FORMAÇÃO GESAC

KIT SOS WINDOWS

Comentários dos autores

Não tenha receio de aprender coisas novas, pois a vida é uma escola. Algumas ilustrações apresentadas são apenas arte representativa. Qualquer semelhança com a realidade é mera coincidência.

PRESIDÊNCIA DA REPÚBLICA

Luiz Inácio Lula da Silva
Presidente da República

MINISTÉRIO DAS COMUNICAÇÕES

José Artur Filardi Leite
Ministro de Estado das Comunicações

Secretaria Executiva

Fernando Rodrigues Lopes de Oliveira
Secretário Executivo

Secretaria de Telecomunicações

Roberto Pinto Martins
Secretário

Departamento de Serviços de Inclusão Digital

Heliomar Medeiros de Lima
Diretor

Elias Nagib David
Coordenador Geral do Projeto Formação Gesac

MINISTÉRIO DAS COMUNICAÇÕES
Secretaria de Telecomunicações
Departamento de Serviços de Inclusão Digital
Programa Gesac
Projeto Formação Gesac

KIT SOS GESAC

Ubuntu Gesac
&
KIT SOS para Windows

William da Silva Vianna
Ronaldo Amaral Santos
Organizadores

Brasília, DF
2010

1ª Edição – 2010

Realização
Ministério das Comunicações

Parceiros
Ministério da Educação
Conselho Nacional de Desenvolvimento Científico e Tecnológico
Rede Federal de Educação Profissional e Tecnológica

Organização
William da Silva Vianna
Ronaldo Amaral Santos

Conteudistas
Ewerton Lyrio Nascimento
Filipe Ribeiro Viana de Almeida
Wesley Folly Volotão de Souza

Arte da Capa
Pedro Henrique Parreiras de Meireles

Projeto Gráfico e Diagramação
Pedro Henrique Parreiras de Meireles

Revisão

Elias Nagib David
Janei Cristina Santos Resende
Maria da Graça Miranda da Silva

Sobre o Projeto
Esplanada dos Ministérios, Bloco L, Anexo I, sala 207
CEP: 70.047-900, Brasília – DF
Fone: (61) 2022-8686 / 8687
http://www.formacao.gesac.gov.br

Projeto Formação Gesac

KIT SOS Gesac – Ubuntu Gesac & KIT SOS para Windows. William da Silva Vianna e Ronaldo Amaral Santos. 1. ed. - Brasília: Ministério das Comunicações, 2010; [Campos dos Goytacazes]: Instituto Federal de Educação, Ciência e Tecnologia Fluminense.
35p. il. Color. , 27 cm

1. Inclusão Digital 2. Ubuntu 3. Windows. I. Brasil. Ministério das Comunicações. II. Instituto Federal de Educação, Ciência e Tecnologia Fluminense. III. Título.

CDU 37:004

Sumário

Lista de siglas e abreviação

- kbps – kilo bits por segundo;
- kilo – mil;
- WAN - Wide Area Network – rede de longa distância;
- WEB ou WWW - World Wide Web é um sistema hipertexto que funciona sobre a Internet. A visualização da informação e navegação é feita usando uma aplicação específica - o navegador (browser);
- MSN - Microsoft Service Network;
- ICQ - é um programa de comunicação instantânea pela Internet que pertence à companhia América Online;
- plugins - também conhecido por plug-in, add-in, add-on. É um programa de computador usado para adicionar funções a outros programas maiores, provendo alguma funcionalidade especial ou muito específica;

1. Introdução

O Projeto Formação Gesac está inserido no Programa de inclusão digital Gesac, desenvolvido pelo Ministério das Comunicações, que leva Internet em banda larga a mais de 11 mil telecentros em todo o País. Com duração inicial de um ano, o Projeto capacitará até abril de 2011, monitores e multiplicadores de 739 Pontos Gesac em Tecnologias de Informação e Comunicação (TICs).

O objetivo é transformar a realidade dessas comunidades ao apresentar seus integrantes a esse novo universo, oferecendo, além de Internet banda larga, conhecimento nas TICs, possibilitando assim a construção de alternativas reais de interação com autonomia nas redes digitais. A ação é realizada por meio de parceria com o Ministério da Educação, com a Rede Federal de Educação Profissional e Tecnológica e o Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq).

Ao acessar esses instrumentos, os atores podem conquistar a autonomia para encontrar seus próprios caminhos de desenvolvimento, coerentes com sua cultura e objetivos. Esse resultado esperado do projeto é fundamental para o exercício da cidadania, pois leva informação e possibilidade de interação com outras esferas da sociedade, possibilitando desenvolvimento social e econômico nas localidades alcançadas.

O Comitê Gestor da Internet (CGI) no Brasil desenvolveu alguns vídeos que serão utilizados neste kit. Para ilustrar a necessidade da navegação na Internet, veja o vídeo **cgi-navegar-legendado.wmv** localizado na pasta **videos** deste CD/DVD.

Os 739 Pontos Gesac inicialmente atendidos neste projeto, em sua grande maioria, possuem acesso a Internet com link de 512 kbps provido por link de satélite. A tecnologia que provê acesso a Internet por satélite possui algumas limitações, entre elas está a alta latência (tempo de reposta). Satélites são usados em muitas partes do mundo para suprir linhas terrestres indisponíveis ou caras. Apesar de ser possível obter a um custo razoável uma largura de banda significativa para um link baseado em satélite, a distância em relação à Terra causa uma grande latência. Para efeito de comparação, o tempo de ida e volta em link WAN (*Wide Area Network*) transoceânico ou que cruze um continente costuma ficar entre 100 e 200 ms (milissegundos), enquanto o link de um satélite pode facilmente demorar até dois segundo. Esse enorme tempo acarreta atrasos importantes, especialmente em protocolos de aplicativo como o navegador de Internet (Firefox, Opera, Chrome,

Internet Explorer, etc). A figura 1 ilustra o link de satélite permitindo que o PC (computador) em locais distantes possa fazer uso da Internet.

