A Segurança dos dados na *World Wide Web* SEDVC*: Expert System to Detect Computer Viruses*

Álisson de Moraes Zimermann, Fábio Zimermann, Patricia Mariotto Mozzaquatro

Curso de Ciência da Computação – Universidade de Cruz Alta (UNICRUZ)
Rua Andrade Neves, 308. Centro, Cep: 98025810 – Cruz Alta – RS – Brasil

alissonzima@gmail.com, fabiozima@gmail.com,
patriciamozzaquatro@gmail.com

Abstract. *This article presents a brief explanation of the onset and evolution of viruses in the world wide web, but also the development of an Expert System for Detecting Computer Viruses (SDVC). The system was developed with the software Expert Experience, and the base Data based on studies. The proposed system was validated by academics of the courses of Computer Science and Veterinary Medicine, University of Cruz Alta (UNICRUZ), with the objective of informing the user types virus on your computer through the information provided.*

Resumo. *Este artigo apresenta uma breve explanação sobre o início e a evolução dos vírus na rede mundial de computadores, como também o desenvolvimento de um Sistema Especialista para Detectar Vírus de Computador (SDVC). O sistema foi desenvolvido com o software Expert Sinta, sendo a base de dados fundamentada em estudos realizados. O sistema proposto foi validado por acadêmicos dos cursos da Ciência da Computação e Medicina Veterinária da Universidade de Cruz Alta (UNICRUZ), com o objetivo de informar ao usuário os tipos de vírus existentes no computador, mediante as informações fornecidas.*

1. Introdução

Atualmente, devido a evolução tecnológica, circulam na rede mundial de computadores grandes quantidades de informações. As tecnologias estão se multiplicando muito rápido, entretanto algumas destas são desenvolvidas não para auxiliar na melhoria, mas sim muitas vezes são ameaçadoras e poderosas o suficiente para a destruição. Estas são conhecidas como vírus de computador. A relativa facilidade de propagação que temos hoje através da *www* (*World Wide Web*), com a utilização de *e-mail*, redes de compartilhamento de arquivos, juntamente com as falhas de segurança dos produtos e sistemas operacionais, contribuem em muito para esta propagação atingir escalas mundiais. Conforme o autor Cidale,

> Os vírus são pequenos segmentos de códigos, programados com o intuito de provocar algum sintoma indesejável ao usuário do computador infectado. Possuem a característica de se agregarem ao código de outros programas e, ao serem executados inocentemente pelo usuário, trazem em seu bojo, o código alterado para causar intromissões indevidas no processamento normal, causando ou não, danos de leves a irreparáveis. (Cidale, 1990)

Diante disso, expõe-se a seguinte questão: Como detectar quando uma praga cibernética aloja-se em seu computador, ou melhor, rouba e destrói suas informações? É neste contexto de variáveis que se procura apresentar um estudo sobre a evolução dos vírus de computador no cenário atual, como também, desenvolver um Sistema Especialista para diagnosticá-los em um computador (SEDVC), possibilitando assim, ao usuário um maior entendimento sobre o tema de forma que o mesmo possa detectar e diagnosticar situações de risco, ou seja, verificando se seu microcomputador foi afetado por algum vírus.

2. A segurança das informações na Rede Mundial de Computadores

Atualmente, a WWW é um serviço de redes de computadores conectados por diferentes meios. Ela conecta várias redes comerciais, governamentais, de universidades, dentre outras. A internet oferece a seus usuários a capacidade de transpor quaisquer tipos de barreiras, sejam elas de natureza geográfica, econômica ou cultural, criando um mundo virtual globalizado. Ela foi logo incorporada pelas pessoas e empresas por oferecer uma forma nova e ágil de comunicação. Com a expansão da Rede Mundial de Computadores, está cada vez mais difícil manter em segurança as informações referentes a empresas ou pessoas. O descuido nessa área pode causar prejuízos significativos, e muitas vezes irreversíveis. A Segurança da Informação refere-se à proteção requerida para proteger as informações de empresas ou de pessoas, ou seja, o conceito se aplica tanto as informações corporativas quanto às pessoais (ABNT, 2001).

A segurança de uma determinada informação pode ser afetada por fatores comportamentais e de uso de quem se utiliza dela, pelo ambiente ou infra-estrutura que a cerca ou por pessoas mal intencionadas que têm o objetivo de furtar, destruir ou modificar tal informação (Longo, 2007).

