JÚLIO CÉSAR GONÇALVES

# O GERENCIAMENTO DA INFORMAÇÃO E SUA SEGURANÇA CONTRA ATAQUES DE VÍRUS DE COMPUTADOR RECEBIDOS POR MEIO DE CORREIO ELETRÔNICO

TAUBATÉ - SP

2002

**JÚLIO CÉSAR GONÇALVES**

# O GERENCIAMENTO DA INFORMAÇÃO E SUA SEGURANÇA CONTRA ATAQUES DE VÍRUS DE COMPUTADOR RECEBIDOS POR MEIO DE CORREIO ELETRÔNICO

**Dissertação apresentada para obtenção do Certificado de Título de Mestre em Administração de Empresas pelo Curso de Administração de Empresas do Departamento de Economia, Administração, Contabilidade e Secretariado Executivo da Universidade de Taubaté - UNITAU.**

**Área de Concentração: Gestão Empresarial**

**Orientador: Prof. Dr. Marco Antonio Chamon**

**TAUBATÉ – SP**

**2002**

Gonçalves, Júlio César
O Gerenciamento da Informação e sua Segurança contra ataques de vírus de computador recebidos por meio de correio eletrônico / Júlio César Gonçalves. Taubaté / SP:UNITAU/Faculdade de Economia, Contabilidade e Administração 2002.
339 p.: il.

Dissertação(Mestrado) – Universidade de Taubaté, Faculdade de Economia, Contabilidade e Administração, 2002.
Bibliografia.

1. Sistemas de Informação. 2. Política de Segurança 3. Vírus de Computador 4.Criptografia I.Dissertação (Mestrado) – Faculdade de Economia, Contabilidade e Administração. II.Título.

CDD 658.4038

**JÚLIO CÉSAR GONÇALVES**

**O GERENCIAMENTO DA INFORMAÇÃO E SUA SEGURANÇA CONTRA ATAQUES DE VÍRUS DE COMPUTADOR RECEBIDOS POR MEIO DE CORREIO ELETRÔNICO**

**UNIVERSIDADE DE TAUBATÉ, TAUBATÉ, SP**

**DATA: 25 / 05 / 2002.**

**RESULTADO: Aprovado com Distinção**

**COMISSÃO JULGADORA**

| | |
|---|---|
| **Prof. Dr. Edison Oliveira de Jesus, Ph D** | **UNIFEI** |
| **Prof. Dr. José Alberto Fernandes Ferreira** | **UNITAU** |
| **Prof. Dr. Marco Antonio Chamon** | **UNITAU** |

Dedico este trabalho a minha esposa **RITA**, ao meu filho **IGOR** e demais **FAMILIARES**, que muito me apoiaram durante todo o tempo de dedicação ao Mestrado. Dedico também, em particular, ao cãozinho "**SCOTT**" –- pertencente ao meu filho –- e que foi um companheiro inseparável de tantas noites e madrugadas de trabalho "ao pé do microcomputador".

Aos meus amados pais, **JÚLIO** e **ODÍLIA**, e a minha irmã **LÚCIA**, raízes profundas e alicerce da minha perseverança e personalidade.

**AGRADECIMENTOS**

A **Deus** pela saúde, oportunidade e condições para cursar o Mestrado.

A **Universidade de Taubaté – UNITAU**, aos **Departamentos de Informática** e **PRPPG**, pelo apoio recebido e pela bolsa de estudos, a mim concedida, sem a qual certamente eu não estaria aqui.

Ao amigo e **Prof. Dr. Marco Antonio Chamon,** pelo compromisso, comprometimento, empenho, habilidade e dedicação com que orientou meu trabalho.

Ao **Prof. Dr. Francisco C. L. de Melo**, pelo apoio, interesse e incentivo recebido quando da exposição da primeira idéia do tema.

Ao **Prof. Dr. José Luiz Gomes da Silva**, pelo incentivo e apoio recebido quanto ao esclarecimento da atual importância do assunto abordado por este trabalho às organizações.

Aos **Profs. Doutores da primeira turma do curso do MAE** – Mestrado em Administração de Empresas da UNITAU, principalmente ao seu coordenador, o **Professor Doutor Edson Aparecida de Araújo Querido Oliveira**, pela experiência,

disciplina, pelos conhecimentos transmitidos, pela presença constante, apoio e orientação nos momentos decisivos.

A **Prof. Dra. Maria Julia Xavier Ribeiro** pelo apoio, compreensão, presença constante e orientação em momentos ímpares.

Ao **Prof. Acácio de Toledo Netto**, que na ocasião do início deste trabalho era o Chefe do Departamento de Informática da Universidade de Taubaté, pelo apoio, compreensão, presença e colaboração.

A empresa em estudo, que optou por ficar anônima, local onde nasceu a primeira idéia da criação deste trabalho e pelo apoio técnico recebido.

Aos **colegas** e companheiros de estudo do curso do **MAE01**, em especial ao **André Yamada, Élcio Sotkeviciene, João Freitas e Robson Lourenço**, colegas, amigos, companheiros e irmãos pelas valiosas críticas e sugestões.

A **Alda Aparecida dos Santos**, Secretária do PPGAE, pelo apoio e presença constante em todos assuntos administrativos do MAE.

E a **todos** aqueles que, direta ou indiretamente, contribuíram para a realização deste trabalho.

GONÇALVES, J.C. *O Gerenciamento da Informação e sua Segurança contra ataques de vírus de computador recebidos por meio de correio eletrônico*. 2002. 339p. Dissertação (Mestrado em Administração de Empresas) – Departamento de Economia, Administração, Contabilidade e Secretariado, Universidade de Taubaté, Taubaté.

Esta pesquisa sobre a Informação e a Segurança da Informação, efetua um estudo do conceito Informação e as suas aplicações nas organizações, refletindo sobre tópicos como estratégia, sistemas de informação e a importância para a competitividade frente ao mercado empresarial, evidenciando a fragilidade da informação existente nas corporações — armazenada nos servidores de dados dos Centros de Informática — e vulneráveis a ataques de vírus de computador que possam ter como meio de transmissão o correio eletrônico. O objetivo deste trabalho é propor a implementação de uma Política de Segurança da Informação em uma indústria, dando ênfase à proteção contra ataques de vírus recebidos por meio do correio eletrônico. Este é um problema crítico e de grandes proporções, que pode gerar grandes prejuízos às organizações e empresas em geral. A Política de Segurança procura evidenciar meios e diretrizes que possam prover uma informação confiável, segura e que contribua positivamente no processo da tomada de decisões. Esta dissertação tende a avaliar como as corporações estão enfrentando o problema da segurança da informação contra vírus do correio eletrônico, como os dirigentes têm conduzido a preocupação com a perda, integridade e a destruição dos dados armazenados, a enumerar os principais meios e implementações tecnológicas para se minimizar os riscos com a falta de segurança destes dados e evidenciar a importância da implementação desta Política, com o intuito de prover recursos, tecnologia e informação confiável ao negócio.

GONÇALVES, J.C. *The Administration of the Information and its Safety against attacks of computer virus received from the electronic mail.* 2002. 339p. Dissertation (Master's degree in Administration of Companies) - Department of Economics, Administration, Accounting and Executive Secretary, University of Taubaté, Taubaté.

This research, on the Information and the Information Safety, makes a study of the concept Information and its applications, initially in the organizations, reflecting about

topics as strategy, information systems and the importance for the competitiveness to the business market, pointing out the fragility of the existent information in the corporations --- stored in data servers computers on Computers Centers --- which are vulnerable to the attack from computer virus transmited by electronic mail. This work aims to propose the implementation of an Information Safety Policy in a company, giving emphasis to the protection against virus attacks received from electronic mail. This is a critical problem of great proportions, that can cause great damages to organizations and companies as a whole. The Safety Policy tries to point out means and guidelines to provide reliable, safe, information, that contributes positively to the decision marketing process. This dissertation tends to evaluate how the corporations are dealing with the problem of the information safety against electronic mail virus, how the leaders have been concerned about the loss, integrity and the destruction of the stored data, to enumerate the main means and technological implementations to minimize the risks with the lack of safety of these data and to point out the importance of the implementation of this Politicy (aiming to provide) with the intention of providing resources, technology and reliable information to the business.

**SUMÁRIO**

## LISTA DE FIGURAS

## LISTA DE TABELAS



## CAPÍTULO I

## INTRODUÇÃO

## 1.1 SOCIEDADE, COMUNICAÇÃO E SEGURANÇA DA INFORMAÇÃO

Uma das maiores necessidades do ser humano é a comunicação. A sociedade torna-se produtiva quando se comunica e soma esforços para objetivos comuns. O povoamento da Terra e a distância geográfica entre as pessoas tornou a comunicação entre os povos uma necessidade e um desafio constante a ser superado.

A evolução dos meios de comunicação utilizando sinais elétricos deu origem aos maiores sistemas de comunicação da atualidade, como o telefone, o rádio, a televisão e os computadores e, deste modo, as informações passaram a ser tratadas como fator de competitividade e estratégia de grande valor para as nações, para os governos e organizações, com o intuito de obter poder e domínio de mercados comerciais.

A automação da informação evoluiu em duas frentes complexas e que necessitavam de alta tecnologia e grande investimento em pesquisas: o *Hardware* (qualquer dispositivo elétrico ou eletrônico componente de computadores ou dispositivo componente dos mesmos), e o *Software* (programa de computador desenvolvido com a finalidade de executar algum procedimento previamente programado). As empresas, organizações governamentais, centros de pesquisas e universidades buscavam soluções para interligarem seus computadores, compartilhando recursos entre si, pois os centros de computação isolados não poderiam atender as necessidades de comunicação dos usuários.

Como fruto destas pesquisas, a partir do ano de 1970, houve difusão e avanço na área de redes de computadores. Inúmeras soluções e implementações foram desenvolvidas. Atualmente, com o uso intensivo da *Internet* (a maior rede mundial de comunicação entre computadores, também conhecida como WWW-*World Wide Web*, nas universidades, nas residências, nas empresas, nos centros de pesquisas e órgãos governamentais, o objetivo inicial de se promover a comunicação eletrônica entre as pessoas obteve sucesso, porém, apresentou-se um novo problema, também complexo e de imensas proporções: a vulnerabilidade da informação.

Dentre todos os possíveis ataques à informação, aqueles por meio de vírus de computador, em particular, os que em virtude da alta probabilidade de ocorrências são de alto impacto negativo para o negócio.

As empresas atualmente estão preocupadas com a segurança da informação armazenada em meios magnéticos e eletrônicos, sendo que este panorama de fragilidade técnica está induzindo muitas organizações a implementarem soluções tecnológicas para proteger seus dados corporativos, com consciência do cuidado que

deverão tomar no momento de se decidir por qual sistemática adotar e por quais diretrizes implementar. É preciso planejamento, análise das soluções já implementadas no mercado e a montagem de um plano estratégico do projeto total. Inicialmente, como visão macro da situação da empresa, é necessário identificar o máximo de fragilidades possíveis, principalmente com relação a ataques por meio de vírus de computador, que deverão ser analisadas e combatidas.

Um modelo de solução a ser adotada é a implementação de uma Política de Segurança da Informação nas empresas. Quando bem estruturadas, estas diretrizes podem minimizar os riscos contra acessos aos dados por pessoas não autorizadas, perda acidental, furtos de tecnologia e outros, e assim, contribuir para melhorar e difundir o correto uso dos recursos de informática existentes e disponíveis nas empresas. Uma Política de Segurança da Informação explicita normas internas para a utilização dos equipamentos de informática, apresenta detalhes com relação às ferramentas técnicas utilizadas para a segurança da informação e dita normas de segurança de dados.

Os líderes empresariais compreenderam que sem segurança não há *Business* (termo técnico em Inglês que significa o negócio das empresas) nas organizações, que a segurança não é custo, é investimento e fator fundamental para a sobrevivência do negócio. A informação armazenada em meios eletrônicos é um precioso bem e, considerando-se a crescente utilização de microcomputadores ligados em rede, o uso do correio eletrônico, a *Internet*, a *Intranet*, a *Extranet* e os sistemas *ERP* (Enterprise Resource Planning), é possível suspeitar-se de que não exista uma rede de dados totalmente segura e protegida contra danos provocados por pessoas internas, externas à empresa, que possam provocar contaminações ou perdas nos dados, seja por meio de vírus de computador, invasão dos sistemas ou outro.

Esta vulnerabilidade existente nas redes se reflete em prejuízos, extravio de tecnologia, paralisação de sistemas, morosidade nos negócios e na vantagem ou desvantagem competitiva frente às empresas concorrentes. Vandalismo, falsificação, espionagem e imperícia são algumas das ameaças que agem sobre as redes cada vez mais abertas, que interligam um número cada vez maior de computadores e de pessoas. Segundo Lopes (2000), após o *"Bug do Milênio"*, uma grande parte das empresas passaram a direcionar seus recursos financeiros, técnicos e humanos para a implantação de novos sistemas com o intuito de agregar valores aos seus negócios, como o comércio eletrônico e na segurança da informação, este último, considerado um item de alta prioridade. Com o passar dos anos as empresas, na maioria dos casos, foram crescendo sem uma preocupação em se ter implementado uma documentação confiável e detalhada, procedimentos e sistemáticas contendo diretrizes e normas

relacionadas com segurança física, lógica e um plano de contingência frente a uma catástrofe em suas instalações de centros de processamento de dados. Isto se mostra presente também com relação aos vírus de computadores, que estão sendo criados o tempo todo em novas versões e com diferentes ações danosas aos dados e equipamentos.

## 1.2 CARACTERIZAÇÃO DO PROBLEMA

As organizações têm demonstrado uma carência no tocante àproteção dos seus servidores de correio eletrônico, pois trata-se de uma necessidade que envolve investimentos, decisão da alta administração da companhia e conhecimento técnico das pessoas envolvidas. É necessário implementar uma Política de Segurança da Informação com foco no problema do Vírus de Computador que adentra àempresa em estudo, por meio da *Internet* ou anexado a um arquivo de *e-mail* (correio eletrônico). É preciso criar mecanismos de combate a este problema, inclusive para que o desastre não tenha proporções que possam paralisar as atividades não somente da empresa em si, como também das outras organizações parceiras, com as quais a comunicação se faz via correio eletrônico.

## 1.3 OBJETIVO PRINCIPAL DA PESQUISA

Esta pesquisa tem o objetivo de efetuar um estudo do conceito da Informação nas empresas, tomando-se como referências alguns tópicos sobre a estratégia, os sistemas informatizados e a competitividade no mercado, provida pela informação correta, acessível, íntegra e rápida. Uma das maneiras de ter esta informação segura na organização, é a implementação de uma Política de Segurança, que venha a prover a segurança necessária àsobrevivência desta organização, e, neste caso em particular, com o foco para o problema do *e-mail* contendo arquivos contaminados por vírus de computador.

A aplicabilidade dos conceitos desenvolvidos neste trabalho será verificada por meio de um estudo de caso relativo àimplementação de uma Política de Segurança da Informação com foco em *e-mail*, em uma empresa do Estado de São Paulo, localizada no Vale do Paraíba, que tem unidades em todo o Brasil e exterior.

Esta empresa em estudo não tinha implementado nenhuma Política de Segurança da Informação, sendo que apenas existiam alguns critérios e cuidados importantes com relação à segurança, que eram seguidos pelo bom senso dos funcionários que gerenciavam a área de Tecnologia da Informação e que procuravam aplicá-los, porém

não havia qualquer procedimento ou determinação feita, escrita e com a obrigatoriedade de os usuários a respeitarem. Com relação a estes critérios, o que existe, e é seguido pelos profissionais da área de Informática, é uma rotina diária de *back-up* (processo de se executar cópias de segurança de dados em discos ou fitas magnéticas), de dados importantes localizados nos servidores e alguns critérios simples para a criação de contas de acesso à rede e correio eletrônico por parte dos usuários, sendo que a área do *CPD* (Centro de Processamento de Dados) se localiza em sala isolada, com fechadura digital de abertura por meio de uma senha digitada em um painel.

A pergunta que se faz para este trabalho é a seguinte:

*Implementando-se uma Política de Segurança da Informação baseada na proteção do e-mail com vírus de computador é possível contribuir para a melhoria contínua, desempenho e competitividade da empresa?*

## 1.4 JUSTIFICATIVA E RELEVÂNCIA DO TEMA

Como Justificativa e Relevância do Tema pode-se afirmar que este assunto vem ao encontro de um problema atual, existente nas empresas, universidades e órgãos governamentais em caráter mundial. Está sendo estudado em uma vasta literatura abordando a preocupação e as vulnerabilidades das organizações com relação à segurança da informação. Se por um lado a literatura aborda o problema apresentando o fascínio pelo qual os *Hackers* (técnicos altamente especializados em computadores e que por prazer ou desafio, acessam e invadem computadores de outras pessoas, universidades, empresas, bancos e órgãos governamentais), destroem e geram prejuízos e transferem informações entre empresas concorrentes, por outro lado, existem os especialistas que se utilizam de pesquisas e ferramentas semelhantes, porém com a finalidade de proteger estas instituições.

O fato de o trabalho estar voltado para a segurança do correio eletrônico, baseia-se no motivo de esta ferramenta tecnológica ser o principal meio de comunicação e transmissão de dados da atualidade. Em conseqüência o *e-mail* tem sido um portador de vírus de computador e um meio para disseminação de perigos, invasões e danos às informações existentes e armazenadas nos servidores de dados das organizações e da *Internet*. Este fato tem sido motivante para pesquisadores e especialistas trabalharem em busca de soluções de tecnologia, que possam contribuir para a melhoria da segurança da informação e da continuidade dos negócios.

## 1.5 ORGANIZAÇÃO DO ESTUDO

O desenvolvimento do trabalho seguirá uma seqüência normal para o assunto em epígrafe, ou seja:

No Capítulo I - Introdução, esclarecerá a caracterização do problema, o objetivo da pesquisa, bem como a justificativa e relevância do assunto.

No Capítulo II – Sistemas de informação e a Gestão das Empresas, será abordado o conceito teórico da informação, sistemas de informação, a informação como recurso estratégico das organizações, a gestão da informação e o uso estratégico dos sistemas de informações gerenciais. A abordagem deste tema será importante tendo em vista que a informação que tem que ser protegida é o objeto principal da pesquisa.

No Capítulo III – Generalidades Sobre a Segurança da Informação, serão apresentadas algumas generalidades sobre a segurança da informação, histórico sobre segurança, a informação armazenada nas organizações, o controle de acesso, a segurança física e lógica da informação. Os temas abordados serão importantes para a conceituação do que é a segurança da informação.

No Capítulo IV – Segurança de Redes de Comutadores, serão analisados os conceitos de segurança das redes de computadores, vulnerabilidades, ameaças, principais tipos de ataques à informação e é apresentado o conceito de Política de Segurança da Informação.

No Capítulo V – Segurança em Correio Eletrônico (*E-MAIL*), serão evidenciados a segurança, a estrutura de nomes, o formato e a sintaxe dos endereços, os Domínios, considerações sobre a segurança em correio eletrônico, Vírus de Computador e Privacidade e Monitoramento.

O Capítulo VI – Procedimentos Metodológicos, evidenciará os Métodos e Procedimentos empregados no desenvolvimento da pesquisa.

O Capítulo VII – Estudo de Caso, descreverá todo o estudo de caso da implementação de uma Política de Segurança em uma indústria, com foco na proteção do *e-mail* com arquivo anexado e contaminado por vírus de computador. Existe o propósito de se efetuar um amplo relato dos conflitos e problemas existentes e que poderão ser detectados ao longo do desenvolvimento e implementação do projeto, tendo em vista que o mesmo deverá estar sendo feito em unidades diferentes da mesma empresa.

O Capítulo VIII – Resultados, evidenciará os resultados obtidos com o estudo de caso, relacionando com a bibliografia pesquisada.

O Capítulo IX – Conclusão, serão apresentadas as conclusões obtidas com o desenvolvimento da pesquisa.

No final do trabalho, nas considerações finais e conclusivas, serão apresentados alguns comentários sobre toda a pesquisa e a análise dos resultados, como também a apresentação de contribuições para o conhecimento e tendências do uso da segurança da informação, demonstrando a possibilidade da mesma se estender para futuros estudos sobre assuntos similares e sobre o tema abordado.

## CAPÍTULO II

## SISTEMAS DE INFORMAÇÃO E A GESTÃO DAS EMPRESAS

*"Informação é aquilo que sintetiza a natureza de tudo o que existe ou ocorre no mundo físico." Caruso(1999)*

A informação protegida e disponível contribui com uma maior credibilidade, integridade e confiança para a tomada de decisão estratégica nas empresas. Este capítulo analisa os fundamentos relacionados à informação, abordando aplicações relativas ao seu uso dentro das organizações como base para os dirigentes tomarem decisões. Este tema tem uma grande abrangência e, sendo assim, optou-se por discutir aqueles tópicos que possam permitir um embasamento específico ao assunto proposto. Um Sistema de Informações é algo complexo, extenso, necessário às corporações e

imprescindível aos dirigentes empresariais e a necessidade de se manter estas informações confiáveis e seguras é uma constante no processo de gestão do negócio.

## 2.1 A INFORMAÇÃO E OS SISTEMAS DE INFORMAÇÕES

Em relação à conceituação de sistema de informação, pode-se dizer que a automação e a segurança fizeram com que as organizações esquecessem o objetivo principal da informação, que é o de informar, sendo que todos os computadores do mundo somados para nada servirão se os seus usuários não estiverem interessados na informação, nos dados e nas soluções de problemas que esses computadores poderiam gerar. A informação será igualmente inútil se os funcionários de uma empresa, das instituições de ensino e das organizações em geral não a compartilharem, divulgando suas pesquisas, experiências tecnológicas e sucessos expressivos. Desta forma, sistemas desenvolvidos por especialistas não irão proporcionar informações úteis se as mudanças nesta área de conhecimento forem muito rápidas – ou se os criadores destes sistemas não puderem encontrar especialistas dispostos a ensinar o que sabem. A informação e o conhecimento são essencialmente, fruto de pesquisas e criações humanas, e nunca seremos capazes de administrá-los se não levarmos em consideração que as pessoas desempenham, neste cenário, um papel fundamental para a evolução do conhecimento. Em face de todas estas alusões, a segurança da informação é uma preocupação constante, pois anos de pesquisas, trabalho e resultados podem se perder em poucos instantes caso o meio de armazenamento destes registros sejam danificados, se percam ou sejam adulterados. Isto mostra que o ambiente da informação deve ser visto na sua totalidade, ressaltando os valores e as crenças empresariais sobre a informação como cultura e como as pessoas realmente a tratam no processo de trabalho. Do ponto de vista de concepção, segundo Silva Jr. (2000), um Sistema de Informações precisa:

- Atender às reais necessidades dos usuários de microcomputadores das empresas e organizações em geral.
- Estar com o foco centralizado neste usuário final, que é quem necessita da informação para a tomada de decisão, e não no profissional que criou o sistema.
- Atender ao usuário com presteza, rapidez, atenção e profissionalismo.
- Apresentar custos compatíveis com a realidade do mercado e dos serviços prestados.

- Adaptar-se ao mercado e à constantemente evolução de novas tecnologias de informação;
- Estar alinhado com as estratégias de negócios da empresa, que é um requisito fundamental quando se estuda o tipo de sistema especialista para apoio às decisões.

Um sistema de informação pode ser considerado tecnicamente como um conjunto de programas, processos e componentes inter-relacionados que coleta ou recupera dados, processa, armazena, atualiza e distribui informações para suportar o controle e a tomada de decisões nas empresas e nas organizações, contribuindo para a difusão do conhecimento, do controle e dos negócios mundiais. Além de suportar a tomada de decisão, coordenação e controle, os sistemas de informações podem também ajudar os pesquisadores, os administradores de negócios e os trabalhadores a analisar problemas, desenvolver pesquisas abordando assuntos complexos e criar novos produtos e alternativas de serviços. Uma das principais forças motivadoras da tendência àdispersão da informação é a necessidade de que a função sistema de informação, com o passar dos anos e a evolução tecnológica, torne-se mais próxima de seus clientes para poder fornecer sistemas mais rapidamente, em resposta às pressões competitivas do mercado. Empenhadas em se manter e se tornar cada vez mais competitivas, as empresas e as organizações estão procurando encontrar formas de integrar as funções de sistemas de informação com todas as operações do seu negócio. Estas entidades estão também reconhecendo que, à medida que os sistemas de informação tornam-se vitais para as operações dos negócios, devem ser capazes de mudar com rapidez para se adequar às exigências dos mercados, o que significa que as atividades de sistemas de informações têm que ser flexíveis e estar mais intimamente alinhadas com as operações específicas das empresas. Neste sentido, a importância da segurança da informação é uma questão de não somente competitividade, mas também de sobrevivência da empresa ou organização no mercado. Baseando-se no cenário onde a empresa se encontra inserida, pode-se perceber claramente a presença de diversas entidades atuando em parceria ou como concorrentes, seja o governo, o consumidor, os fornecedores, as instituições financeiras, os empregados etc. Todas estas inter-relações, ocorrendo em maior ou menor intensidade, culminam em um complexo processo de gestão empresarial que necessita de segurança dos dados que estão sendo utilizados como base para tomada de decisão ou para análise de perspectiva de negócio. Ressalta-se que, ao mesmo tempo em que a empresa sofre o impacto da turbulência ambiental, ela também interage com o seu ambiente, com suas pesquisas, com o seu produto de

comercialização que também está em constante mutação e estes fatos podem gerar oportunidades ou ameaças para a empresa ou organização.

Seguindo esta linha de raciocínio, Silva Jr. (2000) ainda comenta que os gestores precisam conhecer profundamente a organização que está sob a sua responsabilidade, bem como o mercado e o ambiente competitivo onde ela opera, a fim de avaliar o impacto da turbulência ambiental e desenvolver o cenário para uma solução eficaz e competitiva. Desta maneira observa-se nitidamente a importância da informação confiável e segura, pois é por meio dela que os gestores conseguem identificar tanto as oportunidades quanto as ameaças que o ambiente oferece à empresa ou à organização. Os profissionais responsáveis pelo desenvolvimento, implantação e manutenção de sistemas de informações, ao longo do tempo, têm contribuído para o aperfeiçoamento da interpretação deste ambiente empresarial. O desafio para melhorar esta compreensão também passa por uma incursão nas teorias da decisão, mensuração e informação, que constituem o tripé que sustenta a configuração do sistema provedor de informações. Embora o fornecimento de informações úteis seja uma preocupação constante dos profissionais que têm a responsabilidade de disponibilizá-las nas organizações, surge ainda uma dúvida quanto à variedade e a diversidade de informações geradas, se são suficientes para o gestor definir, executar e avaliar a estratégia que viabilize o sucesso empresarial em determinado ambiente econômico.

Toda a informação gerada nas empresas e nas organizações deve assumir o caráter de disponibilidade e dar o suporte informativo adequado, para que os gestores percebam a eficiência e a eficácia empresarial como uma necessidade contínua, sustentada e, deste modo, cada vez mais a informação deve surgir no suporte ao ciclo de planejamento, execução e controle, que se consubstancia no processo de gestão. Um outro enfoque existente no estudo de sistemas de informações, é o ambiente em que o mesmo será inserido e os seus requisitos. O ambiente de um sistema é o conjunto de elementos que não pertencem ao sistema e que interaja com ele. Qualquer alteração no sistema pode alterar os elementos do ambiente e qualquer alteração nestes elementos pode mudar o sistema. A figura 1 mostra os elementos do ambiente empresarial, base de aplicação de um sistema de informações executivas (enfoque gerencial), que deverão potencialmente ser consideradas:

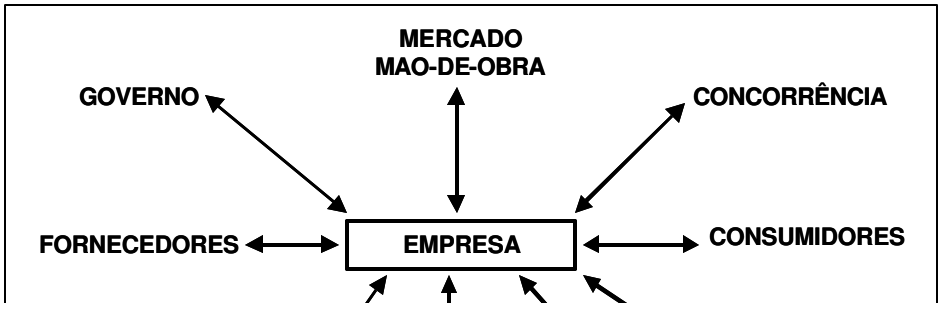


Figura 1 - Ambiente de um sistema empresarial

Fonte: Oliveira, Djalma de P. R. (1993, p.25).

Os sistemas de informações gerenciais podem ser considerados como sistemas informativos que contribuem para o processo de tomada de decisões, apoiando os gerentes no exercício das funções de planejamento, organização, direção e controle das empresas. Assim, a expressão Sistemas de Informações Gerenciais considera inclusive outros conceitos como os Sistemas de Apoio à Decisão, que apresentam uma abordagem mais flexível e ágil, mais relacionados com o apoio aos estilos pessoais de decisão, e também conceitos mais tradicionais como Pesquisa Operacional, que tem uma abordagem serial de especificação das necessidades, projeto detalhado, programação, teste e implementação. Atualmente todos estes conceitos se materializaram numa classe de sistemas de informações especialistas que é rotulado como sistemas de *BI* (Business Intelligence), ou seja, são os sistemas inteligentes voltados aos processos de negócios das corporações empresariais.

Com referência à participação do sistema de informações no modelo de decisão, Beuren (1998) ressalta como um sistema de informações, que auxilie o gestor a melhorar suas decisões, não depende apenas da identificação dos modelos decisórios dos gestores e de suas necessidades informativas, sendo que em muitas das vezes, faz-se necessário repensar o próprio modelo de decisão, além de utilizar informações adicionais com o intuito de se determinar a probabilidade de ocorrência de cada estado da natureza, para se reduzir o problema da incerteza. Um sistema de informação, em consonância com a amplitude do processo de gestão empresarial, deve ter o foco em planejamento estratégico, apuração de resultados e desempenho baseado em módulos de simulação, orçamento, programação e realizado, bem como na mensuração e acumulação da informação, conforme representado na Figura 2.

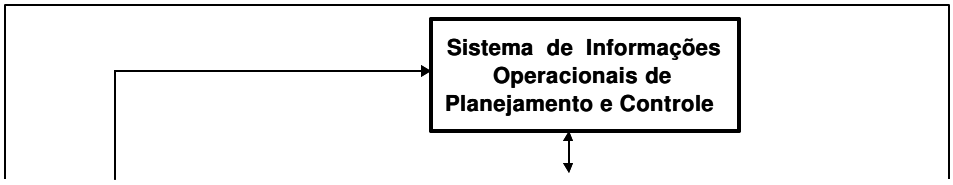


Figura 2 - Sistema de informação com enfoque no processo de gestão empresarial

Fonte: Parisi, Armando *apud* Silva Jr. (2000, p.18).

