PONTIFÍCIA UNIVERSIDADE CATÓLICA DE CAMPINAS

CEATEC

RANIERI MARINHO DE SOUZA

IMPLANTAÇÃO DE FERRAMENTAS E TÉCNICAS DE SEGURANÇA DA INFORMAÇÃO EM CONFORMIDADE COM AS NORMAS ISO 27001 E ISO 17799

CAMPINAS

2007

RANIERI MARINHO DE SOUZA

IMPLANTAÇÃO DE FERRAMENTAS E TÉCNICAS DE SEGURANÇA DA INFORMAÇÃO EM CONFORMIDADE COM AS NORMAS ISO 27001 E ISO 17799

Dissertação apresentada como exigência para obtenção do Título de Mestre em Gestão de Redes de Telecomunicações, ao Programa de Pós-Graduação na área Engenharia Elétrica, da Pontifícia Universidade Católica de Campinas.

Orientador: Prof. Dr. Eric Alberto de Mello Fagotto

PUC-CAMPINAS

2007

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE CAMPINAS

GRÃO-CHANCELER

Dom Bruno Gamberini

MAGNÍFICO REITOR

Prof. Pe. Wilson Denadai

VICE-REITORA

Prof[a]. Dra. Ângela de Mendonça Engelbrecht

PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO

Prof[a]. Dra. Vera Engler Cury

DIRETOR DO CENTRO DE CIÊNCIAS EXATAS, AMBIENTAIS E DE TECNOLOGIAS

Prof. Dr. Orandi Mina Falsarella

COORDENADOR DO PROGRAMA DE

PÓS-GRADUAÇÃO STRICTO SENSU EM ENGENHARIA ELÉTRICA

CURSO DE MESTRADO PROFISSIONAL EM GESTÃO DE REDES DE TELECOMUNICAÇÕES

ÁREA DE CONCENTRAÇÃO: GESTÃO DE REDES E SERVIÇOS

Prof. Dr. Orandi Mina Falsarella

Ficha Catalográfica
Elaborada pelo Sistema de Bibliotecas e
Informação - SBI - PUC-Campinas

t005.8
S729i

Souza, Ranieri Marinho de.
Implantação de ferramentas e técnicas de segurança da informação em conformidade com as normas ISO 27001 e ISO 17799 / Ranieri Marinho de Souza. - Campinas: PUC-Campinas, 2007.
p.

Orientador: Eric Alberto de Mello Fagotto.
Dissertação (mestrado) - Pontifícia Universidade Católica de Campinas, Centro de Ciências Exatas, Ambientais e de Tecnologias, Pós-Graduação em Engenharia Elétrica.
Inclui índice e bibliografia.

1. Redes de computação - Medidas de segurança. 2. Computadores - Medidas de segurança. 3. Organização Internacional de Normalização. 4. Tecnologia da Informação. 5. Telecomunicações. I. Fagotto, Eric Alberto de Mello. II. Pontifícia Universidade Católica de Campinas. Centro de Ciências Exatas, Ambientais e de Tecnologias. Pós-Graduação em Engenharia Elétrica. III. Título.

22.ed.CDD - t005.8

RANIERI MARINHO DE SOUZA

IMPLANTAÇÃO DE FERRAMENTAS E TÉCNICAS DE SEGURANÇA DA INFORMAÇÃO EM CONFORMIDADE COM AS NORMAS ISO 27001 E ISO 17799

Dissertação apresentada ao Curso de Mestrado Profissional em Gestão de Redes de Telecomunicações do Centro de Ciências Exatas, Ambientais e de Tecnologias da Pontifícia Universidade Católica de Campinas como requisito parcial para obtenção do título de Mestre em Gestão de Redes de Telecomunicações.
Área de Concentração: Gestão de Redes e Serviços .
Orientador: Prof. Dr. Eric Alberto de Melo Fagotto

Dissertação defendida e aprovada em 15 de fevereiro de 2008 pela Comissão Examinadora constituída dos seguintes professores:

Prof. Dr. Eric Alberto de Melo Fagotto
Orientador da Dissertação e Presidente da Comissão Examinadora
Pontifícia Universidade Católica de Campinas

Prof. Dr. Omar Carvalho Branquinho
Pontifícia Universidade Católica de Campinas

Prof. Dr. Jürgen Josef Bohn
Universidade Estadual de Campinas

A minha querida esposa Rosimeire,
pelo apoio incondicional em todos os momentos,
aos meus adoráveis filhos Vítor e Vitória pela paciência,
compreensão e apoio em todos os momentos desta jornada.

AGRADECIMENTOS

A Deus,

Pela força e vontade para trilhar os caminhos que me levaram a concluir este mestrado.

Ao Prof. Dr. Eric Alberto de Mello Fagotto,

Pela amizade, paciência, dedicação e perseverança na orientação desta dissertação.

Ao Prof. Dr. Omar Carvalho Branquinho,

Pelo estímulo e importantes sugestões.

Aos colegas de curso de mestrado na figura dos amigos Alberto Lotito, Fernando Lino e Marcelo Ap. Morales pelo companheirismo, enriquecedoras trocas de idéias e incentivo recebido ao longo do curso.

Aos meus pais Joaquim e Ada,

Por me propiciarem a vida e os recursos necessários a trilhar o caminho da educação e do conhecimento.

As minhas irmãs Elisandra e Andiara,

Pelo incentivo e companheirismo ao logo de minha vida.

À Tecnicópias Gráfica e Editora Ltda,

Pela oportunidade de desenvolver o estudo de caso apresentado nesta dissertação.

Aos alunos das Faculdades Hoyler,

Por permitirem a multiplicação do conhecimento que conquistei ao longo do tempo.

Aos que prestigiaram a defesa, aos familiares e amigos que incentivaram e torceram pela conclusão deste trabalho.

"É melhor tentar e falhar, que preocupar-se e ver a vida passar;
é melhor tentar, ainda que em vão, que sentar-se fazendo nada até o final.
Eu prefiro na chuva caminhar, que em dias tristes em casa me esconder.
Prefiro ser feliz, embora louco, que em conformidade viver...".

Martin Luther King
(1929-1968)

RESUMO

SOUZA, Ranieri Marinho. Implantação de ferramentas e técnicas de segurança da informação em conformidade com as normas ISO 27001 e ISO 17799. Dissertação (Mestrado em Gestão de Redes de Telecomunicações) – Pós-Graduação em Engenharia Elétrica, Centro de Ciências Exatas, Ambientais e de Tecnologias, Pontifícia Universidade Católica de Campinas. Campinas, 2007.

A evolução tecnológica que estamos vivendo tanto em relação aos *softwares* de computador quanto aos equipamentos de informática que abastecem o mercado também ocorre em relação às ameaças no assim chamado mundo virtual. Aliado ao fato do avanço tecnológico temos ainda a popularização do acesso à Internet por banda larga, que possibilita uma maior velocidade na proliferação de ameaças. No entanto, os mecanismos de segurança da informação nem sempre estão aptos a detê-las, sendo, portanto, necessário desenvolver um projeto de segurança adequado aos negócios e características de cada empresa, pois um conhecimento específico das vulnerabilidades é um passo fundamental para se minimizar os efeitos de qualquer eventual ameaça. Em vista desse cenário, neste trabalho apresentamos um método para prover a segurança da informação em organizações que utilizem recursos de redes de computadores e de telecomunicações.

Termos de indexação: segurança, tecnologia, informação, telecomunicações, ISO 17799 e ISO 27001.

ABSTRACT

SOUZA, Ranieri Marinho. Implantação de ferramentas e técnicas de segurança da informação em conformidade com as normas ISO 27001 e ISO 17799. Dissertação (Mestrado em Gestão de Redes de Telecomunicações) – Pós-Graduação em Engenharia Elétrica, Centro de Ciências Exatas, Ambientais e de Tecnologias, Pontifícia Universidade Católica de Campinas. Campinas, 2007.

The technical evolution that we are living both in relation to the computer programs and to the hardware equipments that supply the market, it also happens to the threats in the virtual world. Besides the technological advance, we also have the popularization of the broadband Internet access, which makes possible a faster threats proliferation. However, the mechanisms of information security not always are able to withhold such threats, being therefore, necessary to develop a security project tailored to the characteristics of businesses of each company, because a specific knowledge of the vulnerabilities is a fundamental step to minimize the effects of any eventual threat. Bearing this scenario in mind, in this work we present a method to provide information security to organizations that use telecommunications and computer networks resources.

Index terms: security, technology, information, telecommunications, ISO 17799 and ISO 27001

LISTA DE FIGURAS

LISTA DE GRÁFICOS

LISTA DE QUADROS E TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT	= Associação Brasileira de Normas Técnicas
AD	= Active Directory
AW	= Ataque à Servidor Web
CD-ROM	= Compact Disc Ready-Only Memory
CERT.br	= Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CGI	= Common Gateway Interface
DES	= Data Encryption Standard
DHCP	= Dynamic Host Control Protocol
DNS	= Domain Name System
DoS	= Denial of Service
DSS	= Digital Signature Standard
FTP	= File Transfer Protocol
HASH	= Equação matemática que utilize texto para criar códigos MD
HIDS	= Host-Based Intrusion Detection
HTTP	= Hypertext Transfer Protocol
IBM	= International Business Machines
IDS	= Sistema de Detecção de Intrusos do Inglês: Intrusion Detection System
IIS	= Internet Information Server
IP	= Internet Protocol
ISO	= International Organization for Standardization
JPEG	= Joint Photographic Experts Group – Formato de compressão de imagens
LAN	= Rede local do Inglês: Local Area Network
LDAP	= Lightweight Directory Access Protocol
LOG	= Arquivo de Registro de Informações
MD	= Message Digest
MP3	= MPEG-1/2 Audio Layer 3 – Formato de compressão de áudio
MIT	= Massachusetts Institute of Technology
NIDS	= Network-Based Intrusion Detection
NIST	= National Institute of Standards and Technology
PDCA	= Plan-Do-Check-Act
PGP	= Pretty Good Privacy

PKI	= Public Key Infrastructure
RAM	= Random Access Memory
RDP	= Remote Desktop Control
RFC	= Request for Comment
RIPE	= Race Integrity Primitives Evaluation
RSA	= Rivest, Shamir, Adleman
SGSI	= Sistema de Gestão da Segurança da Informação
SHA	= Secure Hash Algorithm
SHS	= Secure Hash Standard
SI	= Sistema de Informação
SLA	= Service Level Agreement
SMB	= Server Message Block
SMTP	= Simple Mail Transfer Protocol
SQL	= Structured Query Language
SSH	=Secure Shell
TCP-IP	= Transmission Control Protocol- Internet Protocol
TI	= Tecnologia da Informação
TS	= Terminal Server
UDP	= User Datagram Protocol
VPN	= Virtual Private Network
WEB	= Forma reduzida de WWW (World Wide Web)

SUMÁRIO

1 INTRODUÇÃO

1.1 Motivação

Nossa motivação para a criação de um método voltado à segurança da informação em um ambiente empresarial pode ser prontamente entendida uma vez que vivemos em plena “Era da Informação” (ALBERTIN, 2001, p.20-22). Dentro deste contexto, uma empresa deverá proteger a informação associada aos seus negócios por diversas razões, dentre elas: a existência de segredos industriais próprios e/ou de parceiros que devem ser tratados de maneira confidencial, pois podem comprometer a imagem dos negócios.

A implantação desses sistemas irá conduzir a uma sensível transformação cultural e organizacional na vida da empresa. Soluções diversas estarão à disposição e ações executadas, de forma a propiciar a competitividade da empresa perante ao mercado.

Além disso, o sistema de segurança da informação deve garantir que a informação seja verificável, completa, útil e eficaz (LAUDON, 2003, p.3-18).

O método que desenvolvemos e apresentamos nesta dissertação deriva de uma leitura cuidadosa das normas ISO 27001 (ABNT ISO 27001) e ISO 17799 (ABNT ISO 17799) e envolve, quando de sua aplicação, a utilização de ferramentas de software e o estabelecimento de políticas de segurança com vistas a atender às necessidades da empresa e às melhores práticas do mercado.

1.2 Objetivos do trabalho

Atualmente, é consenso geral o imperativo de se estabelecer a segurança da informação no meio organizacional face aos constantes ataques (digitais ou por outros meios) e à necessidade de se transmitir uma imagem de confiabilidade aos parceiros e clientes (LAUDON, 2003, p.260-282). Para isso, torna-se fundamental para o gerenciamento de informações nas organizações o uso de ferramentas e técnicas que acompanhem em tempo real as mudanças

tecnológicas e o aparecimento de novas ameaças. Deste modo, o objetivo geral desta dissertação é o desenvolvimento de um método que, se aplicado, colaborará para a segurança da informação de uma organização de qualquer porte.

Entende-se como objetivo específico desta dissertação a realização de um estudo das melhores práticas do mercado associadas às tecnologias disponíveis de *hardware* e *software*, voltadas à segurança da informação em um ambiente empresarial.

1.3 Métodos de pesquisa

Na primeira fase da pesquisa, foi realizado um levantamento da literatura e dos fundamentos básicos de segurança da informação.

Na segunda fase, desenvolvemos *benchmarkings* de ferramentas de *hardware* e *software* utilizadas no mercado a fim de escolher as soluções mais adequadas ao projeto de segurança.

Na terceira fase desenvolvemos um método para implantação de segurança da informação tomado como base as normas ISO 27001 e ISO 17799.

Na quarta e última fase foi realizada a implantação do projeto de segurança da informação baseado no método proposto nesta dissertação.

1.4 Organização da dissertação

No capítulo 1 é fornecida uma visão geral do trabalho, com seus objetivos, justificativa e os resultados esperados.

Já no capítulo 2 de Segurança da Informação, apresentamos o conteúdo necessário para o entendimento dos assuntos tratados neste documento.

No capítulo 3 apresentamos as normas ISO 27001 e ISO 17799 que contêm requisitos para segurança da informação.

O capítulo 4 trata do método proposto para implantação do projeto de segurança da informação em uma organização.

Já no capítulo 5, discutimos a aplicação do método em uma empresa real e os resultados obtidos.

No capítulo 6, são apresentadas as conclusões deste estudo, bem como perspectivas para novos trabalhos.

2 Segurança da Informação

Neste capítulo apresentamos fundamentos básicos de segurança da informação que acreditamos ser importantes para entender os diversos aspectos envolvidos nesta dissertação e também apresentar ferramentas de *hardware* e *software* (a partir deste ponto consideramos ferramentas como sendo o conjunto de *hardware* e *software*), bem como técnicas empregadas em projetos de segurança.

A Segurança da Informação é um tema importante para qualquer empresa (SÊMOLA, 2003, p.39-41), uma vez que vivemos um momento de grande utilização da informação com uma freqüência muito maior do que em qualquer época da civilização humana. Assim, precisamos de uma infra-estrutura de comunicação que suporte todas as transações executadas e também permita o armazenamento de todos os dados de modo seguro.

O valor da informação muitas vezes não é facilmente mensurável dada à quantidade crescente de dados que as empresas possuem e, por conta disso, torna-se essencial identificar todos os elementos que compõem a comunicação de dados (WADLOW, 2000, p.1-10). Esses podem ser divididos em quatro categorias de ativos, são eles:

- As Informações: dados armazenados em meio magnético ou físico, como relatórios, planilhas, configurações entre outros;
- A infra-estrutura de suporte às informações: computadores, mídias, elementos de rede e softwares de computador;
- As pessoas que utilizam as informações: todos os indivíduos que manipulam as informações;
- Estrutura física e organizacional: salas, mesas, armários dentre outros.

2.1 Princípios da Segurança da Informação

Devemos proteger os ativos contra ameaças de todos os tipos, a fim de garantir os três princípios básicos da segurança da informação que são (ABNT ISO 17799, 2005, p.2). Conforme comentado anteriormente, esses princípios são:

- Confidencialidade: as informações devem ser conhecidas apenas pelos indivíduos que detêm as permissões de acesso, evitando assim o “vazamento” de informação e dificultando a espionagem industrial;

- Integridade: as informações devem ser mantidas no seu estado original, sem alterações, garantindo a quem as receber, a certeza de que não foram falsificadas, corrompidas ou alteradas;

- Disponibilidade: o acesso a todos os dados no momento que for necessário para utilização.

2.2 Ameaças

Por ameaças entendem-se os elementos que têm a condição de explorar vulnerabilidades e causar problemas severos aos ativos de uma empresa (MÓDULO, 2007). Os ativos estão continuamente expostos às ameaças existentes, que podem colocar em risco os três princípios da segurança (confidencialidade, integridade e disponibilidade) Dentre as várias classificações na literatura, podemos citar as seguintes:

- Naturais: condições da natureza que podem causar danos como, por exemplo: incêndio, enchentes, terremotos;

- Intencionais: propositais como vírus de computador, espionagem, fraude, vandalismo, roubo entre outros;

- Involuntárias: originadas por falhas não intencionais dos usuários como acidentes, erros, falta de conhecimento dos ativos.

2.3 Vulnerabilidades

Vulnerabilidades são deficiências de diversas origens, as quais muitas vezes, não são identificadas a tempo ou, mesmo quando isso ocorre, não são devidamente tratadas de modo a evitar um ataque (NAKAMURA, 2002, p.29-89).

As vulnerabilidades podem ter origens diversas como apresentado na lista sugerida por SÊMOLA (SÊMOLA, 2003, p.48-49):

- Agentes da natureza umidade, poeira, poluição e calor podem causar danos aos ativos. Deve-se levar em consideração também fatores geográficos que possam resultar em ameaças. Por exemplo, instalações próximas a rios que causam inundações;

- *Hardwares*: falhas no dimensionamento do equipamento a ser utilizado, problemas de projeto e manutenção;

- *Softwares*: falhas no desenvolvimento que permitem a inclusão e execução de softwares com código malicioso.

- Mídias de armazenamento: falhas de fabricação ou estocagem de CD-ROM, discos rígidos, DVD-ROM entre outros.

- Meios de comunicação: problemas no cabeamento, antenas de rádio inadequadas entre outros problemas na infra-estrutura de comunicação.

- Humanas: relativas aos danos que o ser humano pode causar às informações quando de espionagem, má utilização e acidentes derivados da falta de treinamento, insatisfação com o trabalho, erros, dentre outros fatores.

2.4 Riscos

Quanto aos riscos, pode-se dizer que são a possibilidade das ameaças explorarem as vulnerabilidades, ocasionando danos ou perdas de dados, proporcionando prejuízos aos negócios da empresa e que acabam por afetar os princípios de confidencialidade, integridade e disponibilidade (MÓDULO, 2007).

Existem diversas formas de se analisar os riscos e por intermédio de um estudo que classifique as informações em categorias permitindo avaliar o impacto que uma ameaça pode trazer.

Entre estas formas está a análise do sistema de informação e o desenvolvimento de um plano de ação (ABNT ISO 27001, 2006).

2.5 Atacantes

Chamamos de atacantes os indivíduos que realizam um ataque a um sistema computacional, explorando suas vulnerabilidades, podendo ou não obter êxito (NAKAMURA, 2002, p.39-51). Os atacantes são mais conhecidos como *hackers*, no entanto, existe uma grande variedade de atacantes, dentre eles podemos citar:

- *Preackers*: responsáveis por fraudes em telefonia, atualmente o maior alvo é a telefonia celular;

- *Script Kiddies*: maior incidência de ataques, porém com pouco conhecimento técnico, utilizam ferramentas facilmente encontradas na internet;

- *Crackers*: possuem conhecimento avançado, sendo capazes de quebrar segurança de informações, destruindo sistemas e roubando bancos e instituições financeiras;

- *Carders*: responsáveis por fazer compras pela internet utilizando cartões de créditos roubados, ou mesmo clonando números de cartões através de *softwares* desenvolvidos para este fim;

- *Insiders*: colaboradores ou ex-colaboradores insatisfeitos de empresas que têm como objetivo roubar informações configurando espionagem ou mesmo agindo de forma a destruir sistemas e processos dos quais conhece.

Além dos tipos mencionados, existem outros como: *White Hats*, *Black Hats*, *Cyberpunks* e *Coders* (NAKAMURA, 2002, p.40-47) que são variantes do grupo de *Crackers*.

2.6 Ataques

Os ataques podem ocorrer quando as vulnerabilidades não são tratadas de modo a conter ou mesmo corrigir os problemas conhecidos.

Coletar informações da ocorrência dos tipos de ataques é um passo necessário para dar inicío à um plano de ação de segurança da informação, os ataques podem ter origem nas ameaças descritas na seção 2.3 deste trabalho (HATCH, 2003, p.225-646). A seguir apresentamos uma lista de ataques bem comuns:

- Ataque ao nível da aplicação: explora as vulnerabilidades dos softwares que utilizam o protocolo TCP-IP;

- Ataque a servidor *web* (AW): caracterizado pela exploração de vulnerabilidades em *softwares* para publicação de páginas web como o *Internet Information Server* (IIS) (MICROSOFT INTERNET INFORMATION SERVER, 2003) e APACHE (APACHE, 2008);

- *Buffer-overflow*: falha de controle da área de armazenamento temporário em memória RAM (*buffer*), também conhecidos como estouro de pilha e causam falhas em aplicações deixado-as indisponíveis;

- *Exploit*: *software* de código malicioso que explora vulnerabilidades dos mais diversos *softwares* como *Internet Explorer* (MICROSOFT INTERNET EXPLORER, 2007) e *Firefox* (FIREFOX, 2008). Caracteriza-se por causar mau funcionamento, ou mesmo a indisponibilidade da aplicação;

- *SQL-Injection*: é uma técnica que possibilita a inserção de um código na linguagem SQL (*Structured Query Language*) em páginas *web*, permitindo ao invasor o acesso ao servidor de banco de dados;

- *Trojan* ou Cavalo de Tróia: executa funções sem que o usuário atacado tenha conhecimento, permitindo que o computador seja explorado pelos invasores;

- Vírus: talvez a forma de ataque mais conhecida, é *software* que faz cópia de si mesmo, causando diversos problemas, tais como o mau funcionamento de *softwares*;

- *Worm*: *software* que não precisa ser executado para ser utilizado. Fornece informações que são transmitidas a *hackers* de modo secreto, sendo na maioria dos casos de modo imperceptível ao usuário;

- Ataque físico: caracterizado pelo roubo de equipamentos discos, fitas magnéticas, CD-ROM, disquetes ou outros meios de armazenamento de dados que são retirados da empresa para posterior análise ou destruição;

- *Denial of Service* (DoS): ataque de negação de serviço, responsável por sobrecarregar servidores com grande volume de informação, causando a parada do sistema operacional, provocando o preenchimento da memória do computador e a sobrecarga de operações do processador;

- *Packet Sniffing*: *software* que executa a captura de pacotes IP que podem conter informações importantes de *softwares* de bate-papo ou mesmo *softwares* de *e-mail* como o *Outlook Express* (MICROSOFT OUTLOOK EXPRESS, 2004). Um *software* bem conhecido é o *Ethereal* (ETHEREAL, 2007);

- *Scan*: também conhecido como *Port Scanning*, analisa portas IP que possuem serviços associados, como por exemplo, *telnet*. Entre os *softwares* mais utilizados para esta tarefa estão o *Nmap* (NMAP, 2008) e *Languard* (LANGUARD, 2008). Prestam-se também para descobrir vulnerabilidades diversas relacionadas ao protocolo TCP-IP e UDP (*User Datagram Protocol*).

Na seção 2.7 de ataques, citamos as ameaças mais comuns, contudo deve-se ter claro que tal lista não deve ser considerada exaustiva, pois existem muitas ameaças não identificadas e outras que possuem características de diversas ameaças (MÓDULO, 2007).

De acordo com o Gráfico 1, podemos observar os incidentes reportados por empresas situadas no Brasil ao CERT.br - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT 2007), no período compreendido entre os anos de 2001 e 2006.

É possível verificar no Gráfico 1 um aumento considerável no ano de 2006 em relação ao ano de 2005. Os dados ao longo dos anos atestam o número crescente de incidentes de segurança envolvendo comunicação pela *Internet*.

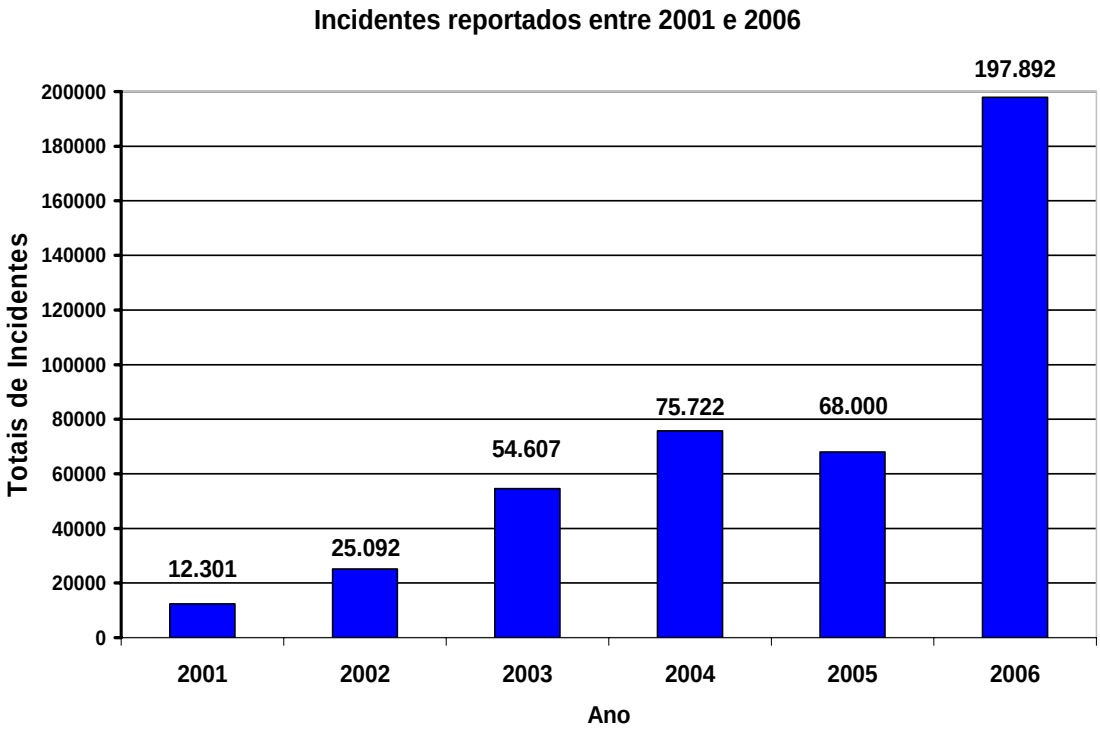


Gráfico 1: Totais de Incidentes de Segurança reportadas ao CERT.
Fonte: adaptado de CERT.br. Disponível em http://www.cert.br/estatisticas. Acesso: 30 nov. 2007.