O maior desafio da indústria mundial de software de segurança é prover soluções no espaço de tempo mais curto possível, a partir da descoberta de determinada ameaça ou problema.

Em pouco tempo, os computadores se tornaram uma parte intrínseca e essencial da vida cotidiana. O resultado é um enorme potencial de lucros financeiros para os criadores de programas mal-intencionados. Com a ascensão de técnicas sofisticadas, está ficando cada vez mais difícil para a base de usuários em geral identificar ou evitar as infecções por programas mal-intencionados.

De acordo com Scambtay (2001), estão mencionadas algumas das falhas mais comumente identificadas, independentemente do porte ou da área de atuação da companhia, bem como da complexidade de sua infra-estrutura tecnológica e dos sistemas que utiliza, são elas: Senhas fracas, Sistemas de *backups* falhos, Portas abertas, Brechas de instalações, Falhas em sistemas de logs, Falha na atualização de camadas de segurança e Sistemas operacionais.

Conforme estudos (Segurança da Informação, 2010), enquanto o volume de fraudes via internet *banking* caiu de 300 milhões de reais em 2007 para 130 milhões de reais este ano, o mercado negro de comercialização de informações confidenciais faturou mais de 276 milhões de dólares, o número de *malwares* triplicou, as redes

sociais como *Orkut, Facebook e Myspace* foram vítimas de ataques de engenharia social.

Em 2008, os *crackers* provaram que os sistemas de segurança (*firewall*, antivírus, anti-spam, IDS) utilizados atualmente passam uma falsa sensação de segurança. Quanto mais segurança implementamos, novas técnicas de ataques e fraudes surgem.

De acordo com (Veloso, 2003), as quatro principais ameaças à segurança de dados são: Falsificação de Links, Mobilidade ameaçada, Clonagem de cartões de crédito com chip e senha, Ataques em banco de dados e Sistemas de gestão.

Anteriormente os criminosos virtuais contentavam-se em invadir um site e deixar ali a sua marca. Hoje, eles são silenciosos e muito mais perigosos. Um computador pode estar mandando milhares de e-mails para o mundo todo sem que seu usuário saiba, ou ainda: a pessoa pode ter um programa espião instalado em sua máquina, capaz de copiar todas as suas senhas.

Embora a Rede Mundial de Computadores tenha e tem dado bons frutos até então, logo surgiram as pragas virtuais. Exemplos delas são vírus, *spams, worms* e *spywares*. Os vírus compreendem programas que têm a capacidade de, facilmente, multiplicar-se e invadir outros programas e sistemas, podendo ser de natureza destrutiva.

Vírus é um programa malicioso desenvolvido por programadores que, tal como um vírus biológico, infecta o sistema, faz cópias de si mesmo e tenta se espalhar para outros computadores, utilizando-se de diversos meios. A maioria das contaminações ocorre pela ação do usuário executando o anexo de um e-mail. A segunda causa de contaminação é por sistema operacional desatualizado, sem a aplicação de corretivos que bloqueiam chamadas maliciosas nas portas do micro. Ainda existem alguns tipos de vírus que permanecem ocultos, mas entram em execução em horas especificas.

A Internet tornou a segurança dos sistemas computacionais mais difícil. Qualquer pessoa pode atacar o computador ou sistema e, uma vez esse esteja infectado, os demais conectados em rede podem ser, automaticamente, infectados também. As pragas da Internet exploram as vulnerabilidades dos sistemas, procuram atacar alvos específicos a fim de roubar informações, corromper dados e danificar sistemas.

Assim como houve a evolução da chamada Segurança 1.0, que restringia ações de usuários, para o padrão 2.0, que mostrava ameaças não apenas no mainframe e passava a contar com a Internet e seus perigos, agora monitorar o perfil dos profissionais e as aplicações de TI também se tornou imprescindível (segurança 3.0) (Zwicky et.al., 2001).