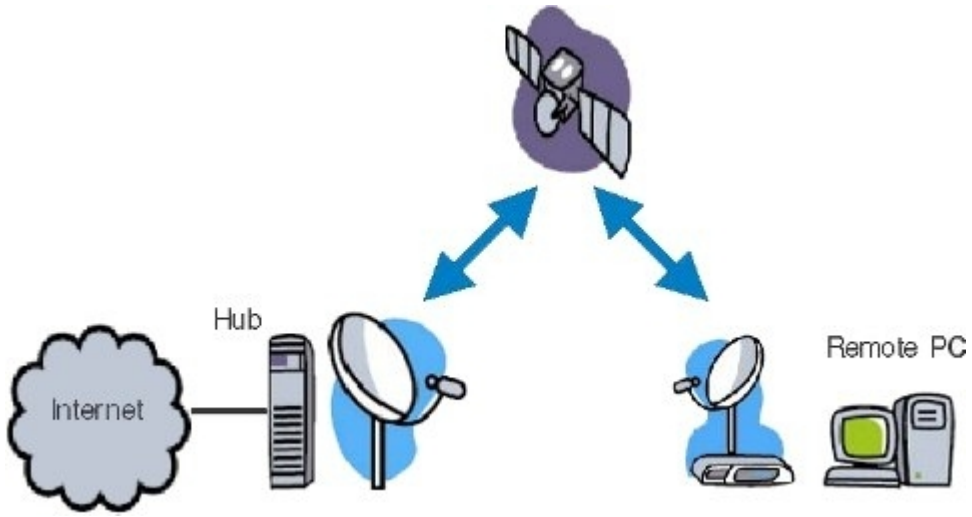

Ilustração 1: Link de Internet por satélite

Como se a latência não fosse o suficiente para degradar o desempenho, ainda podem existir máquinas na rede local do ponto Gesac realizando operações indevidas que aumentam o uso do link sem o usuário ter conhecimento. Estas operações indevidas e não solicitadas são geradas pelo sistema operacional e, em muitos casos, por *softwares* maliciosos como: *vírus*, *worm*, cavalos de tróia, *bot* de *spam*, *bot* de *phishing*, *keylog*, *screenlog*, etc.

Considerando este contexto, este documento tem como objetivo:

1 – Explanar sobre a segurança da informação e sua relação com o desempenho;

2 - Propor soluções práticas e recomendações para aumentar o desempenho do acesso a Internet dos clientes dos pontos Gesac;

2. *Copyleft* versus *Copyright*

Copyleft é uma forma de usar a legislação de proteção dos direitos autorais com o objetivo de retirar barreiras à utilização, difusão e modificação de uma obra criativa devido à aplicação clássica das normas de propriedade intelectual, exigindo que as mesmas liberdades sejam preservadas em versões modificadas. O *copyleft* difere assim do domínio público, que não apresenta tais exigências. "*Copyleft*" é um trocadilho com o termo "*copyright*" que, traduzido literalmente, significa "direitos

de copia" [1-2].

Uma obra, seja de *software* ou outros trabalhos livres, sob uma licença *Copyleft* requer que suas modificações, ou extensões do mesmo, sejam livres, passando adiante a liberdade de copiá-lo e modificá-lo novamente.

Uma das razões mais fortes para os autores e criadores aplicarem *copyleft* aos seus trabalhos é porque desse modo esperam criar as condições mais favoráveis para que mais pessoas se sintam livres para contribuir com melhoramentos e alterações a essa obra, num processo continuado. A figura 2 ilustra símbolos trocadilhos entre o *copyright* e *copyleft*.

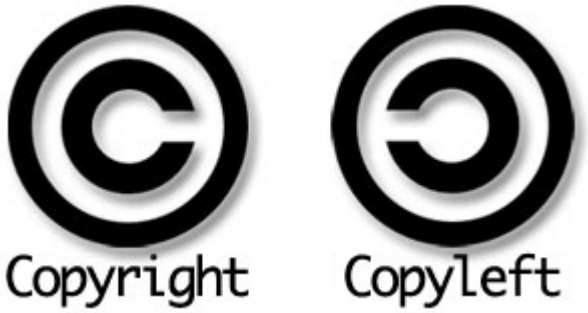

Ilustração 2: simbolo trocadilho copyrugh versus copyleft

Em termos práticos, o sistema operacional *Windows* ® é um produto da empresa *Microsoft* e para fazer uso deve-se pagar a licença. O valor da licença de uso da uma versão recente deste sistema operacional está em torno de R$ 400,00 isto sem contar os softwares adicionais como a suite de escritório com *Word*, *Excel* e outros. Parte do valor pago pela licença dos produtos da *Microsoft* é enviado para Estados Unidos. Isto significa menos recursos para aplicação nos projetos do governo como o Gesac. Usar o *Windows* com uma cópia não oficial (pirata) é ilegal e gera alguns problemas que serão citados.

Em contrapartida existe um sistema operacional livre para que todos possam usar e modificar sem paga nada por ele. O melhor é que este sistema é imune aos softwares maliciosos que afetam o *Windows* ®, este sistema é o Linux. O que quero dizer é:

1 – para não possuir *softwares* maliciosos realizando operações indevidas que degradam o desempenho de acesso a Internet do ponto Gesac, use uma distribuição Linux;

2 – para não ser ilegal com uso de *softwares* piratas, use distribuição Linux.

3. GNU/Linux e suas distribuições

Distribuição Linux é um sistema operacional com outros *softwares* de aplicação livres (GNU), formando um conjunto utilizável com navegador de Internet, gerenciador de arquivos, leitor de fotos, leitor de vídeos, etc. Existem várias distribuições (ou "distros") como: Ubuntu, Fedora, Mandriva, Debian, etc. O mascote do Linux é um pinguim chamado TUX (figura 3).

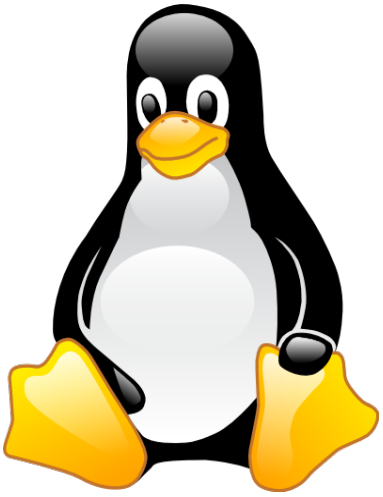

Ilustração 3: Mascote do Linux - adotado em muitas distribuições.

Como o Linux e a maior parte dos softwares incluídos em distribuições são livres, qualquer organização ou indivíduo suficientemente motivado podem criar e disponibilizar (comercialmente ou não) a sua própria distribuição. Isso faz com que hoje haja registro de mais de 1000 distribuições ativamente mantidas, embora menos de 40 delas sejam largamente conhecidas [4].

Acompanhado o kit S.O.S. do ponto Gesac foi implementada uma distribuição customizada a partir do Ubuntu que permitirá realizar todas as operações necessárias sem a necessidade de *download* de *softwares* adicionais. Esta distribuição pode ser instalada a partir do DVD que acompanha o kit.

Com o uso de uma distribuição Linux o microcomputador do ponto Gesac estará imume aos *softwares* maliciosos.

