadas em três categorias: pessoais (omissão ou intenção criminal), de componentes (falha de um equipamento) e de eventos (fogo, inundação). Seguindo o exemplo da Sala dos Servidores, podemos identificar a ameaça da seguinte forma: Fraudes, Sabotagens, Roubo de Informações, Paralisação dos Serviços.

## **12. Objetivos do Gerenciamento**

A segurança de redes de computadores, dentro do conceito de Gerenciamento de Recursos, visa atender aos seguintes objetivos gerais:

- **Confidencialidade ou sigilo:** proteger contra a revelação acidental ou deliberada de informações críticas. É a garantia de que somente as pessoas ou organizações envolvidas na comunicação possam ler e utilizar as informações transmitidas de forma eletrônica pela rede;
- **Integridade:** proteger contra corrupção deliberada ou acidental de informações garantindo que o conteúdo de uma mensagem ou resultado de uma consulta não será alterado durante seu tráfego;
- **Disponibilidade:** proteger contra ações que causem a indisponibilidade de informações críticas aos usuários quando necessitarem;
- **Autenticação:** garantia de identificação das pessoas ou organizações envolvidas na comunicação;
- **Não-Repúdio (Não recusa):** garantia que o emissor de uma mensagem ou a pessoa que executou determinada transação de forma eletrônica, não poderá, posteriormente negar sua autoria.

## **13. Vírus**

Para os usuários em geral, qualquer tipo de código malicioso que apague os dados ou atrapalhe o funcionamento dos computadores é chamado de vírus. Os vírus de computador, assim denominado em função da analogia com o vírus biológico, são programas maliciosos desenvolvidos com o propósito de causar algum efeito danoso sobre o computador e/ou sobre as informações nele contidas e capazes de se reproduzir independente da

vontade ou participação do usuário. O ato de se reproduzir, no caso destes vírus, é a capacidade do mesmo de se copiar de um computador a outro, utilizando-se de diversos meios.

Os danos possíveis causados pela ação de um vírus vão desde a aparição de mensagens (indesejadas ou ofensivas), até o dano de arquivos ou mesmo dos equipamentos (danos a áreas de leitura do disco rígido, memória, CMOS, etc). O vírus passa a ter controle total sobre o computador.

Os vírus são distribuídos através de programas ou arquivos aparentemente inofensivos, como jogos, protetores de tela (*screensavers*), programas diversos copiados de outros ou baixados pela Internet, documentos anexados a e-mails, etc. Eles possuem diversas variações, podendo multiplicar-se automaticamente e ser transmitidos de computador para computador, através do contágio de *e-mails* e arquivos armazenados. Muitos podem, inclusive, apresentar mutações em suas características visando enganar os sistemas antivírus.

Um computador pode ser infectado de diversas maneiras, sendo as formas mais comuns de contágio através de um disquete esquecido no *drive* quando o micro é ligado, executando um programa desconhecido que esteja em um disquete ou, até mesmo CD-ROM, instalando programas de procedência duvidosa, abrindo arquivos do Word, Excel ou abrindo arquivos anexados aos e-mails.

#### **14. Classificação dos vírus**

Os sistemas operacionais dos computadores normalmente não detectam vírus, assim sendo, a primeira providência é verificar com o antivírus, indicando a unidade de arquivo a ser verificada. Detectando um vírus ou permanecendo a sua suspeita, não convém executar o arquivo e deve-se entrar em contato imediatamente com o departamento de responsável na empresa.

Ainda que a rede de computadores já possua softwares antivírus para detectar e eliminar os vírus, isso não é suficiente. Diariamente, novos vírus são criados e difundidos, gerando outros desafios que não aqueles previstos nos antivírus existentes. Devemos lembrar que, independente do atual processo contínuo de atualização dos antivírus pela rede, a melhor defesa está no usuário do sistema. Através da criação de hábitos de segurança, as ações dos usuários devem ser sempre de prevenção para a redução da exposição aos vírus.

Existem programas que podem atuar de forma semelhante aos vírus, mas que apresentam características diferentes, como os *worms* e cavalos de tróia. Os principais tipos de vírus são os seguintes:

##### **Vírus simples**

A RFC 2828 define um vírus de computador como sendo um software com capacidade de se duplicar, infectando outros programas, usualmente com alguma intenção maliciosa. Um vírus não pode executar-se sozinho, requer que o seu programa hospedeiro seja executado para ativar o vírus.