2.1 Evolução dos programas maliciosos no cenário atual

Em 1983, *Len Eidelmen* demonstrou no Seminário sobre Segurança Computacional, um programa auto-replicante em um sistema VAX11/750. Este conseguia instalar-se em vários locais do sistema. Um ano depois, na *7th Annual Information Security Conference*, o termo vírus de computador foi definido como um programa que infecta outros programas, modificando-os para que seja possível instalar cópias de si mesmo. O primeiro vírus para PC nasceu em 1986 e chamava-se *Brain*, era da classe dos Vírus de *Boot*, ou seja, danificava o setor de inicialização do disco rígido. A sua forma de

propagação era através de uma disquete contaminado. Apesar do *Brain* ser considerado o primeiro vírus conhecido, o título de primeiro código malicioso pertence ao *Elk Cloner*, escrito por *Rich Skrenta*. A seguir será apresentada a evolução das pragas virtuais no cenário atual, conforme os estudos de Silva (2005):

1983 – O pesquisador *Fred Cohen* entre suas pesquisas, chamou os programas de códigos nocivos como "Vírus de Computador";

1987 – Surge o primeiro Vírus de Computador escrito por dois irmãos: *Basit e Amjad* que foi batizado como *'Brain*', apesar de ser conhecido também como: *Lahore, Brain-a, Pakistani, Pakistani Brain*, e *UIU*. O Vírus *Brain* documentado como 'Vírus de Boot', infectava o setor de incialização do disco rígido, e sua propagação era através de um disquete que ocupava 3k, quando o boot ocorria, ele se transferia para o endereço da memória "0000:7C00h" da Bios que automaticamente o executava. Em 1988 – Surge o primeiro Antivírus criado por *Denny Yanuar Ramdhani* com o objetivo de imunizar sistema contra o vírus *Brain*;

1989 – Aparece o *Dark Avenger*, o qual vem contaminando rapidamente os computadores, mas o estrago é bem lento, permitindo que o vírus passe despercebido. A IBM fornece o primeiro antivírus comercial;

1992 – *Michelangelo*, o primeiro vírus a aparecer na mídia. É programado para sobre gravar partes das unidades de disco rígido criando pastas e arquivos com conteúdos falsos em 6 de março, dia do nascimento do artista da Renascença;

1994 – Criação do vírus *Pathogen*;

1995 – Vírus *Concept*, o primeiro vírus de macro. Escrito em linguagem *Word Basic da Microsoft,* pode ser executado em qualquer plataforma com *Word* - PC ou *Macintosh*. O *Concept* se espalha facilmente, pois se replicam através do setor de *boot*, espalhando por todos os arquivos executáveis;

1999 – O vírus *Chernobyl*, deleta o acesso a unidade de disco e não deixa o usuário ter acesso ao sistema;

2000 – Criação do vírus *LoveLetter*;

2001 – A "moda" são os códigos nocivos do tipo *Worm* (proliferam-se por páginas da Internet e principalmente por *e-mail*). Nome de um deles é o *VBSWorms Generator*, que foi desenvolvido por um programador argentino de apenas 18 anos;

2007 – 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*. A Figura 1 apresenta a evolução da quantidade de Vírus ao longo dos anos.

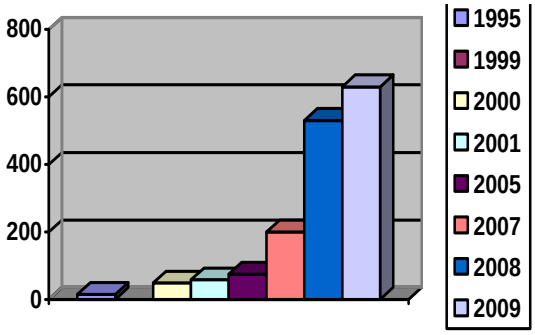

Figura 1. Evolução dos Vírus.

Conforme observa-se na Figura 1, os vírus evoluíram em grande proporção desde o ano de 1995 até os dias atuais.

Deve-se ressaltar que além dos vírus citados nesta seção, foram estudados trinta e quatro tipos de pragas virtuais *(Virus 1253, Virus Halloween, Virus 4096, Virus Helper A E B, Alien.H, Alliance, Jerusalém, Louvado. A, Aragorn, Karin,, Badboy, Kompu, Bad. A, Tamago. A, Boom, Why Windows, Cascade, Concept, Clock:De, Dark-End, Datacrime, Father Christmas, Trojan, Backdoors, Rootkits, Worms, Tentacle, Michelangelo, Klez, Leap-A, Melissa, Mydoom, Mimda, Sasser, Tamago) p*ara a implementação do sistema proposto.