Todas as empresas, organizações financeiras, entidades de ensino, governamentais, enfim, de qualquer ramos de atividade, em seu processo de controle, gerenciamento e estratégia necessitam ter informações confiáveis, atualizadas e disponíveis a todo o instante. No modelo acima, com foco no processo de gestão empresarial, verifica-se que a integração do Sistema de Apuração e Avaliação de Resultado e de Desempenho ocorre por meio da conexão deste com o Sistema de Informações Operacionais de Planejamento e Controle e o Sistema de Planejamento Estratégico. Desta maneira, o primeiro sistema recebe as informações dos outros dois, permitindo que cada gestor, dentro de sua área de atuação e responsabilidade, possa simular as diversas alternativas de uma decisão, além de orçar, programar e realizar cada alternativa escolhida.

Resumidamente, Beuren (1998) ressalta que a concepção do sistema de informações é dependente do sistema de gestão ao qual vai servir de suporte e, deste modo, os esforços dispendidos na arquitetura e no desenvolvimento do sistema de informações devem ser concentrados na identificação das informações necessárias ao processo de gestão empresarial e na determinação dos subsistemas que devem gerá-las. Todos estes fatores sugerem que haja interação do sistema de informação com o sistema organizacional e, portanto, pode-se considerar necessário a ligação dos conceitos de sistema de informações genericamente e o modelo do processo de decisão. Este papel dos Sistemas de Informações no apoio ao processo decisório mostra a função estratégica que a informação assume dentro das empresas. Este tópico será explorado na próxima seção.

## 2.2 A INFORMAÇÃO COMO RECURSO ESTRATÉGICO NAS EMPRESAS

*"... nenhuma empresa pode se dar ao luxo de tal incompetência, embora o custo da obtenção de uma informação errada – ou não-uso da informação correta – seja difícil de medir. Obviamente, um pesquisador não pode ler a mente de um administrador para descobrir que tipo de informação possui, quando a obteve, de onde a recebeu e como é utilizada no momento da tomada de decisões. Mas ninguém pode negar que decisões baseadas em dados inúteis têm custado bilhões de dólares em produtos encalhados, em aquisições que não funcionam, em investimentos em instalações ou equipamentos que não produzem".* Davenport (1998), p.16.

O conhecimento adquirido armazenado e utilizado como recurso estratégico, é fruto de uma ação estruturada sobre as informações disponíveis nas empresas. Estas informações são disponibilizadas pelos vários sistemas de informações –- automatizados ou não –- nas empresas. Entretanto, da mesma forma que um monte de tijolos iguais não é uma casa, também uma grande quantidade de dados não representa conhecimento. É necessário caracterizar o que se entende por dados, informação, conhecimento e seus relacionamentos, para o entendimento do processo de transformação de dados em conhecimentos.

A tabela 1 apresenta resumidamente estes conceitos destacados:

Tabela 1 – Dados, informação e Conhecimento

| **DADOS** | **INFORMAÇÃO** | **CONHECIMENTO** |
|---|---|---|
| ***Simples observações sobre o estado do mundo.*** | ***Dados dotados de relevância e propósito*** | ***Informação valiosa da mente humana. Inclui reflexão, síntese, contexto.*** |
| Facilmente estruturado | Requer unidade de análise | De fácil estruturação |
| Facilmente obtido por máquinas<br><br>Freqüentemente quantificado | Exige consenso em relação ao significado<br>Exige necessariamente a mediação humana | De difícil captura em máquinas<br><br>Freqüentemente tácito |
| Facilmente transferível | | De difícil transferência |

Fonte: Davenport, Thomas H., Prusak, Laurence (1998, p.18).

Segundo Oliveira (1993), os conceitos de dado e informação são diferentes e deve-se distingui-los. O que distingue dado ou um conjunto de dados de informação, a qual auxilia no processo decisório, é o conhecimento que propicia ao tomador de decisões. Dado é qualquer elemento identificado em sua forma bruta que por si só não

conduz a uma compreensão de determinado fato ou situação. É necessário ao executivo obter o conhecimento a partir do dado transformado, o que lhe propicia um processo dinâmico ou um elemento de ação e esta situação dinâmica lhe permite posicionar-se diante de um problema ou situação qualquer. Dados existentes em empresas também podem ser considerados a quantidade de produção, custo de matéria-prima e número de funcionários. A informação poderia ser considerada como o resultado da análise desses dados, ou seja, a capacidade de produção, o custo de venda de produtos, a produtividade do funcionário etc. Estas informações, ao serem utilizadas e manipuladas pelos executivos, podem afetar ou modificar o comportamento existente na empresa, bem como o relacionamento entre as suas várias unidades organizacionais, filiais, outras empresas agregadas a ela e à sociedade que depende –- direta ou indiretamente –- de sua atuação no mercado e na comunidade.

Em resumo, a informação é o dado organizado e trabalhado que permite a tomada de decisões, enquanto que o conhecimento é considerado como o uso aplicado desta informação por meio das habilidades dos executivos (análise, reflexão) para auxiliar suas atividades de decisões. A informação, como um todo, é recurso vital da empresa e integra, quando devidamente estruturada, os diversos subsistemas e, portanto, as funções das várias unidades organizacionais da empresa. Observa-se, no entanto, uma mudança da concepção de informações e sistemas de informações. Por detrás do crescente uso dos sistemas de informações existe uma mudança do conceito do papel da informação nas organizações. As empresas consideram atualmente a informação como um recurso estratégico, mais do que o trabalho e capital, porém este fato não foi sempre assim.

Existem alguns autores que reforçam a característica do uso da informação como recurso estratégico, justificada como elemento fundamental para estruturação de um sistema de informações específico para executivos:

"*... a informação pode ser usada no sentido de identificar alternativas para provocar mudanças no poder de barganha da empresa com o ambiente externo, para remover ou criar barreiras à entrada de novos concorrentes, diferenciar uma empresa das demais que atuam no mesmo segmento, para configurar novas cadeias de valor, para penetrar em economias diferenciadas, dentre outros fatores*". Beuren (1998), p.52.

É possível considerar que o propósito básico da informação é o de habilitar a empresa e as organizações em geral a alcançarem os seus objetivos pelo uso eficiente dos recursos disponíveis, nos quais se inserem pessoas, materiais, equipamentos, tecnologia, dinheiro, além da própria informação. A informação é o produto da análise dos dados existentes na empresa, devidamente registrados, classificados, organizados,

relacionados e interpretados dentro de um contexto para transmitir conhecimento e permitir a tomada de decisão de forma otimizada.

A partir da década de 1980, segundo Laudon e Laudon (1996) *apud* Silva Jr. (2000), a informação tem sido considerada como um recurso estratégico, uma fonte potencial de vantagem competitiva para as empresas e governos, ou uma arma estratégica para derrotar e frustrar a competição. Estas mudanças de conceito da informação refletem os avanços na teoria e planejamento estratégico, ou seja, une-se, dentro dos conceitos da importância da informação até aqui definidos, o seu uso aplicado nas estratégias empresariais, seguindo a tendência de alinhamento de todos os recursos da organização nos focos estratégicos. Alguns autores auxiliam na percepção destes conceitos:

Segundo Gomes e Salas (1997) *apud* Silva Jr. (2000), para atender às necessidades adaptativas impostas pela turbulência ambiental do mercado, as empresas precisam encontrar novos caminhos para alcançar sucesso e isto é facilitado com o uso intensivo da informação, em termos de sua colaboração na descoberta do recurso que mais atende à carência embutida em cada parte da organização. Eles ressaltam uma interessante característica da informação estratégica: ela não requer a precisão da informação contábil tradicional, podendo esta, na maior parte das vezes, ser contraproducente e, sendo assim, a informação não estruturada e imprecisa pode ser, paradoxalmente, muito útil. A estratégia da informação também significa a possibilidade de se fazer escolhas, sem definir um plano imutável. Os gerentes poderão criar estratégias quanto aos tipos de informações que devem ser focalizadas, as atividades a enfatizar e a maneira como a informação poderá ajudar a empresa a alcançar seus objetivos.

Segundo Beuren (1998), a elaboração e a execução da estratégia podem ser aprimoradas com o uso da informação. No entanto, o papel central deste recurso, com a finalidade de alcançar o objetivo estratégico da empresa, não é tratado com muita ênfase no meio empresarial e na literatura tradicional sobre estratégia empresarial. A informação é um instrumento organizacional que se traduz na flexibilidade em identificar no menor período de tempo, o passo à frente que deve ser dado. Com relação aos medidores gerenciais, no passado, os responsáveis pela administração das informações acreditavam que uma das estratégias mais adequadas e utilizadas em gestão era perguntar aos dirigentes quais os dados de que precisavam para o exercício de suas funções e, de posse das pesquisas, começariam a dizer a estes gerentes como suas exigências informacionais deveriam ser, tendo em vista que quando se aborda a informação como recurso estratégico, deve-se avaliar também o grau de participação

dos gestores no uso destes recursos e a integração da informação, com as estratégias da organização. A grande maioria dos gerentes quase sempre reluta em participar dos primeiros e difíceis estágios do desenvolvimento de uma estratégia informacional, na maioria das vezes porque poucos compreendem os conceitos da informação, ou a tecnologia relacionada a ela, o suficiente para poder dscuti-los. Pode-se dizer que a maioria dos administradores possui uma compreensão intuitiva da informação, da sua importância, e que os executivos seniores não costumam ascender a suas posições sem fazer uso efetivo da informação, de alguma maneira. Baseado nestes fatos, os gerentes devem quebrar suas próprias barreiras e avançar no sentido da compreensão e da participação assim que a discussão sobre a estratégia informacional começar. Devem ao menos reconhecer que as falhas de comunicação são partes naturais deste tipo de discussão, não devendo ser consideradas obstáculos intransponíveis.

Há, portanto, que se desenvolver a participação efetiva dos executivos e de uma estrutura de apoio para o tratamento das informações estratégicas (análises, reflexões, sínteses, visão de contexto). Observa-se, assim, que os aspectos relacionados à cultura do uso de informações gerenciais, são considerados um dos fatores críticos de sucesso para implementação deste tipo de sistema de informações. Na prática, em todas as organizações, a informação é influenciada a cada minuto pelo poder, pela política e pela economia e, desta maneira a necessidade do entendimento do executivo, da integração da estratégica empresarial e da informação confiável e disponível como apoio à tomada de decisão é fundamental para a sobrevivência do negócio. Considera-se que, as decisões sobre informações de economia, mercados, ofertas, tecnologia e competência característica são as mais importantes para os administradores e que as organizações que tomam decisões estratégicas inadequadas terão mau desempenho, ou fracassarão. Não existe arquitetura organizacional que possa ajudar uma estratégia mal concebida, no entanto, havendo uma estratégia viável e com objetivos internamente consistentes, o desafio da administração passa a ser o de construir uma organização para realizar esses objetivos estratégicos e a estratégia determina tanto a natureza do trabalho como do produto organizacional crítico. A estratégia identifica a posição da empresa no ambiente competitivo e a forma como ela poderá continuar se mantendo ou, até mesmo, melhorar sua posição em relação a seus concorrentes. Para isso, os gestores precisam de informações sobre a organização e o ambiente externo da empresa, com vistas a identificar ameaças e oportunidades, criando um cenário para uma resposta eficaz e competitiva.

Concluí-se que a construção das informações estratégicas não pode ser sustentada, apenas, com apelos tecnológicos, mas que os aspectos como o

levantamento efetivo das estratégias empresariais e sua vinculação com a Arquitetura de Informações deverão ser considerados, inclusive com os aspectos políticos e culturais da organização. Atualmente, num mercado totalmente de envolvimento do executivo com o gerenciamento da informação é coerente o uso desta informação como recurso estratégico.

## 2.3 A GESTÃO DA INFORMAÇÃO NAS ORGANIZAÇÕES

A informação existente nas corporações é fruto de investimento em equipamentos, pesquisas, mão-de-obra, como também, do conhecimento acumulado ao longo de anos de trabalho. O estudo da gestão da informação, como ponto de apoio estratégico nas corporações, aborda a cultura do uso das informações e seus aspectos, assim dispostos:

- A importância do gerenciamento da informação existente;
- O estudo do ambiente informacional estabelecido e criado nas organizações;
- O entendimento dos estilos de gerenciamento da informação armazenada nas empresas;
- O comportamento do gestor em relação à gestão da informação, neste estudo específico aplicado ao uso de sistema de informações gerenciais no processo decisório organizacional.

A ênfase primária não está na geração e na distribuição de enormes quantidades de informações pela corporação, mas no uso eficiente de uma quantia relativamente pequena, cabendo-se o planejamento do ambiente de informação de uma empresa. Em resumo, a abordagem do gerenciamento da informação é mais modesta, mais comportamental e mais prática que os grandes projetos da arquitetura da informação e de máquina/engenharia. Tem-se, a respeito da administração informacional quatro diferente abordagens, que correspondem a modalidades ou fluxos de informação em uma organização moderna: informação não-estruturada, capital intelectual ou conhecimento, informação estruturada em papel, e informação estruturada em computadores. As quatro abordagens apresentam diversos problemas em comum, pois usam informações que se sobrepõem a outros modelos, vêm adotando estilos gerenciais inadequados e têm ignorado completamente os fatores comportamental e social no uso da informação.

Grande parte das empresas tem feito pouco em relação ao gerenciamento de informações. Elas têm concentrado seus recursos em duas atividades, ou seja, aplicam a tecnologia aos problemas informacionais e procuram usar os métodos de máquina/engenharia para transformar dados em algo útil. Infelizmente, nenhuma dessas

abordagens constitui em abordagem holística da informação. Numa abordagem holística deve-se mobilizar não apenas desenvolvedores arquiteturais e Tecnologia da Informação, mas também estratégia, política e comportamento ligados àinformação, além de suporte a equipes e processos de trabalho para produzir ambientes informacionais melhores. Quando os administradores praticam este gerenciamento, consideram diversas vias para chegar aos objetivos propostos.

Segundo Silva Jr. (2000), uma abordagem holística da informação possui quatro atributos-chave, principalmente em se tratando de informações para tomada de decisões gerenciais:

- Existência da integração dos diversos tipos de informação – muitas organizações já começaram a integrar a administração de diversos tipos de informação: computadorizada e não computadorizada, estruturada e não-estruturada, via texto, áudio, vídeo, vídeo-conferência e voz.
- Existência do reconhecimento de mudanças evolutivas – embora ninguém saiba todas as respostas aos questionamentos sobre estes assuntos – elas diferem de negócio para negócio - reconhecer que a evolução é um fato da vida organizacional é um primeiro passo, necessário a todos os administradores.
- Existência da ênfase na observação e na descrição – é necessário efetuar a pergunta de como a informação é reunida, compartilhada e utilizada atualmente, e o que se pode aprender com ela. Sabe-se muito pouco sobre o uso da informação nas organizações, e o primeiro passo é observar os usuários da informação relevantes em seu local de trabalho.
- Existência da ênfase no comportamento pessoal e informacional – se uma ação ou iniciativa gerencial não altera o comportamento informacional, não vale a pena colocá-la em prática.

Todos estes atributos-chave aplicam-se a um modelo para o gerenciamento da informação, para o qual são necessárias três caracterizações ambientais: ambiente externo, ambiente informacional e ambiente organizacional.

AMBIENTE INFORMACIONAL

- *Estratégia utilizada pela informação:* está diretamente ligada à resposta da pergunta: “O que se quer com a informação nesta empresa?” E o que é mais importante, esta estratégia deve envolver os altos executivos da administração.
- *Política utilizada pela informação:* envolve diretamente o poder proporcionado pela informação e as responsabilidades da direção em seu gerenciamento e uso.

- *Cultura existente na organização e o comportamento em relação à informação:* todos os fatores relacionados a este item são muito importantes na criação de um ambiente informacional bem-sucedido, porém, são os mais resistentes às mudanças. Além disso, comportamentos positivos como compartilhar informação e obter conhecimento duradouro a partir dela são fundamentais e não podem ficar apenas a cargo da iniciativa de cada um.
- *Equipe da informação:* os indivíduos, as pessoas ainda são os melhores 'meios' para identificar, categorizar, filtrar, interpretar e integrar a informação.
- *Processos de administração informacional:* apresenta detalhes de como o trabalho é feito, sendo que alguns pesquisadores têm tentado identificar como os processos de trabalho com o conhecimento podem ser aperfeiçoados, melhorados e otimizados.
- *Arquitetura da informação:* formado por um guia para estruturar e localizar dentro de uma organização, podendo ser descritivo, envolvendo um mapa do ambiente informacional no presente, ou preditivo, oferecendo um modelo do ambiente em alguma época futura.

AMBIENTE ORGANIZACIONAL

- *Situação em que se encontram os negócios:* é necessário prestar atenção à estratégia de negócios, aos processos, à estrutura e cultura organizacional e à orientação dos recursos humanos. Toda a estratégia dos negócios influenciará a estratégia da informação e a recíproca também é verdadeira.
- *Investimentos efetuados em tecnologia:* um investimento efetuado em Tecnologia da Informação, certamente afetará o ambiente informacional, porém o fator mais crítico em questão é o simples acesso à informação, aos dados armazenados nos microcomputadores e servidores existentes na corporação.
- *Distribuição física:* estudos sistemáticos sobre comunicação organizacional mostram que a proximidade física entre as pessoas e do local de trabalho aumenta a freqüência da comunicação ao criar espaços que facilitem a interação.

AMBIENTE EXTERNO

- *Mercados de negócios:* estes fatores criam condições gerais de negócios, o que afeta a capacidade de as empresas adquirirem e gerenciarem suas informações mais importantes, bem como optar pelo tipo de informação de que precisam.

- *Mercados tecnológicos:* são os locais onde são compradas e vendidas (comercializadas) as tecnologias disponíveis que podem afetar o mundo informacional.
- *Mercados da informação:* constantemente surgem novas fontes de informação que tornam disponíveis uma infinidade de novidades. Ainda assim, quando os administradores buscam nos mercados informacionais serviços que poderiam comprar, precisam analisar e avaliar a relevância desses serviços para seus negócios, bem como a qualidade da informação e a confiabilidade do serviço a ser adquirido ou assimilado.

Com relação ao uso e o gerenciamento da informação, para que uma empresa seja bem-sucedida, necessita haver um consenso sobre o que é a informação dentro da organização, quem a possui, sob que forma é conservada e armazenada, quem é o responsável pelo seu gerenciamento, e o mais importante, como controlar e utilizar esta informação existente em todas as organizações, quer estejam interligadas ou não. Certamente, um dos fatores principais para o sucesso deste gerenciamento real da informação é ter um executivo da alta administração que tenha como meta defender a informação. Uma realidade, porém, é a de que poucos executivos se preocupam com estas questões, sendo que as necessidades de informação são atendidas por suas próprias redes e por seus subordinados e a atenção que os executivos dispensam a esse assunto é limitada.

A primeira etapa na elaboração de uma Política de Gerenciamento de Informação em uma organização é saber quais os modelos utilizados pelas pessoas, qual destes modelos predomina no momento, qual o mais desejável e como proceder para alcançá-lo. Desta maneira, Beuren (1998) desenvolveu um raciocínio baseado no processo de gerenciamento da informação com o intuito de auxiliar aos executivos, face às preocupações levantadas. O fluxograma na Figura 3 apresenta a seqüência do funcionamento das tarefas do processo de gerenciamento da informação.

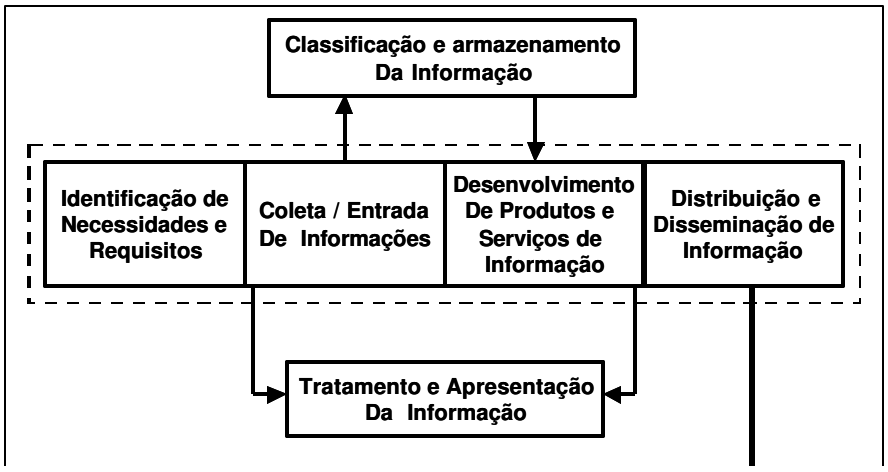


Figura 3 – Tarefas do processo de gerenciamento de informações
Fonte: Mcgee & Prusak (1994) *apud* Silva Jr. (2000, p.42).

Todos os esforços de gerenciamento de informações deverão ser suportados por sistemas de informações gerenciais, que possam fornecer informações básicas de que os gestores necessitem para a tomada de decisão e deste modo, quanto maior for a sintonia entre a informação fornecida e as necessidades informativas dos gestores, melhores decisões poderão ser tomadas.

## 2.4 AS TECNOLOGIAS DE INFORMAÇÕES ESTRATÉGICAS

Um dos maiores desafios da informação é o de permitir aos responsáveis pela alta administração das corporações, alcançar os objetivos propostos para a organização, por meio do uso eficiente dos recursos disponíveis. De acordo com Silva Jr. (2000), a origem e a natureza dos atuais problemas da informação encontram-se no paradoxo quantidade versus qualidade que a tecnologia da informação ajudou a criar, ou seja, há uma grande quantidade de informações disponíveis, porém nem sempre relevantes ao usuário. A atual produção em massa de informações cria a preocupação em disponibilizá-las, cada vez mais, sem definir ou restringir seu público-alvo. A solução para este problema passa pela compreensão de que a informação só será útil se atender às necessidades do usuário final, no prazo, com a qualidade, com a exatidão e a integridade que ele precisa. Analisando por este lado verifica-se que as técnicas e tecnologias disponíveis, passam a ser fundamentais para a viabilidade dos desafios estabelecidos. No estudo deste trabalho, procura-se explorar abordagens vinculadas a tecnologia de segurança da informação, como suporte as arquiteturas de informações para a tomada de decisões estratégicas.

De fato, durante a execução do processo de tomada de decisões, os gestores precisam ser supridos com informações corretas, íntegras e de valor. Este valor, que caracteriza a qualidade da informação, provê uma solidez das decisões que serão tomadas. Conseqüentemente quando esta qualidade deixa de existir, estes gestores são conduzidos a não tomarem as melhores decisões. As informações podem ser consideradas de qualidade quando são relevantes, precisas, acessíveis, concisas, claras, quantificáveis e consistentes, o que requer que a informação, enquanto recurso

básico para o desenvolvimento das atividades empresariais e sua valorização como produto econômico, seja bem gerenciada.

Somente recentemente os computadores se transformaram em ferramentas eficazes e confiáveis no processo de administração do conhecimento, principalmente devido a novos softwares capazes de lidar com textos estruturados, discussões, imagens ou vídeo. Esta contribuição da tecnologia se mostrou presente, facilitando os trabalhos e as empresas começaram a estimular seus funcionários a contribuir para as bases de conhecimento e para os bancos de dados de discussão. No entanto, esta tecnologia não era suficiente para dar respostas condizentes aos principais requisitos da realidade mundial atual abordando temas como a globalização, qualidade, produtividade, capacidade de resposta, *outsourcing* (processo de delegação de atividades e funções a empresas que são enquadradas como Terceiros, sem vínculo empregatício), e controle de custos. Desta maneira, a busca de tecnologias e técnicas que apóiem e viabilizem os esforços da construção da arquitetura de informações estratégicas passa a ser um grande desafio, tanto para os técnicos especialistas em sistemas de informações, como também para os executivos das empresas, responsáveis pela alta administração destas organizações e os usuários finais, que são os maiores interessados no uso destes recursos.

O perfil das tecnologias e das técnicas para atender ao desenvolvimento de sistemas de informações estratégicas deverá, conforme Beuren (1998), abranger todos os conceitos de estratégia de forma compreensível e factível aos membros da organização, sendo que estes passam pela necessidade de disponibilizar informações adequadas aos responsáveis pela elaboração da estratégia empresarial que, aplicada para a adaptação da empresa aos novos paradigmas de um mercado globalizante, exige capacidade de inovação, flexibilidade, rapidez, qualidade, produtividade, exatidão, integridade e segurança dentre outros requisitos, o que torna cada vez mais fundamental o papel que a informação exerce para as organizações. A utilização da informação representa uma intervenção no processo de gestão, podendo, inclusive, provocar mudança organizacional, à medida que afeta os diversos elementos que compõem o sistema de gestão. Esse recurso, que é vital para a corporação, quando devidamente estruturado, integra as funções das várias unidades da empresa, por meio dos diversos sistemas organizacionais e suportados por tecnologias computacionais. A área de Informática sempre presenciou grandes mudanças, novas tecnologias de *hardware* e *software*, metodologias inovadoras para desenvolvimento de ferramentas de controle e desenvolvimento de projetos e, a partir do ano de 1990, teve início uma mudança radical e de grandes proporções do ambiente de processamento de dados em direção a um

processamento distribuído, com mais recursos tecnológicos e mais próximo dos usuários finais.

Muitos fabricantes de *hardware* e *software* estavam bastante empenhados em pesquisas e desenvolvimento de novas ferramentas e aplicativos, com o intuito de se conseguir encontrar soluções de integração das diferentes plataformas computacionais e conectividade. Nesta fase surgiram alguns aplicativos, Sistemas Operacionais e produtos específicos, contendo interfaces mais amigáveis com o usuário final, como, por exemplo, o MS-Windows da *Microsoft* (uma das maiores empresas fabricantes de software voltado para plataforma de microcomputadores pessoais), que despontavam no mercado como soluções muito eficientes. Este fato fez com que as empresas, instituições de ensino e corporações diversas efetuassem uma reciclagem total dos seus aplicativos, e uma nova geração de produtos nasceu juntamente com o ambiente Windows, permitindo uma padronização dos softwares, principalmente os ligados à microinformática. Este avanço tecnológico permitiu que os profissionais da área de tecnologia de informação passassem novamente a ter um controle centralizado sobre o ambiente de Informática até então pulverizado e desintegrado e, desta maneira, servir como base para o desenvolvimento de sistemas que atendessem à realidade própria dos executivos no contexto empresarial.

De acordo com Silva Jr. (2000), com relação a esta realidade, as pessoas têm a tendência a preferir informações oportunas e ricas em detalhes contextuais, fantasiados e atualizados. A informação torna-se mais interessante quando envolve seqüência e causalidade, ou seja, apresentando uma história, ou quando são apresentadas com humor ou quando ganham uma interpretação única, simples e composta por informações visualmente ricas, em cores, texturas, estilos – e que tenham relevância para nossas vidas e nosso trabalho. Estes detalhes podem ter uma conotação do óbvio, porém, o que se obtém dos computadores são normalmente informações datadas, exatas, com pouco ou nenhum contexto ou significado, destituída de seqüência ou causalidade, apresentadas em formatos pobres e em volume muito maior que se deseja ou tenha condições de examinar. Por outro lado, apesar de se conseguir inserir em um computador as últimas informações e novidades do diretor financeiro, quando o mesmo for dar as notícias informando que os resultados do trimestre serão baixos, se gostaria também de saber se o conselho foi avisado do problema, se isso se deve à recessão ou se o maior concorrente está se saindo melhor. O computador dificilmente mostraria a dolorosa expressão facial do diretor financeiro ao transmitir estas notícias, nem explicaria a obscura redação do memorando dizendo que algo vai realmente mal. Muitas pesquisas empíricas indicam que os administradores preferem informações que não residem no

computador, sendo levados pela intuição e experiência profissional quando do trato com algum problema de difícil solução. Alguns estudos comprovam que a informação computadorizada nem sempre oferece a variedade, a velocidade a atualidade ou a relevância que esses executivos exigem. Como resultado, a maioria tem nas informações verbais suas fontes mais importantes, o que pode ser observado no fato de que os administradores tendem a obter de fontes humanas dois terços da informação que utilizam no seu dia-a-dia de trabalho, como em contatos pessoais e conversas telefônicas e o outro terço encontra-se na informação estruturada, vinda de documentos sobre o ambiente interno, externo, de pesquisas de mercado etc. Novos desenvolvimento de aplicações para tomada de decisões são muito importantes, pois se observa nos modelos implementados um negligenciamento no tratamento e formato das informações ditas não-estruturadas. Existe uma grande preocupação dos atuais executivos quanto à quantidade de informação corporativa existente nas organizações, circulando entre os vários departamentos, algumas organizadas, outras totalmente desordenadas e abarrotando os bancos de dados e tudo isso com um agravante, que é a falta de ferramenta adequada para que se possa extrair estas informações. O processamento eletrônico permite que os executivos acessem a informação desejada em menos tempo e com menos papel do que os outros métodos. O crescente avanço da microinformática e redes locais, utilizando altas velocidades de comunicação local, e a conexão com outras redes locais e de longa distância fez com que fosse efetivamente iniciada a integração da tecnologia de informação, viabilizando tecnologicamente o ambiente de informações inteligentes para os gestores corporativos. A tecnologia informacional continua a se expandir e alguns recursos têm sido alocados para implementar novidades. Algumas dessas capacidades podem ser úteis no domínio do ambiente informacional atual, como acessar, armazenar e distribuir textos não-estruturados, áudio e vídeo, por exemplo.

A tecnologia da informação começou a revolucionar o projeto organizacional ao proporcionar alternativas à coordenação de atividades dentro da empresa. Sistemas de informação, arquiteturas comuns, bancos de dados compartilhados, ferramentas de apoio às decisões e sistemas especialistas facilitaram a coordenação do comportamento das pessoas usuárias de recursos de informática e responsáveis por controles diversos permitindo com isso a criação de unidades autônomas ligadas pela informação. Em se tratando de soluções e tecnologias que melhor viabilizem os sistemas de informações executivas, pode-se afirmar que o desafio associado à coleta de dados consiste na capacidade de reunir material potencialmente relevante e organiza-lo, bem como estruturar o fluxo dos dados de modo a transformá-los em informações úteis à elaboração da estratégia empresarial. Consideram-se como tais as informações que

dêem o devido suporte na definição destas estratégias, que evidenciem no que a empresa se diferencia em relação a seus concorrentes, que orientem com requinte de detalhes, que considerem característica específicas do ambiente externo, e mostrem claramente quais são os recursos requeridos do ambiente interno. Levando-se em conta estas observações, tem-se o intuito de obter objetividade materializada numa arquitetura de informações. Essa deve ser a orientação básica para a criação, com auxílio das tecnologias atuais disponíveis, de um sistema especialista para os administradores.

### 2.4.1- A ARQUITETURA DA INFORMAÇÃO

A arquitetura de informações é um conjunto de informações, modelos de dados, e toda a infra-estrutura tecnológica capaz de suportar os fluxos de informações em uma organização. Uma arquitetura da informação define qual a informação mais importante para a organização. Ela se torna o componente de informação de uma visão estratégica ou visão de informação. As organizações coletam, utilizam e armazenam uma enorme quantidade de informações e um dos grandes benefícios da definição de uma arquitetura de informações é a capacidade dos responsáveis pelo processo decisório de acessarem e analisarem grandes quantidades de dados em seus computadores, que podem ser obtidos sinteticamente ou detalhadamente, conforme a necessidade.