3.1. Motivos para usar o GNU/Linux

Alguns motivos para usar o GNU/Linux:

1 – Liberdade: você tem a liberdade de escolher, dentre muitas distribuições que tem um custo mínimo, ou mesmo completamente grátis, sem cobrança de licenças ou medo de violar patentes ou pirataria, porque o Linux está sob proteção da licença GNU GPL;

2 – Estabilidade: O Linux tem uma performance de alto nível, com pouca probabilidade de bloquear o sistema. Os problemas normalmente só ocorrem por problema de hardware e não do sistema operacional como ocorre com certo sistema operacional que conhecemos;

3 – Segurança: não existe qualquer outro sistema com o nível de segurança do Linux. As poucas vulnerabilidades não afetam o sistema Linux da mesma forma que afetam o *Windows* justamente porque a arquitetura dos sistemas e a concepção é totalmente diferente e quaisquer problemas são resolvidos muito rapidamente. Além disso, os programas maliciosos que são executandos no *Windows* não funcionam no Linux mesmo que você tente executá-los;

4 – Eficiência em Redes: uma das características mais comentadas do Linux é a eficiência quando se trata de redes. Linux, além de confiável, suporta quase todos tipos de protocolos existentes;

5 – Fácil Instalação: hoje as instalações de Linux das distribuições mais populares e avaliadas têm muitas facilidades para instalação com procedimentos que dão controle sobre o que você quer instalar no seu computador;

6 – Flexibilidade: seguindo a facilidade da instalação, no Linux você tem a flexibilidade de customizar no seu sistema somente com o que realmente te interessa e o que realmente você vai usar;

7 – Atualizações gratuitas: a grande quantidade de atualizações, pacotes e repositórios (*mirrors*) e sites especializados para que se sistema sempre esteja bem atualizado;

8 – *HardDisk*: sim, o Linux é um sistema que otimiza ao máximo o uso do seu *HardDisk*, não esquecendo de um *bit* sequer.

9 – Suporte Técnico: para os que dizem que a deficiência do Linux é o suporte, esquecem que há milhares senão milhões de técnicos, usuários ou curiosos dispostos a ajudar na solução de qualquer problema (via fóruns e listas);

10 – Escolha do Gigantes: a popularidade e o poder do Linux pode ser estimado pela conquista de grandes empresas como IBM, HP, Cisco, Shell e pela enorme quantidade de Governos que estão usando, migrando ou testando Linux em seus sistemas e plataformas.

4. *Softwares* maliciosos (*malware*)

O termo *malware* é proveniente do inglês malicious software *ou* software *malicioso*; são *softwares* destinados a se infiltrar em um sistema de computador alheio de forma ilícita, com o intuito de causar algum dano ou roubo de informações (confidenciais ou não). Exemplos: vírus de computador, *worms*, *trojan horses* (cavalos de tróia), *bot* de *spam*, *bot* de *phishing*, *spywares* são considerados *malware*. Estes *softwares* maliciosos em sua grande maioria usam o acesso a Internet para se propagar ou até mesmo enviar *emails* com conteúdo indevido como *spam* e outros.

Ilustração 4: Máquina com Windows *sujeita aos* malwares

Lembre-se, no ponto Gesac o link é limitado, logo qualquer uso a mais causa diferença no desempenho do acesso a Internet. São mais de 300.000 *softwares* maliciosos programados para afetar o *Windows*® e não o Linux, ou seja, para se proteger use uma distribuição Linux. Recomendamos usar a distribuição que acompanha o kit S.O.S. Se mesmo assim você ainda reluta em não usar o Linux, não deixe de assistir o vídeo **cgi-invasores-legendado.wmv** localizado na pasta **videos.**

Ilustração 5: Linux não precisa de antivírus

5. Segurança da informação

Na pasta **doc** do DVD do kit S.O.S. existe o arquivo **cartilha-seguranca-internet.pdf** (http://cartilha.cert.br/download/cartilha-seguranca-internet.pdf) que deve ser lido, pois contém dicas e conceitos sobre a segurança da informação. Se depois de tudo que você leu ainda não se convenceu a utilizar o Linux, o que posso fazer é apresentar dicas de como resolver alguns problemas relacionados com programas *malware* no *Windows*.

5.1. Como o Windows pode ser infectado com softwares malware

Existem várias formas do Windows ser infectado por *softwares* maliciosos. Estes *softwares* são desenvolvidos por pessoas que agem de forma a provocar o mal e tirar algum proveito no uso destes *softwares* maliciosos.

5.1.1. *Crackers* e *hackers*

Há quem diga que *cracker* e *hacker* são a mesma coisa, mas tecnicamente há uma diferença. *Hackers* são os que quebram senhas, códigos e sistemas de segurança por puro prazer em achar tais falhas. Preocupam-se em conhecer o funcionamento mais íntimo de um sistema computacional ou seja sem intenções de prejudicar outras ou invadir sistemas. Já o *Cracker* é o criminoso virtual, que extorque pessoas usando seus conhecimentos, usando as mais variadas estratégias. Há cerca de 20 anos, eram aficcionados em informática, conheciam muitas linguagens de programação e quase sempre jovens, que criavam seus vírus, para muitas vezes, saber o quanto eles poderiam se propagar. Hoje em dia é completamente diferente; são pessoas que atacam outras máquinas com

fins criminosos com um objetivo traçado: capturar senhas bancárias, números de conta e informações privilegiadas que lhes despertem a atenção. Porém, já se criou um verdadeiro mercado negro de vírus de computador, onde certos sites, principalmente russos, disponibilizam *downloads* de vírus e kits para qualquer um que puder pagar, virar um *Cracker*, o que é chamado de terceirização da "atividade". Neste contexto, o *Windows* é um sistema operacional muito sujeito a ser atacado e invadido, pois a grande maioria destes kits são desenvolvidos para atigir o *Windows* e não o Linux.

Ilustração 6: Cracker é uma pessoa que promove o mal na Internet

A situação tende a piorar, pois existem várias categorias de *softwares* e técnicas maliciosas.

5.1.2. Vírus de *Boot*

Um dos primeiros tipos de vírus conhecido, o vírus de *boot* infecta a partição de inicialização do sistema operacional. Assim, ele é ativado quando o disco rígido é ligado e o sistema operacional é carregado. Hoje em dia este tipo de vírus é raro.

5.1.3. *Time Bomb*

Os vírus do tipo "bomba-relógio" são programados para se ativarem em determinados momentos, definidos pelo seu criador. Uma vez infectando um determinado sistema, o vírus somente se tornará ativo e causará algum tipo de dano no dia ou momento previamente definido. Alguns vírus se tornaram famosos, como o "Sexta-Feira 13", "Michelangelo", "Eros" e o "1º de Abril (Conficker)".