3. Descrição do Experimento

O experimento consistiu no desenvolvimento e aplicação de um Sistema Especialista que detecta vírus de computador. O software foi desenvolvido com a ferramenta *Expert Sinta*, criada pelo grupo SINTA (Sistemas Inteligentes Aplicados). É uma ferramenta computacional que utiliza técnicas de Inteligência Artificial para a geração automática de sistemas especialistas (Expert Sinta, 1991). A ferramenta utiliza um modelo de representação do conhecimento baseado em regras de produção e probabilidade. As regras foram criados após estudo aprofundado sobre Vírus de Computador (Tipos, Nomes e Conseqüências). Para compor a base de conhecimento, foram realizados os seguintes procedimentos: criação das variáveis, regras, perguntas e objetivos. As figuras 2 e 3 apresentam as regras de produção.

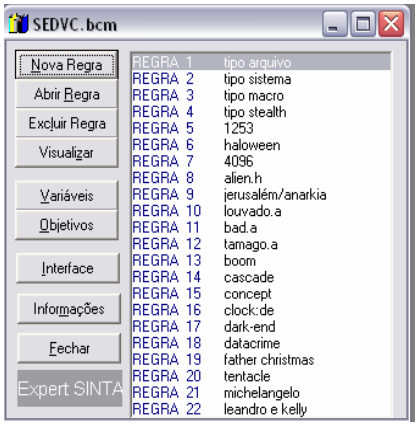

Figura 2. Regra de produção

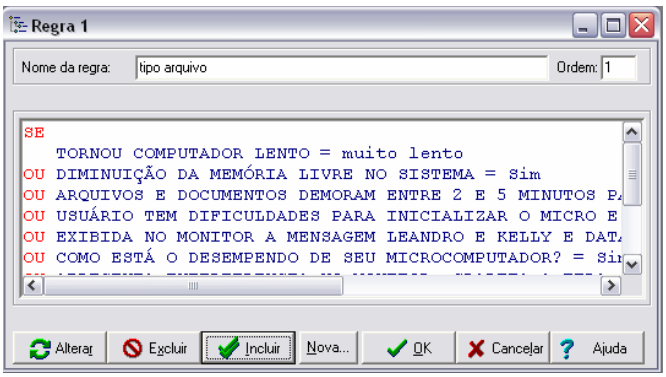

Figura 3. Especificação da regra

Prosseguindo com o processo são geradas as telas com perguntas dirigidas ao usuário, baseadas nas regras e variáveis já criadas. Concluído o sistema, inicia-se a consulta (Figura 4). Os resultados são apresentados em uma janela com todos os valores encontrados, com os respectivos graus de confiança expostos na figura 5.

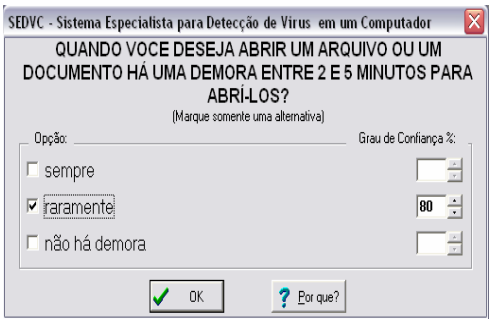

Figura 4. Consulta

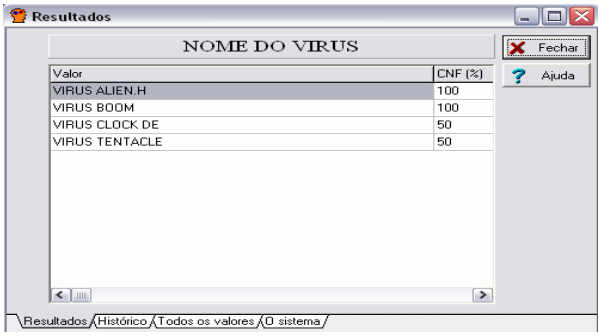

Figura 5. Resultado da Consulta

4. Resultados e discussão

O sistema foi aplicado tendo como base uma amostra de 65 usuários, acadêmicos dos cursos da Ciência da Computação e Medicina Veterinária. De um universo de 283 alunos, foi escolhida aleatoriamente uma amostra de 23% [1]totalizando 65 alunos, os quais integraram a pesquisa. A validação ocorreu nos laboratórios de informática do Curso de Ciência da Computação da Universidade de Cruz Alta.