Conforme mencionado na seção 1.1 desta dissertação, podemos entender que a quantidade de ocorrências de incidentes de segurança por si só motiva as empresas a pensarem a implantar segurança em seus negócios, visto que muitas informações são críticas. Algumas delas são secretas e possuem alto valor estratégico.

A implantação de segurança através de um método pode auxiliar as empresas nas mudanças culturais e organizacionais relacionadas à segurança da informação.

Na Tabela 1 possuímos os mesmos dados apresentados no Gráfico 1 de 2006, distribuídos mensalmente com percentuais por tipo de incidente.

Observa-se na Tabela 1 a grande quantidade de ocorrências dos tipos *Scan*, *Trojan* e *Worm*.

Tabela 1: Incidentes Reportados ao CERT – jan a dez de 2006.

MÊS	AW	DoS	Scan	Trojan	Worm	TOTAL
Janeiro	32	71	3.274	3.687	1.358	8.446
Fevereiro	54	33	2.737	3.636	1.223	7.742
Março	29	41	2.925	4.776	4.062	11.945
Abril	28	3	2.742	3.965	7.327	14.126
Maio	29	81	3.153	3.778	11.139	18.204
Junho	43	24	3.127	3.196	11.036	17.470
Julho	46	11	2.823	2.984	12.833	18.754
Agosto	37	4	5.160	3.295	8.961	17.501
Setembro	38	4	5.507	4.247	13.499	23.321
Outubro	35	3	6.823	2.766	8.944	18.592
Novembro	51	0	3.777	3.188	16.355	23.414
Dezembro	27	2	3.143	2.258	12.939	18.377
TOTAL	449	277	45.191	41.776	109.676	197.892

Fonte: adaptado de CERT.br. Disponível em http://www.cert.br/estatisticas. Acesso: 30 nov. 2007.

2.7 Ferramentas para Segurança da Informação

Chamamos de ferramentas para segurança da informação o conjunto de *software*, *hardware* e técnicas que têm como principal objetivo combater os ataques (CHESWICK, 2005, p.143-334). Elas são encontradas para diversas plataformas de sistemas operacionais como *Microsoft Windows* (MICROSOFT WINDOWS SERVER, 2003) e *Linux* (LINUX, 2008). Muitas dessas ferramentas são utilizadas em conjunto para assim prover maior segurança.

Na lista a seguir apresentam-se algumas ferramentas para segurança da informação que podem ser implantadas nas empresas.

- *Firewall*: é um tipo de *software* que pode ser dividido em várias categorias, mas que tem sempre o mesmo objetivo, que é o de não

permitir a entrada de pacotes IP e, deste modo, contendo ameaças. Entre os tipos disponíveis podemos destacar:

- Filtro de Pacote: utiliza regras estáticas para filtrar pacotes que têm origem em servidores externos. É bastante comum e considerado simples de ser configurado (CHESWICK, 2005, p.175-226). O *Iptables*, nativo do Linux (LINUX, 2008), é um exemplo de filtro de pacote;

- *Proxy*: este tipo de *firewall* tem por finalidade filtrar os pacotes que são gerados na rede interna da empresa (LAN) e muitas vezes ele impede a conexão com servidores externos que podem ser prejudiciais ao sistema de informação. Como prejudiciais podemos citar as redes de compartilhamento de arquivos que contém diversas ameaças conhecidas como *Trojans*, *Worms* e Vírus, estas ameaças muitas vezes utilizam nomes e extensões de arquivos como MP3, JPEG entre outros “disfarces”. Um exemplo bem conhecido é o *Squid* (SQUID, 2008) que é um pacote que vem na maioria das distribuições Linux;

- *Firewall* pessoal: *software* que intercepta as conexões de entrada e saída em um computador. Baseia-se em regras padrão ou definidas pelo usuário e decide quais conexões podem ser aceitas e quais devem ser recusadas. Podemos citar o *Sygate* (SYGATE, 2007) e o Zone Alarm (ZONE ALARM, 2008) como *softwares* de *firewall* pessoal;

- *Firewall* reativo: possui funções que permitem reconhecer ataques e emitir alarmes quando encontrar seqüências de pacotes IP chamadas de assinaturas e bloqueia o acesso indevido automaticamente.

2.7.1 Sistema de Detecção de Intrusos (IDS)

Os sistemas de detecção de intrusos ou *Intrusion Detection Systems* (IDS) são *softwares* que têm como finalidade funcionar em conjunto com um sistema de *firewall* a fim de dar maior segurança na comunicação envolvendo tráfego IP (ROESCH, 2006, p.1-131). Alguns exemplos de IDS são o *Snort* (SNORT, 2007) e o *Airsnort* (AIRSNORT, 2007), este último para redes sem fio.

O IDS permite a verificação do conteúdo de um pacote IP por intermédio de um sistema de assinaturas. Após essa verificação, ele pode emitir um alerta caso as assinaturas do IDS não sejam compatíveis com o conteúdo do pacote que chega*,* permitindo assim aprimorar as configurações do *firewall*. Assim como os sistemas de *firewall,* o IDS possui vários tipos diferentes de configuração. Entre os mais conhecidos estão:

- *Host-Based Intrusion Detection* (HIDS): faz o monitoramento de um sistema com base nos eventos registrados nos arquivos de log. Os eventos mais freqüentemente monitorados são a utilização do processador do computador, a modificação de privilégios em arquivos e usuários além de processos do sistema operacional e softwares que estão em execução;

- *Network-Based Intrusion Detection* (NIDS): monitora o tráfego por intermédio da captura dos pacotes IP e da análise dos seus cabeçalhos e conteúdos.

Uma ilustração da utilização de um IDS pode ser visualizada na Figura 1, que apresenta a infra-estrutura de uma rede com IDS. Nesta figura podemos observar a existência de um computador com IDS conectado a um HUB em rede com um *firewall.* Nesta configuração, o IDS captura todos os pacotes IPs que vem da *internet*, possibilitando verificar todas as ameaças que eventualmente passem pelo *firewall*.

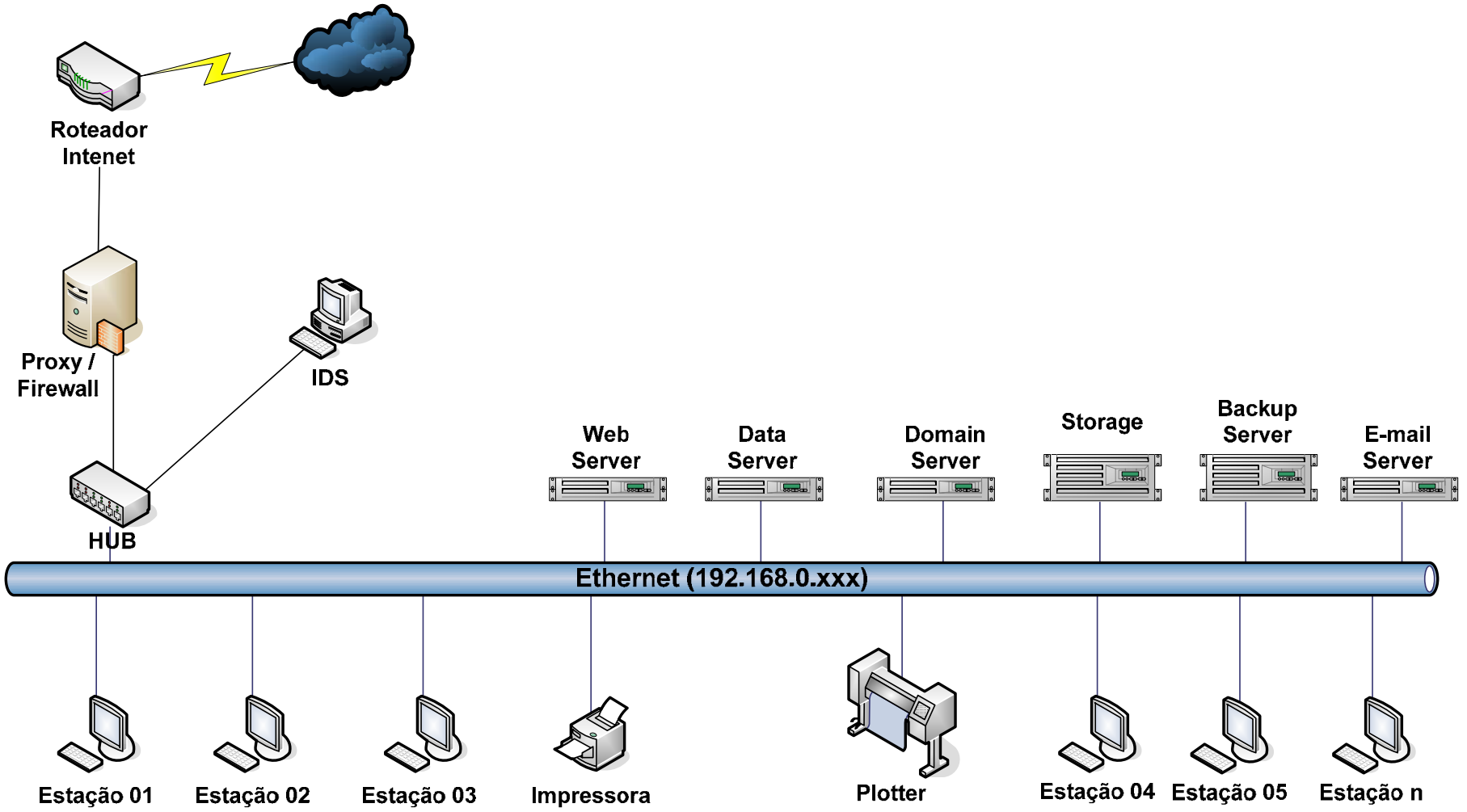


Figura 1: Exemplo da aplicação de um IDS.

Fonte: adaptado de SOUZA, 2007.

As possibilidades de aplicação de um IDS são as mais variadas, podendo ser exploradas outras configurações, em função das necessidades de cada empresa.

2.8 Criptografia

É uma técnica utilizada para cifrar uma informação, tornando-a incompreensível, exceto para o(s) destinatário(s) e o transmissor, que sabem como decifrá-la (KUROSE, 2003, p.605-668).

A criptografia se faz necessária, por exemplo, em operações bancárias e de compras *on-line*, sendo algo bastante comum no dia a dia (PFLEEGER, 1997, p.25-50).

Existem dois tipos fundamentalmente diferentes de criptografia (FITZGERALD, 2005, p. 261-270): a simétrica e a assimétrica. Um algoritmo simétrico é aquele que utiliza a mesma chave para criptografar e descriptografar uma mensagem conforme é ilustrado na Figura 3.

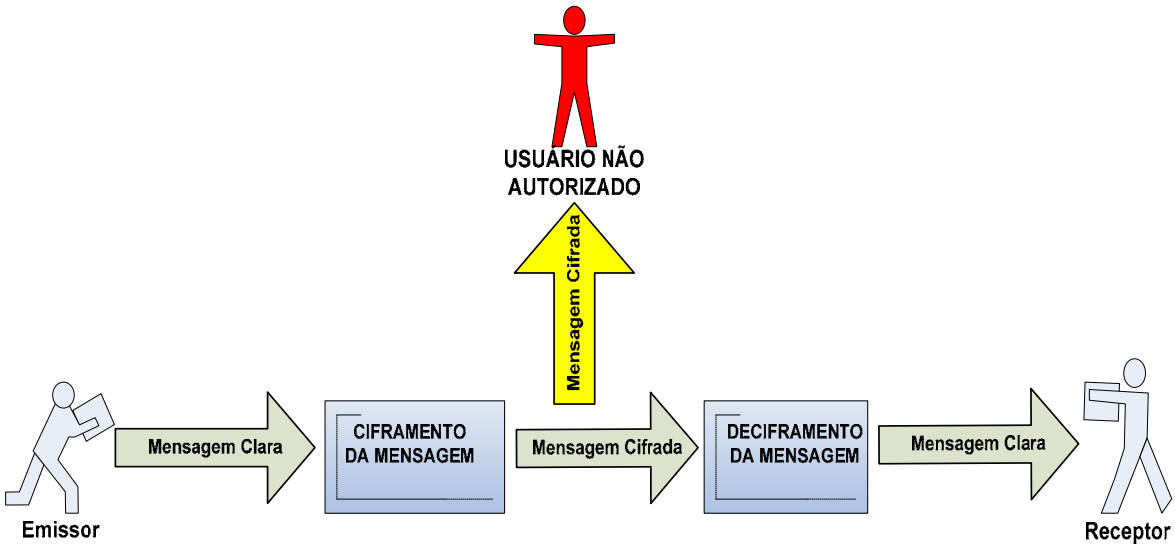


Figura 2: Criptografia Simétrica.

Fonte: adaptado de STALLINGS, 1999.

Na Figura 2 pode-se observar que a mensagem parte do emissor passando por um processo de ciframento, após este processo a mensagem cifrada é encaminhada ao receptor que possui a chave para decifrar a mensagem, desta forma torna-se difícil para quem não têm a chave correta decifrar a mensagem original.

Um algoritmo bem difundido de criptografia simétrica é o DES (Data Encryption Standard) de 56 bits desenvolvido pela IBM (International Business Machines) e mantido pelo NIST (National Institute os Standards and Technology). Outro algoritmo popular é o RC4 (STALLINGS, 1999, p.30-61) que possui uma chave de 256 bits desenvolvido pela RSA Data Security empresa fundada por Rivest, Shamir e Adleman (TANENBAUM, 2003, p.682).

A criptografia assimétrica é também chamada de criptografia de chave pública e possui um conjunto de duas chaves, uma que serve para criptografar a mensagem e outra para descriptografá-la (KUROSE, 2003, p.605-668). Neste caso, o responsável por criptografar não transmite a chave para a descriptografia e, desta forma, se a mensagem for capturada na transmissão, a mesma não poderá ser entendida (Figura 3).

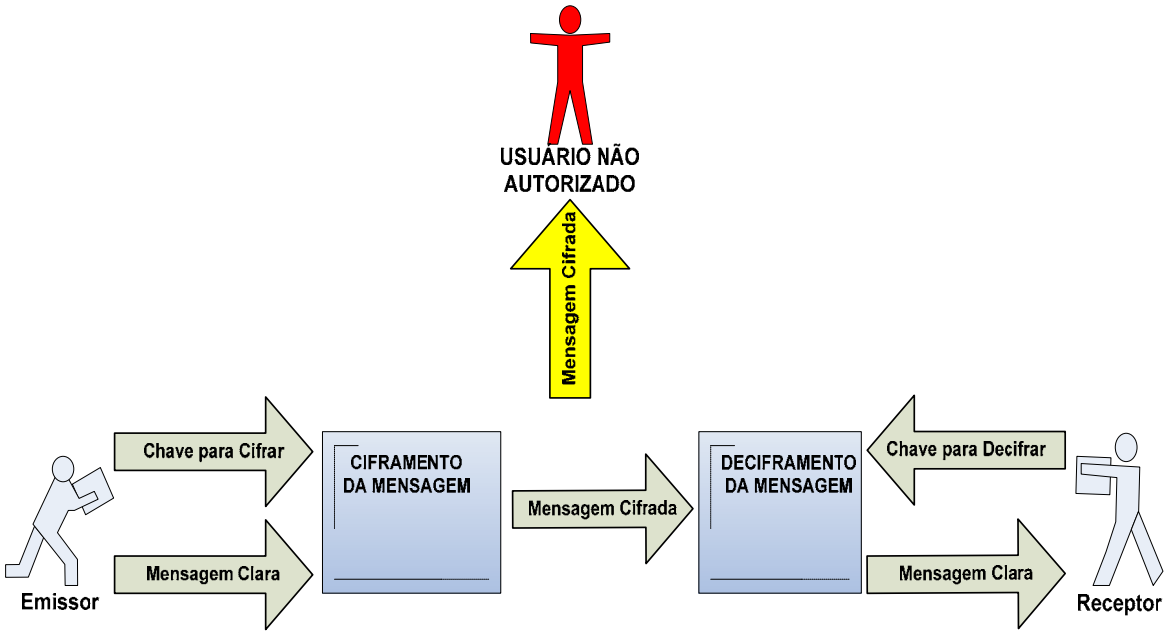


Figura 3: Criptografia Assimétrica.

Fonte: adaptado de STALLINGS, 1999.

Um algoritmo assimétrico bem conhecido é o RSA (sigla formada pelas iniciais de seus criadores Rivest, Shamir, Adleman) e que é mantido pelo MIT (*Massachusetts Institute os Technology*). O RSA forma a base para o atual PKI (*Public Key Infrastructure*) que possibilita a utilização de chaves de até 1024 bits (FITZGERALD, 2005, p. 263).

2.9 HASH

É uma função matemática aplicada em algorítimos que utilizam mensagens de texto para criação de um código chamado *message digest* (*resumo de mensagem*) (STALLINGS, 1999).

Aplicar em um arquivo a função hash significa a execução de um algorítimo de cálculo sobre o arquivo para geração de um número como resultado, toda alteração pode produzir mudança do resultado calculado, possibilitando saber se o arquivo foi alterado. O método pode ser aplicado saber se um arquivo foi contaminado por vírus ou corrompido (FITZGERALD, 2005).

As funções *hash* mais conhecidas são:

MD4 que possibilita valor *hash* de 128-bits (RFC-1320);

MD5 um aprimoramento do MD4, é usado pelo PGP (*Pretty Good Privacy*) (PGP, 2008) (RFC-1321);

SHA-1 (*Secure Hash Algorithm*) possibilita valor *hash* de 160-bits (STALLINGS, 1999).

As funções hash são utilizadas nos mecanismos de assinatura digital que são apresentados na seção 2.10.

2.10 Assinatura Digital

Por assinatura digital entendemos um código utilizado para verificar a integridade de uma informação ou mensagem. Além disso, ela poder ser utilizada

para verificar se o remetente de uma mensagem é mesmo quem diz ser, o que é feito através de criptosistemas assimétricos (FITZGERALD, 2005, p. 2-250). Os algoritmos mais usados em esquemas de assinaturas digitais são o RSA e o DSS (*Digital Signature Standard*) (TANENBAUM, 2003, p-699).

2.11 Autenticação

A autenticação (da origem e do conteúdo) de mensagens é um conjunto de técnicas fundamentais com propriedades criptográficas (TANENBAUM, 2003, p.608-700) para proteção contra: **i)** modificação acidental ou não de uma mensagem; **ii)** atraso ou re-envio de mensagens; **iii)** repúdio da autoria de uma mensagem.

Pode-se dividir a autenticação em três grandes grupos (NAKAMURA, 2002, p. 221-227):

- Autenticação baseada no que o usuário sabe: método baseado em algum conhecimento do usuário, como as senhas. Deve-se considerar as chaves criptográficas nesta categoria. No entanto, todas as técnicas relacionadas ao que o usuário sabe, são passíveis de ataques originados por monitoramento de *softwares* espiões como o CAIN (CAIN, 2007), que vasculham o conteúdo das informações recebidas e transmitidas pelo usuário. Senhas podem ser descobertas caso o usuário não tome os devidos cuidados;

- Autenticação com base no que o usuário possui: neste grupo podemos incluir itens como crachás e cartões magnéticos. Trata-se de um método muito utilizado, mas que também depende do fator humano quanto a sua utilização. Por exemplo, a perda ou o empréstimo de um cartão magnético;

- Autenticação com base nas características do usuário: pode-se incluir neste grupo as digitais do usuário, controle por íris, retina, voz, padrões de escrita entre outros. Para este grupo existe uma

> variedade de dispositivos para implantar segurança nas organizações e algumas já são bastante comuns como a identificação por digitais ou a identificação por voz.

É possível dizer que existem muitas opções de autenticação e que cada empresa deve escolher a que seja mais adequada financeiramente e estrategicamente, sendo um mercado em constante transformação.

2.12 Redes Virtuais Privadas (VPN)

Em uma rede virtual privada ou VPN (*Virtual Private Network*) os dados são codificados por intermédio da utilização de criptografia, possibilitando a utilização de uma rede virtual privada trafegando dados dentro da rede pública. A criptografia permite a criação de túneis para a transmissão e recepção dos dados de modo seguro. Na Figura 4 ilustra-se uma aplicação de VPN.

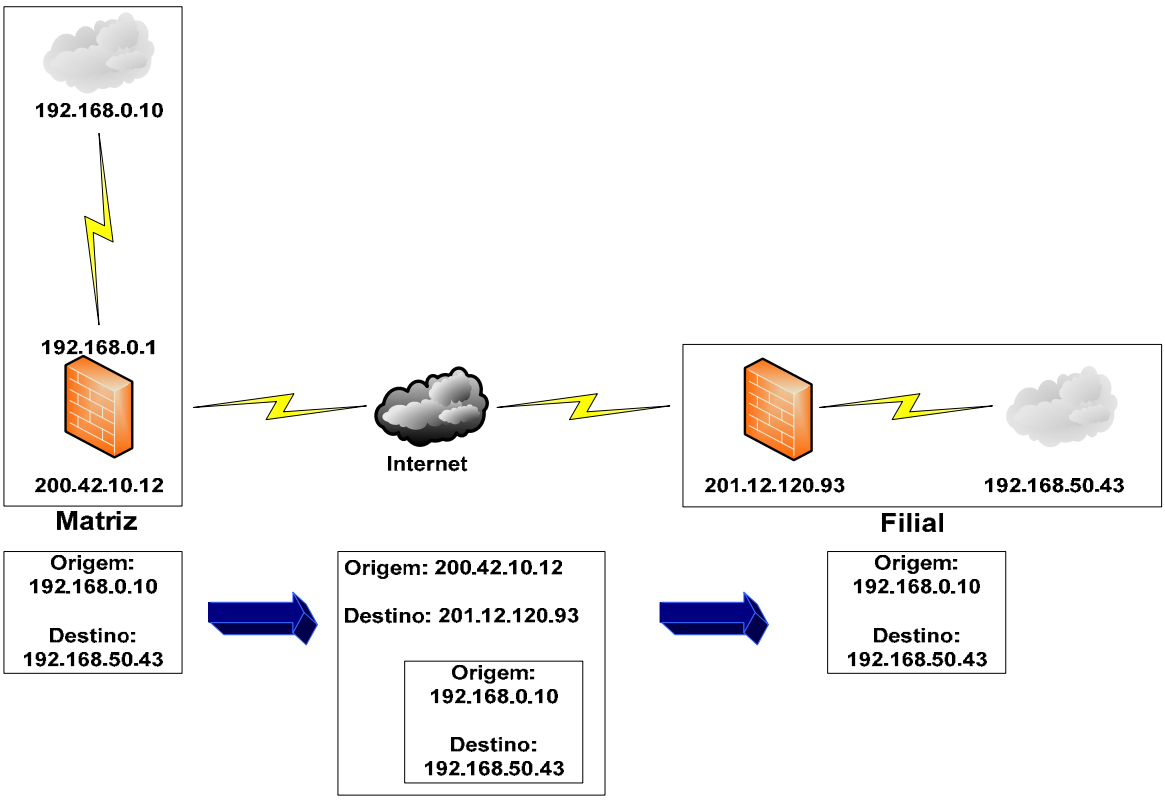


Figura 4: Exemplo de VPN.

Fonte: Adaptação de CHESWICK, 2003, p. 233.

Na ilustração da Figura 4, pode-se observar que existe a formação de um túnel quando o computador com IP origem 192.168.0.10 realiza a conexão com o IP destino 192.168.50.43 através de um tunelamento pelo *Firewall* da matriz com o *Firewall* da filial. O IP do computador com IP 19.168.0.10 fica “mascarado” pelo IP do *Firewall* de origem e do *Firewall* de destino apesar de passar pela Internet.

3 Normas ISO para Segurança da Informação

No Capítulo 2 apresentamos os conceitos envolvendo segurança da informação e, neste capítulo, discutimos as normas ISO 27001 (ABNT ISO 27001, 2006) e ISO 17799 (ABNT ISO 17799, 2005) que serviram como base do método descrito no capítulo 4 desta dissertação.

A ISO "*International Organization for Standardization"* é uma organização com sede na Suíça (ABNT ISO 27001, 2006). A Sigla ISO foi originada da palavra Isonomia, e tem como função desenvolver e promover normas que possam ser utilizadas igualmente em todos os países. O Brasil é representado pela Associação Brasileira de Normas Técnicas - ABNT.

3.1 Normas ISO 27001 e ISO 17799

A norma ISO 27001 (ABNT ISO 27001, 2006) provê e apresenta requisitos para que a organização possa estruturar um sistema de gestão de segurança da informação (SGSI). Por sua vez, a norma ISO 17799 (ABNT ISO 17799, 2005) é um conjunto de boas práticas que podem ser aplicadas por um SGSI.

O conjunto das duas normas pode ser descrito como: i) um método estruturado reconhecido internacionalmente para segurança da informação; ii) um processo definido para avaliar, implantar, manter e gerenciar a segurança da informação; iii) um grupo completo de controles contendo as melhores práticas para a segurança da informação; iv) uma base para as melhores práticas a serem adotadas por empresas (ABNT ISO 27001, 2006).

As duas normas não são: **i)** normas técnicas; **ii)** dirigidas para produtos ou tecnologias; **iii)** métodos para avaliação de equipamentos. Portanto, devemos entendê-las como normas para a gestão da informação.

3.2 ISO 27001 – Sistema de Gestão de Segurança da Informação (SGSI)

A ISO 27001 (ABNT ISO 27001, 2006) incorpora um processo de escalonamento de risco e valorização de ativos, orientando quanto à análise e

identificação de riscos e a implantação de controles para minimizá-los. O grau em que o sistema é organizado e contêm processos estruturados irá facilitar a replicação do sistema de um local para outro. Uma empresa pode implantar a ISO 27001 em sua sede e depois replicá-la em suas filiais.

O SGSI pode ser simplesmente definido como um comitê multidisciplinar que tem com principal responsabilidade estabelecer políticas de segurança, multiplicar o conhecimento envolvido e também determinar os responsáveis e as medidas cabíveis dentro de seus limites de atuação (ABNT ISO 27001, 2006).

Com a alta direção compromissada e o treinamento eficaz dos colaboradores, é possível se reduzir o número de ameaças que exploram eventuais vulnerabilidades. No Quadro 1 apresentam-se os requisitos existentes na norma ISO 27001.

Quadro 1: Requisitos da Norma ISO 27001.