5.1.4. Minhocas, *worm* ou vermes

Um *Worm* (verme, em português), em computação, é um programa auto-replicante, semelhante

a um vírus. Enquanto um vírus infecta um programa e necessita deste programa hospedeiro para se propagar, o *Worm* é um programa completo e não precisa de outro para se propagar.

Um *worm* pode ser projetado para tomar ações maliciosas após infestar um sistema *Windows*, além de se auto-replicar, pode deletar arquivos em um sistema ou enviar documentos por *email*.

A partir disso, o *worm* pode tornar o computador infectado vulnerável a outros ataques e provocar danos apenas com o tráfego de rede gerado pela sua reprodução – o *Mydoom*, por exemplo, causou uma lentidão generalizada na Internet no pico de seu ataque.

Como o interesse de fazer um vírus é ele se espalhar da forma mais abrangente possível, os seus criadores por vezes, deixaram de lado o desejo de danificar o sistema dos usuários infectados e passaram a programar seus vírus de forma que apenas se repliquem, sem o objetivo de causar graves danos ao sistema. Desta forma, os seus autores visam a tornar suas criações mais conhecidas na Internet. Este tipo de vírus passou a ser chamada de verme ou *worm*. Eles estão mais aperfeiçoados, já há uma versão que ao atacar a máquina hospedeira, não só se replica, mas também se propaga pela Internet, pelos e-*mails* que estão registrados no cliente de *e-mail*, infectando as máquinas que abrirem aquele *e-mail*, reiniciando o ciclo.

Ilustração 7: worm de computador

Estes tipos especiais de vírus, os *worm*, infectam as máquinas conectadas na Internet sem a necessidade do usuário estar acessando alguma página. Estes *worms* exploram vulnerabilidades nos serviços de rede dos sistemas não atualizados como o que ocorre nos *Windows* piratas e não atualizados. Em outras palavras, se você usa *Windows* pirata, faz acesso a Internet, não possui um

bom antivírus e filtro de pacotes (*firewall*), provavelmente seu microcomputador foi infectado sem o seu conhecimento. Para piorar a situação, estes *softwares* maliciosos costumam fazer uso frequente do acesso a Internet deixando a sua conexão ainda mais lenta. Quer a solução ? Use Linux.

5.1.5. *Backdoors*

Existem alguns vírus que abrem portas (virtuais) e permitem o acesso ao microcomputador infectado a partir da Internet. Os *worms Sobig* e *Mydoom* instalaram *backdoors* (brechas) nos computadores, tornando-os abertos a ataques via Internet. Estes computadores "zombies" são utilizados para enviar *emails* de propaganda (*spams*), para atacar endereços de sites da Internet, para envia *emails* de *phishing* (técnica especial de engenharia social). Acredita-se que *spammers* (pessoas que enviam *spams*) pagam para a criação destes *worms*, e criadores de *worms* já foram apanhados vendendo listas de endereços IP de máquinas infectadas.

Agora imagine a situação, o *link* de 512 kbps do ponto Gesac compartilhado com vários microcomputadores e todos infectados com algum tipo de *worm* que envia *email* sem o usuário saber. Grande parte do *link* de 512 kbps será usado para enviar estes *emails* de propaganda e *phishing*. Isto ocorre e provavelmente se você usa *Windows* pirata conectado a Internet seu microcomputador está enviando *emails* de *spam* e *phishing*. Falo isto por experiência.

O último "*worm*" colocado na rede foi no Orkut, chamado "Vírus do Orkut", dissipado na madrugada do dia 25/09/2010 pelo programador Rodrigo Lacerda. O Google, porém, resolveu o problema.

5.1.6. *Trojans* ou cavalos de Tróia e o *Phishing*

Certos vírus trazem em seu bojo um código a parte, que permite a um estranho acessar o micro infectado ou coletar dados e enviá-los pela Internet para um desconhecido, sem notificar o usuário. Estes códigos são denominados de *Trojans* ou cavalos de Tróia.

Inicialmente, os cavalos de Tróia permitiam que o micro infectado pudesse receber comandos externos, sem o conhecimento do usuário. Desta forma o invasor poderia ler, copiar, apagar e alterar dados do sistema. Atualmente os cavalos de Tróia agora procuram roubar dados confidenciais do usuário, como senhas bancárias.

Os vírus eram no passado, os maiores responsáveis pela instalação dos cavalos de Tróia, como parte de sua ação, pois eles não têm a capacidade de se replicar. Atualmente, os cavalos de Tróia não mais chegam exclusivamente transportados por vírus, agora são instalados quando o usuário

baixa um arquivo da Internet e o executa. Prática eficaz devido a enorme quantidade de *e-mails* fraudulentos que chegam nas caixas postais dos usuários (*phishing*). Tais *e-mails* contém um endereço na Web para a vítima baixar o cavalo de Tróia, ao invés do arquivo que a mensagem diz ser. Esta prática se denomina *phishing*, expressão derivada do verbo to *fish*, "pescar" em inglês. Atualmente, a maioria dos cavalos de Tróia visam a sites bancários, "pescando" a senha digitada pelos usuários dos micros infectados. Estes *softwares* maliciosos são criados para funcionar no *Windows*. Se você usa Linux, então não se preocupe, caso use *Windows* mesmo legalizado você corre um sério risco de ter os seus dados pessoais “furtados” ou “pescados” por alguém mal intencionado.

Ilustração 8: phishing são técnicas para "furtar" dados pessoais dos usuários

Também os cavalos de tróia podem ser usados para levar o usuário para sites falsos, onde sem seu conhecimento, serão baixados trojans para fins criminosos, como aconteceu com os *links* do google, pois uma falha de segurança poderia levar um usuário para uma página falsa. Por este motivo o serviço esteve fora do ar por algumas horas para corrigir esse *bug*, pois caso contrário as pessoas que não distinguissem o site original do falsificado seriam afetadas.

Outra conseqüência é o computador tornar-se um zumbi e, sem que o usuário perceba, executar ações como enviar *Spam*, se auto-enviar para infectar outros computadores e fazer ataques a servidores (normalmente um DDoS, um acrônimo em inglês para *Distributed Denial of Service* – em português, ataque distribuído de negação de serviço). Ainda que apenas um micro de uma rede esteja infectado, este pode consumir quase toda a banda de conexão com a Internet realizando essas

ações mesmo que o computador esteja sem utilização, apenas ligado. O objetivo, muitas vezes é criar uma grande rede de computadores zumbis que, juntos, possam realizar um grande ataque a algum servidor que o autor do vírus deseja "derrubar" ou causar grande lentidão.