O processo foi desenvolvido nas seguintes etapas: Interação com o sistema; Utilização do sistema pelos acadêmicos; aplicação de um instrumento de avaliação do sistema; análise qualitativa dos resultados; apresentação dos resultados; e, elaboração das conclusões. A partir dos dados coletados, foram feitas demonstrações gráficas, apresentando os resultados obtidos. A Figura 6, apresenta os vírus que mais predominaram na pesquisa.

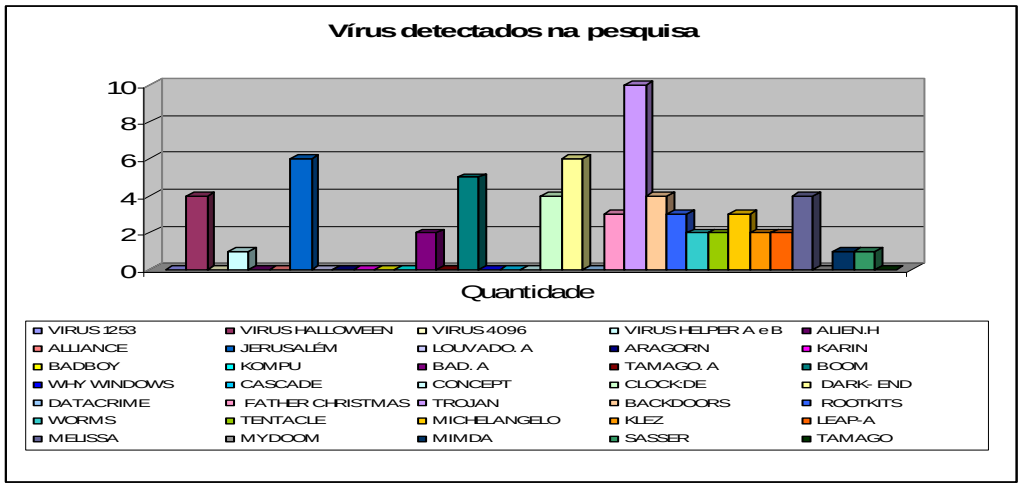

Figura 6. Vírus que mais predominaram na pesquisa

[1] Critérios IBGE

Em relação aos Vírus detectados na amostra, observou-se que os de maior predominância foram: *Trojan, Jerusalém, e Dark-End* seguido dos vírus *Boom, Halloween, Clock, Backdoors e Melissa*. Em menor proporção, aparecem os vírus *Father Christmas, Michelangelo, Rootkits*, seguido dos virus *Helper* A e B, *Tentacle, Mimda* e *Sasser*.

Como atividade final, foi solicitado aos alunos que utilizaram o sistema, responderem a um questionário eletrônico, com a finalidade de identificar a percepção dos mesmos em relação a interação com o sistema.

