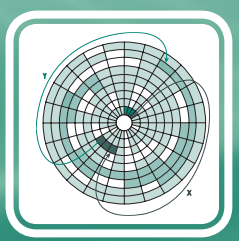
e-Tec Brasil
Escola Técnica Aberta do Brasil

Softwares de Segurança da Informação

Jorge Procópio da Costa Novo

Curso Técnico em Manutenção e Suporte em Informática



CETAM
Centro de Educação Tecnológica do Amazonas

UNIVERSIDADE FEDERAL
DE SANTA CATARINA

Ministério da Educação

e-Tec Brasil
Escola Técnica Aberta do Brasil

Softwares de Segurança da Informação

Jorge Procópio da Costa Novo

CETAM
Centro de Educação Tecnológica do Amazonas

Manaus - AM
2010

Presidência da República Federativa do Brasil

Ministério da Educação

Secretaria de Educação a Distância

Este Caderno foi elaborado em parceria entre o Centro de Educação Tecnológica do Amazonas e a Universidade Federal de Santa Catarina para o Sistema Escola Técnica Aberta do Brasil – e-Tec Brasil.

Equipe de Elaboração
Centro de Educação Tecnológica do Amazonas – CETAM

Coordenação Institucional
Adriana Lisboa Rosa/CETAM
Laura Vicuña Velasquez/CETAM

Coordenação do Curso
Helder Câmara Viana/CETAM

Professor-autor
Jorge Procópio da Costa Novo/CETAM

Comissão de Acompanhamento e Validação
Universidade Federal de Santa Catarina – UFSC

Coordenação Institucional
Araci Hack Catapan/UFSC

Coordenação de Projeto
Silvia Modesto Nassar/UFSC

Coordenação de Design Instrucional
Beatriz Helena Dal Molin/UNIOESTE e UFSC

Coordenação de Design Gráfico
Carlos Antonio Ramirez Righi/UFSC

Design Instrucional
Renato Cislaghi/UFSC

Web Design
Beatriz Wilges/UFSC
Gustavo Pereira Mateus/UFSC

Diagramação
André Rodrigues da Silva/UFSC
Andréia Takeuchi/UFSC
Bruno César Borges Soares de Ávila/UFSC
Guilherme Ataide Costa/UFSC

Revisão
Júlio César Ramos/UFSC

Projeto Gráfico
e-Tec/MEC

Catalogação na fonte pela DECTI da Biblioteca Universitária da Universidade Federal de Santa Catarina

N945s Novo, Jorge Procópio da Costa
Softwares de segurança da informação / Jorge Procópio da Costa Novo. - Manaus : Centro de Educação Tecnológica do Amazonas, 2010.
116 p. : il., tabs.

Inclui bibliografia
Curso Técnico em Manutenção e Suporte em Informática, desenvolvido pelo Sistema Escola Técnica Aberta do Brasil, e-Tec Brasil.

ISBN: 978-85-63576-20-0
1. Software – Medidas de segurança. 2. Software - Proteção. I. Título.

CDU: 681.31.004.4

Apresentação e-Tec Brasil

Prezado estudante,

Bem-vindo ao e-Tec Brasil!

Você faz parte de uma rede nacional pública de ensino, a Escola Técnica Aberta do Brasil, instituída pelo Decreto nº 6.301, de 12 de dezembro 2007, com o objetivo de democratizar o acesso ao ensino técnico público, na modalidade a distância. O programa é resultado de uma parceria entre o Ministério da Educação, por meio das Secretarias de Educação a Distancia (SEED) e de Educação Profissional e Tecnológica (SETEC), as universidades e escolas técnicas estaduais e federais.

A educação a distância no nosso país, de dimensões continentais e grande diversidade regional e cultural, longe de distanciar, aproxima as pessoas ao garantir acesso à educação de qualidade, e promover o fortalecimento da formação de jovens moradores de regiões distantes, geograficamente ou economicamente, dos grandes centros.

O e-Tec Brasil leva os cursos técnicos a locais distantes das instituições de ensino e para a periferia das grandes cidades, incentivando os jovens a concluir o ensino médio. Os cursos são ofertados pelas instituições públicas de ensino e o atendimento ao estudante é realizado em escolas-polo integrantes das redes públicas municipais e estaduais.

O Ministério da Educação, as instituições públicas de ensino técnico, seus servidores técnicos e professores acreditam que uma educação profissional qualificada – integradora do ensino médio e educação técnica, – é capaz de promover o cidadão com capacidades para produzir, mas também com autonomia diante das diferentes dimensões da realidade: cultural, social, familiar, esportiva, política e ética.

Nós acreditamos em você!

Desejamos sucesso na sua formação profissional!

Ministério da Educação
Janeiro de 2010

Nosso contato
etecbrasil@mec.gov.br

Indicação de ícones

Os ícones são elementos gráficos utilizados para ampliar as formas de linguagem e facilitar a organização e a leitura hipertextual.

Atenção: indica pontos de maior relevância no texto.

Saiba mais: oferece novas informações que enriquecem o assunto ou "curiosidades" e notícias recentes relacionadas ao tema estudado.

Glossário: indica a definição de um termo, palavra ou expressão utilizada no texto.

Mídias integradas: sempre que se desejar que os estudantes desenvolvam atividades empregando diferentes mídias: vídeos, filmes, jornais, ambiente AVEA e outras.

Atividades de aprendizagem: apresenta atividades em diferentes níveis de aprendizagem para que o estudante possa realizá-las e conferir o seu domínio do tema estudado.

Sumário

Palavra do professor-autor

Caro(a) Estudante!

Seja bem-vindo à disciplina de Segurança da Informação (SI). Como muitas disciplinas, a SI é fascinante e instigante. Todos os dias, pessoas mal-intencionadas apresentam novas formas de corromper, adquirir, recuperar ou utilizar indevidamente informações de usuários desatenciosos. Portanto, é importantíssimo que estejamos preparados. E preparo subentende adquirir conhecimento, trabalhar com ética e transmitir o que aprendeu.

Esta disciplina está inserida em um ambiente virtual e voltada à modalidade de Educação a Distância, que permite ao estudante conhecer e decidir o ritmo de seu aprendizado, estimulando seu autodidatismo.

O conhecimento aqui contido de modo algum é definitivo ou imutável. É esperado (e recomendado) que você procure explorar cada uma das aulas ao máximo, buscando assimilar conhecimentos correlatos e que não estão contidos explicitamente neste material. Explore os hiper*link*s sugeridos e, se possível, procure ter acesso às obras indicadas no item "Referências". Explore também os recursos disponíveis na sala de aula virtual, participe dos fóruns, cumpra as tarefas designadas, leia os textos e assista aos vídeos sugeridos.

Este caderno de nada valerá sem sua dedicação, esforço e vontade, pois tão nobre quanto decidir aprender é perseverar no aprendizado.

Um grande abraço,

Jorge Procópio da Costa Novo

Apresentação da disciplina

> O mantra de qualquer bom engenheiro de segurança é: "Segurança não é um produto, mas um processo". É mais que implantar criptografia forte, é desenhar todo o sistema de tal forma que todas as medidas de segurança, incluindo a criptografia, trabalhem em conjunto.
>
> Bruce Schneier

A Segurança da Informação (SI) é o ramo do conhecimento responsável pela preservação e descarte de um dos bens materiais mais preciosos da história da humanidade: a informação.

Ao longo da existência humana, a informação foi gerada, acumulada, passada de geração em geração e, por muitas vezes, perdida definitivamente. Com ela, nossa civilização pôde desenvolver tecnologias que permitiram, por exemplo, aumentar a produção de alimentos, combater e prevenir doenças, crescer tecnológica e financeiramente.

Neste caderno, a Segurança da Informação é apresentada através de noções introdutórias, concentrando-se nos softwares que permitem a aplicação e o entendimento dos princípios desta disciplina – Confidencialidade, Integridade, Disponibilidade, Autenticidade e Irretratabilidade.

De modo algum o conhecimento aqui contido está perfeito e acabado. Este caderno mostra tão somente a direção a ser seguida. Pois o caminho é construído com o esforço e a dedicação do estudante.

Projeto instrucional

Disciplina: Softwares de Segurança da Informação (carga horária: 40h).

Ementa: Visão histórica - fatos históricos relevantes para a Segurança da Informação (SI) e o seu papel no mundo de hoje. Conceitos iniciais: dado, informação, ativos de informação, vulnerabilidades, ameaças, riscos, impactos, medidas de segurança e princípios da SI, ciclo da SI, problemas enfrentados pela SI: danos, *malwares*, *spam* e razões para tantos problemas. *Softwares* de SI: gerenciadores de senha, gerenciadores de *backup*, ferramentas de criptografia, ferramentas para descarte seguro, ferramentas antivírus, ferramentas *antispyware* e *firewalls*. O papel do usuário: razões para instalação de softwares de segurança, atualizações de *software*, varreduras semanais, escolha de boas senhas, cuidado com as mídias removíveis, uso de *lan-houses*, proteção dos endereços de *e-mail*, cuidados com o phishing, cópias de segurança (backup), atualização do próprio conhecimento e ética.

AULA	OBJETIVOS DE APRENDIZAGEM	MATERIAIS	CARGA HORÁRIA (horas)
1 – Visão histórica	Conhecer fatos históricos relevantes para a SI; Reconhecer a importância da SI no mundo de hoje.	Indicação de hiperligações para sítios na internet sobre o tema; Vídeo do sítio Youtube sobre a história da internet; Indicação da obra O Livro dos Códigos de Simon Singh.	05
2 – Conceitos básicos	Identificar os conceitos básicos da Segurança da Informação; Entender e diferenciar os princípios norteadores da SI; Conhecer o ciclo da SI.	Indicação de hiperligações para sítios na internet sobre o tema; Vídeo do sítio Youtube sobre vulnerabilidades de transmissão.	05
3 – Problemas enfrentados pela SI – danos, vírus, cavalos de tróia e *spywares*	Identificar os principais problemas enfrentados pela Segurança da Informação; Reconhecer esses problemas como ameaças aos ativos de informação.	Indicação de hiperligações para sítios na internet sobre o tema; Indicação do filme "Troia", do diretor Wolfgang Petersen.	05

AULA	OBJETIVOS DE APRENDIZAGEM	MATERIAIS	CARGA HORÁRIA (horas)
4 – Problemas enfrentados pela SI – *ransomwares*, *worms* e *SPAM*	Identificar os principais problemas enfrentados pela Segurança da Informação; Reconhecer esses problemas como ameaças aos ativos de informação.	Indicação de hiperligações para sítios na internet sobre o tema; Vídeo do sítio *Youtube* sobre a origem do termo *spam*.	05
5 – *Softwares* de SI – gerenciadores de senha, de *backup* e ferramentas de criptografia	Conhecer os conceitos básicos sobre o tema *softwares* de Segurança da Informação; Realizar estudos de caso em cada um dos tipos de ferramentas apresentadas.	Indicação de hiperligações para sítios na internet sobre o tema.	05
6 – *Softwares* de SI – ferramentas de descarte de dados e antivírus	Conhecer os conceitos básicos sobre o tema *softwares* de Segurança da Informação; Realizar estudos de caso em cada um dos tipos de ferramentas apresentadas.	Indicação de hiperligações para sítios na internet sobre o tema.	05
7 – *Softwares* de SI – *antispywares* e *firewalls*	Conhecer os conceitos básicos sobre o tema softwares de Segurança da Informação; Realizar estudos de caso em cada um dos tipos de ferramentas apresentadas.	Indicação de hiperligações para sítios na internet sobre o tema.	05
8 – O papel do usuário	Perceber que o fator humano é o elemento mais importante da Segurança da Informação.	Indicação de hiperligações para sítios na internet sobre o tema; Indicação do livro *Segredos e Mentiras* de Bruce Schneier.	05

Aula 1 – Visão histórica

Um computador permite que você cometa rapidamente mais erros que qualquer outra invenção na história da humanidade – exceto pelas armas de fogo e pela tequila, possivelmente.

Mitch Ratliff

Objetivos

Conhecer fatos históricos relevantes para a SI.

Reconhecer a importância da SI no mundo de hoje.

1.1 Fatos históricos relevantes para a SI

Os primórdios da Segurança da Informação estão vinculados à própria evolução do homem e de sua vida em comunidade. Em determinado momento, a humanidade sentiu necessidade de representar seu dia a dia, sua religiosidade e a si própria. Muitas vezes, esses registros eram feitos através de entalhes em rocha (Figura 1.1), pinturas em cavernas ou mesmo através da manufatura de joias. Dependendo da ritualística, a poucos era dado conhecer o significado daquelas obras ou mesmo acessar os locais onde essas peças eram armazenadas.

Figura 1.1: Litografia pré-histórica
Fonte: http://www.sxc.hu/photo/288753

A invenção da escrita há aproximadamente 6.000 anos permitiu que conceitos abstratos e tradições orais fossem registrados e passados de geração em geração. Os antigos povos da China, Egito, Mesopotâmia (Figura 1.2) e da América Central disputam a paternidade dessa ferramenta, que lhes permitiu alçar a condição de grandes civilizações em seu tempo.

Figura 1.2: Escrita cuneiforme
Fonte:http://en.wikipedia.org/wiki/File: Letter_Luenna_Louvre_AO4238.jpg

A Segurança da Informação, como hoje conhecemos, surgiu com o advento da burocracia na Renascença, através do registro dos atos de administração dos governos e das guerras, passando pelas Câmaras Negras no século XVIII, responsáveis pela análise de toda correspondência que circulasse pelos territórios europeus.

Escrita Cuneiforme.
http://pt.wikipedia.org/wiki/Cuneiforme

Câmaras Negras.
http://en.wikipedia.org/wiki/Cabinet_noir

Cifra de Vigenère.
http://pt.wikipedia.org/wiki/Cifra_de_Vigen%C3%A8re

A máquina Enigma.
http://pt.wikipedia.org/wiki/Enigma_%28m%C3%A1quina%29

No século XIX, a invenção do telégrafo e da codificação Morse permitiu que mensagens fossem enviadas rapidamente dentro de um país ou mesmo entre países. Já havia a preocupação com a confidencialidade das mensagens, o que tornou a Cifra de *Vigenère* bastante utilizada.

No século XX, é relevante o uso da criptografia e da criptanálise como ferramentas militares na Segunda Guerra Mundial, a ascensão e queda da máquina Enigma alemã e o início da era da computação e da telecomunicação.

Na década de 1950, os computadores estavam localizados em instalações militares e se apresentavam na forma de *mainframes*, ocupando salas inteiras e exigindo um grande número de especialistas para sua operação e manutenção.

A interação homem-máquina se dava através do rearranjo de fios e cabos ou do uso de cartões perfurados. Não havia ainda as redes de dados e cada *mainframe* era uma máquina isolada.

A comunicação entre os ***mainframes*** só era possível através do envio de fitas magnéticas pelo correio.

A Segurança da Informação resumia-se a proteção física dos equipamentos e dos meios de armazenamento externos, garantindo que nada fosse roubado, furtado, danificado ou modificado sem autorização.

Em 1957, é lançado o primeiro satélite artificial da Terra, o *Sputnik* I, pela União Soviética. Sua função básica era transmitir um sinal de rádio capaz de ser sintonizado por qualquer radioamador. O *Sputnik* I iniciou a era das comunicações via satélite.

Na década de 1960, a quantidade de *mainframes* instalados para suportar a expansão militar decorrente da Guerra Fria era tão grande que o isolamento entre os diversos equipamentos não podia mais ser tolerado. Na verdade, tornou-se imperativo que os diversos computadores trocassem informações entre si de modo rápido e confiável.

Da necessidade de troca de informações nasceu a ARPANET, uma rede de dados redundante, territorialmente ampla e confiável, utilizada pelos *mainframes* para comunicação de dados.

A ARPANET expandiu sobremaneira a abrangência da Segurança da Informação. Antes, a SI estava centrada na proteção física dos equipamentos e dos meios de armazenamento; agora, devia se preocupar também com os acessos remotos, permissões de usuário, senhas de acesso fáceis de quebrar e tentativas de invasão, no intuito de evitar o furto, a corrupção ou o uso indevido de informações.

Em 1964, a IBM lançou um novo *mainframe*, chamado *System*/360, com a peculiaridade de não ser mais uma máquina de uso militar e sim de uso comercial, sendo adquirida por universidades e agências civis do governo norte-americano.

Além de novos equipamentos, era necessário que os sistemas operacionais fornecessem ferramentas para auxiliar os gestores de SI. Em 1964, um consórcio entre o *Massachusetts Institute of Technology* (MIT), a *General Electric e o* Laboratórios *Bell* apresentou o *Multiplexed Information and Computer Service* (MULTICS), um sistema operacional concebido para permitir autenticação de segurança em vários níveis e tratar de modo robusto as senhas de usuário.

A-Z

Mainframes:
são computadores com capacidade de processar um grande volume de informações. Seus serviços podem ser utilizados por até milhares de usuários através de terminais conectados diretamente ou através de uma rede de dados. Atualmente são empregados no processamento de informações de instituições bancárias, universidades, siderúrgicas, instituições geradoras de energia elétrica, entre outras.

ENIAC.
http://pt.wikipedia.org/wiki/Eniac

Sputinik.
http://pt.wikipedia.org/wiki/Sputnik

Guerra Fria.
http://pt.wikipedia.org/wiki/Guerra_fria

ARPANET.
http://pt.wikipedia.org/wiki/Arpanet

IBM System 360.
http://pt.wikipedia.org/wiki/IBM_System/360

Multics.
http://pt.wikipedia.org/wiki/Multics

Na década de 1970, os profissionais de tecnologia perceberam que, além de *hardwares* e *softwares* adequados, era necessário consolidar seus conhecimentos e práticas de Segurança da Informação em algum documento capaz de guiar os profissionais da área. A primeira iniciativa nesse sentido partiu do Departamento de Defesa norte-americano, intitulada "Controles de Segurança para Sistemas Computacionais", também conhecida como Relatório *Rand R-609*.

Entre as principais ideias contidas nesse relatório, temos o reconhecimento da informação como um bem material muito valioso, a importância da verificação das credenciais de cada usuário, a noção de que a Segurança da Informação é responsabilidade de todos e não apenas dos gestores de tecnologia etc.

DES.
http://pt.wikipedia.org/wiki/Data_Encryption_Standard

RSA.
http://pt.wikipedia.org/wiki/rsa

Em 1974, a IBM solicitou ao *National Bureau of Standards* (NBS) que registrasse seu algoritmo Lúcifer como padrão de encriptação de dados nos Estados Unidos da América (EUA). O pedido foi aceito em 1977, após avaliação e modificação de alguns parâmetros do algoritmo pela *National Security Agency* (NSA). O Lúcifer é rebatizado com o nome de *Data Encryption Standard* (DES).

Em 1976, o artigo "*New Directions in Cryptography*", de Whitfield Diffie e Martin Hellman, apresentou o conceito de criptografia de chave pública e fundou as bases da criptografia na internet.

Em 1977, os pesquisadores Whitfield Diffie e Martin Hellman propuseram um modelo de *hardware* capaz quebrar em apenas um dia, via força bruta, o algoritmo DES. A construção dessa máquina consumiria 20 milhões de dólares.

Nesse mesmo ano, Ronald Rivest, Adi Shamir e Leonard Adleman inventaram o algoritmo RSA, que implementa a criptografia de chave pública baseada na dificuldade de fatoração de grandes números inteiros. O algoritmo RSA é utilizado até hoje.

A década de 1980 caracterizou-se principalmente pelo início da computação pessoal. Consequentemente, a questão da Segurança da Informação se tornou mais relevante. Os computadores começaram sua carreira no ambiente de trabalho e pouco a pouco foram surgindo nos lares.

A popularidade das *Bulletin Board System* (BBS) alcançou seu auge, permitindo aos usuários o *download* e o *upload* de arquivos, leitura de notícias, troca de mensagens, participação em fóruns de discussão, jogos e bate-

-papo. Permitia, ainda, integrar a atividade de funcionários externos aos Sistemas de Informação da empresa, bastando que esse funcionário dispusesse de um computador e uma linha telefônica.

Eventualmente, uma BBS podia se tornar um foco de problemas de segurança, caso os arquivos postos à disposição dos usuários estivesse contaminado com vírus de computador, por exemplo.

Em 1982, é noticiado o 1° programa com características de vírus de computador. Foi criado para a plataforma *Apple II* e chamava-se ElkCloner. Nesse mesmo ano, se inicia a comercialização dos *Compact Discs* (CD), inicialmente para uso na indústria fonográfica e posteriormente para o armazenamento de dados. Tal tecnologia permitiu a redução de custos e o aumento da integridade das cópias de segurança dos dados.

Em 1984 é fundada a *Information Systems Security Association* (ISSA), a primeira associação de profissionais de Segurança da Informação.

Em 1985, a *Microsoft* lança um gerenciador de interface gráfica para o MS-DOS, chamado *Windows* 1.0. Tecnicamente, o *Windows* ainda não era um sistema operacional, em razão de sua instalação exigir um computador com o MS-DOS.

Em 1986, é publicada nos EUA a primeira lei a tratar de crimes cometidos através do uso de computadores. O vírus de computador conhecido como BRAIN é o primeiro a infectar em larga escala o setor de *boot* de discos rígidos.

Em 1988, o estudante da *Cornell University*, Robert Tappan Morris, dissemina o primeiro *worm* de computador, causando a parada de 10% dos servidores ativos da internet. O *worm* explorava uma série de erros nos sistemas operacionais BSD Unix e similares, propagando-se rapidamente. Pelos prejuízos causados, Morris foi julgado e condenado a cumprir 400 horas de serviço comunitário e ao pagamento de multa no valor de 10 mil dólares. O episódio dá início à criação do CERT, uma equipe de especialistas em Segurança da Informação, localizada no Instituto de Engenharia de *Software* da Universidade Carnegie Mellon, dedicada ao estudo das vulnerabilidades de segurança na internet, ao desenvolvimento de melhorias nas redes de dados e na capacitação de profissionais de tecnologia. O Brasil também conta com uma equipe que tem mesmo objetivo, o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CEST.br).

CEST.
http://www.cert.org

CEST.br.
http://www.cert.br

Revolução Digital.
http://pt.wikipedia.org/wiki/Revolu%C3%A7%C3%A3o_digital

WWW.
http://pt.wikipedia.org/wiki/Www

Navegador.
http://pt.wikipedia.org/wiki/Navegador

Por que você precisa do PGP?
http://www.dca.fee.unicamp.br/pgp/why_PGP.shtml

Ainda em 1988, Denny Yanuar Ramdhani cria o primeiro *software* antivírus. Foi escrito para eliminar e imunizar sistemas operacionais contra o vírus BRAIN. No ano seguinte, surgem os primeiros *softwares* antivírus comerciais. Caracterizavam-se por combater e proteger sistemas contra várias espécies de vírus.

Na década de 1990 acontece a desmilitarização da ARPANET, surgindo a internet como conhecemos hoje. Tal fato permitiu que empresas se conectassem a essa rede e vendessem acesso a usuários domésticos. A combinação da venda crescente de computadores pessoais, o aumento no fornecimento de serviços de acesso à internet e o advento da telefonia celular dão início à Revolução Digital.

Em 1990 surge a *World Wide Web* (WWW), um serviço executado na internet e capaz de prover interligação entre documentos (vídeos, sons, textos, animações, etc.) hospedados em diversos servidores dessa rede. Surgem os primeiros navegadores para internet (*browsers*). Essas ferramentas permitem explorar graficamente os recursos da WWW, enriquecendo a experiência do utilizador.

Paralelamente ao crescimento da WWW, pesquisadores suíços apresentam o *International Data Encryption Algorithm* (IDEA), com a intenção de substituir o algoritmo DES. O IDEA era mais seguro, pois utilizava chaves maiores e era mais rápido, em razão de utilizar instruções básicas de processamento.

Em 1991, Philip Zimmermann publica o *software* de criptografia *Pretty Good Privacy* (PGP), o qual tornou-se muito popular em razão de combinar criptografia de chave pública, criptografia de chave privada e assinaturas digitais com uma interface simples e fácil de usar. Foi criado para ajudar na defesa das liberdades individuais e do direito à privacidade.

O PGP fornece um alto grau de segurança aos dados e às comunicações do usuário pela internet. Em razão disso, seu autor sofreu investigação federal para determinar se ele havia descumprido o determinado pela *Arms Export Control Act*. Essa lei classificava a criptografia forte como armamento militar e restringia sua exportação. Após três anos, o processo foi encerrado e arquivado.

Ainda em 1991, o finlandês Linus Benedict Torvalds anuncia a primeira versão oficial do *Linux*.

Em 1994, a *Microsoft* lança o *Windows* 95, sistema operacional com várias inovações tecnológicas, tais como sistema de arquivos FAT32, suporte a nomes longos de arquivo (até 256 caracteres), dispensa de instalação prévia do MS-DOS, suporte ao barramento USB e ao Ultra DMA.

O *Windows* 95 tornou a *Microsoft* líder no mercado mundial de *softwares* de computador.

Em 1995, é criado o *Digital Versatile Disc* (DVD), mídia que apresenta maior capacidade de armazenamento e maior taxa de transmissão de dados que os *Compact Discs*. Até hoje é aproveitado na indústria cinematográfica e no armazenamento de dados.

Em 1996, o congresso dos EUA publica o *Communications Decency Act* (CDA), lei que classificava como criminosa qualquer pessoa que transmitisse material indecente ou obsceno através da internet. A Suprema Corte norte-americana declarou que a CDA era inconstitucional.

Em 1997, o Brasil passa a ser o primeiro país do mundo onde o cidadão pode enviar sua declaração de Imposto de Renda pela internet. Tal iniciativa permitiu à Secretaria da Receita Federal maior agilidade e precisão no processamento das declarações, reduzindo a sonegação e o período de restituição ao contribuinte.

A partir desse ano, novas tecnologias e esforços culminaram na quebra do DES. O projeto DESCHALL foi o primeiro a vencer o DES *Challenge*, série de desafios propostos pela RSA *Security Inc.*, que consistia em recuperar uma mensagem criptografada com o DES. O êxito do projeto se deu após 96 dias, a uma taxa de sete bilhões de operações por segundo, valendo-se do processamento ocioso de milhares de computadores distribuídos pela internet.

Em 1998, a *Electronic Frontier Foundation* (EFF) constrói uma máquina, chamada DES-*Cracker*, que em três dias recupera a senha utilizada na encriptação DES de um arquivo, demonstrando a insegurança do algoritmo diante de um adversário obstinado. A curiosidade está no fato de a quebra acontecer 21 anos mais tarde e a um custo 80 vezes menor que o previsto por Whitfield Diffie e Martin Hellman, na época da homologação do DES.

Em 1998, o presidente dos EUA Bill Clinton assina o *Digital Millennium Copyright Act* (DMCA). Essa lei classifica como crime a construção e distribuição de tecnologias e qualquer tentativa de burlar as proteções existentes em material coberto por direitos autorais.

O ano de 1999 foi muito expressivo para a Segurança da Informação. Em janeiro, já era possível quebrar o algoritmo DES em menos de 24 horas,

Linux.
http://pt.wikipedia.org/wiki/GNU/Linux

FAT32. http://pt.wikipedia.org/wiki/FAT32

USB.
http://pt.wikipedia.org/wiki/Usb

Ultra DMA.
http://pt.wikipedia.org/wiki/ATA

DVD.
http://pt.wikipedia.org/wiki/DVD

Projeto DESCHALL.
http://www.interhack.net/projects/deschall/

DES-*Cracker*.
http://w2.eff.org/Privacy/Crypto/Crypto_misc/DESCracker/HTML/19980716_eff_des_faq.html

DES-Triplo.
http://pt.wikipedia.org/wiki/3DES

Banda larga.
http://pt.wikipedia.org/wiki/Banda_larga

forçando o governo norte-americano a recomendar a utilização do padrão DES-Triplo, considerado relativamente seguro até os dias de hoje.