Ilustração 9: softwares maliciosos podem transformar o microcomputador em zumbi

5.1.7. *Hijackers*

Hijackers são programas ou *scripts* que "sequestram" navegadores de Internet. Quando isso ocorre, o *hijacker* altera a página inicial do browser e impede o usuário de mudá-la, exibe propagandas em *pop-ups* ou janelas novas, instala barras de ferramentas no navegador e podem impedir acesso a determinados sites (como sites de *software* antivírus, por exemplo). Isto ocorre especialmente com o navegador *Internet Explorer* da *Microsoft* não atualizado.

5.1.8. Vírus no Orkut

Atualmente as rede sociais são muito utilizadas para a construção de comunidades virtuais e troca de informações.

O sistema de rede social mais conhecido é o Orkut. Em torno de 2006 e 2007 houve muitas ocorrências de vírus no Orkut que é capaz de enviar *scraps* (recados) automaticamente para todos os contatos da vítima na rede social, além de roubar senhas e contas bancárias de um micro infectado através da captura de teclas e cliques. Apesar de que aqueles que receberem o recado precisam clicar em um *link* para se infectar, a relação de confiança existente entre os amigos aumenta muito a possibilidade de o usuário clicar sem desconfiar de que o *link* leva para um *worm*.

Ao clicar no *link*, um arquivo bem pequeno é baixado para o computador do usuário. Ele se encarrega de baixar e instalar o restante das partes da praga, que enviará a mensagem para todos os contatos do Orkut. Além de simplesmente se espalhar usando a rede do Orkut, o vírus também rouba senhas de banco, em outras palavras, é um clássico *Banker*.

5.1.9. Vírus de Macro

Os vírus de macro (ou macro vírus) vinculam suas macros a modelos de documentos gabaritos e a outros arquivos de modo que, quando um aplicativo carrega o arquivo e executa as instruções nele contidas, as primeiras instruções executadas serão as do vírus.

Vírus de macro são parecidos com outros vírus em vários aspectos: são códigos escritos para que, sob certas condições, este código se "reproduz", fazendo uma cópia dele mesmo. Como outros vírus, eles podem ser escritos para causar danos, apresentar uma mensagem ou fazer qualquer coisa que um programa possa fazer.

Resumindo, um vírus de macro infecta os arquivos do *Microsoft Office* (.doc - word, .xls - excel, .ppt - power point, .mdb – access.).

Uma alternativa para reduzir a possibilidade do vírus de macro atacar a sua máquina é utilizar a suite de escritório BROffice (http://www.broffice.org/). Este conjunto de softwares provê os mesmos recursos que o *Microsoft Office*. Esta suite de escritório possui versão para *Windows* e Linux.

5.1.10. *Spyware*

Spyware consiste num programa automático de computador, que recolhe informações sobre o usuário, sobre os seus costumes na Internet e transmite essa informação a uma entidade externa na Internet, sem o seu conhecimento nem o seu consentimento.

Diferem dos cavalos de Tróia por não terem como objetivo que o sistema do usuário seja dominado, seja manipulado, por uma entidade externa, por um *cracker*.

Os *spywares* podem ser desenvolvidos por firmas comerciais, que desejam monitorar o hábito dos usuários para avaliar seus costumes e vender este dados pela internet. Desta forma, estas firmas costumam produzir inúmeras variantes de seus programas-espiões, aperfeiçoando-o, dificultando em muito a sua remoção.

Por outro lado, muitos vírus transportam *spywares*, que visam roubar certos **dados confidenciais** dos usuários. Roubam dados bancários, montam e enviam registros das atividades do

usuário, roubam determinados arquivos ou outros documentos pessoais.

Com frequência, os *spywares* costumavam vir legalmente embutidos em algum programa que fosse *shareware* ou *freeware*. Sua remoção era por vezes, feita quando da compra do *software* ou de uma versão mais completa e paga.

Traduzindo ao pé da letra, *Spyware* significa "aplicativo ou programa espião".

Eventualmente anexos de *e-mails* ou mensagens vindas de mensageiros como o MSN e o ICQ, também podem conter *spywares*. Firmas comerciais exploram maldosamente a curiosidade dos usuários e desenvolvem novas formas de transmissão e de instalação de *spywares*.

Recentemente uma grande parte dos *spywares* são assimilados pelo navegador, como *plug-ins*. O usuário deve ser cuidadoso ao instalar os diversos *plug-ins* disponíveis na Internet.

Ilustração 10: spyware são programas espiões

5.1.11. *Adwares*

Costuma-se incluir os ***adwares*** no estudo dos spywares, pois assemelham-se na sua forma de infecção e na sua forma de desinstalação. Seriam como se fossem um sub-grupo dos *spywares*.

Os *adwares* são conhecidos por trazerem para a tela do usuário algum tipo de **propaganda**. Como geralmente são **firmas comerciais** que os desenvolvem, é comum os *adwares* virem embutidos em diversos programas de livre *download* e uso (*freeware*), com a autorização de seus autores.

Softwares como *Kazaa* e *Emule* são programas de compartilhamento de arquivos, sendo um exemplo do casamento de um *software* gratuito com *adwares*, pois estes lhe proporcionam uma fonte de renda.

Inicialmente os *adwares* procuravam exibir propagandas em janelas, chamados de *banners*, pequenas janelas de propagandas, embutidas em *softwares* de terceiros. Caso o usuário gostasse deste *software*, poderia adquirir uma versão mais avançada, paga, livre destas propagandas.

Posteriormente os *adwares* passaram a monitorar a atividade do usuário na Internet, podendo desta forma mostrar propagandas personalizadas, além de enviar dados sobre hábitos do usuário a certos sites, tendo então funções de *spyware* e *adware*, de forma simultânea.

Mais adiante certos *adwares* passaram a exibir janela do tipo *pop-up*, pequena janela de propaganda solta pela tela, em vez de *banners*.

Um pouco mais a frente os *adwares* passaram a se instalar no navegador do usuário, acrescentando certas funcionalidades duvidosas, principalmente no ***Internet Explorer***. Avanços (ou *upgrades*) no *Internet Explorer,* passaram a exigir o consentimento do usuário para a sua instalação.

Porém com o passar do tempo, os *adwares* sofisticaram-se, incluindo propagandas persistentes, com inúmeras variantes, onde a sua desinstalação passou a ser um tarefa bastante penosa ou mesmo impossível, sem uma ajuda externa. A insistência no aparecimento das propagandas e sua difícil desinstalação, levaram os usuários a classificá-los como pragas ou *spywares* e não mais como simples *adwares*.