Nº	**Requisito**	**Descrição**
1	Escopo	Abrangência da Norma
2	Referência Normativa	Normas e padrões relacionados à norma 27001
3	Termos e Definições	Termos e definições relacionados à segurança da informação
4	Sistema de Gestão de Segurança da Informação	Referente à criação, implementação, monitoramento e melhoria do SGSI, também trata de documentação e registros de informações
5	Responsabilidade da Direção	Definição de responsabilidades, treinamento e provisão de recursos do SGSI
6	Auditorias Internas	Auditorias internas realizadas por pessoal treinado e comprometido com o SGSI
7	Analise crítica do SGSI	Análise realizada pelo corpo diretivo da organização das ações efetuadas pelo SGSI
8	Melhoria do SGSI	Trata das ações corretivas e preventivas efetuadas pelo SGSI

Fonte: Adaptado de (ABNT ISO 27001, 2006).

No capítulo 4 apresentamos uma sugestão para implantação do SGSI em uma ambiente empresarial contento todos os requisitos apresentados no Quadro 1 e nas seções seguintes deste capítulo 3 apresentamos a ISO 17799 e seus principais requisitos.

3.3 ISO 17799 - Código de Prática para SGSI

Foi baseada na norma britânica BS 17799-1:1999 (ABNT ISO 17799, 2005) sendo aplicada como um documento de referência, que é chamada de guia de melhores práticas (de orientações para as organizações).

Consistindo de uma grande lista de controles para garantir a segurança da informação. A ISO 17799 é composta pelos requisitos principais apresentados no Quadro 2 (ABNT ISO 17799, 2005).

Quadro 2: Requisitos da Norma ISO 17799.

Requisito	Descrição
Política de segurança	São as normas desenvolvidas que consideram as responsabilidades, punições e autoridades
Segurança organizacional	Estrutura da gerência de segurança
Classificação e controle de ativos de informação	Classificação, registro e controle dos ativos
Segurança relacionada às pessoas	Foco do risco decorrente de atos decorrentes de ações das pessoas
Segurança ambiental e física	Levantamento da necessidade de definição das áreas de circulação restrita e de se proteger equipamentos e infra-estrutura de TI
Gerenciamento das operações e comunicações	Aborda temas relacionados a: procedimentos operacionais, homologação e implantação de sistemas, entre outras
Controle de acesso	Controle do acesso aos sistemas, definição de competências e responsabilidades
Desenvolvimento e manutenção de sistemas	Requisitos para sistemas, criptografia, arquivos e desenvolvimento e suporte de sistemas
Gestão de incidentes de segurança	Notificação de vulnerabilidades, ocorrências de segurança e gestão de incidentes
Gestão da continuidade do negócio	Reforço na necessidade de ter um plano de continuidade e contingência

Conformidade	Referente à necessidade de observar os requisitos legais, como a propriedade intelectual

Fonte: Adaptado de (ABNT ISO 17799, 2005).

Após apresentar a definição e requisitos das normas ISO 27001 e ISO 17799, passaremos a discutir no Capítulo 4 o método proposto nesta dissertação, para implantação de um projeto de segurança da informação.

4 Método para Implantação da Segurança da Informação

O método proposto nesta dissertação tem como objetivo de orientar o processo de implantação de um projeto de segurança da informação em um ambiente organizacional. Tal método é baseado nas normas ISO 27001 e ISO 17799.

Não pretendemos aqui, defender nenhuma plataforma de *hardware* ou de *software.* Muito se fala em custo, no entanto custo não está relacionado apenas com a compra de licenças de *software*, mas também com a garantia de suporte e a qualidade dos produtos. No estudo de caso que apresentamos no capítulo 5, escolhemos uma solução mista (i.e., *software* livre e comercial) com ferramentas conhecidas no mercado.

Na literaura estudada, podemos verificar que as normas ISO não citam quais ferramentas devemos utilizar ou quais linhas de trabalho deveram adotar. O autor Marcos Sêmola (SÊMOLA, 2003) sugere uma série de medidas, no entanto não diz qual caminho devemos tomar, apenas faz sugestões que podemos encontrar nas próprias normas ISO, portando resolvemos desenvolver o método apresentado nesta dissertação, com o intuito de proporcionar um método lógico para implantar segurança da informação.

Uma pergunta que sempre aparece em relação à implantação de projetos é quanto ele vai custar? Para responder a esta questão, não podemos pensar só no que vai ser gasto, mas também no retorno que isso vai trazer. Quanto custa uma empresa parada por 3 horas devido à falha de um servidor cujo valor de mercado seja algo em torno de R$ 12.000,00?

Se uma empresa funciona no horário comercial (das 08:00 às 18:00) e fatura por dia R$ 90.000,00, ela vai deixar de faturar R$ 30.000,00 na média do dia, sem contar os transtornos causados aos clientes, fornecedores e demais colaboradores. Na Figura 5 apresentamos o fluxograma do método sugerido nesta dissertação.

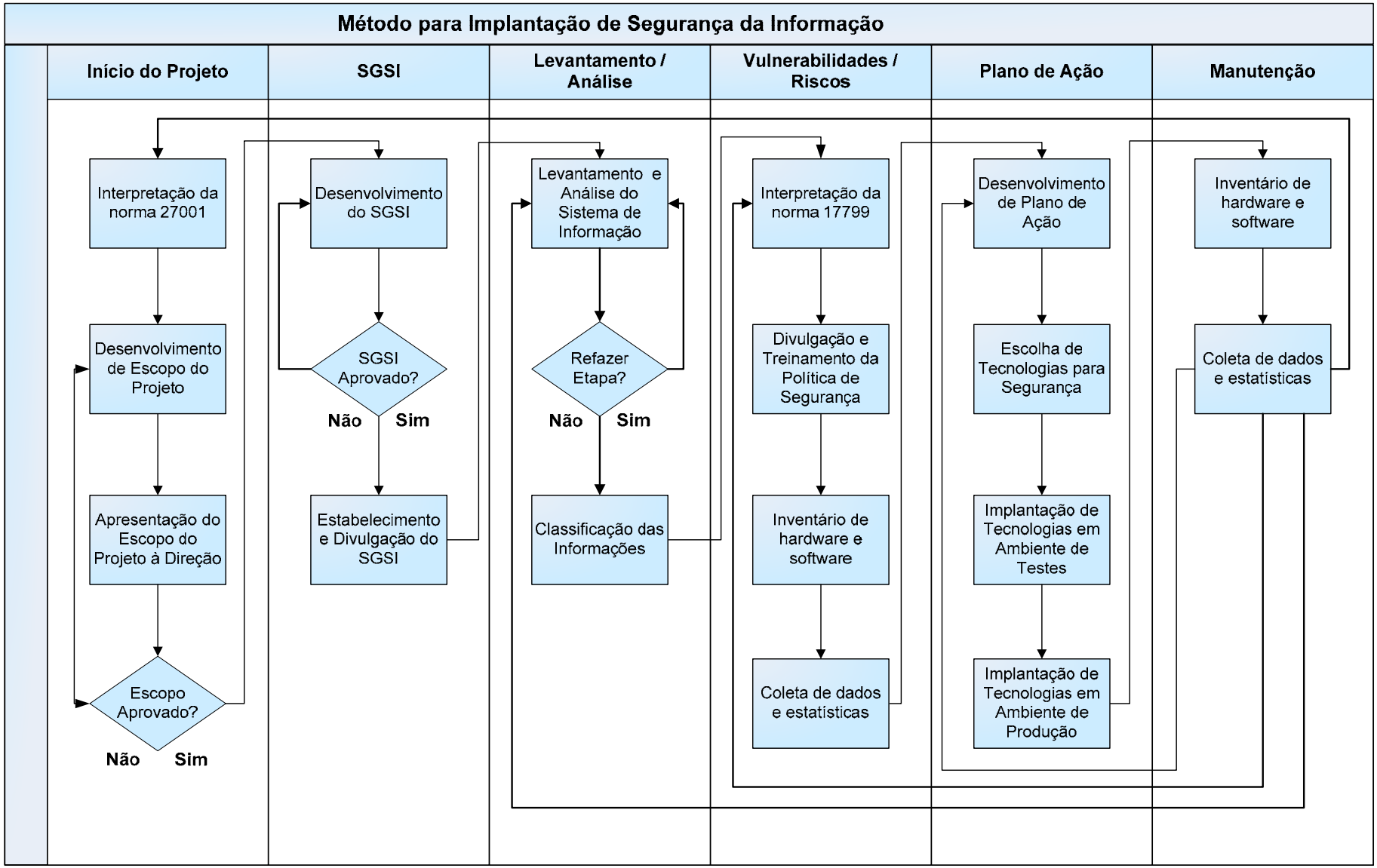


Figura 5: Fluxo do Método para Implantação do Projeto de Segurança da Informação.

A Figura 5 é uma contribuição deste trabalho para empresas interessadas em implantar um projeto de segurança, pois apresenta um fluxo de trabalho que não é apresentado na norma ou em trabalhos correlatos.

Nas seções a seguir são apresentados os passos do método apresentado na Figura 5 de forma detalhada.

4.1 Início do Projeto de Segurança

O início de um projeto de segurança da informação normalmente está associado ao departamento de TI. No entanto o compromisso com a segurança deve ser assumido por todos na empresa.

4.1.1 Interpretação da norma ISO 27001

Esta etapa compreende o entendimento dos requisitos da norma que foram apresentados nesta dissertação na seção 3.2

Os Requisitos de nº. 1, 2 e 3, referem-se, respectivamente ao Escopo, Referência Normativa e aos Termos e Definições, sendo todos informativos.

O Requisito 4 trata da criação, implementação, monitoramento e melhoria do SGSI, é através deste requisito que definimos os membros participantes do SGSI, os documentos necessários e quais registros devemos manter.

No Requisito 5 é apresentado a responsabilidade da direção que refere-se à atribuição das responsabilidades do SGSI, tais como provisionar treinamentos e recursos necessários ao SGSI.

O Requisito 6 trata das auditorias internas e define quais áreas devem ser auditadas, a periodicidade das mesmas e quem poderão ser os auditores responsáveis. Com relação a este último ponto, notamos que o auditor não deve avaliar processos pelos quais é responsável.

No Requisito 7 de análise crítica do SGSI é apresentada a necessidade da direção verificar as ações efetuadas pelo SGSI, agindo como um elemento de controle do mesmo.

E finalmente o requisito de Número 8 trata da melhoria do SGSI. O SGSI é um comitê que possui uma dinâmica que, através das auditorias internas e análise crítica da direção, pode melhorar suas ações e deste modo cuidar da segurança da informação.

4.1.2 Desenvolvimento de Escopo do Projeto

O escopo do projeto deve ser desenvolvido apresentando uma visão geral sobre segurança da informação alinhada aos negócios da empresa. Devemos aqui enfatizar a necessidade da segurança e suas implicações nos processos envolvendo clientes, fornecedores e colaboradores.

4.1.3 Apresentação do Escopo do Projeto

Nesta etapa o escopo do projeto é apresentado à direção da empresa, devendo ser salientados os problemas que podem ocorrer caso não seja implantado um projeto de segurança e as questões financeiras envolvidas.

Alguns números se fazem necessários para aceitação do projeto, como, por exemplo, quanto à empresa pode deixar de faturar se um servidor de banco de dados ficar inativo, conforme já comentamos anteriormente. É importante avaliar o impacto da segurança da informação no que se refere à imagem da empresa.

Se o escopo não for aprovado, deve-se então reiniciar o desenvolvimento de um novo escopo e então reapresentá-lo à direção.

Nesta seção enfatizamos a questão financeira, tema que não é apresentado de forma enfática na normas ISO 27001 e ISO 17799.

4.2 SGSI (Sistema Gestor de Segurança da Informação)

Aqui definimos o SGSI e o apresentamos à direção e a todos os envolvidos com os negócios da empresa, neste grupo podemos incluir clientes, fornecedores

e colaboradores. São apenas duas etapas, mas com grande relevância para todo o projeto de segurança.

4.2.1 Desenvolvimento do SGSI

Após o escopo aprovado, partimos para o desenvolvimento do SGSI e nesta fase definimos os seguintes itens: i) participantes do comitê do SGSI; ii) objetivos do SGSI; iii) responsabilidades do SGSI; iv) limites de atuação do SGSI; v) observância dos fatores legais e contratuais envolvidos nos negócios da empresa; vI) critérios para avaliação de riscos nos negócios.

Como base para o SGSI, podemos utilizar o modelo de ciclo PDCA (Plan-Do-Check-Act) (ABNT ISO 27001, 2006) que possibilita o acompanhamento de todas as fases do SGSI e assim possibilitando rever algumas medidas adotas e quais os impactos na cadeia de valor (BRASILIANO, 2002). O ciclo PDCA é ilustrado na Figura 6.

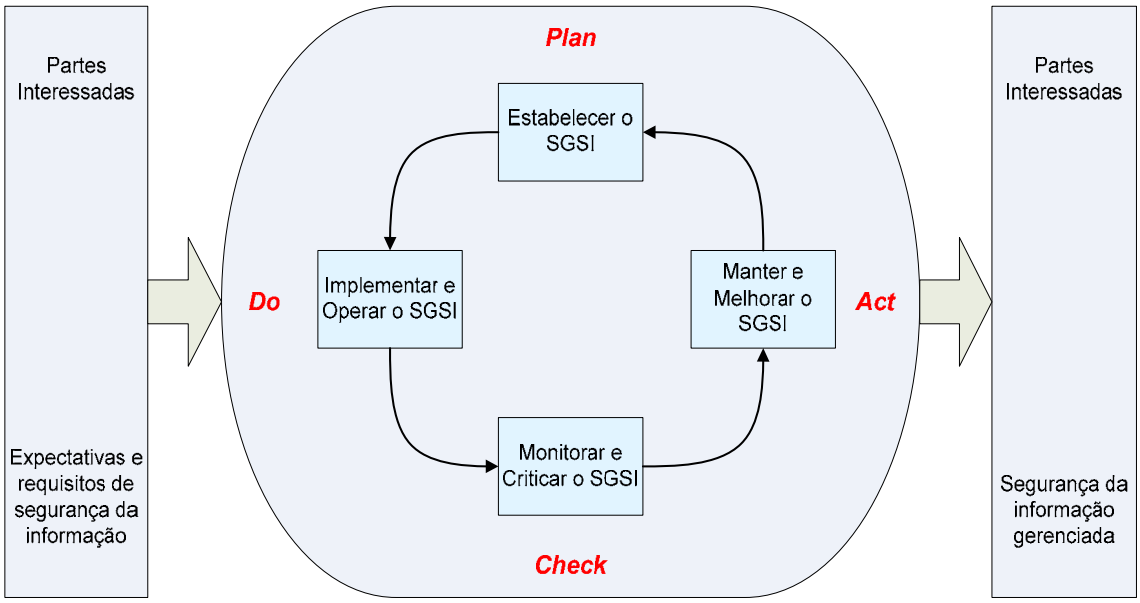


Figura 6: Ciclo PDCA

Fonte: adaptado de ISO 27001, 2006

Como o modelo PDCA, temos uma visão de como planejar, executar, verificar e montar o plano de ação de modo contínuo, buscando o aperfeiçoamento constante. Estabelecimento e Divulgação do SGSI.

Depois da definição dos itens apresentados em 4.1.4 e com o aval da direção, partimos para o estabelecimento do SGSI e sua divulgação para clientes, fornecedores e colaboradores. A divulgação deve abranger todos os itens apresentados em 4.1.4, expondo de modo claro os objetivos do SGSI.

A sequência apresentada nesta seção para implantação do SGSI não é encontrada na norma ISO 27001.

4.3 Levantamento e Análise

Após o estabelecimento do SGSI devemos proceder aos levantamentos e análises necessários para o desenvolvimento da política de segurança da informação.

4.3.1 Levantamento e Análise do Sistema de Informação (SGSI)

Nesta etapa do projeto mapeamos os processos da empresa e a partir disso analisamos como a informação trafega pela empresa e mesmo sai dela, mediante os relacionamentos existentes com clientes e fornecedores. O resultado dessa análise pode ser convenientemente colocado sob a forma de um diagrama de blocos. No capítulo 5, apresentamos um exemplo baseado em um estudo de caso para uma empresa real.

Observamos que está etapa só estará concluída caso o Levantamento e a Análise esteja de acordo com os anseios da empresa.

4.3.2 Classificação das Informações

Aqui classificamos as informações de acordo com as características que envolvem o negócio da empresa, por exemplo, as informações financeiras que são transmitidas aos bancos que são confidenciais e só devem ser visualizadas pelas pessoas autorizadas pela direção da empresa.

Classificar as informações é um passo necessário para podermos aplicar ferramentas de segurança como criptografia, VPN entre outras mencionadas no Capítulo 2.

Um modo de classificar uma informação é avaliando o impacto que a mesma poder ter sobre as operações da empresa.

Como sugestão para análise do impacto é importante considerar os itens na lista a seguir:

- Multas contratuais com clientes e fornecedores;
- Multas decorrentes de operações ilegais que possam existir pos desconhecimento da legislação ou das implicações existentes;
- Cliente pode se recusar a receber determinado produto devido a atrasos decorrentes de problemas de segurança da informação;
- Arquivos corrompidos que podem afetar a produção de um determinado item.

4.4 Vulnerabilidades e Riscos

Nesta etapa do projeto ocorre a interpretação da norma ISO 17799, que trata do desenvolvimento e treinamento relacionados à política de segurança, bem como da coleta de dados e estatísticas necessários ao fornecimento de informações para a construção do plano de ação apresentado na Seção 4.5.

4.4.1 Interpretação da norma ISO 17799

A interpretação dos requisitos da norma ISO 17799 se faz necessária pois dá uma visão abrangente dos controles de segurança que podemos ter em uma empresa.

Como apresentado no Capítulo 3, os requisitos da norma ISO 17799 são: **i)** política de segurança; **ii)** segurança organizacional; **iii)** classificação e controle de ativos de informação; **iv)** segurança relacionada às pessoas; **v)** segurança ambiental e física; **vi)** gerenciamento das operações e comunicações; **vii)** controle de acesso; **viii)** desenvolvimento e manutenção de sistemas; **ix)** gestão de incidentes de segurança; **x)** gestão da continuidade do negócio e **xi)** conformidade com as diretrizes da empresa.

Como podemos observar, o primeiro requisito da norma é a política de segurança de informação, enquanto os demais itens podem ser colocados em um grande grupo de controles e tecnologias para a segurança da informação.

4.4.2 Desenvolvimento e Treinamento da Política de Segurança da Informação

Nesta fase desenvolvemos as políticas necessárias à segurança da informação, as quais devem abranger os anseios da empresa, os itens que devem constar obrigatoriamente da política são: direitos, responsabilidades e punições cabíveis.

A política deve ser desenvolvida constantemente, num processo de melhoria contínua, não sendo algo estático, pois a tecnologia e os processos mudam constantemente.

Após o desenvolvimento da política procedemos ao treinamento de todos na empresa e a divulgação da mesma junto aos clientes e fornecedores.

4.4.3 Inventário de Hardware e Software

Devemos inventariar todo *hardware* e *software* presentes na empresa, pois somente assim poderemos ter um panorama das licenças existentes e das características e condições dos equipamentos. Apesar de ser uma tarefa razoavelmente simples de ser realizada, não raro que empresas não dêem o devido valor a este quesito.

4.4.4 Coleta de Dados e Estatísticas

Apenas a política desenvolvida e divulgada não garante um sistema seguro, é necessário dispor de ferramentas que permitam coletar dados e gerar estatísticas de segurança para tomar a medidas necessárias em um plano de ação. Para coletar os dados utilizamos ferramentas como IDS (*Intrusion Detection System*), *Port Scan* e *Sniffer*. Com os dados coletados podemos gerar estatísticas e assim aprimorar os controles de segurança.

4.5 Plano de Ação

O plano de ação consiste em analisar as ocorrências de ameaças baseando-se nos mecanismos instalados e também em ações concretas que visem reduzir os riscos existentes em um processo de melhoria contínua (CARVALHO, 2005, p.1-100).

Aqui montamos o plano de ação que pode resultar em ações corretivas, preventivas, ou mesmo de contenção. Tais ações podem acarretar a adoção de novas ferramentas e técnicas para gestão da segurança da informação.

4.5.1 Escolha de Tecnologias para Segurança

Como escolher uma tecnologia? Esta é uma questão importante e em muitos casos escolhemos as ferramentas de tecnologia de modo incorreto, muitas são adotadas sem critérios bem estabelecidos. Nossa sugestão nesta etapa é adotar um método bem conhecido chamado *benchmarking* que foi aplicado no Capítulo 5 desta dissertação. O método consiste em estabelecer critérios para avaliar as opções existentes de acordo com as necessidades de cada empresa.

Como critérios para adoção de *softwares* de segurança da informação, adotamos os parâmetros relacionados na lista a seguir:

Antivírus

- Preço
- Atualizações
- Ameaças Detectadas
- Sistemas Operacionais Suportados
- Uso Corporativo
- Proteção de *E-mail*
- Proteção de mensagens instantâneas
- Agendamento de verificação

Backup

- Preço
- Sistemas Operacionais Suportados

- Compactação de Arquivos
- Uso Corporativo
- Agendamento de *Backup*
- Envio Informações *E-mail*
- Backup Password Protection
- Verificação de *Backup*

IDS

- Preço
- Número de Equipamentos
- Sistemas Operacionais Suportados
- Uso Corporativo
- Portas Detectadas
- Envio Informações *E-mail*

Algumas considerações sobre as listas com critérios:

Parâmetros como: i) Preço, ii) Uso Corporativo; iii) Sistemas Operacionais Suportados são básicos devido a todos os softwares, para tanto cabe justificar cada um dos critérios.

Preço: Este parâmetro é importante em qualquer compra, pois corresponde ao valor financeiro dispensado para compra.

Uso Corporativo: devido à quantidade de equipamentos existentes na empresa, softwares de uso corporativo também possuem a característica de serem aplicações que executam nos servidores de rede, instalando-se nas estações apenas as aplicações clientes.

Sistemas Operacionais Suportados: este parâmetro é importante para todos os *softwares* à serem implantados devido a diversificação possível em uma rede, onde é possível utilizar diferentes arquiteturas formando uma rede heterogêna.

Dos critérios específicos apresentamos a seguir uma lista com as justificativas:

Antivírus

- Atualizações: quanto mais rápido o conhecimento de novas ameaças e a disponibilização de novas atualizações, mais confiável é o *software*;
- Ameaças Detectadas: a quantidade de ameaças identificadas também permite avaliar a eficiência do *software*;
- Proteção de *E-mail*: proteção do *e-mail* se faz necessário ante a quantidade de emails recebidos e que transportam arquivos muitas vezes com conteúdo danoso;
- Proteção para mensagens instantâneas: necessário assim com a proteção para *e-mails* devido à possibilidade de envio de mensagens com conteúdo danoso;
- Agendamento de verificação: item que possibilita verificação de ameaças sem interferência do usuário;

Backup

- Compactação de Arquivos: item necessário para racionalizar o tamanho dos arquivos de backups que podem ocupar tamanho excessivo;
- Agendamento de *Backup*: possibilitar melhor controle dos horários de *backup* e minimizando o trabalho manul;
- Envio Informações *E-mail*: para que o administrador responsável pelo *backup* tenha possibilidade de receber informes das operações em a necessidade de interagir com o *software*;
- Verificação de *Backup*: após realizar o backup é importante verificar se o(s) arquivo(s) gerado(s) estão consistentes.

IDS

- Portas Detectadas: deve dar suporte a todos os protocolos utilizados em uma rede IP;

- Envio Informações *E-mail*: para que o administrador responsável pelo *backup* tenha possibilidade de receber informes dos *logs* gerados pelo IDS.

Na lista de *softwares* apresentados pode-se incluir novos parâmetros, no entanto depende dos critérios que cada empresa adota ou quais funções são implementadas ao *software*.

4.5.2 Implantação de Tecnologias em Ambiente de Testes

Após escolher as tecnologias necessárias, procedemos à implantação em um ambiente de testes que possibilite diferentes configurações e análises. Algumas empresas não possuem um ambiente para testes e acabam por implantar as tecnologias no ambiente de produção, o que pode acarretar problemas sérios.

O ambiente de testes pode consistir em aplicar as soluções em um setor específico da empresa (departamento de TI, por exemplo), que faça uso dos serviços existentes como acesso a internet e aplicativos diversos.

4.5.3 Implantação de Tecnologias em Ambiente de Produção

Depois de realizar a implantação no ambiente de testes com o entendimento do funcionamento das tecnologias em questão, estamos prontos utilizá-las com mais segurança no ambiente de produção.

4.6 Manutenção

Esta etapa representa a melhoria contínua do projeto de segurança, pois aqui realimentamos todo o processo e procedemos um laço contínuo iniciando com uma nova coleta de dados e estatísticas e voltando para o plano de ação.

Outros laços são possíveis como:

Interpretação da norma ISO 27001: a norma passa por alterações constantes, as alterações podem trazer outras visões e novos requisitos;

Levantamento e análise do Sistema de Informação: o Sistema de Informação de uma empresa é dinâmico, sofre alterações constantes, com a criação de novos processos e descontinuação de outros;

Interpretação da norma ISO 17799: o mesmo que a norma 17799 pode passar por alterações.

O método também pode sofrer aprimoramentos, como a inclusão de novas técnicas e procedimentos. Consideramos esta etapa contínua que deve existir durante toda a vida do projeto de segurança da informação.

Na lista a seguir apresentamos aquilo que consideramos como principal contribuição para a implantação das normas ISO 27001 e ISO 17799:

- Método com fluxo de trabalho para implantação de um projeto de segurança da informação;
- Enfatizamos a questão financeira para o projeto;
- Sequencia para implantação de um SGSI;
- Sugestão para análise de impactos de ameaças;
- Apresentação de ferramentas de IDS, *Port Scan* e *Sniffer* para apoio ao desenvolvimento do projeto
- Critérios para escolha de ferramentas de segurança;
- Desenvolvimento do Plano de ação.