No mês de março, um vírus de macro chamado Melissa disseminou-se rapidamente pela internet, aproveitando-se de uma falha no programa *Microsoft Outlook*, obrigando algumas empresas a suspender seus serviços de *e-mail* para evitar maior contaminação. O vírus Melissa provocou em prejuízos calculados em 600 milhões de dólares ao redor do mundo. David Smith, criador do vírus, foi condenado a vinte meses de prisão e ao pagamento de multa no valor de cinco mil dólares.

Ainda em 1999, o jovem norueguês Jon Lech Johansen, de 15 anos, publica o código de seu DeCSS, um *software* capaz de quebrar a proteção regional presente nos DVDs comerciais.

A década de 2000, até o momento, foi marcada principalmente pela popularização do acesso banda larga à internet, proliferação dos "cibercrimes", discussões sobre privacidade, consolidação do *software* livre como modelo de negócios e pelos *malwares*.

Em maio de 2000, o mundo conhece o *worm I LOVE YOU* da pior maneira: quase cinquenta milhões de computadores do mundo inteiro infectados em 24 horas. Segundo a consultoria americana *Computer Economics*, o *worm* causou prejuízos na ordem de 8,75 bilhões de dólares.

Em 2001, os EUA sofrem o maior ataque terrorista de sua história: os atentados de 11 de setembro. Durante a manhã desse dia, dois aviões comerciais sequestrados colidiram contra as torres do *World Trade Center*, na cidade de Manhattan – Nova York, destruindo completamente esses edifícios. Além da tragédia humana, várias empresas instaladas nesses prédios simplesmente deixaram de existir, tornando esse evento o pior dia para a Segurança da Informação.

A-Z

Kernel:
É a camada do sistema operacional mais próxima do hardware, sendo responsável pela troca de informações entre ambos.

Em outubro é lançado o *Microsoft Windows XP*, o primeiro sistema opracional construído sob nova arquitetura e ***kernel***, o qual conta com as seguintes características: nova interface gráfica mais fácil e intuitiva, maior estabilidade, menor tempo de inicialização e desligamento, dispensa de reinicialização do sistema para conexão e desconexão de novos dispositivos, assistência remota e suporte para DVD e redes sem fios.

Essas características tornaram o *Windows XP* o sistema operacional mais popular do mundo, com um pico de 85% de participação do mercado em 2006.

Ainda em 2001, o Brasil se torna a primeira nação do mundo a ter uma infraestrutura de chaves públicas prevista em sua legislação. Surgem os *worms* Sircam, CODE RED, NINDA e Klez, todos com alta capacidade de disseminação e contaminação de arquivos.

Em 2002, o algoritmo Rijndael, criado pelos belgas Vincent Rijmen e Joan Daemen, é escolhido pelo governo dos EUA como o novo padrão criptográfico, substituindo o obsoleto DES. Tem como principais características: facilidade de implementação em *hardware* e *software*, alto grau de segurança e desempenho, resistência a ataques conhecidos e pouco consumo de memória. O Rijndael foi rebatizado com o nome de *Advanced Encryption Standard* (AES).

AES.
http://pt.wikipedia.org/wiki/AES

Lei *Sarbanes-Oxley.*
http://pt.wikipedia.org/wiki/Sarbanes-Oxley

Enron Corporation.
http://pt.wikipedia.org/wiki/Enron

Skype.
http://pt.wikipedia.org/wiki/Skype

DCOM.
http://pt.wikipedia.org/wiki/DCOM

Ainda em 2002 é publicada a *Sarbanes-Oxley Act*, lei criada com o objetivo de garantir a criação de mecanismos de auditoria, segurança e controles confiáveis nas empresas. Tais mecanismos buscam evitar a fuga de investimentos financeiros dos EUA, após os escândalos envolvendo a *Enron Corporation*.

No ano de 2003, um vírus de computador chamado SQL-Slammer torna-se o mais rápido do mundo, infectando mais de setenta mil servidores SQL no mundo todo, paralisando por várias horas os serviços de internet.

Cresce o número de fraudes no Brasil e em outros países do mundo. Surge o primeiro serviço de telefonia da internet – o *Skype*.

Em agosto, aproveitando-se de uma falha de segurança no serviço *Distributed Component Object Model* (DCOM), o vírus Blaster disseminou-se por quase meio milhão de computadores. O autor do Blaster, Jeffrey Lee Parsons, de apenas 18 anos, foi condenado a três anos de serviço comunitário.

Em 2004 nascem as primeiras redes sociais virtuais, como o *MySpace*, *Orkut* e *Facebook*.

Em 2005 é lançado o Ubuntu, uma distribuição *Linux* voltada para computadores pessoais e dedicada ao usuário pouco experiente. Nasce o *Youtube*, sítio da internet voltado ao compartilhamento de vídeos. Os *gadgets* tornam-se cada vez mais populares.

No ano de 2008, os discos *Blu-ray* começam a substituir os DVDs na indústria cinematográfica. Surge o vírus Conficker, ativo até os dias de hoje. É considerado o vírus que mais se disseminou na internet, tirando o primeiro lugar do SQL Slammer.

Redes Sociais Virtuais.
http://pt.wikipedia.org/wiki/Redes_Sociais_Virtuais

Gadget.
http://pt.wikipedia.org/wiki/Gadget

Blu-ray.
http://pt.wikipedia.org/wiki/Disco_Blu-ray

A história secreta do Conficker.
http://info.abril.com.br/noticias/seguranca/a-historia-secreta-do-conficker-14092009-14.shl

1.2 A SI no mundo de hoje

No decorrer da história da humanidade, a Segurança da Informação tem se mostrado um elemento cada vez mais importante para as pessoas e para os negócios das empresas.

Nas residências, os computadores estão repletos de documentos, planilhas, correspondências eletrônicas, fotografias, vídeos, declarações de Imposto de Renda e até mesmo listas de amigos.

Nas empresas, a situação não é diferente. Servidores armazenam transações eletrônicas, planos, estratégias de negócios, segredos industriais, informações fiscais e previdenciárias, contratos etc.

A onipresença da tecnologia da informação é uma realidade irreversível. A humanidade está cercada e a cada instante cria e consome um volume cada vez maior de informações. E mantê-las confiáveis custa dinheiro. Afinal, tudo tem valor.

Este é o principal papel da SI no mundo moderno: garantir que os recursos financeiros investidos na criação, conservação, uso, transmissão e descarte das informações sejam resguardados.

A história da internet.
http://www.youtube.com/watch?v=6cyYX2PD5kc

Para conhecer mais detalhes sobre aspectos históricos da Segurança da Informação, leia a obra O Livro dos Códigos de Simon Singh. Existe também uma versão desse livro na internet, que pode ser obtida em:
http://www.simonsingh.net/The_CDROM.html

Resumo

Na década de 1950, os computadores estavam localizados em instalações militares e se apresentavam na forma de *mainframes*, ocupando salas inteiras e exigindo um grande número de especialistas para sua operação e manutenção. A década de 1960 caracterizou-se pela expansão rápida da computação para fins militares e assistiu ao início da computação comercial. Os computadores ficaram menores e menos caros. A década de 1970 caracterizou-se pelo início da normatização da SI, pela expansão da computação comercial, pelo surgimento dos primeiros padrões criptográficos e da criptografia de chave pública. Os computadores continuavam diminuindo e ficando mais baratos. A década de 1980 caracterizou-se principalmente pelo início da computação pessoal, pela expansão do uso de computadores nos escritórios, pela expansão das redes privadas de dados, pela conexão dessas redes à internet, pelo surgimento dos vírus de computador. A década de 1990 caracterizou-se pela conexão dos computadores pessoais domésticos à internet, pelo surgimento da *WEB* e dos navegadores, pela consolidação da interface gráfica nos computadores pessoais, pelo início da discussão sobre privacidade *on-line*, pela propagação de vírus de computador em escala mundial. A década de 2000 caracterizou-se pela mudança no objetivo do vírus de computador (antes queriam destruir os dados, hoje querem roubá-los), pela expansão no uso de *softwares* livres, proliferação do "cibercrime", ataques DOS e DDOS, *SPAM*, *Spywares*.

Atividades de aprendizagem

1. Pesquise na internet e construa um gráfico relacionando à quantidade de *malwares* e o ano de seu surgimento. Poste um arquivo com o gráfico no AVEA.

2. A evolução na tecnologia vem trazendo mais segurança à informação ou vem expondo a informação a novos tipos de vulnerabilidades? Justifique. Poste o arquivo com sua resposta e justificativas no AVEA.

Aula 2 – Conceitos iniciais

A Segurança em TI é como trancar sua casa ou seu carro – não vai impedir os bandidos, mas se a tranca for boa o bastante, eles podem preferir buscar um alvo mais fácil.

Paul Herbka

Objetivos

Identificar os conceitos básicos da Segurança da Informação.

Entender e diferenciar os princípios norteadores da SI.

Conhecer o ciclo da SI.

2.1 Segurança da Informação

A Segurança da Informação (SI) é o ramo do conhecimento responsável pela preservação e descarte dos ativos de informação, seja ela pessoal ou corporativa, através da elaboração de critérios que protejam esses ativos contra o furto, roubo, perda, corrupção ou uso indevido. A SI é considerada um fator de competitividade e sobrevivência das empresas no atual mundo dos negócios.

2.2 Dado

Os dados são a menor unidade componente da informação. Assim, a construção de qualquer sistema de informação está estruturalmente fundamentada em dados. Podem ser exemplos de dados: fatos, imagens, gravações etc. Isoladamente, os dados não possuem valor.

2.3 Informação

A informação é um conjunto de dados, ao qual se atribui valor, utilidade ou interpretação, que pode representar um grande diferencial para os seus detentores.

Atualmente, pode-se dizer que a informação é o ativo mais valioso de uma empresa, integrando o patrimônio desta.

Toda informação possui um ciclo de vida composto de três fases, conforme indicado pela Figura 2.1.

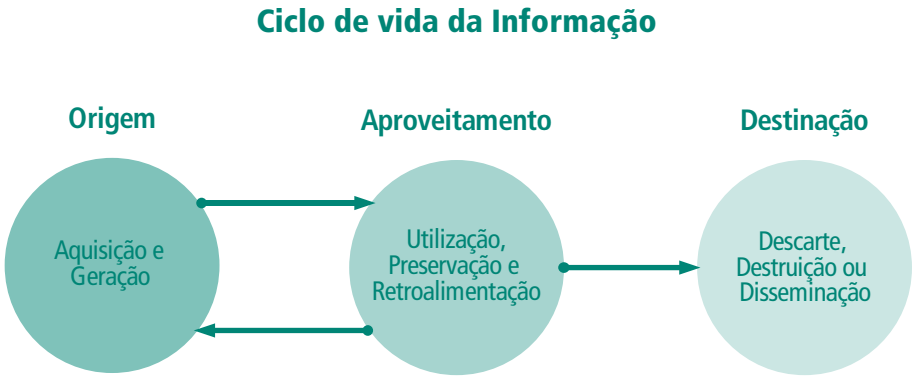


Figura 2.1: Ciclo de vida da informação

Na **Origem**, os dados e informações são adquiridos através de pesquisa, processos técnicos, reflexões, deduções matemáticas, experimentação ou observação da natureza. Também são adquiridos como resultado das inter-relações entre os processos da segunda fase: o **Aproveitamento**.

O **Aproveitamento** responde pela exploração econômica da informação ou dos produtos gerados a partir dela. Um de seus processos mais importantes é a **Preservação**, que objetiva manter a informação bem guardada e disponível para seus detentores.

A terceira fase é a **Destinação**, que acontece quando a informação não pode ou não precisa mais ficar sob a tutela exclusiva de seu detentor.

A **Destinação** acontece em três casos: no primeiro, os direitos de autor caducaram e o detentor não pode mais explorá-la de modo exclusivo (patentes, por exemplo). Desse modo, a informação deve ser disponibilizada ao público. No segundo caso, a informação perdeu utilidade para o detentor, porém ainda pode ser valiosa para terceiros mal-intencionados. Por fim, há o caso em que a informação deve ser transferida de um lugar para outro, por diversas razões.

Como exemplo, pode-se citar a necessidade do detentor em expandir a estrutura de armazenamento de suas informações, através da troca de um disco rígido por outro maior. Acontece que a informação não é simplesmente "movida" do disco rígido antigo para o disco rígido novo, ela é apenas "copiada".

Desse modo, se a informação contida no disco rígido antigo não for apropriadamente descartada, ela pode ser obtida novamente, expondo o detentor.

2.4 Ativos de informação

Qualquer coisa que tenha valor para uma empresa é chamado de ativo. Assim, podemos dizer que um ativo de informação é o conjunto de informações que tem valor para a empresa.

Podemos incluir nos ativos de informação os meios físicos que os suportam (e que permitem seu transporte) e as pessoas que os utilizam. Como exemplos de meios físicos, temos os discos rígidos, *pen drives*, CDs, DVDs, cabeamento de redes, *switches* e roteadores. Além desses, também podemos citar documentos impressos, correspondências, linhas de código de programação, relatórios financeiros, projetos de engenharia, etc.

Pesquise na internet sobre Gestão do Ciclo de Vida da Informação, para conhecer mais sobre o assunto.

Switch.
http://pt.wikipedia.org/wiki/Switch

São esses ativos de informação que a Segurança da Informação busca manter protegidos.

2.5 Vulnerabilidades

As vulnerabilidades são fatores internos capazes de expor as informações de um sistema ao furto, roubo, perda, corrupção ou uso indevido. São pontos fracos que devem ser identificados e eliminados do ambiente empresarial.

As vulnerabilidades podem ser classificadas de vários modos. A seguir, enumeramos uma dessas classificações.

2.5.1 Vulnerabilidades ambientais

São aquelas relacionadas ao meio ambiente e à geografia do local onde a infraestrutura de tecnologia da informação da empresa está instalada. Exemplos: proximidade a refinarias de petróleo (explosões e corrosão de componentes pela poluição), proximidade a rios (inundações), locais muito distantes de usinas elétricas ou que possuam apenas uma unidade de geração de energia (desabastecimento), proximidade do litoral (*tsunamis*, maremotos, corrosão de componentes pela maresia), instalações em áreas de atividade sísmica (terremotos, erupções vulcânicas), instalações em áreas hostis (furacões, tornados, tempestades), entre outras.

2.5.2 Vulnerabilidades de infraestrutura

São aquelas restritas ao ambiente que abriga a infraestrutura de tecnologia da informação da empresa, bem como os locais por onde a informação trafega. Exemplos: ambientes mal refrigerados ou muito úmidos, ausência de filtros contra poeira e poluição, ausência de elementos de combate a incêndio, ausência de aterramento elétrico, ausência de trancas nas portas de acesso, cabeamento assentado em discordância às normas técnicas, existência de goteiras, existência de encanamento hidráulico próximo à sala de equipamentos, existência de sobrecarga nos equipamentos de alimentação elétrica, ambiente sem controle de acesso para usuários, entre outros.

2.5.3 Vulnerabilidades de armazenamento

Memórias SSD.
http://pt.wikipedia.org/wiki/SSD

Brasileiros são presos por utilizar ilegalmente satélite americano.
http://www.geek.com.br/blogs/832697632/posts/9852-brasileiros-sao-presos-por-utilizar-ilegalmente-satelite-americano

Satélites "bolinha".
http://www.py2adn.com/artigos/Satelite-Bolinha.pdf

São aquelas relacionadas aos meios físicos, também conhecidos como mídias, onde a informação está armazenada. Dentre os meios físicos podemos citar os discos rígidos, as mídias compactas (CDs e DVDs), as fitas magnéticas e os dispositivos SSD (*pen drives* e *flashdrives*). Incluem-se, ainda, toda documentação transcrita em papel.

As vulnerabilidades de armazenamento incluem a contaminação do ambiente por fungos, por excesso de umidade e por eletricidade estática, proximidade do fim da vida útil do equipamento (panes eletrônicas), exposição ao calor, má acomodação dos equipamentos (quedas), falta de controle no transporte (extravio), existência de defeitos de fabricação ocultos, procedimento inadequado para o descarte das mídias, entre outras.

2.5.4 Vulnerabilidades de transmissão

Assista ao vídeo e discuta com os demais estudantes sobre as implicações dessa vulnerabilidade.
http://www.youtube.com/watch?v=TUrYwMK2V5s

São aquelas relacionadas aos aspectos da comunicação de dados, abrangendo os meios físicos de transmissão (cabeamento, ondas de rádio, micro-ondas, etc.) e os meios onde estes estão assentados (postes, tubulações, etc.). São exemplos desse tipo de vulnerabilidade: proximidade a florestas (quedas de árvores sobre o cabeamento), tráfego intenso de veículos (postes derrubados por acidentes de trânsito), tráfego de caminhões (podem romper o cabeamento que atravessa a via), obras de saneamento básico (podem destruir o cabeamento subterrâneo), grampeamento da transmissão (para furtar ou alterar informações), utilização indevida de canais de transmissão (rádios piratas), ratos (podem roer o cabeamento), entre outros.

2.5.5 Vulnerabilidades de *hardware*

São aquelas relacionadas aos equipamentos, vistos de modo individual. São exemplos de vulnerabilidades de *hardware* a ausência de atualizações de *firmware* pelos fabricantes, incompatibilidade com alguns *softwares*, dimensionamento inadequado (muitas informações para poucos dispositivos de armazenamento), muitas transações para pouco processamento (número insuficiente de CPUs), muito tráfego de dados para pouca banda de transmissão, desgaste natural, entre outros.

2.5.6 Vulnerabilidades de *software*

São aquelas relacionadas às falhas de desenvolvimento e implantação dos aplicativos, sistemas operacionais e protocolos de comunicação, comumente conhecidos como *softwares*. Essas vulnerabilidades são muito comuns e poderosas, permitem que um invasor domine um sistema informatizado ou o faça deixar de responder a solicitações.

São exemplos dessa vulnerabilidade o transbordamento de dados (*buffer overflow*), inundação de sincronia (*SYN flood*), ponteiros pendentes (*dangling pointers*), entre outros.

2.5.7 Vulnerabilidades humanas

São aquelas decorrentes da ação ou omissão dos seres humanos. Em geral, são causadas pelo desconhecimento das normas básicas de segurança durante a utilização do ambiente de tecnologia da informação. Essas vulnerabilidades também podem decorrer de ações ou omissões intencionais. Como exemplos de vulnerabilidades humanas, podemos citar a falta de capacitação do usuário, a ignorância às normas de segurança, a insatisfação com o ambiente de trabalho, erros, falta de cuidado com os equipamentos, escolha de senhas fracas, compartilhamento de senhas de acesso, entre outros.

2.6 Ameaças

As ameaças são fatores externos capazes de explorar uma ou mais vulnerabilidades, permitindo furto, roubo, perda, corrupção ou uso indevido dos ativos de informação.

São exemplos de ameaças a invasão de sistemas de informação, as fraudes, o vandalismo contra equipamentos ou meios de transmissão, os atentados terroristas, as catástrofes naturais, a espionagem industrial ou internacional, o vírus de computador, os *Spywares*, o recebimento de *spam*, entre outros.

Múltiplas Vulnerabilidades no Cisco IOS.
http://www.rnp.br/cais/alertas/2008/secunia-sa31990.html

Vulnerabilidade de DOS em dispositivos *wireless* IEEE 802.11.
http://www.rnp.br/cais/alertas/2004/AusCERT-AA-200402.htm

Vulnerabilidades em implementação do NTP.
http://www.rnp.br/cais/alertas/2009/uscert-vu853097.html

Erro de programação inofensivo vira ameaça à segurança.
http://tecnologia.terra.com.br/interna/0,,OI1790208-EI4805,00.html

Veja os 10 casos mais curiosos de perda e recuperação de dados.
http://tecnologia.terra.com.br/interna/0,,OI1284657-EI4799,00.html

Descoberta rede de espionagem chinesa que agia em 103 países.
http://noticias.terra.com.br/mundo/interna/0,,OI3666205-EI10495,00.html

Não é possível se proteger contra todas as ameaças, pois elas sempre existirão e sempre estarão por perto. Uma das funções da Segurança da Informação é impedir que as ameaças se concretizem, garantindo a continuidade das atividades da empresa.

As ameaças podem ser classificadas de vários modos. A seguir, enumeramos uma dessas classificações.

2.6.1 Ameaças naturais

São aquelas relacionadas ao meio ambiente, clima ou geografia do local. São exemplos as inundações de rios, os terremotos, as descargas atmosféricas, *tsunamis*, etc.;

2.6.2 Ameaças de cunho doloso ou intencionais

São aquelas decorrentes da atividade consciente, com o propósito de furtar, roubar, destruir, corromper ou usar indevidamente os ativos de informação. Incluem os *spywares*, o vírus de computador, as invasões e o vandalismo.

2.6.3 Ameaças de cunho culposo ou não intencionais

São aquelas relacionadas à atividade inconsciente do usuário do ambiente de tecnologia da informação. Em geral, decorrem de ações equivocadas, do despreparo para evitar acidentes e do desconhecimento no uso dos ativos de informação. São exemplos o usuário que não sabe utilizar um extintor de incêndio, o usuário que não verificou a voltagem do equipamento antes de ligá-lo à tomada, o apagamento de um arquivo essencial para o funcionamento do sistema, entre outros.

2.6.4 Riscos

Os riscos são a probabilidade de uma ameaça se concretizar, provocando danos aos ativos de informação.

A Figura 2.2 mostra como medir o valor do risco, através da seguinte expressão:

Risco = vulnerabilidade x ameaça.

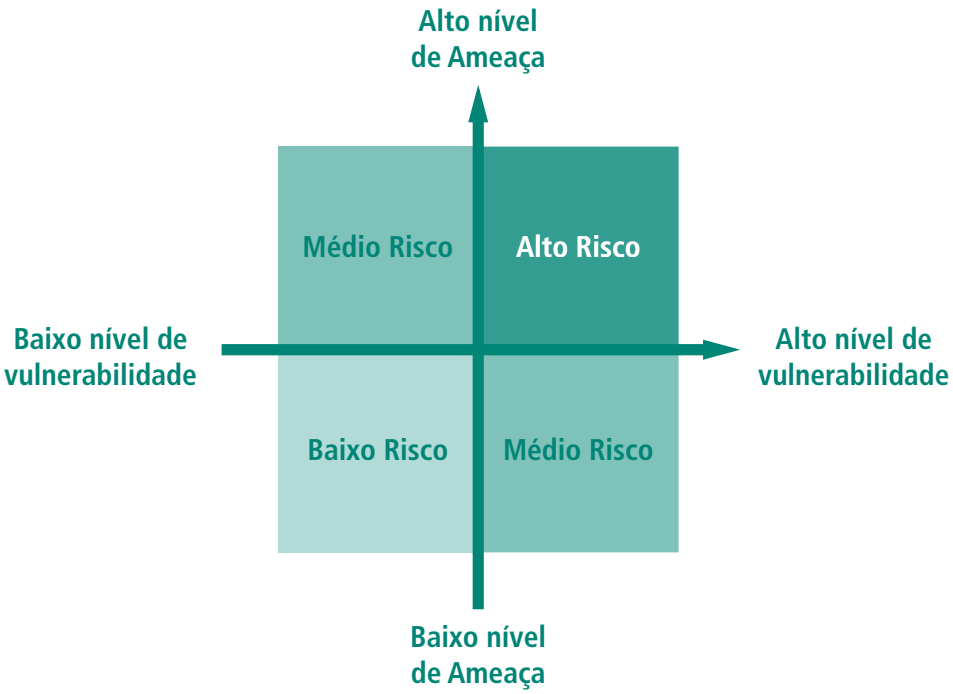


Figura 2.2: Medida do grau de risco

Por exemplo, se uma empresa não conta com proteção contra inundações, ela está vulnerável. Entretanto, se ela está instalada numa região que não sofre alagamento, ou está na proximidade de um rio que não costuma transbordar, então não há ameaça e o risco é mínimo.

Há ainda a questão da probabilidade de um evento acontecer. Por exemplo, a chance de um meteoro atingir o prédio de sua empresa é mínima; porém, se acontecer, o risco de extinção do negócio é altíssimo. Outro exemplo, a chance de se apagar acidentalmente um arquivo é alta; porém, em um ambiente munido de um sistema cópias de segurança, o risco de esse arquivo se perder definitivamente é mínimo.

É importante perceber que os custos para minorar as vulnerabilidades e para controlar ameaças devem ser mais baixos que se sujeitar ao risco. Por exemplo, será vantagem investir mais alguns milhões de reais para construir um edifício à prova de terremotos aqui no Brasil? Com certeza, não. Afinal, nosso país não sofre com esse tipo de problema. É por esse motivo que uma análise de custo/benefício é valiosa.

2.7 Impactos

Os impactos são os danos causados pela concretização dos riscos. Significa que o ativo de informação foi perdido, furtado, corrompido ou usado indevidamente.

O valor do impacto é medido pela seguinte expressão:

Impacto = risco x valor do ativo de informação

A Figura 2.3 mostra esse relacionamento.

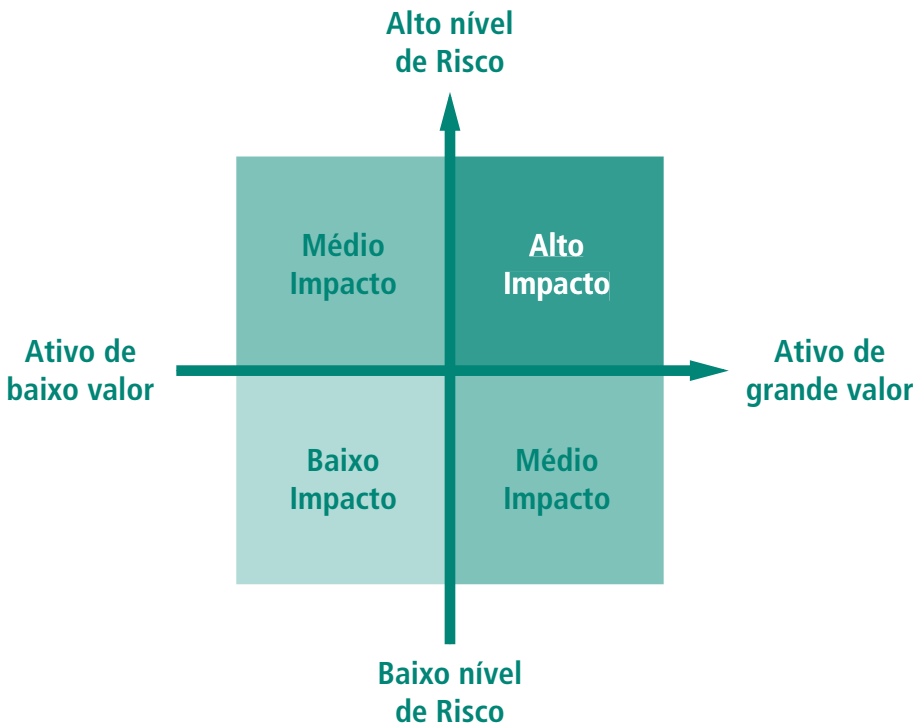


Figura 2.3: Medida do valor do impacto

11 de setembro. http://www.softsis.com.br/epate/11-de-setembro

Quanto maior o valor do ativo, maior será o valor do impacto. Quanto menor o grau do risco, menor será o valor do impacto. Por exemplo, no atentado ao *World Trade Center*, nos Estados Unidos da América, no dia 11 de setembro de 2001, muitas empresas simplesmente deixaram de existir por causa da destruição completa de seus ativos de informação. O risco de aquele atentado ocorrer e ter sucesso era considerado mínimo, porém, aconteceu e o impacto foi gigantesco.

Por isso, é muito importante identificar as vulnerabilidades e as ameaças, calcular os riscos, avaliar os ativos de informação e estar preparado para minimizar os impactos. A Figura 2.4 consolida os relacionamentos entre esses conceitos.