Certos *adwares* passaram a ser instalados no *Internet Explorer*, quando o usuário navegava em sites maliciosos como os pornográficos, pedofilia, *cracker* e de pirataria.

Os *adwares* se sofisticaram, tornaram-se pragas. Produzem alterações no registro do *Windows* e depois somem ou se escondem para garantir que as alterações não sejam desfeitas, exigindo então não mais a ação de um antivírus ou de um simples *anti-spyware*, mas sim de um programa específico de conserto do registro.

Por vezes os *adwares* exibem propagandas pornográficas, falsas propagandas de infecção do sistema por vírus, falsa propaganda de venda de produtos e passaram também a causar instabilidade no sistema, principalmente no navegador.

Pode ser observado que estes *adwares* geram tráfego de Internet não desejado ocupando o *link* de internet do ponto Gesac com propagandas inúteis.

5.1.12. Novos meios

Muito se fala de prevenção contra vírus de computador em computadores pessoais, o famoso

PC, mas pouca gente sabe que com a evolução, aparelhos que tem acesso à Internet, como muitos tipos de telefones celulares, *handhelds*, VOIP, etc podem estar atacando e prejudicando a performance dos aparelhos em questão. Por enquanto são casos isolados, mas o temor entre especialistas em segurança digital é que com a propagação de uma imensa quantidade de aparelhos com acesso à Internet, *hackers* e *crackers* irão se interessar cada vez mais por atacar esses novos meios de acesso a WEB. Também se viu recentemente que vírus podem chegar em produtos eletrônicos defeituosos, como aconteceu recentemente com iPODS da Apple, que trazia um "inofensivo" vírus (qualquer antivírus o elimina, antes que ele elimine alguns arquivos contidos no iPOD), nessas situações, avisar o fabricante é essencial para evitar danos muito grandes.

5.1.13. Vírus que usam o autorun.inf do Windows

Atualmente, existem várias técnicas de infecção do sistema operacional *Windows* muitas delas usando a Internet como meio de propagação, mas já existem vírus especialmente escritos para infectar unidades de armazenamento como *pendrive*, cartões de memória e celulares.

Os vírus de *pendrive* se aproveitam do mecanismo de execução automática (*AutoRun*/*AutoPlay*) presente em sistemas operacionais da *Microsoft*. Este mecanismo utiliza um arquivo chamado autorun.inf que é lido no momento em que uma mídia removível é montada pelo sistema operacional. Neste momento o malware armazenado no *pendrive* é executado pela chamada existente no arquivo autorun.inf do próprio *pendrive*, mas quem faz isto é o sistema operacional *Windows*. Agora que a máquina está infectada, qualquer unidade armazenamento como *pendrives*, celulares e cartões de memória conectados serão automaticamente infectados também e o ciclo prossegue.

Ilustração 11: unidades de armazenamento como o pendrive pode ser infectado no Windows

5.1.14. SPLOG

Existe também o falso blog, ou splog, que no contexto de propaganda serve para alavancar as vendas de algum produto. Raramente faz algum mal, porém pode conter links que podem ser perigosos.

6. Comentários, dicas e recomendações para evitar os programas maliciosos

Em função deste grande número de softwares maliciosos existentes e diversas técnicas de invasão, a prevenção deve ser um trabalho constante, pois estes *malwares* geram uso indevido de recursos como: banda de acesso a Internet, processamento e memória da máquina. Desta forma, caso o seu acesso a Internet possua recursos limitados como banda é muito importante não deixar que estes *malwares* infectem as máquinas.

Ilustração 12: o Windows está sujeito a ser infectado por softwares malware.

Dica 1 - Uma boa sugestão é utilizar uma distribuição GNU/Linux como sistema operacional ao invés do *Windows*. Os programas maliciosos que prejudicam a máquina e o seu acesso a Internet não funcionam no Linux, logo este sistema operacional está imune.

Ilustração 13: Linux é imune aos softwares malware

Além disso, certos navegadores de Internet (*browsers*) implementam tecnologias que permitem a execução de programas maliciosos na máquina simplesmente ao acessar certos sites da Internet. Principalmente o *Windows* pode ser infectado simplesmente ao acessar sites com conteúdo do tipo: ponográficos, *cracker*, pirataria e outros.

Dica 2 – não faça acesso a sites com conteúdo pornográfico, *cracker* ou de pirataria, pois este sites podem conter programas *malware* que infectarão a sua máquina.

Ilustração 14: sites cracker, pornográficos e de pirataria geralmente contém malware.

Dica 3 – mantenha seu sistema operacional atualizado, pois algumas vulnerabilidades serão corrigidas com esta atualização e consequentemente certos programas *malware* não poderão invadir o seu microcomputador

Dica 4 – se você usa *Windows* desabilite o autorun.inf ou crie uma pasta chamada autorun.inf na raiz (fora de qualquer diretório) das unidades de armazenamento. As instruções estão no arquivo "desabilitar_autorun.odt" localizado no diretório doc do Kit SOS.

Dica 5 – utilize ***softwares* de proteção** como antivírus, *antispyware* e *firewall*.

Veja o vídeo **cgi-defesa-legendado.wmv** localizado no diretório **videos**, nele existem várias recomendações úteis.

6.1. Softwares de proteção

Estes *softwares* de proteção aplicam-se principalmente para o *Windows*, pois o Linux é imune a estas mazelas existentes nas veias digitais do planeta. A instalação dos *softwares* de proteção no microcomputador sempre causa "lentidão" no funcionamento do sistema operacional.

6.1.1. Detectando, prevenindo e combatendo os vírus

Os antivírus são *softwares* desenvolvidos por empresas de segurança, com o objetivo de detectar e eliminar vírus encontrados no computador. Os antivírus possuem uma base de dados contendo as assinaturas dos vírus de que podem eliminar. Desta forma, somente após a atualização de seu banco de dados, os vírus recém-descobertos podem ser detectados.

Hoje em dia os Antivírus podem ter "Proteção em Tempo Real" que detecta os códigos maliciosos desde que você inicie o computador até que o desligue. Esta tecnologia torna mais fácil de o utilizador ficar protegido. Entretanto, nada pode garantir a segurança de um computador usando *Windows*. Entretanto, você pode melhorar a segurança dele e diminuir a probabilidade de ser infectado, mas caso faça opção de usar uma distribuição GNU/Linux você não será infectado e não terá parte da banda de acesso a Internet roubada pelos programas maliciosos.

Remover um vírus de um sistema sem a ajuda das ferramentas necessárias é uma tarefa complicada até mesmo para um profissional. Alguns vírus e outros programas maliciosos (incluindo o *spyware*) estão programados para re-infectar o computador mesmo depois de detectados e removidos. Alguns vírus são capazes de desabilitar o antivírus e, até mesmo "enganá-lo" impossibilitando sua localização.