### **Vírus polimorfo**

Tipo de vírus que modifica a si mesmo à medida que se dissemina, dificultando a sua localização e eliminação.

### **Vírus de Macro**

Utiliza-se da linguagem VBScript, podendo ser executado em qualquer computador que possua aplicativos baseados nessa linguagem (por exemplo, Word).

### **Vírus de disco**

Infecta o setor de *boot*, responsável pela manutenção dos arquivos de inicialização de um computador.

### **Vírus residente em memória**

O vírus permanece na memória após o uso do programa infectado.

### **Vírus residente em setor ou arquivos**

Infectam arquivos executáveis ou de extensões do tipo SYS, OVL, MNT;

### **Retrovírus**

São vírus que têm como alvo os programas de antivírus.

### **Vírus Multi-partite**

Infectam tanto o setor de *boot* quanto os arquivos executáveis e são extremamente sofisticados.

### **Cavalos de Tróia**

Segundo a mitologia grega, houve uma guerra entre as cidades gregas de Atenas e Tróia. Como a cidade de Tróia era extremamente fortificada, os militares gregos a consideravam inexpugnável. Para dominá-la, os atenienses construíram uma estátua de madeira na forma de um cavalo e deram de presente para os troianos que a aceitaram de bom grado. A estátua do cavalo era oca e transportou centenas de soldados que durante a noite abriram os portões da cidade possibilitando a entrada dos do exército ateniense, o que levou à dominação de Tróia. Daí surgiu os termos “Presente de Grego” e “Cavalo de Tróia”.

Em tempos modernos o cavalo virou um programa e a cidade o computador. Conhecidos como Cavalos de Tróia ou *Trojan Horses*, são programas aparentemente normais e inofensivos (jogos, *screensavers*, figuras, etc) que carregam dentro de si instruções que não são originalmente deles,

inseridas com outro propósito, como permitir a um *hacker* invadir o computador, capturar e divulgar senhas ou informações, destruir arquivos, etc.

São definidos pela RFC 2828 como sendo programas que aparentam ter uma função útil, mas possui alguma função maliciosa que burla os mecanismos de segurança. Não possui a capacidade de se auto-replicar. Normalmente, o usuário recebe o Cavalo de Tróia como presente (de grego). Ele pode ser oferecido de várias maneiras. Na maioria das vezes vem anexado a algum e-mail. Estes e-mails vêm acompanhados de belas mensagens e figuras.

No caso de recebimento desse tipo de arquivo, principalmente de origem desconhecida, a melhor política é nunca abrir um arquivo anexado. Programas piratas, adquiridos pela rede, poderão conter Cavalos de Tróia, por esse motivo deve-se evitar a instalação de programas de procedência desconhecida ou duvidosa.

O Cavalo de Tróia, na maioria das vezes, possibilita ao invasor o controle total da máquina. Ele poderá ter acesso e copiar todos os arquivos existentes, inclusive as senhas que forem digitadas, formatar o disco rígido, entre outras possibilidades. A maioria dos programas antivírus é capaz de detectar os Cavalos de Tróia e tratam de eliminá-los como se fossem vírus. Mesmo assim a proteção é parcial, uma vez que os Cavalos de Tróia recentes poderão passar despercebidos. O ideal é nunca abrir documentos anexados aos e-mails, a menos que tenha certeza de sua integridade. Existem ainda programas *spyware* que podem ser utilizados para barrar as conexões dos invasores com os Cavalos de Tróia que possam estar instalados no computador. Tais programas não eliminam os Cavalos de Tróia, mas bloqueiam seu funcionamento.

## Worm

*Worm* (verme em inglês) é um termo genérico para designar qualquer software que seja capaz de propagar a si próprio em redes de computadores, sem necessariamente modificar programas nas máquinas de destino. Um vírus comum também apresenta esta característica, mas diferentemente deste, os *worms* são capazes de executar a si próprios, sem intervenção humana.

É definido pela RFC 2828 como sendo um programa de computador que pode se executar independentemente e propagar-se pelos computadores de uma rede, podendo consumir os recursos disponíveis destrutivamente. Os *worms* geralmente não modificam outros programas, embora possam carregar outros códigos que o façam (como vírus, por exemplo). Alguns apenas se propagam de sistema para sistema, sem causar maiores danos, mas o fato de não precisar de intervenção humana para se propagar os torna altamente perigosos. Um exemplo de contaminação ocorreu em maio de 2000, quando o VBS/LoveLetter e suas variantes, causaram problemas em redes do mundo inteiro.