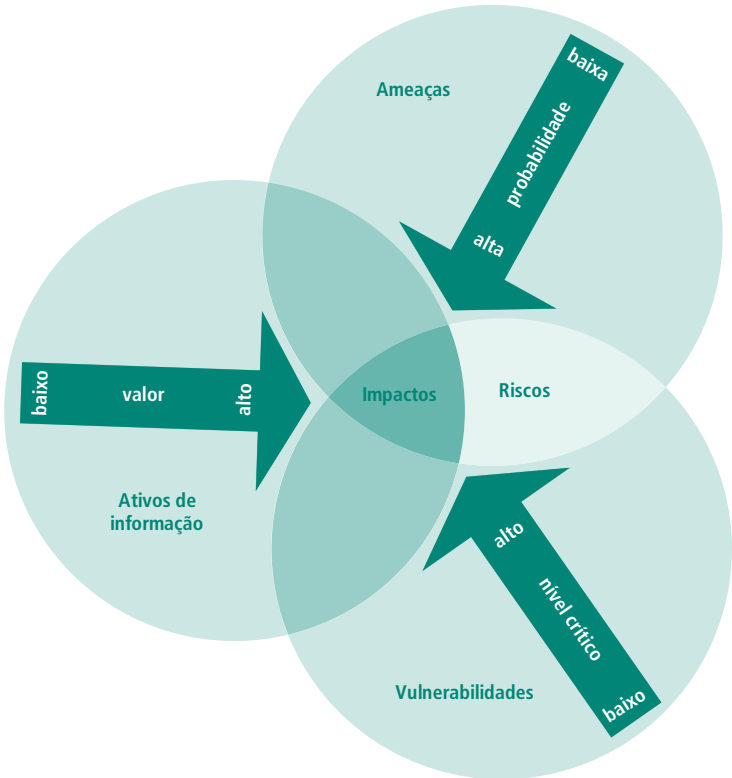


Figura 2.4: Relacionamento entre os conceitos abordados
Fonte: Adaptado de *McAfee Security Insights* (2003)

2.8 Medidas de segurança

São ações que minimizam a existência de riscos e os custos dos impactos, através da redução e eliminação de vulnerabilidades e de ameaças. O conjunto de medidas de segurança e sua prática constituem a essência da Segurança da Informação.

Existem três tipos básicos de medida de segurança.

2.8.1 Medidas preventivas

São aquelas planejadas e executadas no intuito de evitar a ocorrência de danos aos ativos de informação. Buscam reduzir as vulnerabilidades e manter as ameaças sob controle. Aplicam-se às vulnerabilidades conhecidas e ameaças identificadas.

2.8.2 Medidas prospectivas

São aquelas planejadas e executadas durante o ciclo normal de atividades da empresa. A prospecção busca identificar vulnerabilidades e ameaças que

estejam ocultas ou que façam parte de produtos e soluções que a empresa pretende adquirir.

2.8.3 Medidas corretivas

São aquelas executadas após o dano ao ativo de informação. Buscam eliminar ou minorar os impactos sofridos, bem como colaborar com a criação de outras medidas de seguranças que evitem a repetição do problema.

2.9 Princípios da SI

São conceitos gerais que orientam a atividade de segurança contra furto, roubo, perda, corrupção ou uso indevido da informação. São cinco princípios: a confidencialidade, a integridade, a disponibilidade, a autenticidade e a irretratabilidade. Nenhum deles deve ser aplicado de modo isolado, pois um complementa o outro.

2.9.1 Confidencialidade

É um princípio de natureza restritiva. Estabelece que somente pessoas previamente autorizadas tenham conhecimento do conteúdo da informação. Além disso, estabelece os casos em que a divulgação da existência da informação é proibida.

A confidencialidade deve ser aplicada tanto a informações armazenadas como a informações em transmissão. Também se aplica à ética, pois alguns profissionais são obrigados a manter sigilo dos dados de seus clientes, tais como advogados, psicólogos, médicos e jornalistas.

Esteganografia. http://www.numaboa.com.br/criptografia/esteganografia

As principais ferramentas utilizadas pela confidencialidade são a esteganografia e a criptografia. A primeira dedica-se a esconder a existência da informação e a segunda dedica-se a proteger seu significado.

A perda de confidencialidade pode gerar grandes prejuízos. Por exemplo, se os dados do cartão de crédito vazarem, seu proprietário estará exposto a um grande número de fraudes, compras e empréstimos indevidos, etc.

É importante lembrar que não existe mecanismo 100% confidencial, durante 100% do tempo.

Termos associados à confidencialidade: sigilo, segredo.

2.9.2 Integridade

É um princípio de natureza conservativa. Estabelece que a informação só pode sofrer reduções, acréscimos ou atualizações por pessoas previamente autorizadas, o que mantém suas características originais e respeita seu ciclo de vida.

O princípio da integridade é essencial para o êxito de qualquer comunicação. O emissor deve possuir absoluta confiança que a informação transmitida é exatamente a mesma que chegou às mãos do receptor e vice-versa. A perda de integridade pode gerar informações incorretas, que não correspondam mais à sua finalidade, impedindo sua utilização.

A integridade abrange ainda os sistemas que armazenam ou transmitem a informação, tais como arquivos de configuração de elementos ativos de rede, trocas indevidas de senhas de usuário, invasão de sistemas etc.

As principais ferramentas utilizadas na integridade são os algoritmos *Hash*, que geram uma espécie de assinatura da informação, indicando imediatamente quaisquer alterações.

Algoritmos *Hash*.
http://pt.wikipedia.org/wiki/Hash

Termos associados à integridade: confiança, conservação, originalidade.

2.9.3 Disponibilidade

É um princípio de natureza permissiva. Estabelece que a informação deve estar sempre acessível às pessoas previamente autorizadas, no momento em que necessitam utilizá-la. Sua eficiência é atrelada aos princípios anteriores, pois no momento em que a informação está disponível é necessário que sejam garantidas a confidencialidade e a integridade do material acessado.

A disponibilidade está completamente vinculada a um ambiente de tecnologia da informação bem estruturado e a um corpo profissional bem treinado.

A perda de disponibilidade impede, ou pelo menos limita, a capacidade dos usuários em acessar determinada informação.

As principais ferramentas utilizadas na disponibilidade são o controle de acesso (esquemas *login*/senha, *smartcards*, biometria) e as cópias de segurança (*backup*).

Termos associados à disponibilidade: acessível.

2.9.4 Autenticidade

É um princípio de natureza identificativa. Estabelece que as informações, transações e comunicações devem ter uma origem comprovada, autores e/ou operadores identificados, e não terem sido alvo de alterações imprevistas. É fortemente ligada ao princípio da integridade.

Token.
http://pt.wikipedia.org/wiki/Token_(chave_eletr%C3%B4nica

Assinatura digital.
http://pt.wikipedia.org/wiki/Assinatura_digital

Selo de tempo.
http://pt.wikipedia.org/wiki/Selo_cronol%C3%B3gico

A autenticidade é comprovada de três modos:

a) algo que o usuário sabe, tais como senhas de acesso;

b) algo que o usuário tem, tais como *tokens* ou cartões de acesso;

c) algo que o usuário é, tais como impressões digitais.

As principais ferramentas utilizadas na autenticidade são as assinaturas digitais e os selos de tempo (*timestamp*).

Termos associados à autenticidade: verdadeiro, original, identidade, genuíno.

2.9.5 Irretratabilidade

É um princípio de natureza contratual. Estabelece que pessoas identificadas e autenticadas em um sistema de informações não possam repudiar terem criado ou alterado dados contidos em informações, transações ou comunicações. Pode ser de três tipos:

a) irretratabilidade de origem: protege o receptor, autenticando a identidade do emissor dos dados;

b) irretratabilidade de entrega: protege o emissor, autenticando a identidade do receptor dos dados;

c) irretratabilidade de transmissão: protege o emissor e o receptor, autenticando o registro de recebimento dos dados pelo receptor.

As principais ferramentas utilizadas na irretratabilidade são as assinaturas digitais e os selos de tempo (*timestamp*).

Termos associados à irretratabilidade: não repúdio.

2.10 Ciclo da Segurança da Informação

A Segurança da Informação é um processo; portanto, deve obedecer a uma série de atividades encadeadas, em que o resultado de um passo é o valor de entrada do passo seguinte, formando um ciclo. As atividades enumeradas a seguir devem ser realizadas em todos os ativos de informação:

a) identificação e definição do valor dos ativos;

b) identificação e classificação das vulnerabilidades;

c) identificação e classificação das ameaças;

d) cálculo dos riscos;

e) cálculo do valor dos impactos;

f) definição e implantação de medidas de segurança.

A Figura 2.5 inter-relaciona essas atividades.

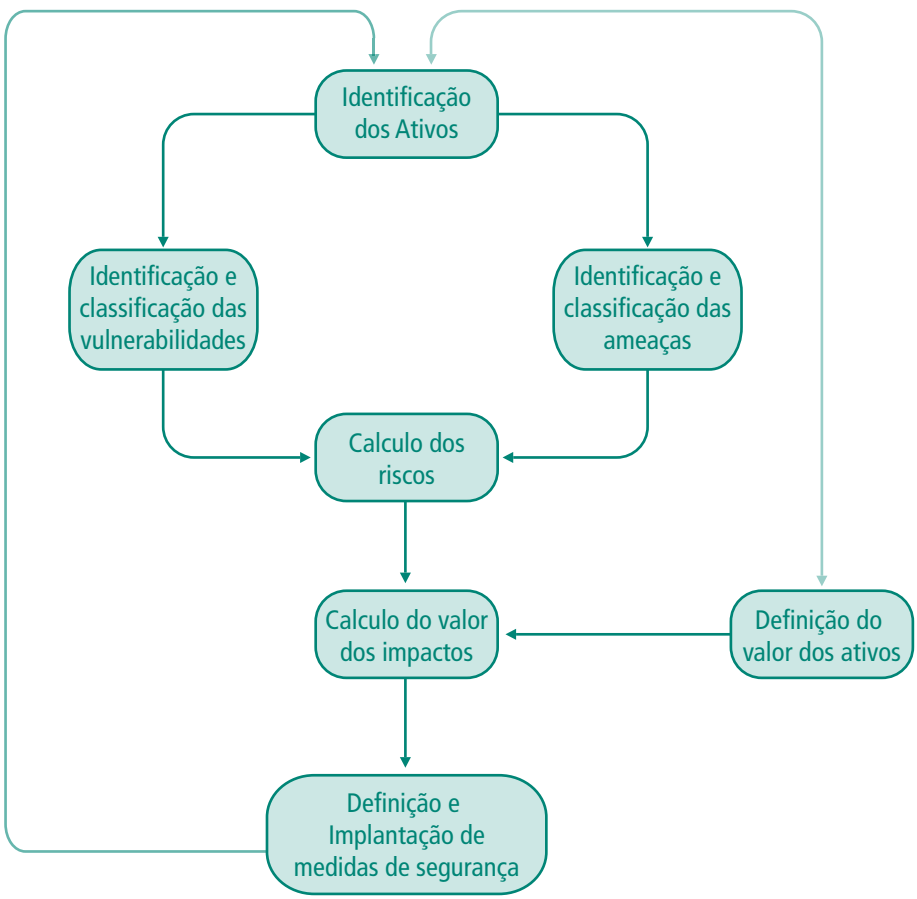


Figura 2.5: Ciclo da Segurança da Informação
Fonte: Elaborada pelo autor

Resumo

As informações são construídas com dados e têm um ciclo de vida com três fases – origem, aproveitamento e destinação. Vulnerabilidades são pontos fracos e podem ter natureza ambiental, infraestrutural, de armazenamento, de transmissão, de *hardware*, de *software* e humanas. Ameaças são tudo o que pode explorar um ponto fraco. Podem ser naturais, intencionais e não intencionais. O risco é o grau de exposição à ameaça. Os impactos são os prejuízos potenciais, a probabilidade de algum risco se concretizar. As medidas de segurança buscam minimizar esses problemas. Podem ser preventivas, prospectivas e corretivas. Os princípios da SI são confidencialidade, integridade, disponibilidade, autenticidade e irretratabilidade, considerando que cada um sempre complementa os demais. O ciclo de SI segue uma série de atividades encadeadas, em que o resultado de um passo é o valor de entrada do passo. Esse processo permite a melhora contínua na salvaguarda das informações.

Atividades de aprendizagem

1. Pesquise na internet e apresente pelo menos dois exemplos de cada um dos tipos de medidas de segurança.

2. Responda: O que é mais valioso para uma empresa, as informações ou os equipamentos que as contêm? Justifique.

Poste os arquivos com suas respostas e justificativas no AVEA.

Aula 3 – Problemas enfrentados pela SI - danos, vírus, cavalos de troia e *spyware*

Em 2006, os atacantes querem pagar o aluguel. Eles não querem escrever um worm que destrói o seu hardware. Eles querem dominar computadores e usá-los para ganhar dinheiro.

Mike Danseglio

Objetivos

Identificar os principais problemas enfrentados pela Segurança da Informação.

Reconhecer esses problemas como ameaças aos ativos de informação.

3.1 Danos

Danos são quaisquer prejuízos sofridos pela informação ou por seus detentores, podendo ser de três tipos.

3.1.1 Danos lógicos

Os danos lógicos são aqueles que comprometem apenas as informações armazenadas em um meio físico. As informações podem ser comprometidas de três maneiras.

3.1.1.1 Exclusão total

A informação armazenada é completamente excluída do meio físico.

3.1.1.2 Exclusão parcial

Apenas uma parte da informação armazenada é excluída do meio físico, por causa de falhas na gravação.

3.1.1.3 Substituição

A informação antiga é substituída por outra mais nova, em geral incorreta ou imprecisa.

3.1.2 Danos físicos

Os danos físicos são aqueles que comprometem o meio físico onde a informação está armazenada. Em boa parte dos casos de danos físicos, a informação também fica comprometida.

São exemplos de danos físicos a queima de componentes de discos rígidos por causa da sobretensão elétrica, CDs e DVDs riscados como consequência da má conservação, documentos em papel descartados por engano, entre outros.

3.1.3 Danos pessoais

Os danos pessoais são aqueles que comprometem o dono da informação ou o seu patrimônio. Em geral, ocorrem após o furto, roubo, perda, corrupção ou uso indevido dessas informações.

Médica britânica perde mais de R$ 1 milhão com golpe virtual. http://g1.globo.com/Noticias/Tecnologia/0,,MRP1094096-6174,00.html

3.2 *Malwares*

Malwares é o termo que designa um grupo de programas de computador desenvolvidos com três finalidades:

a) provocar a perda ou corrupção das informações contidas no computador;

b) usar indevidamente informações pessoais do usuário;

c) controlar remotamente o computador do usuário.

O termo *malware* foi criado da contração do termo em inglês *malicious software* e significa código malicioso ou *software* malicioso. As principais espécies de *malwares* são:

a) vírus de computador;

b) cavalos de troia;

c) *spywares*;

d) *ransomware*;

e) *worms*.

Os *malwares* se aproveitam de falhas existentes nos *softwares* comerciais, da curiosidade e da falta de cuidado do usuário, disseminando-se pelos sistemas de informática das seguintes maneiras:

a) infecção de programas;

b) infecção de *boot*;

c) infecção de macro;

d) infecção de *autorun*;

e) infecção por *phishing*;

f) infecção combinada.

Malware.
http://pt.wikipedia.org/wiki/Malware

A Figura 3.1 mostra uma árvore de decisão usada para classificar os *malwares*.

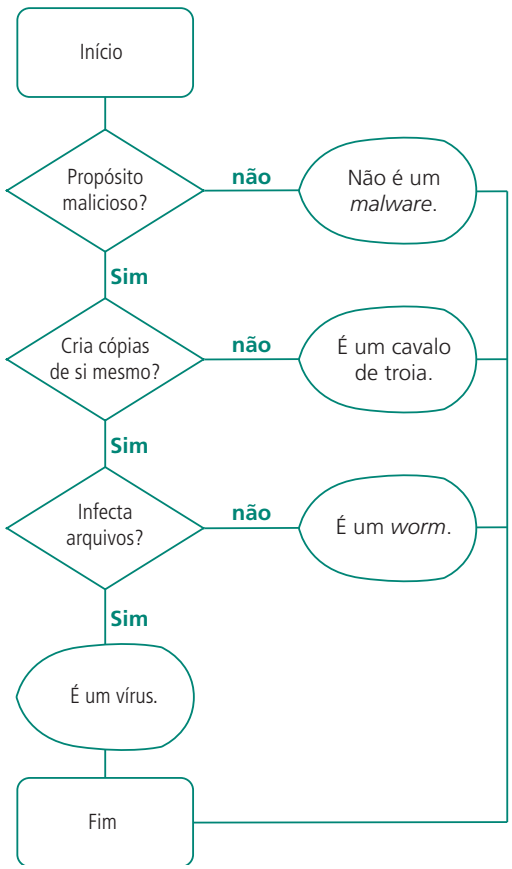


Figura 3.1: Árvore de decisão para classificação de um *malware*
Fonte: Adaptado de Microsoft (2004)

Nos item a seguir são mostrados mais detalhes a respeito dos *malwares*.

3.3 Vírus de computador

Os vírus de computador, semelhantes a um vírus da natureza, são desenvolvidos por programadores com a intenção de infectar sistemas operacionais e espalhar cópias de si mesmos para outros sistemas.

De modo geral, uma infecção por vírus de computador pode diminuir o desempenho do equipamento, destruir ou furtar informações do usuário e impedir o acesso a sítios e serviços de internet.

3.3.1 Classificação

Os vírus de computador compartilham outra característica com os vírus da natureza: a necessidade de um hospedeiro para se multiplicarem. Um hospedeiro é um recurso ou um serviço associado aos computadores. Além disso, uma infecção por vírus não acontece sem a ação do usuário do sistema. Os vírus se classificam de acordo com os meios de infecção e propagação descritos a seguir.

3.3.1.1 Infecções de programas

Nesse modo, os vírus de computador procuram incorporar seu código malicioso em programas legítimos; assim, sempre que um programa infectado é executado pelo usuário, o código do vírus também se executa, sem que o usuário perceba, aumentando a infecção do sistema.

Em geral, a infecção acontece quando o usuário executa um programa infectado, contido em CDs, DVDs ou *Pen drives*, recebidos por *e-mail* ou copiados da internet.

As principais fontes de infecção são os programas terminados com extensões *.bat, *.cmd, *.com, *.dll, *.exe, *.pif, *.scr, *.url, *.vbe, *.vbs e *.ws.

A Figura 3.2 mostra um programa infectado por vírus. O vírus de computador incorpora seu código ao final do programa e acrescenta um ponteiro X no início do hospedeiro. No final do código malicioso há um ponteiro Y que aponta para o início do código do programa hospedeiro.

Figura 3.2: Infecção de programas

Fonte: Adaptado de *PC-cillin Virus Immune System User's Guide*

Toda vez que o usuário abrir o programa infectado, o sistema operacional irá carregar o programa na memória principal (RAM) e iniciará a execução. Ao iniciar a leitura dos *bytes* do programa, o sistema operacional fará o salto determinado pelo ponteiro X, executará o código do vírus, fará o salto determinado pelo ponteiro Y e só então o programa original será executado.

Quando o computador está contaminado por vários tipos de infectores de arquivos, a execução fica mais complexa, pois cada vírus irá incorporar seu próprio código ao final do programa, acrescentando mais e mais ponteiros até o sistema entrar em colapso.

Atualmente, a disseminação de vírus de computador através de infectores de programas não é muito eficiente. Por isso, esta técnica tem sido usada apenas para dificultar a remoção de *malwares* de computador.

3.3.1.2 Infecções de *boot*

Nesse modo, os vírus de computador procuram incorporar seu código malicioso nos primeiros 512 *bytes* de um disco rígido. Essa região é conhecida por *Master Boot Sector* (MBR) e é responsável pelo registro e qualificação das partições contidas no disco.

Partição. http://pt.wikipedia.org/wiki/Parti%C3%A7%C3%A3o

O MBR é uma área muito importante, pois é lido sempre que o computador é iniciado ou reiniciado. Um vírus de *boot* se propaga sempre que um disquete é inserido na unidade de disco flexível de um computador infectado. Se essa mídia for usada para o *boot* em outro computador, ou o computador for iniciado inadvertidamente com o disquete na unidade, um novo sistema se infecta, reiniciando o ciclo.

Boot. http://pt.wikipedia.org/wiki/Boot

A Figura 3.3 mostra uma infecção por vírus de *boot*. Normalmente, a MBR apontaria para o início do sistema operacional a ser carregado na memória do computador. O vírus altera a MBR, fazendo-a apontar para o código do vírus (ponteiro X), que se encontra no disco rígido. Após o vírus ser carregado na memória principal (RAM), o ponteiro Y indica o início do sistema operacional, que é carregado normalmente.

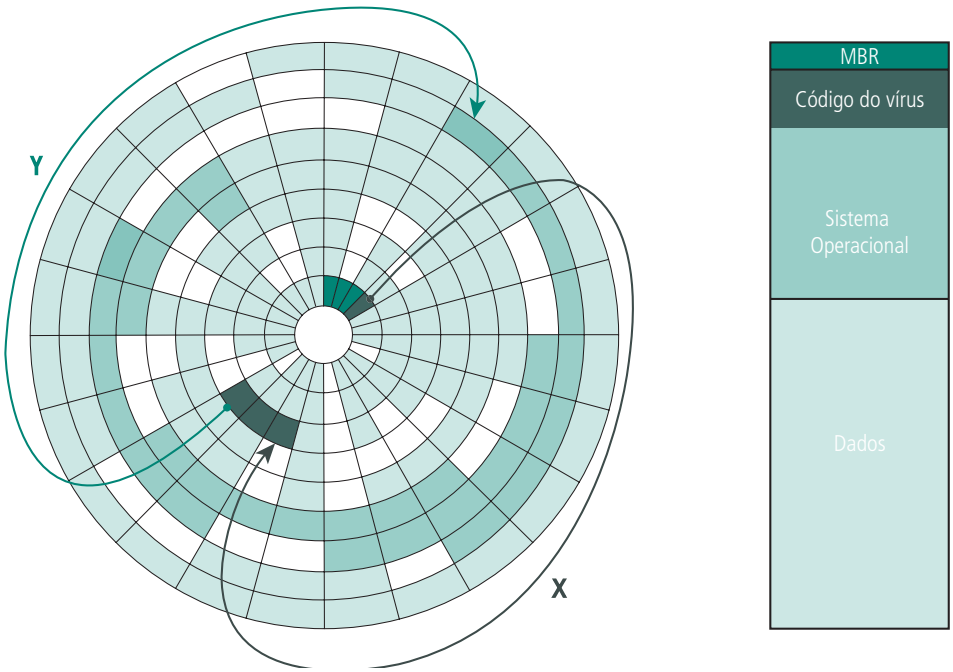


Figura 3.3: Infecção de *boot*

As infecções de *boot* eram muito comuns na era pré-internet, quando a troca de arquivos acontecia principalmente por meio de disquetes, apesar de, em tese, vírus de *boot* também poderem ser escritos para infectar CDs ou DVDs, no momento de sua gravação.

Atualmente, a facilidade de detecção desses *malwares* por programas antivírus associados à característica de uma única gravação dessas mídias compactas tornou pouco eficiente a disseminação através de infectores de *boot*.

3.3.1.3 Infecções de macros

Nesse modo, os vírus de computador procuram incorporar seu código malicioso em arquivos de documentos (textos e planilhas). Certos pacotes *softwares* para escritório oferecem um conjunto de comandos que podem ser executados automaticamente, chamado *macro*. Atualmente, a linguagem de macro mais difundida no mundo é o *Microsoft Visual Basic for Applications* (VBA).

O VBA é uma linguagem poderosa, sendo capaz de manusear e controlar praticamente todos os aspectos da aplicação que editam os documentos.

VBA. http://pt.wikipedia.org/wiki/Visual_Basic_for_Applications

Os infectores de macros aproveitam-se do potencial desse tipo de linguagem para se disseminarem rapidamente; afinal, os documentos têm muito mais mobilidade que mídias inteiras. Basta que se abra um documento contaminado para que a infecção se espalhe pelos demais documentos contidos no computador.

Os infectores de macro tornaram-se a primeira categoria de *malwares* independente de sistemas operacionais. Existem editores de textos construídos para serem executados em plataformas diferentes, como por exemplo, *Microsoft Windows* e *Apple Mac OS X*. Desse modo, um vírus de macro pode infectar e causar danos em mais sistemas, pois o número de vítimas é maior.

Mac OS X. http://pt.wikipedia.org/wiki/Mac_OS_X

Atualmente, devido ao esforço das companhias desenvolvedoras de *softwares* para escritório, o risco de infecções através de vírus de macro tornou-se muito menor, porém ainda exige cautela dos usuários.

3.3.1.4 Infecções de *autorun*

As infecções de *autorun* são similares às infecções de *boot*. Exploram uma funcionalidade dos sistemas operacionais, chamada execução automática, que executa um ou mais programas assim que uma mídia (*pen drives*, CDs ou DVDs) é inserida no computador.

O *autorun* é um recurso que facilita o trabalho do usuário, quando este necessita instalar programas ou executar recursos multimídia (sons, vídeos etc.) a partir de *pen drives*, CDs ou DVDs. Porém tem sido muito utilizado para disseminar automaticamente toda a sorte de *malwares*.

Qual é a diferença entre reprodução automática e execução automática? http://windows.microsoft.com/pt-PT/windows-vista/Whats-the-difference-between-AutoPlay-and-autorun

As infecções de *autorun* têm obtido muito sucesso com o advento e barateamento dos *pen drives*, que se tornaram um meio muito prático de carregar arquivos de um computador para outro.

A contaminação acontece quando o usuário conecta um *pen drive* em um sistema infectado. O vírus que se encontra na memória principal (RAM) do computador acrescenta um arquivo chamado "autorun.inf", responsável por chamar a execução de um programa. Este programa carrega o código malicioso do vírus. Algumas vezes, este programa é gravado no diretório-raiz do *pen drive;* outras, numa pasta chamada *Recycler* ou *Recycled*. A contaminação se efetiva assim que o *pen drive* é conectado em outro computador.

A Figura 3.4 mostra o conteúdo de um *pen drive* contaminado por uma infecção de *autorun*. Essa contaminação é indicada pelo fato de o sistema operacional *Microsoft Windows XP*, cuja janela é mostrada na figura, não criar a pasta Lixeira (*Recycler*) em dispositivos removíveis.

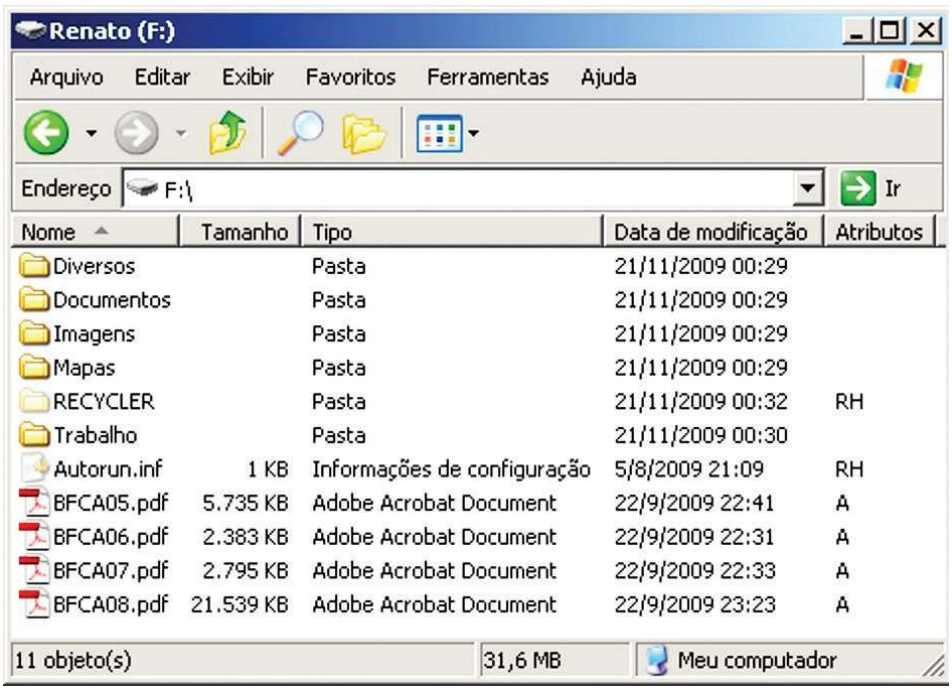


Figura 3.4: Infecção de *autorun*
Fonte: Imagem copiada do *Windows Explorer* de autoria da *Microsoft Corporation*

Ainda que o *Microsoft Windows XP* criasse a pasta Lixeira (*Recycler*), ela jamais estaria com o atributo R, que significa que a pasta é somente leitura. Uma pasta com esse atributo não poderia receber os arquivos que são excluídos pelo usuário.