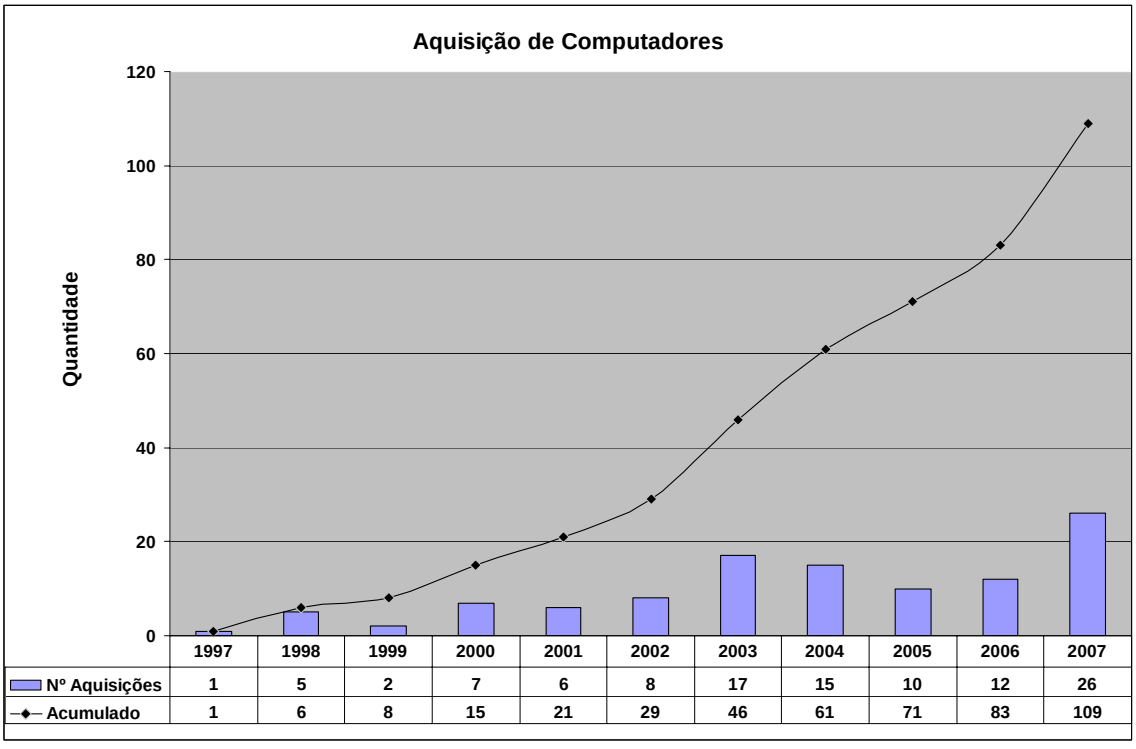
Neste capítulo apresentamos o método proposto para implantação de um projeto de segurança da informação, no Capítulo 5 apresentaremos um estudo de caso que exemplifica a implantação do método proposto.

5 Estudo de Caso

O presente trabalho foi realizado na empresa Tecnicópias Gráfica e Editora Ltda, no período de novembro de 2006 a dezembro de 2007, encontram-se localizada à Rua Flávio Telles, 15 – Jardim Santa Genebra, Campinas – SP, sendo constituída por 210 colaboradores, sendo 4 na área de tecnologia.

A empresa atua no ramo de impressão de manuais técnicos para empresas de tecnologia, telecomunicação e montadoras de veículos, praticando uma intensa e volumosa troca de dados entre seus colaboradores, clientes e fornecedores, sendo a informação o seu principal ativo.

Para melhor entender a utilização da tecnologia na empresa estudada, apresentamos no Gráfico 2 a aquisição de computadores ao longo dos últimos 10 anos pela empresa Tecnicópias.



	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007
Nº Aquisições	1	5	2	7	6	8	17	15	10	12	26
Acumulado	1	6	8	15	21	29	46	61	71	83	109

Gráfico 2: Aquisição de computadores nos últimos 10 anos.

Fonte: Tecnicópias Gráfica e Editora LTDA.

Como observado no Gráfico 2, ocorreu um crescimento considerável na quantidade de computadores na empresa, com isto aumentou a complexidade das redes, a quantidade de *softwares* utilizados que pode ser visualizado no Gráfico 3, o volume de dados armazenados, o número de vulnerabilidaes entre outras cararacterísticas.

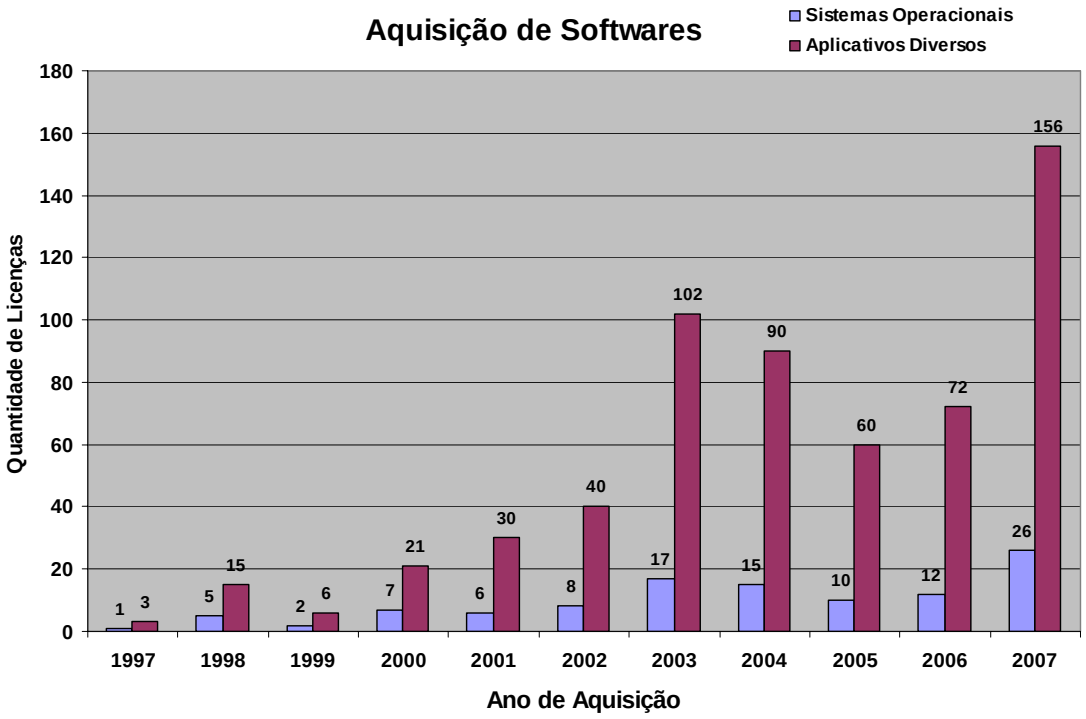


Gráfico 3: Aquisição de *Softwares* nos últimos 10 anos.
Fonte: Tecnicópias Gráfica e Editora LTDA.

Apresentamos neste capítulo a implantação do projeto de segurança em um ambiente de rede que conta com diversos serviços tais como servidor de *e-mail*, servidor de hospedagem de páginas, banco de dados, DHCP (*Dynamic Host Control Protocol*), DNS (*Domain Name Server*), *Terminal Server* (TS), *Active Directory* (AD) entre outros.

5.1 Início do Projeto de Segurança

O projeto de segurança foi motivado pelo ramo de negócio do qual a empresa faz parte e também pelos processos que envolvem toda cadeia de clientes e fornecedores, ficando o departamento de TI responsável por desenvolver e apresentar o escopo do projeto para direção da empresa.

5.1.1 Interpretação da norma ISO 27001

A fase de interpretação da norma ISO 27001 ocorreu no período de novembro de 2006 a dezembro de 2006.

Começamos pelo requisito 1 de escopo como visto no Capítulo 4, onde compreendemos que a norma ISO 27001 trata-se do desenvolvimento de um comitê gestor de segurança da informação denominado SGSI.

O requisito de Número 2 nos apresentou a norma ISO 17799 que contém as melhores práticas adotadas para segurança da informação, tratado no Capítulo 3 desta dissertação.

No Requisito 3 temos os termos e definições relacionados à segurança da informação, por exemplo, à definição de ameaças, vulnerabilidades entre outros, como apresentado no Capítulo 2 desta dissertação. Após a leitura do Requisito 3 passamos a leitura dos próximos requisitos o que nos possibilitou desenvolver e apresentar um projeto de segurança para a empresa estudada.

5.1.2 Desenvolvimento de Escopo do Projeto

Para o desenvolvimento do escopo foi utilizado o método de *benchmarking* (ALBERTIN, 2001), com visitas a empresas que possuem projeto de segurança. Esta tarefa ocorreu no período de janeiro de 2007 a fevereiro de 2007.

Em cada visita realizada pudemos constatar o quanto é diferente a percepção de segurança entre as empresas. Em algumas empresas o acesso à *internet* é totalmente liberado e não monitorado, em outros é totalmente liberado e monitorado e em alguns casos o acesso é liberado dependendo da autorização do funcionário e, mesmo assim, monitorado.

Chegamos a conclusão que o melhor método para a empresa Tecnicópias é de liberar o acesso dependente de autorização e monitoração, esta prática foi adotada pois permite aos responsáveis dos setores acompanhar quais recursos são necessários aos seus funcionários e também possibilita a geração de relatórios que podem servir como base de avaliação das ativiades diárias de cada colaborador.

Os relatórios de monitoração permitem a visualização de informações como tempo de acesso, quantidade de downloads por funcionário, entre outras informações.

No desenvolvimento do escopo consideramos os processos envolvendo as transações eletrônicas existentes com seus clientes e fornecedores, que necessitam de acesso com banda larga 24 horas por dia em 7 dias da semana.

Para apresentação do escopo, levantamos a informação do faturamento médio mensal da empresa estudada que se encontrava na época em R$ 5.000.000,00, o que possibilitou projetar um custo mensal com segurança em 1% do total que equivale a R$ 50.000,00.

É importante salientar que a direção da Tecnicópias concordou com o custo de 1% ao mês, no entanto o percentual gasto com segurança deve ser definido dentro das possibilidades de orçamento de cada empresa.

5.1.3 Apresentação do Escopo do Projeto

Após o desenvolvimento do escopo, apresentamos o mesmo para os membros da direção, gerência e supervisão.

O escopo do projeto foi assim constituído:

- Custos e prazos;
- Exemplo: Custo para aquisição da norma ISO 27001 - R$ 79,90;
- Exemplo: Prazo para aquisição da norma ISO 27001 – 7 dias úteis.
- Criação de um comitê denominado SGSI;
- Ver descrição Figura 7.
- Descrição de atribuições e responsabilidades a clientes, colaboradores, fornecedores incluindo termos de responsabilidade e acordos de confidencialidade (atividade contínua em função da dinâmica evolutiva do setor de Tecnologia da Informação realizada em conjunto com a área de Recursos Humanos);

- Elaboração de Política de Segurança da Informação, caracterizada pelo conjunto de princípios e valores estruturais, nos quais a

empresa explicita os seus propósitos, traduzidos em regras específicas para proteger as informações que são de sua propriedade ou que estão sob sua responsabilidade;

- Classificação de Informações e outros Objetos de TI;

- Definição dos mecanismos de Tecnologia da Informação que deverão dar suporte à Política.

5.2 SGSI (Sistema Gestor de Segurança da Informação)

Após a aceitação do projeto, efetuamos os devidos ajustes no escopo (como por exemplo, o aumento do prazo para início do projeto em um mês) e partimos para a criação do SGSI, esta última, uma tarefa que consumiu a primeira quinzena de fevereiro de 2007.

Sobre o aumento de prazo para o início do projeto, podemos justificar dizendo que a primeira estimativa não considerava apenas os dias úteis do mês, mas todos os dias da semana, ocasionando um aumento de 28% no tempo necessário para o projeto.

5.2.1 Desenvolvimento do SGSI

Nesta fase com a aprovação da direção foi possível implementar o SGSI com os responsáveis de cada setor da empresa, ficando a cargo do Gerente de TI (Tecnologia da Informação) e do Analista de RH (Recursos Humanos) a responsabilidade de organizar os itens apresentados a seguir:

- Participantes do SGSI: foram chamados a participar do comitê do SGSI os representantes de cada setor que são os responsáveis por seus departamentos. A participação do departamento de RH foi considerada essencial, pois este detem os dados referentes aos colaboradores e também é responsável por gerenciar todos os treinamentos internos e externos. Quanto ao departamento de TI, ele

é o responsável pelo treinamento dos colaboradores e também pelas definições de *hardware* e *software*, além de implantar, configurar e monitorar toda atividade de troca e armazenamento de informações na empresa;

- Objetivos do SGSI: entende-se como principal objetivo do SGSI ser um comitê aberto a discussões e voltado ao desenvolvimento contínuo do projeto de segurança da informação;

- Responsabilidades do SGSI: o SGSI é responsável por divulgar a política da segurança da empresa e pelas auditorias internas;

- Limites de atuação do SGSI: o SGSI subordinado a direção da empresa;

- Observar fatores legais e contratuais envolvidos nos negócios da empresa: o SGSI deve respeitar as leis federais, estaduais e municipais, bem como todos os contratos existentes com seus parceiros;

- Critérios para avaliação de riscos aos negócios: devem ser desenvolvidos em conjunto com seus parceiros de negócios, sendo associado às leis e contratos existentes.

Para apoiar o desenvolvimento do SGSI foi adotado o modelo de ciclo PDCA (*Plan-Do-Check-Act*) que foi discutido na Seção 4.2.1 desta dissertação.

Após o desenvolvimento foi possível estabelecer o SGSI conforme apresentado na Figura 7 do comitê gestor. Podemos observar na formação do SGSI que a Gestão de negócios representada pelos diretores são responsáveis por todo o processo de gestão.

Ainda na Figura 7 verificamos que a Gestão de Recursos está distribuída entre o departamento de RH e o departamento de TI. O RH ficou sendo

responsável pelas regras, treinamento e mediação de conflitos e a TI é responsável por tecnologia e treinamentos específicos de sistemas.

A participação do departamento de RH foi considerada essencial, pois na empresa Tecnicópias é o departamento responsável por todo agendamento e controle dos treinamentos e normas de conduta dos colaboradores.

Os representantes dos setores são responsáveis por aplicar e multiplicar o conhecimento da política de segurança da informação. Na Figura 7 observamos que todos os colaboradores, clientes e fornecedores devem atender aos requisitos estabelecidos pelo SGSI.

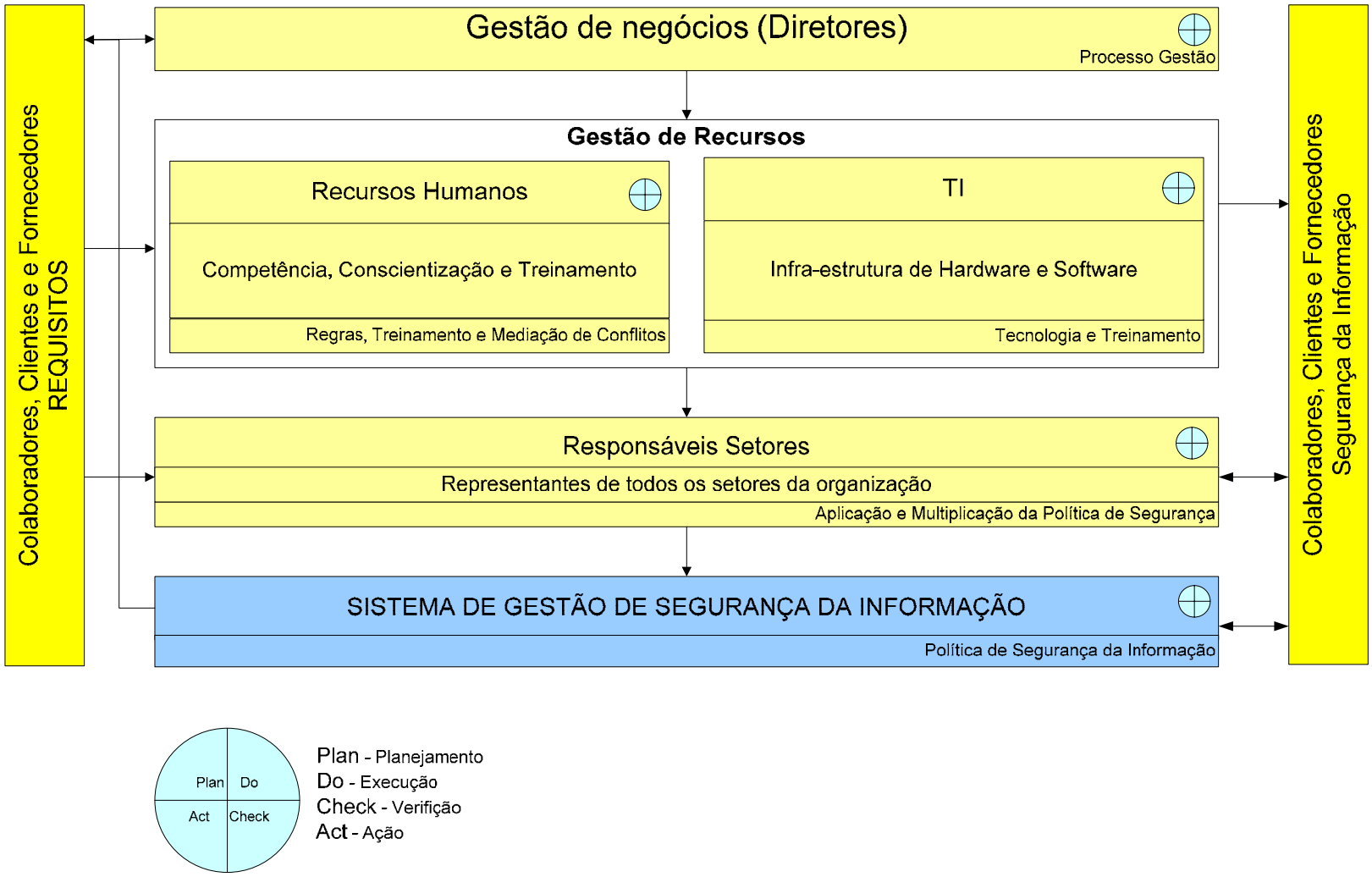


Figura 7: Comitê Gestor do SGSI

Fonte: Tecnicópias Gráfica e Editora LTDA.

5.2.2 Interações no SGSI

Para melhor entender a Figura 7 apresentações as interações existentes no SGSI:

- Gestão de Negócios: processo representado pelos diretores da empresa. São os patrocinadores do projeto e os membros responsáveis por auditar todos os trabalhos do SGSI aplicando o conceito PDCA.
- Gestão de Recursos: este processo é composto por dois departamentos:
- Recursos Humanos (RH): responsáveis pelos treinamentos, construção das regras, mediação de conflitos entre os setores da empresa;
- Tecnologia da Informação (TI): responsável pelos treinamentos dos recursos informatizados (*hardware* e *software*) e também por manter a infra-estrutura.
- Responsáveis dos Setores: são todos os gerentes, supervisores e encarregados de todos os setores da empresa que participam do desenvolvimento, aplicação e multiplicação da política de segurança da informação.
- Sistema de Gestão de Segurança da Informação: formado por todos os componentes do SGSI. Responsável por criar, manter e desenvolver a política de segurança da informação.
- Colaboradores, clientes e fornecedores: são responsáveis por antender aos requisitos da política de segurança da informação e com a atuação do SGSI recebem como produto final a segurança apoiada nos treinamentos e na infra-estrutura.

5.3 Levantamento e Análise

Após o desenvolvimento do SGSI procedemos aos levantamentos e análises para o desenvolvimento da política de segurança da informação.

5.3.1 Levantamento e Análise do Sistema de Informação (SGSI)

O levantamento processos possibilitou o desenvolvimento do diagrama de blocos apresentado na Figura 8 do sistema de informação (SI).

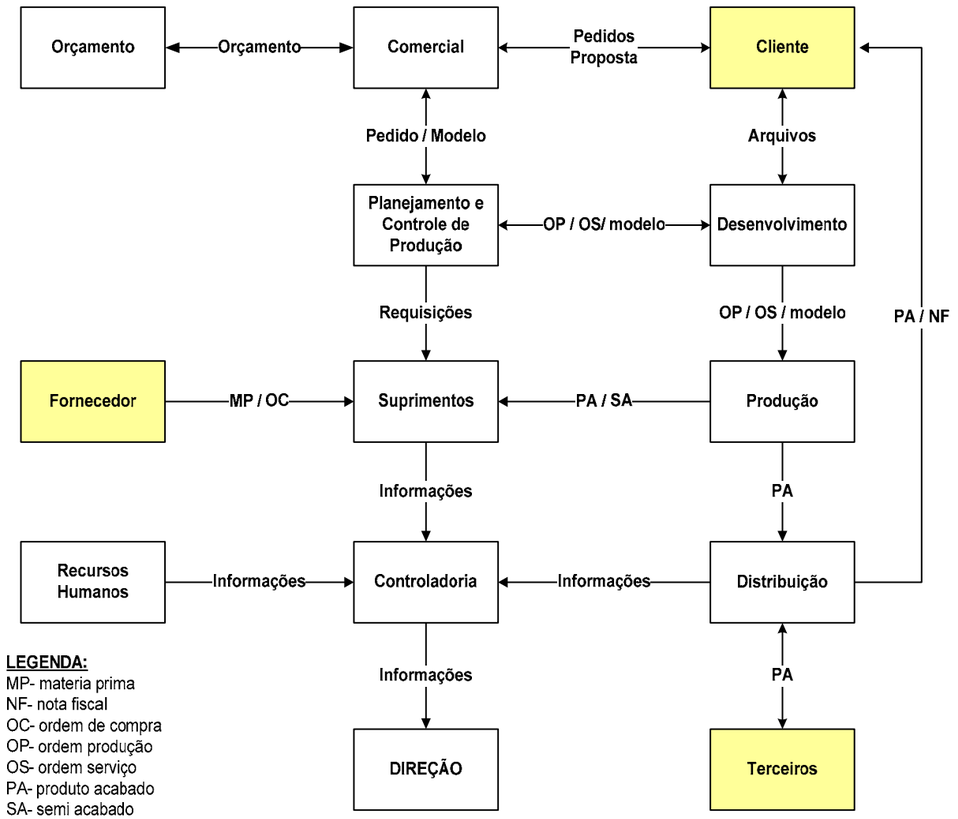


Figura 8: Diagrama de blocos da empresa estudada

Fonte: Tecnicópias Gráfica e Editora LTDA.

Podemos observar na Figura 8 que os processos estão intimamente relacionados aos clientes e fornecedores, havendo ainda um grupo especial de fornecedores de serviço que são chamados de Terceiros, que são responsáveis por parte da industrialização dos produtos da empresa.

Com o levantamento realizado, verifica-se que os seguintes pontos precisam ser considerados no SI: **i)** Ordem de compra; **ii)** Ordem de produção; **iii)** Ordem de

serviço e **iv)** Nota Fiscal que são os documentos mais importantes que circulam na empresa.

Análise de processos e discussão com os responsáveis: utilizando a análise obtida por intermédio do diagrama de blocos, podemos discutir com os membros do SGSI os colaboradores, clientes e fornecedores a classificação das informações e seus atributos de confidencialidade, disponibilidade e integridade.

5.3.2 Classificação das Informações

Com as análises realizadas no sistema de informação da empresa chegamos a classificação das informações que pode ser vista a seguir:

- Informação confidencial: toda e qualquer informação que contenha dados referentes a produtos de clientes e fornecedores, como especificação técnica e características funcionais;

- Informação Interna: informação que circula internamente na empresa e que não deve ser divulgada a clientes e fornecedores;

- Informação Pública: são todas as informações que não possuem qualquer restrição de confidencialidade ou segredo industrial;

- Informação Secreta: grau de acesso de cada colaborador de acordo com o tipo de informação.

Esta classificação deverá passar por uma revisão, pois constatou-se a necessidade de se criar uma classificação que leve em consideração se a informação é vital, crítica ou urgente.

5.4 Vulnerabilidades e Riscos

Conhecer as vulnerabilidades e riscos de um sistema de informação é uma tarefa que envolve muita análise e constante estudo dos processos inerentes às atividades corporativas.

A seguir demonstraram a aplicação do método proposto nessa dissertação começando pelo item que compreende a interpretação da norma ISO 17799.

5.4.1 Interpretação da norma ISO 17799

Pode-se dizer sem dúvida que a atividade foi facilitada após o levantamento do sistema de informações da empresa, sendo que neste levantamento observamos que alguns requisitos já estavam sendo atendidos, que são mencionados ao longo das seções.

5.4.2 Desenvolvimento e Treinamento da Política de Segurança da Informação

O primeiro requisito da norma é a política de segurança de informação, os demais itens podem ser colocados em um grande grupo de controles e tecnologias para a segurança da informação.

Temos nas seções a seguir o conjunto de diretrizes e regras que compõem a política da informação da empresa estudada e elas têm como intuito apresentar os procedimentos para normatizar, melhorar e disciplinar o uso dos recursos da rede.

O documento da política foi originado após intensas discussões entre o departamento de TI e os demais departamentos da empresa. A política apresentada a seguir deve passar por uma reformulação, para adequar por exemplo os tipos de controles existentes aos requisitos da política.

ITEM 1: AUTONOMIA DO DEPARTAMENTO DE TI

- O departamento de TI possui total autonomia para atuar sobre os equipamentos da empresa, sem prévio aviso, no que se refere aos seguintes tópicos:
- Realização de auditoria local ou remota;

- Definição de perfis de usuários cujos privilégios não permitam a realização de atividades tidas como prejudiciais ao *hardware* e *software* ou à rede como um todo;
- A instalação e configuração de *softwares* de monitoramento;
- A desinstalação de quaisquer *softwares* considerados prejudiciais à rede;
- O credenciamento e descredenciamento de usuários;

ITEM 2: DIRETRIZES QUANTO À UTILIZAÇÃO DA *INTERNET*

- A *internet* deve ser utilizada para fins corporativos, o enriquecimento intelectual de seus colaboradores ou como ferramenta para busca de informações que venham contribuir para o desenvolvimento de seus trabalhos.
- O uso para fins pessoais, mediante o consentimento do responsável pelo setor, fica restrito à consulta de movimento bancário e ao acesso ao *e-mail* pessoal, estando vedadas práticas abusivas tais como a circulação de correntes, material ponográfico entre outros.

ITEM 3: *E-MAIL* CORPORATIVO

- Desconfiar de todos os *e-mails* com assuntos estranhos ao ambiente de trabalho. Não reenviar *e-mails* do tipo corrente, aviso de vírus, avisos da Microsoft/AOL/Symantec, criança desaparecida, entre outros.
- Evitar enviar anexos acima de 10 Mbytes.

ITEM 4: A REALIZAÇÃO DE *DOWNLOAD*

- A realização de *downloads* exige banda de navegação do servidor e , se realizado em demasia, congestiona o tráfego e torna a navegação para os demais usuários mais demorada.
- A realização de *downloads* deve ser vista com muito cuidado e feita somente em casos de extrema necessidade.Além disso, estará limitada a arquivos de no máximo 1 MB (*Mega Byte*), pois *downloads* de arquivos de tamanho superior podem congestionar o fluxo de tráfego e comprometer os sistemas que funcionam *on-line*.