Atualizar o computador periodicamente é uma ação preventiva contra os vírus. Além dessa

opção, existem algumas empresas que fornecem ferramentas não gratuitas, que ajudam na detecção, prevenção e remoção permanente dos vírus. Se você usa uma cópia não legal do *Windows* ® recomendo migrar para uma distribuição Linux para evitar a infecção de sua máquina.

Se você usa Linux, não se preocupe com os vírus, mas caso use *Windows* deve-se instalar um bom antivírus e mantê-lo periodicamente atualizado. Existem vários antivírus gratuitos para *Windows*, entre eles estão o AVG, Panda, Avira, ClamWin e Avast.

Recomendamos o uso do Avira para identificar e combater os vírus. No diretório **doc,** existe o arquivo "" com as instruções de instalação. No diretório ***softwares*** existe uma versão do **Avira**, mas você pode fazer o *download* por meio da url:

http://dl1.avgate.net/package/wks_avira/win32/ptbr/pecl/avira_antivir_personal_ptbr.exe

Ilustração 15: O antivírus não garante proteção total no Windows

O **Avira** versão grátis é considerado um dos melhores antivírus. No diretório **doc** existe o arquivo **avc_report25.pdf** que contém um comparativo entre diversos antivírus existentes no mercado. Entretanto, mesmo sendo um bom antivírus, recomendamos executar o programa **ComboFix** para remover alguns programas maliciosos que o **Avira** não é capaz de remover. Este software pode ser encontrado no diretório ***softwares*** de kit S.O.S. ou é possível fazer download por meio da url:

http://download.bleepingcomputer.com/protected/dd22d4a60702ee4a38e111a47ec957e9/4cb4691b/ComboFix.exe

6.1.2. *Firewall* Pessoal

Os *firewall's* pessoais são programas desenvolvidos por empresas de *software* com o objetivo de evitar que o computador pessoal seja vítima de ataques maliciosos (ou os "*Blended Threats*" -

códigos maliciosos que se espalham pela Internet sem que o utilizador do computador que infecta/está a infectar saiba) e os ataques de programas espiões. Falando da sua função relacionada com os vírus, este programa vigia as "portas" (as portas TCP/IP são os meios de comunicação, associado a um determinado aplicativo, que deixam trafegar a informação do computador para a rede), de maneira a impedir que os vírus ataquem num determinado protocolo. Assim, se instalar e configurar um *firewall* pessoal em seu computador, o usuário estará protegido contra ataques de muitos tipos de *malware*, evitando que eles tenham acesso ao seu computador e a seus arquivos. O *firewall* também protege de ataques de *cracker's* (pessoas que pretendem invadir o seu sistema), porque ao vigiar o tráfego das portas dos protocolos, conseguem detectar tentativas de intrusões no seu sistema por um computador remoto.

Existem vários *firewalls* gratuitos que podem ser utilizados em sua máquina, mas lembre-se cada novo software de proteção instalado reduz o desempenho da máquina deixando-a mais lenta. O ideal é não utilizar estes programas, mas isto só é possível caso você use Linux.

Existem várias ferramentas de proteção listadas no arquivo "**tabela_de_ferramentas.odt**" do diretório **doc**, procure na seção ***Free Firewalls***. Recomendamos o uso do **Comodo Firewall** ou o **ZoneAlarm.**

É importante lembrar que estes softwares de proteção degradam o desempenho do microcomputador. Alguns dizem que é um mal necessário, mas diria que não é bem assim, basta usar uma distribuição GNU/Linux como sistema operacional.

Ilustração 16: Um firewall ajuda a proteção da máquina Windows, mas não impede o acesso a ponografia

6.1.3. Antiespiões (*anti-spywares*)

Um *anti-spyware* é um *software* indicado para eliminar os espiões (*spywares*), ou, quando pouco, detectá-los e, se possível, inativá-los, enviando-os a quarentena. Tal como os antivírus, necessitam ter sua base de dados atualizada constantemente.

Os *anti-spywares* costumam vigiar certas entradas no registro do *Windows* para detectar tentativas de infecção, mas eventualmente não conseguem identificar o que está tentando alterar o registro - podendo ser mesmo um *spyware* ou de fato um vírus.

Existem várias ferramentas *antispam* listadas no arquivo "**tabela_de_ferramentas.odt**" do diretório **doc**. Recomendamos o uso do ***Spybot*** que pode ser obtido gratuitamente na Internet ou pode-se utilizar a versão existente no diretório ***softwares*** do kit S.O.S. (**spybotsd162.exe**).

Ilustração 17: Cuidado com os malwares spywares

Pode ser observado que toda ferramenta de proteção necessita de atualização periódica. Se você possui um *link* de Internet limitado recomendamos o uso do Linux para evitar o uso excessivo do *link* para as atualizações que são necessárias nestas ferramentas para *Windows*.

6.1.4. Engenharia social

Embora se tenha dado um grande avanço no sentido de se tornar sistemas computacionais cada vez mais seguros, isso pode de nada valer frente a engenharia social, que consistem em técnicas para convencer o usuário a entregar dados como senhas bancárias, número do cartão de crédito, dados financeiros em geral. Estes atos geralmente ocorrem numa conversa informal e despreocupada em uma sala de bate papo, como por exemplo o *messenger* (MSN). Também pode ocorrer de um usuário receber um *email* que o convença a fazer o *download* e execute um programa *malware* no microcomputador ou a fornecer seus dados pessoais (*phishing*).

Por isso, **NUNCA** se deve fornecer qualquer tipo de senha de qualquer espécie, pois a porta de entrada para a perda de informações, espionagem, furto de dinheiro em uma conta bancária e detalhes pessoais podem cair nas mãos de pessoas desconhecidas, não sabendo o destino dessas informações. Atualmente, são obtidos dados dessa espécie e dados mais específicos também (tipo senhas de redes de computadores de empresas, localização de *backdoor*, etc.).