Normalmente os *worms* entram nos sistemas através da exploração de *bugs* (falhas no código) do sistema. Podem ser executados independentemente e trafegam de uma máquina para outra através das conexões de rede, podendo ter instruções alocadas em máquinas diferentes na mesma rede.

## Bactéria

Programa que gera cópias de si mesmo com intuito de sobrecarregar um sistema. As bactérias são programas que não causam explicitamente danos aos arquivos. Seu único propósito é a sua replicação. Essa reprodução é exponencial, podendo assumir toda a capacidade do processador, da memória ou do espaço em disco, impedindo o acesso de usuários autorizados a esses recursos.

## Bomba lógica

Ameaça programada, camuflada em programas, que é ativada quando certas condições são satisfeitas. As bombas lógicas permanecem inativas em softwares de uso comum por um longo período de tempo até que sejam ativadas. Quando isso ocorre, executam funções que alteram o comportamento do software instalado na máquina, podendo alterar ou destruir dados, travar o computador ou danificar o sistema.

As condições ativadoras de bombas lógicas são geralmente um dia da semana ou do ano, a presença ou ausência de certos arquivos ou um determinado usuário rodando a aplicação.

## Backdoor

*Backdoor* (porta dos fundos) é definido pela RFC 2828 como sendo um mecanismo que provê acesso a um sistema e seus recursos através de um procedimento diferente do usual. Normalmente é projetado pelos produtores de sistemas para ser utilizada na fase de testes do *software* ou *hardware*, normalmente não sendo de conhecimento público.

Não possui necessariamente intenção maliciosa. O seu objetivo seria, por exemplo, a possibilidade de o fabricante acessar um software remotamente sem utilizar um acesso normal. Alguns autores consideram o *backdoor* como uma falha na segurança de um sistema de computadores, deixada deliberadamente pelos fabricantes e, uma vez conhecida, o intruso pode utilizá-la para acessar outros computadores sem ser bloqueado pelos mecanismos de segurança. Segundo a mesma RFC, com essa utilização, passa a ser denominada *Trap Door*.

Existe uma grande lista de *backdoors* deixadas pelos fabricantes de *hardware* e *software*. Essas listas são de conhecimento dos invasores e, no processo de enumeração de um ataque, são usadas contra os possíveis alvos.

Existe também uma confusão entre o que é um *backdoor* e um cavalo de tróia, principalmente porque o estrago provocado por ambos é semelhante. Um cavalo de tróia é um programa que cria deliberadamente um *backdoor* na máquina. Programas que usam a Internet e que são de uso corriqueiro, como *browsers*, programas de correio eletrônico, ICQ ou IRC podem apresentar *backdoors*. Existem versões do ICQ que abrem um *backdoor* que permite derrubar a conexão do programa com o servidor, fazendo que ele pare de funcionar.

A melhor maneira para se prevenir dos *backdoors* é manter atualizadas as versões dos programas instalados no computador. É de responsabilidade do fabricante do *software* avisar aos usuários e prover uma nova versão corrigida do programa quando é descoberto um *backdoor* no mesmo. A dica é sempre visitar os sites dos fabricantes e verificar a existência de novas versões do software ou de pacotes que eliminem os backdoors. Os pacotes de correção são conhecidos como *patches* ou *service packs*. Os programas antivírus não são capazes de descobrir backdoors, somente a atualização dos programas é que podem eliminar em definitivo este problema. Programas de firewall pessoal, no entanto, podem ser úteis para amenizar (mas não eliminar) este tipo de problema.

### Outras Ameaças virtuais

Além dos programas maliciosos, uma rede de computadores pode ser ameaçada por outras fontes. Podemos destacar:

### Código Móvel

Essa ameaça à segurança de redes é descrita como sendo aplicativos que usam tecnologias legítimas, como Java e ActiveX, com intenções de roubar informações, instalar backdoors nos computadores atingidos, entre outros. Essas tecnologias normalmente apresentam alguma vulnerabilidade, que poderá ser descoberta pelos crackers e utilizadas para alguma atividade maliciosa. Os códigos podem ser disseminados como anexos de e-mail (comportam-se como vírus) ou simplesmente através da visita a páginas mal intencionadas (o código malicioso chega ao computador através da própria página Web).