Segundo Silva Jr. (2000), uma grande parte dos conceitos abordados indicam que o uso da arquitetura de informação é muito mais adequado para identificar e classificar o tipo de informação disponível e onde encontrá-la, do que para tentar planejar o futuro, ou seja, o mapeamento das informações é um guia para o ambiente informacional presente e descreve não apenas a localização do informe, mas também quem é o responsável por ele, para que foi utilizado, a quem se destina e se está acessível. O benefício mais óbvio do mapeamento é que ele pode melhorar o acesso à informação. Entretanto seu maior benefício é de caráter organizacional.

De fato, a criação de uma arquitetura da informação bem definida, estabelecida de comum acordo entre as diversas áreas envolvidas no processo e gerenciada de forma coerente, permite que todas as áreas de interesse em uma empresa tenham a mesma diretriz e conduzam seus processos de acordo com uma padronização e utilizem a informação confiável para a tomada de decisões significativas. Recomenda-se que os principais objetivos centralizados no usuário devem estar abrigados numa arquitetura da informação, segundo algumas especificações, conforme Figura 4.

**OBJETIVOS DE UMA ARQUITETURA DA INFORMAÇÃO**

- Definir o espaço de informação da organização em termos de domínios de interesse de informações essenciais de fluxo de informação.
- Definir os limites críticos do espaço de informação da organização ( o

Figura 4 – Objetivos de uma Arquitetura da Informação
Fonte: Mcgee & Prusak (1994) *apud* Silva Jr. (2000, p.50).

A arquitetura da informação bem planejada e desenvolvida constitui uma série de ferramentas que adaptam os recursos às necessidades da informação. Quando um projeto é bem implementado, tem a característica de estruturar os dados em formatos, categorias e relações específicas e a arquitetura, vista desse modo, faz a ligação entre o comportamento das pessoas envolvidas, os processos, todo o pessoal técnico especializado e demais aspectos da empresa, tais como métodos administrativos, estrutura organizacional e espaço físico.

Segundo Silva Jr. (2000), um dos motivos que levam ao uso e implementação desta arquitetura vem do fato de que as informações normalmente encontram-se muito dispersas nas organizações e se originam de muitas e diferentes fontes, como também são utilizadas para finalidades variadas, ficando armazenadas em uma diversidade de meios e formatos. A dificuldade presente nas organizações para se acessar dados é um fato e, sendo este acesso tão difícil, não é de se estranhar que as empresas invistam milhões de dólares com a expansão da capacidade de armazenamento de dados que, muitas vezes estão duplicados em seus computadores servidores de rede.

Desta maneira, qualquer fornecedor de informação pode agregar valor àmesma ao torná-la mais acessível, sendo que a arquitetura informacional, ao conduzir o usuário ao local onde os dados se encontram, melhora consideravelmente a possibilidade de estes serem utilizados de maneira eficiente, e a informação já obtida pode ser mais facilmente reutilizada. Quando os usuários sabem que tipos de dados estão disponíveis, dificilmente comprarão ou criarão a mesma informação, fato que também ajuda a baixar os custos de aquisição e de tecnologia para armazenamento. Um número reduzido de organizações calcula seus custos e investimentos nesta área ou se preocupam com

estes detalhes. Assim, a maioria das empresas freqüentemente enfrentam problemas com informações redundantes, armazenadas nos servidores de dados. A arquitetura é uma articulação de visões que integram os desejos e os limites dos clientes dentro das possibilidades da engenharia. Ela poderá fornecer uma declaração da forma pela qual a organização encara o mundo e, sem dúvida, qualquer abordagem à arquitetura da informação deverá acomodar os diversos tipos de informação que os gerentes e executivos necessitam regularmente. Na atualidade, esta informação pode ser encontrada em bancos de dados, documentos e materiais publicados, sendo que ela existe tanto no interior quanto fora de uma organização e pode assumir praticamente qualquer forma, seja em papel, seja eletronicamente, ou uma conversa telefônica, etc.

Uma arquitetura da informação será flexível o bastante para abranger as que ainda estão por ser descobertas e a sua gramática estabelece e representa os fluxos de informação sob formas capazes de acrescentar valor. Ela poderá indicar as unidades e executivos que deveriam estar recebendo informação e não estão, e vice-versa. Ela fornece um mapa da forma pela qual a informação atua, para aperfeiçoar a eficácia organizacional. De um modo geral, focalizar a atenção nesta questão já traz um valor substancial à organização, pois a maneira pela qual a empresa organiza seus esforços pode ser uma fonte de grande vantagem competitiva, particularmente nas épocas em que aumenta o valor da flexibilidade, da adaptação e da administração da mudança. Uma observação importante é a de que "organização" refere-se a todos os vários sistemas, estruturas, processos de administração, estratégias etc., que constituem o modo de operação da empresa. A maioria das teorias modernas sobre organizações classifica como tarefa básica da estrutura organizacional o processamento da informação. Apesar da tecnologia da informação ter facilitado as tarefas de coleta, classificação e armazenamento de dados, é preciso ter o devido cuidado para não sobrecarregar os gestores com a proliferação de fontes e volumes de informações, sob pena de extrapolar os limites do uso destas pelos usuários. Embora a arquitetura da informação contenha uma orientação para focalizar o ambiente interno, há um ambiente de informação externo que precisa ser considerado e, desta maneira, a perspectiva arquitetônica também deve contemplar a complexidade e volatilidade das exigências do ambiente externo por meio de uma estrutura mais dinâmica e flexível do ambiente de informação. O modelo da Figura 5 representa todo o contexto que deverá abranger e preocupar o desenvolvedor da arquitetura de informações, para atender às necessidades dos gestores.

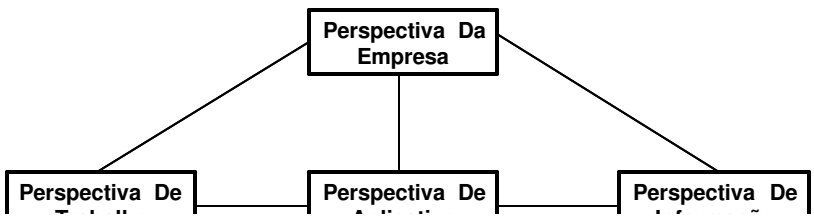


Figura 5 – As cinco perspectivas da arquitetura
Fonte: Tapscott (1997) *apud* Silva Jr. (2000, p.54).

Segundo Tapscott (1997) *apud* Silva Jr. (2000), analisando os modelos para arquitetura das empresas, verifica-se que modelam a empresa futura utilizando unidades lógicas de serviços para representar a empresa que sofreu um processo de reengenharia e esta perspectiva dá suporte ao princípio de que as empresas devem em primeiro lugar passar por esta reengenharia antes que os seus processos de trabalho sofram um segundo planejamento e novos aplicativos da tecnologia de informação sejam desenvolvidos. O modelo da empresa é apresentado como uma rede de funções de serviço interligando clientes e servidores internos e externos, sendo que as transações são compostas pelos fluxos de informações que percorrem caminhos de comunicação definidos entre tais funções de serviço para disparar atividades da empresa e interações adicionais. Desta forma, pode ser criado um modelo muito dinâmico da empresa que sofreu o processo de reengenharia.

Com referência à arquitetura do trabalho, as funções de serviço de reengenharia são modeladas utilizando-se as atividades de trabalho, os recursos humanos a ela associados –- as chamadas classes de usuários –-, os locais de trabalho e os recursos humanos a eles associados, inclusive informações, sendo que a meta dessa modelagem é a determinação do meio mais eficaz para dar suporte a tais atividades com a tecnologia da informação. Em complemento à teoria da reengenharia, a arquitetura do trabalho resulta na criação de modelos de processos de negócio, que são muito úteis para evidenciar o impacto da tecnologia de informação na natureza mutável do trabalho, inclusive evidenciando quem faz o quê, quando e com quais ferramentas da tecnologia de informação. Por conseguinte, como a perspectiva do trabalho é derivada do modelo da empresa que sofreu reengenharia, o mesmo ocorre com o modelo de informação da empresa e esta perspectiva de informação também fornece a perspectiva da engenharia de informação na arquitetura. Com o conhecimento destes fatos e compreendendo as funções de serviço básicas da empresa, os arquitetos da informação determinam as exigências fundamentais em termos de recursos de informação, representando tais

recursos na forma de um modelo de informação. Seguindo este raciocínio, os modelos de processos de empresas e os modelos de informação estão interligados pela perspectiva do aplicativo cuja meta é manter a maior proporção possível de informações da empresa em formatos que possam ser armazenados em bancos de dados existentes nos servidores de dados e acessados por meio de microcomputadores. Para que haja um perfeito sincronismo de ações entre necessidade de informação a ser obtida e utilizada para a tomada de decisão, os bancos de dados automatizados precisam ser criados, atualizados, acessados, administrados e eliminados por meio de aplicativos específicos. Estes aplicativos provêm apoio às atividades de trabalho dos processos do negócio, mediante o fornecimento de procedimentos automatizados e o gerenciamento do armazenamento e recuperação das informações que dão suporte às funções de serviços integrados da empresa, como também aos usuários associados a essas funções. Com relação à perspectiva da tecnologia, esta se interliga com o modelo de trabalho, por meio do fornecimento das plataformas de tecnologias necessárias ao cumprimento das necessidades, das diversas classes de usuários, em locais de trabalho identificados. Quanto a toda a equipe técnica dos arquitetos do trabalho e os da tecnologia, estes têm a responsabilidade por atender os requisitos básicos em termos de *workstations* (computadores com grande capacidade de processamento, robustez e de armazenamento de dados e que geralmente utilizam o Sistema Operacional Unix), e servidores, inclusive seus aspectos de funcionalidade, periféricos, portabilidade, funcionamento etc. A perspectiva de tecnologia, interliga-se também com os modelos de aplicativo diversos e informação. Os muitos tipos de aplicativos da tecnologia de informação exigem que diferentes tipos de tecnologia estejam integrados e sincronizados com o objetivo de dar suporte aos aplicativos de múltiplas funções, inclusive aos voltados para os processos decisórios, estratégicos e de vital importância para as empresas. Os profissionais que se enquadram no perfil dos arquitetos da tecnologia não apenas necessitam colocar estes aplicativos em plataformas apropriadas, como também resolver o uso que eles farão dos diversos bancos de dados. Todos os aplicativos de banco de dados têm como principal função viabilizar e disponibilizar rapidamente os insumos básicos ao processamento e geração de informações, porém não basta apenas disponibilizar informações. É preciso garantir a qualidade da informação, que ela seja íntegra, exata, precisa e segura. Desta maneira, a criação de uma arquitetura da informação, em que há consonância entre necessidades informativas dos usuários executivos e os atributos da estrutura da informação e suas inter-relações, bem como seu adequado gerenciamento, viabilizam o uso da informação pelas diversas partes envolvidas em todo o processo de gestão empresarial.

Segundo Silva Jr. (2000), um outro recurso também importante e agregado aos recursos essenciais de manipulação de banco de dados é a revolução tecnológica de distribuir e exibir informações, desencadeada pelo uso do *HTML* (Hypertext Markup Language), que permite a disposição de textos e imagens na *Internet.* Algumas partes de documentos podem ser conectadas a outros, relacionados ao primeiro, em qualquer lugar do mundo de forma rápida, confiável e segura. Várias arquiteturas baseadas na *Internet* começam a surgir também nas organizações como um desenvolvimento fascinante, utilizando recursos e padrões relativamente simples de formatar, buscar e capturar informações que podem florescer em uma complexa série de documentos. Um dos principais segredos do uso da *Internet* reside em sua simplicidade. A facilidade para se produzir e acessar as informações, seus conteúdos e a tecnologia não interfere no seu modo de usar e tem agregado tecnologias que permitem cada vez mais aos executivos acessarem informações gerenciais que contribuam no seu processo decisório estratégico, de qualquer parte do mundo em que o mesmo esteja trabalhando. A resolução de todas estas diversas interligações arquitetônicas e a opção tecnológica constitui o desafio da construção do modelo da arquitetura da informação adequada a cada organização.

## 2.5 O USO ESTRATÉGICO DE SISTEMAS DE INFORMAÇÕES GERENCIAIS

O conceito de informação é rico em detalhes e inicia um processo de complexidade a partir do instante em que o gerenciamento por meio de recursos computadorizados se faz presente, conforme breve comentário anterior. Na seqüência, ressalta-se os aspectos do uso estratégicos de sistemas de informações gerenciais e as suas implicações na sobrevivência das organizações.

Segundo relatado por Davenport (1998), ao invés de se concentrar na tecnologia, é conveniente se basear na maneira como as pessoas criam, distribuem, compreendem, utilizam e administram a informação. Em outras palavras, os administradores, nesta abordagem devem ter a conscientização de que:

- Toda a informação existente em uma organização não é facilmente arquivada em computadores, como também, toda a informação não é constituída apenas por dados digitais que possam ser manuseados por dispositivos informatizados;
- Quanto maior complexidade existir no modelo de informação e no modo de manuseio e aplicabilidade, menor será sua utilidade;
- A informação pode ter muitos significados em uma organização;

- A tecnologia é apenas um dos componentes do ambiente de informação e freqüentemente não se apresenta como meio adequado para operar mudanças.

O gerenciamento informacional pode ser visto como um processo formado por um conjunto estruturado de atividades que incluem o modo como as empresas obtêm, distribuem e usam a informação e o conhecimento, conforme a seqüência: determinação das exigências ➔ obtenção ➔ distribuição ➔ utilização.

Cada um dos elementos dessa seqüência pode ser definido da seguinte maneira:

- Determinação das exigências da informação: genericamente, uma grande parte dos livros sobre a tomada de decisões tentam desenvolver abordagens sistemáticas ao ato de se dar respostas, porém existem alguns fatos curiosos que chamam a atenção quanto a este detalhe. Para os japoneses, o elemento importante em uma decisão é definir a pergunta, ou seja, os passos fundamentais são decidir se existe necessidade de uma decisão, e a que ela se refere.
- Obtenção de informações: existe a necessidade de uma exploração eficaz, que é um fator essencial para qualquer processo de gerenciamento informacional, o qual depende de uma combinação de abordagens fundamentais, ou seja, a automatizada e a humana. Os sistemas de busca automática de dados tornam-se cada vez mais sofisticados, basta observar as novas ferramentas que surgem a todo instante na *World Wide Web* e, mesmo dentro da empresa, são várias as mudanças ocorrendo, mudando e gerando novas informações a serem administradas.
- Distribuição: o processo de distribuição está diretamente ligado ao modo como a informação é formatada e como é preparada dentro da instituição, pois toda a empresa possui dados inestimáveis que são fornecidos aos gerentes, no entanto poucas ou quase nenhuma das pessoas que precisam delas sabem onde se encontram ou como acessá-las.
- Utilização: quanto à utilização da informação, em muitas empresas as políticas de gerenciamento lembram a maneira como se trata de doenças, pois, são gastas grandes quantidades de recursos para desenvolver medicamentos de alta tecnologia, porém os pacientes não os tomam, ou não seguem a receita médica de maneira adequada. Como um medicamento que não é tomado, a informação de nada servirá até que seja utilizada, ou seja, o uso é a etapa final de todo processo de gerenciamento informacional, mas até mesmo pesquisadores e gerentes da área o têm ignorado.

Conforme as citações anteriores, é importante desenvolver uma cultura e comportamentos em relação à informação, as pessoas devem mudar a maneira como pensam e utilizam a informação e, como objetivo maior, construir uma cultura informacional, que é a meta principal. E, em se tratando do uso da informação disponível, é importante ressaltar a necessidade de procurar manter critérios de segurança, com o intuito de se evitar dano ou perda de dados importantes. Em diversos setores, líderes e gerentes de todos os níveis descobriram, pesarosos, que a dimensão comportamental e cultural da mudança com freqüência é a mais difícil de se obter. As organizações que procuram aperfeiçoar a qualidade, buscar a excelência dos fluxos da informação, redefinir processos ou aumentar a satisfação do cliente, percebem que os processos aparentemente mais fáceis são, na verdade, as mais difíceis. Numa comparação, o planejamento de novos processos de trabalho, novas estruturas organizacionais, novas estratégias muitas vezes parecem ação simples e sem importância, quando comparado às alterações diárias de comportamentos e de atitudes.

Segundo Silva Jr. (2000) a administração bem-sucedida do conhecimento sempre ocorre por intermédio de uma combinação entre mudanças tecnológicas e comportamentais. Entretanto, enquanto mudanças tecnológicas recebem muita atenção por parte da alta administração e dos desenvolvedores de *SIG* (Sistemas de Informações Gerenciais), as mudanças comportamentais são relegadas a um segundo plano. Assim, muito do esforço investido no desenvolvimento e implantação desses sistemas acaba sendo pouco eficaz. Alguns dos motivos normalmente apontados para isso são:

- Um dos fatores é a mudança de comportamento que quase nunca é um dos objetivos das arquiteturas informacionais. No máximo, sua finalidade pode ser aumentar a percepção, por parte dos envolvidos no processo, ou seja, funcionários e gerentes, para a quantidade existente e os custos de dados redundantes, mas a percepção sozinha não pode efetuar qualquer mudança.
- Todo o conteúdo das arquiteturas informacionais não tem a intenção de conduzir a alterações de comportamento, pois normalmente é incompreensível não apenas para os não-técnicos, como também às vezes para os técnicos e existem poucas ferramentas disponíveis que possam contribuir para as discussões centradas nos clientes e para as negociações sobre as exigências e as estruturas da informação.
- Outro fator importante é a crença de que o processo de desenvolver a arquitetura informacional inibe as mudanças, sendo que todos os responsáveis depositários da informação não participam inteiramente deste desenvolvimento

e raramente entendem o que está em jogo na arquitetura informacional, portanto não se comprometem com ela quando implementada.

Analisando as tendências para o futuro, verifica-se o surgimento de um novo modelo de arquitetura de informações executivas, com maior grau de qualificação, a partir da evolução cultural do uso e tratamento das informações gerenciais. Dentro deste novo modelo destacam-se alguns atributos e tarefas chaves da informação, como mostrado na tabela abaixo Tabela 2:

Tabela 2 – Tarefas chaves da informação

| | TAREFAS | | | |
|---|---|---|---|---|
| **ATRIBUTOS** | **CONDENSAÇÃO** | **CONTEXTUALIZAÇÃO** | **APRESENTAÇÃO** | **MEIO** |
| Exatidão | ♦ | | | |
| Oportunidade | ♦ | ♦ | | |
| Acessibilidade | ♦ | ♦ | ♦ | ♦ |
| Envolvimento | ♦ | ♦ | ♦ | ♦ |
| Aplicabilidade | ♦ | ♦ | | |
| Escassez | ♦ | | | |

Fonte: Davenport, Thomas H., Prusak, Laurence (1998, p.156).

Com relação aos atributos da informação, segundo Davenport (1998), temos:

Exatidão: é um dos princípios mais básicos existentes com relação a uma informação. Para ser percebida como valiosa e utilizada com confiança, a informação dever ser exata. No nível mais primário, exatidão significa ausência de erros simples na transcrição, na coleta e na agregação de dados.

Oportunidade: a informação só é útil se estiver atualizada, disponível e livre de qualquer pendência de alterações. A definição de oportunidade envolve sempre uma situação específica. Assim, para o planejamento estratégico, uma informação gerada há muitos anos ainda pode ser útil, ao se levar em conta a projeção e tendências.

Acessibilidade: a informação deve estar disponível e acessível a todas as pessoas e usuários da organização que tenham permissão para usá-la. Caso a obtenção da informação seja difícil ou muito demorada, pode não valer a pena procurá-la ou dispender tempo na tentativa de localização. Nos atuais ambientes computadorizados, o acesso normalmente está relacionado à conectividade ou à capacidade de um computador em estabelecer conexão com outro para obter dados em uma rede. Nesses casos, os critérios e procedimentos de segurança da informação tornam-se altamente relevantes.

Envolvimento: independentemente do seu valor ou importância, a informação deve ser apresentada como útil, pois o impacto da informação é a medida de como ela pode envolver o usuário potencial por meio do formato, do meio utilizado, da apresentação e de outros métodos.

Aplicabilidade: semelhante ao item anterior, a informação deve ser útil e ter um objetivo prático. Ela deve representar resultados ou valores que possam ser trabalhados para se chegar a conclusões estratégicas.

Escassez: tendo em vista que a informação normalmente significa poder e que ambientes informacionais normalmente são de cunho político, conclui-se que a raridade de uma informação pode ter grande influência em seu valor.

Quanto às tarefas chaves de um sistema de gerenciamento da informação podemos definir:

1. Condensação: para o armazenamento da informação em meio magnético ou em outro dispositivo qualquer, existe o fator custo envolvido e sendo assim, a informação seria mais útil se todos os que a gerenciam tivessem o hábito de escrever contos, pois o desafio fundamental para um contista é manter a história curta e concisa. De maneira similar, gerentes informacionais devem incansavelmente cortar o obsoleto, o irrelevante, a imprecisão dos principais meios de comunicação e fontes.

2. Contextualização: o conceito de se contextualizar informações é o meio mais poderoso para aumentar tanto o interesse do público quanto à propensão deste em interagir com a informação de uma determinada maneira. Contextualizar geralmente implica detalhar a fonte e comparar a informação disponível com o histórico que a envolve.

3. Apresentação: este conceito deve ser uma das principais preocupações em se adequar o estilo da informação, pois melhorar a apresentação da informação é uma das chaves para lhe agregar valor. Uma apresentação que cause impacto positivo faz com que a informação seja respeitada, ao passo que uma apresentação pobre ou pouco atraente só pode causar rejeição.

4. Meio: a informação quando veiculada por meio coerente com o propósito desejado torna-se mais convincente. Atualmente, há a disposição uma ampla variedade de meios de comunicação: apresentação em vídeo, videoconferência, apresentação de slides, relatórios em papel, comunicação interpessoal, ligações telefônicas, fax, serviço de correio interno e externo e correio eletrônico.

Com referência ao uso estratégico de sistemas de informações gerenciais, é imprescindível que as empresas dediquem esforços contínuos no que concerne a sua modernização e agilização, para absorver os impactos do ambiente e, ao mesmo tempo,

exercer um poder de pressão sobre ele. Neste contexto, a informação deve desempenhar seu papel enquanto elo essencial de funcionamento do todo, pois a empresa que possuir informações compatíveis com as exigências desse ambientes, altamente competitivo, certamente, terá em mãos um instrumento decisivo para o sucesso. Quando se trabalha com o gerenciamento de informações, é importante destacar algum sinal útil na tomada de decisões. Quanto ao uso estratégico de sistemas de informações executivos, pode-se mencionar dois tipos de sinais:

(1) Adverte sobre a existência de um problema, por exemplo, o declínio no faturamento é um nítido sinal de perigo; e

(2) Diagnóstico que identifica o problema, por exemplo, o tempo gasto para o atendimento de clientes pode ser uma resposta àqueda nas vendas.

A empresa que não tem informações confiáveis, seguras e ágeis, por meio de sistemas de informações executivas eficientes, para fomentar suas decisões estratégicas e a execução das mesmas, estará em desvantagem em relação à outra, do mesmo ambiente, que consegue parametrizar, em um tempo mínimo, suas alternativas de decisões, além de mensurar e reportar o resultado decorrente da decisão tomada. Assim, o desenvolvimento de Sistemas de Informações Gerenciais capazes de garantir a concretização das funções básicas da informação dentro da empresa torna-se fator de vantagem competitiva e de sobrevivência da empresa no mercado. Entretanto, hoje em dia, dada a complexidade crescente dos mercados e a rapidez das mudanças do meio ambiente das empresas, a implementação de uma estratégia de gerenciamento da informação passa necessariamente pela informatização. É nesse contexto que a segurança da informação ganha importância. Se os riscos decorrentes de uma má política de segurança (ou simplesmente da ausência de uma) já eram significativos no passado, eles se tornam críticos na era das comunicações via *Internet*.

Segundo Caruso (1999), na medida em que as atividades administrativas dos negócios e os controles de processos em indústrias tornam-se mais dependentes da Informática, mais vulneráveis ficam as informações armazenadas nas organizações a crimes e fraudes cometidas com o uso dos recursos computacionais. A capacidade de operação declina em 90%, em média, após a ocorrência de um desastre completo no Centro de Processamento de Dados. Conforme estatísticas mundiais, mais de três quartos das empresas que sofrem um sério desastre em suas instalações de processamento de informações, deixam de existir ou acabam sendo adquiridas por outras. Ainda que não se deva chegar ao exagero de tratar a segurança da informação como um segredo militar ou diplomático, não se deve deixá-la ao acaso. Mais cedo ou mais tarde, surge alguém que não somente conhece os meios técnicos para se apossar

das informações, como também para lucrar com elas. Dessa maneira, o assunto sobre Segurança da Informação, Segurança em Rede de Computadores e Segurança do Correio eletrônico são fatores de extrema importância para a sobrevivência das organizações. Tais temas serão, assim, abordados nos capítulos seguintes.

# CAPÍTULO III

# GENERALIDADES SOBRE A SEGURANÇA DA INFORMAÇÃO

*"Segurança é prevenir que atacantes alcancem seus objetivos por meio de acessos não autorizados ou uso não autorizado de computadores e redes".* Hitech(1998).

A informação protegida e disponível garante uma maior credibilidade, integridade e confiança para a tomada de decisão estratégica nas empresas e atualmente, mais pessoas buscam cada vez mais informações, os *Hackers* e os vírus existentes estão ficando mais sofisticados a cada novo dia e a criação de leis adaptadas a estas novas formas de interação por meio das redes mundiais de computadores exige maior conhecimento sobre a tecnologia informatizada.

## 3.1 BREVE HISTÓRICO SOBRE SEGURANÇA

Segundo Caruso (1999), o bem de maior valor para uma empresa pode não ser exatamente o que é produzido em sua linha de produção, mas sim as informações relacionadas a este bem de consumo ou serviço. Durante toda a História da Humanidade,

desde a antiguidade, o Homem sempre procurou proteger ou controlar as informações que considerava importantes, os registro de suas descobertas e os apontamentos relativos às pesquisas desenvolvidas. Inicialmente as informações eram armazenadas na memória das pessoas e passavam de pai para filho. Somente após a criação dos primeiros alfabetos iniciou-se um processo de maior preocupação em registrar e armazenar o conhecimento, que era transcrito – em uma codificação própria – para paredes das habitações humanas. Nos dois últimos séculos é que as informações tiveram uma função vital para as organizações humanas na luta contra seus concorrentes. Devido aos materiais pouco apropriados e à precária tecnologia utilizada para o armazenamento das informações, o controle e a disseminação do conhecimento eram restritos a uma pequena parcela da população, que detinha o poder econômico e político da sociedade na época. Com o advento das placas de barro dos Sumérios, dos papiros, dos Egípcios, e do pergaminho, as informações passaram a ser registradas em meios portáveis. O Imperador Romano Júlio César criou um sistema rudimentar de criptografia a fim de garantir o sigilo das informações que seus mensageiros transportavam. Por meio de uma tabela de conversão alfabética a mensagem era reescrita de forma ilegível para quem desconhecesse a fórmula correta de decriptografá-la. Desta forma, mesmo que a mensagem caísse em mãos inimigas, dificilmente seria decifrada. Além disso, caso o destinatário recebesse uma mensagem não cifrada, saberia que era falsa, não proveniente do Imperador. Este exemplo simples nos mostra as grandes preocupações básicas: garantir que informações importantes não fossem desviadas para pessoas não autorizadas e assegurar a autenticidade da informação recebida.

Com a chegada da imprensa, que promoveu uma alfabetização mais ampla, a informação passou a ser divulgada, a circular e chegar a locais longínquos. A evolução do comércio e o nascimento das empresas fabricantes de produtos para a sociedade impulsionaram a preocupação com relação à divulgação das informações confidenciais. Esta preocupação se faz presente hoje em todas as empresas, com o intuito de conseguir proteger as informações corporativas contra a sua perda ou dano. Não existe organização Humana atualmente que não seja dependente da Informática. As organizações ao longo de sua existência concentraram uma grande quantidade de informações importantes sobre *Marketing* (área ou processo da empresa com enfoque comercial dos produtos para vendas e promoções), cadastro de clientes, políticas estratégicas relacionadas com seus processos de produção e de negócios, tudo em um único local físico e restrito, onde o meio de registro é, simultaneamente, o meio de transmissão, armazenamento, acesso e divulgação das informações. As informações são

armazenadas em meios eletrônicos e magnéticos recebendo o nome de Dado. Esta característica acarreta para as organizações em geral um sério problema com relação às pessoas, pois desperta nas mesmas o desafio de tentar conseguir o acesso às informações com ou sem as devidas permissões. Como exemplo temos os cadastros de bancos, cartões de crédito, cartórios e lojas. Uma grande parte destes dados são confidenciais e sigilosos por força de diretriz legal, ou por considerações estratégicas, que demonstram ou controlam a vida econômica de clientes, que podem vir a sofrer danos caso sejam levadas a público. São de um valor inestimável não somente para a organização que as gerou, como também para os concorrentes e, mesmo que não sejam sigilosas, estão relacionadas com atividades diárias e relacionadas ao desempenho das empresas que sem elas poderiam se encontrar em sérias dificuldades. As organizações têm por tradição não dedicar a mesma atenção à proteção dos seus ativos de informação, como o fazem a seus ativos patrimoniais e financeiros. Ainda assim, a informação envolve os três fatores de produção tradicional: capital, mão-de-obra e processos que geram ativos como produtos e bens. Desta maneira, mesmo que as informações não recebam o mesmo tratamento físico-contábil que os outros ativos, do ponto de vista do negócio, elas também são ativos da empresa e devem ser protegidas. Esta proteção é necessária tanto para os dados armazenados como também para os meios de suporte, ou seja, para todo o ambiente de informações.

### 3.2 A INFORMAÇÃO ARMAZENADA E CENTRALIZADA PELAS EMPRESAS

Segundo Caruso (1999), quando as organizações decidiram centralizar dentro de suas dependências físicas todo o armazenamento das informações pertinentes ao seu negócio, iniciou-se o processo de aquisição de equipamentos – computadores – que pudessem prover esta necessidade. Os fabricantes desenvolveram seus computadores, os *Mainframes* (sistema de computador de grande porte que pode abrigar software abrangente, vários periféricos e uma rede de computadores com múltiplos usuários), e uma infra-estrutura física, de *Hardware* e *Software* e sistemáticas de trabalho, como manutenção preventiva, rotinas de *Back-up* (processo de se executar cópias de segurança de dados em discos ou fitas magnéticas), e *Restore* (processo de se executar o retorno dos dados gravados em cópias de segurança de dados em discos ou fitas magnéticas), salas isoladas e protegidas, com ar-condicionado independente, redundante de alta capacidade e potência, alarmes, linhas telefônicas e com proteção contra incêndio, no sentido de dar segurança e credibilidade às organizações, na certeza de que não haveria uma maneira da informação ser extraída de seus dispositivos sem

que houvesse intervenção humana. Cada profissional era altamente treinado tecnicamente e preparado para qualquer emergência até que um especialista do fabricante chegasse para resolver o problema, ou seja, somente as pessoas de confiança da organização tinham acesso às dependências onde as máquinas estavam instaladas. Esta era a filosofia dos antigos *CPD*, que mantinham todo um aparato tecnológico de controle de acesso às suas dependências com o intuito de manter a guarda e o sigilo das informações.