Microsoft acaba com *AutoPlay* no *Windows*.
http://info.abril.com.br/noticias/seguranca/microsoft-acaba-com-autoplay-no-windows-15092009-4.shl

Em 25 de agosto de 2009, a *Microsoft Corporation* decidiu extinguir a funcionalidade de execução automática em seus sistemas operacionais para conter a disseminação de vírus de computador.

3.3.1.5 Infecções por *phishing*

O *phishing* é a técnica que faz o usuário trazer para seu computador um programa infectado por vírus e instalá-lo em seu próprio sistema.

A técnica funciona através do oferecimento de um conteúdo de interesse do usuário. Ao buscar esse conteúdo, tudo o que o usuário obtém é a infecção de seu computador. O conteúdo de interesse do usuário pode chegar das seguintes formas:

a) *e-mail*: são oferecidos ao usuário produtos com preços muito abaixo dos praticados no mercado, facilidades para que adquira medicamentos controlados, avisos que o usuário tem processos pendentes na Justiça, avisos indicando que seu CPF será cancelado, avisos indicando a existência de cartões virtuais de felicitação, mensagens com fotos digitais anexas de uma suposta admiradora, etc.;

b) mensagens instantâneas: durante conversas *on-line*, o usuário é surpreendido por convites para visitar *links* supostamente oferecidos por seus contatos, com assuntos os mais diversos;

c) recados no *Orkut*: o usuário é convidado a clicar em *links* contidos em recados deixados por seus contatos. Os recados versam sobre eventos para os quais o usuário não foi e onde ele pode ver as fotos, admiradores secretos, piadas, fofocas, notícias, convites para ingresso em comunidades, etc.;

d) páginas *Web*: o usuário é levado a acessar *links* para páginas falsas, clonadas de páginas legítimas. Uma vez convencido, o usuário pode fornecer dados sigilosos, tais como números de contas e senhas bancárias, dados do cartão de crédito ou outras informações pessoais. Essas informações podem levar a fraudes, prejuízos financeiros e até mesmo roubo de identidade.

e) resultado em sítios de busca: o usuário faz uma busca na internet e um dos resultados exibe um *link* que aponta para o código malicioso.

Em todos os casos acima, o *link* oferecido aponta para programas que são baixados e executados, infectando o computador do usuário.

Phishing Scam – A fraude inunda o correio eletrônico. http://www.mhavila.com.br/topicos/seguranca/scam.html

3.3.1.6 Infecções combinadas

Infecções combinadas são aquelas que utilizam várias técnicas de propagação para se espalharem para o maior número possível de computadores. São os casos mais comuns.

Por exemplo, uma infecção que chega por um *pen drive* pode furtar a senha do *Orkut* do usuário e começar a mandar recados contendo *links* para páginas falsas de um banco e induzindo seus contatos a fornecer seus dados pessoais, levando um grande número de pessoas a se tornarem vítimas de golpes financeiros.

3.4 Cavalo de troia

Os cavalos de troia (*trojans*) são a segunda das espécies de *malwares*. São programas aparentemente legítimos que secretamente executam funções prejudiciais ao sistema e por vezes ao usuário.

Esses programas aparentemente legítimos podem estar disponíveis em sítios de *downloads*, na forma de editores de imagens, visualizadores de documentos, programas antivírus, jogos de computador, protetores de tela (*screensavers*), etc.

Os cavalos de troia também podem chegar até o computador do usuário através de infecções por *phishing*. Por isso, o usuário tem de ser muito criterioso com os programas que baixa para seu computador e com os *links* que recebe.

A-Z

Backdoor
Significa porta dos fundos. São canais de acesso remoto a sistema operacional, via internet. Quando são abertas, permitem a um atacante ter controle completo da máquina do usuário

Por exemplo, o usuário encontra na internet um editor de fotos digitais gratuito. Faz o *download* desse programa e o instala em seu computador. Passa a usar esse programa retocando imagens, acrescentando efeitos e outras funções características de um editor de fotos digitais. Porém, o que o usuário não sabe é que esse editor de imagens contém um código malicioso capaz de abrir ***backdoors*** no sistema, permitindo ao atacante:

a) furtar informações do usuário, tais como fotos, vídeos, gravações, documentos e informações pessoais ou sigilosas;

b) hospedar arquivos ilegais na máquina invadida, tais como imagens ou vídeos de pedofilia, *malwares*, informações pessoais de outros usuários etc.;

c) apagar e alterar arquivos do usuário;

d) controlar remotamente via internet o computador do usuário, usando-o como ponte para ataques de negação de serviço e distribuição de *spam*;

e) ativar programas *spywares* para coletar furtivamente informações comportamentais do usuário, tais como o que ele compra, quais sítios de internet ele visita, para quem ele manda ou de quem ele recebe *e-mails*;

f) instalar ***keyloggers*** e ***screenloggers***;

g) invadir a privacidade do usuário, ativando *webcam* ou microfone sem o usuário saber;

h) imprimir documentos na impressora do usuário, acabando com a tinta e estragando papéis;

i) instalar *rootkits* – programas que ajudam a manter um ataque bem-sucedido, escondendo as evidências de sua instalação no computador;

j) programar o envio de *spams* para milhares de contas de *e-mail*.

Em geral, os cavalos de troia têm as seguintes características:

a) não infectam outros programas;

b) não disseminam cópias de si mesmos;

c) são compostos de um único arquivo;

d) são explicitamente executados pelo usuário ou ficam residentes na memória principal (RAM);

e) necessitam que os computadores invadidos estejam conectados à internet.

A-Z

Keyloggers
São programas de computador que trabalham capturando e armazenando os caracteres digitados em um teclado com a finalidade de descobrir senhas de acesso do usuário. Alguns desses programas são capazes de enviar os dados capturados para servidores na internet sob controle de criminosos.

Screenloggers
São programas de computador similares aos *keyloggers*, porém, ao invés de capturarem o que é digitado, trabalham coletando e armazenando pequenas imagens copiadas da tela do computador nas áreas dos cliques do *mouse*.

Assista ao filme "Troia", do diretor Wolfgang Petersen, lançado em 2004, para conhecer a origem do termo cavalo de troia

3.5 *Spywares*

Os *spywares* (*softwares* espiões) são a terceira das espécies de *malwares*. São programas criados com a intenção de coletar informações do usuário, tais como o tipo de *websites* que visita, produtos que costuma comprar, assuntos que lhe interessam, horários de acesso, tipo de *e-mails* que recebe etc., e enviá-las para uma entidade externa. E o mais importante: sempre sem o consentimento ou o conhecimento do usuário espionado.

Existem dois tipos básicos de *spyware*:

a) coletor de informações bancárias: especializado em capturar números de conta, senhas de acesso, dados de cartões de crédito etc. Seu maior perigo é a exposição do usuário a fraudes financeiras;

b) coletor de informações comportamentais: especializado em capturar o tipo de sítio na internet que o usuário visita, produtos que ele costuma comprar, assuntos que lhe interessam, horários de acesso, tipo de *e-mails* que envia e recebe, tipo de pagamento mais usado (cartão de crédito, de débito ou boleto bancário).

É importante saber que nem toda coleta de informações do usuário é ilegal. Algumas empresas disponibilizam serviços na internet (*webmails, blogs, fotoblogs,* editores de texto, redes sociais, etc.) a qualquer pessoa, desde que essa pessoa aceite os termos de prestação de serviço ou as políticas de privacidade. Nesses documentos constam cláusulas pelas quais o usuário autoriza expressamente a atividade de coleta de suas informações.

Central de Informações sobre Privacidade.
http://info.yahoo.com/privacy/br/all/

Spyware.
http://pt.wikipedia.org/wiki/Spyware

Normalmente, os *spywares* são instalados quando o usuário é vítima de *phishing*. Após a contaminação, esses programas ficam recolhendo informações do usuário e assim que o computador é conectado à internet, essas informações são enviadas para sistemas especializados em condensar, processar e tirar proveito dessas informações comercialmente úteis.

Resumo

Danos são prejuízos sofridos pela informação. Podem ser lógicos, físicos ou pessoais. *Malwares* são programas de computador desenvolvidos para destruir, corromper ou usar indevidamente informações. Permitem controlar remotamente um computador. Os principais tipos vistos nesta aula são os vírus, cavalos de troia e *spywares*. Os vírus de computador necessitam de um hospedeiro e da ação do usuário do sistema para se multiplicarem. Os cavalos de troia aparentam ser legítimos, porém executam funções prejudiciais ao sistema secretamente. Os *spywares* coletam informações comportamentais do usuário e as envia para uma entidade externa, sem o consentimento ou o conhecimento da vítima.

Atividades de aprendizagem

1. Sabendo que existem três tipos de danos lógicos, descreva dois exemplos de situações que podem resultar em cada um deles.

2. Pesquise na internet e confeccione um texto descrevendo como o conceito de *adware* corrompeu-se no conceito de *spyware*.

Poste os arquivos com suas respostas e justificativas no AVEA.

Aula 4 – Problemas enfrentados pela SI - *ransomwares, worms* e SPAM

Nós precisamos ter sorte apenas uma vez. Você precisa ter sorte o tempo todo.

Exército Republicano Irlandês (IRA) à Margaret Thatcher, após ela ter sobrevivido a um atentado à bomba.

Objetivos

Identificar os principais problemas enfrentados pela Segurança da Informação.

Reconhecer esses problemas como ameaças aos ativos de informação.

4.1 *Ransomwares*

Os *ransomwares* são a quarta espécie de *malware*. Seu funcionamento implica no sequestro dos dados do usuário ou mesmo no bloqueio de acesso ao computador.

No primeiro caso, o *ransomware* criptografa o todo ou uma parte do disco rígido do usuário, impedindo o seu acesso. No segundo, muda as senhas de *login* do sistema operacional. Após o sequestro, informa à vítima que seus dados apenas serão liberados se a pagar um resgate por eles.

Os *ransomwares* são ferramentas de extorsão. Após o pagamento, o usuário recebe uma senha que permite recuperar seus dados.

Piratas virtuais anunciam "sequestro" de dados e exigem US$ 10 milhões nos EUA. http://www1.folha.uol.com.br/folha/informatica/ult124u561249.shtml

Falso antivírus cobra US$ 50 para liberar arquivos 'sequestrados'. http://g1.globo.com/Noticias/Tecnologia/0,,MRP1087313-6174,00.html

4.2 *Worms*

Os *worms* (vermes) são a quinta espécie de *malwares*, considerada a mais perigosa. Suas principais características são:

a) alta velocidade de propagação de suas cópias;

b) aproveitar-se de falhas de desenvolvimento em sistemas operacionais, em *softwares* aplicativos e em protocolos de transmissão de dados;

Worms. http://pt.wikipedia.org/wiki/Worm

c) não contaminar programas;

d) não exigir intervenção do usuário para se propagar, disseminando-se automaticamente;

e) fazer uso de técnicas combinadas de infecção para aumentar sua capacidade de propagação.

Sua notável capacidade de disseminação tem provocado a sobrecarga de vários servidores de *e-mail* ao redor do mundo, bem como a diminuição da banda disponível para conexões de dados.

Link sugerido para a origem do termo *spam*: http://www.youtube.com/watch?v=3kjdrl6qjwY

4.3 *Spam*

O *spam* é a atividade de enviar mensagens eletrônicas (*e-mails*) massivamente para usuários que não consentiram e nem solicitaram seu recebimento.

4.3.1 Problemas advindos do *spam*

Segundo o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br), o *spam* afeta os serviços de *e-mail* das seguintes formas:

a) impede o recebimento de *e-mails* legítimos, por ocuparem o espaço que normalmente é limitado pelos provedores de acesso à internet. Uma caixa postal cheia rejeita novos *e-mails* até que o usuário libere mais espaço, apagando os *spams*;

b) desperdiça o tempo do usuário, pois este dedica alguns segundos para ler a mensagem, identificá-la como *spam* e apagá-la de sua caixa postal. Algumas dezenas de *spams* diários consomem preciosos minutos do usuário, todos os dias;

c) aumenta os gastos com conexão à internet, pois os minutos desperdiçados no item anterior forçam o usuário a passar mais tempo conectado para que consiga manter o mesmo rendimento de trabalho. Como quem paga pelo acesso à internet é o usuário vítima do *spam*, cada mensagem não solicitada equivale a alguns centavos de real;

d) diminui a produtividade, pois aumenta o tempo dedicado à leitura de *e-mails*, identificação de *spam* e seleção de mensagens legítimas. Eventualmente, o usuário corre o risco de não ler uma mensagem importante, lê-la com atraso ou apagá-la por engano;

e) expõe o usuário a conteúdo impróprio ou ofensivo, pois o emissor de *spam* não faz nenhuma discriminação de seus destinatários. Assim, é possível, por exemplo, que um jovem menor de idade receba "convites" para gastar sua mesada em cassinos *on-line*;

f) expõe a fraudes, pois o *spam* é comumente utilizado como veículo disseminador de esquemas que tentam induzir o usuário a erro ou instalar programas maliciosos em seu computador – *phishing*. Os *spams* podem conter *links* para páginas clonadas de bancos, nas quais o usuário pode informar os dados de sua conta e senha de acesso.

O *spam* causa ainda um sétimo problema: a lentidão na rede de dados ou na internet, tendo em vista que ocupa parte da banda disponível para conexões de dados.

O *spam* não está restrito às correspondências eletrônicas, podendo se manifestar nos recados do *Orkut*, em fóruns de discussão e mesmo através de janelas *pop-up* em páginas da internet.

12% dos usuários respondem a *spams*.
http://br.tecnologia.yahoo.com/article/20072009/7/tecnologia-12-dos-usuarios-mail-respondem.html

Spam responde por 97% das mensagens de *e-mail*, diz *Microsoft*.
http://g1.globo.com/Noticias/Tecnologia/0,,MRP1077797-6174,00.html

Spam.
http://www.linhadefensiva.org/2005/11/spam/

Mineração de dados.
http://pt.wikipedia.org/wiki/Data_mining

4.4 Por que existem tantos problemas?

Há um grande mercado para as informações coletadas dos usuários, tanto para as obtidas legalmente com para as obtidas ilegalmente.

As informações coletadas legalmente fornecem às empresas subsídios que alimentam grandes sistemas de mineração de dados, permitindo que a empresa conheça os gostos comuns das pessoas, quais as tendências de consumo, se uma campanha de *marketing* está dando resultado, etc.

No outro lado, as informações obtidas ilicitamente têm o único condão de tirar dinheiro do usuário descuidado com suas senhas, contas bancárias e cartões de crédito ou de usar o computador desse usuário como uma estação-zumbi, promovendo extorsões através de ataques de negação de serviço a servidores de empresas na internet (ou as empresas pagam, ou os malfeitores tiram o servidor de funcionamento).

Há ainda um mercado para esse tipo de informações coletadas, no qual quanto maior a exclusividade da informação, maior o seu valor, como por exemplo, listas com milhares de dados de cartões de crédito, obtidas após invasão da rede de dados das empresas que gerenciam esse serviço.

Dmitry Samosseiko *What is it & why should you care.* http://www.sophos.com/

Hackers rake in fortune selling fake antivirus software. http://www.smh.com.au/news/technology/security/hackers-rake-in-fortune-selling-fake-antivirus-software/2008/11/05/1225560902070.html

Um computador invadido se presta ainda para mascarar a origem e a identidade do invasor, permitir o armazenamento clandestino de dados, disseminação de *spam*, contaminação e invasão de outros computadores, etc.

Com os dados bancários furtados das vítimas, os criminosos podem fazer transferências de valores entre contas, pagamento de faturas de terceiros, compras em lojas *on-line,* etc.

Resumo

Malwares são programas de computador desenvolvidos para destruir, corromper ou usar indevidamente informações. Permitem controlar remotamente um computador. Os principais tipos vistos nesta aula são os *ransomwares* e *worms*. Os *ransomwares* sequestram os dados do usuário ou bloqueiam o acesso ao computador. Os *worms* (vermes) são espécie mais perigosa de *malwares*, propagam-se rápida e automaticamente, aproveitando-se de falhas em *softwares* e sem contaminar programas. Os *spams* são mensagens eletrônicas (*e-mails*) enviadas massivamente para milhares de usuários que nunca autorizaram seu recebimento. No final de tudo, a maioria dos *malwares* e o *spam* existem apenas para ganhar dinheiro ou tirar dinheiro dos outros, desonestamente.

Atividades de aprendizagem

1. Tendo em mente os conceitos de *ransomwares*, *worms* e *spam*, responda: Como indivíduos mal-intencionados ganham dinheiro com cada um deles?

2. Pesquise na internet e confeccione um texto descrevendo o que são, como funcionam e como os *web bugs* se relacionam com o *spam*.

Poste os arquivos com suas respostas e justificativas no AVEA.

Aula 5 – *Softwares* de SI - gerenciadores de senha, de *backup* e ferramentas de criptografia

Se você acha que a tecnologia pode resolver seus problemas de segurança, então você não entende nem de segurança nem de tecnologia.

Bruce Schneier

Objetivos

Conhecer os conceitos básicos sobre o tema *softwares* de Segurança da Informação.

Proceder a estudos de caso em cada um dos tipos de ferramentas apresentadas.

5.1 Introdução

Os *softwares* de SI são as ferramentas que permitem ao usuário aplicar os princípios da Segurança da Informação em seu dia a dia e no dia a dia da empresa.

Nesta aula são abordados os principais tipos de ferramentas, seus conceitos básicos e um estudo de caso para cada uma delas. Entretanto, não serão abordadas todas as funcionalidades disponíveis, mas somente as funcionalidades principais.

Os softwares foram escolhidos por estarem licenciados sob a forma de freewares, estarem disponíveis para download, serem atualizados com frequência e estarem entre os preferidos nas várias listas de sugestões pesquisadas.

Freeware.
http://pt.wikipedia.org/wiki/Software_gratuito

5.2 Gerenciadores de senha

São ferramentas que possibilitam ao usuário gerenciar de modo seguro a infinidade de senhas advindas da atual revolução digital.

As senhas estão por todo lado. São senhas para *login* na rede de dados do trabalho, senhas de *e-mail*, senhas de acesso a redes sociais virtuais, senhas de banco, senhas do cartão de crédito, etc. É natural que o usuário não consiga lembrar-se de todas. Entretanto, o usuário não se pode dar ao luxo de

anotar essas senhas em papel, nem dentro de arquivos no computador, pois estariam vulneráveis a pessoas mal-intencionadas ou a bisbilhoteiros.

Outro erro comum é utilizar a mesma senha de acesso em vários serviços *on-line*. Basta que o atacante descubra uma delas para que todas as demais sejam expostas.

A-Z

Criptografia
É a ciência que trata das técnicas de transformação através das quais a informação pode ser protegida de pessoas não autorizadas.

Os gerenciadores de senha armazenam de modo seguro a lista de senhas de serviço e a respectiva lista de nomes de usuário. O usuário deve apenas lembrar uma senha-mestre, que permite acesso às senhas **criptografadas** pelo gerenciador.

5.2.1 Estudo de caso – *Password Safe*

O *Password Safe* é uma ferramenta de código aberto, criada por Bruce Schneier. Atualmente, o projeto *Password Safe* é ganhador de vários prêmios internacionais e está hospedado no sítio **http://passwordsafe.sourceforge.net/**. Ainda não possui versão traduzida para o português brasileiro.

Twofish.
http://www.gta.ufrj.br/~natalia/SSH/twofish.html

Software livre.
http://pt.wikipedia.org/wiki/Software_livre

A segurança do *Password Safe* está no algoritmo de encriptação *Twofish*, escolhido por ser *software* livre e ter alto desempenho. A seguir, são mostradas suas principais funcionalidades.

5.2.1.1 Criando e abrindo um banco de dados para senhas

Para criar um banco de dados de senha, execute o *Password Safe*. Em seguida, clique no botão "*New Database*", mostrado na Figura 5.1

Figura 5.1: Janela inicial
Fonte: Imagem copiada do *PasswordSafe*, de autoria do *Password Safe Project*

Abrir-se-á uma janela do *Windows Explorer* solicitando que o usuário indique o nome e a localização de seu banco de dados de senha (Figura 5.2). Após definidos, é necessário clicar no botão "Salvar".

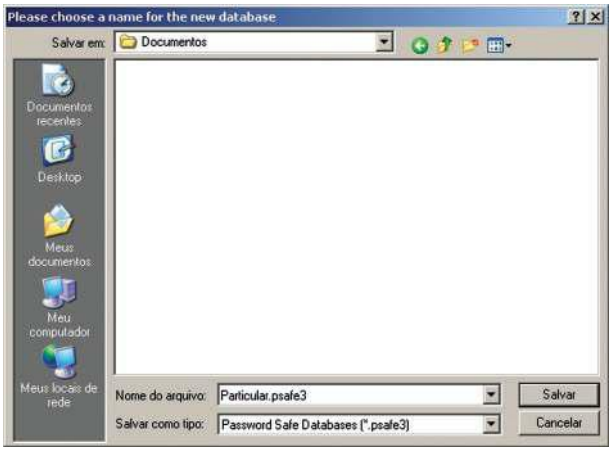


Figura 5.2: Nome e local do arquivo

Fonte: Imagem copiada do *Windows Explorer*, de autoria da *Microsoft Corporation*

Em seguida, surgirá uma janela solicitando que o usuário defina a "*Safe Combination*", ou seja, a senha-mestre (Figura 5.3). Essa é a única senha que o usuário jamais pode perder.

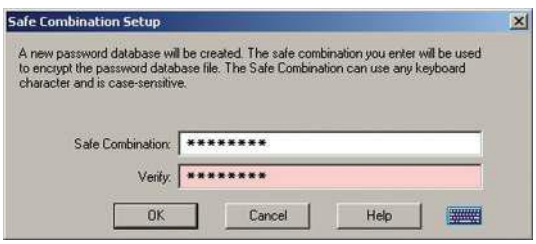


Figura 5.3: *Safe Combination*

Fonte: Imagem copiada do *PasswordSafe,* de autoria do *Password Safe Project*

O usuário tem opção de utilizar o teclado virtual para digitar a senha-mestre. O teclado virtual torna-se disponível ao se clicar no ícone do teclado azul da Figura 5.3. Abaixo é mostrado o teclado virtual do *Password Safe* (Figura 5.4).

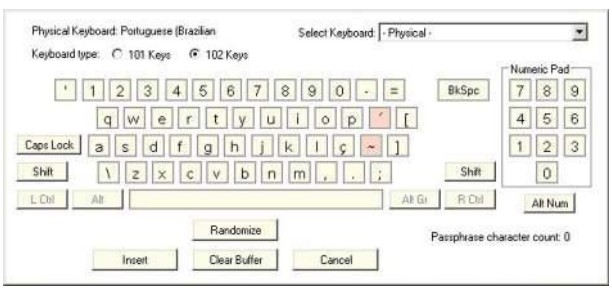


Figura 5.4: Teclado virtual

Fonte: Imagem copiada do *PasswordSafe,* de autoria do *Password Safe Project*

Caso o programa considere que a senha-mestre digitada é muito fraca, o usuário tem duas opções: continuar assim mesmo, clicando no botão "Sim", ou tentando uma nova senha, após clicar no botão "Não" (Figura 5.5).

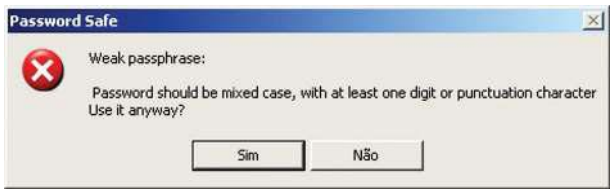


Figura 5.5: Alerta de senha fraca

Fonte: Imagem copiada do *PasswordSafe,* de autoria do *Password Safe Project*

Para abrir um banco de dados de senhas existente, basta clicar no botão "..." (Figura 5.1) e indicar o local e o nome do arquivo, na janela do *Windows Explorer*. Por padrão, é sempre exibido o nome do último arquivo utilizado. Os arquivos do *Password Safe* têm extensão ".psafe3".

5.2.1.2 Adicionando e excluindo entradas do banco de dados de senhas

O *Password Safe* chama de entrada cada uma das senhas de serviço que armazena em seu banco de dados de senhas.

Para adicionar uma entrada a partir da janela principal, é necessário clicar no menu "*Edit*" e na opção "*Add entry*" (Figura 5.6).

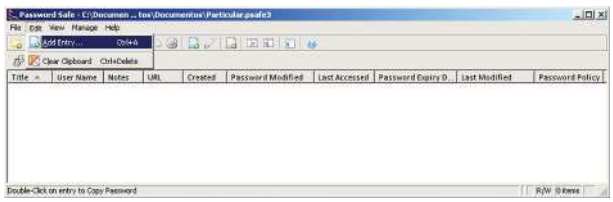


Figura 5.6: Nova entrada

Fonte: Imagem copiada do *PasswordSafe,* de autoria *do Password Safe Project*

É aberta uma nova janela (Figura 5.7) onde o usuário deve informar os dados da entrada, tais como grupo, nome da entrada, nome de usuário, senha, *link* do sítio e observações.

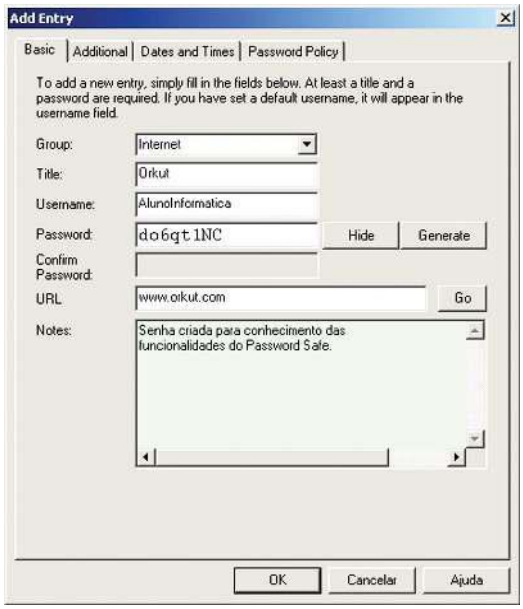


Figura 5.7: Dados da entrada

Fonte: Imagem copiada do *PasswordSafe,* de autoria do *Password Safe Project*

Uma vez inseridos os dados, basta clicar no botão "Ok" e a entrada será adicionada ao banco de dados de senhas (Figura 5.8). Esse procedimento deve ser repetido para cada uma das senhas de serviço que o usuário possui. O *Password Safe* admite centenas de entradas em um banco de dados de senha.

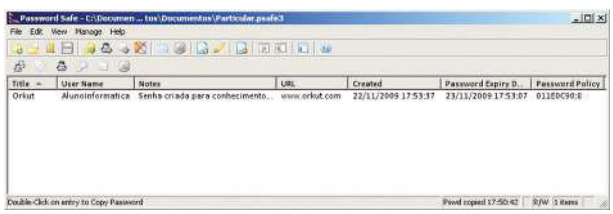


Figura 5.8: Lista de entradas

Fonte: Imagem copiada do *PasswordSafe,* de autoria do *Password Safe Project*

Para excluir uma entrada, basta selecioná-la e pressionar a tecla "*Delete*".