ITEM 5: EXECUÇÃO DE JOGOS E RÁDIOS *ON-LINE*

- É terminantemente proibida a execução de jogos, músicas ou rádios *on-line*, visto que esta prática congestiona a banda de *internet*, dificultando a execução de serviços que necessitam deste recurso.

ITEM 6: SENHAS DE ACESSO

- Cada setor deverá, através de comunicado oficial, indicar novos colaboradores e o perfil que devem possuir na rede e nos sistemas da empresa.
- A senha de acesso é pessoal, intransferível, cabendo ao seu titular total responsabilidade quanto seu sigilo.
- O compartilhamento de senhas de acesso é absolutamente proibido e o titular que divulgar sua senha a outrem responderá pelas infrações por esse cometidas, estando passível de advertência. Caso o usuário desconfie que sua senha não seja mais segura, poderá solicitar ao departamento de TI a alteração desta.
- As senhas têm validade de 30 dias.

ITEM 7: *SOFTWARES* DE CONVERSAÇÃO INSTANTÂNEA

- É permanentemente proibido aos setores o uso de *softwares* de conversação instantânea, ou de qualquer mecanismo que venha promover serviço semelhante, existentes ou que venham a existir.
- Pode haver permissão especial a qualquer setor para utilização de *Instant Messengers,* desde que seja para fins corporativos e comprovadamente utilizados em assuntos comerciais e/ou para suporte.

ITEM 8: A INSTALAÇÃO DE *SOFTWARES*

- Qualquer *software* que, por necessidade do serviço, necessitar ser instalado, deverá ser comunicado ao departamento de TI, que procederá a instalação caso constate a necessidade do mesmo. Fica proibida a instalação de qualquer *software* sem licença de uso.
- O departamento de TI poderá utilizar de sua autonomia citada no Item 2 deste instrumento para desinstalar, sem aviso prévio, todo e qualquer *software* sem licença de uso, em atendimento à lei do *software* (Lei 9.609/98).

ITEM 9: PENALIDADES

- O usuário que infringir qualquer uma das diretrizes de segurança expostas neste instrumento estará passível das seguintes penalidades (sem prévio aviso):
- Perda da senha de acesso aos sistemas e *Internet*;
- Cancelamento da caixa de *e-mail*;
- Advertência formal por intermédio do departamento de RH podendo levar inclusive a demissão do colaborador.

ITEM 10: EQUIPE DE SEGURANÇA DA INFORMAÇÃO

- Os servidores relacionados a seguir são diretamente responsáveis pela implantação presente política:
- Gestor de TI;
- Analista de Sistemas;
- Analista de Suporte.

ITEM 11: DIVULGAÇÃO E TREINAMENTO

- A política deve ser divulgada por intermédio de treinamento aos colaboradores, clientes e fornecedores, podendo ainda ser divulgada por *e-mail*, mural ou jornal interno.

ITEM 12: VIGÊNCIA E VALIDADE

- A presente política passa a vigorar a partir da data de sua homologação e publicação, sendo válida por tempo indeterminado podendo ser alterada conforme necessidades previamente detectadas.

5.4.3 Inventário de *Hardware* e *Software*

Devemos inventariar todo *hardware* e *software* presente na empresa, pois assim podemos ter um panorama das licenças existentes e das características e condições dos equipamentos.

É uma tarefa necessária, porém muitas empresas não dão o devido valor a este quesito. Primeiramente foram realizadas anotações manuais, entretanto após algum estudo, decidiu-se por adotar um *software* DUDE (DUDE, 2007) por ser gratuito e que permitiu o inventário em tempo real e *on-line* de todos os

equipamentos e *softwares* da rede da empresa. Poderíamos adotar outras ferramentas disponíveis no mercado como HP OpenView e Tívoli, no entanto devido ao custo utilizamos o DUDE.

As informações parciais obtidas para as licenças de *software* e o *hardware* encontram-se nas Tabelas 3 e 4, respectivamente.

Tabela 3: Lista parcial do Inventário de *Software*.

Item	Software	Qtd Total
1	Adobe Acrobat 7	12
2	Adobe Photoshop CS 3	10
3	Call Terminal Service Microsoft	5
4	EMS Datasul 204	50
5	Linux - Debian	2
6	Microsoft Office 2003	92
7	Microsoft Office 2004 MAC	10
8	Microsoft SQL Server 2000	5
9	Microsoft Windows 2003 Server	10
10	Microsoft Windos XP	92
11	Norton antivírus MAC	10
12	Norton antivírus Windows	97

Fonte: Tecnicópias Gráfica e Editora LTDA.

Tabela 4: Lista parcial do Inventário de *Hardware*.

Ano	Tipo	Descrição	Qtd
2005	REDE	CHAVEADOR PLANET KVM-400	1
2005	REDE	RACK FECHADO 44 U X 770 mm,	1
2005	REDE	SWITCH 3Com 24 PORT 3824 10/100/1000	4
2000	REDE	SWITCH 8 PORTAS 10/100 MBPS 3COM	1
2005	COMPONENTE	1 GB (2X512) DDR PC3200	4
2005	COMPONENTE	146.8 GB 10K U320 SCSI H. SWAP	4
2006	COMPONENTE	Bateria SURT192XLBP	1
2005	COMPONENTE	CATRACA WR-39 WOLPAC	1
2005	COMPONENTE	CATRACA WR-39 WOLPAC COM CONTADOR	1
2006	COMPONENTE	Disco Rígido 1200GB, U320, SCSI, 10K, 80P	1
2006	COMPONENTE	Disco Rígido 300GB, U320, SCSI, 10K, 80P	2
2006	COMPONENTE	Extensão de Garantia 7x24x4 (910-7660	1
2006	COMPONENTE	Fita Backup LTO3 - 10 unidades	1

Fonte: Tecnicópias Gráfica e Editora LTDA.

5.4.4 Coleta de Dados e Estatísticas

Para coletar os dados podemos utilizar ferramentas como IDS (*Intrusion Detection System*), *Port Scan* e *Sniffer*. Com os dados coletados podemos gerar estatísticas e assim aprimorar os controles de segurança.

Neste trabalho utilizamos o *software* Snort (SNORT, 2007) como ferramenta de IDS e o *Ethereal* (ETHEREAL, 2008) como *Sniffer*. Na Figura 9 podemos observar a configuração original dos componentes da rede antes da instalação do IDS Snort.

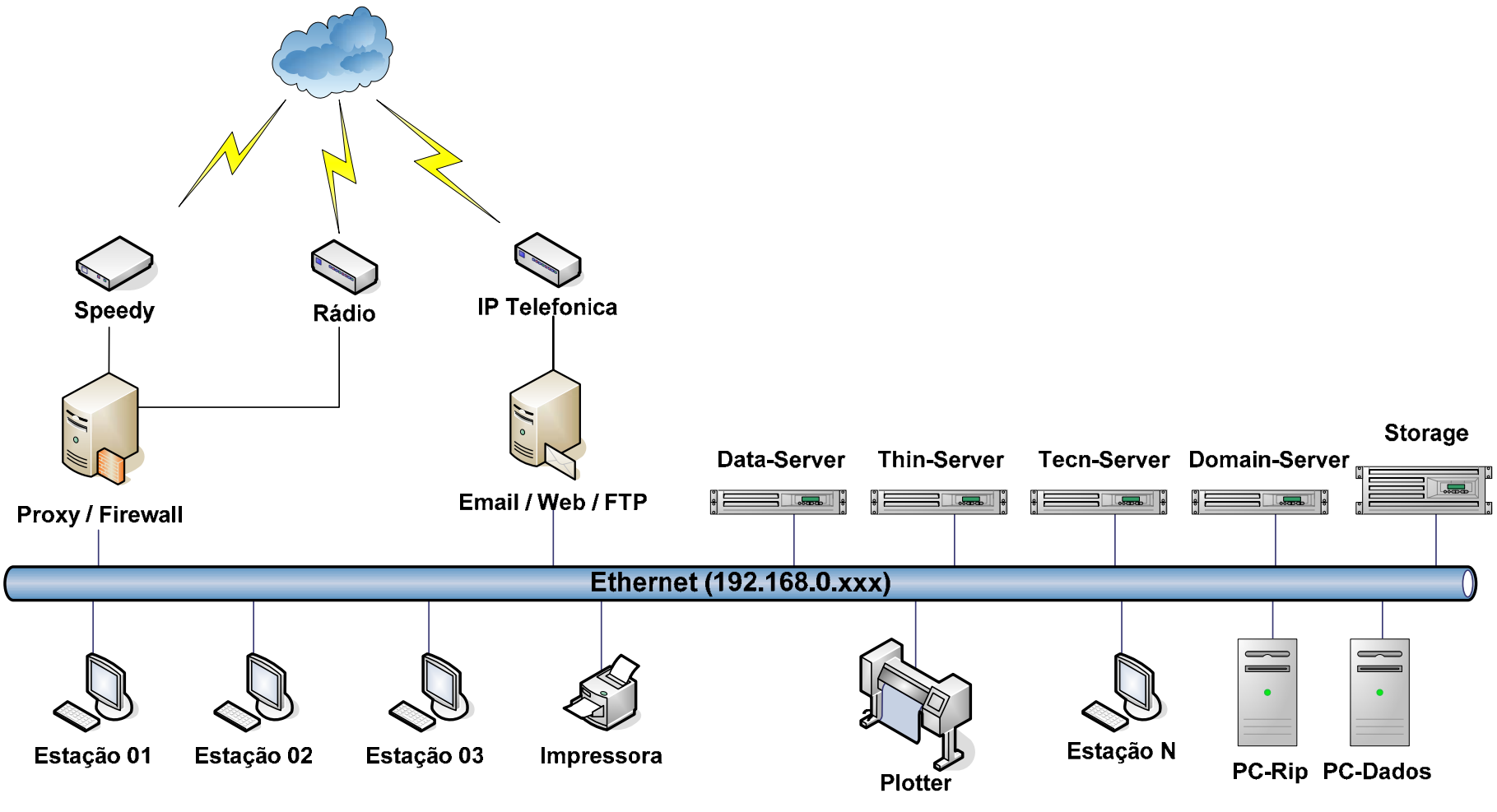


Figura 9: Diagrama original de rede.

Fonte: Tecnicópias Gráfica e Editora LTDA.

Fazendo uma análise da Figura 9 verificamos a existência de três *links* de *internet*. As conexões *Speedy* e Rádio com o servidor de *proxy/firewall* são utilizadas para navegação na internet, e o *link* IP da empresa Telefonica que dá suporte às aplicações de *e-mail*, páginas web e servidor de FTP.

Não existia na rede nenhum *software* que possibilitasse a verificação de ocorrências de ameaças, apesar da existência de um servidor de *Proxy* e *firewall*, que apenas filtram os pacotes IP que trafegam pela rede. Como solução para coletar dados estatísticos de ameças, adotamos um *software* IDS e, dentre as opções possíveis, escolhemos o Snort através de *benchmarking*. Com os dados coletados, chegamos às estatísticas de ocorrências no período de 01 a 31 de outubro de 2007 conforme resultados apresentadas no Gráfico 2.

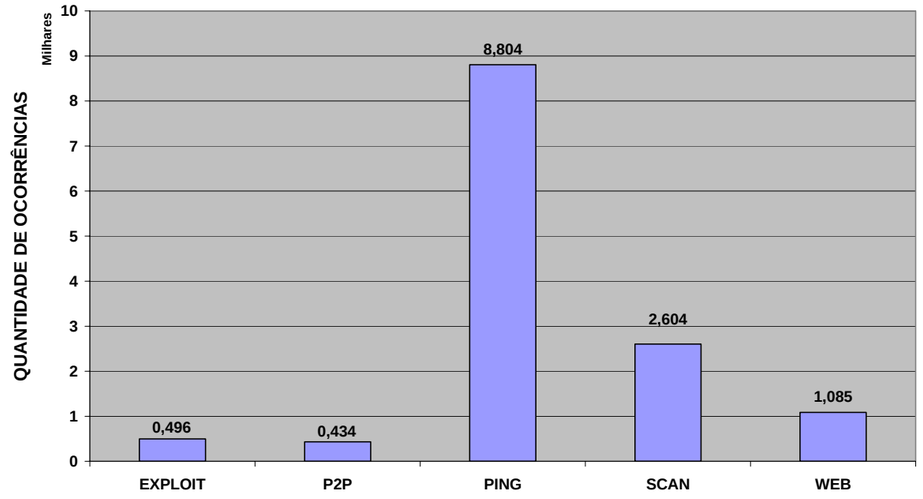


Gráfico 2: Ocorrências antes das configurações realizadas.

Para obter aos dados apresentados no Gráfico 2 precisamos configurar a rede com os equipamentos IDS como apresentado na Figura 10.

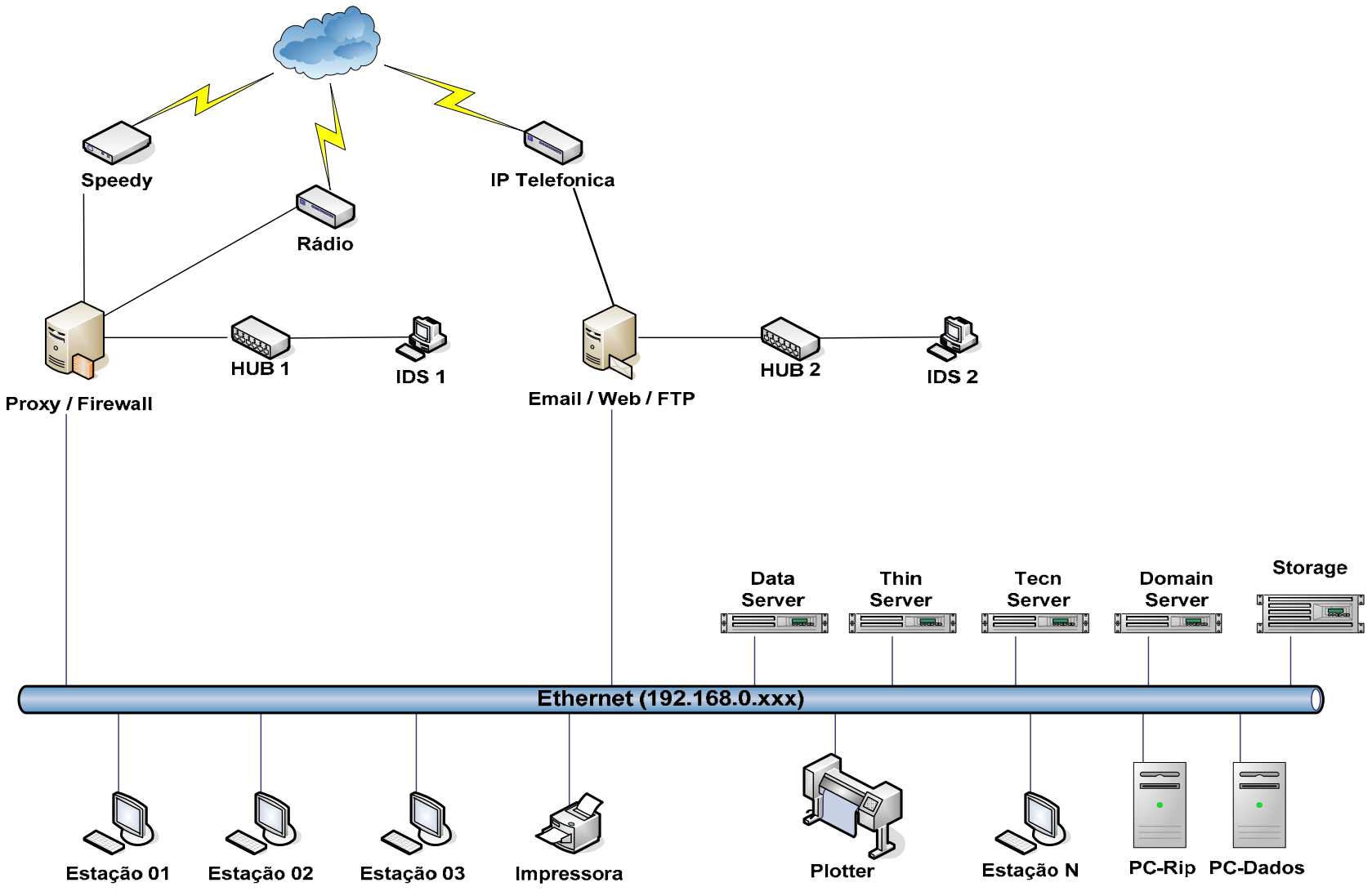


Figura 10: Diagrama de rede com IDS

Fonte: Tecnicópias Gráfica e Editora LTDA.

Na Figura 10, apresentamos a configuração após a instalação do equipamento IDS e um HUB junto ao servidor *proxy/firewall* e também da instalação de um segundo conjunto de IDS e HUB junto ao servidor de *e-mail*, *web* e FTP.

Como critério para configurar a rede dado a grande quantidade de ocorrências, consideramos a necessidade de bloquear todas as portas e liberar apenas as portas necessárias a execução de serviços. No Quadro 3 a seguir são apresentadas as portas liberadas por servidor.

Quadro 3: Portas abertas por Servidor.

Porta	Descrição	Proxy Firewall	E-mail Web Firewall	Data Server	Thin Server	Tecn Server	Domain Server	Storage
21	FTP	X						
22	SSH Interno	X	X					
25	SMTP	X	X					
53	DNS	X	X					
80	WEB		X					
135 a 139	NetBios				X	X	X	X
389	LDAP						X	
445	Microsoft-DS				X	X	X	X
636	LDAP						X	
3128	Proxy Interno	X						
3389	RDP				X	X	X	X
1433 a 1434	MS-SQL Server					X		
1723	VPN					X		

15000 a 15050	Progress			X				
25000 a 25010	Progress			X				
5555	SSH Externo	X						

Fonte: Tecnicópias Gráfica e Editora LTDA.

A liberação das portas apresentadas no Quadro 3 é justificada pelo serviço disponibilizado na rede em cada servidor. No Quadro 4 a seguir apresentamos a descrição do serviço de cada porta liberada.

Quadro 4: Portas abertas por Servidor.

Porta	Descrição	Descrição do Serviço
21	FTP	Transferência de arquivos entre empresa e parceiros
22	SSH Interno	Acesso remoto para manutenção interna
25	SMTP	Acesso a e-mail
53	DNS	Servidor de nomes
80	WEB	Acesso a páginas WEB
135 a 139	NetBios	Compartilhamento de Pastas
389	LDAP	Servidor de e-mail
445	Microsoft-DS	Serviço de diretório
636	LDAP	Servidor de e-mail
3128	Proxy Interno	Acesso interno a WEB
3389	RDP	Acesso remoto a servidor windows
1433 a 1434	MS-SQL Server	Servidor de banco de dados
1723	VPN	Rede virtual privada para clientes

15000 a 15050	Progress	Servidor de banco de dados
25000 a 25010	Progress	Servidor de banco de dados
5555	SSH Externo	Acesso remoto para manutenção externa

Fonte: Tecnicópias Gráfica e Editora LTDA.

Uma observação é que as portas descritas acima podem ser utilizadas como referência para outras empresas que possuam servços semelhantes.

Todos os serviços foram desativados por não serem utilizados, não possuindo qualquer utilidade à empresa. O servidor de *internet* possuía um serviço de páginas web que foi desativado, o servidor instalado era o APACHE (APACHE, 2008).

Constatou-se a utilização na rede de uma conexão P2P após a detecção da conexão pelo IDS conseguimos determinar exatamente qual equipmento estava utilizand o acesso através da identificação do IP pelo *Sniffer Ethereal*.

A ocorrência de *exploit* foi ocasionada pelo servidor web que respondia a programas maliciosos. Para auxiliar na análise foi desenvolvido o Gráfico 3 que apresenta a quantidade de ocorrências acumuladas por dia da semana.

Constatamos a utilzação de *e-mails* para o envio de arquivos com tamanhos acima de 10 Mbytes, sendo o serviço de *e-mail* uma forma inadequada para arquivos grandes.

Foi diagnosticado que o *software* antivírus e o sofware de *backup* não possuíam licença para utilização.

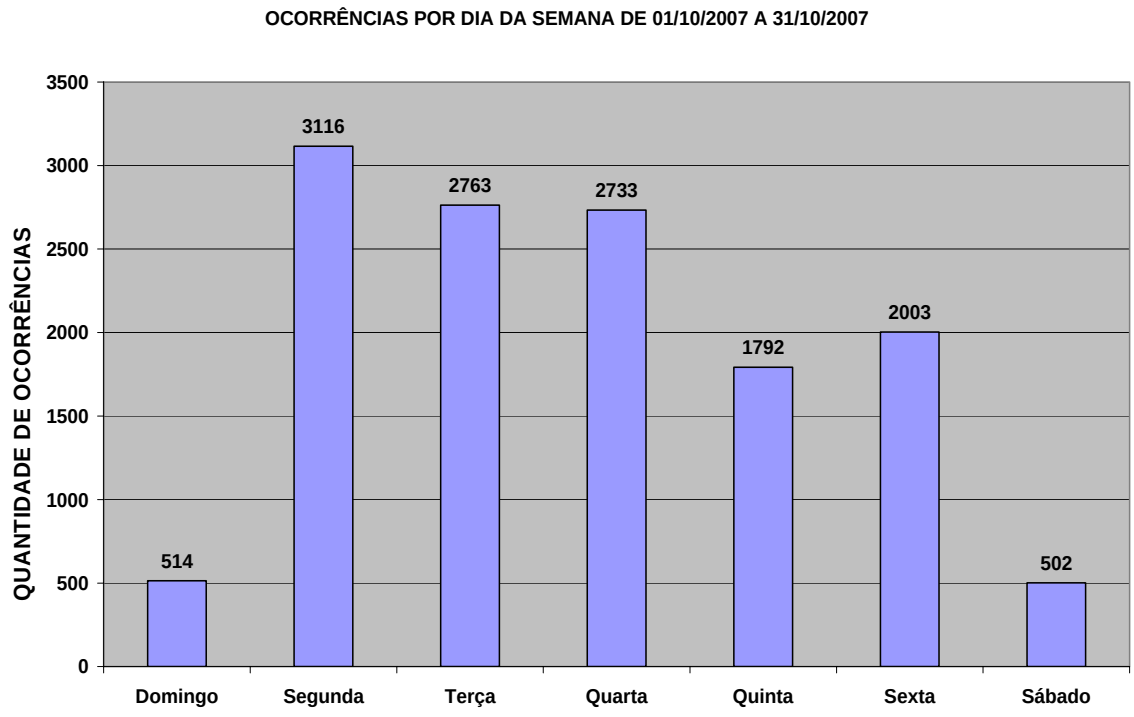


Gráfico 3: Ocorrências antes das configurações realizadas.

No Gráfico 3 verificamos que os dias com maiores ocorrências são a segunda, terça e quarta-feira, nestes dias existe uma intensa troca de dados com clientes e fornecedores pelo serviço de FTP.

Ainda podemos observar no Gráfico 4 as ocorrências do pior dia da semana durante o período estudado, trata-se de toda segundda-feira, porque é o dia que o setor de desenvolvimento de produto recebe a maioria dos arquivos dos clientes e foenecedores.

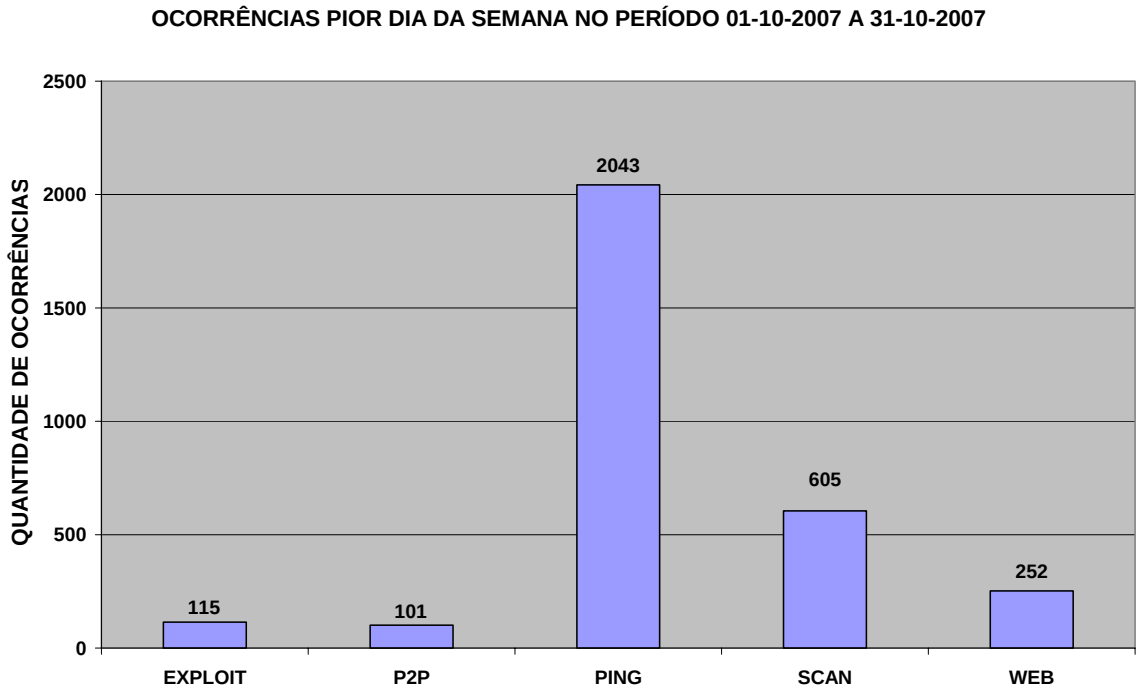


Gráfico 4: Ocorrências antes das configurações realizadas no pior dia da semana.

Devemos lembrar que a empresa em questão trabalha 24 horas por dia, durante 7 dias na semana. Com a posse dos dados coletados partimos para o desenvolvimento do plano de ação como descrito na seção 5.5 que busca oerganizar e determinar: **i)** O que vai fazer; **ii)** Porque; **iii)** Quem fará; **iv)** Como fará e **v)** Prazo.

5.5 Plano de Ação

Considerando a análise da empresa, o diagnóstico e os objetivos do projeto de segurança, foi elaborado o Quadro 5 com o plano de ação. Este plano teve o intuito de contribuir para o desenvolvimento e melhoria do processo de segurança da informação da empresa estudada.