### 3.2.1 A PROPRIEDADE E A GUARDA DA INFORMAÇÃO

Segundo Caruso (1999), o conceito de propriedade da informação está diretamente ligado aos ativos de informações da empresa e às pessoas que delas fazem uso no desempenho de suas funções, normalmente os seus criadores ou gestores. O termo custódia se refere aos responsáveis pela guarda de um ativo de propriedade de terceiros. Em Informática está relacionada às pessoas que têm a responsabilidade pela guarda, manutenção da integridade e processamento das informações armazenadas pelas outras áreas da empresa. Geralmente, depois de recebida a custódia do proprietário, ela não pode ser delegada. Somente o proprietário ou a pessoa expressamente autorizada por ele pode transferi-la a outrem. Isto implica no fato de que uma vez concedida a custódia, ela tem que ser exercida diretamente pelo receptor e por mais ninguém. A custódia implica também na responsabilidade do receptor quanto à integridade dos ativos custodiados, contribuindo para a segurança da informação no processo de armazenamento e guarda desta. Esta guarda inclui sistemáticas de controle de acesso com a necessidade de implementação de *hardware* e *software*.

### 3.2.2 O CONTROLE DE ACESSO

Segundo Soares et al. (1995), o processo de informatização gerou algumas conseqüências, como a preocupação com a Segurança de Acesso ou o Controle de Acesso às informações armazenadas e guardadas nas empresas. O receio de se perder informações importantes que pudessem chegar até um concorrente e que deixassem a empresa em dificuldades, incentivou a criação de mecanismos de controle que pudessem minimizar o acesso de pessoas não autorizadas às dependências onde os computadores principais estivessem localizados. A preocupação com a saída da informação se restringia apenas a estas salas, pois não havia meio de os usuários finais extraírem informações por meio dos terminais simples, de consulta (denominados terminais "burros"), que estavam disponíveis e espalhados pela empresa nos diversos

departamentos. Estes terminais funcionavam apenas como entrada e saída de dados digitados pelo seu teclado. Sendo assim, o Controle de Acesso foi dividido em Controle de Acesso Físico e Controle de Acesso Lógico.

#### 3.2.2.1 O CONTROLE DE ACESSO FÍSICO

Segundo Soares et al. (1995), o Controle de acesso físico é caracterizado pela posse ou pelo uso que se faz de um determinado recurso. O objeto sujeito ao controle é tangível, ou seja, em uma determinada área somente as pessoas que tenham permissão de acesso poderão adentrar. Apesar de mais perceptível e deixar a impressão de ser sujeito a maiores riscos que o Controle de Acesso Lógico, ele é, na realidade, menos sujeito a estes riscos. O controle em si, por outro lado, pode ser mais difícil, pois depende da intervenção humana. Existem equipamentos específicos de bloqueio físico onde a identificação se faz por meio de senhas, cartões codificados, impressões digitais e com auxílio de câmeras de vídeo. As ferramentas de segurança são os dispositivos utilizados para proteger e controlar o acesso de pessoas às informações das corporações. Com relação aos aspectos físicos, existem dispositivos eletrônicos instalados nos locais onde estão armazenadas as informações e sobre os aspectos lógicos, são os sistemas compostos por programas que executam o controle do acesso às informações. Estes sistemas são complementados pelos outros dispositivos já citados, tais como, cartões de identificação, voz, imagem da íris, planta da mão, impressões digitais etc.

#### 3.2.2.2 O CONTROLE DE ACESSO LÓGICO

Segundo Soares et al. (1995), o Controle de acesso lógico se refere aos acessos que os indivíduos têm a aplicações residentes em ambientes informatizados. Necessita de algumas ferramentas "invisíveis" aos olhos das pessoas externas à área de Informática, que tomam ciência da existência das mesmas quando têm seu acesso barrado pelo sistema de controle. Este controle de acesso lógico está relacionado com permissões de acesso, atividades de auditoria e controle, normalmente utilizados em grandes organizações.

As senhas são consideradas como os mecanismos de controle de acesso mais antigos utilizados pelo homem para impedir acessos indevidos e não autorizados. Atualmente ainda são bastante utilizadas, apesar da fragilidade e dos riscos existentes em se passá-las para outros usuários. Os equipamentos de leitura, identificação e autenticação à medida que estão evoluindo tendem a substituir as senhas constituídas por combinações de letras e números por características físicas dos usuários, ou seja,

impressão digital, planta da mão, imagem da íris, voz etc. As *chave*s de acesso *ou* identificação são códigos eletrônicos únicos atribuídos a cada usuário. Cada *chave* de acesso é destinada a autenticar a identidade do indivíduo que a possui e está diretamente associada a cada recurso do sistema que o perfil do seu usuário tenha o direito de acessar, o que responsabiliza individualmente cada usuário. Um outro recurso também utilizado é a lista de acessos, que é constituída por uma tabela onde constam o tipo e o nome do recurso de informática ao qual são associadas as identificações dos usuários e os tipos de transações e operações permitidas aos mesmos.

Estas *chave*s podem associar direitos de leitura, gravação, alteração, exclusão, eliminação ou execução de uma informação. Os privilégios são as permissões concedidas aos usuários para acessar determinadas informações armazenadas e normalmente, quanto maiores os privilégios de acesso, maior o grau hierárquico do seu detentor. A segurança da informação passou a ser um fator de preocupação e prioridade para as organizações.

### 3.3 A SEGURANÇA DA INFORMAÇÃO

Segundo Soares et al. (1995), a partir do momento em que as corporações perceberam a necessidade de implementação de tecnologias de comunicação mais ágeis, com maiores recursos tecnológicos e menores custo, iniciaram o processo de desativação da antiga estrutura dos *Mainframes* e partiram para a implementação da tecnologia de Redes de Computadores, como uma nova solução de comunicação entre seus computadores. Esta decisão e o novo ambiente que ela gerou trouxeram melhorias incontestáveis, mas trouxeram também outras preocupações e perigos praticamente inexistentes na situação anterior. Preocupações e perigos relacionados ao acesso por pessoas não autorizadas às informações armazenadas nos servidores de dados. Na tecnologia anterior, os terminais "burros" somente permitiam o acesso às telas dos sistemas que estavam disponíveis para trabalho, enquanto que nas Redes de Computadores, cada microcomputador conectado tem a característica de poder não apenas inserir dados no ambiente interno da rede, como também de extrair dados da mesma, por meio de disquetes, fitas magnéticas e *CD-ROM*.

A informação armazenada em meio magnético é bastante frágil e sujeita a ataques de pessoas mal intencionadas, com o intuito de danificá-la, destruí-la ou modificá-la. Estes ataques podem ser iniciados internamente à corporação ou externamente por um *Hacker*.

Segundo Akiyama (1999), a segurança relacionada à Informática trata da garantia da integridade, confidencialidade, disponibilidade e legalidade das informações armazenadas, como também da infra-estrutura de rede nas empresas. Toda pessoa ou usuário interno que inicia um processo de ataque à informação armazenada em computadores, normalmente irá executar este ataque pelo menos uma segunda vez. Um *Hacker* jamais desiste de atingir seus objetivos no sentido de concretizar uma invasão. Quando não consegue, inicia um processo de novas tentativas enviando arquivos contaminados com vírus de computador destinados à fonte de ataque, para que estes, no destinatário, possam enviar-lhe informações importantes para uma nova tentativa de invasão com maior possibilidade de sucesso.

### 3.3.1 A SEGURANÇA LÓGICA

A segurança lógica está relacionada à integridade da informação, seu correto manuseio e à certeza de que é única e correta. Como a informação está sempre trafegando em rede, adentrando a empresa por meio de mensagens de correio eletrônico, armazenada em microcomputadores e servidores, é necessário a implementação de ferramentas, procedimentos e regras, *hardware* e *software,* que promovam uma garantia de que esta informação estará protegida. Segundo Penteado e Marino (2000), quando se trata de segurança de sistemas e de dados dentro das corporações, muitas empresas têm boas intenções, mas os ataques de *Hackers* e outros tipos de problemas continuam a exigir investimentos e atenção. Os ataques de vírus e as fraudes que são capazes de paralisar o trabalho em uma empresa estão acumulando um considerável somatório de divisas que estão preocupando os dirigentes e acionistas. Cada paralisação de sistemas representa uma significativa perda para os negócios. Garantir a segurança das redes, dos dados contidos nos microcomputadores móveis e das operações de comércio eletrônico é uma tarefa dispendiosa, tanto em termos de capital como também de trabalho especializado. As equipes de Tecnologia da Informação estão sendo solicitadas a implementar um número cada vez maior de aplicativos de segurança que, por sua vez, são muito complexos. A preocupação com relação ao correio eletrônico, objeto deste trabalho, também está cada vez mais acentuada, pois muitos usuários utilizam esta ferramenta para trabalho e disseminam vírus de computador alojado em arquivo de dados, muitas vezes sem ter conhecimento da contaminação.

Vírus de computadores são programas desenvolvidos com o objetivo de provocar danos, perdas de informação ou simplesmente para congestionar o tráfego de mensagens em uma rede de microcomputadores. Existe uma infinidade de tipos de vírus

atualmente espalhados pela *Internet*, via mensagens de correio eletrônico, nos microcomputadores residenciais, nas universidades, escolas diversas e empresas em geral. Para combater esses vírus, foram criados outros softwares que são capazes de identificar, classificar e destruir programas de vírus. Estes programas são denominados antivírus e, a partir do instante em que são instalados nos servidores ou no microcomputador de trabalho, tornam-se residentes na memória destas máquinas e monitoram todos os arquivos que são manipulados nas mesmas. Quando algum arquivo contaminado com vírus é detectado, automaticamente é iniciado um processo de limpeza e eliminação do vírus do arquivo pelos programas antivírus. Este processo visa assegurar que a informação não seja danificada por ataques de vírus de computador, tendo em vista que alguns vírus podem se multiplicar, mudar de comportamento durante sua ação causando enormes prejuízos aos dados armazenados. Todo o cuidado, precaução e Política de Segurança implementada tem a finalidade de procurar garantir que a segurança da informação seja mantida, que os dados armazenados nos computadores sejam confiáveis e estejam disponíveis para uso.

### 3.3.2 ASPECTOS DE SEGURANÇA

Segundo Hitech (1998), no processo de análise das variáveis de segurança em uma empresa, é necessário analisar todos os aspectos que estejam relacionados ao problema, que podem ser divididos em três grupos: Físico, Sistema e Humano. O item Físico aborda tudo o que esteja relacionado aos equipamentos, *hardware* e ao ambiente onde estes estejam localizados. Este sistema inclui a prevenção contra falhas de sistemas externos, rede elétrica, incêndios, encanamentos, gases, etc. O sistema abrange todos os sistemas operacionais e aplicativos diversos, os "*bugs*" (nome dado a um problema ou falha em um software, geralmente desenvolvido e comercializado por um fabricante especializado), e problemas de indisponibilidade. O aspecto humano trata das pessoas que utilizam o sistema, seja internamente ou externamente à organização, abordando a prevenção contra erros na interação com os níveis de Sistema ou Físico, e a indisponibilidade de pessoas importantes ao funcionamento de todo o processo (por motivo de estar de férias, doença, em greve ou de morte).

Segundo Americano (2000), a enorme corrida para implementação dos recursos de comércio eletrônico na *Internet*, a partir de Janeiro de 2000, refletiu diretamente no mercado de tecnologia, culminando com uma busca por padrões de segurança da informação adequados aos novos cenários tecnológicos. Isso já se transformou na

principal preocupação dos setores de Tecnologia da Informação, por se tratar de um assunto cada vez mais estratégico para as empresas.

A segurança se transformou em um meio efetivo para viabilizar os negócios das empresas, tendo em vista que o comércio eletrônico depende de confidencialidade, integridade, disponibilidade e confiabilidade da informação. Em uma pesquisa efetuada pela revista Network Computing Brasil (2000), dos 170 dirigentes de empresas que foram entrevistados, oriundos de diversos setores da indústria, 34% dão prioridade máxima para a questão da segurança em Informática. Uma grande parte dos consultores de segurança da informação são unânimes em afirmar que antes de se implantar qualquer infra-estrutura de proteção, deve haver um estudo detalhado das necessidades e vulnerabilidades da empresa e de seu ambiente, e as empresas estão adotando um caminho inverso.

As empresas têm, na realidade, uma grande dificuldade em classificar as informações em suas redes que necessitam de proteção, com um agravante de que 58% das corporações não dispõem de padrões regulares definidos em uma Política de Segurança. A principal causa para esta inversão pode ser a ansiedade do mercado digital, pois as empresas tiveram que optar entre dois caminhos distintos, o de adiar o processo de implementação dos recursos de *Internet*, com o intuito de ganhar tempo para perceber as fragilidades do ambiente, porém pagando um valor alto por perderem posições no mercado, ou saírem à frente – no pioneirismo – correndo o risco de errar pela falta de experiência, apostando em uma tecnologia nova sem exemplos para seguir. Como solução para este impasse, algumas empresas optaram por terceirizar algumas fases do processo de segurança até que seus funcionários responsáveis pelo projeto adquirissem a cultura necessária. Esta atitude foi positiva, pois liberou parte dos profissionais que estariam dedicados aos assuntos relacionados com a segurança para trabalhar em projetos do negócio das corporações.

Segundo Penteado (1999), uma pesquisa realizada pela revista Informationweek em conjunto com a consultoria PricewaterhouseCooper em 49 países, revelou que as empresas brasileiras já iniciaram um trabalho sério com relação a segurança da informação e dois em cada três diretores ou profissionais de Tecnologia da Informação brasileiros estão considerando o assunto com alta prioridade. Os bancos são os únicos a considerar o assunto como prioridade absoluta, devido à natureza de suas atividades e a regulamentação do setor. De acordo com esse estudo, quase dois terços das empresas participantes da pesquisa foram atacadas por vírus de computador nos últimos anos.

Em conjunto com os vírus, várias tentativas de entrada nos sistemas de telefonia, manipulação de software e ataques à integridade dos dados foram os principais

problemas enfrentados pelas empresas, que somados provocaram uma paralisação 14% maior em 1998 que no ano de 1997. Quase 60% das companhias brasileiras paralisaram suas atividades de informática por pelo menos quatro horas devido a problemas em seus sistemas de segurança, sendo que os principais responsáveis foram funcionários ou ex-funcionários das empresas.

Realmente os vírus não são o principal problema das organizações, apesar de terem sido responsáveis por 64% dos ataques deflagrados às empresas em 1998. A utilização de *Firewalls* (sistemática que promove a segurança em rede por meio de *software* e *hardware*), é praticada atualmente por 76% das empresas pesquisadas e, no caso do Brasil, esta ferramenta está presente em 49% das empresas. Há, porém, uma deficiência no gerenciamento dos *Firewalls* instalados, que poderiam apresentar relatórios mais exatos e com maior nível de detalhes do que atualmente, ou seja, uma grande parte das empresas têm o produto, mas falta capacitação técnica para saber utilizá-lo em sua total plenitude.

#### 3.3.2.1 *FIREWALL*

Segundo Soares et al. (1995), *Firewalls* são dispositivos, ou grupos de dispositivos, colocados entre uma rede segura (rede interna de uma empresa) e uma rede não segura (*Internet*), com o objetivo de autenticar usuários para utilizarem a rede interna. São também conhecidos como paredes corta-fogo. Existem três tipos principais:

- O primeiro tipo efetua uma filtragem de pacotes, analisando os endereços de origem e destino, e descartando o tráfego indesejado. São indicados para empresas que utilizam apenas os serviços de *FTP* (File Transfer Protocol, um sistema de acesso a diretórios e cópia de arquivos em rede), e correio eletrônico. Todavia, são de difícil configuração e seus esquemas de autenticações são menos sofisticados.
- O segundo tipo é o *Gateway* (*hardware* que permite a interligação entre duas redes de dados), composto por implementações de *software* que realizam vários procedimentos para tentar bloquear intrusos e usam um agente procurador para autenticar e filtrar as transações. Isto diminui o desempenho dos aplicativos da rede, visto que o agente é acionado em qualquer transação entre as redes.
- O terceiro tipo combina os dois anteriores, filtrando pacotes antes de inspecioná-los por *software*.

O *Firewall*, sozinho, não garante a segurança, mas é uma ferramenta absolutamente necessária. Ele controla o acesso entre uma, duas ou mais redes, como

também para uma única máquina e funcionando como uma espécie de barreira contra intrusos. Ao detectar tentativas sucessivas e frustradas de acesso àrede a partir de uma estação de trabalho ou de um *notebook* (computador portátil), o *firewall* faz soar o alarme para o administrador da rede e, dependendo da configuração, pode barrar o intruso por espaços de tempo determinados. É como se alguém, de posse do seu cartão de banco, tentasse tirar dinheiro do caixa eletrônico e errasse a senha uma, duas, três vezes. No caso dos caixas, o cartão é recolhido automaticamente. Já o *firewall* pode ser configurado para negar o acesso por uma hora ou por 15 minutos.

#### 3.3.2.2 DETECTOR DE INVASÃO

Um outro produto também em uso é o Detector de Invasões, também conhecido como IDS (Intrusion Detection Systems), que identifica e inibe a tentativa de invasão por pessoas não autorizadas ao sistema. Segundo Penteado (1999), no Brasil cerca de 37% das empresas entrevistadas já utilizam este recurso de proteção e segurança.

#### 3.3.2.3 OUTRAS TÉCNICAS DE SEGURANÇA

Segundo Penteado (1999), o uso de Senhas se faz presente em 71% das empresas pesquisadas. Um total de 55% das empresas no Brasil não utilizam qualquer tipo de recurso de Criptografia (processo pelo qual um arquivo ou informação é codificado para armazenamento ou envio por correio eletrônico). Apenas 16% utilizam *chave*s criptográficas secretas e somente 6% utilizam Criptografia por meio de *Chave* Pública. A implementação desse recurso tem se intensificado devido à sua evolução, tornando-se mais fácil de usar e mais efetivo, não necessitando um grande tempo dos funcionários de Informática para configurá-los. A pesquisa revelou também que mais de 60% dos entrevistados no Brasil adotaram a conscientização dos usuários sobre os cuidados que se devem tomar com relação àsegurança para minimizar os problemas.

### 3.3.3 SEGURANÇA EM REDES DE COMPUTADORES

É importante ressaltar que todo o processo de implementação de critérios de segurança em uma rede de dados de uma organização está calcado em tecnologia de *hardware*, *software*, dispositivos físicos, modelos e diversos recursos adicionais que proporcionam esta segurança. Segundo Soares et al. (1995), uma rede de computadores é uma solução adotada e implementada baseada em pesquisas, modelos, padrões e testes exaustivos. Neste trabalho estarão sendo abordados os recursos de implementações tecnológicas do modelo de interconexão de sistemas entre computadores propostos pelas normas OSI / I.S.O Trata-se da organização internacional

denominada *I.S.O* (International Standards Organization), que desenvolveu um modelo de interconexão de sistemas abertos chamado OSI (Open System Interconnection) o qual, juntamente com as regras e padrões de comunicação definidos em um do protocolo provê a comunicação com segurança entre Redes de Computadores e sistemas diversos.

Portanto, qualquer que seja a estrutura de redes de computadores existente dentro de uma organização, as tecnologias e conceitos de protocolos (regras que governam a transmissão de dados implementadas via *software*), tem auxiliado e contribuído para a segurança das informações que trafegam diariamente nas redes de comunicação de dados. Estas redes precisam inspirar confiança aos seus usuários e, para isso, são necessários tecnologia, pessoal e investimento. Segurança em Redes de Computadores, é um assunto complexo, repleto de conceitos técnicos relacionados à Segurança da Informa, onde se busca tanto detectar a vulnerabilidade como também prover meios para melhorar esta segurança, assuntos que serão discutidos no próximo capítulo.

# CAPÍTULO IV

# SEGURANÇA DE REDES DE COMPUTADORES

## 4.1 ASPECTOS RELACIONADOS À SEGURANÇA DE REDES DE COMPUTADORES

As equipes de Tecnologia da Informação estão sendo solicitadas a implementar um número cada vez maior de aplicativos de segurança que, por sua vez, são muito complexos. A preocupação com relação ao correio eletrônico também está cada vez mais acentuada, pois muitos usuários utilizam esta ferramenta para trabalho e disseminam vírus de computador alojado em arquivo de dados muitas vezes sem ter conhecimento da contaminação. Ao final deste trabalho, no APÊNDICE poderão ser encontrados detalhes sobre a Arquitetura de Redes de Computadores, bem como informações técnicas relacionadas a Protocolos.

### 4.1.1 SEGURANÇA E VULNERABILIDADE DA INFORMAÇÃO

Segundo Soares et al. (1995), o termo segurança é utilizado com o significado de minimizar a vulnerabilidade de bens e recursos. Vulnerabilidade é qualquer fraqueza que pode ser explorada para se violar um sistema ou as informações que ele contém, alterando e causando dano qualquer àintegridade da mesma.

A segurança está relacionada à necessidade de proteção contra o acesso ou manipulação –- intencional ou não –- de informações confidenciais por elementos não autorizados, e a utilização não autorizada do computador ou dos seus dispositivos e periféricos. A necessidade de proteção deve ser definida em termos das possíveis ameaças e riscos e dos objetivos de uma organização, formalizada nos termos de uma política de segurança concisa, objetiva e apoiada pela alta direção da empresa.

Segundo Moreira (2001), em se tratando de vulnerabilidades existentes na organização, cada uma delas pode permitir a ocorrência de determinados incidentes de segurança. Quando o sistema de segurança da informação existente em uma empresa apresenta algumas falhas, torna-se vulnerável a um ataque por meio de pessoas mal intencionadas ou mesmo via vírus de computador, sendo que um possível invasor poderia explorar as fraquezas de uma incompleta configuração de *firewall* ou de uma

versão antiga de software do sistema Operacional do Servidor, ter acesso a informações estratégicas da empresa ou mesmo provocar uma destruição de dados existentes nos servidores da rede.

É possível se concluir, portanto, que as vulnerabilidades existentes no sistema de segurança da informação de uma empresa poderão provocar um incidente de segurança, que afetará diretamente o negócio da organização, gerando impacto negativamente à própria empresa, ao produto fabricado (marca), aos clientes e à sua imagem no mercado.

A figura 6, a seguir, apresenta um esquema ilustrativo do impacto dos incidentes de segurança da informação nos negócios.

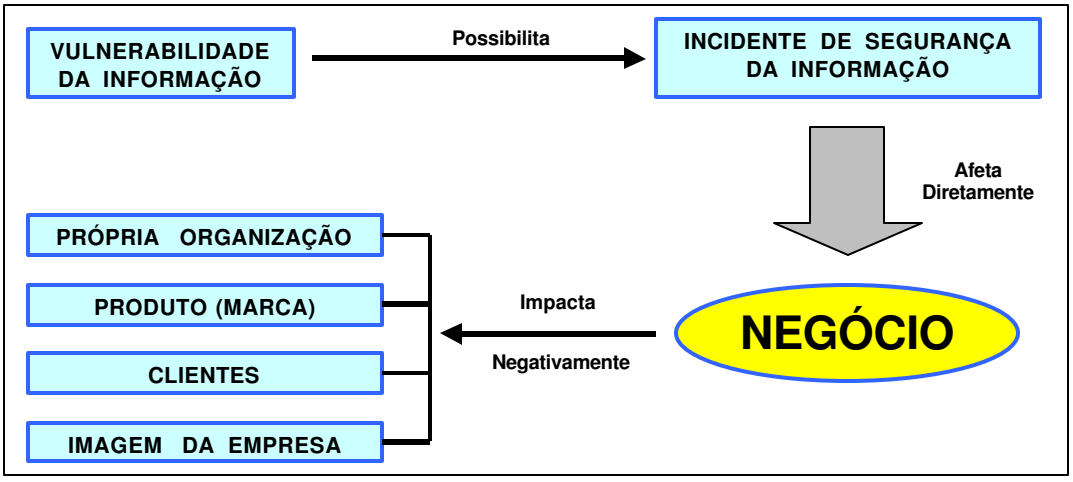



Figura 6 – Impacto dos Incidentes de Segurança da Informação nos Negócios
Fonte: Moreira, Nilton S. (2001, p.27).

### 4.1.2 AMEAÇAS E ATAQUES À INFORMAÇÃO

Segundo Luz (1999), uma ameaça consiste de uma possível violação da segurança de um sistema. E como algumas das principais ameaças as redes de computadores, pode-se citar:

- Destruição, danificação da informação ou de outros recursos.
- Modificação ou deturpação da informação.
- Furto, remoção ou perda de informação ou de outros recursos.
- Revelação de informação o pessoal não autorizado.
- Interrupção de serviços de servidores ou estações de trabalho.

As ameaças podem ser classificadas como acidentais e intencionais, podendo ambas ser ativas ou passivas.

- Ameaças acidentais são as que não estão associadas à intenção premeditada. Por exemplo, por descuidos operacionais, por desconhecimento de causa, falta de treinamento, falta de atenção e *bugs* de *software* e *hardware*. A concretização de uma ameaça intencional varia desde a absorção de dados com ferramentas simples de monitoramento de redes, a ataques sofisticados baseados no conhecimento do funcionamento do sistema. A realização de uma ameaça intencional configura um ataque.
- Ameaças Passivas são as que, quando realizadas, não resultam em qualquer modificação nas informações contidas em um sistema, em sua operação ou em seu estado. Uma estação que processa todos os quadros e dados que recebe em uma rede local (incluindo os que não são a ela endereçados), é um exemplo da realização de uma ameaça passiva.
- Ameaças Ativas: uma realização de ameaça ativa envolve a alteração da informação contida no sistema ou modificações em seu estado ou operação. Uma estação de uma rede com topologia em anel que não retransmite mensagens quando deveria fazê-lo (ela não é a responsável pela retirada da mensagem do anel), é um exemplo de realização de uma ameaça ativa.

Os principais tipos de ataque que podem ocorrer em um ambiente de comunicação de dados também podem receber classificações conforme o ocorrido, ou seja, os ataques passivos estão relacionados com interceptação, monitoramento e análise de tráfego, sendo que os ataques ativos estão relacionados com adulteração, fraude, imitação e bloqueio:

- DoS – Denial of Service (Interrupção de Serviço): esta ação interrompe um serviço ou impede totalmente que usuários ou entidades autorizadas o utilizem. Seu objetivo principal é "tirar do ar" (não deixar disponível) um serviço ou o sistema, apenas para causar o prejuízo, transtorno ou eliminar um serviço de proteção que possa permitir que se tenha acesso a outros serviços não autorizados.
- Personificação: uma entidade se faz passar por outra. Uma entidade que possui poucos privilégios pode fingir ser outra, para obter privilégios extras.
- Replay: uma mensagem, ou parte dela é interceptada e, posteriormente transmitida para produzir um efeito não autorizado. Por exemplo, uma mensagem válida, levando informações que autenticam uma entidade K, pode ser capturada e posteriormente transmitida por uma entidade Y tentando autenticar-se no sistema.

- Modificação: conteúdo de uma mensagem alterada, implicando em efeitos não autorizados, sem que o sistema consiga detectar a alteração. Um exemplo seria a troca de uma informação contendo o valor 2000 para o valor 20000, considerando-se este valor uma unidade monetária, o efeito é desastroso e prejudicial.
- Recusa ou impedimento do serviço: ocorre quando uma entidade não executa sua função apropriadamente ou atua de forma a impedir que outras entidades possam executar suas tarefas adequadamente. Uma entidade pode utilizar esta forma de ataque para suprimir as mensagens, por exemplo, direcionadas a entidade encarregada da execução do serviço de auditoria de segurança. Outro exemplo é a geração de mensagens com o intuito de atrapalhar o funcionamento dos *algoritmo*s de roteamento.
- Ataques internos: ocorre quando usuários legítimos comportam-se de modo não autorizado ou não esperado, executando softwares inadequados com o objetivo de burlar segurança ou na tentativa de efetuar algum acesso em que o mesmo não tenha permissão;
- Armadilhas: ocorre quando uma entidade do sistema é modificada para produzir efeitos não autorizados em resposta a um comando ou evento. Por exemplo, um envio de *broadcast* (processo pelo qual se consegue enviar uma mensagem partindo de um único emissor para todos os computadores conectados à rede de dados), indicando parada de um determinado computador, em resposta a uma combinação de teclas especificadas, por exemplo, “Ctrl-Alt-U”, em uma determinada máquina;
- *Trojans Horses* (Cavalos de Tróia): nesse ataque, uma entidade executa funções não autorizadas, em adição às que estão autorizadas a executar. Um procedimento de *login* modificado que, além de uma função normal de iniciar uma sessão de trabalho dos usuários, grava suas senhas em um arquivo desprotegido, é um exemplo de um Cavalo de Tróia na rede. Este arquivo poderá ser lido num outro momento futuro, onde então a senha de acesso será descoberta. Após esta ação, a fragilidade já estará exposta e a senha estará conhecida.
- *War Dialing*: método “força-bruta” para se encontrar uma conexão discada ou um sistema de rede conectado via *modem* (MOdulator-DEModulator, é um dispositivo que adapta os sinais digitais de um computador ou terminal para os sinais de áudio de uma linha telefônica e vice-versa), normalmente autorizada,

utilizando uma faixa de um prefixo de telefone associado a uma grande empresa para fazer a invasão.

- *E-mail Bomb* (Mensagem-Bomba): consiste em enviar *e-mail* gigantesco com o intuito de causar sobrecarga nos servidores ou no usuário final.
- *Spam / Junk Mail*: consiste no envio de *e-mail* não autorizado em larga escala. Normalmente é muito usado para enviar mensagens de propagandas ou solicitação de *marketing* de empresas tentando vender ou divulgar algo, na grade maioria das vezes coisas das quais não precisamos ou não queremos. Grandes quantidades de SPAM podem ser usadas para causar sobrecarga em servidores *de e-mail*. Falsos *e-mails* solicitando o cancelamento de cadastros de SPAM (remove@...) também são usados para confirmação de *e-mails* válidos;
- *Smurf*: o atacante envia um ECHO_REQUEST *ICMP* (solicitação de respostas) geral, fazendo um *spoof* (simulação de endereço em uma rede) do endereço de origem como endereço *IP* da máquina alvo solicitando uma resposta (ECO) *ICMP* a todas as máquinas de uma rede, fingindo ser a máquina alvo. Todas as máquinas conectadas respondem ao pedido enviando a resposta para a máquina alvo real, sobrecarregando a rede e principalmente o sistema alvo;
- *Ping of Death* (Ping da Morte): de aplicação simples, este ataque se baseia na vulnerabilidade do comando *Ping* (Packet Internet Groper), que envia um pacote de 32bits para um endereço *IP* e verifica, de acordo com a resposta, se aquele endereço esta conectado, pois este sistema não analisa com detalhes os pacotes *ICMP* (pacotes de controle ao nível de *IP*) com mais de 32bits, então envia-se uma seqüência de *ping* com o tamanho máximo possível (aproximadamente 2000 *bits*).
- Interrupção de Serviço: usa-se o *SYN Flooding* (grande volume de *SYN*). O *Hacker* ataca o *handshake* (sinais de controle enviados entre as partes envolvidas na comunicação para o estabelecimento de uma conexão válida), de três vias do estabelecimento *TCP*: o cliente envia um *bit SYN* (Synchronous Idle, ou Synchronize sequence number, é o caracter de controle utilizado para manter o sincronismo na ausência de dados trafegando pela rede), o servidor reconhece e responde com o *SYN-ACK* (SYN-ACKNOWLEDGMENT, código de comunicação enviado por uma estação receptora para uma estação transmissora, reconhecendo que os dados transmitidos foram recebidos sem erros ou que a estação receptora está pronta para receber mais dados), o

cliente reconhece a resposta enviando um *ACK* e se inicia a transferência de dados. O ataque consiste em enviar os *SYNs* e não responder aos *SYN-ACK*, deixando em aberto os estabelecimentos de conexão até ocupar todos os *buffers* (segmentos de memória utilizados para armazenamento de dados durante um determinado processamento), de conexão do servidor, então os outros clientes não conseguem estabelecem conexões reais com o servidor. Isto pode vir a causar queda de todo o sistema caso a situação consuma toda a memória livre do servidor.