A Figura 5.9 mostra como ficam os caracteres do arquivo criptografado Particular.psafe3.

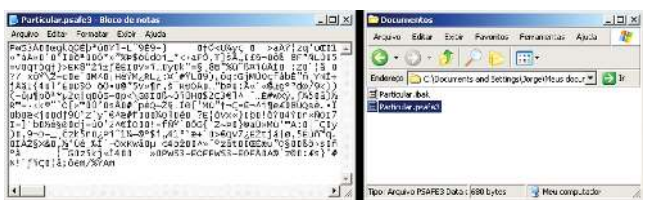


Figura 5.9: Arquivo encriptado

Fonte: Composição de imagens copiadas do Bloco de Notas e do *Windows Explorer*, ambas de autoria da *Microsoft Corporation*

5.3 Gerenciadores de *backup*

São ferramentas que permitem automatizar a criação e atualização de cópias de segurança (*backup*). Os gerenciadores de *backup* podem ser utilizados de forma preventiva ou corretiva.

No modo preventivo, essas ferramentas confeccionam as cópias de segurança, antes da ocorrência do dano. No modo corretivo, a informação foi perdida e a ferramenta se encarrega de auxiliar no processo de recuperação.

Cópia de segurança. http://pt.wikipedia.org/wiki/C%C3%B3pia_de_seguran%C3%A7a

Entre as funcionalidades mais importantes em um gerenciador de *backup* estão: varrer os arquivos contra *malwares* antes do armazenamento, compactação dos dados, envio dos arquivos via rede de dados ou *e-mail*, permitir agendamento, criação de perfis, etc.

5.3.1 Estudo de caso – *SyncBackup*

O *SyncBackup* é uma ferramenta *freeware*, criada pela empresa *2BrightSparks Pte Ltd*. e disponibilizada na internet no sítio **http://www.2brightsparks.com/**, inclusive no idioma português brasileiro.

O *SyncBackup* permite a criação de perfis tanto para execução de *backups* como para a restauração de cópias de segurança. A seguir, são mostradas suas principais funcionalidades.

O *SyncBackup* trabalha com o conceito de perfis. Cada perfil contém todas as informações que caracterizam uma rotina de *backup*, tais como pasta de origem, pasta de destino, filtros, opções de compactação, etc.

Para criar um perfil a partir da janela principal, basta clicar no menu "Perfil" e em seguida na opção "Novo" (Figura 5.10).

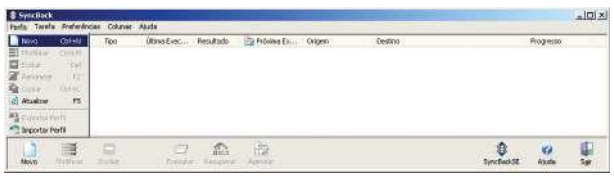


Figura 5.10: Criando um perfil
Fonte: Imagem copiada do *SyncBackup,* de autoria da *2BrightSparks Pte Ltd*

Em seguida, deve ser definido o tipo do *backup*. Neste estudo, será trabalhada a opção "Sincronização" (Figura 5.11).

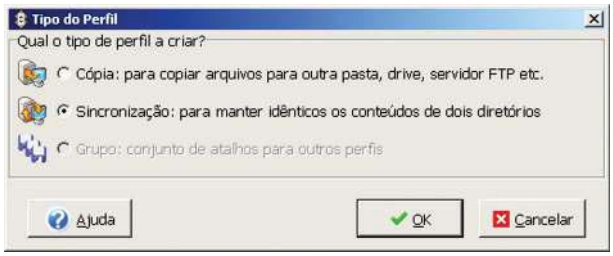


Figura 5.11: Tipo de perfil

Fonte: Imagem copiada do *SyncBackup,* de autoria da *2BrightSparks Pte Ltd*

Após clicar no botão "Ok", o *SyncBackup* solicita um nome para o perfil (Figura 5.12).

Figura 5.12: Nome do perfil

Fonte: Imagem copiada do *SyncBackup,* de autoria da *2BrightSparks Pte Ltd*

O programa então passa às configurações do perfil. É mandatório que o usuário indique a pasta de origem (que contém os dados) e a pasta de destino (que receberá o *backup*). Na opção "Sub-dirs" é recomendado que se escolha a opção "Incluir todos os subdiretórios e seus arquivos (e usar o filtro de diretório)", pois é a mais completa. Na guia "Simples" é apresentada uma configuração padrão, sem muitos detalhes (Figura 5.13). Em geral, essas configurações bastam para a maioria dos usuários.

Figura 5.13: Configuração do perfil: simples

Fonte: Imagem copiada do *SyncBackup,* de autoria da *2BrightSparks Pte Ltd*

A Figura 5.14 mostra a guia "Avançado", onde se definem a prioridades de sobrescrição de arquivos. A sobrescrição do arquivo pode estar relacionada à origem/destino, à condição de mais velho/mais novo, à condição de maior/menor, à inexistência do arquivo na origem e à inexistência do arquivo no destino.

É ideal que, em um *backup*, os arquivos mais novos sobrescrevam os mais velhos, que se um arquivo está somente na origem, seja copiado para o destino e que se um arquivo está somente no destino, seja excluído.

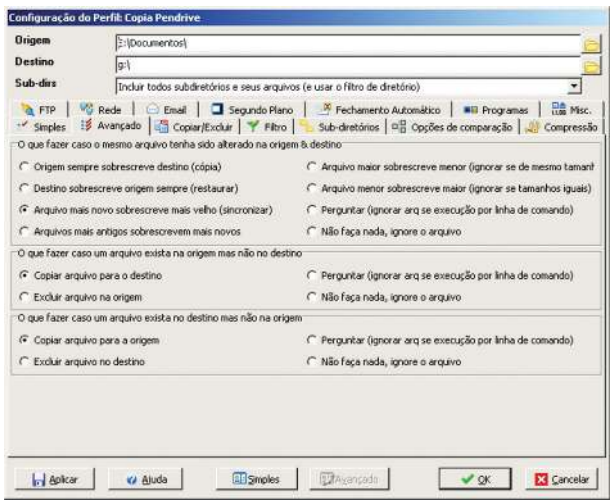


Figura 5.14: Configuração do perfil: avançado

Fonte: Imagem copiada do *SyncBackup,* de autoria da *2BrightSparks Pte Ltd*

A Figura 5.15 mostra a guia "Copiar/Excluir", onde são definidas questões de desempenho (opção "Não usar o *Windows shell* para copiar ou excluir arquivos") e questões de integridade (opção "Verificar se cópia ok").

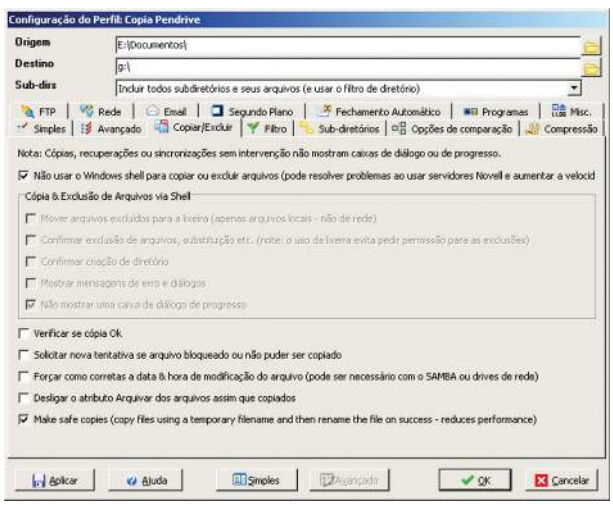


Figura 5.15: Configuração do perfil: Copiar/Excluir

Fonte: Imagem copiada do *SyncBackup,* de autoria da *2BrightSparks Pte Ltd*

A Figura 5.16 mostra a guia "Filtro", onde são definidos quais arquivos e quais pastas serão incluídos ou não no *backup*. É interessante que se excluam pastas do sistema operacional, pouco relacionadas com os arquivos de um *backup*. Deve-se excluir arquivos temporários também, pois isso ajuda a reduzir espaço em disco, necessário para armazenar o *backup*.

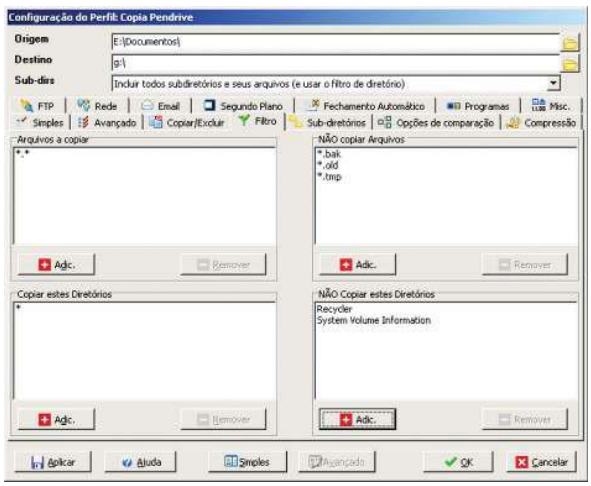


Figura 5.16: Configuração do perfil: filtro

Fonte: Imagem copiada do *SyncBackup,* de autoria da *2BrightSparks Pte Ltd*

A Figura 5.17 mostra a guia "Compressão", onde são definidas as opções de compactação dos arquivos de *backup*. O *Syncbackup* permite configurar se deve ser gerado um único arquivo compactado ou se cada arquivo deve ser compactado separadamente. Permite, ainda, definir uma senha de proteção e o nível de compressão.

A compressão de dados tem algumas limitações, pois não permite mais que 65.535 arquivos em um arquivo compactado e nem que seu tamanho seja superior a quatro *gigabytes*.

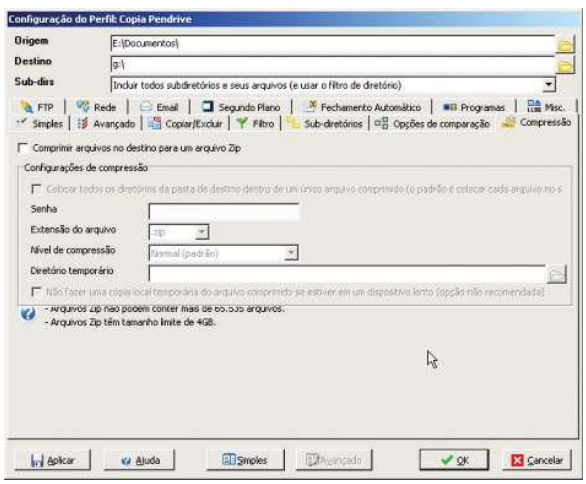


Figura 5.17: Configuração do perfil: compressão

Fonte: Imagem copiada do *SyncBackup*, de autoria da *2BrightSparks Pte Ltd*

FTP.
http://pt.wikipedia.org/wiki/Ftp

Intranet.
http://pt.wikipedia.org/wiki/Intranet

A Figura 5.18 mostra a guia "FTP", onde são definidas as opções do protocolo de transferência de arquivos, tais como nome do servidor, nome de usuário, senha de acesso e dados de conexão com a internet.

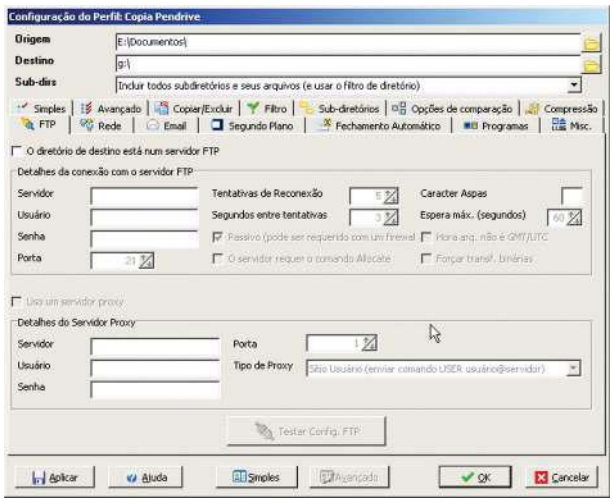


Figura 5.18: Configuração do perfil: FTP

Fonte: Imagem copiada do *SyncBackup*, de autoria da *2BrightSparks Pte Ltd*

A Figura 5.19 mostra a guia "Rede", onde são definidas as opções de envio dos arquivos de *backup* para pastas de uma Intranet, tais como local da pasta, nome de usuário e senha.

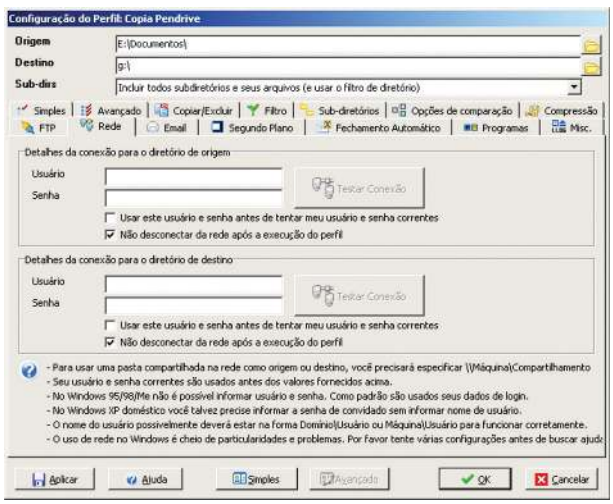


Figura 5.19: Configuração do perfil: rede

Fonte: Imagem copiada do *SyncBackup*, de autoria da *2BrightSparks Pte Ltd*

Terminadas as configurações, a janela principal do *SyncBackup* mostra uma lista com os perfis criados pelo usuário (Figura 5.20). A partir dessa janela é possível excluir, modificar ou executar um perfil criado.

Figura 5.20: Perfis criados pelo usuário

Fonte: Imagem copiada do *SyncBackup*, de autoria da *2BrightSparks Pte Ltd*

5.4 Ferramentas de criptografia

São ferramentas que possibilitam ao usuário trabalhar com criptografia de dados, garantindo que as informações serão mantidas confidenciais. Existem basicamente três tipos de ferramentas de criptografia:

Criptografia de chave pública.
http://pt.wikipedia.org/wiki/Criptografia_de_chave_pública

Criptografia de chave privada.
http://pt.wikipedia.org/wiki/Criptografia_Sim%C3%A9trica

a) *softwares* para criptografia de arquivos: encriptam um arquivo ou um conjunto de arquivos, para envio através de redes de dados, *e-mail,* etc.;

b) *softwares* para criptografia de unidades de armazenamento: encriptam partições de discos rígidos ou *pen drives*, protegendo todos os arquivos contidos na unidade;

c) *softwares* para criptografia para transmissão de dados: encriptam comunicações do usuário, conexões de dados, acesso remoto, etc.

É importante que os usuários procurem por *softwares* que utilizem algoritmos de criptografia reconhecidamente seguros pela comunidade científica.

5.4.1 Estudo de caso – *TrueCrypt*

5.4.1.1 Introdução

O *TrueCrypt* é uma ferramenta *freeware*, criada pela *TrueCrypt Foundation* e disponibilizada na internet no sítio **http://www.truecrypt.org/**. Dispõe de suporte multi-linguagem, inclusive para idioma português brasileiro.

Devido à característica dos discos rígidos em manter informações por longos períodos, especialistas da área de segurança da informação têm recomendado o uso de criptografia de disco como a melhor forma de manter a confidencialidade, pois, sem a chave secreta, a única coisa que um atacante pode conseguir, após tentar recuperar informações de um disco rígido descartado, é um longo conjunto de dados sem sentido.

Serpent.
http://en.wikipedia.org/wiki/Serpent_(cipher)

O *TrueCrypt* trabalha com os seguintes algoritmos criptográficos: AES-256, *Serpent* e *Twofish*, todos reconhecidamente seguros pela comunidade científica.

A seguir, são mostradas as principais funcionalidades da versão 6.2 do *TrueCrypt*.

5.4.1.2 Criação de um disco seguro

Um disco seguro permite que se guardem arquivos onde somente o conhecedor da senha pode recuperá-los. A partir da janela principal (Figura 5.21), clicar no botão "Criar Disco".

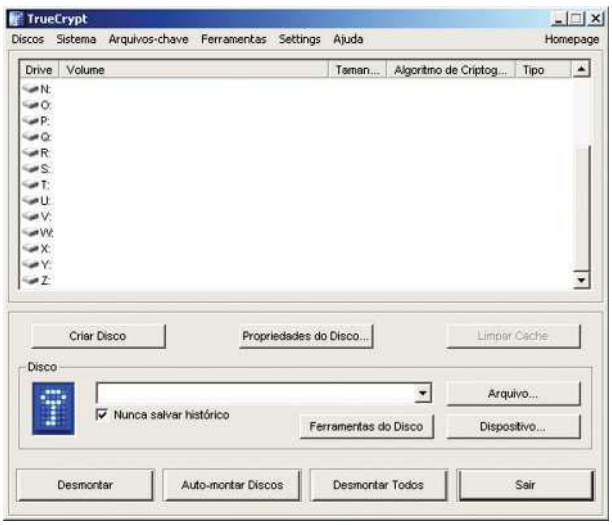


Figura 5.21: Tela principal do *TrueCrypt*

Fonte: Imagem copiada do *TrueCrypt*, de autoria da *TrueCrypt Foundation*

Na janela "Assistente para a Criação de Volume" (Figura 5.22), escolha a opção "*Create an encrypted file container*" e clique no botão "Avançar".

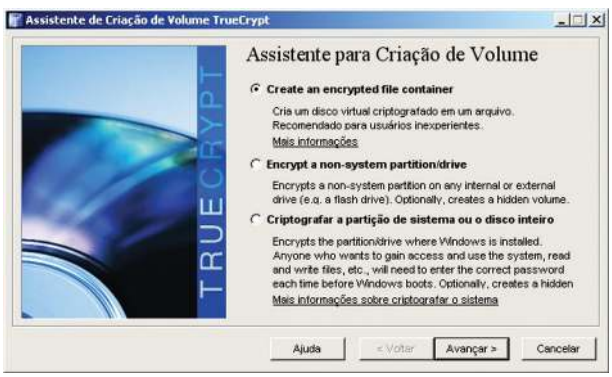


Figura 5.22: Assistente para a criação de volume

Fonte: Imagem copiada do *TrueCrypt*, de autoria da *TrueCrypt Foundation*

Na janela "Tipo de Volume" (Figura 5.23), escolha a opção "Volume *True-Crypt* padrão" e clique no botão "Avançar".

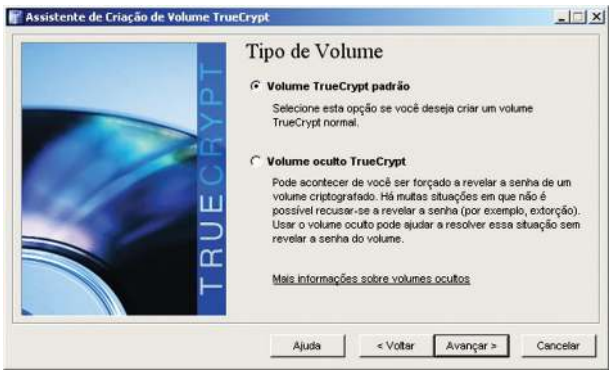


Figura 5.23: Tipo de volume

Fonte: Imagem copiada do *TrueCrypt*, de autoria da *TrueCrypt Foundation*

Na janela "Localização do Disco" (Figura 5.24), clique no botão "Arquivo".

Figura 5.24: Localização do disco

Fonte: Imagem copiada do *TrueCrypt*, de autoria da *TrueCrypt Foundation*

Na janela do *Windows Explorer* (Figura 5.25), selecione o caminho e escreva o nome do arquivo e clique no botão "Salvar".

Figura 5.25: Definindo o local e o nome do arquivo

Fonte: Imagem copiada do *Windows Explorer*, de autoria da *Microsoft Corporation*

Na janela "Localização do Disco" (Figura 5.26), aparecerá o caminho completo do arquivo escolhido. Clique no botão "Avançar".

Figura 5.26: Localização do disco

Fonte: Imagem copiada do *TrueCrypt*, de autoria da *TrueCrypt Foundation*

Na janela "Opções de Criptografia" (Figura 5.27), escolha o algoritmo de criptografia e o algoritmo de *hash* a serem utilizados. Clique no botão "Avançar".

Figura 5.27: Opções de criptografia

Fonte: Imagem copiada do *TrueCrypt*, de autoria da *TrueCrypt Foundation*

Na janela "Tamanho do disco" (Figura 5.28), defina o tamanho do volume que conterá os arquivos criptografados. É importante planejar o tamanho desse arquivo para evitar criar um arquivo muito pequeno (insuficiente) ou grande demais (desperdício). Clique no botão "Avançar".

Figura 5.28: Tamanho do disco

Fonte: Imagem copiada do *TrueCrypt,* de autoria da *TrueCrypt Foundation*

O passo seguinte é um dos mais importantes, pois a segurança dos arquivos a serem contidos no volume criptografado depende do tamanho e da qualidade da senha. Quanto maior a senha, melhor. Quanto mais misturar letras maiúsculas, minúsculas, símbolos e dígitos numéricos melhor. Quanto mais o usuário for capaz de lembrar a senha, melhor.

Na janela "Senha do Volume" (Figura 5.29), defina a senha de criptografia do volume. Clique no botão "Avançar".

Figura 5.29: Senha do volume

Fonte: Imagem copiada do *TrueCrypt*, de autoria da *TrueCrypt Foundation*

Caso a senha escolhida seja muito curta, o aplicativo vai informar a existência de uma vulnerabilidade ao usuário e se ele quer correr o risco mesmo assim (Figura 5.30).

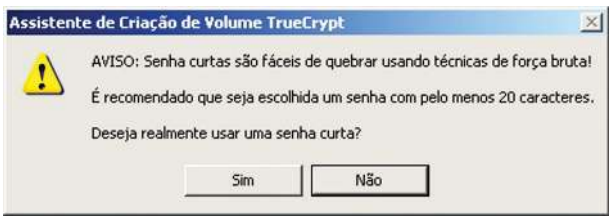


Figura 5.30: Aviso de senha muito curta

Fonte: Imagem copiada do *TrueCrypt*, de autoria da *TrueCrypt Foundation*

Após aceitar o risco, ou ter digitado uma nova senha, o usuário será conduzido à janela "Formatação do Disco" (Figura 5.31), onde informará o sistema de arquivos e o tamanho do *cluster*. Após os ajustes, clique no botão "Formatar".

Figura 5.31: Formatação do disco

Fonte: Imagem copiada do *TrueCrypt,* de autoria da *TrueCrypt Foundation*

O aplicativo informa se a formatação foi bem-sucedida ou não (Figura 5.32) e fornece a opção de criar mais um volume ou de sair do assistente (Figura 5.33).

Figura 5.32: Volume criado com sucesso

Fonte: Imagem copiada do *TrueCrypt*, de autoria da *TrueCrypt Foundation*

Figura 5.33: Opção de criar mais discos

Fonte: Imagem copiada do *TrueCrypt*, de autoria da *TrueCrypt Foundation*

O volume criado aparecerá no *Windows Explorer* como um arquivo comum, sem extensão. Para que se possa utilizá-lo, é necessário montar a unidade de disco.

5.4.1.3 Montagem e desmontagem de um disco seguro

Na janela principal do *TrueCrypt*, o usuário deve selecionar uma letra para a unidade de disco que pretende montar. Neste exemplo, foi escolhida a unidade T:\ (Figura 5.34). Clique no botão "Arquivo".

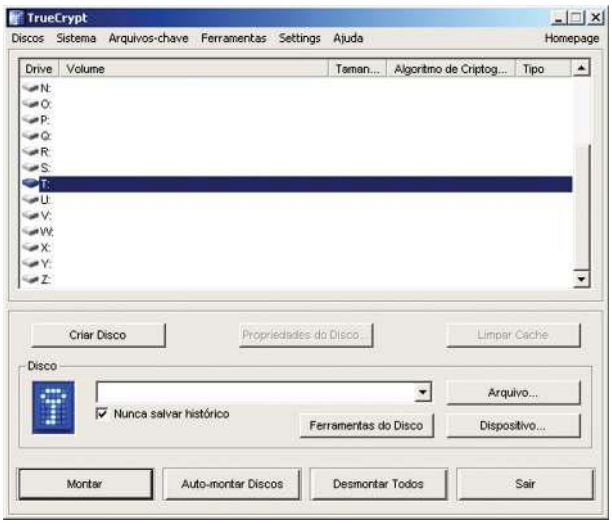


Figura 5.34: Seleção de unidade de disco

Fonte: Imagem copiada do *TrueCrypt*, de autoria da *TrueCrypt Foundation*

Na janela do *Windows Explorer*, selecione o arquivo onde quer montar o volume (Figura 5.35). Clique em "Abrir".

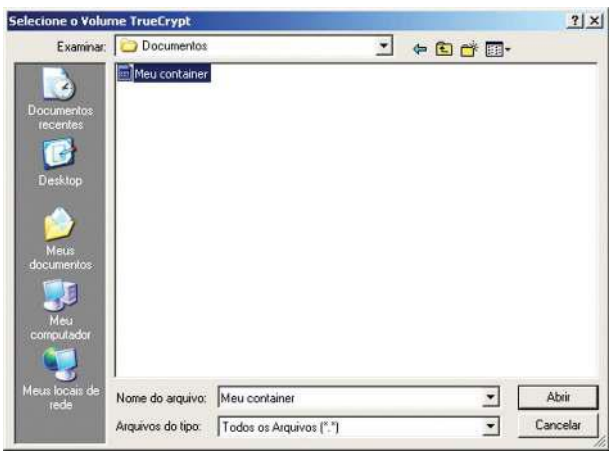


Figura 5.35: Seleção do volume *TrueCrypt*

Fonte: Imagem copiada do *Windows Explorer*, de autoria da *Microsoft Corporation*

O caminho completo para o arquivo é mostrado no campo "Disco", da janela principal do *TrueCrypt* (Figura 5.36). Clique no botão "Montar".

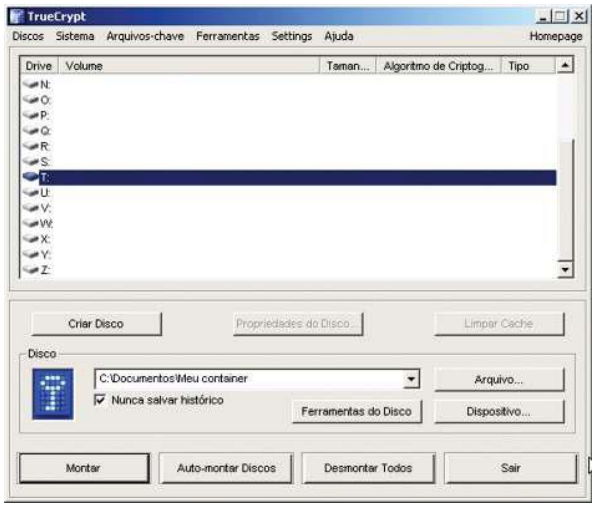


Figura 5.36: Janela principal do *TrueCrypt*

Fonte: Imagem copiada do *TrueCrypt*, de autoria da *TrueCrypt Foundation*

Será solicitada a senha usada na criação do volume (Figura 5.37). Após a digitação, clique no botão "Ok".

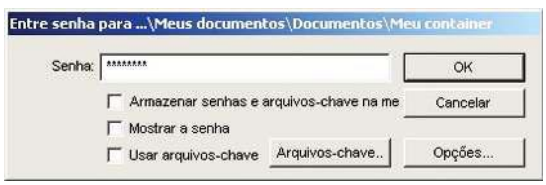


Figura 5.37: Entrada da senha

Fonte: Imagem copiada do *TrueCrypt*, de autoria da *TrueCrypt Foundation*

Se a senha foi digitada corretamente, o volume será montado com a letra escolhida e listado na janela principal do *TrueCrypt* (Figura 5.38).