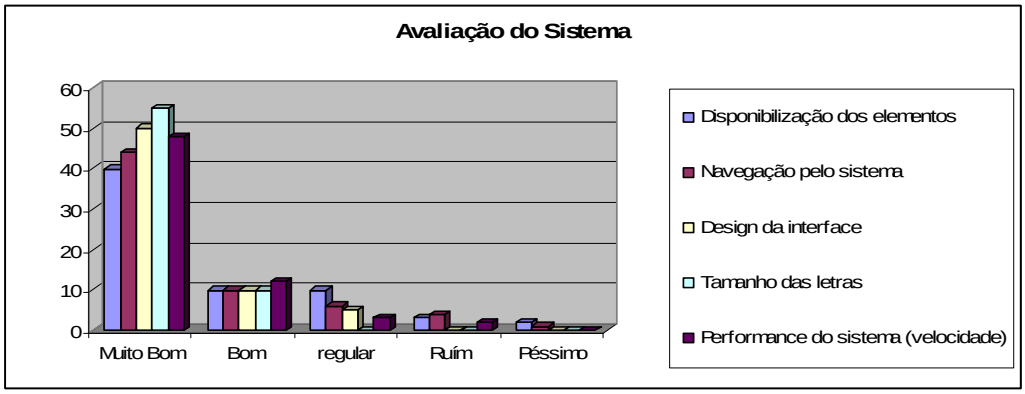

Figura 7. Avaliação do Sistema

Em relação a interface com o usuário, estrutura e funcionalidades constatou-se que a maioria classificou–os como muito bons, onde os elementos integrantes encontram-se bem distribuídos apresentando um *feedback* coerente ao usuário. Quanto ao aspecto referente a navegação pelo sistema os integrantes consideraram muito boa. Também o Sistema avaliado, quanto a performance (velocidade) foi considerado muito bom pelos entrevistados (Figura 7). Para melhor embasar a pesquisa foram feitos questionamentos aos acadêmicos. Ratificando o que foi exposto anteriormente, o sistema proposto, atingiu os objetivos. Segundo as suas opiniões: “O Sistema foi muito bem organizado, disponibilizando um fácil acesso e navegação relacionado as perguntas integrantes.” (Aluno - Ciência da Computação); “A forma de utilização do sistema foi bastante satisfatória. Atingiu meus objetivos, pois através dele pude verificar se meu microcomputador foi afetado por alguns vírus” (Aluno - Medicina Veterinária).

5. Considerações Finais

Quanto mais uma empresa depende de redes de computadores, maiores devem ser as preocupações com segurança. E isso significa preocupar-se com a integridade de dados, com o tempo de manutenção devido a problemas de segurança, e com muitos outros aspectos. O número de incidentes de segurança está em pleno crescimento, não apenas porque as redes de computadores são vulneráveis, mas também porque quanto mais poderosos tornam-se os aparatos de segurança – leia-se, *firewalls, software*, etc –, maior se torna o interesse de *hackers* em invadir.

O sistema especialista desenvolvido, serviu como colaborador, mostrando-se válido e viável, pois através do mesmo foi possível detectar e informar aos usuários os principais vírus existentes na atualidade. Este trabalho corrobora com outras pesquisas às quais também concluíram que detectar vírus de computador é uma tarefa complexa, e

requer estudos aprofundados afim de ser oferecido ao usuário respostas conclusivas relacionadas a infecção de pragas virtuais.

Falhas em políticas de segurança expõem não apenas informações e dados de uma empresa, mas também causam danos sérios à imagem da companhia. E é o zelo pela imagem que, muitas vezes, impulsiona a implantação de uma política de segurança, com a utilização de *firewalls*, mecanismos de autenticação, algoritmos de encriptação, e outras medidas de prevenção. Mas será que apenas investindo em tecnologia a empresa estará 100% segura? No contexto atual, mais do que nunca, segurança é vital para o sucesso de um negócio.

Devido a informática avançar muito rápido e diariamente, circulando milhares de vírus na rede, o sistema proposto necessita de atualizações periódicas para por fim, apresentar resultados definitivos quanto aos tipos de vírus existentes.

Para futura atualização do SEDVC pretende-se implementar o mesmo utilizando a linguagem de programação PHP com banco de dados *MySQL* e servidor *Linux.*

Referências

ABNT, NBR ISO/IEC 17799 (2001), Tecnologia da Informação – Código de Prática para a gestão da informação de informações. Rio de Janeiro: ABNT, 2001.

Cidale, Ricardo A. (1990). “Vírus digital. Uma abordagem para prevenção e manutenção de seus sistemas de informação”. São Paulo: Makron McGraw-Hill.

“Expert *SINTA*”. (1991). Laboratório de Inteligência Artificial/LIA-UFC. Página consultada em 03 de abril de 2010, <www.lia.ufc.br>.

Longo, Gustavo Dobkowski. (2007). Artigo Científico: Segurança da Informação. Universidade Estadual Paulista, Bacharelado em Sistemas de informação.

Scambtay, J.; Mc Clure S.; Kurtz, G. Hackers Expostos: Segredos e Soluções para a Segurança de Redes. (2001). 2.ed. São Paulo: Makron Books.

Segurança da Informação (2010). Certified Professional pelo Dialogo TI – INTEL, 2010

Silva, João Pedro da. (2005). “Evolução das Pragas Virtuais”. Faculdade Senac de Ciências Exatas e Tecnologia. São Paulo.

Veloso, Caio Júlio Martins. (2003). Segurança da Informação: Uma abordagem sistêmica e a prática nas empresas brasileiras de telecomunicações. Dissertação de Mestrado.

Zwicky, E.; Cooper, S.; Chapman, D. (2001). Construindo *Firewalls* para a internet. 2.ed, Rio de Janeiro: Ed. Campus.