- Adulterando rotas ou *DNS*: ao invés de desativar um serviço o *Hacker* impede o acesso do usuário ao serviço legítimo.
- Consumo de Recurso do Sistema: este processo é executado criando-se situações de abuso ou sobre-carga que ultrapassem o limite do recurso disponível (memória, HD, processador, etc.).
- Consumo de Banda da Rede: e feita quando o atacante tem uma banda maior que o do atacado ou e feita por vários atacantes ao mesmo tempo enviando informações simultaneamente.
- *BackDoor* (porta dos fundos) ou Trap Door (armadilha): é uma forma não documentada de acessar uma rede ou sistema, normalmente inserida na rede ou sistema por que o projetou. Pode-se também ser um programa inserido ou modificado para dar acesso exclusivo a uma determinada pessoa.
- Bomba lógica: é um programa ou uma parte projetado com o intuito malicioso, que é ativado por uma determinada condição lógica e é normalmente introduzido por um funcionário mal-intencionado.
- *Port Scanning* (Varredura de Portas): é uma técnica muito usada por *Hackers* para reconhecimento de possíveis entradas na rede. Para isso usa-se um programa que analisa os números de portas mais conhecidos para detectar informações ou serviços em execução no sistema. Exemplo de porta lógica:
  - (20) FTP (Transferência de arquivos);
  - (23) Telnet (Terminal);
  - (24) SMTP (Envio de *e-mail*)
  - (110) POP3 (Recepção de *e-mail*)
- *Spoofs* (Falsificação ou disfarce de identidade): Existem várias formas de *spoofs*:
  - *IP Address Spoofing* (Falsificação de endereço *IP*): todo dispositivo em uma rede *TCP/IP* utiliza um endereço *IP* único como identificação, o

*IP Address Spoofing* utiliza uma máquina com o endereço *IP* aceito pelo sistema de validação para ter acesso àrede.

- *Sequence Number Spoofing* (Falsificação de números Seqüenciais): conexões em redes *TCP/IP* utilizam números de seqüência incluídos em transmissões e trocados por transações, se o *algoritmo* de geração deste número é previsível, um *Hacker* poderá monitorar e gravar a troca de números de seqüência e prever os próximos a serem inseridos na conexão.
- *MIM – Man in the Middle* (Homem no Meio): esta é uma técnica utilizada para se interpor no meio de uma comunicação, isto pode ser feito registrando um domínio parecido, quando se comete o erro de digitação, o atacante se interpõe e pode repassar a comunicação com o domínio correto, mas acaba capturando informações ou inserindo *links* (formato de uma rede permanente ou um elo temporário de comunicação entre computadores), para endereços falsos.
- *Replay* (Reprodução): consiste em interceptar e capturar uma transmissão legitima e retransmiti-la mais tarde, pode-se evitá-la usando *timestamp* (controle de tempo).

- *Stack Overflow* (Estouro de Pilha): consiste em preencher um *buffer* alocado na pilha com informações que excedem o tamanho previsto, fazendo com que o endereço de retorno seja alterado, esta modificação normalmente faz com que uma nova função seja adicionada no retorno da mensagem original.
- Quebra de Senha: é uma das formas mais comuns de invasão e pode-se usá-la de várias maneiras para se quebrar uma senha. Pode-se tentar várias senhas diferentes como intuito de se verificar se uma coincide com a de algum usuário. Utilizar o mesmo *algoritmo* que codifica (protege) de um sistema para codificar cada tentativa e comparar resultado com a lista de senhas do sistema, usar dicionário de palavras e expressões comuns e existem ainda muitos programas quebra-senha disponíveis na *internet*, para a maioria dos sistemas operacionais de rede existentes.
- Engenharia Social: consiste em métodos não-técnicos para se obter acesso a um sistema, em geral é um processo de convencer alguém a fornecer ou revelar informações. Um exemplo típico é ligar para alguém que tenha acesso ao sistema e se identificar com sendo do suporte técnico e desta forma inventar uma história e solicitar a senha de acesso da vítima.

- *Sniffing* (Grampo, Monitoração): consiste no monitoramento de pacotes transmitidos na rede e muitas vezes são usadas ferramentas de fabricantes ou comerciais criadas com o propósito de gerenciar ou fazer o monitoramento da rede. Exemplo destas ferramentas e o *Telnet* e o *rlogin* que não utiliza criptografia para senha usada pelo usuário.
- *Web Site Defacement:* este é muito mais comum na *internet*, pois é utilizado para inserir mensagens de protestos, avisos, ridicularizações, etc. na *home page* de um *site*. Normalmente os *Hackers* exploram alguma falha ou vulnerabilidade do servidor da *Internet*, do sistema operacional ou dos protocolos e componentes envolvidos.

## 4.2 A NECESSIDADE DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Segundo Fontes (2000), uma Política de Segurança é formada por decisões que coletivamente determinam a postura de uma organização em relação àsegurança. Mais precisamente determina os limites aceitáveis de comportamento e as medidas a serem tomadas no caso de sua violação. Os principais objetivos de uma Política de Segurança são os de definir as expectativas da organização quanto ao uso dos seus computadores e rede e de se estabelecer procedimentos visando prevenir e responder a incidentes relativos àsegurança da informação.

A criação de uma Política de Segurança precisa ser um esforço conjunto entre o pessoal técnico e o pessoal responsável pelas decisões da organização. É importante fazer uma avaliação de riscos para se decidir o que realmente precisa ser protegido e a quantidade de recursos que deve ser usado para protegê-los. Deve-se ter o máximo de situações possíveis analisadas para que se tenha alternativas claras na tomada de ações corretivas quando se fizer necessário.

Uma Política de Segurança é um conjunto de diretrizes e regras bem definidas e práticas que regulam como uma organização gerencia, protege e distribui suas informações e recursos. Um dado sistema é considerado seguro em relação a uma Política de Segurança, caso garanta o cumprimento das diretrizes definidas nesta política.

Muito mais do que ferramentas para proteger as redes, é preciso ter implementada uma Política de Segurança. Fabricantes, consultores, integradores e executivos da área de Tecnologia da Informação, são unânimes em afirmar que métodos, objetivos e procedimentos definidos de forma que as próprias ferramentas sejam integradas e

tenham seu desempenho otimizado, é o que garante, de fato, a proteção das redes e da informação. Um dos aspectos importantes é a definição da responsabilidade de cada usuário e sua conscientização no sentido de não abrir arquivos recebidos via correio eletrônico que tenham origem duvidosa.

Segundo Dreyfuss (2000), uma adequada Política de Segurança da Informação, preocupada com o problema de contaminação por meio de vírus de computador, é importante e resulta de uma decisão de negócios, pois divide a atenção de investimentos com outras iniciativas empresariais, que também podem ser consideradas estratégicas para o negócio da empresa.

A criação de uma Política de Segurança precisa ser um esforço conjunto entre o pessoal técnico e o pessoal responsável pelas decisões da organização. É importante fazer uma avaliação dos riscos envolvidos para se decidir o que realmente precisa ser protegido e a quantidade de recursos que devem ser utilizados para minimização dos mesmos. Deve-se ter o máximo de situações possíveis analisadas para que se tenha alternativas claras na tomada de ações corretivas quando se fizer necessário. O recebimento e envio de arquivos por meio de correio eletrônico deve ter um tratamento detalhado e criterioso devido ao risco que se apresenta por meio de arquivos que possam estar contaminados por vírus de computador.

O problema de segurança é tão político quanto técnico e a maioria das empresas ainda não têm uma Política de Segurança completa implementada. O risco aumenta na medida em que cresce o uso da tecnologia da corporação. A principal fonte de ataque continua sendo os próprios funcionários e as empresas estão colocando a implantação de uma Política de Segurança como assunto de alta prioridade, principalmente devido à disseminação de vírus de computador, que pode atingir todo o servidor do correio eletrônico e, em conseqüência, todos os usuários e inclusive disseminando esta contaminação para além da empresa, para clientes, parceiros de negócios e etc.

Segundo Fontes (2000), uma Política de Segurança para ter sucesso deve ser verdadeira, ter recursos financeiros para implementação, deve ser curta, válida para todos os colaboradores, sejam eles funcionários ou subcontratados, deve ser simples, ter o apoio da alta direção, deve-se fazer uma análise dos riscos, implementar medidas de proteção, analisar as possíveis ameaças, estabelecer responsabilidades, ter critérios de senhas, ter uma definição de auditorias internas periódicas, e saber objetivamente a resposta para questões do tipo: o que deve ser feito quando algum tópico for violado? Com referência ao uso do correio eletrônico, deve ser criteriosa e clara em suas proposições para que o usuário tenha condições de trabalhar sem o receio de que está sendo monitorado o tempo todo.

Para que uma política tenha sucesso após a implantação, é importante o comprometimento dos usuários, ter uma sistemática de auditorias internas periódicas e ter definidas as punições para os casos omissos ou o de não cumprimento das diretrizes determinadas. Somente desta maneira a mesma poderá ser observada e ter funcionalidade. É importante a adoção de rotinas de treinamento buscando a colaboração e conscientização dos usuários no sentido de que os usos dos recursos de Informática, fornecidos pela empresa, são para o seu desempenho funcional e não para o uso pessoal.

### 4.2.1 OBJETIVOS DE UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Segundo Luz (1999), o principal objetivo de uma Política de Segurança da Informação é informar e conscientizar a todos os profissionais e colaboradores da organização, parceiros, prestadores de serviços internos, empresas ou instituições quais são as suas obrigações para a proteção da tecnologia e do acesso à informação. A política deve definir as expectativas da organização quanto ao uso dos seus computadores, recursos de rede e Informática, deve estabelecer procedimentos que possam prevenir e responder a incidentes relativos à segurança da informação e deve, ainda, especificar os mecanismos por meio dos quais estes requisitos possam ser alcançados. Um outro propósito também existente é o de oferecer um ponto de referência a partir do qual se possa adquirir, configurar e executar auditorias de sistemas computacionais e de redes, para que aos requisitos propostos sejam adequados e, desta maneira, uma tentativa de utilizar um conjunto de ferramentas de segurança na ausência de pelo menos uma Política de Segurança implícita não faz sentido.

É importante que se efetue um Planejamento das Necessidades de Segurança, ou seja, nesta fase é que se justifica procurar descobrir a maior quantidade possível das vulnerabilidades do sistema –- físico e lógico –-, ou seja, em quais partes existe maior fragilidade para ataques e quais as possíveis ameaças. Existem diversas possibilidades, como vulnerabilidades físicas (arrombamento de salas/prédios), naturais (desastres, incêndio, inundação, perda de energia, poeira, umidade), de *Hardware* e *Software* (*bugs* e falhas do sistema), de mídia (discos, fitas e materiais impressos furtados ou danificadas), de comunicação (dados em trânsito podem ser interceptados), de emanação (todos equipamentos elétricos emitem radiações, que podem ser captadas e decifradas) e humanas (erros acidentais ou intencionais). Com referência ao *Hardware*, é imprescindível estar atentos aos seguintes pontos:

Equipamentos Servidores: os servidores de dados em geral, podem ser considerados o coração da rede, ou da empresa. São as portas de entrada e de saída de informações para as estações de trabalho e para a *Internet*, caso não haja proteção, a entrada de intrusos e o acesso aos dados tornam-se um alvo fácil.

Estações de trabalho: estes equipamentos dos utilizados para trabalho pelos usuários, quando não são protegidos, podem se transformar em porta de acesso a informações sigilosas ou ponto de partida para ataques de *Hackers*.

*Link* Direto: é quando se tem uma única estação de trabalho conectada diretamente à *Internet* via *modem*. Este equipamento compromete todo um sistema de segurança implantado.

*Notebook* e ou Usuário Remoto: estes equipamentos efetuam um acesso direto à empresa e à *Internet* via *modem* podem levar pessoas mal intencionadas para a rede corporativa, quando em um momento de conexão àrede.

*Internet*: traz para a rede corporativa e torna presente toda a falta de segurança de uma rede sem controle algum, que é o caso da *Internet*.

Documentos: toda a documentação de inventário, definições de projetos de sistemas, programas de computadores e formulários administrativos.

### 4.2.2 PROFISSIONAIS ENVOLVIDOS NA FORMULAÇÃO DA POLÍTICA

De acordo com Luz (1999), o projeto de implantação de uma Política de Segurança da Informação é delicado, depende da aceitação não somente da alta direção da empresa, como também dos funcionários em geral que deverão aceitar e colaborar com o seu desenvolvimento. Portanto, para que uma Política de Segurança se torne apropriada e efetiva, ela deve ter a aceitação e o suporte de todos os níveis de colaboradores dentro da organização ou instituição. É especialmente importante que a gerência corporativa suporte de forma completa o processo da política, caso contrário haverá pouca chance de que ela tenha o impacto desejado. A relação abaixo é de pessoal técnico e profissionais que deverão estar envolvidos na criação e revisão dos documentos da política de segurança a ser implantada:

- O administrador de segurança da rede.
- O pessoal técnico da área de Tecnologia da Informação.
- Os administradores de grandes grupos de usuários dentro da organização.
- A equipe de reação a incidentes de segurança.
- Os representantes de grupos de usuários afetados pela política de segurança.

- O conselho legal e Jurídico da Organização.

A relação acima é representativa para muitas organizações que têm controle acionário, mas não necessariamente todas. E a idéia é aproximar representações dos membros, gerentes com autoridade sobre o orçamento e política, pessoal técnico que saiba o que pode e o que não pode ser suportado, e o conselho legal que conheça as decorrências legais das várias diretrizes a serem adotadas. Em algumas organizações, pode ser apropriado incluir pessoal de auditoria e, envolver este grupo é importante para que a política resultante possa alcançar a maior aceitabilidade possível, sendo que também é importante mencionar que o papel do conselho legal irá variar de país para país.

### 4.2.3 CARACTERÍSTICAS PRINCIPAIS DE UMA POLÍTICA DE SEGURANÇA

Ainda, segundo Luz (1999), em termos genéricos, as características mínimas principais que uma Política de Segurança precisa ter devem ser as seguintes:

- Efetuar uma análise dos riscos procurando medidas de proteção, como também, observando o custo-benefício de todo o projeto.
- Revisar todo o processo continuamente e melhorá-lo sempre que for encontrada alguma fraqueza.
- Ser implementável por meio de procedimentos de administração, publicação das regras de uso aceitáveis, ou outros métodos apropriados.
- Ser exigida com ferramentas de segurança, onde apropriado, e com sanções onde a prevenção efetiva não seja tecnicamente possível;
- Definir claramente as áreas de responsabilidade para os usuários, administradores e gerentes.
- Definir claramente quais usuários terão privilégios para acessos e execução de rotinas na rede e nos sistemas informatizados.
- Definir claramente quais as atividades e privilégios dos administradores dos sistemas, tendo como segurança, a gravação e a contabilização dos acessos aos dados, gravados em arquivos de *logs* (arquivo contendo informações relacionadas a uma execução de rotina ou de software, onde são registrados todos os detalhes quanto à data de início e término, como também problemas que possam ter acontecido durante o processamento), referente a todas as atividades executadas por estes profissionais.
- Informar aos usuários, equipe e gerentes, as suas obrigações para a proteção

da tecnologia e do acesso àinformação.

- Especificar os mecanismos por meio dos quais seus requisitos podem ser alcançados.
- Oferecer um ponto de referência a partir do qual se possa adquirir, configurar e efetuar auditorias dos sistemas computacionais e redes, para que sejam adequados aos requisitos propostos.
- Expressar o que os usuários devem e não devem fazer em relação aos diversos componentes do sistema, incluindo o tipo de tráfego permitido nas redes.
- Ser tão explícita quanto possível para evitar ambigüidades ou maus entendimentos.

Segundo Fontes (2000), a Política de Segurança deve, ainda, ter as características:

- Envolver aspectos técnicos, humanos e organizacionais com foco àproteção da Informação.
- Explicitar para todos os usuários que acessam e utilizam a informação, qual é a filosofia da empresa sobre este recurso, devendo-se considerar as características operacionais e culturais da empresa, bem como o relacionamento entre as pessoas.
- Ser um elemento de um conjunto de ações que compõem o Processo de Segurança da Empresa, independente da informação estar no ambiente computacional ou no ambiente convencional. O cuidado com a informação deve ser o mesmo.
- Precisa ter vida e chegar a todas as pessoas.
- Conscientizar todos os usuários, mostrando o valor da informação e quais são suas responsabilidades.
- Deve ser verdadeira.
- Deve exprimir o pensamento da empresa e ser coerente com as ações da organização.
- Deve ter o patrocínio da direção da empresa.
- O documento normativo que formalizará a Política deve ser assinado pelo mais alto executivo, explicitando assim o seu total apoio àpolítica implementada.
- A Política e o documento principal da Política de Segurança não devem ser caracterizados como um Manual de Procedimentos nem um documento

extremamente técnico. A Política deve definir as regras estruturais e os controles básicos para o acesso e uso da informação.

- Deve estar disponível para consulta dos funcionários envolvidos sempre que se fizer necessário.
- Deve ser simples e não deve conter definições técnicas e aspectos de implementações.
- Deve ser entendida por todos os usuários em toda a sua plenitude e profundidade até pelo Presidente da Empresa.
- A Informação deve ser tratada como um Bem da Empresa.

### 4.2.4 COMPONENTES DE UMA POLÍTICA DE SEGURANÇA

Ainda, segundo Fontes (2000), geralmente os componentes principais que uma Política de Segurança deve ter como condições mínimas para obtenção de sucesso após sua implementação, devem ser as seguintes:

- Controle do acesso à Informação.
- Definição do Gestor da Informação.
- Responsabilidades do usuário, da gerência e do Gestor da Informação.
- Preparação para situações de contingência, garantindo a continuidade da execução do negócio.
- Definição do uso profissional da informação da empresa.
- Definição da possibilidade, ou não, da empresa acessar arquivos pessoais do usuário, quando de investigações criminais.
- Definição da identificação do usuário como pessoal e única, bem como o sigilo da senha.
- Conscientização dos usuários.
- Medidas disciplinares que serão utilizadas caso a Política não seja cumprida.

Segundo Luz (1999), alguns dos principais componentes que uma política de segurança deve ter, ainda, são os seguintes:

- Guias para a compra de tecnologia computacional que especifiquem os requisitos ou características que os produtos devem possuir.
- Uma política de privacidade que defina expectativas razoáveis de privacidade relacionadas a aspectos como a monitoração de correio eletrônico, *logs* de atividades e acesso aos arquivos dos usuários.

- Uma política de acesso que defina os direitos e os privilégios para proteger a organização de danos, por meio da especificação de linha de conduta dos usuários, pessoal e gerentes. Ela deve oferecer linhas de condutas para conexões externas, comunicação de dados, conexão de dispositivos a uma rede, adição de novos *softwares*, etc. Também deve especificar quaisquer mensagens de notificação requeridas (por exemplo, mensagens de conexão devem oferecer aviso sobre o uso autorizado, e monitoração de linha, e não simplesmente "bem vindo");
- Uma política de contabilidade que defina as responsabilidades dos usuários. Deve especificar a capacidade de auditoria, e oferecer a conduta no caso de incidentes (por exemplo, o que fazer e a quem se dirigir caso seja detectada uma possível invasão), sendo que uma violação poderá ocorrer em virtude de negligência, erro acidental, desinformação ou incompreensão a respeito da política em uso, violação direta e consciente da política definida.
- Uma política de investigação deve ser feita e uma ação prontamente tomada, acordando com o tipo de violação ocorrida.
- Ter um representante legal, da área Jurídica da empresa, para análise e tomada de ações legais que se façam necessárias, para assuntos da parte da empresa para com seus funcionários e da parte dos funcionários para com a empresa, quando se tratar de casos de suspeita de invasão de privacidade de caixas postais do correio eletrônico, que porventura tenham sido executadas pelos administradores da rede.
- Definir quem interpretará a política implementada em casos de dúvidas ou despertar desconfianças ou questionamentos.
- Uma política de autenticação que estabeleça confiança por meio de uma política de senhas efetiva, e por meio da linha de conduta para autenticação de acessos remotos e o uso de dispositivos de autenticação.
- Um documento de disponibilidade que define as expectativas dos usuários para a disponibilidade de recursos. Ele deverá endereçar aspectos como redundância e recuperação, bem como especificar horários de operação e de manutenção, como também deverá incluir informações para contato para relatar falhas de sistema e de rede.
- Um sistema de tecnologia de informação e política de manutenção de rede que descreva como, tanto o pessoal de manutenção interno como externo, deverão manipular e acessar a tecnologia. Um tópico importante a ser observado é como a manutenção remota será permitida e como tal acesso será controlado.

Sobre *Outsourcing*, (processo de delegação de atividades e funções a empresas que são enquadradas como Terceiros, sem vínculo empregatício), considerar como deverá ser gerenciada, quais os critérios de controle e monitoramento das atividades e dos acessos dos profissionais pertencentes à categoria de Terceiros.

- Uma política de relatório de violações que indique quais os tipos de violações deverão ser relatados e a quem estes relatos deverão ser feitos. Uma atmosfera de não ameaça e a possibilidade de denúncias anônimas irá resultar uma grande probabilidade que uma violação seja relatada.
- Suporte que ofereça aos usuários informações para contato para cada tipo de violação, linha de conduta sobre como gerenciar consultas externas sobre um incidente de segurança, ou informação que seja considerada confidencial ou proprietária. Devem ser analisadas também algumas referências cruzadas para procedimentos de segurança e informações relacionadas, tais como as políticas da companhia, leis e regulamentações governamentais.

Pode haver requisitos necessários que possam regular e que afetem alguns aspectos da Política de Segurança, como por exemplo, a monitoração. Os criadores da política devem considerar a busca de assistência legal na criação da mesma e, no mínimo, a política deve ser revisada por um conselho legal. É importante que se façam reuniões periódicas analisando os problemas detectados e verificando possíveis alternativas e soluções que possam ser adotadas.

Uma vez que a política tenha sido estabelecida ela deve ser claramente comunicada aos usuários, profissionais de diversas categorias, gerentes e responsáveis pela alta direção da organização. Deve-se criar um documento que os usuários assinem, estando de acordo com cada parágrafo e expressando sua ciência de que leram, entenderam e concordaram com a política estabelecida. Esta é uma parte importante do processo. Finalmente essa política deverá ser revisada regularmente para verificar se ela está suportando com sucesso as necessidades de segurança requisitada.

### 4.2.5 CARACTERÍSTICAS DE UMA POLÍTICA DE SEGURANÇA FLEXÍVEL

Ainda segundo Luz (1999), após a implantação da Política de Segurança, são necessárias algumas medidas estratégicas que devem ser executadas, com o intuito de torná-la viável em longo prazo. É recomendável a existência de flexibilidade baseada no conceito de segurança arquitetural, sendo que uma política deve ser largamente

independente de *hardware* e *softwares* específicos. Os mecanismos para a atualização da política devem estar claros. Isso inclui o processo e as pessoas envolvidas.

É importante reconhecer também que há expectativas para cada regra e, sempre que possível, a política em uso deve expressar quais expectativas foram determinadas para a sua existência, por exemplo, sob quais condições um administrador de sistema tem direito a pesquisar nos arquivos do usuário. Também pode haver casos em que múltiplos usuários terão acesso à mesma "senha". Por exemplo, em sistemas com um usuário *root* (nome dado ao usuário principal de um sistema Unix), múltiplos administradores de sistema talvez conheçam a senha e utilizem a conta.

### 4.2.6 VISÃO DA EMPRESA ORIENTADA À POLÍTICA DE SEGURANÇA

Segundo Graça (2000), uma Política de Segurança se diferencia bastante dependo do tipo de corporação, organizações, empresas, instituições que a adotam e, de um modo geral, o que mais influência na elaboração de uma política de segurança é o tipo de negócio realizado, o tipo de informação utilizada e o fluxo desta informação pela organização. Deste modo, é de vital importância antes do início de qualquer estudo para a elaboração e implementação, uma análise das expectativas e conceitos esperados pela corporação.

Na Figura 7, abaixo, é demonstrado como esta visão dos negócios pode ser orientada em se tratando de uma política de segurança.

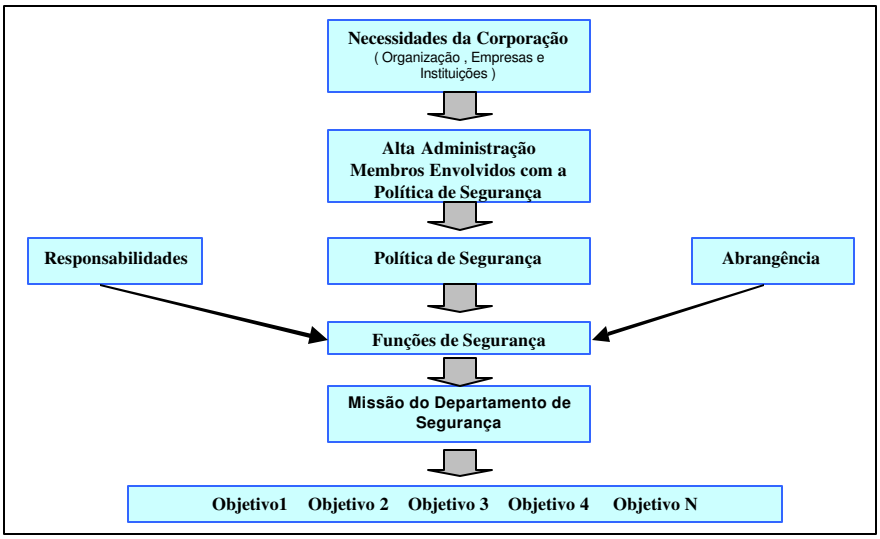
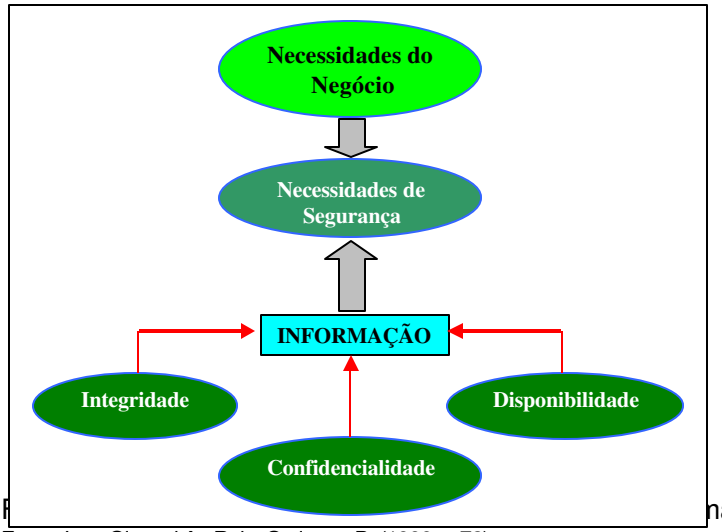



Figura 7– Política de Segurança com Visão ao Negócio da Organização
Fonte: Luz, Giovani A., Reis, Gutierres B. (1999, p.71).

A corporação tem vida própria, tem metas, objetivos e necessidades para se manter competitiva no mercado em que atua. A alta administração, bem como os profissionais envolvidos com a política de segurança da informação, têm o dever de monitorar e verificar se todas as diretrizes que estejam sendo implementadas estão condizentes com os princípios de segurança previstos no documento da política.

Após uma análise da abrangência, das responsabilidades de cada um e dos critérios de segurança, passa-se à análise dos objetivos diversos a serem trabalhados. Na Figura 8, demonstra-se um esquema da idéia de que o Negócio (a Organização), depende da segurança para ter uma informação confiável, como também a Informação depende da segurança para ter os seus três aspectos característicos eficientes para a tomada de decisão empresarial, ou seja, integridade, confidencialidade e disponibilidade.




Fonte: Luz, Giovani A., Reis, Gutierres B. (1999, p.72).

Os três aspectos citados podem ser definidos da seguinte forma:

- Confidencialidade: este aspecto está ligado à manutenção do segredo, do sigilo ou da privacidade das informações. Esta propriedade indica que os dados e informações não deveriam ser acessíveis, ficarem disponíveis para ou ser divulgados a usuários, entidades, sistemas ou processos não autorizados e aprovados.
- Integridade: trata-se de manutenção das informações tal e qual tenham sido geradas, sendo que esta propriedade indica que os dados e as informações não deveriam ser alterados ou destruídos de maneira não autorizada e aprovada.
- Disponibilidade: trata-se da possibilidade de acesso contínuo, sem falhas,

ininterrupto, constante e atemporal às informações. Esta propriedade indica que o acesso às informações pelo sistema deveria ser sempre possível para um usuário, entidade, sistema ou processo autorizado e aprovado.

Uma Política de Segurança é o conjunto de decisões que coletivamente determinam a postura de uma organização em relação à segurança de dados. Mais precisamente determina os limites aceitáveis de comportamento e as medidas a serem tomadas no caso de sua violação. Alguns dos objetivos mais importantes de uma Política de Segurança são os de definir as expectativas da organização quanto ao uso dos seus computadores instalados e conectados em rede e de se estabelecer procedimentos visando prevenir e responder a incidentes relativos àsegurança da informação.

### 4.2.7 CICLO DE IMPLEMENTAÇÃO DE UMA POLÍTICA DE SEGURANÇA

O processo de implementação de uma Política de Segurança da Informação deverá ser criterioso e bem planejado, pois a política implementada deverá garantir o mínimo de segurança às organizações, porém o comprometimento de todos os funcionários e responsáveis pela sua implementação da mesma deve ser uma constante.

A Figura 9 mostra o ciclo de implementação de uma Política de Segurança da Informação:

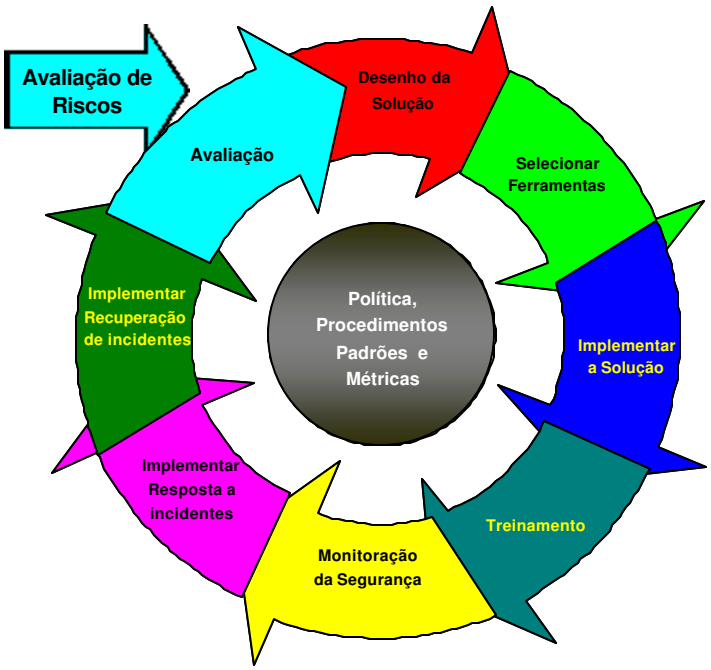



Figura 9 – O Ciclo de Implementação de uma Política de Segurança da Informação

Fonte: CASE SOLECTRON (2000).