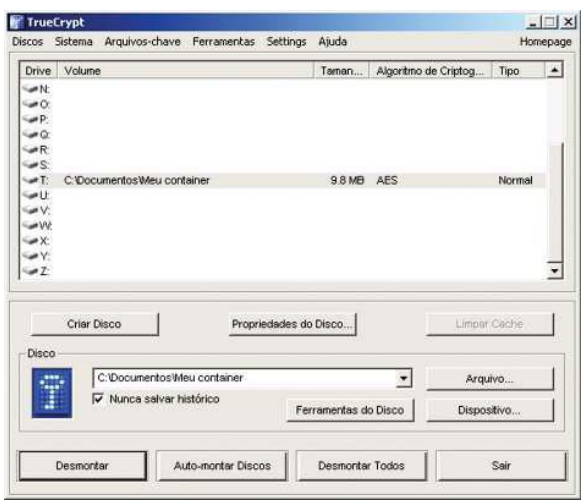


Figura 5.38: Lista de volumes montados

Fonte: Imagem copiada do *TrueCrypt*, de autoria da *TrueCrypt Foundation*

A Figura 5.39 mostra a janela e o conteúdo da unidade T:\. Todos os arquivos que forem movidos para esta pasta serão automaticamente encriptados. Esses

arquivos estarão acessíveis aos usuários enquanto a unidade T:\ estiver montada.

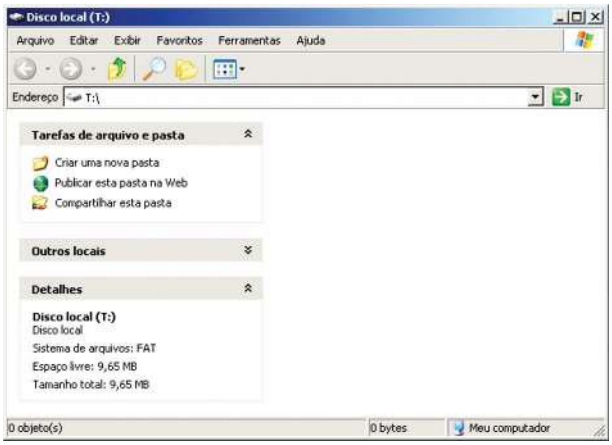


Figura 5.39: Conteúdo do volume montado

Fonte: Imagem copiada do *Windows Explorer,* de autoria da *Microsoft Corporation*

Os volumes *TrueCrypt*, após montados, são vistos pelo sistema operacional como unidades comuns de disco (Figura 5.40).

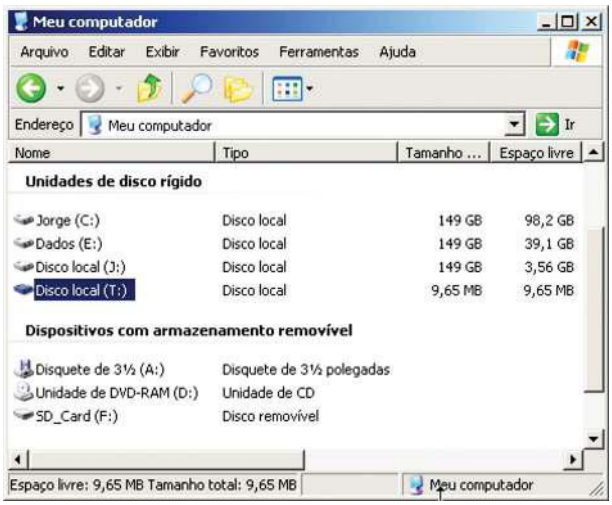


Figura 5.40: Lista de unidades de disco do sistema

Fonte: Imagem copiada do *Windows Explorer,* de autoria da *Microsoft Corporation*

Para desmontar a unidade T:\ e impedir o acesso ao seu conteúdo, basta apenas fechar todos os aplicativos que estejam utilizando arquivos da unidade T:\ e, na janela principal do *TrueCrypt* (Figura 5.38), selecionar a unidade de disco que se quer desmontar e clicar no botão "Desmontar".

Resumo

Os gerenciadores de senha protegem com criptografia a infinidade de senhas de acesso advindas da atual revolução digital. Os gerenciadores de *backup* automatizam a criação e atualização de cópias de segurança. Podem ser utilizados de forma preventiva ou corretiva. As ferramentas de criptografia permitem ao usuário trabalhar com criptografia de dados, garantindo a confidencialidade das informações.

Atividades de aprendizagem

1. Pesquise na internet e descreva duas técnicas que permitem gerar boas senhas.

2. Pesquise na internet qual solução apresenta maior segurança: um volume *TrueCrypt* padrão ou um volume *TrueCrypt* oculto? Justifique.

Poste os arquivos com suas respostas e justificativas no AVEA.

Aula 6 – *Softwares* de SI – ferramentas de descarte de dados e antivírus

Você não pode se defender. Você não pode impedir. A única coisa que você pode fazer é detectar e reagir.

Bruce Schneier

Objetivos

Conhecer os conceitos básicos sobre o tema *softwares* de Segurança da Informação.

Realizar estudos de caso em cada um dos tipos de ferramentas apresentadas.

6.1 Ferramentas para o descarte seguro de dados

São ferramentas criadas para dificultar a recuperação de arquivos excluídos de unidades de armazenamento magnético.

Quando um usuário exclui um arquivo, seu sistema operacional apenas remove os índices que informavam que naquela região havia um arquivo. Os *bytes* do arquivo continuam no mesmo lugar e podem ser recuperados com *softwares* especializados, mesmo que essa região tenha sido sobrescrita e contenha um novo arquivo. Essa propriedade de reter informações é chamada **remanência de dados** e pode trazer problemas ao usuário.

HDs usados facilitam roubo de identidade. http://tecnologia.terra.com.br/interna/0,,OI1947225-EI4799,00.html

Os *softwares* de descarte seguro de dados trabalham sobrescrevendo várias vezes a região onde os *bytes* do arquivo excluído se encontram, utilizando sequências específicas ou valores aleatórios, dificultando a recuperação dessas informações.

Entretanto, a técnica não oferece 100% de eficiência, pois os discos rígidos têm uma capacidade de retenção de informações muito grande, permitindo a um atacante obstinado ou aos serviços de inteligência nacionais recuperar parcial ou totalmente o conteúdo de um HD. Somente utilizando os méto-

dos de encriptação prévia do disco rígido, ***degaussing*** e destruição física da mídia, nessa ordem, podem garantir que dado algum possa ser recuperado.

A-Z

Degaussing
É a aplicação de um forte campo magnético capaz de remover as marcações que definem o valor zero e o valor um existentes em um disco rígido. Essa técnica oferece mais segurança que a sobrescrição usada nas ferramentas de descarte seguro de dados, pois aumenta a garantia de que não haverá remanência de dados suficiente para reconstruir as informações de um disco rígido.

6.1.1 Estudo de caso – *Eraser*

O *Eraser* é uma ferramenta *freeware*, criada por Sami Tolvanen e Garret Trant e disponibilizada na internet no sítio **http://eraser.heidi.ie/**. Não possui suporte ao idioma português brasileiro. É um *software* avançado que permite aos usuários remover com muita segurança dados sensíveis de seu disco rígido, sobrescrevendo-os várias vezes com padrões cuidadosamente selecionados. A seguir, são mostradas suas principais funcionalidades.

6.1.1.1 Agendamento de tarefas

O *Eraser* permite automatizar sua execução através de tarefas. Cada tarefa contém todas as informações que caracterizam uma rotina de limpeza, tais como local a ser limpo, agendamento e algoritmo.

A Figura 6.1 mostra a janela principal do *Eraser*.

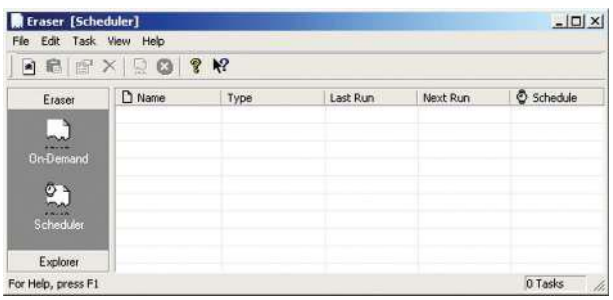


Figura 6.1: Janela principal
Fonte: Imagem copiada do *Eraser*, de autoria do Projeto *Eraser*

Para criar uma nova tarefa, basta clicar no menu "*File*" e em seguida na opção "*New Task*" (Figura 6.2).

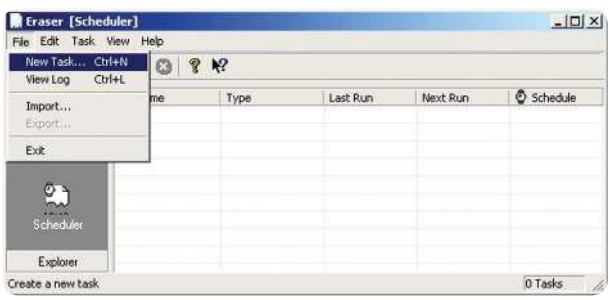


Figura 6.2: Nova tarefa
Fonte: Imagem copiada do *Eraser*, de autoria do Projeto *Eraser*

Na guia "*Data*" da janela que se abriu, deve-se escolher quais dados ou áreas serão sobrescritos, tais como espaço livre de uma unidade de armazenamento, o conteúdo de uma pasta ou um determinado arquivo (Figura 6.3).

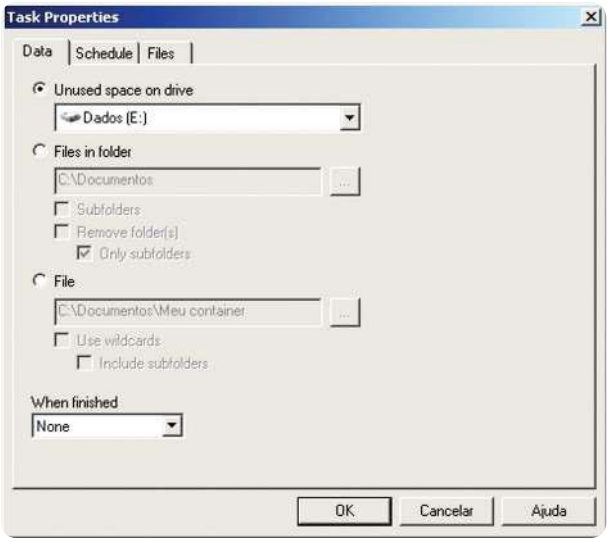


Figura 6.3: Guia Data
Fonte: Imagem copiada do *Eraser*, de autoria do Projeto *Eraser*

No campo "*Every*" da guia "*Schedule*", deve-se indicar a se a tarefa será executada diariamente, ou em determinado dia da semana ou a cada reinicialização do computador (Figura 6.4).

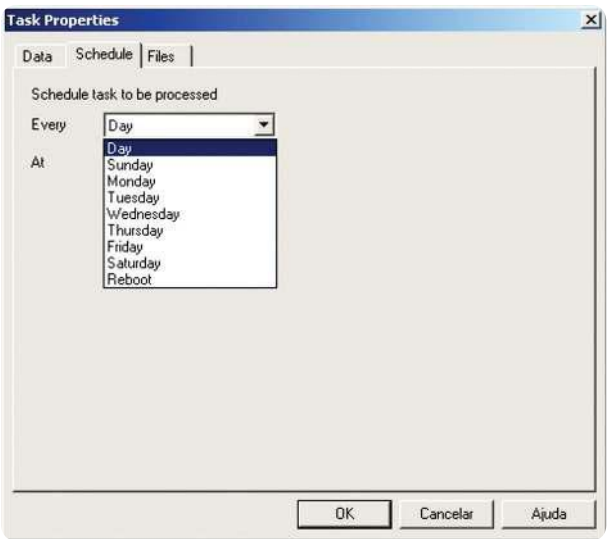


Figura 6.4: Guia *Schedule*: Frequência
Fonte: Imagem copiada do *Eraser*, de autoria do *Projeto Eraser*

No campo "*At*" da guia "*Schedule*", deve-se indicar a hora em que a tarefa deve ser executada (Figura 6.5).

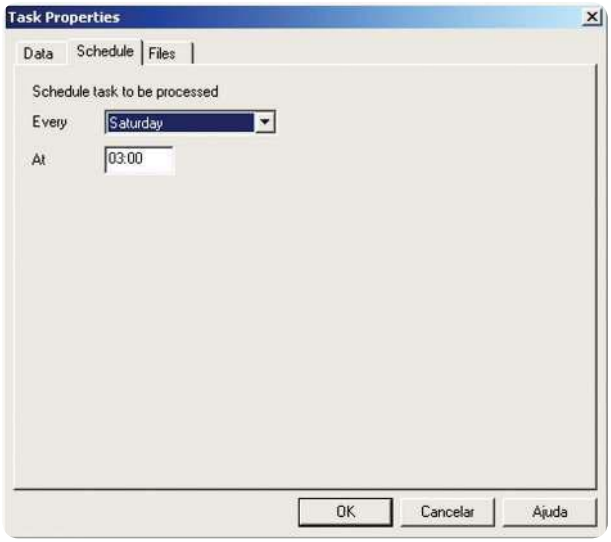


Figura 6.5: Guia *Schedule*: hora
Fonte: Imagem copiada do *Eraser*, de autoria do Projeto *Eraser*

Na guia "*Files*" deve-se escolher o algoritmo de limpeza dentre as seis opções disponíveis. Em princípio, quanto mais passos o algoritmo tiver, mais segura e mais lenta será a limpeza (Figura 6.6).

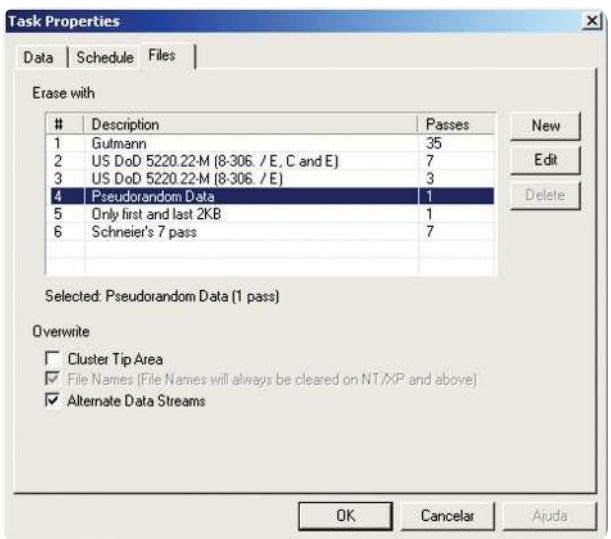


Figura 6.6: Guia *Files*
Fonte: Imagem copiada do *Eraser*, de autoria do Projeto *Eraser*

Para salvar as opções da tarefa, basta clicar no botão "Ok". A tarefa criada passa a ser mostrada na janela principal do *Eraser* (Figura 6.7).

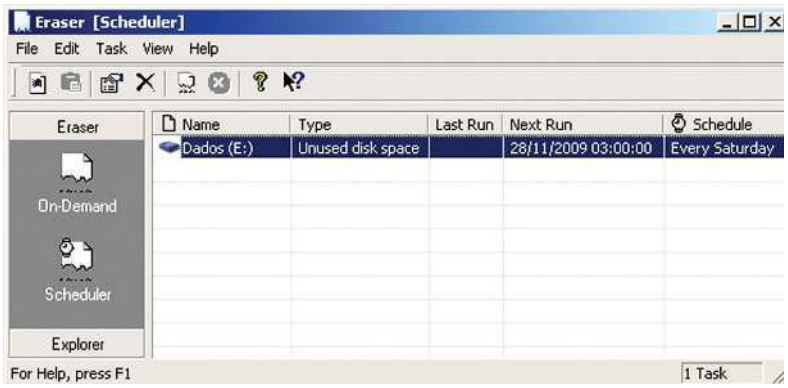


Figura 6.7: Agendamento completo
Fonte: Imagem copiada do Eraser, de autoria do Projeto Eraser

6.1.1.2 Limpeza da lixeira do *Windows*

O *Eraser* permite a limpeza da lixeira do *Windows* diretamente da área de trabalho. Basta clicar com o botão direito do *mouse* sobre o ícone da lixeira e escolher uma opção (Figura 6.8).

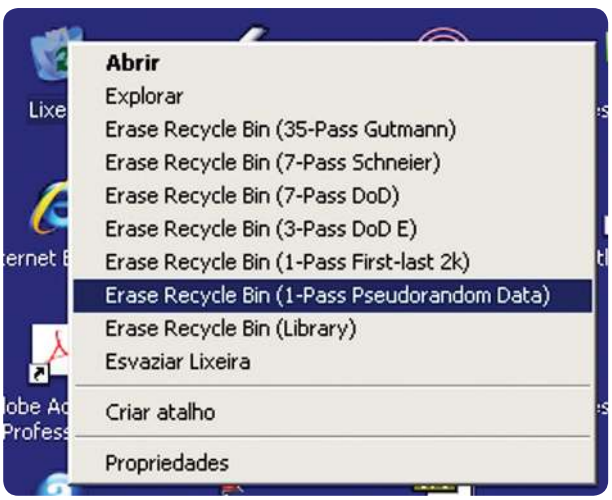


Figura 6.8: Limpeza da Lixeira do *Windows*
Fonte: Imagem copiada do *Windows* XP, de autoria da *Microsoft Corporation*

Escolhida a opção de limpeza, o *Eraser* pede a confirmação do usuário (Figura 6.9).

Figura 6.9: Confirmação da limpeza
Fonte: Imagem copiada do *Eraser*, de autoria do Projeto *Eraser*

Ao clicar no botão "*Yes*", o *Eraser* inicia a limpeza da Lixeira (Figura 6.10).

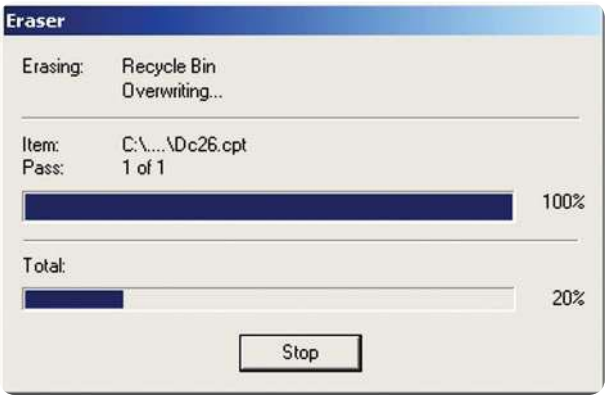


Figura 6.10: Execução da limpeza
Fonte: Imagem copiada do *Eraser*, de autoria do Projeto *Eraser*

Ao término da operação, o *Eraser* descreve o resultado da limpeza (Figura 6.11).

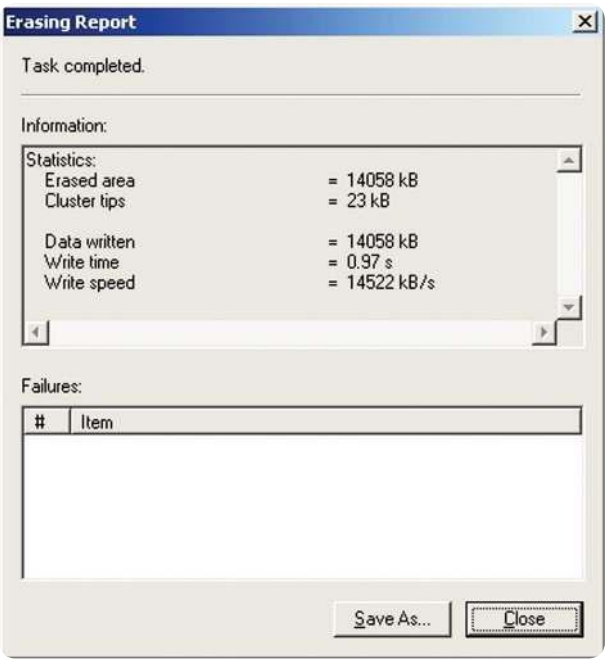


Figura 6.11: Resultado da limpeza
Fonte: Imagem copiada do *Eraser*, de autoria do Projeto *Eraser*

6.1.1.3 Limpeza do espaço não usado do disco rígido

O *Eraser* permite a limpeza do espaço não usado do disco rígido. Basta que o usuário clique com o botão direito do *mouse* sobre o ícone da unidade de disco que deseja limpar e escolha a opção "*Erase Unused Space*" (Figura 6.12).

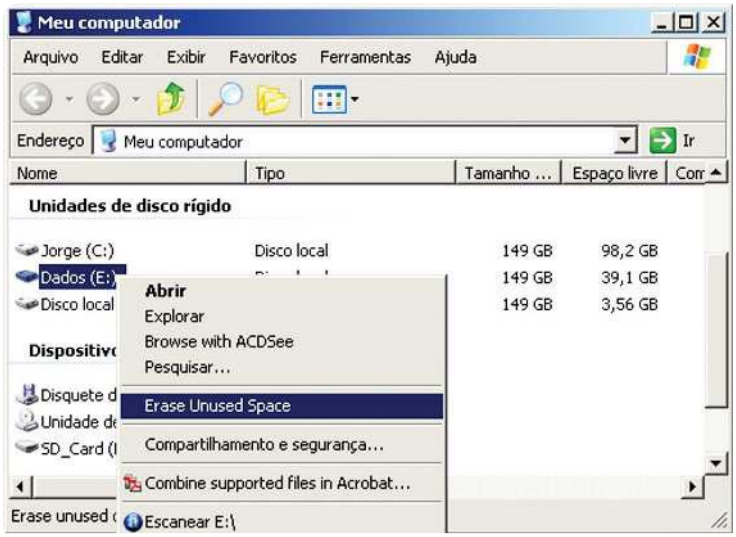


Figura 6.12: Seleção de unidade para limpeza

Fonte: Imagem copiada do *Windows Explorer*, de autoria da *Microsoft Corporation*

Em seguida, abrir-se-á uma janela de confirmação, onde o usuário pode iniciar imediatamente, através do botão "*Yes*", ajustar as opções de limpeza, através do botão "*Options*" ou cancelar a limpeza, através do botão "*No*" (Figura 6.13).

Figura 6.13: Confirmação de limpeza
Fonte: Imagem copiada do Eraser, de autoria do Projeto Eraser

Após clicar no botão "*Options*", o usuário deverá escolher o algoritmo de limpeza que julgue adequado (Figura 6.14).

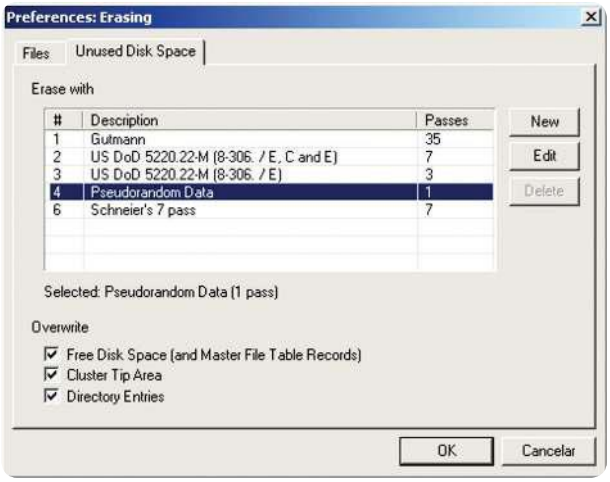


Figura 6.14: Escolha do algoritmo de limpeza
Fonte: Imagem copiada do *Eraser*, de autoria do Projeto *Eraser*

Após clicar no botão "*Yes*", é iniciada a limpeza do espaço não usado do disco rígido (Figura 6.15). Essa limpeza é bastante demorada e consome muito do processamento e do acesso ao disco do computador. É recomendado que a limpeza de espaço não usado seja feita apenas quando o usuário não estiver utilizando o computador.

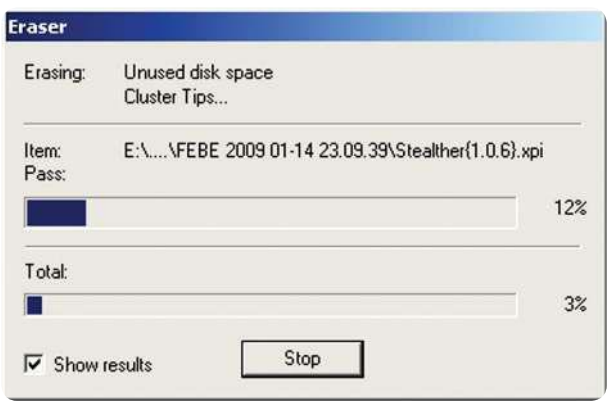


Figura 6.15: Execução da limpeza
Fonte: Imagem copiada do *Eraser*, de autoria do Projeto *Eraser*

Ao término da operação, o *Eraser* descreve o resultado da limpeza (Figura 6.16).

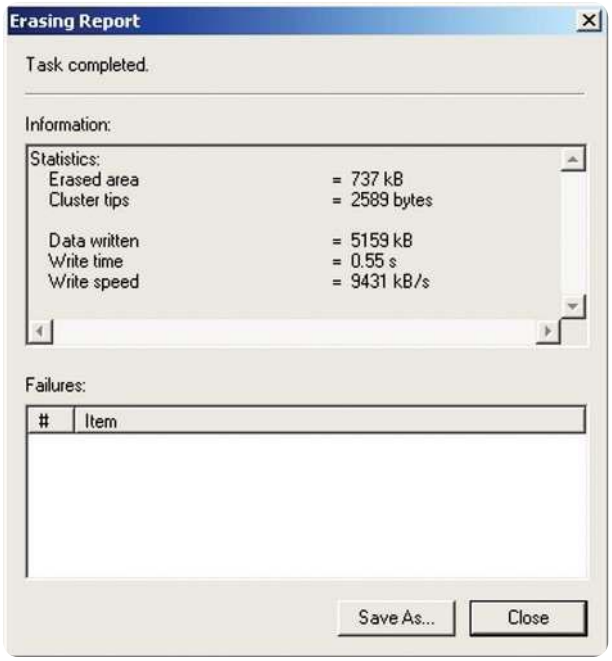


Figura 6.16: Resultado da limpeza
Fonte: Imagem copiada do *Eraser*, de autoria do Projeto *Eraser*

6.2 Ferramentas antivírus

São *softwares* especializados na prevenção, detecção e remoção de vírus de computador. Alguns antivírus modernos incluem em suas rotinas de varredura a detecção de cavalos de troia, *Worms* e *Spyware*, além de vírus de computador. Podem ser classificados em:

a) antivírus pessoais: são instalados no computador pessoal. Recebem atualizações pela internet e são gratuitos;

b) antivírus corporativos: são instalados em servidores de rede de dados. Recebem suas atualizações de um servidor dedicado e são pagos.

A detecção dos vírus de computador por essas ferramentas é feita de duas formas:

a) com o auxílio de uma base de dados contendo sequências de caracteres que identificam cada um desses *malwares*, chamadas assinaturas de vírus. Essa base deve ser sempre atualizada, pois são criados cerca de dez vírus e suas variantes, todos os dias;

b) através de avaliação heurística, pela qual são verificados os comportamentos característicos de um *malware*, tais como alteração no código de programas e acesso a áreas reservadas de memória, evitando assim que vírus mesmo desconhecidos tomem o controle do computador.

6.2.1 Estudo de caso – *Avast! Antivirus*

O *Avast*! Antivirus é uma ferramenta *freeware*, criada pela empresa ALWIL *Software* e disponibilizada na internet no sítio **http://www.avast.com/index_por.html**, inclusive no idioma português brasileiro. Possui atualmente 100 milhões de utilizadores no mundo inteiro e é vencedor de vários prêmios. Apesar de gratuito, o *software* exige o cadastramento do usuário para o envio das atualizações. Esse cadastro tem validade de um ano, podendo ser renovado indefinidamente. A seguir, são mostradas suas principais funcionalidades.