Quadro 5: Plano de Ação.

ITEM	O QUE FAZER	PORQUE	QUEM FARÁ	COMO FARÀ	PRAZO
1	Escolha de	Compra de	Dep. TI	Benchmarking	07/10/07

	tecnologias para segurança	*softwares* em substituição de *softwares* sem licença	e Dep. de Compras	baseado em critérios estabelecidos	
1.1	Compra de *software* Antivírus	*Sofware* sem licença	Dep. TI e Dep. de Compras	Benchmarking baseado em critérios estabelecidos	07/10/07
1.2	Compra software Backup	*Sofware* sem licença	Dep. TI e Dep. de Compras	Benchmarking baseado em critérios estabelecidos	07/10/07
2	Implantação de Tecnologias em Ambiente de Testes	Testes de novos *softwares* e novas configurações de segurança	Dep. TI	Testes e documentação por intermédio de operações na rede da empresa	15/10/07
2.1	Alterar Permissões de Acesso	Usuários com acesso para instalar *software* e alterar configuração de equipamentos	Dep. TI	Alterar permissões no servidor de domínio	03/10/07
2.2	Reconfigurar Firewall	Para não responder a comandos *PING* e bloquear portas	Dep. TI	Alterar *Script Firewall* baseando-se em *Logs* do IDS	05/10/07
2.3	Reconfigurar	Não permitir	Dep. TI	Alterar *Script*	10/10/07

	Proxy	acesso a redes P2P		*Proxy* baseando-se em *Logs* do IDS	
2.4	Implantar software Antivírus	Usuários com acesso a instalar *softwares* e alterar configurações de equipamentos	Dep. TI	Remoção software não licenciado e instalação de novo *software*	09/10/07
2.5	Criar Política de Backup	*Backup* atualmente não segue regras claras	Dep. TI	Pesquisa políticas de *Backup*	05/10/07
2.6	Instalar Servidor VPN	Para acesso remoto de clientes, fornecedores e colaboradores	Dep. TI	Configuração do servidor *Web*	10/10/07
2.7	Instalar Servidor FTP	Para troca de arquivos com cliente	Dep. TI	Configuração do servidor *Web*	25/10/07
2.8	Instalar *Software* de Backup	Instalar *Software* Comprado	Dep. TI	Instalação em servidor de arquivos	20/10/07
2.9	Desinstalar serviços em servidores	Remover *softwares* desnecessarios que podem ser alvo de ameaças como	Dep. TI	Remoção com base nos *logs* do IDS	15/10/07

		o servidor de páginas web			
3	Implantação de Tecnologias em ambiente de produção	Depois de realizar todos os testes realizar tarefas no ambiente de produção	Dep. TI	Implantação com base na documentação gerada a partir do ambiente de teste	31/10/07

Fonte: Tecnicópias Gráfica e Editora LTDA.

5.5.1 Escolha de Tecnologias para Segurança

Para escolher as tecnologias para segurança utilizamos os critérios apresentados na seção 4.5.1 desta dissertação.

No Quadro 6 apresentamos os critérios aplicados para o *software* anti-vírus, no Anexo D podemos encontrar os quadros com os critérios de ecolha de *software* para as ferramentas aplicadas no projeto de segurança.

Quadro 6: Critérios aplicados na escolha de *Software* Anti-Vírus.

Critério	Kaspersky	Symantec Norton	BitDefender	Eset NOD32	Panda	Alwil Avast	Grisoft AVG	Trend Micro
Preço	$ 39,50	$ 45,00	$ 41,00	$ 42,50	$ 30,00	$ 45,00	$ 31,00	$ 40,00
Atualizações	Diária	Diária	Diária	Diária	Diária	Diária	Diária	Diária
Ameaças Detectadas	96%	95%	96%	90%	90%	92%	91%	82%
Sistemas Operacion	Windows	Windows	Windows	Windows	Windows	Windows	Windows	Windows

ais Suportados		Macintosh						
Uso Corporativo	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Proteção E-mail	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Proteção de mensagens instantâneas	Sim	Sim	Sim	Sim	Sim	Sim	Não	Não
Agendamento de verificação	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim

Fonte: Fonte: Tecnicópias Gráfica e Editora LTDA.

Para validar as verificações do *software* antivírus optamos por instalar em um ambiente de testes, o amiente de testes utilizado foi o setor de TI.

Como no caso apresentado no Quadro 6, também utilizamos esta forma de pesquisa para IDS, *Firewall* e *Backup*

5.5.2 Implantação de Tecnologias em Ambiente de Testes

Nesta fase colocamos em prática o plano de ação em um ambiente de testes que reproduziu as operações que ocorrem no ambiente de produção, o que possibilitou realizar tarefas sem prejuízo do dia-a-dia da empresa.

A documentação das atividades permitiu reproduzir todas as ações necessárias reproduzir as instalações e configurações no ambiente de produção de modo mais seguro e sem grandes riscos a empresa.

5.5.3 Implantação de Tecnologias em Ambiente de Produção

Depois de realizar a implantação no ambiente de testes e a familiarização com o funcionamento das tecnologias, estamos prontos a implantar no ambiente de produção com segurança.

No Gráfico 5 apresentam-se os resultados obtidos após a implantação das configurações de segurança na empresa estudada.

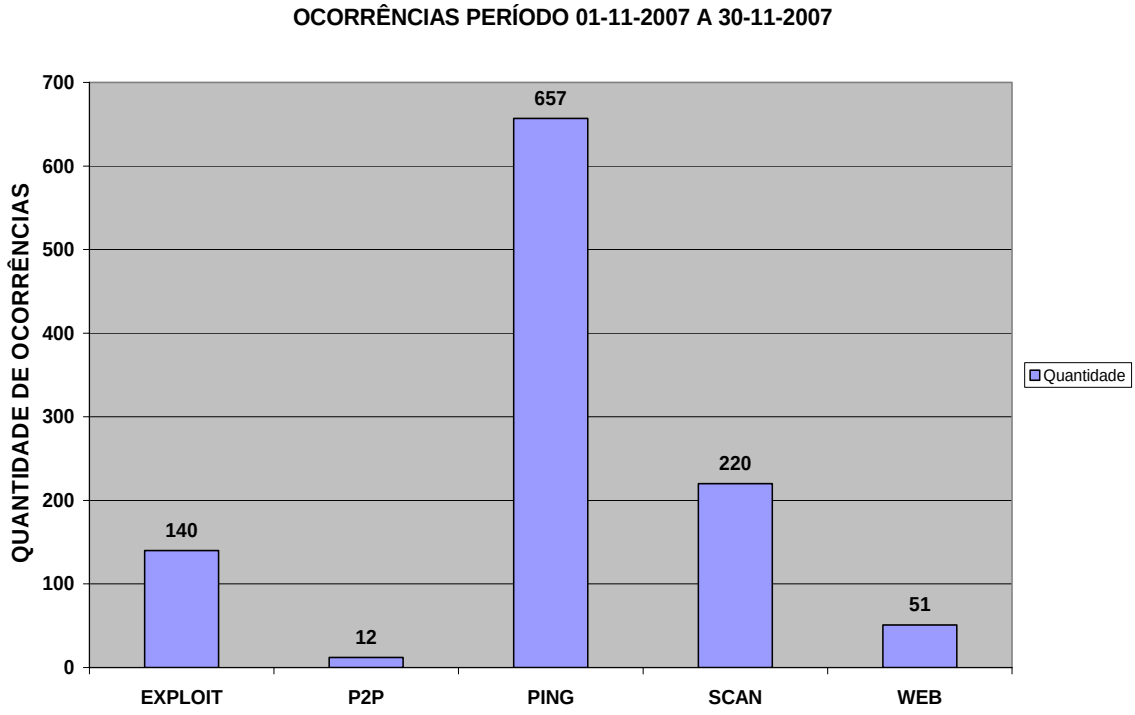


Gráfico 5: Ocorrências após configurações de segurança realizadas.

No Gráfico 6 apresenta-se os resultados obtidos antes e após a implantação das configurações de segurança na empresa estudada.

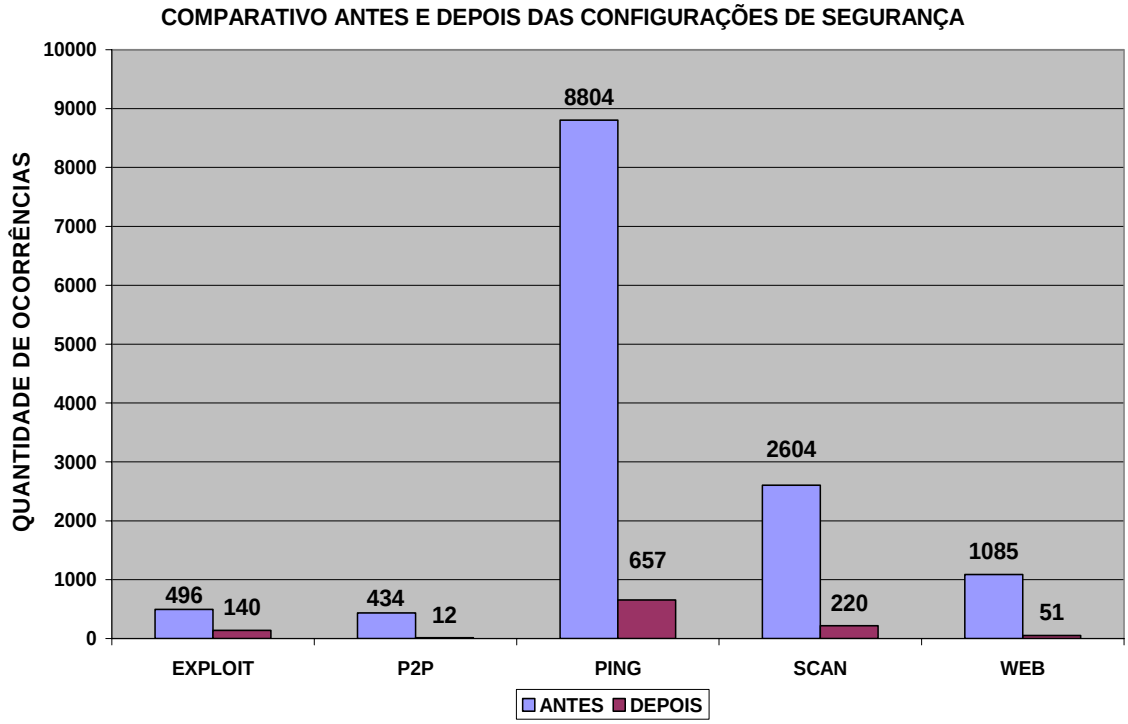


Gráfico 6: Ocorrências antes e após configurações de segurança realizadas.

Foram selecionadas para o Gráfico 6 as ocorrências de ameaças em dois períodos distintos, o período nomeado como “antes” ocorreu entre 02/10/2007 e 31/09/2007 e aquele identificado como “depois” entre 01/11/2007 e 30/11/2007.

Podemos observar uma sensível redução na ocorrência de ameaças, podendo chegar à estes números aplicando um conjunto de práticas recomendadas pela ISO 17799, como monitoração e prevenção.

5.6 Manutenção

Esta etapa representa a melhoria contínua do projeto de segurança, pois aqui iniciamos o 4.4.3 de Inventário de *Hardware* e *Software* e procedemos a um laço contínuo passando por uma nova coleta de dados e estatísticas e voltando para o plano de ação.

6 Conclusão

Concluímos através de nosso trabalho que a tarefa de segurança da informação é algo que envolve diversas questões normativas, tecnológicas e políticas, necessitando de um método para implantação de projetos de segurança.

Neste trabalho buscou-se desenvolver um método que permita as empresas implantarem um sistema para a segurança da informação de modo customizado, de acordo com suas necessidades e percepções.

Com a implantação do método conseguimos uma redução no número de ocorrências de ataques, melhor controle de licenças de *softwares*, também conseguimos racionalizar a utilização dos equipamentos e recursos de rede e maior comprometimento dos colaboradores.

Este trabalho não pretende ser uma solução definitiva para os problemas de segurança da informação, pois se entende que a segurança é realmente algo dinâmico, em vista das novas ameaças que surgem diariamente. Por conta disso, os gestores de TI devem se manter constantemente atualizados com a literatura da área.

Acreditamos que conseguimos dar nossa contribuição ao tema, pois não se encontra na literatura nada que indique quais ferramentas de software ou hardware que devem ser utilizadas, enquanto neste trabalho apresentamos um conjunto de ferramentas e técnicas que se implantadas podem reduzir os problemas de segurança.

Para trabalhos futuros, a aplicação ou adequação do método a redes sem fio e a redes hetereogêneas, as quais envolvem uma maior complexidade e variedade de equipamentos.

7 Referências

ABNT ISO 17799. Associação Brasileira de Normas Técnicas (ABNT). Norma ABNT NBR ISO/IEC 17799:2005 – Código de prática para a Gestão da Segurança da Informação, 2005.

ABNT ISO 27001. Associação Brasileira de Normas Técnicas (ABNT). Norma ABNT NBR ISO/IEC 27001:2006 – Sistemas de Gestão de Segurança da Informação - Requisito, 2006.

AIRSNORT. Version 2.6. Sourceforge. 2007. Disponível em <http://airsnort.shmoo.com/>. Acesso em: 10 dez. 2007.

ALBERTIN, A. Luiz; MOURA, Rosa Mª de. Administração de Informática: Funções e Fatores Críticos de Sucesso. SP: Atlas, 2001.

APACHE. Version 2. The Apache Software Foundation. 2008. Disponível em: <http://www.apache.org/>. Acesso em: 09 jan. 2008.

BRASILIANO, Antonio Celso Ribeiro. A (In) Segurança nas Redes Empresariais: A inteligência Competitiva e a Fuga Involuntária das Informações. SP: Scicurezza: Brasiliano & Associados, 2002.

CARVALHO, Luciano Gonçalves. Segurança de Redes. RJ: Ciência Moderna LTDA, 2005.

CAIN. Version 4.9: Oxid IT. 2007. Disponível em: <http://www.oxid.it/cain.html>. Acesso em: 14 dez. 2007.

CERT.br. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Estatísticas do CERT.br. Disponível em: <http://www.cert.br/incidentes/>. Acesso em: 18 out. 2007.

CHESWICK, W.; BELLOVIN, S. M. ; RUBIN. A. D.; Firewalls e Segurança na Internet. 2.ed. RS. Bokman. 2005.

DUDE. Versin 3: Mikrotik. 2007. Disponível em: <http://www.mikrotik.com/thedude.php/>. Acesso em: 02 mai. 2007.

ETHEREAL. Version 1: Ethereal Inc.. 2007. Disponível em: <http://www.ethereal.com/>. Acesso em: 01 out. 2007.

FIREFOX. Version 2: The Mozilla Foundation. 2008. Disponível em: <http://www.mozilla.org/>. Acesso em: 07 jan. 2008.

FITZGERALD, Jerry; DENNIS, Alan. Comunicação de Dados Empresariais e Redes. RJ: LTC, 2005.

HATCH, Brian; LEE, James; KURTZ, George. Segurança contra Hackers. SP: Futura, 2003.

KUROSE. J.F., ROSS, K. W. Redes de Computadores e a Internet. São Paulo. Addison Wesley. 2003.

LANGUARD. Version 8: GFI. 2008. Disponível em: <http://www.gfi.com/languard/>. Acesso em: 07 jan. 2008.

LAUDON, Kenneth, Jane P. Gerenciamento de sistemas de informação. RJ: LTC, 2003.

LINUX. Linux Org. 2008: Disponível em: <http://www.linux.org/>. Acesso em: 08 jan. 2008.

MICROSOFT INTERNET EXPLORER. Version 7: Microsoft Corporation, 2007. 1 CD-ROM.

MICROSOFT INTERNET INFORMATION SERVER. Version 4: Microsoft Corporation, 2003. 1 CD-ROM.

MICROSOFT OUTLOOK EXPRESS. Version 6: Microsoft Corporation: 2004. 1 CD-ROM.

MICROSOFT WINDOWS SERVER. Version 2003: Microsoft Corporation, 2003. 1 CD-ROM.

MÓDULO Security Solution. 2006. Disponível em: <http://www.modulo.com.br>. Acesso em: 18 jul. 2007.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício. Segurança de Redes em Ambientes Cooperativos. SP: Berkeley, 2002.

NMAP. Version 4: Insecure. 2008. Disponível em: <http://www.insecure.org/>. Acesso em: 07 jan. 2008.

PFLEEGER, Charles P. Security in Computing. 2. Ed. New Jersey, USA: Prentice Hall, 1997.

PGP. PGP Corpotarion. 2007. Disponível em: <http://www.pgp.com/>. Acesso em: 17 dez. 2007.

RFC 1320. RIVEST, R., “MD4 – Message Digest Algorithm,” RFC 1320, MIT, APRIL 1992.

RFC 1321. RIVEST, R., “MD5 – Message Digest Algorithm,” RFC 1321, MIT, APRIL 1992.

RFC 2140. TOUCH, J., "TCP CONTROL BLOCK INTERDEPENDENCE," RFC 2140, USC/ISI, APRIL 1997.

ROESCH, Martin. Snort Users Manual – The Snort Project. Sourcefire Inc, 2006.

SNORT. Version 2.7: Sourcefire. 2007. Disponível em: <http://www.snort.org/>. Acesso em: 09 dez. 2007.

SOUZA, Ranieri M., LOTITO, Alberto, MORALES, Marcelo A., FAGOTTO, Eric A. M. A Methodology for Integration of Technologies and Procedures for Security of Information in: 4th CONTECSI, USP. SP, 2007.

SQUID. Version 2.6: Squid Org. 2008. Disponível em: <http://www.squid-cache.org/>. Acesso em: 09 jan. 2008.

STALLINGS, William. Cryptography and Network Security: Principles and Practice, Third Edition. Prentice-Hall, 2003.

SYGATE. Version 5.6: Symantec. 2007. Disponível em: <http://www.symantec.com/>. Acesso em: 30 dez 2007.

TANENBAUM, A. S. Redes de Computadores. 4. Ed. Rio de Janeiro, Brasil: Ed. Campus, 2003.

WADLOW, Thomas. Segurança de Redes - Projeto e Gerenciamento de Redes Seguras. SP: Campus, 2000.

ZONE ALARM. Version 6.1.7: Check Point Software Technologies Ltda. 2008. Disponível em: <http://www.zonealarm.com/>. Acesso em: 06 jan 2008.

8 Bibliografias Consultadas

A.G. KOTULIC AND J.G. CLARK, “Why There Aren’t More Information Security Research Studies,” *Information & Management*, vol. 41, 2004, pp. 597–607.

ANDRZEJ BIALAS: Information Security Systems vs. Critical Information Infrastructure Protection Systems - Similarities and Differences. DepCoS-RELCOMEX 2006: 60-67.

ANÔNIMO. Segurança Máxima: O Guia de um Hacker para Proteger seu Site da Internet e sua Rede. RJ: Campus, 2001.

A. PASUPULATI ET AL. BUTTERCUP: On network-based detection of polymorphic buffer overflowvulnerabilities. In *IEEE/IFIP Network Operation and Management Symposium*, 2004.

A. R. BERESFORD AND F. STAJANO. Location privacy in pervasive computing. *IEEE Pervasive Comp.*, 3(1):46–55, 2003.

A. R. BERESFORD AND F. STAJANO. Mix zones: User privacy in location-aware services. *IEEE PerSec*, 2004.

ASLAN ASKAROV, ANDREI SABELFELD. Gradual Release: Unifying Declassification, Encryption and Key Release Policies. Proceedings of the 2007 IEEE Symposium on Security and Privacy, p.207-221, May 20-23, 2007.

B. V. CHESS. Improving computer security using extended static checking. In *Proceedings of 2002 IEEE symposium on security and privacy*, 2002.

BEAL, Adriana. Manual de Segurança da Informação. Vydia Tecnologia, Março 2002.

BONAN, Adilson Rodrigues. Configurando e usando o Sistema Operacional Linux. SP: Futura, 2003.

CASANAR, ALEX DELGADO GONÇALVES.Impacto da Implementação da norma de segurança NBR ISO/IEC 17799: Código de Prática para a Gestão da Segurança da Informação nas empresas; UFSC: Universidade Federal de Santa Catarina.

C. KREIBICH AND J. CROWCROFT. Honeycomb - creating intrusion detection signatures using honeypots. In *HotNets-II*, 2003.

C. YAN, D. ENGLENDER, M. PRVULOVIC, B. ROGERS, AND Y. SOLIHIN. Improving cost, performance, and security of memory encryption and authentication. In *Proceedings of the 33rd International Symposium on Computer Architecture (*ISCA*'06)*, pages 179–190. IEEE Computer Society, June 2006.

CHATEL, M. *Classical versus Transparent IP Proxies*: RFC 1919. Annecy-Le-Vieux, France: Internet Engineering Task Force, Network Working Group, 1996.

CHEN, H. et al. (2004) "Crime Data Mining: A General Framework and Some Examples", *IEEE Computer*, 37(4), pp. 50-56.

COMER, D. E. Interligação em redes com TCP/IP. 5. ed. São Paulo: Campus, 2006.

COMMON CRITERIA PROJECT. Common Criteria for Information Technology Security Evaluation (CC 2.2), Part 2: Security functional requirements, January 2004.

CRISPIN COWAN, PERRY WAGLE, CALTON PU, STEVE BEATTIE E JONATHAN WALPOLE. Buffer overflows: Attacks and defenses for the vulnerability of the decade. Em DARPA Information Survivability Conference and Exposition, p´aginas 119–129, 2000.

D. Box, F. Curbera, M. Hondo, C. Kaler, D. Langworthy, A. Nadalin, N. Nagaratnam, M. Nottingham, C. von Riegen, and J. Shewchuk. Web Services Policy Framework (WSPolicy). Version 1.1, September 2004.

D. CLARKE, G. E. SUH, B. GASSEND, A. SUDAN, M. VAN DIJK, AND S. DEVADAS. Towards constant bandwidth overhead integrity checking of untrusted data. In *Proceedings of the 2005 IEEE Symposium on Security and Privacy*, pages 139–153. IEEE Computer Society, May 2005.

D. EVANS AND A. TWYMAN. Flexible policy-directed code safety. In *Proceedings of 1999 IEEE symposium on security and privacy*, May 1999.

D. J. PACK AND B. E. MULLINS. A portable microcontrollerbased HTTP tunnelling activity detection system. In Proceedings of the 2003 IEEE International Conference on Systems, Man and Cybernetics, volume 2, pages 1544–1549, October 2003.

D.W STRAUB AND R.J. WELKE, “Coping with Systems Risk: Security Planning Models for Management Decision-Making,” MIS Quarterly, vol. 22, no. 4, 1998, pp. 441–470.

D. WAGNER AND D. DEAN. Intrusion detection via static analysis. In *Proceedings of 2001 IEEE symposium on security and privacy*, 2001.

DIPANKAR DASGUPTA E HAL BRIAN. Mobile security agents for network traffic analysis. Em Proceedings of the Second DARPA Information Survivability Conference and Exposition II, p´aginas 332–340, 2001.

DIPANKAR DASGUPTA E FABIO GONZÁLEZ. An immunity-based technique to characterize intrusions in computer networks. IEEE Transactions on Evolutionary Computation, volume 6, p´aginas 281–291, 2002.

DRAFT BS 7799-2:2002, Information Security Management - Part2: Specification for Information Security Management System. BSI, Novembro de 2001.

F. HSU AND T. CHIUEH. CTCP: A centralized TCP/IP architecture for networking security. In *ACSAC*, 2004.

FABRÍCIO DE PAULA, MARCELO DOS REIS, DIEGO FERNANDES E PAULO DE GEUS. ADenoIdS: A hybrid IDS based on the immune system. Em Proceedings of the Ninth International Conference on Neural Information Processing, páginas 479–484, 2002.

FERNANDO ESPONDA, STEPHANIE FORREST E PAUL HELMAN. A formal framework for positive and negative detection schemes. IEEE Transactions on Systems, Man and Cybernetics, p´aginas 357–373, 2004.

FERREIRA, AURÉLIO BUARQUE DE HOLANDA. Dicionário Aurélio Eletrônico Século XXI, 1. ed. São Paulo: Editora Nova Fronteira, 1999. 3V.

G. DHILLON AND J. BACKHOUSE. Information Systems Security Management in the New Millennium, Comm. ACM, vol. 43, no. 7, 2000, pp. 125–128.

G. E. SUH, C. W. O'DONNELL, I. SACHDEV, AND S. DEVADAS. Design and implementation of the AEGIS single-chip secure processor using physical random functions. In *Proceedings of the 32nd Annual International Symposium on Computer Architecture (*ISCA*'05)*, pages 25–36. IEEE Computer Society, June 2005.

G. KC, A. KEROMYTIS, AND V. PREVELAKIS. Countering code-injection attacks with instruction-set randomization. In *ACM CCS*, 2003.

H. FENG et al. Anomaly detection using call stack information. In *IEEE S&P*, 2003.

H. KIM AND B. KARP. Autograph: Toward automated, distributed worm signature detection. In *USENIX Security*, 2004.

H. WANG et al. Shield: Vulnerability-driven network filters for preventing known vulnerability exploits. In *SIGCOMM*, 2004.

ISSA. Information System Security Association Journal. Módulo Security – acessado em 13-11-2006 – disponível em http://www.modulo.com.br.

J. GIFFIN, S. JHA, AND B. MILLER. Efficient context-sensitive intrusion detection. In *NDSS*, 2004.

J. NEWSOME ET AL. POLYGRAPH: Automatically generating signatures for polymorphic worms. In *IEEE S&P*, 2005.

J. NEWSOME AND D. SONG. Dynamic taint analysis for automatic detection, analysis, and signature generation of exploits on commodity software. In *NDSS*, 2005.

J. P. EARLY, C. E. BRODLEY, AND C. ROSENBERG. Behavioral authentication of server flows. In ACSAC ’03: Proceedings of the 19th Annual Computer Security Applications Conference, December 2003.

J. REYNOLDS et al. On-line intrusion detection and attack prevention using diversity, generate-and-test, and generalization. *Hawaii Intl. Conference on System Sciences*, 2003.

J. XU, P. NING, C. KIL, Y. ZHAI, AND C. BOOKHOLT. Automatic diagnosis and response to memory corruption vulnerabilities. In *CCS*, 2005.

JASON, J., RAFALOW, L. E VYNCKE. 2003. IPSec configuration policy information model. RFC 3585.

K. ASHCRAFT AND D. ENGLER. Using programmer-written compiler extensions to catch security holes. In *Proceedings of 2002 IEEE symposium on security and privacy*, 2002.