As atividades em código móvel podem ser classificadas de acordo com os problemas que acarretam:

- **Modificação do sistema:** o código alterar o registro do sistema, alterar configurações de segurança do navegador de Internet, introduzir componentes ActiveX e Java adicionais para abrir portas de acesso, introduzir um vírus, alterar arquivos de dados e fazer com que um aplicativo se comporte de forma inesperada;
- **Invasão de privacidade:** o código móvel exporta informações do sistema do computador atingido para qualquer destino como envio de e-mail utilizando a conta do usuário, documentos, planilhas, senhas, etc;
- **Recusa de serviço:** o código tenta alocar toda a memória disponível ou criar várias de janelas na máquina para ocupá-la, evitando que outros programas funcionem adequadamente.

## Hoax

Além do aparecimento de novas ameaças diariamente, os usuários de redes de computadores sofrem a ação do boato (*hoax*), que causa prejuízos semelhantes aos dos vírus.

Um hoax é um alarme falso, um boato, enfim uma notícia sobre uma ameaça inexistente. Estas notícias são normalmente propagadas através de listas de e-mail, causando freqüentemente prejuízos devido a recomendações maliciosas e falsas para ajuste e atualização de programas e sistemas. Por exemplo, é comum um boato sugerir que o usuário apague um arquivo manualmente.

O hoax é escrito de forma a parecer um alerta autêntico, geralmente fazendo referências a fontes conhecidas e respeitadas. Não é raro que o alerta instrua os usuários a passarem a mensagem para outros usuários, criando uma corrente que espalha o boato com grande velocidade.

As mensagens de boatos geralmente utilizam uma linguagem técnica de difícil compreensão. Um hoax típico alerta para vírus não monitorados pelos programas de antivírus, havendo casos em que o alerta avisa que o vírus é capaz de destruir até mesmo o hardware. Na verdade, elas visam causar pânico, coletar dados de usuários ou mesmo aumentar o tráfego nas linhas de comunicação ou sites famosos, congestionando-os.

## Cookies

Os *cookies* são blocos de texto recebidos pelo usuário ao acessar um site. O cookie pode ficar armazenado em um computador e ser ativado a cada novo acesso. O principal propósito do cookie é identificar o usuário e personalizar a navegação. Por esse motivo, são considerados coletores de informações pessoais.

Um cookie pode ser usado pelos sites da Internet para rastrear a identificação on-line do usuário, o número de visitas que fez e para guardar a sua identificação e senha quando se pula de uma página para outra, e de forma que o visitante não precise reescrevê-la quando retornar ao site, entre outras aplicações.

Embora os cookies sejam geralmente utilizados para agilizar a resposta do site, o usuário nem sempre sabe, no instante em que recebe o cookie, qual a sua finalidade. O grande problema é que os cookies são utilizados por empresas que vasculham as preferências pessoais do usuário e espalham estas informações para outros sites de comércio eletrônico. Assim o usuário de internet sempre terá páginas de promoções ou publicidade, nos sites de comércio eletrônico, dos produtos de seu interesse. Na verdade, não se trata de um problema de segurança, mas alguns usuários podem considerar este tipo de atitude uma invasão de privacidade.

## Spam

Spams são as famosas mensagens eletrônicas não solicitadas. A palavra spam é uma alusão ao barulho que os vikings faziam ao bater na mesa

das tabernas para aborrecer o cliente. O spam não é oficialmente proibido, mas considera-se, na Internet, uma falta de ética.

Deve-se ter cuidado ao remeter dados pessoais (nome, e-mail, endereço, números de documentos e, principalmente, número de cartão de crédito) para qualquer site visitado. Deve-se ter sempre em mente que estas informações são guardadas em algum banco de dados do site e podem ser vendidas para outras empresas.

### **Programas para a Troca Instantânea de Mensagens**

São programas que possibilitam a troca de mensagens e endereços de sites da Internet. O programa utiliza a Internet para se conectar a um servidor específico. Vírus e worms também podem ser enviados em mensagens instantâneas, sem estarem sujeitos à análise dos antivírus, filtragem de conteúdo e outras medidas geralmente usadas na segurança de programas corporativos de correio eletrônico.