6.2.1.1 Proteção residente

A proteção residente é responsável por manter a saúde do computador. É composta por oito módulos que monitoram partes específicas do sistema operacional e seus aplicativos, evitando em tempo real uma infecção um vírus. Cada módulo é configurado de modo independente dos demais. São eles:

a) proteção padrão: é responsável por verificar os programas em execução e os documentos que estão abertos, sendo capaz de impedir o acesso ao documento ou programa se estiverem infectados;

Peer-to-peer. http://pt.wikipedia.org/wiki/P2P

b) proteção P2P: é responsável por verificar os arquivos baixados pelos programas de compartilhamento de arquivos (*peer-to-peer*) mais comuns;

c) proteção de rede: é responsável pela proteção do sistema contra a invasão por *worms;*

d) proteção de *e-mail*: é responsável por verificar o tráfego entre o servidor e o cliente de *e-mail*, recusando o envio ou o recebimento de mensagens que possuam vírus de computador;

e) proteção de internet: é responsável por verificar o tráfego de dados entre os servidores da internet e o navegador do usuário, verificando páginas e o *download* de arquivos;

f) *outlook/exchange*: é responsável por verificar o tráfego entre o servidor de *e-mail* e os programas *Microsoft Outlook* e *Microsoft Exchange*, recusando o envio ou o recebimento de mensagens que possuam vírus de computador;

g) mensagens instantâneas: é responsável por verificar os arquivos que são enviados ou recebidos através de programas de mensagens instantâneas, tais como *Windows Live Messenger* e *Pidgin*.

A Figura 6.17 mostra a janela de configuração dos módulos da proteção residente do *Avast*.

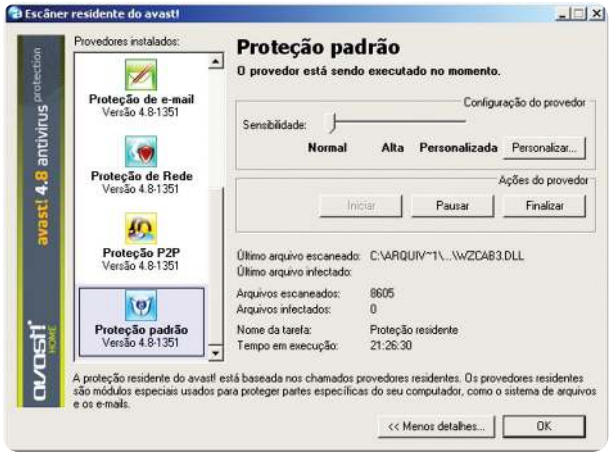


Figura 6.17: Proteção residente do *Avast*
Fonte: Imagem copiada do *Avast*! *Antivirus*, de autoria da ALWIL *Software*

6.2.1.2 *Virus Recovery Data Base* (VRDB)

É a ferramenta capaz de recuperar arquivos infectados por vírus, trazendo-os de volta ao seu estado original.

A ativação do VRDB cria um banco de dados que armazenas informações sobre o estado atual dos arquivos e de suas três versões anteriores. O banco de dados é criado apenas uma vez e atualizado automaticamente a cada três semanas.

Para ativar o VRDB, basta clicar com o botão direito do *mouse* sobre o ícone do Avast na bandeja da barra de tarefas, escolher a opção "VRDB" e em seguida a opção "Criar o VRDB agora!" (Figura 6.18).

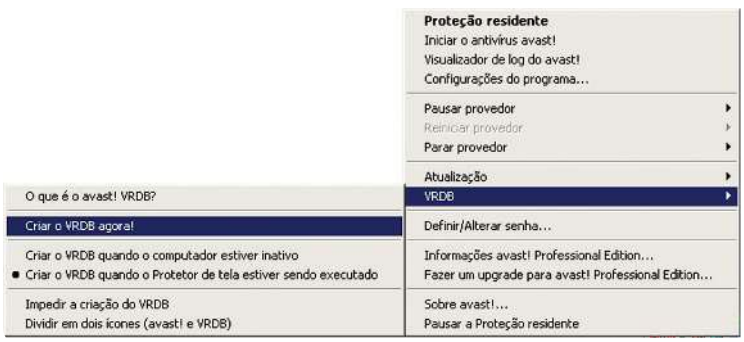


Figura 6.18: Ativando o VRDB
Fonte: Imagem copiada do *Avast*! *Antivirus*, de autoria da ALWIL *Software*

6.2.1.3 Varredura contra vírus

Para iniciar a varredura contra vírus, basta clicar com o botão direito do *mouse* sobre o ícone do *Avast* na bandeja da barra de tarefas e escolher a opção

"Iniciar o antivírus *Avast*". Após verificar se há vírus na memória principal do computador, a janela principal do *Avast* abrir-se-á (Figura 6.19).

Figura 6.19: Janela principal do *Avast*
Fonte: Imagem copiada do *Avast*! *Antivirus*, de autoria da ALWIL *Software*

A varredura exige algumas informações antes de começar, tais como o local e a profundidade da varredura (Figura 6.20).

Figura 6.20: Local e a profundidade da varredura
Fonte: Imagem copiada do *Avast*! *Antivirus*, de autoria da ALWIL *Software*

Para iniciar a varredura, basta clicar com o *mouse* no botão "Iniciar", na janela principal do *Avast* (Figura 6.21).

Figura 6.21: Iniciar varredura
Fonte: Imagem copiada do Avast! *Antivirus*, de autoria da ALWIL Software

6.2.1.4 Agendamento da varredura no próximo *boot*

A varredura durante o *boot* traz a vantagem de procurar por vírus quando o sistema operacional ainda não foi completamente carregado, permitindo uma busca mais profunda e rápida desses *malwares*. Para ativar essa ferramenta, basta clicar no botão "Menu", no canto superior esquerdo da janela principal do Avast e escolher a opção "Agendar escaneamento no *boot*" (Figura 6.22).

Figura 6.22: Agendamento da varredura no próximo *boot*
Fonte: Imagem copiada do *Avast*! *Antivirus*, de autoria da ALWIL *Software*

Abrir-se-á a janela com as opções dessa varredura (Figura 6.23), tais como o local (discos locais ou uma pasta específica) e o que fazer caso vírus sejam encontrados (excluir, mover para quarentena, reparar o arquivo infectado etc.).

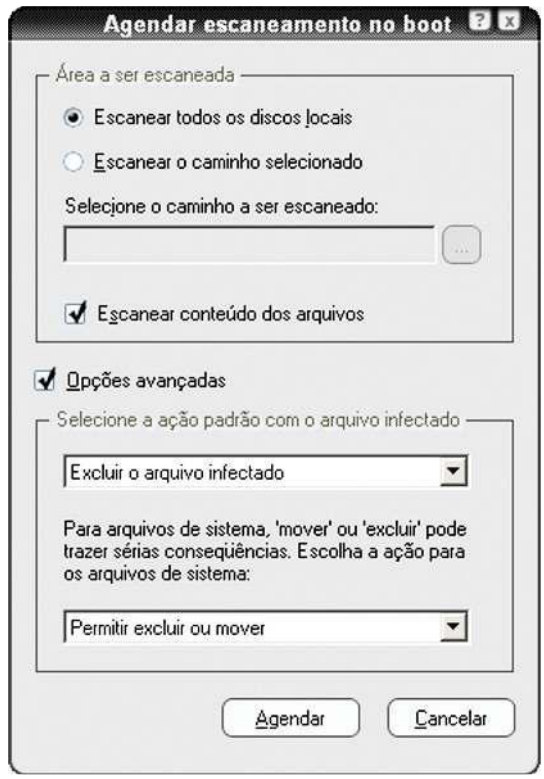


Figura 6.23: Opções da varredura no *boot*
Fonte: Imagem copiada do *Avast*! *Antivirus*, de autoria da ALWIL *Software*

Definidas as opções de varredura, basta clicar no botão "Agendar". O Avast irá perguntar se a varredura deve ser feita imediatamente (reiniciando o computador) ou se deve aguardar o próximo *boot* da máquina.

Resumo

As ferramentas para o descarte seguro de dados dificultam a recuperação de arquivos excluídos de unidades de armazenamento magnético. As ferramentas antivírus previnem, detectam e removem vírus de computador. Os mais modernos permitem a varredura contra cavalos de troia, *worms* e *spywares*, além dos vírus.

Atividades de aprendizagem

1. Pesquise na internet e cite cinco características de um antivírus corporativo, classifique-as em vantagem ou desvantagem e justifique.

2. Pesquise na internet e apresente duas soluções (produtos) para o descarte de mídias físicas, sendo uma para CDs, DVDs ou *pen drives* e outra para discos rígidos.

Poste os arquivos com suas respostas e justificativas no AVEA.

Aula 7 – Softwares de SI - *antispywares* e *firewalls*

Como administradores de segurança ou de firewall, temos basicamente as mesmas preocupações de um encanador: saber o tamanho e o tipo do duto, saber se o conteúdo certo está passando pelo duto certo, saber se os dutos são seguros contra rachaduras e vazamentos. É claro que quando os dutos estouram, nós, como encanadores, somos os responsáveis por limpar a bagunça e somos nós que saímos cheirando mal.

Marcus J. Ranum

Objetivos

Conhecer os conceitos básicos sobre o tema softwares de Segurança da Informação.

Realizar estudos de caso em cada um dos tipos de ferramentas apresentadas.

7.1 Ferramentas *Antispyware*

As ferramentas *Antispyware* são muito similares às ferramentas Antivírus, diferenciando-se apenas no fato de serem específicas na detecção, prevenção e remoção de *spywares* do computador.

Em geral, sua varredura é mais rápida que a dos antivírus, pois procura em pontos específicos do sistema operacional, sabidamente preferidos pelos *spywares*. Também trabalha com o auxílio de uma base de dados contendo sequências de caracteres que identificam cada um desses *malwares*. Essa base deve ser sempre atualizada antes de uma varredura.

A varredura contra *spywares* também inclui os chamados *cookies* de rastreamento – pequenos arquivos gravados pelo navegador de internet que registram algumas informações sobre as páginas que o usuário visitou. Os *cookies* foram criados com o intuito de manter a persistência de sessões das páginas de internet, evitando, por exemplo, que o usuário tenha de informar sua senha sempre que trocar de página.

Cookie.
http://pt.wikipedia.org/wiki/Cookie

GUID.
http://pt.wikipedia.org/wiki/GUID

O problema é que alguns sítios de internet forçam o navegador a gravar *cookies* contendo um identificador chamado GUID, que podem denunciar quais os sítios visitados, quais os tipos desses sítios, se foi feita alguma compra etc., acabando com a privacidade do usuário.

7.1.1 Estudo de caso – *Spybot Search & Destroy*

O *Spybot Search & Destroy* é uma ferramenta *freeware*, criada pela empresa Safer Networking Limited e disponibilizada na internet no sítio **http://www.safer-networking.org/pt/spybotsd/index.html.** Oferece suporte ao idioma português brasileiro.

A seguir, são mostradas suas principais funcionalidades.

7.1.1.1 Atualização

Para atualizar o banco de dados de *spywares* do *Spybot* S&D, é necessário clicar no botão "*Search for Updates*", na janela principal (Figura 7.1).

Figura 7.1: Janela principal do *Spybot* S&D
Fonte: Imagem copiada do *Spybot S&D*, de autoria da *Safer Networking Limited*

Em seguida, o *Spybot S&D* vai localizar, baixar e instalar as atualizações de seu banco de dados (Figura 7.2). A partir de agora, o *Spybot S&D* está pronto para a varredura.

Figura 7.2: Busca de atualizações
Fonte: Imagem copiada do *Spybot S&D*, de autoria da *Safer Networking Limited*

7.1.1.2 Varredura

Após clicar no botão "Examinar", na janela principal (Figura 7.1), é iniciado processo de varredura do computador contra *spywares* (Figura 7.3).

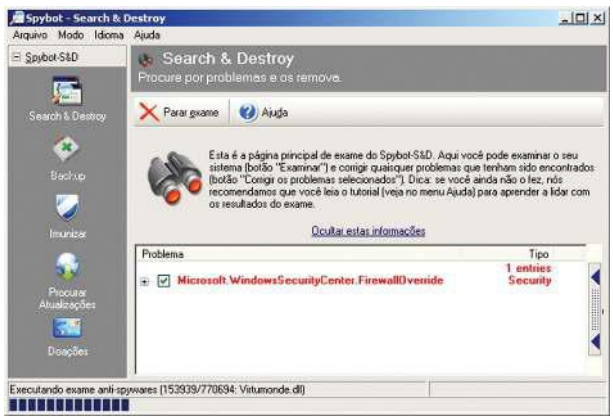


Figura 7.3: Varredura
Fonte: Imagem copiada do *Spybot S&D*, de autoria da *Safer Networking Limited*

O tempo de varredura do sistema depende do tamanho do disco rígido e da quantidade de arquivos armazenados. Ao término desse procedimento o *Spybot S&D* mostra uma lista com os problemas encontrados (Figura 7.4). Para eliminar os *spywares* e *cookies* de rastreamento é necessário clicar no botão "Corrigir os problemas selecionados".

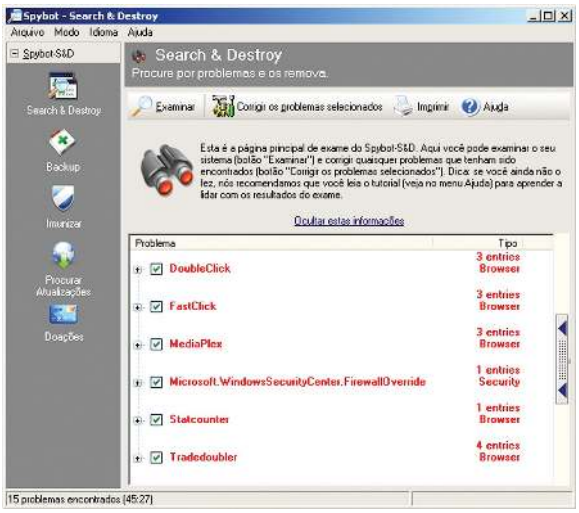


Figura 7.4: Lista de problemas encontrados
Fonte: Imagem copiada do *Spybot S&D*, de autoria da *Safer Networking Limited*

Em seguida, será solicitada confirmação do usuário. Para remover os problemas encontrados, basta clicar no botão "Sim" (Figura 7.5).

Figura 7.5: Confirmação de exclusão
Fonte: Imagem copiada do *Spybot S&D*, de autoria da *Safer Networking Limited*

Após a confirmação, o *Spybot S&D* mostra a lista com os problemas corrigidos (Figura 7.6). É recomendado que essas varreduras sejam realizadas pelo menos uma vez por semana.

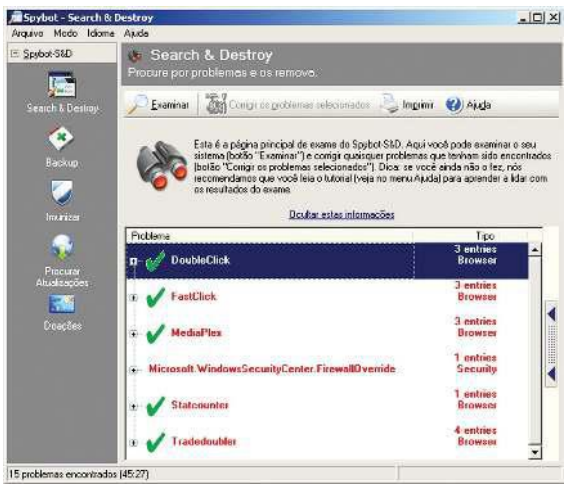


Figura 7.6: Problemas corrigidos
Fonte: Imagem copiada do *Spybot S&D* de autoria da *Safer Networking Limited*

7.2 *Firewalls*

Os *firewalls* são dispositivos desenvolvidos com a finalidade de aplicar políticas de segurança ao tráfego de dados entre um computador e uma rede ou entre redes, bloqueando qualquer transmissão não autorizada de informações. Além disso, também protegem contra invasões e ataques de *malwares*, monitorando as portas do protocolo TCP/IP.

TCP/IP.
http://pt.wikipedia.org/wiki/TCP/IP

Firewall.
http://pt.wikipedia.org/wiki/Firewall

Os *firewalls* podem ser classificados em:

a) *firewall* pessoal: é aquele desenvolvido com o intuito de proteger o tráfego de dados entre um computador pessoal e a internet. Em geral, oferece poucas opções de configuração, podendo ser gratuito ou pago;

b) *firewall* corporativo: é aquele desenvolvido com o intuito de proteger o tráfego de dados entre uma rede de dados empresarial e a internet. Oferece muitas opções de configuração, necessitando de profissionais qualificados para operá-lo. Pode ser *software* livre ou *software* comercial proprietário. A Figura 7.7 esquematiza um *firewall* corporativo;

c) *firewall* em *software*: são programas de computador que executam atividades comuns a *firewalls*. Podem ser instalados na máquina do usuário ou na borda externa de uma rede de dados. Têm a desvantagem de consumir recursos de processamento e memória do computador onde está instalado;

d) *firewall* em *hardware*: são equipamentos dedicados a executar atividades comuns a *firewalls*. Podem ser instalados na máquina do usuário ou na borda externa de uma rede de dados. Têm desempenho superior, porém são mais caros que as soluções em *software*, além de necessitar de alimentação elétrica.

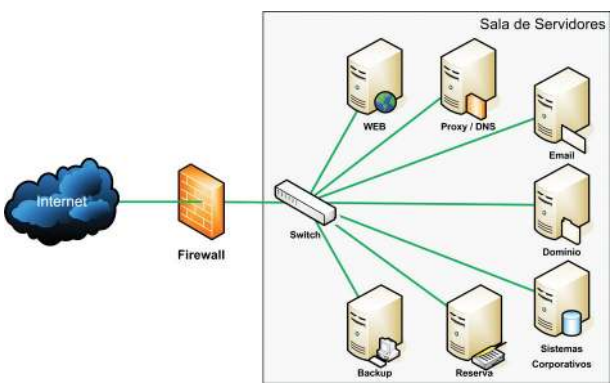


Figura 7.7: *Firewall* corporativo

7.2.1 Estudo de caso – *Comodo Firewall*

O *Comodo Firewall* é uma ferramenta *freeware*, criada pela empresa *Comodo Security Solutions*, com suporte ao idioma português brasileiro e disponibilizada na internet no sítio **http://personalfirewall.comodo.com/**, na forma de um conjunto de aplicativos chamado *Comodo Internet Security*. São três componentes:

a) *Comodo Firewall*: responde pela segurança do tráfego de dados, definindo quais portas de protocolo podem ser usadas, que aplicativos podem acessar a rede, etc.;

b) *Comodo Antivirus*: responde pela proteção do computador contra *malwares;*

c) *Comodo Defense+*: responde pela prevenção do computador contra invasões, furto de dados, ataques de *buffer overflow*, etc.

Buffer overflow.
http://pt.wikipedia.org/wiki/Buffer_overflow

A seguir, são mostradas as principais funcionalidades do *Comodo Firewall*.

7.2.1.1 Apresentação

A janela principal do *Comodo Firewall* traz um sumário com informações sobre as atividades executadas pelos componentes do programa. Informa a banda consumida pelos principais aplicativos, se todos os serviços estão operantes, quantas atividades suspeitas foram bloqueadas, etc. (Figura 7.8).

Figura 7.8: Janela principal do *Comodo Firewall*
Fonte: Imagem copiada do *Comodo Firewall*, de autoria da *Comodo Security Solutions Inc.*

7.2.1.2 Definir aplicativo como confiável

Definir um aplicativo como confiável significa dizer que o programa pode acessar a rede de dados. Para tanto, é necessário clicar no botão "*Firewall*" da janela principal do *Comodo*, seguido da opção "Tarefas comuns" e "Definir um novo aplicativo confiável".

Abrir-se-á uma nova janela. É necessário clicar no botão "Selecionar" e na opção "Explorar" (Figura 7.9).

Figura 7.9: Definir aplicativo confiável
Fonte: Imagem copiada do *Comodo Firewall,* de autoria da *Comodo Security Solutions Inc.*

Abrir-se-á uma janela do *Windows Explorer*. É necessário informar o local, o nome do aplicativo e clicar no botão "Abrir" (Figura 7.10).

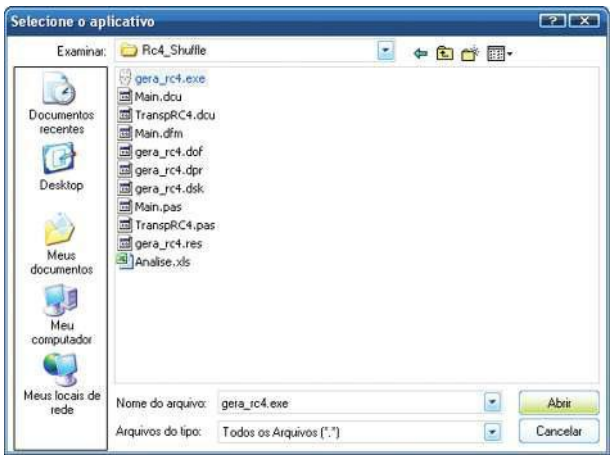


Figura 7.10: Local e nome do aplicativo
Fonte: Imagem copiada do *Comodo Firewall,* de autoria da *Comodo Security Solutions Inc.*

Após o caminho do aplicativo aparecer na janela "Definir um novo aplicativo confiável", basta clicar no botão "Aplicar" para salvar a inclusão (Figura 7.11).

Figura 7.11: Aplicar definição
Fonte: Imagem copiada do *Comodo Firewall*, de autoria da *Comodo Security Solutions Inc.*

7.2.1.3 Definir aplicativo como bloqueado

Definir um aplicativo como bloqueado significa dizer que o programa não poderá acessar a rede de dados e que o usuário não será incomodado, mesmo que aplicativo insista. Para tanto, é necessário clicar no botão "*Firewall*" da janela principal do Comodo, seguido da opção "Tarefas comuns" e "Definir um novo aplicativo bloqueado".

Abrir-se-á uma nova janela. É necessário clicar no botão "Selecionar" e na opção "Explorar" (Figura 7.12).

Figura 7.12: Definir aplicativo confiável
Fonte: Imagem copiada do *Comodo Firewall,* de autoria da *Comodo Security Solutions Inc.*

Abrir-se-á uma janela do *Windows Explorer*. É necessário informar o local, o nome do aplicativo e clicar no botão "Abrir" (Figura 7.13).

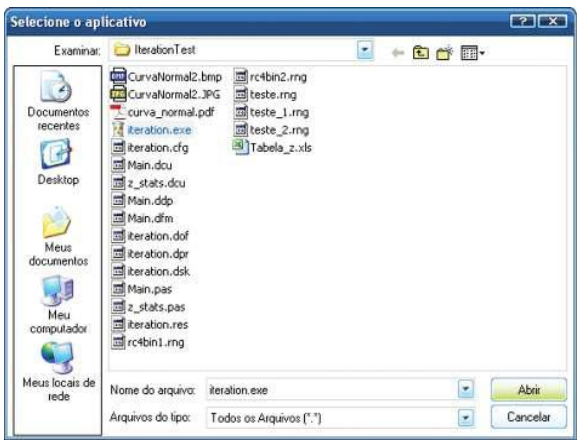


Figura 7.13: Local e nome do aplicativo
Fonte: Imagem copiada do *Comodo Firewall*, de autoria da *Comodo Security Solutions Inc.*

Após o caminho do aplicativo aparecer na janela "Definir um novo aplicativo bloqueado", basta clicar no botão "Aplicar" para salvar a inclusão (Figura 7.14).

Figura 7.14: Aplicar definição
Fonte: Imagem copiada do *Comodo Firewall*, de autoria da *Comodo Security Solutions Inc.*

Resumo

As ferramentas *antispyware* são especializadas na detecção, prevenção e remoção de *spywares* do computador. Os *firewalls* são dispositivos que vigiam o tráfego de dados entre computadores, autorizando ou bloqueando a passagem de informações.

Atividades de aprendizagem

1. Pesquise na internet e apresente dois produtos *antispyware*, destacando suas vantagens e desvantagens em relação ao *Spybot S&D*.

2. Pesquise na internet e apresente quatro produtos diferentes, em que cada um implementa um *firewall* pessoal em *software*, um *firewall* pessoal em *hardware*, um *firewall* corporativo em *software* e um *firewall* corporativo em *hardware*.

Poste os arquivos com suas respostas e justificativas no AVEA.

Aula 8 – O papel do usuário

Nós, os profissionais de segurança, somos muito parecidos com médicos cardiologistas. Nossos pacientes sabem que a falta de exercício, dieta rica em gorduras e que o tabagismo são péssimos para a saúde. Mas eles vão continuar fumando e comendo frituras deitados em seus sofás até que tenham um infarto. Então, eles querem uma pílula mágica que os tornem saudáveis de uma só vez, sem esforço. E a propósito, costumam alegar a todos que sua condição não é sua culpa – é culpa da genética, ou das empresas de cigarro, ou do McDonalds. E nos culpam por não termos cuidado melhor deles. Isso soa familiar?

Gene Spafford

Objetivo

Perceber que o fator humano é o elemento mais importante da Segurança da Informação.

8.1 Introdução

A humanidade passa por um momento muito peculiar em sua história, comumente chamado Revolução Digital. Em nenhum momento de nossa passagem por este lindo planeta produzimos e consumimos tanta informação. A cada dia, mais e mais pessoas juntam-se a essa revolução, acelerando enormemente essa produção e esse consumo. A cada dia, a informação torna-se mais valiosa e a segurança da informação, cada vez mais necessária.

As pessoas são os principais atores da Segurança da Informação; logo, têm profunda responsabilidade neste momento revolucionário.

Os itens a seguir procuram alertar para cuidados que devem ser tomados, apresentando recomendações e dicas sobre o que pode acontecer caso as pessoas não sejam cuidadosas.

8.2 Instalação de *softwares* de segurança

Todo computador precisa contar com *softwares* de segurança, tais como antivírus, *antispyware* e *firewall*, para conter ameaças e evitar o furto de informações do usuário.

Resquícios em memória RAM permitem quebra de criptografia de discos rígidos. http://www.linhadefensiva.org/2008/02/criptografia-hd-analise-ram

HDs usados podem conter informações privadas. http://tecnologia.terra.com.br/interna/0,,OI1430371-EI4801,00.html

Mesmo assim, é importante ressaltar que soluções milagrosas não existem. Cada ferramenta deve ser usada tendo-se em mente suas limitações.

O usuário deve dedicar especial atenção às informações que mantém sob sua guarda. Por exemplo, um dia o usuário vai precisar de um disco rígido maior. E provavelmente venderá o disco antigo para ajudar na nova aquisição. Se alguns cuidados não forem tomados, é problema na certa. Recomendações:

a) utilizar uma ferramenta de criptografia de disco. Desse modo, os dados contidos no disco rígido antigo já estariam protegidos, não sendo necessária mais nenhuma intervenção;

b) utilizar uma ferramenta para fazer o descarte seguro dos dados, escolhendo adequadamente o número de passos e o algoritmo mais eficiente.

É claro que essas recomendações atendem o usuário com um nível normal de paranoia. Para casos mais severos, é possível combinar as técnicas mostradas nas aulas anteriores: criptografia de disco + descarte seguro + *degaussing* + destruição física e química (ácido). É óbvio que, nesse caso, o disco antigo não poderia ser dado como entrada para o disco novo.

8.3 Atualizações de *software*

Todos os *softwares* de um computador precisam estar atualizados para fornecer o maior grau de confiabilidade possível. Isso inclui atualizações automáticas do sistema operacional, do banco de dados do antivírus e do *antispyware*. *Softwares* atualizados são imunes a falhas conhecidas.

8.4 Varreduras semanais

Pelo menos uma vez por semana, o computador deve ser completamente varrido contra vírus de computador, *spywares*, *worms* e cavalos de troia. É importante sentir-se seguro com o computador.