K. WANG AND S. STOLFO. Anomalous payload-based network intrusion detection. In *RAID*, 2004.

KENT, S. E ATKINSON, R. 1998. Security architecture for the internet protocol. RFC 2401.

KLENSIN, J. *Simple Mail Transfer Protocol*: RFC 2821. Boston, MA: Internet Engineering Task Force, Network Working Group, 2001.

Kwon, Sungho Jang, Sangsoo Lee, Jaeill. Study on the General Defects in the Information Security Management System (ISMS). Proceedings of the 2007: Information & Communications Technology, 2006. ICICT '06. ITI 4th International Conference on Publication Date: Dec. 2006 On page(s): 1-2.

L. Lymberopoulos, E. Lupu, and M. Sloman. Ponder policy implementation and validation in a CIM and differentiated services framework. In IFIP/IEEE Network Operations and Management Symposium (NOMS 2004), Seoul, Korea, April 2004.

LAUDON, Kenneth C.; LAUDON, Jane Price. Sistemas de Informação com Internet. Rio de JANEIRO: LTC – Livros Técnicos e Científicos S.A., 1998.

Lück, I., Vögel, S., and Krumm, H. (2002). Model-based con_guration of VPNs. In Stadtler, R. and Ulema, M., editors, Proc. 8th IEEE/IFIP Network Operations and Management Symposium NOMS 2002, pages 589.602, Florence, Italy. IEEE.

M. Lin and I.Wassell. Impact of channel sounder frequency offset on the estimation of channel parameters. In *IEEE Vehicular Technology Conference 2006 Fall*, September 2006.

M. Locasto, K. Wang, A. Keromytis, and S. Stolfo. FLIPS: Hybrid adaptive intrusion prevention. In *RAID*, 2005.

M. Rinard et al. A dynamic technique for eliminating buffer over-flow vulnerabilities (and other memory errors). In *ACSAC*, 2004.

MANION, A. Vulnerability Note VU#150227 – Multiple vendors' HTTP proxy default configurations allow arbitrary TCP conections. CERT Advisory, Pittsburgh, PA, Mai.2002.

Martim Carbone e Paulo de Geus. A mechanism for automatic digital evidence collection on high-interaction honeypots. Em Proceedings of the Fifth Annual IEEE Information Assurance Workshop, p´aginas 1–8, 2004.

Martin, C.; Abuosba, K.A. Utilizing a Service Oriented Architecture for Information Security Evaluation and Quantification Business-Driven IT Management, 2007. BDIM apos;07. 2nd IEEE/IFIP International Workshop on Volume , Issue , 21-21, Page(s): 114 - 115 May 2007.

MATOSO, Maria Cristina. *Orientações para apresentação de trabalhos acadêmicos*. 18ª edição. Campinas: PUC-Campinas, 2007.

MCCLURE, Stuar; SCAMBRAY, Joel; KURTZ, George - Hacking Exposed - 2a edition. McGraw Hill, 2000.

Mont, M., Baldwin, A., and Goh, C. (2000). POWER prototype: Towards integrated policy-based management. In Hong, J. and Weihmayer, R., editors, Proc. IEEE/IFIP Network Operations and Management Symposium (NOMS2000), pages 789.802, Hawaii, USA.

MOREIRA, Stringasci Nilton. Segurança da Informação: uma visão coorporativa da segurança de informações. Rio de Janeiro: Axcel Books, 2001.

O. Ruwase and M. Lam. A practical dynamic buffer overflow detector. In *NDSS*, 2004.

O.S. Saydjari, “Multilevel Security: Reprise,” IEEE Security & Privacy, vol. 2, no. 5, 2004, pp. 64–67.

PEIKARI, C.; CHUVAKIN, A. Security Warrior - Know Your Enemy. O’Reilly, 2004.

PETERSON, Larry L.; DAVIE, Bruce. S. Redes de Computadores: Uma Abordagem de Sistemas. RJ: Elsevier, 2004.

Piper, D. 1998. The internet IP security domain of interpretation for ISAKMP. RFC 2407.

Porto de Albuquerque, J. and de Geus, P. L. (2003). A framework for network security system design. WSEAS Transactions on Systems, 2:139.144.

Porto de Albuquerque, J., Krumm, H., and de Geus, P. L. (2005). Policy modeling and re_nement for network security systems. In IEEE 6th International Workshop on Policies for Distributed Systems and Networks, Stockholm, Sweden.

R. Sekar et al. A fast automaton-basedmethod for detecting anomalous program behaviors. In *IEEE S&P*, 2001.

R.T. Mercuri, “Computer Security: Quality Rather than Quantity,” Comm. ACM, vol. 45, no. 10, 2002, pp. 12–14.

Ramos, Fabio Furtado; NBR-ISO/IEC 17799: Benefícios e Aplicações; Março de 2002.

REZENDE, Denis Alcides; ABREU, Aline França. Tecnologia da informação aplicada a sistemas de informação empresariais : o papel estratégico da informação e dos sistemas de informação nas empresas. São Paulo: Atlas, 2001.

S. Bhatkar, D. DuVarney, and R. Sekar. Address obfuscation: An efficient approach to combat a broad range of memory error exploits. In *USENIX Security*, 2003.

S. Illner, A. Pohl, and H. Krumm. Security service adaptation for embedded service systems in changing environments. In Proceedings of the 2nd IEEE International Conference on Industrial Informatics (INDIN’04), pages 457–462, Berlin, Germany, 2004.

S. Sidiroglou and A. Keromytis. A network worm vaccine architecture. In *WETICE*, 2003.

S. Sidiroglou, M. Locasto, S. Boyd, and A. Keromytis. Building a reactive immune system for software services. In *USENIX Annual Technical Conference*, 2005.

S. T. Sarasamma, Q. A. Zhu, J. Huff, ”Hierarchical Kohonenen net for anomaly detection in network security”, IEEE Transactions on Systems, Man and Cybernetics, Part B, vol. 35, no. 2, 2005.

SEVERINO, Antônio Joaquim. *Metodologia do trabalho Científico*. 22ª edição. São Paulo: Cortez, 2002.

Sloman, M. and Lupu, E. C. (2002). Security and management policy speci_cation. IEEE Network, Special Issue on Policy-Based Networking, 16(2):10.19.

T. Chiueh and F. Hsu. RAD: A compile-time solution to buffer overflow attacks. In *ICDCS*, 2001.

T. Garfinkel, “Traps and pitfalls: Practical problems in system call interposition based security tools,” in *Proceedings of Network and Distributed System Security (NDSS 2003)*, (San Diego,CA), Feb. 2003.

T. Jim et al. Cyclone: a safe dialect of C. In *USENIX Annual Technical Conference*, 2002.

T. Toth and C. Kruegel. Accurate buffer overflow detection via abstract payload execution. In *RAID*, 2002.

TEIXEIRA, R. C. *O Pesadelo do SPAM*. News Generation, Rio de Janeiro, RJ, v.5, n.1, Jan.2001.

TMFORUM: TeleManagement Forum. GB921, enhanced Telecom Operations Map (eTOM). The business process framework for the information and communications services industry. Version 6.1, nov. 2005a. Disponível em: <http://www.tmforum.org/>. Acesso em: 21 out. 2006.

V. Yegneswaran, J. Giffin, P. Barford, and S. Jha. An architecture for generating semantics-aware signatures. In *USENIX Security*, 2005.

W. Lee, S. Stolfo, ”A Framework for constructing features and models for intrusion detection systems”, ACM Transactions on Information and System Security, vol. 3, no. 4, 2000.

W. Shi, H.-H. S. Lee, M. Ghosh, C. Lu, and A. Boldyreva. High efficiency counter mode security architecture via prediction and precomputation. In

*Proceedings of the 32nd Annual International Symposium on Computer Architecture (*ISCA*'05)*, pages 14–24. IEEE Computer Society, June 2005.

W. Xu, D. DuVarney, and R. Sekar. An efficient and backwardscompatible transformation to ensure memory safety of C programs. In *FSE*, 2004.

W. Yurcik, J. Barlow, K. Lakkaraju, and M. Haberman. Two visual computer network security monitoring tools incorporating operator interface requirements. In ACM CHI Workshop on Human-Computer Interaction and Security Systems (HCISEC), Fort Lauderdale, Florida, USA, April 2003.

Z. Liang, R. Sekar, and D. DuVarney. Immunizing servers from buffer-overflow attacks. Presentation in *ARCS Workshop*, 2004.

Z. Liang, R. Sekar, and D. DuVarney. Automatic synthesis of filters to discard buffer overflow attacks: A step towards realizing selfhealing systems. In *USENIX Annual Technical Conference*, (*Short Paper)* 2005.

Z. Liang and R. Sekar. Fast and automated generation of attack signatures: A basis for building self-protecting servers. In *CCS*, 2005.

Y. Tang and S. Chen. Defending against Internet worms: A signature-based approach. In *INFOCOM*, 2005.

9 Anexos

Anexo A – Regras Snort

Nesta seção apresentamos fragmentos das regras aplicadas no equipamento onde foi instalado o IDS (*Intrusion Detection System*), é importante lembrar que o desenvolvimento das regras é dinâmico, pois depende de estudos e acompanhamento das ameaças existentes e notícia de novas ameaças.

REGRAS IDS SNORT TECNICÓPIAS

1 # BACKDOOR RULES

alert tcp any 27374 -> any any (msg:"BACKDOOR subseven 22"; flow:to_server,established; content:"|0d0a5b52504c5d3030320d0a|"; reference:arachnids,485; reference:url,www.hackfix.org/subseven/; sid:103; rev:5;)

alert tcp any 16959 -> any any (msg:"BACKDOOR subseven DEFCON8 2.1 access"; flow:from_server,established; content:"PWD"; sid:107; rev:6;)

alert tcp any 12345:12346 -> any any (msg:"BACKDOOR netbus active"; flow:from_server,established; content:"NetBus"; reference:arachnids,401; sid:109; rev:4;)

alert tcp any any -> any 12345:12346 (msg:"BACKDOOR netbus getinfo"; flow:to_server,established; content:"GetInfo|0d|"; reference:arachnids,403; sid:110; rev:3;)

alert tcp any 20034 -> any any (msg:"BACKDOOR netbus active"; flow:to_server,established; content:"NetBus"; reference:arachnids,401; sid:115; rev:4;)

alert udp any any -> any 2140 (msg:"BACKDOOR DeepThroat 3.1 Connection attempt"; content:"00"; depth:2; sid:1980; rev:1;)

2 # SCAN RULES

alert tcp any 10101 -> any any (msg:"SCAN myscan"; stateless; ttl: >220; ack: 0; flags: S;reference:arachnids,439; sid:613; rev:2;)

alert tcp any any -> any 113 (msg:"SCAN ident version request"; flow:to_server,established; content: "VERSION|0A|"; depth: 16;reference:arachnids,303; sid:616; rev:3;)

alert tcp any any -> any 80 (msg:"SCAN cybercop os probe"; stateless; flags: SF12; dsize: 0; reference:arachnids,146; sid:619; rev:2;)

alert tcp any any -> any 3128 (msg:"SCAN Squid Proxy attempt"; stateless; flags:S,12; sid:618; rev:5;)

alert tcp any any -> any 1080 (msg:"SCAN SOCKS Proxy attempt"; stateless; flags:S,12; reference:url,help.undernet.org/proxyscan/; sid:615; rev:5;)

3 # FTP RULES

alert tcp any any -> any 21 (msg:"FTP CEL overflow attempt";flow:to_server,established; content:"CEL"; nocase; isdataat:100,relative; pcre:"/^CEL\s[^\n]{100}/smi"; reference:bugtraq,679; reference:cve,CVE-1999-0789; reference:arachnids,257; sid:337; rev:7;)

alert tcp any any -> any 21 (msg:"FTP XCWD overflow attempt"; flow:to_server,established; content:"XCWD"; nocase; isdataat:100,relative; pcre:"/^XCWD\s[^\n]{100}/smi"; reference:bugtraq,8704; sid:2344; rev:1;)

alert tcp any any -> any 21 (msg:"FTP CWD overflow attempt"; flow:to_server,established; content:"CWD"; nocase; isdataat:100,relative; pcre:"/^CWD\s[^\n]{100}/smi"; reference:cve,CAN-2000-1035; reference:cve,CAN-2000-1194; reference:cve,CAN-2002-0126; reference:bugtraq,7950; sid:1919; rev:6;)

4 # ICMP RULES e ICMP-INFO

alert icmp any any -> any any (msg:"ICMP ISS Pinger"; content:"|495353504e475251|";itype:8;depth:32; reference:arachnids,158; sid:465; rev:1;)

alert icmp any any -> any any (msg:"ICMP L3retriever Ping"; content: "ABCDEFGHIJKLMNOPQRSTUVWABCDEFGHI"; itype: 8; icode: 0; depth: 32; reference:arachnids,311; sid:466; rev:1;)

alert icmp any any -> any any (msg:"ICMP Nemesis v1.1 Echo"; dsize: 20; itype: 8; icmp_id: 0; icmp_seq: 0; content: "|00000000000000000000000000000000000000|"; reference:arachnids,449; sid:467; rev:1;)

alert icmp any any -> any any (msg:"ICMP PING NMAP"; dsize: 0; itype: 8; reference:arachnids,162; sid:469; rev:1;)

alert icmp any any -> any any (msg:"ICMP icmpenum v1.1.1"; id: 666; dsize: 0; itype: 8; icmp_id: 666 ; icmp_seq: 0; reference:arachnids,450; sid:471; rev:1;)

alert icmp any any -> any any (msg:"ICMP redirect host";itype:5;icode:1; reference:arachnids,135; reference:cve,CVE-1999-0265; sid:472; rev:1;)

alert icmp any any -> any any (msg:"ICMP redirect net";itype:5;icode:0; reference:arachnids,199; reference:cve,CVE-1999-0265; sid:473; rev:1;)

5 # DDOS RULES

alert icmp any any -> any any (msg:"DDOS TFN Probe"; id: 678; itype: 8; content: "1234";reference:arachnids,443; sid:221; rev:1;)

alert icmp any any -> any any (msg:"DDOS tfn2k icmp possible communication"; itype: 0; icmp_id: 0; content: "AAAAAAAAAA"; reference:arachnids,425; sid:222; rev:1;)

alert udp any any -> any 31335 (msg:"DDOS Trin00 Daemon to Master PONG message detected"; content:"PONG";reference:arachnids,187; sid:223; rev:2;)

alert icmp any any -> any any (msg:"DDOS TFN client command BE"; itype: 0; icmp_id: 456; icmp_seq: 0; reference:arachnids,184; sid:228; rev:1;)

alert tcp any any -> any 20432 (msg:"DDOS shaft client to handler"; flow:established; reference:arachnids,254; sid:230; rev:2;)

alert udp any any -> any 31335 (msg:"DDOS Trin00 Daemon to Master message detected"; content:"l44";reference:arachnids,186; sid:231; rev:2;)

6 # ATTACK RESPONSES

alert tcp any any -> any any (msg:"ATTACK-RESPONSES directory listing"; content: "Volume Serial Number"; flow:from_server,established; sid:1292; rev:7;)

alert tcp any any -> any any (msg:"ATTACK-RESPONSES command completed"; content:"Command completed"; nocase; flow:from_server,established; sid:494; rev:6;)

alert tcp any any -> any any (msg:"ATTACK-RESPONSES command error"; content:"Bad command or filename"; nocase; flow:from_server,established; sid:495; rev:6;)

alert tcp any any -> any any (msg:"ATTACK-RESPONSES file copied ok"; content:"1 file(s) copied"; nocase; flow:from_server,established; sid:497; rev:6;)

alert tcp any any -> any any (msg:"ATTACK-RESPONSES Invalid URL"; content:"Invalid URL"; nocase; flow:from_server,established; reference:url,www.microsoft.com/technet/security/bulletin/MS00-063.asp; sid:1200; rev:8;)

alert tcp any any -> any any (msg:"ATTACK-RESPONSES index of /cgi-bin/ response"; flow:from_server,established; content:"Index of /cgi-bin/"; nocase; reference:nessus,10039; sid:1666; rev:5;)

alert tcp any any -> any any (msg:"ATTACK-RESPONSES 403 Forbidden"; flow:from_server,established; content:"HTTP/1.1 403"; depth:12; sid:1201; rev:7;)

7 # BAD TRAFFIC RULES

alert tcp any any <> any 0 (msg:"BAD-TRAFFIC tcp port 0 traffic"; stateless; sid:524; rev:7;)

alert udp any any <> any 0 (msg:"BAD-TRAFFIC udp port 0 traffic"; reference:cve,CVE-1999-0675; reference:nessus,10074; sid:525; rev:5;)

alert tcp any any -> any any (msg:"BAD-TRAFFIC data in TCP SYN packet"; flags:S,12; dsize:>6; stateless; reference:url,www.cert.org/incident_notes/IN-99-07.html; sid:526; rev:7;)

alert ip any any <> 127.0.0.0/8 any (msg:"BAD-TRAFFIC loopback traffic"; reference:url,rr.sans.org/firewall/egress.php; sid:528; rev:4;)

alert ip any any -> any any (msg:"BAD-TRAFFIC same SRC/DST"; sameip; reference:cve,CVE-1999-0016; reference:url,www.cert.org/advisories/CA-1997-28.html; sid:527; rev:4;)

alert ip any any -> any any (msg:"BAD-TRAFFIC ip reserved bit set"; fragbits:R; sid:523; rev:4;)

alert ip any any -> any any (msg:"BAD-TRAFFIC 0 ttl"; ttl:0; reference:url,www.isi.edu/in-notes/rfc1122.txt; reference:url,support.microsoft.com/default.aspx?scid=kb\;EN-US\;q138268; sid:1321; rev:6;)

8 # TELNET RULES

alert tcp any any -> any 23 (msg:"TELNET Solaris memory mismanagement exploit attempt"; flow:to_server,established; content:"|A0 23 A0 10 AE 23 80 10 EE 23 BF EC 82 05 E0 D6 90 25 E0|"; sid:1430; rev:6;)

alert tcp any any -> any 23 (msg:"TELNET SGI telnetd format bug"; flow:to_server,established; content:"_RLD"; content:"bin/sh"; reference:arachnids,304; sid:711; rev:5;)

alert tcp any any -> any 23 (msg:"TELNET ld_library_path"; flow:to_server,established; content:"ld_library_path"; reference:cve,CVE-1999-0073; reference:arachnids,367; sid:712; rev:5;)

alert tcp any any -> any 23 (msg:"TELNET livingston DOS"; flow:to_server,established; content:"|fff3 fff3 fff3 fff3 fff3|"; rawbytes; reference:arachnids,370; sid:713; rev:6;)

alert tcp any any -> any 23 (msg:"TELNET resolv_host_conf"; flow:to_server,established; content:"resolv_host_conf"; reference:arachnids,369; sid:714; rev:4;)

alert tcp any 23 -> any any (msg:"TELNET Attempted SU from wrong group"; flow:from_server,established; content:"to su root"; nocase; sid:715; rev:6;)

alert tcp any 23 -> any any (msg:"TELNET not on console"; flow:from_server,established; content:"not on system console"; nocase; reference:arachnids,365; sid:717; rev:6;)

9 # SQL RULES

alert tcp any any -> any 139 (msg:"MS-SQL/SMB sp_start_job - program execution"; content: "s|00|p|00|_|00|s|00|t|00|a|00|r|00|t|00|_|00|j|00|o|00|b|00|"; nocase; flow:to_server,established; offset: 32; depth: 32; sid:676; rev:4;)

alert tcp any any -> any 139 (msg:"MS-SQL/SMB sp_password password change"; content: "s|00|p|00|_|00|p|00|a|00|s|00|s|00|w|00|o|00|r|00|d|00|"; nocase; flow:to_server,established; sid:677; rev:5;)

alert tcp any any -> any 139 (msg:"MS-SQL/SMB sp_delete_alert log file deletion"; content: "s|00|p|00|_|00|d|00|e|00|l|00|e|00|t|00|e|00|_|00|a|00|l|00|e|00|"; nocase; flow:to_server,established; sid:678; rev:5;)

alert tcp any any -> any 139 (msg:"MS-SQL/SMB sp_adduser database user creation"; content: "s|00|p|00|_|00|a|00|d|00|d|00|u|00|s|00|e|00|r|00|"; nocase; flow:to_server,established; offset:32; depth:32; sid:679; rev:4;)

alert tcp any any -> any 139 (msg:"MS-SQL/SMB xp_enumresultset possible buffer overflow"; content: "x|00|p|00|_|00|e|00|n|00|u|00|m|00|r|00|e|00|s|00|u|00|l|00|t|00|s|00|e|00|t|00|"; nocase; flow:to_server,established; offset:32; reference:bugtraq,2031; reference:cve,CAN-2000-1082; sid:708; rev:5;)

#10 # RPC RULES

alert tcp any any -> any 111 (msg:"RPC portmap proxy integer overflow attempt TCP"; flow:to_server,established; content:"|00 01 86 A0 00|"; offset:16; depth:5; content:"|00 00 00 05|"; distance:3; within:4; byte_jump:4,4,relative,align; byte_jump:4,4,relative,align; byte_test:4,>,2048,12,relative; reference:cve,CAN-2003-0028; reference:bugtraq,7123; content:"|00 00 00 00|"; offset:8; depth:4; sid:2093; rev:3;)

alert udp any any -> any 111 (msg:"RPC portmap proxy integer overflow attempt UDP"; content:"|00 01 86 A0 00|"; offset:12; depth:5; content:"|00 00 00 05|"; distance:3; within:4; byte_jump:4,4,relative,align; byte_jump:4,4,relative,align; byte_test:4,>,2048,12,relative; reference:cve,CAN-2003-0028; reference:bugtraq,7123; content:"|00 00 00 00|"; offset:4; depth:4; sid:2092; rev:3;)

alert tcp any any -> any 111 (msg:"RPC portmap proxy attempt TCP"; flow:to_server,established; content:"|00 01 86 A0|"; offset:16; depth:4; content:"|00 00 00 05|"; distance:4; within:4; content:"|00 00 00 00|"; offset:8; depth:4; sid:1922; rev:5;)

11 # P2P

alert tcp any any -> any 8888 (msg:"P2P napster login"; flow:to_server,established; content:"|00 0200|"; offset:1; depth:3; sid:549; rev:6;)

alert tcp any any -> any 8888 (msg:"P2P napster new user login"; flow:to_server,established; content:"|00 0600|"; offset:1; depth:3; sid:550; rev:6;)

alert tcp any any -> any 8888 (msg:"P2P napster download attempt"; flow:to_server,established; content:"|00 cb00|"; offset:1; depth:3; sid:551; rev:5;)

alert tcp any 8888 -> any any (msg:"P2P napster upload request"; flow:from_server,established; content:"|00 5f02|"; offset:1; depth:3; sid:552; rev:5;)

alert tcp any any -> any !80 (msg:"P2P GNUTella GET"; flow:to_server,established; content:"GET "; offset:0; depth:4; sid:1432; rev:4;)

12 # X11

alert udp any any -> any any (msg:"RPC ypserv maplist request UDP"; content:"|00 01 86 A4|"; offset:12; depth:4; content:"|00 00 00 0B|"; distance:4; within:4; reference:bugtraq,6016; reference:bugtraq,5914; reference:cve,CAN-2002-1232; content:"|00 00 00 00|"; offset:4; depth:4; sid:2033; rev:5;)

alert tcp any any -> any any (msg:"RPC ypserv maplist request TCP"; flow:to_server,established; content:"|00 01 86 A4|"; offset:16; depth:4; content:"|00 00 00 0B|"; distance:4; within:4; reference:bugtraq,6016; reference:bugtraq,5914; reference:Cve,CAN-2002-1232; content:"|00 00 00 00|"; offset:8; depth:4; sid:2034; rev:5;)

alert udp any any -> any 111 (msg:"RPC portmap network-status-monitor request UDP"; content:"|00 01 86 A0|"; offset:12; depth:4; content:"|00 00 00 03|"; distance:4; within:4; byte_jump:4,4,relative,align; byte_jump:4,4,relative,align; content:"|00 03 0D 70|"; within:4; content:"|00 00 00 00|"; offset:4; depth:4; sid:2035; rev:4;)

13 # WEB-IIS RULES

alert tcp any any -> any any (msg:"WEB-IIS MDAC Content-Type overflow attempt"; flow:to_server,established; uricontent:"/msadcs.dll"; content:"Content-Type\:"; content:!"|0A|"; within:50; reference:cve,CAN-2002-1142; reference:url,www.foundstone.com/knowledge/randd-advisories-display.html?id=337; sid:1970; rev:1;)

alert tcp any any -> any any (msg:"WEB-IIS repost.asp access"; flow:to_server,established; uricontent:"/scripts/repost.asp"; nocase; reference:nessus,10372; sid:1076; rev:6;)

alert tcp any any -> any any (msg:"WEB-IIS .htr chunked Transfer-Encoding"; flow:to_server,established; uricontent:".htr"; nocase; content:"Transfer-Encoding\:"; nocase; content:"chunked"; nocase; reference:bugtraq,5003; reference:cve,CAN-2002-0364; sid:1806; rev:2;)

alert tcp any any -> any any (msg:"WEB-IIS .asp chunked Transfer-Encoding"; flow:to_server,established; uricontent:".asp"; nocase; content:"Transfer-

14 # WEB-CLIENT RULES

alert tcp any any -> any any (msg:"WEB-CLIENT Outlook EML access"; uricontent:".eml"; flow:from_client,established; sid:1233; rev:8;)

alert tcp any any -> any any (msg:"WEB-CLIENT readme.eml download attempt"; flow:from_client,established; uricontent:"/readme.eml"; nocase; sid:1284; reference:url,www.cert.org/advisories/CA-2001-26.html; rev:9;)

alert tcp any any -> any any (msg:"WEB-CLIENT readme.eml autoload attempt"; flow:to_client,established; content:"window.open(\"readme.eml\""; nocase; sid:1290; reference:url,www.cert.org/advisories/CA-2001-26.html; rev:8;)

alert tcp any any -> any any (msg:"WEB-CLIENT Javascript document.domain attempt"; flow:to_client,established; content:"document.domain("; nocase; reference:bugtraq,5346; sid:1840; rev:3;)

alert tcp any any -> any any (msg:"WEB-CLIENT Javascript URL host spoofing attempt"; flow:to_client,established; content:"javascript\://"; nocase; reference:bugtraq,5293; sid:1841; rev:3;)