Segundo o Case Solectron (2000), para se implementar uma Política de Segurança da Informação é necessário disciplina, organização e determinação das pessoas envolvidas, bem como um comprometimento da Alta Gerência.

#### 4.2.7.1 LEVANTAMENTO E AVALIAÇÃO DOS RISCOS

Segundo Luz (1999), todo o processo se inicia com uma análise e Levantamento dos Riscos existentes e que serão contemplados na Política, ou seja, nesta fase é montado todo o escopo de abrangência do trabalho.

Numa visão mais resumida, o processo poderia até ser dividido em quatro grandes momentos e fases:

- Avaliação.
- Desenho da Solução (Elaboração da Arquitetura de Segurança).
- Implementar a Solução (Implementação).
- Monitoração da Segurança (Monitoração).

A etapa de Avaliação consiste em realizar um estudo sobre a corporação avaliando as necessidades de segurança da mesma. Nesta etapa devem ser levados em conta os seguintes itens:

- Análise de vulnerabilidades, ameaças e riscos.
- Avaliação dos riscos.
- Elaboração de recomendações e planos de ação.

Para a realização da análise de vulnerabilidades, as ameaças e os riscos, é necessário, inicialmente, conhecer o conceito de cada um dos itens para uma melhor compreensão dos mesmos:

Vulnerabilidades: para que uma agressão se concretize torna-se indispensável que existam vias de acesso, ou um ponto suscetível para um ataque aos recursos alvo dessa agressão. Cada uma destas vias de acesso a determinado recurso constitui para a organização uma vulnerabilidade. As vulnerabilidades podem ser agrupadas em duas grandes categorias, relacionadas com as vias de acesso, sendo elas:

- Vulnerabilidades de vias de acesso lógico.
- Vulnerabilidades de vias de acesso físico.

Vulnerabilidades de vias de acesso lógico: são aquelas em que as vias de acesso

lógico e as vulnerabilidades associadas representam todas as formas de se acessar aos dados ou às informações por via lógica, isto é, por intermédio do sistema de informação sem ter acesso físico a um suporte de informação determinado, por pessoas efetivamente pertencentes ou não a organização. Estas vulnerabilidades podem agrupar-se segundo a forma como o acesso é concretizado:

- Acesso autorizado: é a vulnerabilidade resultante do fato de pessoas autorizadas acessarem a uma determinada informação e poderem, acidentalmente ou intencionalmente, divulgá-la, alterá-la ou destruí-la.
- Usurpação de direitos: engloba todas as formas camufladas ou não previstas de acessar a uma informação ou a um recurso por meio de atribuição ilegítima de direitos de acesso, aquisição ilegítima de direitos de acesso, pirataria de *software*, abuso de direitos, portas falsas ou Cavalos de Tróia, utilização abusiva de utilitários privilegiados e violação intencional dos sistemas de segurança.

Vulnerabilidades de vias de acesso físico: Englobam todas as formas de se acessar fisicamente a um recurso do sistema de informação, recursos físicos ou suportes que podem ser desencadeados por pessoas ou por elementos naturais como a ar, o fogo e a água. Neste caso há a distinguir entre as vulnerabilidades:

- O acesso às instalações por meio das vias normais, portas e janelas, piso e tetos falsos, paredes e divisórias.
- O acesso aos recursos guardados nas instalações da organização como suporte de dados, estações de trabalho e equipamentos, em particular os de telecomunicações e os de climatização e de energia.
- O acesso aos recursos localizados no exterior da organização ou em trânsito, redes públicas, influência eletromagnética e suporte de dados em trânsito.

Ameaças: ações desencadeadas por uma pessoa, usuário ou acontecimento susceptível de conduzir a uma alteração não desejada de um recurso do sistema de informação, qualquer que seja o seu tipo. Uma ameaça, portanto, é uma agressão potencial que ainda não se manifestou.

Riscos: avaliação de um perigo e da perda de dados, em função da probabilidade da sua concretização e das conseqüências associadas ao mesmo. Para a avaliação dos riscos é necessário a verificação da potencialidade dos mesmos e o seu impacto à organização.

Segundo Chamon (2001), "*O conceito de risco admite numerosas definições, não havendo consenso entre os diversos autores. Entretanto, todas as definições possuem dois elementos em comum: incerteza e magnitude. Risco está associado à idéia de incerteza visto que ele se refere a situações futuras imprevisíveis e/ou fora do controle do gerente ou tomador de decisões. Sob esse aspecto, ao risco está associada uma probabilidade de ocorrência. Além disso, o evento ao qual o risco se refere pode causar uma perda ou conseqüência indesejável maior ou menor, isto é, ele contém uma certa capacidade de dano. Sob esse aspecto, ao risco está associada uma magnitude. Essas duas dimensões combinadas permitem uma avaliação global do risco numa determinada situação*".

Ainda, segundo Luz (1999), os riscos podem ter as classificações potenciais:

Potencialidade de riscos: com relação à questão da potencialidade de um cenário de risco, prende-se com a necessidade de saber se os riscos correspondentes fazem realmente parte do envolvimento habitual da organização e em que medida e com que ponderações devem ser tomadas em conta. A principal dificuldade reside em saber distinguir os cenários daqueles que podem acontecer na ausência de qualquer medida de segurança específica. No caso da segurança na informática, o importante é distinguir os riscos próximos e reais daqueles cuja eventualidade de surgir é longínqua, sendo que é esta característica de proximidade que se chama potencialidade para acentuar o grau de possibilidade, plausibilidade ou probabilidade do risco considerado.

Níveis de potencialidade: considera-se que um número limitado de níveis é suficiente para descrever a potencialidade dos cenários de risco, apresentam-se nesta circunstância quatro níveis: forte, médio, fraco e insignificante.

Potencialidade forte: corresponde aos cenários que fazem parte da vida normal da organização e cuja concretização não devem constituir surpresa, sendo que os cenários de forte potencialidade compreendem as situações que têm na sua origem ações humanas motivadas e intencionais perante fatores de dissuasão fracos ou inexistentes, por exemplo, furto de informações a favor da concorrência, perturbações causadas voluntariamente para prejudicar a concorrência e daí tirar vantagens, etc. Em síntese, considera-se cenário de forte potencialidade os casos de concorrência desleal, roubo e desvio de informação, destruição de recursos, informações, equipamentos e suporte lógico, que um concorrente ou colaborador interno pode desencadear sem grande dificuldade e sem sofrer prejuízos. Podem igualmente ser considerados de forte potencialidade os cenários que são gerados por uma ação humana involuntária, por exemplo, erro cometido por um empregado no desempenho das suas funções ou os que resultam de um gesto de mau humor não premeditado.

Igualmente, a atividade dos *Hackers* ao tentarem invadir um computador por meio da rede de telecomunicações.

Potencialidade média: Os cenários de potencialidade média não fazem parte da

atividade corrente da organização, nunca se verificaram ao longo da sua existência, mas podem vir a acontecer num futuro mais ou menos próximo. São incluídos nesta categoria de acidentes, os desastres naturais e os erros acidentais, muito pouco prováveis, mas que de qualquer forma podem acontecer. São desta forma considerados como cenários de potencialidade média os atos humanos que levam os seus autores a cometer ilegalidades e assumir riscos tais como a perda de emprego ou a demanda judicial.

Potencialidade fraca: Os cenários de potencialidade fraca são aqueles de ocorrência excepcional, mas de qualquer forma possíveis. Insere-se nesta categoria os acontecimentos que só se concretizam em circunstâncias excepcionais. Grandes catástrofes têm uma potencialidade fraca, mas em circunstâncias particulares pode-se verificar estes acidentes. Os delitos inserem-se muitas vezes neste cenário.

Potencialidade insignificante: Os cenários de potencialidade insignificante estão no limite do possível, mas de qualquer forma são imagináveis, por exemplo, descobrir por acaso uma "senha" de doze caracteres, alterados dinamicamente e sem significado.

Após a análise e avaliação dos riscos, bem como a identificação das potencialidades, espera-se que seja gerado um relatório contendo os seguintes itens:

- Identificação das vulnerabilidades.
- Classificação dos riscos identificados.
- Dimensionamento dos recursos necessários.
- Apresentação das observações e efeitos, impactos.
- Recomendações para minimizar os riscos identificados.
- Comentários da administração.
- Conclusão final.

Existem alguns benefícios esperados com a análise e avaliação dos riscos, que são os seguintes:

- Identificação de requisitos mínimos de Segurança e Auditoria para cada plataforma.
- Avaliação do grau de envolvimento dos usuários com a confidencialidade, integridade e disponibilidade.
- Plano de ação contendo contra-medidas, visando a redução de riscos.

Após a análise e avaliação dos riscos fica evidenciada a necessidade da elaboração de recomendações para a redução e eliminação dos mesmos, entre estas recomendações se encaixam os seguintes itens:

- Proposta para a elaboração de uma Política de Segurança para a organização.
- Proposta para a elaboração de planos de continuidade dos negócios.

- Proposta para a elaboração de planos de ação visando a implementação de estratégias, política de segurança, e monitoramento para a melhoria da segurança da informação na organização.

Observando-se estes conceitos é possível de se fazer um estudo de penetração na organização, ou seja, um estudo levando em conta todos os aspectos possíveis relacionados com as vulnerabilidades, ameaças e riscos.

Em resumo, segundo Moreira (2001), todos os bens e ativos de uma organização estão sujeitos a vulnerabilidades em maior ou menor escala e estas vulnerabilidades proporcionam riscos para a empresa, que muitas vezes são causados por falhas nos seus controles.

Desta maneira, pode-se afirmar que riscos surgem em decorrência da presença de fraquezas e vulnerabilidades. Por outro lado, as ameaças exploram as vulnerabilidades existentes devido às falhas de configuração ou inexistência de medidas de proteção adequadas e, deste modo, os danos causados pela ação das mesmas causam impactos negativos ao negócio, aumentando ainda mais os riscos.

Em contrapartida, medidas de proteção adequadas protegem os ativos e o negócio diminuindo os riscos a níveis aceitáveis. Na figura 10, abaixo, apresenta-se um esquema ilustrativo sobre a influência do risco na organização.

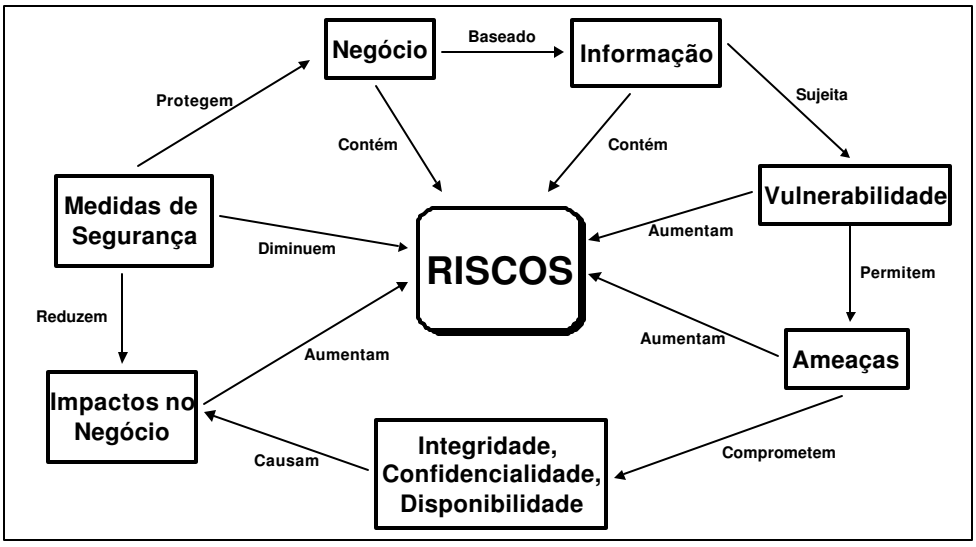



Figura 10 – O Ciclo da Segurança da Informação em Função de Riscos
Fonte: Moreira, Nilton S. (2001, p.21).

#### 4.2.7.2 DESENHO DA SOLUÇÃO

Na seqüência, segundo Luz (1999), inicia-se o processo de desenho da solução, ou seja, todas as definições dos tópicos que serão contemplados nos procedimentos, todos os documentos e formulários que serão criados, as regras que deverão estar descritas nos procedimentos, formação do grupo de trabalho para gerir todo o processo e definição dos profissionais que representarão todas as áreas da empresa.

Elaboração da arquitetura de segurança: a etapa de elaboração da arquitetura de segurança consiste na formulação das diretrizes e estruturas relacionadas com a segurança. Nesta etapa devem ser levados em conta os seguintes itens:

- Definição das diretrizes da alta administração.
- Estruturação da função de administração de segurança.

Definição das diretrizes da alta administração: consiste na definição do tipo de política, padrões e diretrizes, requerimentos máximos e mínimos, que serão necessários segundo a alta administração, tendo o seu posicionamento voltado para a "visão do negócio", ou seja, o tipo de empreendimento realizado. Estas definições são de suma importância, pois refletem as expectativas esperadas com a implementação da política e das medidas de segurança. A Figura 11, a seguir, demonstra um exemplo, numa estrutura hierárquica, utilizando-se uma pirâmide, este item –- a Política –-, com as suas definições, se posicionaria no topo da pirâmide devido ao seu alto grau de importância:

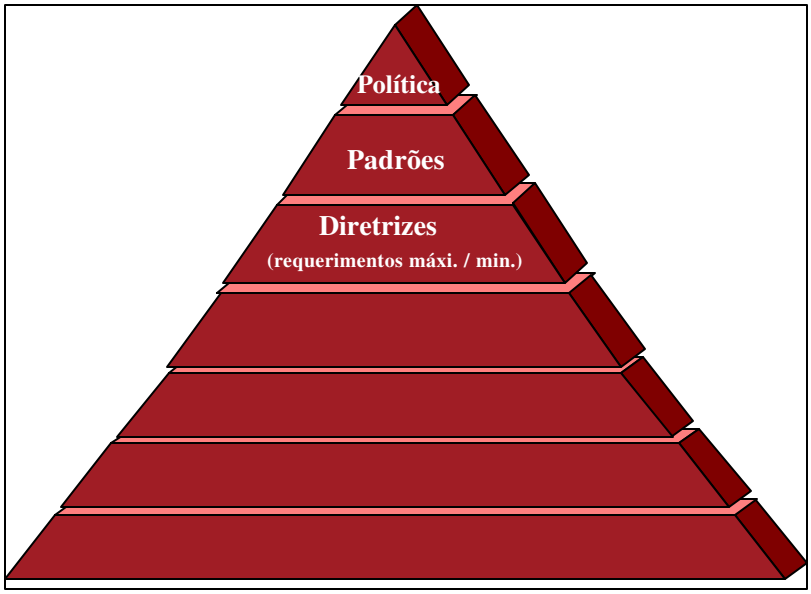



Figura 11 – A Importância da Definição da Política, Padrões e Diretrizes
Fonte: Luz, Giovani A., Reis, Gutierres B. (1999, p.86).

A estruturação da função de administração de segurança, ainda segundo Luz

(1999), consiste na formulação de uma estrutura que compreenda três segmentos distintos existentes na organização:

- A área de Informática: responsável pela manutenção dos sistemas, equipamentos entre outros e pelo desenvolvimento de novos projetos;
- Os usuários: aqueles que utilizam os serviços de maneira a facilitar o seu trabalho, sendo responsáveis por manter a integridade, disponibilidade e confidencialidade das informações;
- A alta administração: responsável por estabelecer as diretrizes, políticas e padrões a serem adotados tendo uma visão voltada para o negócio.

Analisando a estrutura em evidência, é possível de se observar que demonstra a que nível cada segmento compreende, definindo as responsabilidades dos mesmos quanto à segurança das informações e recursos, permitindo uma visão da distribuição destes na estrutura da organização, conforme mostrado no item anterior a representação dessa estrutura é feita com a utilização de uma "pirâmide".

Na Figura 12, na seqüência, há uma comparação entre as etapas para a elaboração e a implementação de uma política de segurança e as estruturas de administração de segurança.

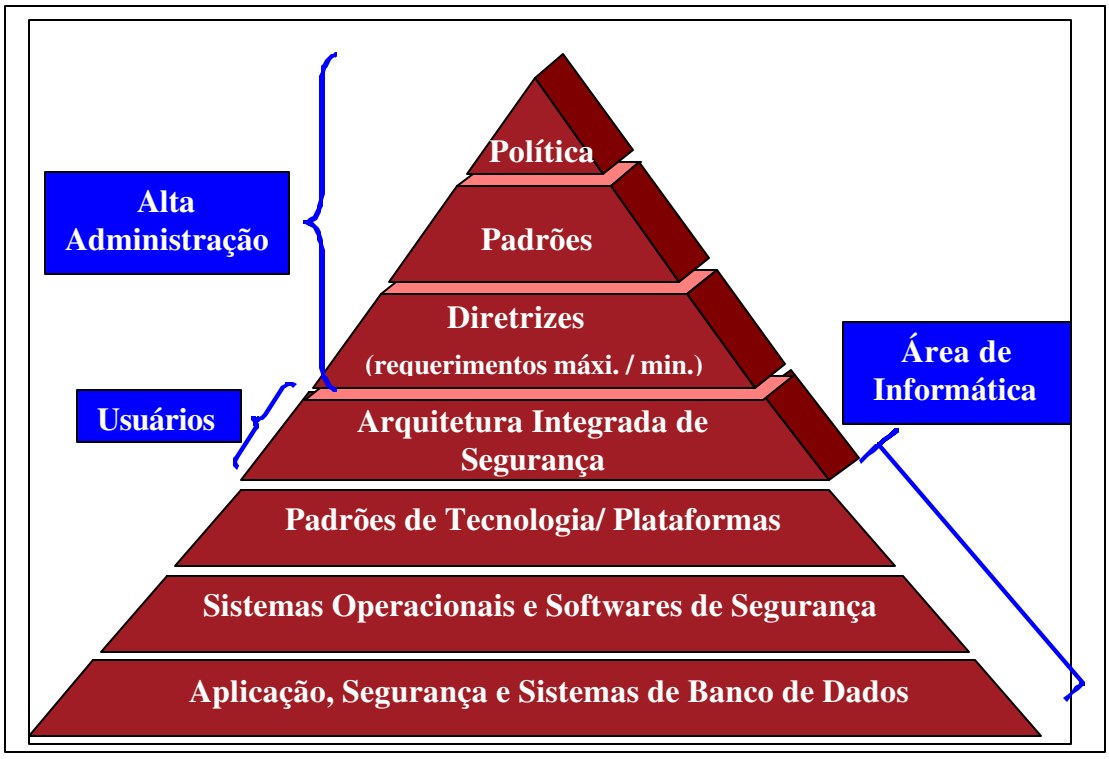


Figura 12 - Os Segmentos da Organização e Suas Responsabilidades
Fonte: Luz, Giovani A., Reis, Gutierres B. (1999, p.88).

Neste ponto do desenvolvimento e das definições do Desenho da Solução, é possível de se começar a ter uma visão de como o trabalho estará sendo conduzido, que itens estarão sendo abordados e aplicados na abrangência da política de segurança a ser implementada.

Na Figura 13, abaixo, é apresentada uma comparação entre as etapas principais para a elaboração de uma política de segurança da informação e a estrutura de diretrizes da alta administração da organização:

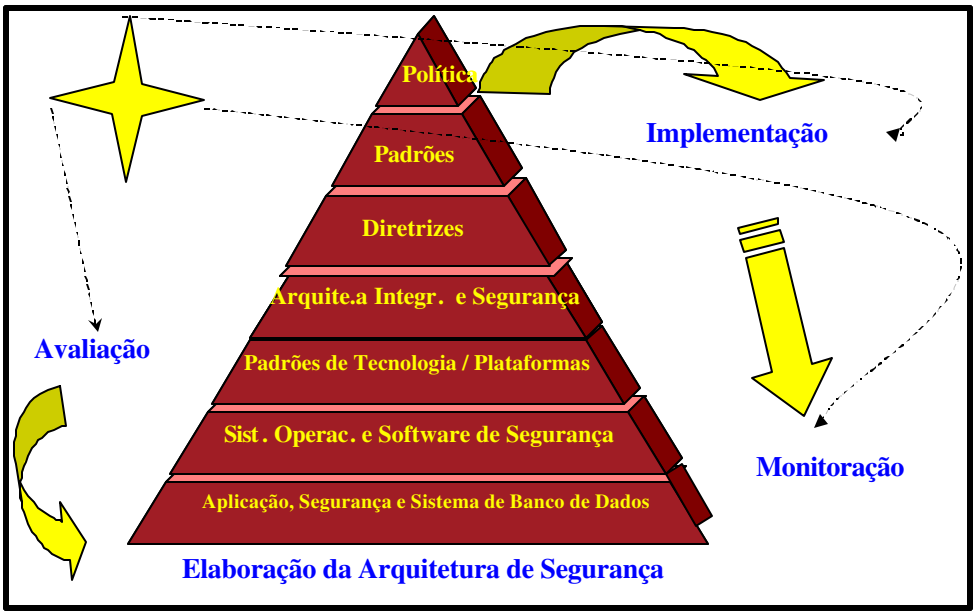



Figura 13 – Etapas de Elaboração e Estrutura de Diretrizes da Administração
Fonte Luz, Giovani A., Reis, Gutierres B. (1999, p.88).

A Implementação: esta etapa de implementação consiste na elaboração, identificação e estruturação dos elementos da política de segurança para sua efetiva implantação na organização, sendo que se recomenda a observação dos seguintes itens:

- Estruturação do comitê de segurança, ou grupo de profissionais responsáveis pela implementação das diretrizes de Segurança da Informação.
- Elaboração dos procedimentos de administração da segurança.
- Elaboração das metodologias detalhadas para a área.

- Elaboração do Documento da Política de Segurança da Informação e o Plano de Implementação, bem como o cronograma detalhado.
- Identificação das ferramentas e recursos tecnológicos de informática para viabilizar o projeto.
- Definição e implementação do programa de conscientização dos usuários.

A Estruturação do Comitê de Segurança da Informação: com o intuito de que a implementação da Política de Segurança tenha condições de se evoluir e ser produzida, é importante a criação de um grupo de profissionais que possam dedicar às atividades necessárias, reuniões e que esteja estruturado em um comitê ou comissão de Gestão da Segurança, cujas responsabilidades são:

- Aprovar e rever a Política de Segurança da informação existente.
- Fixar as funções e os objetivos de segurança da informação.
- Coordenar a implementação da segurança dentro da organização.
- Classificar a informação e o fluxo da informação dentro da organização como Confidencial, Restrita e Irrestrita e a quem pode ser divulgada.
- Constituir, eventualmente, um núcleo de especialistas em consultoria em segurança dentro da organização que possa analisar as ferramentas e os critérios definidos nas diretrizes a serem implementadas.
- Estabelecer mecanismos de articulação com especialistas externos em segurança e consultores, tendo em vista acompanhar as tendências, normas e avaliações da indústria e solucionar os incidentes de segurança.
- Responsabilizar-se pela manutenção da classificação de segurança de programas e dados.
- Designar o responsável ou responsáveis pela segurança da informação.
- Verificar e identificar as maiores ameaças a que os recursos de informação estão expostos.
- Rever e verificar os incidentes de segurança ocorridos nas dependências da empresa.
- Aprovar as principais iniciativas da instituição tendo em vista aumentar a segurança da informação.

Elaboração dos procedimentos de administração de segurança: o objetivo da elaboração dos procedimentos de administração de segurança consiste em garantir que as atividades críticas da organização sejam restabelecidas e mantidas o mais rapidamente possível logo após um incidente de desastre ou falha importante que possa ter afetado os recursos ou serviços essenciais à disponibilidade e integridade da informação. É essencial a existência de um método de planejamento para desenvolver e

manter planos de segurança dentro da organização, que possa ser acionado em momentos emergenciais, como um Plano de Contingência.

Método de planejamento da segurança: O planejamento da segurança implica na identificação e redução dos riscos de ameaças acidentais ou intencionais aos serviços vitais da organização, ou seja, aos servidores de dados e à informação corporativa da empresa. É essencial que se encontrem respostas objetivas e precisas às seguintes questões:

- Que acidentes e desastres se pretendem prevenir?
- Contra que ameaças é importante implementar mecanismos de proteção?
- Que riscos se podem correr?

O método de planejamento e controle da segurança deve incidir fundamentalmente sobre a manutenção das atividades críticas e serviços em execução, incluindo pessoal e outros recursos não computacionais e deverá cobrir:

- Identificação e verificação das prioridades das atividades críticas.
- Avaliação do impacto potencial dos vários tipos de acidentes, desastres, nas atividades vitais da organização.
- Identificação e aprovação de todas as responsabilidades, diretrizes e medidas de segurança.
- Documentação dos métodos, procedimentos e processos aprovados.
- Treinamento, preparação e formação do pessoal dos profissionais.
- Execução de teste dos planos implementados.
- Atualização dos planos existentes.

Estrutura dos planos de segurança: Uma estrutura única de planos de segurança deve ser estabelecida para garantir que todos os níveis do plano são coerentes e possíveis de implementação, sendo que cada plano de segurança deverá especificar claramente as condições da sua atuação, como também as responsabilidades individuais pela execução de cada componente do plano. Novos planos de segurança devem ser coerentes com os procedimentos de emergência estabelecidos, por exemplo, planos de evacuação total dos prédios e com os recursos alternativos existentes para sistemas de informática, comunicações e instalações. Cada plano de segurança deverá ter diferentes níveis, porque cada nível terá incidências diferentes e poderá envolver diferentes equipes de recuperação.

Recomenda-se que um modelo de estrutura de planos de segurança envolva quatro componentes principais:

- Procedimentos de emergência: são os procedimentos que descrevem as ações imediatas a tomar após um incidente importante que ponha em perigo

as atividades da organização ou vidas humanas.

- Procedimentos de recursos alternativos: descrevem as ações a tomar para deslocar atividades essenciais ou serviços de apoio para instalações alternativas temporárias, de *back-up* ou suporte específico.
- Procedimentos de reposição: descrevem as ações a tomar para reiniciar o normal funcionamento das atividades, usualmente nas instalações de origem.
- Programas de testes: especifica como e quando o plano será testado.

Cada nível do plano de segurança e cada plano autônomo deve especificar um responsável concreto, sendo que os procedimentos de emergência, planos de reposição e planos de contingência são responsabilidades dos "proprietários" das respectivas atividades e, as soluções de recursos alternativos para serviços técnicos, tais como sistemas informáticos e comunicações, são usualmente da responsabilidade dos fornecedores.

Testes dos Planos de Segurança: Toda a eficácia de um plano de segurança só pode ser avaliada por meio da realização de testes regulares simulando uma situação real. Somente os testes garantem que o plano é do conhecimento de todos os elementos envolvidos. Uma programação dos testes de plano de segurança deve ser definida, estabelecendo como e quando cada elemento envolvido no plano será testado, sendo que as atividades do plano deverão ser objeto de testes freqüentes e tal procedimento garante que o plano se mantém real e atualizado ao longo do ano e reduz a dependência, ou menor freqüência de testes globais do plano.

Atualização dos Planos de Segurança: Os planos de segurança sofrem desatualizações rapidamente em conseqüência de alterações nos aspectos organizacionais ou de gestão e, as atualizações regulares são essenciais para se proteger o investimento realizado com o desenvolvimento do plano inicial. O plano de segurança deverá ser atualizado sempre que se verifiquem quaisquer das seguintes alterações:

- Aquisição de novo equipamento ou expansões do sistema existente.
- Adoção de novas tecnologias de controle e detecção de acidentes.
- Adoção de novas tecnologias de controle ambiental.
- Alterações nos aspectos organizacionais ou de pessoal.
- Mudança de fornecedores ou prestadores de serviços.
- Alterações de números de telefone ou de endereço de empresas ou de pessoas envolvidas.
- Alterações nos processos de gestão.
- Alterações no leque de aplicações.

- Alterações nas atividades de operação.
- Alterações de legislação pertinente.

Devem ser atribuídas responsabilidades pela identificação e introdução de alterações ao plano. Todas as alterações efetuadas, por menor que sejam, devem ser introduzidas pelo menos mensalmente, devendo este processo ser complementado com uma breve revisão anual da globalidade do plano.

Elaboração de Metodologias para a Área: a elaboração de metodologias para a área, numa implementação de Política de Segurança, consiste na formulação escrita dos métodos e procedimentos, bem como instruções técnicas, que serão utilizados na realização dos diversos trabalhos relacionados com a segurança. Durante a elaboração destas metodologias deverão estar envolvidos, fundamentalmente, os membros relacionados com a Política de Segurança, o grupo de profissionais pertencentes ao comitê de segurança, que definiram um sistema metódico pelo qual seus trabalhos passaram a ser realizados, ou seja, métodos para:

- Avaliação dos riscos que possam surgir dentro da organização.
- Atribuição de responsabilidades relacionadas com os itens estabelecidos na Política de Segurança, tais como os procedimentos e planos de segurança.
- A classificação dos dados, informações e aplicações.
- A manutenção das principais etapas resumidas do ciclo de vida da política de segurança, a avaliação, a elaboração, a implementação e a monitoração.

O benefício com a descrição deste método consiste principalmente na padronização da forma pela qual são realizados os estudos e trabalhos relacionados com a segurança das informações, oferecendo assim uma possibilidade de maior participação dos membros envolvidos em vários projetos em andamento. Para uma perfeita integridade da metodologia empregada para a segurança da informação é necessário que haja um processo de atualização e revisão constante destes métodos, documentações, sendo que esta atualização deverá ser feita quando se sentir a necessidade da mesma ou periodicamente com a definição de um tempo previamente determinado.

Elaboração do Documento da Política de Segurança da Informação e do Plano de Implementação: após a execução das fases anteriores para a implementação da política de segurança da informação, se faz necessário a elaboração do documento oficial da Política de Segurança da Informação da organização, no qual deverá conter todas as informações relacionadas a este item. Neste documento deverão constar todas as regras, procedimentos, metodologias, instruções técnicas e planos que devem ser seguidos por todos os membros da organização que tenham envolvimento direto ou

indireto com a manipulação de recursos relacionados com as informações.

O documento da Política de Segurança da informação implementada na organização, uma vez elaborado, deverá ser divulgado a todos os elementos que a integram, e esta divulgação deve cobrir no mínimo os seguintes aspectos:

- A definição de segurança da informação, os seus objetivos globais, a esfera de ação e a sua importância como mecanismo essencial para a partilha da informação, bem como a classificação das informações na organização.
- A apresentação das diretrizes da Política de Segurança da organização, princípios, normais e requisitos de conformidade.
- A definição das responsabilidades gerais da gestão e específicas da organização para todos os aspectos de segurança da informação.
- A apresentação do processo de relato de incidentes de segurança suspeitos.