A Engenharia Social, não possui o menor vínculo com o *hacking*, são técnicas totalmente diferentes uma da outra. "O Engenheiro Social prevê a suspeita e a resistência, e ele está sempre preparado para transformar a desconfiança em confiança. Um bom Engenheiro planeja o seu ataque como um jogo de xadrez. "

Com tantos *crackers* obtendo senhas ao redor do mundo, é inevitável a criação de vínculos entre eles, que passam a usar dados roubados como moeda de troca. Hoje os dados de acesso dos usuários são comercializados por verdadeiras quadrilhas *online*. É comum encontrar mensagens do tipo

"Tenho a senha de 100 contas bancárias do banco X, quem dá mais por elas?" em diversos fóruns especializados. Um verdadeiro mercado negro se forma em salas de bate-papo clandestinas, onde essas negociatas são realizadas entre um verdadeiro oceano de códigos, siglas e abreviaturas - um prato cheio para os cyberladrões. De posse de dados de acesso a contas bancárias, os criminosos virtuais conseguem realizar fraudes e transferências ilegais de dinheiro com grande facilidade. Há um golpe também conhecido onde os ladrões realizam pagamentos de contas de terceiros *online* utilizando contas correntes roubadas. Mas as contas bancárias não são os únicos alvos: contas de acesso em comunidades virtuais também são utilizadas em fraudes e para plantar mensagens com links para *download* de vírus e *trojans*.

Não existe ferramenta contra a engenharia social, a melhor prevenção é ficar atento e desconfiar de mensagens de pessoas desconhecidas. Procure também orientar seus amigos, parentes e principalmente filhos, pois existem criminosos no mundo e a Internet, de forma virtual, coloca-os dentro de sua casa.

Veja o vídeo **cgi-spam-legendado.wmv** localizado na pasta **videos**.

6.2. Pedofilia

A pedofilia (também chamada de *paedophilia* erotica ou pedosexualidade) é a perversão sexual, na qual a atração sexual de um indivíduo adulto ou adolescente está dirigida primariamente para crianças pré-púberes (ou seja, antes da idade em que a criança entra na puberdade) ou para crianças em puberdade precoce. A palavra pedofilia vem do grego *παιδοφιλια* (*paidophilia*) onde *παις* (pais, "criança") e *φιλια* (philia, "amizade", "afinidade", "amor", "afeição", "atração", "atração ou afinidade patológica" ou "tendência patológica", segundo o Dicionário Aurélio).

O Estatuto da Criança e do Adolescente - ECA

(Lei nº 8.069/90)

estabelece que:

Art. 241. Fotografar ou publicar cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:

Pena - detenção de um a quatro anos, e multa.

Ilustração 18: Fique atento as crianças e adolecentes

6.2.1. Como denunciar a pedofilia

- Por telefone: Disque 100 - Disque Denúncia Nacional de Abuso e Exploração Sexual contra Crianças e Adolescentes. Discagem gratuita em todo o território nacional.
- Polícia: Em caso de flagrante, a polícia deve ser acionada imediatamente.
- Conselhos tutelares: Os conselhos tutelares foram criados para zelar pelo cumprimento dos direitos das crianças e dos adolescentes. A eles cabem receber a notificação e analisar a procedência de cada caso, visitando as famílias. Se for confirmado o fato, o Conselho deve levar a situação ao conhecimento do Ministério Público.
- Varas da Infância e Juventude: Em municípios onde não há conselhos tutelares, as Varas da Infância e Juventude podem receber as denúncias.
- Delegacias de Proteção à Criança e ao Adolescente. Delegacias da Mulher também podem receber queixas.
- Pela Internet
    - Centro de Defesa da Criança e do Adolescente http://www.cedeca.org.br
    - Campanha Nacional de Combate à Pedofilia na Internet www.censura.com.br
    - Departamento da Polícia Federal: aceita denúncia clicando em "fale conosco" em http://www.dpf.gov.br/
    - Ministério da Justiça: Aceita denúncia pelo e-mail crime.internet@dpf.gov.br ou em "fale conosco" no site http://www.mj.gov.br
    - Rede Nacional de Direitos Humanos: http://www.direitoshumanos.gov.br/

- Agência de Notícias dos Direitos da Infância: http://www.andi.org.br/denuncie/
- Kids denúncia: http://www.portalkids.org.br Fonte: Childhood (Instituto WCF-Brasil)

Ilustração 19: Ajude a combater a pedofilia. Denuncie.

7. Comentários finais

Manter o sistema operacional é muito importante para evitar *softwares* maliciosos. Não *softwares* piratas, pois devido a falta de atualização, o microcomputador pode ser comprometido. Além disso, é crime.

A grande maioria dos *softwares malware* fazem algum uso do acesso a Internet, deixando a abertura de páginas do seu navegador mais lenta. Estes *softwares* são preparados para funcionar no *Windows* e não no Linux. Logo, o uso do sistema operacional Linux torna o seu acesso seguro e otimiza o uso da bande de acesso a Internet.

Caso use o *Windows*, procure sempre utilizar e atualizar os programas de proteção como antivírus, *antispyware* e *firewalls*. Entretanto, estes programas de proteção deixam o sistema operacional mais lento.

Junto com o kit S.O.S. existe uma distribuição Linux baseada no Ubuntu. Esta distribuição foi customizada para atender as necessidades dos usuários do ponto Gesac sem precisar a instalação de novos *softwares*. Entretanto, caso necessário, outros *softwares* podem ser instalados gratuitamente com o uso a “Central de Programas do Ubuntu”.

8. Bibliografia

CAMPOS, Augusto. O que é uma distribuição Linux. BR-Linux. Florianópolis, mar. 2006. Disponível em <http://br- linux.org/faq-distribuicao/>. Acesso em: 04 out.2010.

CENTRO de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Cartilha de Segurança para Internet**. Versão 3.1. São Paulo: Comitê Gestor da Internet no Brasil, 2006.

COMITÊ Gestor da Internet no Brasil. Produção/criação do Studio Hector Gómes Alisio. **Videos**: 1. Navegar é preciso; 2. Os invasores; 3. Spam; 4. A Defesa. [S.l.]: NIC.br, 2007. 1 DVD. Vídeo com legendas em português (640 x 480), son., color. Disponível em: <http://www.antispam.br/videos/ >. Acesso em: 04 out. 2010.

COPYLEFT. In: Wikipédia, a enciclopédia livre. [S.l.], 2010. Disponível em: <http://pt.wikipedia.org/wiki/Copyleft > Acesso em: 04 out. 2010.

FORMULÁRIO de denúncia de pedofilia. In: O Estatuto da Criança e do Adolescente - ECA **(**Lei nº 8.069/90). Disponível em: <http://www.prgo.mpf.gov.br/denuncia/denun1.htm >.

STALLMAN, Richard. **The first software-sharing community**. In: The GNU Project. [S.l.]: Free Software Foundation, Inc., 2010. Disponível em: <http://www.gnu.org/gnu/thegnuproject.html>. Acesso em: 04 out. 2010.

VÍRUS de computador. Disponível em: <http://pt.wikipedia.org/wiki/V% C3%ADrus de computador > >. Acesso em: 05 out. 2010.

FORMAÇÃO

GESAC