8.5 Escolher boas senhas

O especialista em Segurança da Informação Bruce Schneier ensina que há um paradoxo na administração de senhas, pois as boas senhas são difíceis de lembrar e as senhas fáceis de lembrar não são boas. Esse fato explica os quatro problemas mais comuns, relacionados às senhas:

a) senhas são esquecidas, afinal é recomendado que senhas jamais sejam anotadas em lugar algum;

b) senhas são descobertas por terceiros, pois alguns usuários insistem em anotá-las em papéis ou escolhem senhas fáceis de adivinhar, tais como datas importantes, esportes favoritos, nomes de familiares etc.;

c) senhas são reutilizadas, pois quando alguns usuários finalmente conseguem criar e lembrar uma boa senha, eles decidem ficar com ela para sempre, usando-a em todos os tipos de acesso. O grande problema nisso é que basta descobrir uma senha para ter acesso a todos os serviços do usuário;

d) senhas são compartilhadas, pois é muito mais cômodo fornecer a própria senha para um colega de trabalho copiar um arquivo do computador que ir até o escritório, digitar a própria senha e entregar o arquivo a quem precisa. A comodidade é inimiga da Segurança da Informação.

Utilizar um bom gerenciador de senhas é uma excelente prática. Escolhe-se uma única senha-mestre para guardar todas as senhas de serviço. As senhas de serviço podem ser completamente aleatórias e ter muitos caracteres. Permitem, ainda, que se defina um período de validade. Na hora de usar uma senha de serviço, basta abrir o gerenciador, digitar a senha-mestre e copiar a senha de serviço para o campo correspondente.

Procure conhecer o livro Segredos e Mentiras, de Bruce Schneier, que trata do elo mais fraco da Segurança da Informação: as pessoas.

8.6 Cuidado com as mídias removíveis

As mídias removíveis (CDs, DVDs, *pen drives*, cartões de memória) são produtos tecnológicos extremamente práticos, muito leves, relativamente baratos (algumas dezenas de reais) e com boa capacidade de armazenamento (700 Mb a 16 Gb, em média).

Todas essas vantagens trazem um grande problema: mídias removíveis são muito fáceis de perder! Existem pessoas que carregam a vida inteira em *pen drives* (fotos, vídeos, documentos, diários, etc.). Sem a proteção adequada, o extravio dessas mídias expõe severamente a privacidade do proprietário.

Para evitar problemas, são recomendados alguns cuidados:

a) não gravar informações privadas, íntimas ou sigilosas em mídias removíveis;

b) se for imperativo o transporte desse tipo de informações nessas mídias, é necessário que se dispense o mesmo tratamento dado aos discos rígidos: criptografia em todos os dados.

Assim, em caso de extravio só se perde o *hardware* e não as noites de sono.

Governo britânico perde dados de 25 milhões de pessoas. http://g1.globo.com/Noticias/Tecnologia/0,,MUL187073-6174,00.html

8.7 Evite *lan houses*

As *lan houses* e *cyber* cafés são locais onde o usuário e os seus dados ficam muito expostos. Afinal, é difícil saber se o sistema operacional, antivírus e o *antispyware* dos computadores estão atualizados. É difícil saber se há *keyloggers* ou *screenloggers* instalados. Esses locais não são seguros para as informações e eles não têm como lhe dar essa garantia.

É recomendado que as *lan houses* e *cyber* cafés sejam frequentados apenas para jogar *on-line* e imprimir documentos. E mesmo assim, muito cuidado com o seu *pen drive*. Usar *e-mail*, mensageiros instantâneos, fazer compras *on-line*, nem pensar.

8.8 Não divulgue seu *e-mail* em qualquer lugar

É importante tratar o endereço de *e-mail* como se trata o número de seu próprio telefone celular. Não o informe para qualquer pessoa, sob risco de receber ligações indesejadas ou mesmo ligações a cobrar.

Existem muitas pessoas ganhando dinheiro de modo desonesto na internet. Quanto mais endereços válidos de *e-mail* elas conseguirem coletar, mais dinheiro irão receber. Quanto mais *spam* e *phishing* essas pessoas distribuírem, melhor pra elas e pior para todos os demais.

8.9 Não clique em tudo o que lhe oferecerem

O *spam* e o *phishing* são perigosos, pois são construídos para convencer as pessoas que clicar nos *links* que eles oferecem, é uma boa ideia.

É importante ter cuidado com os anexos em *e-mails.* Arquivos com extensões *.bat, *.cmd, *.com, *.dll, *.exe, *.pif, *.scr, *.url, *.vbe, *.vbs e *.ws são potencialmente perigosos.

É recomendado que, ao receber um *link* ou um arquivo anexado a um *e-mail*, perguntar ao remetente, se conhecido, se ele realmente mandou aquele objeto. Dá um pouquinho mais de trabalho, mas compensa.

As pessoas têm de ser mais atentas com esse tipo de golpe. Afinal, os tribunais de justiça, Receita Federal ou bancos não enviam *e-mails* contendo *links*, nem arquivos anexos. No Brasil, o *e-mail* não tem valor jurídico para intimação. Porém, alguns usuários se apavoram e saem distribuindo informações confidenciais sem pensar nas possíveis consequências.

8.10 Fazer cópias de segurança (*backup*)

As cópias de segurança são a única garantia que seus dados têm. Afinal, por mais cuidadosas que sejam as pessoas, ninguém está completamente a salvo de fatalidades.

É recomendado que todas as informações importantes sejam replicadas em outros meios de armazenamento, tais como CDs, DVDs, *pen drives* e discos rígidos externos, preferencialmente longe do armazenamento principal e protegidos com criptografia.

8.11 Manter-se atualizado

Os usuários devem se habituar a ler notícias em sítios especializados. Dessa forma, podem aprender com os erros daqueles que não foram muito cuidadosos, podem conhecer novos tipos de ataques, novos tipos de golpes etc.

Cracker "perde" *pen drive* para aplicar golpe.
http://info.abril.com.br/aberto/infonews/042007/26042007-19.shl

É recomendado avaliar constantemente as vulnerabilidades, ameaças, riscos e impactos a que estamos sujeitos todos os dias, e buscar identificar medidas de segurança para saná-los.

Dica importante: Lembre-se do dia 11 de setembro de 2001. Ninguém achou que podia acontecer e aconteceu.

8.12 Conhecer a cartilha de segurança para internet do CGI.br

O Comitê Gestor da Internet no Brasil (CGI.br) elaborou uma cartilha muito interessante sobre segurança na internet. É recomendado baixá-la, estudá-la e indicá-la aos familiares, amigos e colegas de trabalho ou escola. Trata-se de um material muito didático, acessível e excelente fonte de consulta. Pode ser obtida no sítio **http://cartilha.cert.br/**.

8.13 Ser ético

Viver com ética significa preocupar-se com as demais pessoas e com a sociedade. É ter o compromisso de respeitar a liberdade do próximo e de exigir o respeito à própria liberdade.

Estudo relaciona alta de crimes *on-line* com ex-funcionários de empresas de TI. http://g1.globo.com/Noticias/Tecnologia/0,,MRP1229453-6174,00.html

E o que ética tem a ver com Segurança da Informação? Tudo. Pessoas éticas não enganam, não ludibriam, não extorquem nem se aproveitam das fraquezas de seu semelhante. Pessoas éticas não procuram descobrir o segredo dos outros, suas senhas de acesso, nem enviam *spam*.

Ser ético é trabalhar para o bem de todos, em benefício de si mesmo.

Resumo

As pessoas são os principais atores da Segurança da Informação. Sua responsabilidade está em preservar a informação e os meios que a contém. Para isso, devem estar preocupadas em instalar *softwares* de segurança, cuidar para que os sistemas estejam sempre atualizados, fazer uma varredura semanal contra *malwares*, escolher boas senhas e trocá-las de tempos em tempos, cuidar de suas mídias removíveis, para que não se extraviem nem sejam descartadas com dados desprotegidos, cuidar de seu *e-mail*, pensar antes de clicar em um *link*, fazer *backup*, manter-se atualizado e sempre estudando, e ser ético.

Atividades de aprendizagem

1. Pesquise na internet e elabore um texto descrevendo o conceito, a finalidade e os tipos de técnicas usadas pela Engenharia Social.

2. Pesquise na internet e elabore um texto descrevendo os tipos de *backup* existentes, suas vantagens e desvantagens.

Poste os arquivos com suas respostas e justificativas no AVEA.

Referências

BROCHI, Adinei. **Satélite Bolinha:** informações sobre os satélites militares SatCom**.** Disponível em: < http://www.py2adn.com/artigos/Satelite-Bolinha.pdf>. Acesso em: 15 jun. 2009.

BURNETT, Steve; PAINE, Stephen. **Criptografia e segurança:** o guia oficial RSA. Rio de Janeiro: Editora Campus, 2002.

CERT.BR –Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Cartilha de segurança para internet.** Versão 3.1. Disponível em: <http://cartilha.cert.br/>. Acesso em: 15 jun. 2009.

CERT.ORG Coordination Center. **About.** Disponível em: <http://www.cert.org/meet_cert/>. Acesso em: 15 jun. 2009.

COMPUTER ECONOMICS. **Malicious code attacks had $13.2 billion economic impact in 2001.** Disponível em: <http://www.computereconomics.com/article.cfm?id=133>. Acesso em: 15 jun. 2009.

CURTIN, Matthew. **Projeto DESCHALL.** Disponível em: <http://www.interhack.net/projects/deschall/>. Acesso em: 15 jun. 2009.

DAS ÜBERGEEK. **Brasileiros são presos por utilizar ilegalmente satélite americano.** Geek, 2009. Disponível em: <http://www.geek.com.br/blogs/832697632/posts/9852-brasileiros-sao-presos-por-utilizar-ilegalmente-satelite-americano>. Acesso em: 15 jun. 2009.

D'ÁVILA, Márcio Henrique C. **Phishing Scam:** a fraude inunda o correio eletrônico**.** Disponível em: <http://www.mhavila.com.br/topicos/seguranca/scam.html>. Acesso em: 17 set. 2009.

ELETRONIC FRONTIER FOUNDATION. **"DES Cracker" machine.** Disponível em:<http://w2.eff.org/Privacy/Crypto/Crypto_misc/DESCracker/HTML/19980716_eff_des_faq.html>. Acesso em: 15 ago. 2009.

ÉPATÊ. **11 de setembro.** Disponível em: <http://www.softsis.com.br/epate/11-de-setembro>. Acesso em: 15 jun. 2009.

FERNANDES, Natália Castro. **Twofish.** Disponível em: <http://www.gta.ufrj.br/~natalia/SSH/twofish.html>. Acesso em: 15 jun. 2009.

FUNARO, Vânia Martins et al. **Diretrizes para apresentação de dissertações e teses da USP:** documento eletrônico e impresso. 2.ed. São Paulo: USP, 2009.

G1. **Estudo relaciona alta de crimes on-line com ex-funcionários de empresas deTI.** Disponível em:<http://g1.globo.com/Noticias/Tecnologia/0,,MRP1229453-6174,00.html>. Acesso em: 10 ago. 2009.

__. **Falso antivírus cobra US$ 50 para liberar arquivos 'sequestrados'.** Disponível em: <http://g1.globo.com/Noticias/Tecnologia/0,,MRP1087313-6174,00.html>. Acesso em: 10 ago. 2009.

__. **Governo britânico perde dados de 25 milhões de pessoas.** Disponível em: <http://g1.globo.com/Noticias/Tecnologia/0,,MUL187073-6174,00.html>. Acesso em: 15 jun. 2009.

__. **Médica britânica perde mais de R$ 1 milhão com golpe virtual.** Disponível em: < http://g1.globo.com/Noticias/Tecnologia/0,,MRP1094096-6174,00.html>. Acesso em: 15 jun. 2009.

__. **Spam responde por 97% das mensagens de e-mail, diz Microsoft.** Disponível em: < http://g1.globo.com/Noticias/Tecnologia/0,,MRP1077797-6174,00.html>. Acesso em: 15 jun. 2009.

INFO ONLINE. **A história secreta do Conficker.** Disponível em: <http://info.abril.com.br/noticias/seguranca/a-historia-secreta-do-conficker-14092009-14.shl>. Acesso em: 20 set. 2009.

_____. **Cracker "perde" pendrive para aplicar golpe.** Disponível em: <http://info.abril.com.br/aberto/infonews/042007/26042007-19.shl>. Acesso em: 20 set. 2009.

_____. **Microsoft acaba com AutoPlay no Windows.** Disponível em: <http://info.abril.com.br/noticias/seguranca/microsoft-acaba-com-autoplay-no-windows-15092009-4.shl>. Acesso em: 20 set. 2009.

_____. **Piratas virtuais anunciam "sequestro" de dados e exigem US$ 10 milhões nos EUA.** Disponível em: <http://www1.folha.uol.com.br/folha/informatica/ult124u561249.shtml>. Acesso em: 20 set. 2009.

MCAFEE. **Security insights – fatos relevantes:** Medindo riscos para analisar a vulnerabilidade. 2003. Disponível em: <http://www.mcafee.com/br/enterprise/security_insights/measuring_risk_gauge_vulnerability.html>. Acesso em: 15 jun. 2009.

MICROSOFT. **Estratégias de gerenciamento de riscos de malware.** 2006. Disponível em: < http://technet.microsoft.com/pt-br/library/cc875818.aspx>. Acesso em: 21 dez. 2009.

_____. **Qual é a diferença entre reprodução automática e execução automática?** Disponível em: < http://windows.microsoft.com/pt-PT/windows-vista/Whats-the-difference-between-AutoPlay-and-autorun>. Acesso em: 30 jun. 2009.

_____. **The Antivirus Defense-in-Depth Guide.** 2004. Disponível em: < http://download.microsoft.com/download/a/d/c/adc58511-8285-465b-87fb-d19fe6d461c1/Antivirus_Defense-in-Depth_Guide.pdf>. Acesso em: 21 dez. 2009.

MÓDULO EDUCATION CENTER. **Curso básico em segurança da informação - 1st Step.** Rio de Janeiro. 2003. 1 CD-ROM.

MOSES, Asher. **Hackers rake in fortune selling fake anti-virus software. Sydney Morning Herald.** Disponível em: <http://www.smh.com.au/news/technology/security/hackers-rake-in-fortune-selling-fake-antivirus-software/2008/11/05/1225560902070.html>. Acesso em: 20 jun. 2009.

REDE NACIONAL DE ENSINO E PESQUISA. **Múltiplas vulnerabilidades no Cisco IOS.** Disponível em: <http://www.rnp.br/cais/alertas/2008/secunia-sa31990.html>. Acesso em: 15 jun. 2009.

_____. **Vulnerabilidade de DoS em dispositivos wireless IEEE 802.11.** Disponível em: <http://www.rnp.br/cais/alertas/2004/AusCERT-AA-200402.html>. Acesso em: 15 jun. 2009.

_____. **Vulnerabilidades em implementação do NTP.** Disponível em: < http://www.rnp.br/cais/alertas/2009/uscert-vu853097.html>. Acesso em: 15 jun. 2009.

ROHR, Altieres. **Spam. Linha Defensiva**, 2005. Disponível em: <http://www.linhadefensiva.org/2005/11/spam/>. Acesso em: 15 jun. 2009.

_____. Resquícios em memória RAM permitem quebra de criptografia de discos rígidos. **Linha Defensiva**, 2008. Disponível em: < http://www.linhadefensiva.org/2008/02/criptografia-hd-analise-ram/>. Acesso em: 15 jun. 2009.

SAMOSSEIKO, Dmitry. **What is it & why should you care.** Disponível em: < http://www.sophos.com/sophos/docs/eng/marketing_material/samosseiko-vb2009-paper.pdf >. Acesso em: 10 out. 2009.

SECRETARIA DA RECEITA FEDERAL DO BRASIL. **Linha do tempo.** Disponível em: <http://www.receita.fazenda.gov.br/10anos/linhatempo/default.htm>. Acesso em: 20 out. 2009.

SCHNEIER, Bruce. **Secrets and lies:** digital security in a networked world. London: Wiley. 2004.

SINGH, Simon. **O Livro dos códigos.** Rio de Janeiro:Editora Record,2001.

TERRA NOTÍCIAS. **Descoberta rede de espionagem chinesa que agia em 103 países.** Disponível em: <http://noticias.terra.com.br/mundo/interna/0,,OI3666205-EI10495,00.html>. Acesso em: 20 ago. 2009.

TERRA TECNOLOGIA. **Erro de programação inofensivo vira ameaça à segurança.** Disponível em: <http://tecnologia.terra.com.br/interna/0,,OI1790208-EI4805,00.html>. Acesso em: 15 jun. 2009.

_____. **HDs usados facilitam roubo de identidade.** Disponível em: <http://tecnologia.terra.com.br/interna/0,,OI1947225-EI4799,00.html>. Acesso em: 15 jun. 2009.

_____. **HDs usados podem conter informações privadas.** Disponível em: < http://tecnologia.terra.com.br/interna/0,,OI1430371-EI4801,00.html>. Acesso em: 15 jun. 2009.

_____. **Veja os 10 casos mais curiosos de perda e recuperação de dados.** Disponível em: < http://tecnologia.terra.com.br/interna/0,,OI1284657-EI4799,00.html>. Acesso em: 15 jun. 2009.

TKOTZ, Viktoria. **Esteganografia.** Aldeia Numaboa. Disponível em: <http://www.numaboa.com.br/criptografia/esteganografia>. Acesso em: 15 jun. 2009.

TREND MICRO DEVICES INC. **PC-cillin virus immune system user's manual.** 1994.

WIKIPÉDIA. **AES.** Disponível em: <http://pt.wikipedia.org/wiki/AES>. Acesso em: 15 jun. 2009.

_____. **ARPANET.** Disponível em: <http://pt.wikipedia.org/wiki/Arpanet>. Acesso em: 15 jun. 2009.

_____. **Assinatura digital.** Disponível em: <http://pt.wikipedia.org/wiki/Assinatura_digital>. Acesso em: 15 jun. 2009.

_____. **Ataques de 11 de setembro.** Disponível em: <http://pt.wikipedia.org/wiki/Ataques_de_11_de_Setembro_de_2001>. Acesso em: 15 jun. 2009.

_____. **Banda larga.** Disponível em: <http://pt.wikipedia.org/wiki/Banda_larga>. Acesso em: 15 jun. 2009.

_____. **Boot.** Disponível em: <http://pt.wikipedia.org/wiki/Boot>. Acesso em: 15 jun. 2009.

_____. **Buffer overflow.** Disponível em: <http://pt.wikipedia.org/wiki/Buffer_overflow>. Acesso em: 15 jun. 2009.

_____. **Câmaras negras.** Disponível em: <http://en.wikipedia.org/wiki/Cabinet_noir>. Acesso em: 15 jun. 2009.

_____. **Cifra de Vigenère.** Disponível em: <http://pt.wikipedia.org/wiki/Cifra_de_Vigen%C3%A8re>. Acesso em: 15 jun. 2009.

_____. **Compact disc.** Disponível em: <http://pt.wikipedia.org/wiki/CD>. Acesso em: 15 jun. 2009.

_____. **Cookie.** Disponível em: <http://pt.wikipedia.org/wiki/Cookie>. Acesso em: 15 jun. 2009.

_____. **Cópia de segurança.** Disponível em: <http://pt.wikipedia.org/wiki/C%C3%B3pia_de_seguran%C3%A7a>. Acesso em: 15 jun. 2009.

_____. **Criptografia de chave privada.** Disponível em: <http://pt.wikipedia.org/wiki/Criptografia_Sim%C3%A9trica>. Acesso em: 15 jun. 2009.

_____. **Criptografia de chave pública.** Disponível em: <http://pt.wikipedia.org/wiki/Criptografia_de_chave_pública>. Acesso em: 15 jun. 2009.

_____. **Data Encryption Standard**. Disponível em: <http://pt.wikipedia.org/wiki/Data_Encryption_Standard>. Acesso em: 15 jun. 2009.

_____. **DCOM.** Disponível em: <http://pt.wikipedia.org/wiki/DCOM>. Acesso em: 15 jun. 2009.

_____. **DES-Triplo.** Disponível em: <http://pt.wikipedia.org/wiki/3DES>. Acesso em: 15 jun. 2009.

_____. **Disco Blu-ray.** Disponível em: <http://pt.wikipedia.org/wiki/Disco_Blu-ray>. Acesso em: 15 jun. 2009.

_____. **DVD.** Disponível em: <http://pt.wikipedia.org/wiki/DVD>. Acesso em: 15 jun. 2009.

_____. **ENIAC.** Disponível em: <http://pt.wikipedia.org/wiki/Eniac>. Acesso em: 15 jun. 2009.

_____. **Enigma_(máquina).** Disponível em: <http://pt.wikipedia.org/wiki/Enigma_%28m%C3%A1quina%29>. Acesso em: 15 jun. 2009.

_____. **Enron Corporation.** Disponível em: <http://pt.wikipedia.org/wiki/Enron>. Acesso em: 15 jun. 2009.

_____. **Escrita cuneiforme.** Disponível em: <http://pt.wikipedia.org/wiki/Cuneiforme>. Acesso em: 15 jun. 2009.

_____. **FAT32.** Disponível em: <http://pt.wikipedia.org/wiki/FAT32>. Acesso em: 15 jun. 2009.

_____. **Firewall.** Disponível em: <http://pt.wikipedia.org/wiki/Firewall>. Acesso em: 15 jun. 2009.

_____. **Freeware.** Disponível em: <http://pt.wikipedia.org/wiki/Software_gratuito>. Acesso em: 15 jun. 2009.

_____. **FTP.** Disponível em: <http://pt.wikipedia.org/wiki/Ftp>. Acesso em: 15 jun. 2009.

_____. **Gadget.** Disponível em: <http://pt.wikipedia.org/wiki/Gadget>. Acesso em: 15 jun. 2009.

_____. **Guerra Fria.** Disponível em: <http://pt.wikipedia.org/wiki/Guerra_fria>. Acesso em: 15 jun. 2009.

_____. **GUID.** Disponível em: <http://pt.wikipedia.org/wiki/GUID>. Acesso em: 15 jun. 2009.

_____. **Hash.** Disponível em: <http://pt.wikipedia.org/wiki/Hash >. Acesso em: 15 jun. 2009.

_____. **IBM System 360.** Disponível em: <http://pt.wikipedia.org/wiki/IBM_System/360>. Acesso em: 15 jun. 2009.

_____. **ISSA.** Disponível em: <http://pt.wikipedia.org/wiki/ISSA >. Acesso em: 15 jun. 2009.

_____. **Lei Sarbanes-Oxley.** Disponível em: <http://pt.wikipedia.org/wiki/Sarbanes-Oxley>. Acesso em: 15 jun. 2009.

_____. **Linux.** Disponível em: <http://pt.wikipedia.org/wiki/GNU/Linux>. Acesso em: 15 jun. 2009.

_____. **Mac OS X.** Disponível em: <http://pt.wikipedia.org/wiki/Mac_OS_X>. Acesso em: 15 jun. 2009.

_____. **Malware.** Disponível em: <http://pt.wikipedia.org/wiki/Malware>. Acesso em: 15 jun. 2009.

_____. **Memórias SSD.** Disponível em: <http://pt.wikipedia.org/wiki/SSD>. Acesso em: 15 jun. 2009.

_____. **Mineração de dados.** Disponível em: <http://pt.wikipedia.org/wiki/Data_mining>. Acesso em: 15 jun. 2009.

_____. **MS-DOS.** Disponível em: <http://pt.wikipedia.org/wiki/MS-DOS>. Acesso em: 15 jun. 2009.

_____. **Multics.** Disponível em: <http://pt.wikipedia.org/wiki/Multics>. Acesso em: 15 jun. 2009.

_____. **Navegador.** Disponível em: <http://pt.wikipedia.org/wiki/Navegador >. Acesso em: 15 jun. 2009.

_____. **Partição.** Disponível em: <http://pt.wikipedia.org/wiki/Parti%C3%A7%C3%A3o>. Acesso em: 15 jun. 2009.

_____. **Peer-to-peer.** Disponível em: <http://pt.wikipedia.org/wiki/P2P >. Acesso em: 15 jun. 2009.

_____. **Redes sociais virtuais.** Disponível em: <http://pt.wikipedia.org/wiki/Redes_Sociais_Virtuais>. Acesso em: 15 jun. 2009.

_____. **Revolução digital.** Disponível em: <http://pt.wikipedia.org/wiki/Revolu%C3%A7%C3%A3o_digital>. Acesso em: 15 jun. 2009.

_____. **RSA.** Disponível em: <http://pt.wikipedia.org/wiki/rsa>. Acesso em: 15 jun. 2009.

_____. **Selo de tempo.** Disponível em: <http://pt.wikipedia.org/wiki/Selo_cronol%C3%B3gico>. Acesso em: 15 jun. 2009.

_____. **Serpent.** Disponível em: <http://en.wikipedia.org/wiki/Serpent_(cipher)>. Acesso em: 15 jun. 2009.

_____. **Skype.** Disponível em: <http://pt.wikipedia.org/wiki/Skype>. Acesso em: 15 jun. 2009.

_____. **Software livre.** Disponível em: <http://pt.wikipedia.org/wiki/Software_livre>. Acesso em: 15 jun. 2009.

_____. **Solid State Drive - SSD.** Disponível em: <http://pt.wikipedia.org/wiki/SSD>. Acesso em: 15 jun. 2009.

_____. **Sputinik.** Disponível em: <http://pt.wikipedia.org/wiki/Sputnik>. Acesso em: 15 jun. 2009.

_____. **Spyware.** Disponível em: <http://pt.wikipedia.org/wiki/Spyware>. Acesso em: 15 jun. 2009.

_____. **Switch.** Disponível em: <http://pt.wikipedia.org/wiki/Switch>. Acesso em: 15 jun. 2009.

_____. **TCP/IP.** Disponível em: <http://pt.wikipedia.org/wiki/TCP/IP>. Acesso em: 15 jun. 2009.

_____. **Token.** Disponível em: <http://pt.wikipedia.org/wiki/Token_(chave_eletr%C3%B4nica)>. Acesso em: 15 jun. 2009.

_____. **Ultra DMA.** Disponível em: <http://pt.wikipedia.org/wiki/ATA>. Acesso em: 15 jun. 2009.

_____. **USB.** Disponível em: <http://pt.wikipedia.org/wiki/Usb>. Acesso em: 15 jun. 2009.

_____. **VBA.** Disponível em: <http://pt.wikipedia.org/wiki/Visual_Basic_for_Applications>. Acesso em: 15 jun. 2009.

_____. **Worms.** Disponível em: <http://pt.wikipedia.org/wiki/Worm>. Acesso em: 15 jun. 2009.

_____. **WWW.** Disponível em: <http://pt.wikipedia.org/wiki/Www>. Acesso em: 15 jun. 2009.

YAHOO BRASIL. **12% dos usuários de e-mail respondem a spams, diz estudo.** Disponível em: <http://br.tecnologia.yahoo.com/article/20072009/7/tecnologia-12-dos-usuarios-mail-respondem.html>. Acesso em: 30 jun. 2009.

_____. **Central de informações sobre privacidade.** Disponível em: <http://info.yahoo.com/privacy/br/all/>. Acesso em: 30 jun. 2009.

ZIMMERMANN, Philip. **Por que você precisa do PGP?** Disponível em: < http://www.dca.fee.unicamp.br/pgp/why_PGP.shtml>. Acesso em: 30 jun. 2009.

Currículo do professor-autor

Jorge Procópio da Costa Novo possui graduação em Tecnologia em Processamento de Dados pelo Instituto Manauara de Ensino Superior (1998), graduação em Direito (1999) e especialização em Informática para Aplicações Empresariais (2001), ambas pela Universidade Federal do Amazonas. Tem experiência na área de Ciência da Computação, com ênfase em Segurança da Informação, atuando principalmente nos seguintes temas: criptografia, segurança da informação, direito eletrônico e projetos de redes de dados. Atualmente é um dos administradores de Rede de Dados da Universidade do Estado do Amazonas (UEA).

ISBN 978-85-63576-20-0