Para a implantação da Política de Segurança, se faz necessário a criação de um plano de implementação contendo a estratégia que será adotada com a definição das datas e responsabilidades por esse processo, ou seja, a criação de um cronograma detalhado de cada fase da implantação, como também um estudo dos custos que serão gastos com o projeto numa visão macro.

#### 4.2.7.3 SELECIONAR FERRAMENTAS

Em complemento, segundo Luz (1999), passa-se, então, para a fase de se Selecionar Ferramentas e recursos adequados e que serão utilizados na Política de Segurança. É o momento de se efetuar testes de viabilidades de produtos para avaliação se atenderão os princípios estipulados pela Política ou não. Faz-se necessário a identificação das ferramentas e os recursos que serão utilizados e até mesmo requisitados para se fazer valer as regras descritas. Dentre as ferramentas disponíveis que se enquadram neste contexto, temos entre outras, o *Firewall*, conjunto de recursos incluindo *hardware*, *software* e pessoal, que visam proteger, como também, restringir o acesso às informações disponíveis em uma rede de computadores. Estas ferramentas quando bem implantadas nas organizações garantem grande parte do sucesso de uma Política de Segurança da Informação.

#### 4.2.7.4 IMPLEMENTAÇÃO DA SOLUÇÃO

A próxima fase, conforme Luz (1999), é a de Implementação da Solução, ou seja, todos os procedimentos, diretrizes, critérios, formulários e ferramentas que foram validados nas fases anteriores deverão ser colocados em prática nesta fase.

É a uma das etapas mais críticas do projeto, onde todo e qualquer conflito existente entre áreas, ou qualquer interesse alheio ao sucesso das diretrizes propostas para o bem da empresa poderão ser questionadas ou mesmo dificultadas. Neste momento é importante que se tenha pessoas influentes apoiando o projeto como um todo, principalmente com acesso à alta direção da empresa, para que por meio destes profissionais, o projeto possa seguir suas fases de implantação naturalmente.

#### 4.2.7.5 TREINAMENTO

Na seqüência, passa-se para a fase de Treinamento, onde deverá ser feita toda a divulgação à empresa como um todo e todos os funcionários receberão uma cópia da cartilha "Uma Questão de Segurança", resumo das diretrizes principais da Política que está sendo implantada. Para a implementação da política de segurança é necessário que seja definido um programa de conscientização de usuários, por meio de campanhas e palestras que expliquem a importância da mesma, procurando com isso uma padronização na forma de se manusear a informação como um elemento fundamental para integridade das informações e para o sucesso do negócio. Um treinamento e uma conscientização bem feita é sinônimo de sucesso do projeto. Este treinamento deve ser constante e deve ter um período repetitivo, com o objetivo de incutir nos profissionais o hábito de ter a preocupação com a informação e sua segurança.

#### 4.2.7.6 MONITORAÇÃO DA SEGURANÇA

A fase seguinte é a da Monitoração da Segurança, ou seja, é a fase de análise do cumprimento das diretrizes da Política por parte de todos os usuários envolvidos e da definição de critérios que deverão ser alinhados ou alterados. A etapa de monitoração consiste na criação de mecanismos para o gerenciamento e dispositivos capazes de medir a efetividade da política de segurança da informação. Nesta etapa devem ser levados em conta os seguintes itens:

- Elaboração e implementação do plano de monitoração.
- Medição de indicadores e apuração de índices.

Elaboração e implementação do plano de monitoração: uma etapa importante após a implementação da política de segurança da informação é a elaboração e implementação de um plano de monitoração. Este sistema de monitoração pode ser executado por meio de uma auditoria de segurança com o objetivo de controlar a observância das medidas de segurança aprovadas. Esta auditoria deve ser executada periodicamente e incidindo com maior freqüência sobre as áreas mais críticas e os

sistemas aplicativos mais sensíveis, sendo que a mesma pode ser feita por auditores internos ou externos.

Medição de indicadores e apuração de índices: este item consiste na criação de indicadores para gerenciar e fornecer dados para a avaliação dos efeitos com a implementação da política de segurança da informação e a apuração destes índices permitirá as tomadas de ações, visando a contínua melhoria desta ferramenta para a organização.

#### 4.2.7.7 IMPLEMENTAR RESPOSTAS A INCIDENTES

Na seqüência, surge a fase de se Implementar Respostas a Incidentes, ou seja, é a fase onde serão analisados todos os eventos ocorridos, questionamentos, incidentes e problemas com o cumprimento das diretrizes propostas na Política implementada. É o momento ainda de se tomar a decisão para analisar se algum item não está exagerado ou outro que poderia ter um caráter mais rígido, etapa se verificar a aplicabilidade da Política se está sendo produtiva e cabível ou não.

#### 4.2.7.8 IMPLEMENTAR A RECUPERAÇÃO DE INCIDENTES

A próxima fase é a fase se Implementar a Recuperação de Incidentes, ou seja, é o momento, de se efetuar o realinhamento do propósito inicial da Política, que poderá ser implementado na próxima versão da mesma, ou em caráter de emergência, a mudança poderá ser efetuada imediatamente.

Retorna-se, então, à fase de Avaliação dos Riscos, ou seja, cumpriu-se todo o primeiro ciclo de vida da Política de Segurança da Informação. É o momento de se avaliar novamente os riscos existentes e os propósitos aos quais a Política está atendendo se realmente está sendo útil e eficiente ou não ou o pode ser feito para poder ser melhorada.

### 4.2.8 CONSIDERAÇÕES SOBRE PLANO DE CONTINGÊNCIA

O Plano de Contingência ou Plano de Continuidade do Negócio é um documento que contem rotinas a serem executadas quando houver casos de desastre ou catástrofe na área de Informática, ou seja, dano físico ou lógico às informações armazenadas. A situação de emergência deverá sempre ser analisada em concordância com os trechos descritos neste plano que contém diretrizes de atividades a serem seguidas, como também cautelas a serem tomadas em situações emergenciais. Segundo Sette (2001), o plano de continuidade de negócios ou plano de contingência é um procedimento

contendo ações para serem iniciadas como medidas extremas no tocante à continuidade do negócio, em caso de contingência, funcionando como um mecanismo de segurança da informação onde deve citar a definição do escopo, a identificação dos desastres, as ameaças e a seleção das estratégias. Deve possuir, ainda, ações que posam garantir que os processos relacionados à realização do negócio irão continuar acontecendo, apesar de ter ocorrido uma situação de desastre. A solução deve contemplar todos os recursos, sejam eles técnicos ou humanos. A criação do plano de contingência destaca, numa etapa inicial, a definição do escopo, onde se deve contemplar todas as áreas, todos os recursos, todos os sistemas da empresa, além de considerar também os aspectos geográficos, tecnológicos e funcionais. Uma maneira de se realizar este trabalho é a Análise do Impacto de um desastre, que consiste num método para identificação das perdas em virtude de possíveis paralisações de um processo crítico para o negócio. Com base nestas perdas deve-se identificar o nível de criticidade de cada processo e a sua devida prioridade.

A segunda etapa é identificar quais desastres a empresa está exposta, tais como falta de energia elétrica, vendavais, enchentes, terremoto, incêndio, greve de funcionários, falta de transporte em geral, falência ou não cumprimento de prazos por parte de fornecedores, ataques de *Hackers*, contaminação por meio de vírus de computador ou outros sistemas que possam –- direta ou indiretamente –- afetar o negócio da empresa. Esta atividade de identificação é possível de ser obtida por meio de uma Análise de Risco e a elaboração do plano de contingência compreende o detalhamento do que será feito, por quem será executado, como estas pessoas podem ser encontradas e onde estão os recursos necessários para cada execução. O documento completo do Plano deve estar sempre atualizado, localizado em local de fácil acesso, bem como deve existir uma cópia de segurança em local distinto. No momento em que se deverá implementar um Plano de contingência é necessário haver um treinamento de todos os envolvidos, a contratação de serviços, assim como a compra e a instalação dos recursos necessários para a implementação e testes.

Segundo Wladlow (2000), um sistema redundante deverá ser realmente redundante em todos os níveis, inclusive no roteamento físico de cabos. É importante efetuar testes em luzes de emergência, geradores de energia elétrica, sistemas de segurança e dispositivos diversos que tornarão a operação de contingência funcional.

A segurança física envolve todos os fatores relacionados aos equipamentos, dispositivos físicos, prediais e que garantam condições confiáveis para a correta armazenagem e utilização dos meios processadores da informação.

Atualmente existem salas especiais destinadas a armazenamento de servidores, fitas de *back-up* e toda a infra-estrutura para Informática, como também prédios comerciais. No Brasil e no exterior, que são uma vitrine de tecnologia, onde tudo é informatizado, desde as luzes, torneiras, ar-condicionado e dispositivos de segurança diversos, como alarmes e circuitos internos de televisão, todos independentes, os circuitos são interligados e controlados via *software*.

Os *softwares* utilizados controlam todos os alarmes do prédio e, como cada circuito é integrado, se houver algum problema o alarme entra em ação e informa todo o sistema citando detalhes da falha ocorrida e que precisa ser corrigida. Uma central de operações com pessoal técnico especializado se mantém sempre de plantão para os casos de qualquer pane de *software*. É recomendável que todos os equipamentos de informática tenham uma alimentação elétrica totalmente independente de outros dispositivos diversos da empresa, como por exemplo, ar-condicionado, máquinas de copiadoras e trituradoras de papel. As tomadas devem ser estabilizadas, todas com aterramento feito à base de barras de cobre para garantir uma perfeita alimentação elétrica aos equipamentos diversos de Informática. Para que se tenha uma maior segurança, é recomendável que se instale os servidores e estações de trabalho em *nobreaks*, equipamentos com bateria temporária interna para que se tenha tempo para desligar os comutadores em perfeitas condições. Os *nobreaks* devem ter capacidade para manter os dispositivos a ele conectados por pelo menos quinze minutos, tempo necessário para seu correto desligamento, em caso de queda de energia elétrica.

Para os casos de equipamentos que necessitem de máxima segurança e que tenham que manter seu pleno funcionamento ininterrupto é necessário a instalação de um gerador de energia elétrica, alimentado por óleo combustível, e que entraria em funcionamento automaticamente sempre que houver queda deste tipo de energia.

Segundo Shaffer (1994), fenômenos elétricos precisam ser tratados com importantes considerações, pois a eletricidade estática pode danificar os computadores. Quando houver a necessidade de uso de piso com carpete, o mesmo deverá ser especial com característica que combata a energia estática. Não é recomendado também trabalhar no microcomputador comendo, bebendo ou fumando, pois o perigo de danificar o equipamento é grande. Cuidado semelhante também deve ser considerado com disquetes e outros meios de armazenamento magnético de informações com as devidas proteções e observando-se ainda, a temperatura no manuseio destas mídias, que deve estar na faixa de 50-120 graus Fahrenheit.

Os equipamentos de Informática precisam ser dotados de recursos próprios de segurança, que lhes permitam um funcionamento adequado e ininterrupto. Os fabricantes

estão dotando as máquinas de fontes redundantes duplas, ou seja, caso uma falhe, a outra imediatamente assume o trabalho. Em complemento da alta disponibilidade destas máquinas, podemos citar também a existência dos discos de armazenamento com redundância e com dispositivos de espera, ou seja, em caso de falha de algum dos discos em uso, um outro, que estava em modo de espera, inicia o funcionamento em substituição ao danificado. O disco danificado pode ser substituído por outro novo, mesmo com a máquina em funcionamento, sem que haja qualquer dano físico e os dados serão reconstituídos automaticamente, processos denominados *Hot Plugable* (tecnologia existente nos computadores servidores de dados fabricados pela IBM, Compaq, HP e DELL, na qual é possível remover um disco danificado, mesmo com o equipamento ligado e em funcionamento, e instalar um disco novo sem que haja qualquer dano físico ao *hardware*.), e *Hot Swap* (tecnologia existente nos computadores servidores de dados fabricados pela IBM, Compaq, HP e DELL, na qual é possível a reconstituição dos dados gravados em um novo disco – a partir dos outros discos existentes –-, após a remoção de um disco danificado, mesmo com o equipamento ligado e em funcionamento, sem que haja qualquer dano físico ao *hardware*).

No caso de funcionários que tenham permissão de acesso à informação, estes podem danificar o dado armazenado sem a intenção ou intencionalmente. Há o caso do funcionário que grava arquivos confidenciais da empresa em disquetes, ou os envia anexados a uma mensagem de correio eletrônico para trabalhar em casa e, quando retorna para a empresa o arquivo pode estar contaminado por algum vírus de computador. Em todos estes casos citados, a perda ou dano da informação armazenada é uma constante que precisa ser analisada e tratada com critério rígido de segurança.

Atualmente as empresas estão preocupadas com o fluxo de seus dados que estão circulando pela rede de computadores podendo sofrer ataques e destruição. A informação armazenada nos servidores é alvo de constantes ataques de pessoas autorizadas ou não ao seu acesso. Outro caso é a do invasor externo, chamado de *Hacker*, que é o intruso que tenta invadir as redes para danificar as informações das empresas ou mesmo pelo prazer de conseguir ter acesso às mesmas sem provocar qualquer tipo de dano. Em todos estes casos citados, a perda ou dano da informação armazenada é uma constante que precisa ser analisada e tratada com critério rígido de segurança.

A rotina de se efetuar *back-up dos* dados armazenados nos servidores da rede, consiste em se ter uma diretriz e procedimentos para se executar as cópias de segurança destas informações. O *back-up* envolve *Hardware* e *Software*, bem como área restrita e segurança para se guardar os meios magnéticos contendo os dados. Geralmente uma

área de *back-up* segura se localiza fisicamente distante da área de Informática, como uma estratégia de segurança.

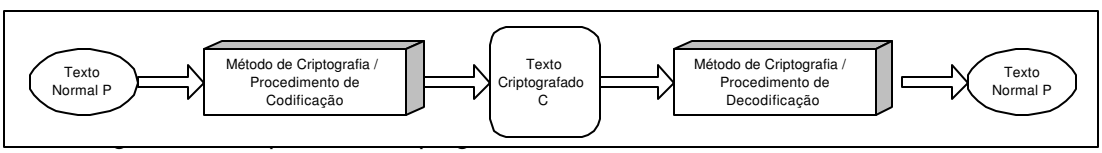
Segundo Wladlow (2000), o *back-up* deve ser uma importante preocupação da estratégia de Segurança Física, pois ele será a salvação das informações da organização caso ocorra algum desastre muito sério com referência a perda de dados armazenados nos servidores. A propriedade intelectual da empresa é algo importante, vital e que exigiu tempo e investimento é imprescindível o cuidado com os cartuchos contendo as cópias dos dados.

O *restore* é o processo de se retornar os dados armazenados magneticamente em cartuchos, fitas, ou disquetes utilizando softwares específicos para esta finalidade. O *restore* devolve ao servidor ou a uma estação de trabalho os dados que foram salvos anteriormente e que serão retornados após um desastre ou uma necessidade presente.

Uma Política de Segurança deve incluir regras detalhadas, objetivas definindo como as informações e recursos da organização devem ser manipulados ao longo de seu ciclo de vida, ou seja, desde o momento que passam a existir no contexto da organização até quando deixam de existir. As regras que definem uma Política de Segurança são funções das designações de sensibilidade, associadas aos recursos e informações (por exemplo, não classificado, confidencial, secreto e ultra-secreto), do grau de autorização das entidades e das formas de acesso suportadas por um sistema. Segundo Soares et al. (1995), uma empresa tendo uma Política de Segurança, a sua implementação é feita com a utilização de vários mecanismos de segurança, tais como:

A criptografia teve seu surgimento da necessidade de se enviar informações sensíveis e sigilosas por meio de meios de comunicação de voz não confiáveis, ou seja, em meios onde não é possível garantir que um intruso irá interceptar o fluxo de dados, tanto para leitura, no caso de intruso passivo, ou para alteração, no caso de intruso ativo. A forma de contornar esse problema é utilizar um método que modifica um texto original da mensagem a ser transmitida, gerando texto criptografado na origem, por meio de um processo de codificação definido por um método de criptografia.

A característica principal de um bom método de criptografia é a de ele garantir que haja uma dificuldade para que um intruso, a partir de um texto criptografado e do conhecimento do método de criptografia não consiga decifrar as mensagens ou as informações do arquivo. Na Figura 14 temos um exemplo de esquema de criptografia.



Fonte: Soares, Luiz F. G., Lemos, Guido, Colcher, Sérgio. (1995, p.452).

Dentre os métodos de criptografia utilizados, podem ser citados:

Criptografia com *chave* secreta: Este método tem a característica de substituir as letras de um texto pela n-ésima letra após a sua posição no alfabeto utilizado.

*Data Encryption Standard (DES)*: Este método tem a característica de codificar os blocos de 64 bits de texto normal gerando 64 bits de texto criptografado, sendo que o *algoritmo* de compactação é parametrizado por uma *chave* K de 56 bits e possui 19 estágios diferentes.

Criptografia com *chave* pública: Este método se baseia na utilização de uma *chave* para uma codificação (E) e uma outra para a decodificação (D), escolhidas de forma que a derivação de D a partir de E seja praticamente impossível para outra pessoa tentar ter acesso a estas informações.

*Rivest, Shamir e Adleman (RSA)*: É uma das mais famosas soluções do mercado e baseia-se na dificuldade em se fatorar números muito grandes.

Segundo Soares et al. (1995), a Certificação Digital permite a autenticação por meio da utilização de assinatura digital e controle de acesso com o emprego de criptografia de *chave* pública. O uso da criptografia na troca de informações visa impedir a captura dos dados durante a sua transmissão. Este não é o único problema a ser resolvido, pois tão importante quanto à transmissão de dados, é a garantia de qual fonte originou tal informação e a certeza de que somente as pessoas autorizadas terão acesso aos dados.

O mecanismo de Assinatura Digital é formado por dois procedimentos, a assinatura de uma unidade de dados e a verificação desta assinatura em uma unidade de dados. O primeiro procedimento baseia-se em informação privada (única e secreta). O segundo utiliza-se da informação pública para reconhecer a assinatura. Analisando o procedimento da assinatura digital observamos que o mesmo envolve a codificação da unidade de dados completa ou a codificação de uma parte, por exemplo, de um campo de verificação, da unidade de dados, ambos utilizando informação privada. Uma das características essenciais da assinatura digital é que ela deve garantir que uma mensagem assinada somente poderá ter sido gerada com informações privadas suas. Portanto, uma vez verificada a assinatura com a *chave* pública, é possível posteriormente provar para um terceiro que só o proprietário da *chave* privada poderia ter gerado a mensagem. Como compromisso de um Terceiro, este mecanismo de compromisso baseia-se no conceito de que um terceiro parceiro de confiança atestaria certas propriedades da informação intercambiada entre duas entidades, como sua origem, sua

integridade ou o momento em que ela foi enviada e recebida. O mecanismo de Autenticação depende do ambiente onde o mesmo será implementado, podendo ser destacadas três situações:

1. Os parceiros e os meios de comunicação são todos de confiança. Neste caso, a identificação de uma entidade par pode ser confirmada por uma senha. Cabe mencionar que as senhas não protegem contra ataques do tipo *Replay*. A autenticação mútua pode ser implementada com a utilização de uma senha distinta em cada direção da comunicação.
2. Cada entidade confia em seu parceiro, porém não confia no meio de comunicação. Neste caso, a proteção contra ataques, pode ser fornecida com o emprego de métodos de criptografia, como por exemplo, utilização do esquema da *chave* pública, juntamente com uso de senhas.
3. As entidades não confiam em seus parceiros, nem no meio de comunicação. Neste caso, devem ser empregados mecanismos de assinatura digital ou mecanismos que envolvam o compromisso de um terceiro confiável, usado em conjunto com técnicas de criptografia e técnicas de senhas.

Um exemplo desse mecanismo é o sistema de autenticação Kerberos, onde existe um *ticket* (cartão ou local onde se encontra armazenado algum dado que possa ser processado por computadores), que contém informações que identificam o serviço, o cliente e a *chave* secreta que será usada para criptografar as mensagens que serão trocadas entre o cliente e o servidor e somente este servidor a conhecerá.

Os mecanismos de Controle de Acesso são utilizados para garantir que o acesso ao recurso de *hardware* ou *software* é limitado aos usuários devidamente autorizados. As técnicas incluem a utilização de listas ou matrizes de controle de acesso, que associam recursos aos usuários autorizados ou *password* (senha para acesso a algum sistema lógico), *capabilities* (capacidade de execução de um determinado processamento), e *tokens* (frame que busca transmissões em uma rede Token Ring (IBM) ou semelhante), associados aos recursos, cuja posse determina os direitos de acesso do usuário que as possui.

O mecanismo de Controle de Integridade de Dados atua em dois níveis: controle da integridade de unidade de dados isolada e controle da integridade de uma conexão, isto é, das unidades de dados e da seqüência de unidade de dados transmitidas no contexto da conexão.

Para garantir a integridade dos dados, podem ser usadas técnicas de detecção de modificações, normalmente associadas com a detecção de erros em *bits*, em blocos, ou erros de seqüência, introduzidos por enlaces e redes de comunicação. Entretanto, se os

cabeçalhos e fechos carregando as informações de controle não forem protegidas contra modificações, um intruso que conheça as técnicas pode contornar a verificação. Portanto, para garantir a integridade é necessário manter confidenciais e íntegras as informações de controle, usadas na detecção de modificações.

Os mecanismos de Enchimento de Tráfego consistem em uma geração de tráfego esporádico e o enchimento das unidades de dados, fazendo com que elas apresentem um comprimento constante, de modo a fornecer proteção contra análise de tráfego. Cabe ressaltar que, o mecanismo de enchimento só tem sentido caso as unidades de dados sejam criptografadas, impedindo que o tráfego esporádico seja distinguido do tráfego real. Esse mecanismo pode ser empregado, por exemplo, para impedir que o inimigo localize o computador central da rede, usando a técnica de análise de tráfego.

Existe a possibilidade de se Controlar o Roteamento de dados especificando rotas preferenciais (ou obrigatórias) para transferência das informações, podendo-se utiliza-las para garantir que estes dados sejam transmitidos em rotas fisicamente seguras, ou para garantir que informação sensível possa ser transportada em rotas, cujos canais de comunicação forneçam os níveis apropriados de proteção contra possíveis invasores não autorizados e indesejados.

Algumas medidas que garantam a Integridade Física e de Pessoal dos recursos de um sistema são indispensáveis para garantir a segurança do sistema como um todo. Por exemplo, não adianta usar um esquema sofisticado de autenticação para impedir acessos remotos aos arquivos em um disco, se o intruso puder ter acesso físico à máquina e roubar o seu disco rígido, se esta pessoa pode conectar pela porta de saída paralela do microcomputador um cabo de transferência de dados também ligado a outro microcomputador e, por meio deste cabo, conseguir transferir todas as informações necessárias. Para que se possa confiar nos mecanismos de segurança ao nível de *software* e *hardware*, que implementam a Política de Segurança do sistema, deve haver garantia do funcionamento correto do *hardware* e do *software* que implementam estes mecanismos. Para tanto, devem ser exigidas a aplicação de métodos formais de prova, verificação e validação, a detecção e o registro das tentativas de ataques identificadas e ainda, a garantia de que sua construção foi feita por pessoal de confiança em ambiente seguro, além da certeza de que não haverá violação física do equipamento. Os recursos no sistema devem ser associados a rótulos de segurança que indicam, por exemplo, seu nível de sensibilidade. O rótulo de segurança deve ser mantido junto com os dados quando eles são transmitidos.

A Detecção de Eventos Relevantes no contexto da segurança inclui a monitoração constante com o intuito de se efetuar uma detecção de aparentes violações a segurança

e deve incluir, adicionalmente, a detecção de eventos normais como, por exemplo, um *login* bem sucedido. Este mecanismo necessita do apoio de uma função de gerenciamento, que determinam quais são os eventos que devem ser detectados. É necessário ter recursos ao nível de *software* e *hardware* que possam registrar eventos significativos de ameaças à segurança de um sistema, que constitui-se em um importante mecanismo de segurança, pois possibilita a detecção e a investigação de possíveis violações da segurança, além de tornar possível realizar auditorias de segurança. Os serviços de segurança *OSI* são empregados nas camadas em combinações apropriadas, usualmente junto com os serviços e mecanismos que estão fora do escopo *OSI*, para satisfazer os requisitos de uma Política de Segurança.

A Autenticação é um serviço que trata da autenticação das entidades que são parceiras em uma comunicação, ou da autenticação da entidade que originou uma unidade de dados. O serviço de Autenticação de Parceiro, quando fornecido pela camada N, oferece a uma entidade N+1 uma comprovação de que sua parceira em uma comunicação é realmente quem diz ser. Este serviço é fornecido para ser utilizado no estabelecimento de uma conexão, ou esporadicamente durante a fase de transferência de dados de uma conexão, para confirmar as identidades das entidades participantes da conexão. O objetivo é garantir que uma entidade não está se passando por outra, ou repetindo de forma não autorizada uma mensagem previamente transmitida. Este serviço evita ataques do tipo Personificação e *Replay*.

O serviço de Autenticação da Origem de Uma Unidade de Dados, quando fornecido pela camada N, oferece a uma entidade N+1, uma comprovação de que a origem de uma unidade de dados, outra entidade N+1, é realmente quem reclama ser. O objetivo único desse serviço é autenticar a fonte de uma unidade de dados.

O serviço de Controle de Acesso tem o objetivo de fornecer proteção quanto ao uso não autorizado dos recursos, cujo acesso se dê via sistema de comunicação de dados via modelo *OSI*. Os recursos protegidos podem ser, ou não, recursos *OSI*. O serviço de proteção aplica-se aos diferentes tipos de acessos a um recurso. Por exemplo, o uso de um recurso de comunicação, a escrita, a leitura, ou a remoção de informações, ou a execução dos recursos de processamento.

O serviço de Confidencialidade dos Dados fornece proteção aos dados intercambiados no ambiente *OSI* contra revelação não autorizada da informação neles transportada. Este serviço é fornecido em diferentes níveis: em uma conexão, em uma unidade de dados, em campos selecionados das unidades de dados, ou protegendo contra monitoramento do fluxo de dados.

O serviço de Integridade de Dados atua no sentido de proteger os dados contra ataques ativos que implicam na modificação, remoção ou injeção não autorizada de unidades de dados. Esse serviço também é fornecido em diferentes níveis: em uma conexão com ou sem a opção de recuperação da informação original, em unidades de dados isoladas com ou sem recuperação e em campos selecionados nas unidades de dados trocadas em serviços com ou sem conexão.

O Serviço de Impedimento de Rejeição atua impedindo a rejeição de serviço, por meio de da prova da identidade das entidades que solicitam a execução de serviços, ou da prova que uma entidade de destino recebeu corretamente uma solicitação para realização de um determinado serviço.

Este tipo de serviço visa garantir duas situações:

1. Proteger a entidade receptora contra qualquer tentativa da entidade transmissora de negar o envio de uma unidade de dados. Por exemplo, um usuário, tendo se arrependido de uma compra realizada por meio de da rede, pode tentar alegar que não foi ele que enviou a mensagem com o pedido de compra.
2. Proteger o transmissor contra alegações falsas do receptor de que não recebeu uma unidade de dados ou o seu conteúdo. Por exemplo, proteger um cliente de uma companhia aérea que fez uma reserva e, ao chegar ao aeroporto, é informado que sua reserva não foi realizada.

### 4.2.9 CONCEITOS E DEFINIÇÕES DE *FIREWALL*

Segundo Soares et al. (1995), o *Firewall* é um mecanismo muito utilizado na prática para aumentar a segurança de redes, padrão *TCP/IP*, ligadas a *Internet*, que funciona como uma espécie de barreira de proteção à rede. A utilização de barreiras de proteção fundamenta-se no fato de que normalmente a segurança é inversamente proporcional a complexidade. Desta maneira, proteger máquinas de uso geral onde são executadas diferentes aplicações, de variados portes, é uma tarefa complicada, pois é muito improvável que nenhuma das várias aplicações apresente falhas que possam ser exploradas para violar a segurança do sistema. Sendo assim, torna-se muito mais fácil garantir a segurança isolando as máquinas de uso geral de acessos externos, usando uma barreira de proteção, ou *Firewall*, impedindo a exploração das possíveis falhas. O princípio da simplicidade tem como conseqüência a seguinte consideração: para diminuir os riscos, a configuração de um *Firewall* deve ser minimizada, excluindo tudo que não seja estritamente necessário. Um *Firewall* é definido como uma coleção de componentes, colocada entre duas redes, que coletivamente possua as seguintes propriedades:

- Todo o tráfego de dentro para fora da rede, e vice-versa, deve passar pelo *Firewall*;
- Só o tráfego autorizado pela política de segurança pode atravessar o *Firewall*;
- O *Firewall* deve ser àprova de violações.

Um *Firewall* pode ser visto como um monitor de referências para uma rede, sendo seu objetivo garantir a integridade dos recursos ligados a ela. A centralização demanda uma administração mais cuidadosa, por parte dos administradores do sistema e da(s) máquina(s) que implementa(m) o *Firewall*. Enquanto as máquinas de uso geral são configuradas para otimizar o desempenho e a facilidade de utilização, no *Firewall* tudo isso passa para o segundo plano, cedendo lugar ao seu objetivo principal no sistema: a segurança da rede. Os *Firewalls* são construídos tomando como base uma Política de Segurança da Informação, ou seja, em cima de critérios que asseguram a segurança da rede. Tais critérios são impostos para que os usuários externos possam acessar a rede interna e para que serviços de dentro possam dar acesso a *Hosts* externos.

Quaisquer tráfegos da rede, que não se encontram dentro destes critérios, são bloqueados por não estarem nos padrões pré-estabelecidos na lista de critérios.

Um *Firewall* normalmente obedece a um esquema conforme Figura 15:

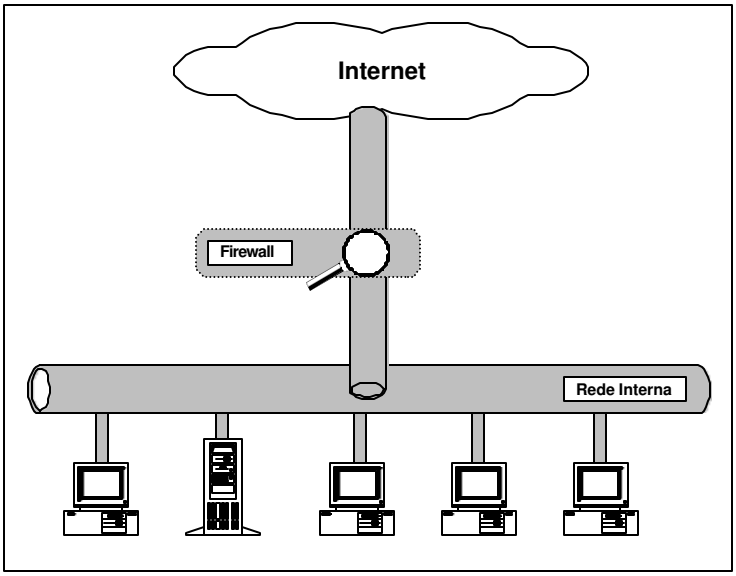



Figura 15 - Esquema de Firewall

Fonte: Wladlow, Thomas A. (2000, p. 237).