Normalmente, a troca de mensagens não passa pelo servidor. Toda vez que a conexão é feita, o servidor passa a conhecer o endereço na Internet (endereço IP) do computador. Os programas que utilizam a Internet para prestar algum serviço (neste caso troca de mensagens) ficam conectados permanentemente a um servidor e, como normalmente esses programas possuem backdoors, ficam sujeitos a ataques externos.

### **Programas de Distribuição de Arquivos**

Arquivos podem ser enviados (*upload*) ou recebidos (*download*) por um computador por vários meios diferentes. Os meios mais comuns são através do correio eletrônico, programas de mensagem instantânea e através dos browsers.

Quando um programa de distribuição de arquivos se conecta ao servidor, este envia uma lista dos arquivos que estão em uma pasta específica (já pré-configurada na instalação do programa) e esta lista fica disponível para os demais usuários do programa no mundo todo. Quando se busca por um tipo de arquivo específico (música, por exemplo), o programa pergunta ao servidor quais computadores possuem aquele arquivo. Quando se escolhe um dos arquivos, o programa que está rodando na máquina se conectará ao programa da outra máquina e baixará o arquivo escolhido para alguma pasta do computador (já pré-configurada e, normalmente, diferente da pasta anterior). Assim, o único trabalho do servidor é manter uma lista de quais computadores estão no ar (conectados à internet e rodando o programa de distribuição de arquivos) e a lista dos arquivos disponíveis. O trabalho de baixar os arquivos e enviar os arquivos é do computador.

Difícilmente arquivos de música, foto ou vídeo apresentarão problemas, a dificuldade maior será com os arquivos de programas que poderão conter vírus ou um cavalo de tróia embutido. Assim, quanto à segurança, vale a mesma regra dos casos anteriores, evite baixar da rede programas ou arquivos de desconhecidos, pois eles podem conter vírus ou cavalos de tróia.



Atualmente, os chamados vírus de computador são classificados em vários tipos (Figura 2), cada um com suas particularidades de funcionamento, formas de contágio e disseminação.

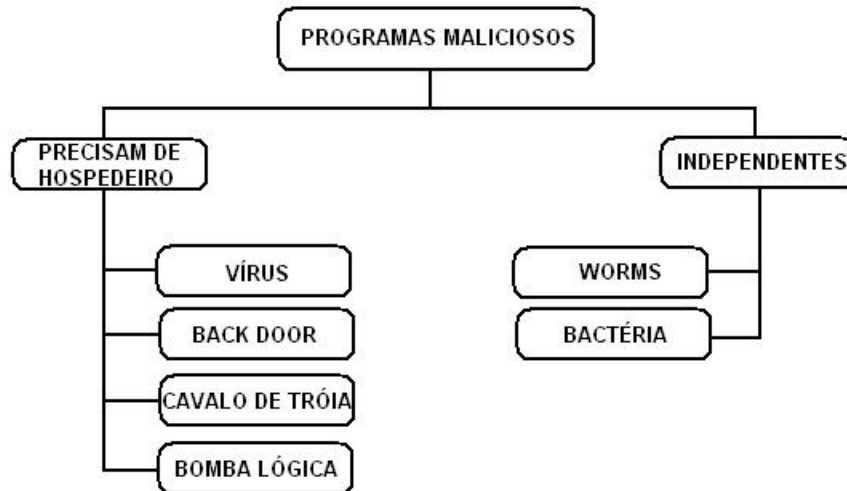


Figura 2 - Hierarquia dos principais tipos de programas maliciosos

## Questionário

1. Defina “informação”.
2. Quais são as categorias das ameaças para redes de computadores?
3. Um sistema de segurança da informação visa atender alguns objetivos gerais. Comente sobre um deles.
4. O que significa classificar informações?
5. Dentro dos critérios de classificação das informações, como podemos definir os níveis de confidencialidade?
6. O que é uma informação vital?
7. Enumere as possíveis ameaças para a segurança de um sistema de informação.
8. O que é a política de segurança da informação? Onde pode ser usada?
9. Quais as principais ameaças que devem ser tratadas pela política de segurança da informação?
10. Na classificação das informações devemos definir as funções e os responsáveis por cada etapa desta classificação. Quem é considerada custodiante?