15 # WEB-CGI RULES

alert tcp any any -> any any (msg:"WEB-CGI HyperSeek hsx.cgi directory traversal attempt"; uricontent:"/hsx.cgi"; content:"../../"; content:"%00"; distance:1; flow:to_server,established; reference:bugtraq,2314; reference:cve,CAN-2001-0253; sid:803; rev:7;)

alert tcp any any -> any any (msg:"WEB-CGI HyperSeek hsx.cgi access"; uricontent:"/hsx.cgi"; flow:to_server,established; reference:bugtraq,2314; reference:cve,CAN-2001-0253; sid:1607; rev:3;)

alert tcp any any -> any any (msg:"WEB-CGI SWSoft ASPSeek Overflow attempt"; flow:to_server,established; uricontent:"/s.cgi"; nocase; content:"tmpl="; reference:cve,CAN-2001-0476; reference:bugtraq,2492; sid:804; rev:7;)

17 # NETBIOS RULES

alert tcp any any -> any 139 (msg:"NETBIOS nimda .eml"; content:"|00|.|00|E|00|M|00|L"; flow:to_server,established; reference:url,www.f-secure.com/v-descs/nimda.shtml; sid:1293; rev:8;)

alert tcp any any -> any 139 (msg:"NETBIOS nimda .nws"; content:"|00|.|00|N|00|W|00|S"; flow:to_server,established; reference:url,www.f-secure.com/v-descs/nimda.shtml; sid:1294; rev:8;)

alert tcp any any -> any 139 (msg:"NETBIOS nimda RICHED20.DLL"; content:"R|00|I|00|C|00|H|00|E|00|D|00|2|00|0"; flow:to_server,established; reference:url,www.f-secure.com/v-descs/nimda.shtml; sid:1295; rev:7;)

alert tcp any any -> any 139 (msg:"NETBIOS DOS RFPoison"; flow:to_server,established; content: "|5C 00 5C 00 2A 00 53 00 4D 00 42 00 53 00 45 00 52 00 56 00 45 00 52 00 00 00 00 00 01 00 00 00 01 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00|";reference:arachnids,454; sid:529; rev:5;)

Anexo B – Regras Firewall

Nesta seção apresentamos o script que contém as regras aplicadas no equipamento de *Firewall*.

```
# REGRAS FIREWALL TECNICÓPIAS
#########################################################################
# Local Settings
SYSCTL="/sbin/sysctl -w"
IPT="/sbin/iptables"
IPTS="/sbin/iptables-save"
IPTR="/sbin/iptables-restore"
# Internet Interface
INET_IFACE="eth0"
INET_ADDRESS="200.204.62.203"
# Local Interface Information
LOCAL_IFACE="eth1"
LOCAL_IP="192.168.1.1"
LOCAL_NET="192.168.1.0/24"
LOCAL_BCAST="192.168.1.255"
# Localhost Interface
LO_IFACE="lo"
LO_IP="127.0.0.1"
# Save and Restore arguments handled here
if [ "$1" = "save" ]
then
        echo -n "Saving firewall to /etc/sysconfig/iptables ... "
```

```
        $IPTS > /etc/sysconfig/iptables
        echo "done"
        exit 0
elif [ "$1" = "restore" ]
then
        echo -n "Restoring firewall from /etc/sysconfig/iptables ... "
        $IPTR < /etc/sysconfig/iptables
        echo "done"
        exit 0
fi

########################################################################
# Load Modules
echo "Loading kernel modules ..."
# core netfilter module
/sbin/modprobe ip_tables
# the stateful connection tracking module
/sbin/modprobe ip_conntrack
# The ftp nat module is required for non-PASV ftp support
/sbin/modprobe ip_nat_ftp
# the module for full ftp connection tracking
/sbin/modprobe ip_conntrack_ftp
# the module for full irc connection tracking
/sbin/modprobe ip_conntrack_irc

########################################################################
```

```
# Kernel Parameter Configuration

# Alternatively, it can be set in /etc/sysctl.conf
if [ "$SYSCTL" = "" ]
then
    echo "1" > /proc/sys/net/ipv4/ip_forward
else
    $SYSCTL net.ipv4.ip_forward="1"
fi
if [ "$SYSCTL" = "" ]
then
    echo "1" > /proc/sys/net/ipv4/tcp_syncookies
else
    $SYSCTL net.ipv4.tcp_syncookies="1"
fi
if [ "$SYSCTL" = "" ]
then
    echo "1" > /proc/sys/net/ipv4/conf/all/rp_filter
else
    $SYSCTL net.ipv4.conf.all.rp_filter="1"
fi
if [ "$SYSCTL" = "" ]
then
    echo "1" > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts
else
    $SYSCTL net.ipv4.icmp_echo_ignore_broadcasts="1"
```

```
fi
if [ "$SYSCTL" = "" ]
then
    echo "0" > /proc/sys/net/ipv4/conf/all/accept_source_route
else
    $SYSCTL net.ipv4.conf.all.accept_source_route="0"
fi
# This option accepts only from gateways in the default gateways list.
if [ "$SYSCTL" = "" ]
then
    echo "1" > /proc/sys/net/ipv4/conf/all/secure_redirects
else
    $SYSCTL net.ipv4.conf.all.secure_redirects="1"
fi
# This option logs packets from impossible addresses.
if [ "$SYSCTL" = "" ]
then
    echo "1" > /proc/sys/net/ipv4/conf/all/log_martians
else
    $SYSCTL net.ipv4.conf.all.log_martians="1"
fi

#########################################################################
# Flush Any Existing Rules or Chains
echo "Flushing Tables ..."
# Reset Default Policies
```

```
$IPT -P INPUT ACCEPT
$IPT -P FORWARD ACCEPT
$IPT -P OUTPUT ACCEPT
$IPT -t nat -P PREROUTING ACCEPT
$IPT -t nat -P POSTROUTING ACCEPT
$IPT -t nat -P OUTPUT ACCEPT
$IPT -t mangle -P PREROUTING ACCEPT
$IPT -t mangle -P OUTPUT ACCEPT
# Flush all rules
$IPT -F
$IPT -t nat -F
$IPT -t mangle -F
# Erase all non-default chains
$IPT -X
$IPT -t nat -X
$IPT -t mangle -X
if [ "$1" = "stop" ]
then
        echo "Firewall completely flushed!  Now running with no firewall."
        exit 0
fi

########################################################################
# Rules Configuration

########################################################################
```

```
# Filter Table

##############################################################################
# Set Policies
$IPT -P INPUT DROP
$IPT -P OUTPUT DROP
$IPT -P FORWARD DROP

##############################################################################
# User-Specified Chains
# Create user chains to reduce the number of rules each packet
# must traverse.
echo "Create and populate custom rule chains ..."
# Create a chain to filter INVALID packets
$IPT -N bad_packets
# Create another chain to filter bad tcp packets
$IPT -N bad_tcp_packets
# Create separate chains for icmp, tcp (incoming and outgoing),
# and incoming udp packets.
$IPT -N icmp_packets
# Used for UDP packets inbound from the Internet
$IPT -N udp_inbound
# Used to block outbound UDP services from internal network
# Default to allow all
$IPT -N udp_outbound
# Used to allow inbound services if desired
```

```
# Default fail except for established sessions
$IPT -N tcp_inbound
# Used to block outbound services from internal network
# Default to allow all
$IPT -N tcp_outbound

#####################################################################
# Populate User Chains
# bad_packets chain
# Drop packets received on the external interface
# claiming a source of the local network
$IPT -A bad_packets -p ALL -i $INET_IFACE -s $LOCAL_NET -j LOG \
   --log-prefix "fp=bad_packets:2 a=DROP "
$IPT -A bad_packets -p ALL -i $INET_IFACE -s $LOCAL_NET -j DROP
# Drop INVALID packets immediately
$IPT -A bad_packets -p ALL -m state --state INVALID -j LOG \
   --log-prefix "fp=bad_packets:1 a=DROP "
$IPT -A bad_packets -p ALL -m state --state INVALID -j DROP
# Then check the tcp packets for additional problems
$IPT -A bad_packets -p tcp -j bad_tcp_packets
# All good, so return
$IPT -A bad_packets -p ALL -j RETURN
# bad_tcp_packets chain
# All tcp packets will traverse this chain.
# Every new connection attempt should begin with
# a syn packet.  If it doesn't, it is likely a
```

```
# port scan.  This drops packets in state
# network.
$IPT -A bad_tcp_packets -p tcp -i $LOCAL_IFACE -j RETURN
$IPT -A bad_tcp_packets -p tcp ! --syn -m state --state NEW -j LOG \
   --log-prefix "fp=bad_tcp_packets:1 a=DROP "
$IPT -A bad_tcp_packets -p tcp ! --syn -m state --state NEW -j DROP
$IPT -A bad_tcp_packets -p tcp --tcp-flags ALL NONE -j LOG \
   --log-prefix "fp=bad_tcp_packets:2 a=DROP "
$IPT -A bad_tcp_packets -p tcp --tcp-flags ALL NONE -j DROP
$IPT -A bad_tcp_packets -p tcp --tcp-flags ALL ALL -j LOG \
   --log-prefix "fp=bad_tcp_packets:3 a=DROP "
$IPT -A bad_tcp_packets -p tcp --tcp-flags ALL ALL -j DROP
$IPT -A bad_tcp_packets -p tcp --tcp-flags ALL FIN,URG,PSH -j LOG \
   --log-prefix "fp=bad_tcp_packets:4 a=DROP "
$IPT -A bad_tcp_packets -p tcp --tcp-flags ALL FIN,URG,PSH -j DROP
$IPT -A bad_tcp_packets -p tcp --tcp-flags ALL SYN,RST,ACK,FIN,URG -j LOG \
   --log-prefix "fp=bad_tcp_packets:5 a=DROP "
$IPT -A bad_tcp_packets -p tcp --tcp-flags ALL SYN,RST,ACK,FIN,URG -j DROP
$IPT -A bad_tcp_packets -p tcp --tcp-flags SYN,RST SYN,RST -j LOG \
   --log-prefix "fp=bad_tcp_packets:6 a=DROP "
$IPT -A bad_tcp_packets -p tcp --tcp-flags SYN,RST SYN,RST -j DROP

$IPT -A bad_tcp_packets -p tcp --tcp-flags SYN,FIN SYN,FIN -j LOG \
   --log-prefix "fp=bad_tcp_packets:7 a=DROP "
$IPT -A bad_tcp_packets -p tcp --tcp-flags SYN,FIN SYN,FIN -j DROP
# All good, so return
```

```
$IPT -A bad_tcp_packets -p tcp -j RETURN
# icmp_packets chain
# of a denial of service attack.
$IPT -A icmp_packets --fragment -p ICMP -j LOG \
    --log-prefix "fp=icmp_packets:1 a=DROP "
$IPT -A icmp_packets --fragment -p ICMP -j DROP
# Echo - uncomment to allow your system to be pinged.
# Uncomment the LOG command if you also want to log PING attempts
# $IPT -A icmp_packets -p ICMP -s 0/0 --icmp-type 8 -j LOG \
#    --log-prefix "fp=icmp_packets:2 a=ACCEPT "
# $IPT -A icmp_packets -p ICMP -s 0/0 --icmp-type 8 -j ACCEPT
# By default, however, drop pings without logging. Blaster
# and other worms have infected systems blasting pings.
# Comment the line below if you want pings logged, but it
# will likely fill your logs.
$IPT -A icmp_packets -p ICMP -s 0/0 --icmp-type 8 -j DROP
# Time Exceeded
$IPT -A icmp_packets -p ICMP -s 0/0 --icmp-type 11 -j ACCEPT
# Not matched, so return so it will be logged
$IPT -A icmp_packets -p ICMP -j RETURN
# TCP & UDP
# chatter from Windows systems.
$IPT -A udp_inbound -p UDP -s 0/0 --destination-port 137 -j DROP
$IPT -A udp_inbound -p UDP -s 0/0 --destination-port 138 -j DROP
# Not matched, so return for logging
$IPT -A udp_inbound -p UDP -j RETURN
```

```
# No match, so ACCEPT
$IPT -A udp_outbound -p UDP -s 0/0 -j ACCEPT
# tcp_inbound chain
# This chain is used to allow inbound connections to the
# system/gateway.  Use with care.  It defaults to none.
# It's applied on INPUT from the external or Internet interface.
# Not matched, so return so it will be logged
$IPT -A tcp_inbound -p TCP -j RETURN
# tcp_outbound chain
#
# This chain is used with a private network to prevent forwarding for
# requests on specific protocols.  Applied to the FORWARD rule from
# the internal network.  Ends with an ACCEPT
# No match, so ACCEPT
$IPT -A tcp_outbound -p TCP -s 0/0 -j ACCEPT

##########################################################################
# INPUT Chain
echo "Process INPUT chain ..."
# Allow all on localhost interface
$IPT -A INPUT -p ALL -i $LO_IFACE -j ACCEPT
# Drop bad packets
$IPT -A INPUT -p ALL -j bad_packets
# Drop them without logging.
$IPT -A INPUT -p ALL -d 224.0.0.1 -j DROP
# Rules for the private network (accessing gateway system itself)
```

```
$IPT -A INPUT -p ALL -i $LOCAL_IFACE -s $LOCAL_NET -j ACCEPT
$IPT -A INPUT -p ALL -i $LOCAL_IFACE -d $LOCAL_BCAST -j ACCEPT
# Allow DHCP client request packets inbound from internal network
$IPT -A INPUT -p UDP -i $LOCAL_IFACE --source-port 68 --destination-port 67 \
    -j ACCEPT
# Inbound Internet Packet Rules
# Accept Established Connections
$IPT -A INPUT -p ALL -i $INET_IFACE -m state --state ESTABLISHED,RELATED
\
    -j ACCEPT
# Route the rest to the appropriate user chain
$IPT -A INPUT -p TCP -i $INET_IFACE -j tcp_inbound
$IPT -A INPUT -p UDP -i $INET_IFACE -j udp_inbound
$IPT -A INPUT -p ICMP -i $INET_IFACE -j icmp_packets
# Drop without logging broadcasts that get this far.
# broadcast protocols.
$IPT -A INPUT -m pkttype --pkt-type broadcast -j DROP
# Log packets that still don't match
$IPT -A INPUT -j LOG --log-prefix "fp=INPUT:99 a=DROP "

#####################################################################
# FORWARD Chain
echo "Process FORWARD chain ..."
# Used if forwarding for a private network
# Drop bad packets
$IPT -A FORWARD -p ALL -j bad_packets
```

```
# Accept TCP packets we want to forward from internal sources
$IPT -A FORWARD -p tcp -i $LOCAL_IFACE -j tcp_outbound
# Accept UDP packets we want to forward from internal sources
$IPT -A FORWARD -p udp -i $LOCAL_IFACE -j udp_outbound
# If not blocked, accept any other packets from the internal interface
$IPT -A FORWARD -p ALL -i $LOCAL_IFACE -j ACCEPT
# Deal with responses from the internet
$IPT -A FORWARD -i $INET_IFACE -m state --state ESTABLISHED,RELATED \
    -j ACCEPT
# Log packets that still don't match
$IPT -A FORWARD -j LOG --log-prefix "fp=FORWARD:99 a=DROP "

#####################################################################
# OUTPUT Chain
echo "Process OUTPUT chain ..."
# Generally trust the firewall on output
# However, invalid icmp packets need to be dropped
# to prevent a possible exploit.
$IPT -A OUTPUT -m state -p icmp --state INVALID -j DROP
# Localhost
$IPT -A OUTPUT -p ALL -s $LO_IP -j ACCEPT
$IPT -A OUTPUT -p ALL -o $LO_IFACE -j ACCEPT
# To internal network
$IPT -A OUTPUT -p ALL -s $LOCAL_IP -j ACCEPT
$IPT -A OUTPUT -p ALL -o $LOCAL_IFACE -j ACCEPT
# To internet
```

```
$IPT -A OUTPUT -p ALL -o $INET_IFACE -j ACCEPT
# Log packets that still don't match
$IPT -A OUTPUT -j LOG --log-prefix "fp=OUTPUT:99 a=DROP "

##################################################################
# nat table
echo "Load rules for nat table ..."

##################################################################
# PREROUTING chain

##################################################################
# POSTROUTING chain
$IPT -t nat -A POSTROUTING -o $INET_IFACE \
    -j SNAT --to-source $INET_ADDRESS

##################################################################
# mangle table
##################################################################
echo "Load rules for mangle table ..."
```

Anexo C – Regras Proxy

Nesta seção apresentamos o script que contém as regras aplicadas no equipamento de *Proxy*.

```
# REGRAS PROXY SQUID TECNICÓPIAS

### SEGURANCA
htcp_port 0
icp_port 0
http_port 192.168.0.1:3128
log_fqdn on
ftp_passive on

### GERAL
error_directory /var/www/squid
cachemgr_passwd admin all

# tempo de espera para fechar
shutdown_lifetime 10 seconds

# e-mail do admin
cache_mgr hostmaster@email.com.br

### TUNNING
cache_dir ufs /var/spool/squid 64 8 128
cache_mem 32 mb
logfile_rotate 1
coredump_dir /var/spool/squid
visible_hostname gw
cache_store_log none


## Tempo de espera apos cliente conectar, mandar pedido
```

```
request_timeout 15 seconds

##AUTENTICACAO
auth_param ntlm program /usr/bin/ntlm_auth --helper-protocol=squid-2.5-ntlmssp
auth_param ntlm children 35
auth_param ntlm max_challenge_reuses 5
auth_param ntlm max_challenge_lifetime 5 minutes
auth_param ntlm use_ntlm_negotiate on
auth_param basic program /usr/bin/ntlm_auth --helper-protocol=squid-2.5-basic
auth_param basic children 15
auth_param basic realm Squid proxy-caching web server
auth_param basic credentialsttl 2 hours

### ACLS
# rede
acl ftp proto ftp
acl max_conn maxconn 30
acl autenticacao proxy_auth REQUIRED
acl pdf url_regex -i \.pdf$
acl zip url_regex -i \.zip$

acl dominios_download dstdomain "/etc/squid/dominios_download.txt"
acl horario_lib src "/etc/squid/filtros/horario/liberado.txt"
acl maquinas_proibidas src "/etc/squid/maquinas_proibidas.txt"
acl maquinas_restritas src "/etc/squid/maquinas_restritas.txt"
acl maquinas_liberadas src "/etc/squid/maquinas_liberadas.txt"
acl sites_permitidos dstdomain "/etc/squid/sites_permitidos.txt"
acl wupdate dstdomain "/etc/squid/wupdate.txt"
acl msn url_regex "/etc/squid/msn.txt"
acl all src 0.0.0.0/0.0.0.0
acl rede src 192.168.0.0/24
acl intranet dst 192.168.0.0/24
acl localhost src 127.0.0.1/255.255.255.255
acl SSL_ports port 443
```

```
acl SSL_ports port 80
acl Safe_ports port 80
acl Safe_ports port 20
acl Safe_ports port 21
acl Safe_ports port 443
acl Safe_ports port 8080
acl manager proto cache_object
acl mundo dst 0.0.0.0/0.0.0.0

# segunda, terca, quarta, quinta e sexta das 7 as 20
acl horario_comercial time MTWHF 07:00-20:00
acl horario_prepress time MTWHF 06:00-22:00

# sabado das 7 as 12
acl horario_sabado time A 07:00-12:00

# connect para SSL
acl CONNECT method CONNECT

### REGRAS
no_cache deny mundo

# localhost liberado
http_access allow localhost

# manager liberado somente para localhost
http_access allow manager localhost
http_access deny manager

# intranet nada de cache
# interno, sem restricoes de horario e porta, e etc
# libera acesso aos icones do squid
always_direct allow rede intranet
http_access allow rede intranet
```

```
# limita todos ao maximo de conexoes
http_access deny rede max_conn

# Windows update
http_access allow wupdate

# liberar symantec update
acl symantec_update dstdomain liveupdate.symanteclive update.com
http_access allow symantec_update

# maquinas sem internet
http_access deny maquinas_proibidas

# sites permitidos
http_access allow rede sites_permitidos

# maquinas restrita apenas acessam sites permitidos
deny_info ERR_MAQ_RESTRITAS maquinas_restritas
http_access deny maquinas_restritas

# se eu nao tenho restricoes, liberado
http_access allow maquinas_liberadas autenticacao

# bloquear msn
http_access deny msn

# proibir que for diferente das portas liberadas
http_access deny CONNECT !SSL_ports autenticacao
http_access deny !Safe_ports autenticacao

# rede local e no horario de sabado, liberado
http_access allow rede horario_sabado autenticacao
```

```
# os demais negado
http_access deny all
icp_access deny all
http_reply_access allow all

## Restricoes de tamanho de resposta (download)
reply_body_max_size 0 allow zip all
reply_body_max_size 0 allow pdf all
reply_body_max_size 0 allow ftp all
reply_body_max_size 0 allow wupdate all
reply_body_max_size 0 allow dominios_download all
reply_body_max_size 0 allow sites_permitidos all
reply_body_max_size 2048000 allow all !maquinas_liberadas !horario_lib
```

Anexo D – Critérios aplicados na escolha de ferramentas de segurança.

Quadro 7: Critérios aplicados na escolha de *Software* Backup.

Critério	Backup Exec	SOS Backup	Turbo Backup
Preço	R$ 2.000,00	R$ 2.200,00	R$ 2450,00
Sistemas Operacionais Suportados	Windows	Windows	Windows
Compactação de Arquivos	Sim	Sim	Não
Uso Corporativo	Sim	Sim	Sim
Agendamento de Backup	Sim	Sim	Sim
Envio Informações E-mail	Sim	Não	Não
Backup Password protection	Sim	Sim	Sim
Verificação de Backup	Sim	Sim	Não

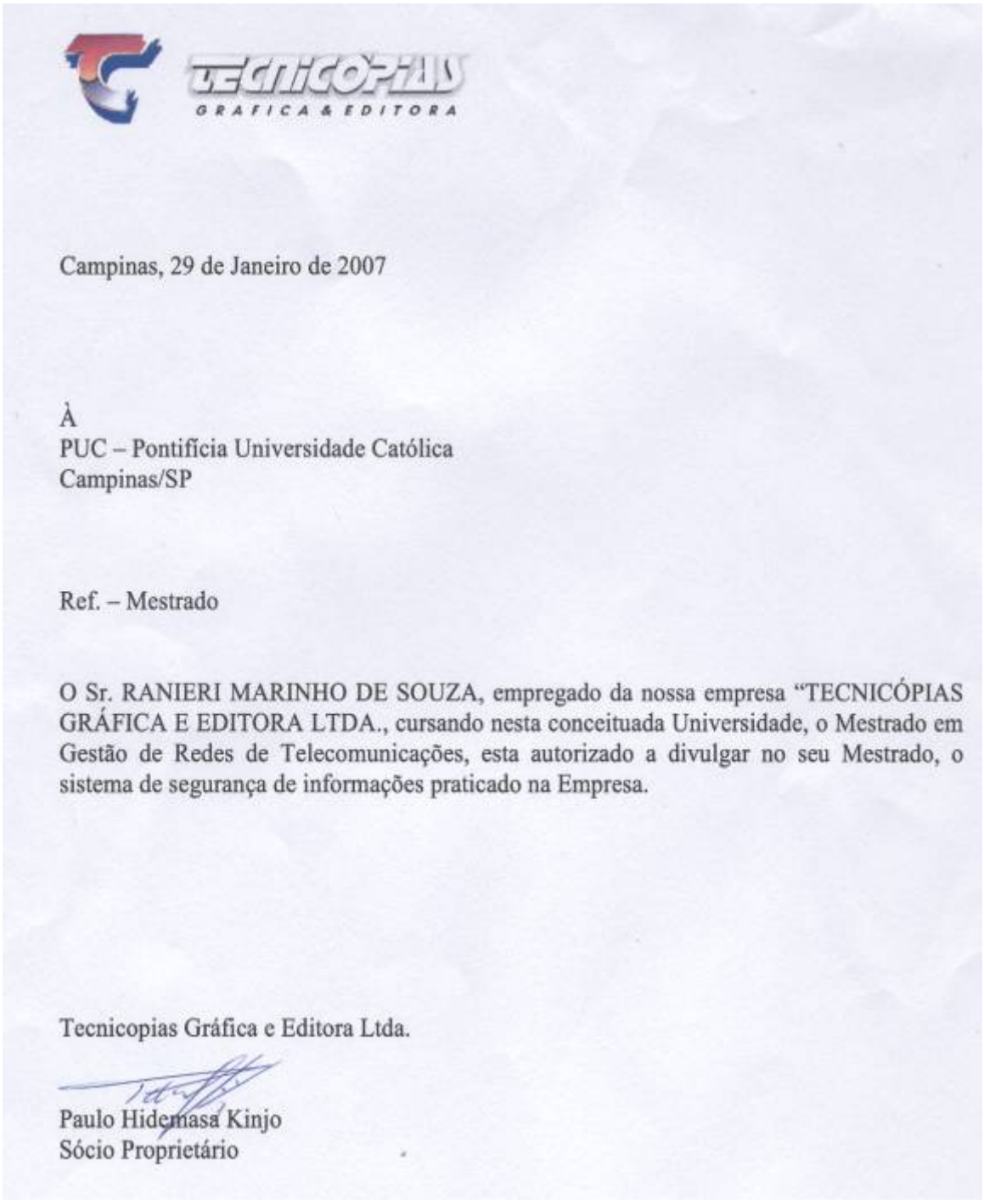
Fonte: Fonte: Tecnicópias Gráfica e Editora LTDA.

Quadro 8: Critérios aplicados na escolha de *Software* IDS.

Critério	Snort	Windows ISA
Preço	Gratuíto	R$ 5.000,00
Número de Equipamentos	Acima de 255	Acima 255
Sistemas Operacionais Suportados	Windows/Linux/Unix	Windows
Uso Corporativo	Sim	Sim
Portas Detectadas	65550	65550
Envio Informações E-mail	Sim	Sim

Fonte: Fonte: Tecnicópias Gráfica e Editora LTDA.

Anexo E – Documento autorização da Tecnicópias Gráfica e Editora Ltda para realização da pesquisa.



TECNICÓPIAS
GRAFICA & EDITORA

Campinas, 29 de Janeiro de 2007

À
PUC – Pontifícia Universidade Católica
Campinas/SP

Ref. – Mestrado

O Sr. RANIERI MARINHO DE SOUZA, empregado da nossa empresa "TECNICÓPIAS GRÁFICA E EDITORA LTDA., cursando nesta conceituada Universidade, o Mestrado em Gestão de Redes de Telecomunicações, esta autorizado a divulgar no seu Mestrado, o sistema de segurança de informações praticado na Empresa.

Tecnicopias Gráfica e Editora Ltda.

Paulo Hidemasa Kinjo
Sócio Proprietário