Os filtros bloqueiam a transmissão de algumas classes de tráfego. O componente *gateway* é uma máquina, ou um conjunto de máquinas conectadas por um segmento de redes, que fornecem serviços de retransmissão.

O filtro colocado na saída (entre a rede externa e o *gateway*) é usado para proteger o *gateway* de ataques externos, enquanto o filtro interno protege a rede interna das conseqüências de um ataque que tenha conseguido comprometer o funcionamento do *gateway*.

Desta maneira, os dois filtros atuando isoladamente, ou em conjunto, protegem a rede interna de ataques externos. *Firewalls* precisam ser capazes de permitir ou não o tráfego, baseando-se:

- No tipo de sessão da rede (*FTP*, *Telnet*, *login* remoto, etc.);
- Endereço de origem e destino do tráfego;
- No usuário que envia, ou no usuário que recebe.

Para flexibilizar, um *Firewall* deve ser capaz de combinar tipos de autenticação. Por exemplo:

- Permitir *Telnet* somente para certos usuários;
- Permitir ou prever usuários externos específicos para usar *FTP* ou serviço da *WWW*;
- Proibir ou não todos os *FTP's* e *Telnet's* externos.

O modo tradicional de se autenticar o usuário é por meio de senhas e nomes de usuários. Este modo, apesar de ser o mais usado, é bastante vulnerável, pois, na maioria dos casos os usuários utilizam a mesma senha para todos os acessos à rede, a qual fica vulnerável a *Hackers* que conseguem utilizar técnicas para descobrir senhas e nomes de usuários por meio de conexões "indesejáveis" à rede. Com a senha, os *Hackers* conseguem ter acesso a outras máquinas da rede.

Ao se configurar um *Firewall* deve se manter fechadas as funções da rede que não são utilizadas com freqüência, pois este ponto pode servir de alvo para ataques. Para se prever uma rede exposta por meio deste ponto de acesso, um *Firewall* deve fechar todas as aplicações e *hardware* abertos que não estejam sendo utilizados. Isto inclui:

- Fechar portas e acessos a redes não mais utilizadas.
- Bloquear todos os limites internos e externos ultrapassados durante o serviço da rede.
- Ser capaz de bloquear qualquer tipo de tráfego inseguro.

# CAPÍTULO V

# SEGURANÇA EM CORREIO ELETRÔNICO ( *E-MAIL*)

## 5.1 O CORREIO TRADICIONAL

Segundo Schneier (1995) *apud* Pagliusi (1998), a linguagem escrita possibilitou ao ser humano deixar seu testemunho e seu conhecimento para ser lembrado ao longo do tempo e da distância geográfica. Esta linguagem é o principal repositório de cultura de uma civilização. O fato de se fazer um testemunho por meio das distâncias geográficas, povos distantes e culturas, é ter poder e influência. Este fato permite a coordenação de atividades envolvendo grandes áreas geográficas e de populações. A infra-estrutura existente para se conseguir este objetivo é denominada correio. Apesar do correio moderno ter nascido oficialmente com a invenção do selo postal, há aproximadamente 150 anos, ele remonta a Pérsia antiga.

O correio na maioria das vezes é considerado uma função governamental e também tem sido uma função exercida pelas igrejas, universidades ou entidades

comerciais. Conforme o passar do tempo, sofreu modificações a cada avanço na tecnologia do transporte. Ele foi uma das primeiras justificativas encontradas para o uso da carruagem, para a estrada de ferro e para a aviação.

Os governos sempre desejaram controlá-lo por razões de segurança de estado e em função da utilização de rendimentos públicos para seu suporte. Desde os tempos do Império Romano, estes fatos relativos ao correio são observados e justificados, em parte, pelo papel dos governos na construção de estradas e expansão geográfica pelo país. A Administração e o controle do correio também tem sido utilizado para justificar a intervenção dos governos em outras áreas. A espionagem industrial e tecnológica se encaixa como exemplos deste tipo de intervenção.

O assunto Segurança tem sido uma preocupação do correio desde os primórdios tempos da Antiguidade, quando as cartas mais importantes eram redigidas pelos soberanos que normalmente mandavam cortar a língua de seus mensageiros, para que não pudessem passar adiante uma informação importante e confidencial. Atualmente, a Segurança ainda é muito importante no correio. A Segurança no correio consiste em se enviar uma mensagem somente para o destinatário, com confidencialidade e ter a certeza que somente ele irá ter acesso àmesma.

O padrão moderno de confidencialidade no correio consiste do envelope branco simples, dentro de onde quase toda correspondência comercial se movimenta. Uma combinação de cultura, leis e capacidade potencial evidenciam o envelopamento como ato de proteger a confidencialidade da informação em seu interior. Existe uma pequena parcela das mensagens que requerem um grau de Segurança mais elevado. Para esta parcela, são utilizados normalmente dois envelopes, ou seja, mala postal lacrada de couro ou de lona, ou até mesmo um mensageiro especial com uma maleta algemada ao seu pulso. Antes do serviço postal moderno, havia uma grande quantidade de correspondências que não conseguiam chegar ao seu destino. O emissor reagia, então, enviando várias mensagens importantes para vários e diferentes caminhos. Esta atitude aumentava, por outro lado, a probabilidade do conteúdo da mensagem ser descoberto ou extraviado.

O correio moderno reagiu a este tipo de atitude oferecendo um serviço diferenciado e com preços também diferenciados. Os serviços de primeira classe passaram a contar com opções de retorno ao emissor, o AR (Aviso de Recebimento), no caso da mensagem ou encomenda não atingir seu destinatário. Serviços opcionais para uma entrega segura foram incluídos, tais como: o retorno do recebimento ao emissor e a correspondência registrada e segurada, para prevenir casos de perda ou furto.

Há dezenas de problemas de segurança nos sistemas de correio atuais. Há problemas internos, tais como o furto de correspondência pelos próprios funcionários do correio, muitas vezes em cooperação ilegal com autoridades judiciais ou da segurança nacional. Há problemas externos, tais como o furto de talões de cheque e de cartões de crédito das caixas de correspondência. Há uma quantidade enorme de fraudes, agravadas também pelo relaxamento das práticas de segurança de grande parte dos usuários, entre elas a não confirmação da mudança de nomes e de endereços.

Estes problemas, apesar de serem preocupantes, não afetam a real necessidade da utilização continuada dos sistemas de correio. Em parte porque os usuários não reconhecem o risco e em parte porque o aceitam ou então não tomam providências para se precaver. Em geral, os problemas de segurança não são graves o suficiente para danificar o sistema. O correio tem prosperado ou ficado debilitado de acordo com a civilização. Ele cresce quando a civilização prospera, e se enfraquece quando a civilização fica em má situação. Ao surgir uma nova era tecnológica, é um ótimo negócio para ambos o fato de o outro prosperar.

## 5.2 O CORREIO ELETRÔNICO

Existem poucas tecnologias sustentando a promessa do correio eletrônico profissional e altamente tecnológico. Para muitos de nós, ele ainda é uma novidade não completamente dominada, mas o correio eletrônico já está no ar há 30 anos e, segundo Grimberg (2001), a sua criação se deu em outubro de 1971, nos Estados Unidos, com a escolha do símbolo @ (arroba), em inglês, "at", como a preposição de lugar, para separar a identificação de uma caixa postal de usuários do nome do local em que a está hospedando. O “pai” do *e-mail* é o engenheiro norte-americano Ray Tomlinson, que mandou a primeira carta eletrônica, toda escrita em letras maiúsculas. O *Spam* - mensagens não solicitadas, especialmente propagandas, que chegam ao computador, geralmente são informações indesejáveis e têm a finalidade de provocar algum problema, seja no microcomputador ou à rede destinatária. Outono de 1971 nos EUA. A missão: desenvolver a *ARPANET*, uma rede criada três anos antes pelo Departamento de Defesa dos EUA e que, anos depois, daria origem à *Internet*. Neste contexto, o engenheiro Ray Tomlinson, que trabalhava para a companhia BBN, empresa envolvida no projeto, resolveu fazer um uso diferente do software *SNDMSG* (contração da expressão "send message", ou "envie mensagem"), que havia desenvolvido para que os programadores e pesquisadores do projeto deixassem mensagens uns para os outros. Existia uma limitação, pois o sistema somente funcionava se os usuários compartilhassem

a mesma máquina. Tomlinson fez, então, uma escolha simples, porém fundamental para o funcionamento do que viria ser um dos maiores fenômenos de popularidade da história, *o e-mail*. A escolha do símbolo @ (arroba) foi bastante significativa, indicando destinatários que estavam em computadores diferentes. Com o sistema funcionando, o *SNDMSG* passou a ser distribuído para pesquisadores em outros locais. Surpreendentemente, uma pesquisa feita dois anos depois revelou que três quartos de todo o tráfego da *ARPANET* era *e-mail*. Desde o tempo em que Tomlinson enviou a primeira mensagem entre computadores, seus princípios não mudaram. Os *e-mails* continuam, como naquela época, sendo mensagens de texto, mesmo quando aparecem com fotos, cores e documentos anexos, que vão de um lado a outro em uma rede de computadores. Seja um documento *HTML* ou um vídeo, a transmissão se dá de maneira igual à de 30 anos atrás: a mensagem é convertida para o formato de texto simples e passa para um servidor, o qual procura o domínio de destino. O servidor deste último, por sua vez, entende o que vem antes da @ como a identificação do destinatário e entrega o texto para a "caixa" dele. Na prática, diferentemente do que se poderia prever, a comunicação eletrônica popularizou-se a ponto de se tornar muito mais do que o simples envio de mensagens de texto. Além das conversas de caráter estratégico e de segurança, como na *ARPANET*, o *e-mail* se tornou instrumento de trabalho, de divulgação de notícias e anúncios, de diversão, e até um meio de realizar transferências monetárias, inclusive nas utilidades diversas, como substituir disquetes para transportar arquivos. Atualmente, segundo um estudo divulgado em setembro pelo IDC, são trocados, atualmente, mais de 10 bilhões de *e-mails* por dia. Em 2005, deverão ser 36 bilhões de *e-mails* em trânsito diariamente. Já o Instituto Messaging Online, no ano passado, previu que, em 2002, a quantidade de caixas postais espalhadas pelo mundo será 1 bilhão, um aumento de 83% em relação àverificada no fim de 1999 (569 milhões). Apesar de o número previsto representar aproximadamente um sexto da população mundial, a quantidade de pessoas beneficiadas por essa tecnologia provavelmente é bem menor, já que muitas pessoas possuem mais de uma conta.

Segundo Pagliusi (1998), o serviço de correio eletrônico que, assim como a *internet*, era de uso restrito até o fim da década de 80, tornou-se popular e atualmente está presente no dia-a-dia e nos computadores de pessoas das mais diferentes idades e atividades, de estudantes a executivos, inclusive entidades terroristas. É possível de se constatar que quase todas as implementações de correio eletrônico que foram executadas até hoje podem ser descritas como tecnologias de brinquedo, nada muito profissional. Elas são divertidas e interessantes, contudo não podem ser consideradas sérias. Embora tenham crescido rapidamente, ainda carregam apenas uma pequena

quantidade de tráfego de mensagens, sendo que não foram projetadas para serem bem sucedidas. Foram apenas concebidas e, para com o passar do tempo, serem aperfeiçoadas. A maioria teve um sucesso muito além do esperado por seus criadores e patrocinadores e a maioria dos sistemas de correio tradicionais também não foi projetada para ser o que é atualmente, pois eles apenas cresceram. Na verdade, isto faz parte de sua beleza. Os serviços foram adicionados, desenvolvidos e introduzidos lentamente como resposta a uma necessidade ou como resposta a algum desenvolvimento tecnológico. O sistema de correio eletrônico também está crescendo da mesma maneira por meio da interconexão de diversos sistemas, pela exploração do uso do telefone, do Fax (FAC-Simile) e até mesmo da tecnologia dos sistemas de páginas. Pela cooperação de milhares de pequenos empreendimentos comerciais com alguns pouco grandes. Em resumo, ele cresce porque seus usuários, sejam indivíduos ou instituições, desfrutam de vantagens econômicas sobre os não usuários.

Até o presente momento, o papel dos governos com relação ao correio eletrônico tem sido limitado. Nos *EUA* (Estados Unidos da América), o governo patrocinou toda a *Internet*, principalmente a pesquisa básica. Em outros países, como no Brasil, por enquanto o governo tem simplesmente ficado indiferente. Desta maneira, o correio eletrônico ainda não é uma função governamental, sendo caracterizado mais para um esforço cooperativo coletivo conduzido mais por acordos e costumes, de modo formal ou informal, do que por leis ou regulamentos. Na medida em que o correio eletrônico provê sua importância, pode-se esperar que haja cada vez mais tentativas por parte dos governos de se efetuar um controle maior sobre ele, da mesma maneira que cooptaram o sistema de correio tradicional. Acredita-se que a desculpa que será utilizada estará relacionada à segurança, porém o real motivo será a manutenção do controle e da influência política.

Em termos com características mais técnicas relacionadas ao assunto, o poder, a força e o valor de um meio de comunicação crescem com o número de suas conexões potenciais e com a velocidade de suas mensagens. O telefone proporciona a habilidade de troca de informações quase instantâneas, mas apenas síncronas e somente entre um número limitado de pessoas ao mesmo tempo. Para a maioria, ele também não deixa nenhum registro. O rádio e a televisão são ambos síncronos e do tipo “um-para-muitos”. Quanto ao sistema de correio eletrônico, ele consegue ser assíncrono e “muitos-para-muitos”, enquanto que os sistemas de hoje são limitados a texto, os do futuro prometem uma troca ilimitada de uma mistura de voz, som, fotografia, imagem e dados. Não se discute que o impacto cultural do correio eletrônico bem sucedido em nossa civilização é potencialmente maior do que o do telefone e cria uma rivalidade com o do papel.

### 5.2.1 O CORREIO ELETRÔNICO SEGURO

Segundo Caruso (1999), segurança, isto é, confidencialidade, confiabilidade e autenticidade da informação tornam-se essenciais para o sucesso do correio eletrônico. As organizações, as universidades, as empresas e as pessoas não irão utilizar um sistema de correio em que elas não possam confiar para despachar suas mensagens. Embora muitas das mensagens poderiam seguir em um cartão postal, elas não irão utilizar um sistema em que todas as suas mensagens devam seguir por meio deste recurso. Embora elas não lacrem todos os seus envelopes, os usuários não irão utilizar um sistema em que não haja envelopes. Apesar de confiarem no carteiro, elas não irão utilizar um sistema em que sejam obrigadas a confiar neste funcionário. Embora se utilize um sistema de brinquedo para algumas aplicações, elas esperam um sistema maduro e robusto para a maioria de suas aplicações. Acredita-se que a Segurança do *e-mail* e do trânsito da informação eletrônica é fundamental para o sucesso da comunicação eletrônica entre os povos e para o comércio eletrônico. O mecanismo fundamental para prover a segurança de mensagens codificadas binárias, em uma rede aberta, consiste da criptografia. Ela possibilita a emulação de todos os controles em que temos, historicamente, confiados. A criptografia de *chave* pública permite a emulação não somente de envelopes, mas também de assinaturas. Embora existam as estruturas primitivas necessárias, não há ainda também uma necessária infra-estrutura para efetuar o seu devido amparo. Muito além de possuir recursos para o armazenamento de uma mensagem, um sistema de correio comum deve ter uma infra-estrutura para seu transporte e distribuição. Ele precisa poder contar com caminhões, aviões, agências, um sistema de endereçamento e códigos postais. Da mesma maneira, um sistema eletrônico de envelopes e assinaturas lógicas deve possuir uma infra-estrutura adequada para atribuição de nomes e distribuição de *chaves* criptográficas (cadeia aleatória de bits utilizada em conjunto com um *algoritmo*). Espera-se que assim que o correio eletrônico evoluir de um sistema de brinquedo para um sistema com a devida infra-estrutura, vários dos seus problemas serão solucionados.

Apesar da Segurança não ser o mais significativo dentre eles, ela também não é o menos importante. A *Internet* é o laboratório onde tais problemas são pesquisados e onde os protótipos das soluções são concebidos e são implementados. Conforme o avanço destes experimentos na *Internet*, espera-se que seja gerado um modelo análogo ao do correio tradicional, pois a maior parte do que os usuários comuns conhecem sobre segurança e controle em um sistema de correio eletrônico, foi aprendida a partir do

modelo de papel. Até o ponto em que o novo sistema seguirá este modelo, ele irá explorar os hábitos dos usuários. Ao passo que, se falhar em operar da maneira que os usuários habitualmente esperam, ele provocará erros de utilização. Na medida em que as expectativas de segurança dos usuários não forem satisfeitas, o sucesso definitivo do correio eletrônico estará colocado em risco e, conforme o seu público se tornar cada vez mais apreensivo e preocupado, a intromissão governamental estará sendo solicitada e será justificada.

### 5.2.2 CARACTERÍSTICAS DO CORREIO ELETRÔNICO

Segundo Garfinkel (1995) *apud* Pagliusi (1998), o complexo existente denominado Correio Eletrônico ou simplesmente *e-mail* é, atualmente, o sistema digital de maior alcance mundial para a troca de mensagens, tendo se tornado um grande fator de motivação para a interconexão das Redes de Computadores. *O e-mail* tem ultrapassado as barreiras geográficas. Não se trata apenas da troca de mensagens eletrônicas dentro de empresas. Atualmente a troca de mensagens eletrônicas entre instituições é corriqueira e intensa. Mais de dez bilhões de *e-mails* circulam pelas redes de computadores todos os dias. Comparado com outras opções tecnológicas, as vantagens da utilização *do e-mail* são evidenciadas por diversos aspectos. Um aspecto importante é a rapidez, permitindo que uma mensagem circule por bairros, cidades ou países, sendo entregue ao destino quase imediatamente após o seu envio. Existe ainda o fato do receptor não precisar estar conectado nem precisar interromper suas atividades para receber mensagens, representando uma enorme vantagem sobre o telefone, que exige a disponibilidade imediata do receptor. Constatamos também a possibilidade do receptor manipular digitalmente a mensagem da forma que mais lhe convier com a opção vantajosa da concisão do assunto. Quando uma pessoa escreve suas mensagens tem o hábito de organizar melhor suas idéias, resultando em uma forma de comunicação mais breve e produtiva. Além disso, as mensagens eletrônicas podem ser compostas de texto, som, imagem, animação e até código executável de programa, mesmo sabendo-se que o majoritário *do e-mail* é na troca de mensagens do tipo texto. Observando todas estas características e vantagens, os sistemas *de e-mail* são o meio de comunicação mais praticado e com maior uso da atualidade. O correio eletrônico tem expandido o seu alcance a cada novo dia. Por meio dele, existe a troca de mensagens entre amigos, clientes e fornecedores, parceiros de negócios e até entre órgãos do governo. Seus usuários podem estar conectados por *e-mail,* mesmo quando em viagem, no trânsito, no

trabalho ou em casa, independentemente do tipo de sistema de correio eletrônico empregado, de sistema operacional executado ou do computador utilizado.

### 5.3 A FALTA DE SEGURANÇA NA TROCA DE *E-MAILS* VIA *INTERNET*

Segundo Pagliusi (1998), uma característica importante é a de que os *e-mails* trafegam de uma rede a outra até seus destinatários, por meio de canais nem sempre seguros. O maior serviço *de e-mail* existente, o da *Internet*, não oferece aos seus usuários os recursos mínimos necessários de privacidade, segurança e autenticação das mensagens que encaminha. Deste modo, ele expõe as mensagens dos seus usuários a uma série de ameaças àsegurança e a diversos tipos de ataques existentes por meio de *Hackers*. A implementação de mecanismos de segurança é de total responsabilidade do próprio usuário. Com o intuito de se dificultar ou até impedir o acesso indevido ou a manipulação por pessoas não autorizadas, dos seus *e-mails* enviados ou recebidos, é necessário que se utilize *algoritmos* de criptografia externos ao seu sistema de correio eletrônico. Para atender às necessidades de sigilo e de autenticação em sua troca de mensagens pela *Internet*, o usuário se vê forçado, então, a recorrer aos pacotes de segurança baseados em criptografia atualmente disponíveis, como os programas *PGP* (Pretty Good Privacy, programa de Criptografia que provê recursos de sigilo e de autenticação para mensagens eletrônicas e arquivos) e *RIPEM* (Riordan´s Internet Privacy Enhanced Mail, implementação assimétrica do padrão *PEM* (Privacy Enhanced Mail, conjunto de procedimentos destinados a prover segurança ao correio eletrônico da *Internet*). Trata-se de um programa de proteção de *e-mail* escrito por Mark Riordan), sendo este último uma implementação do padrão *PEM*.

Existe um agravante, pois estes programas de segurança são de ambientes externos ao sistema de correio eletrônico utilizado pelo usuário e implica em uma enorme perda de produtividade. Um outro agravante é que demanda a aprendizagem de novos comandos que, muitas vezes, não são nada amigáveis para o usuário final. Desta maneira, para se obter a segurança desejada, além do programa de correio eletrônico, o usuário precisa dedicar um tempo adicional para aprender a manusear um programa de criptografia externo e também importar e exportar arquivos contendo mensagens em claro ou cifradas, de um sistema para outro. Atualmente, com a crescente integração de redes, antes isoladas, a *Internet*, usuários do mundo inteiro podendo ter acesso a qualquer rede interligada, tornaram todos os problemas de segurança mais evidentes. Entre tais problemas, os mais comuns são as tentativas e os acessos indevidos aos computadores, especialmente os que trabalham com a captura de pacotes que trafegam

pela rede. Assim, o sistema *de e-mail da* Internet é um alvo fácil de ataque, por não implementar mecanismos de proteção às mensagens. Em geral, elas ficam gravadas em formato texto legível na *mailbox* (localidade de armazenamento de mensagens de correio eletrônico ou de voz), do usuário ou são encaminhadas por este sem nenhum recurso de segurança. Além disso, não há garantias quanto à integridade dos seus conteúdos nem quanto à autenticidade de seus emissores. Também nada garante que o emissor, posteriormente, não possa negar que tenha enviado uma mensagem que na verdade tenha despachado, caso isto lhe convenha.

Uma das formas de se obter segurança na troca de *e-mails* é ter um programa, no nível de aplicação, que os assine e cifre, já incorporado no próprio sistema de correio eletrônico. Consistindo de uma extensão oferecendo segurança, este programa precisa, então, garantir a confidencialidade e a integridade do conteúdo, a autenticidade e o não repúdio da origem da mensagem. Além disso, este programa precisa oferecer não apenas segurança, mas também flexibilidade, por exemplo, podendo ser executado em diferentes plataformas, como o *Unix* ou o *Windows NT Server 4*, e adaptabilidade, oferecendo o emprego de uma variedade de diferentes *algoritmos*, e uma boa *interface* (fronteira compartilhada, ponto físico de demarcação entre dois dispositivos, procedimentos, códigos e protocolos que permitem que duas entidades troquem informações), com o usuário, contendo menus e comandos amigáveis.

## 5.4 CONCEITOS BÁSICOS ENVOLVENDO CORREIO ELETRÔNICO

Segundo Sproull (1995) apud Pagliusi (1998), para possibilitar a localização do destinatário, o correio eletrônico utiliza o conceito de endereço. Um endereço de correio eletrônico equivale a um endereço postal e deve conter todas as informações necessárias para o envio de uma mensagem ao destinatário. Conforme for a sofisticação do programa, a informação enviada pode ser uma mensagem, um documento, um programa, dados estatísticos, som, imagem, animação ou mesmo uma coleção de mensagens organizadas, uma discussão reenviada a partir de alguma outra *mailbox*. Conforme convier ao destinatário, ele pode ler um *e-mail*, editar, salvar, eliminar, mover para outro arquivo, retransmitir para alguém ou responder ao emissor.

### 5.4.1 ATRIBUIÇÃO DE NOMES

Segundo Soares et al. (1995), todas as mensagens eletrônicas devem indicar precisamente *a mailbox* do destinatário. Caso houvesse a possibilidade de se utilizar

nomes como "João da Silva", mas nomes geralmente são únicos, e o sistema de correio eletrônico ou *e-mail,* tem informações insuficientes para resolver tais problemas de ambigüidades de maneira adequada. Alguns sistemas associam números às *mailboxes,* mas esta técnica obriga o emissor a lembrar-se ou a procurar o número da *mailbox* em uma lista.

Uma solução melhor é adicionar endereços a nomes, da mesma forma que endereços são colocados em envelopes, de modo que nomes e endereços juntos identifiquem uma única *mailbox.* Por exemplo, "João da Silva, do Departamento de Informática, da Universidade de Taubaté, no Brasil" pode ser suficiente para o sistema identificar uma única *mailbox e* fornecer ao sistema de correio eletrônico a informação necessária para transportar um *e-mail do* emissor ao destinatário. Tendo-se em vista que mais de dez bilhões de *e-mails* circulam nas redes de computadores todos os dias, parece evidente que as questões em torno de atribuição de nomes e endereçamento são bem mais complexas do que uma simples discussão sugere. Planejar um esquema que possa ser utilizado ao redor do mundo e de maneira harmoniosa, por milhões de pessoas, é um desafio que tem sobrecarregado os comitês que estipulam padrões para o correio eletrônico e gerado um grande número de horas de discussões sobre o assunto.

### 5.4.2 FORMATO DA MENSAGEM

Segundo Teixeira (1996) *apud* Pagliusi (1998), todos os sistemas de computação têm seu próprio sistema de correio eletrônico e, com freqüência os formatos utilizados nas mensagens são incompatíveis, porém, existe um formato amplamente utilizado em diversas redes de computadores. Este formato é muitas vezes identificado pelo nome do documento que o define,por exemplo a RFC 822. *RFC* é uma abreviação para *"Request for Comment"*. Esta *RFC* faz parte do processo de padronização da *IETF* (Internet Engineering Task Force) - comitê especial que define os padrões para o protocolo *TCP/IP.* A RFC 822 é, atualmente, largamente utilizada em várias organizações em pesquisas e no desenvolvimento de redes mundiais. O formato de mensagem RFC 822 tornou-se o padrão de transferência de fato dos sistemas de correio atuais e este formato torna-se particularmente importante quando as mensagens cruzam, de uma rede a outra, por meio dos *gaterways*. Os *gateways* de *e-mail* são máquinas que implementam mais de um protocolo de transferência de *e-mail*, resolvendo o problema da comunicação entre sistemas de correio eletrônico distinto. Tais *gateways* irão reconhecer não apenas

seu próprio formato de mensagem, mas também a sintaxe dos endereços descritos na RFC 822. Um exemplo consiste no *gateway TCP/IP* para *OSI*, onde as mensagens recebidas utilizando uma porta *TCP/IP* em uma rede são repassadas para uma porta de outra rede por meio do *MOTIS* (o protocolo de correio eletrônico da I.S.O). No padrão RFC 822, as mensagens são vistas como tendo um envelope e um conteúdo. O envelope contém a informação necessária para o envio da mensagem e o conteúdo consiste no objeto a ser despachado para o receptor.

Na Figura 16 tem-se um exemplo da anatomia da mensagem de correio eletrônico:

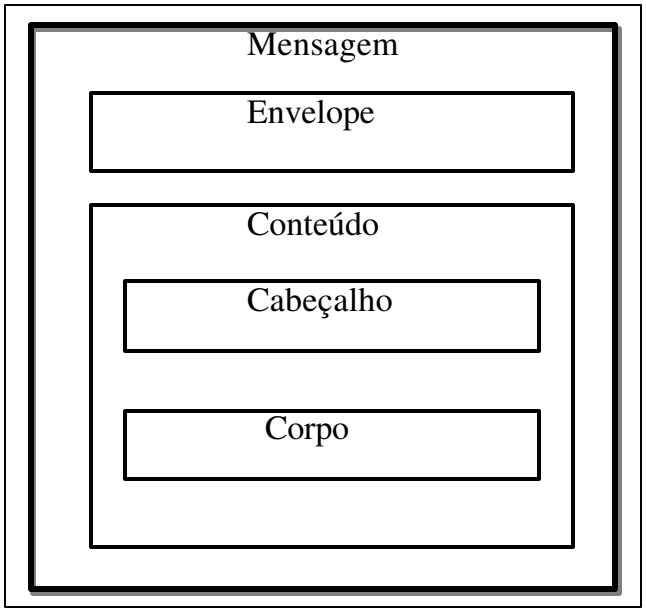



Figura 16 – Anatomia de uma Mensagem

Fonte: Allman (1995) *apud* Pagliusi. (1998, p.11).

Segundo Allman (1995) apud Pagliusi (1998), este padrão aplica-se somente ao formato e a algumas semânticas do conteúdo da mensagem. Não possui especificações sobre a informação contida no envelope, entretanto, alguns sistemas de correio eletrônico podem utilizar informações do conteúdo *do e-mail* para criar o envelope. O padrão RFC 822 facilita a aquisição destas informações por programas. A conceituação de *envelope é* análoga ao envelope físico utilizado para o envio de uma carta postal. Se for preciso enviar cópias de um documento para duas pessoas localizadas em lugares distintos, cada cópia do mesmo seguirá em um envelope diferente e o mesmo ocorrer com uma mensagem eletrônica. Na Figura 17 tem-se um exemplo de mensagem eletrônica via *e-mail*.

From: João da Silva <silva@inf.unitau.br>
To: José de Souza <souza@infocad.com.br>
Cc: Mario Nogueira@TDEInfoway.com.br
Bcc: chaves@Wingate.com.br
Subject: novos contatos.
Date: Sat,31 May 9715:13:38-0200(EDT)
Caro José,
Achei suas idéias interessantes e passei adiante seu esboço (por meio de um "forward" para um amigo Mario Nogueira, no Brasil. Talvez você receba um retorno dele, em breve. Abraços, João.

Figura 17 – Exemplo de Uma Mensagem

Fonte: Allman (1995) *apud* Pagliusi. (1998, p.12).

O conteúdo de uma mensagem divide-se em duas partes, um cabeçalho e um corpo separados por exatamente uma linha em branco, que é uma parte essencial do formato. Muitos sistemas de *e-mail* asseguram sua existência de forma automática.

*O* cabeçalho contém informações sobre o emissor, os receptores, a data do envio e o assunto da mensagem, entre outras. Ele é organizado em linhas e cada linha possui um campo formado por uma palavra-chave, seguida de dois pontos de separação e de uma informação. Uma grande parte dos sistemas de *e-mail* oferece somente as linhas de cabeçalho essenciais. São elas:

**To:**

**From:**

**Date:**

**Subject:**

As linhas From: e Date: são, em geral, inseridas automaticamente, mas pode-se acrescentar mais atributos no cabeçalho de uma mensagem eletrônica. As linhas de cabeçalho, que são mais importantes, e seus respectivos significados são apresentados a seguir:

**From:** Endereço do emissor. Deve haver somente uma destas linhas no cabeçalho.

**To:** Receptor(es) principal(ais) da mensagem. Esta linha pode especificar mais de um endereço de destino. Neste caso, os endereços devem vir separados por vírgulas ou espaços.

**Cc:** Receptor(es) de cópia. Esta é a cópia carbono (Cc é a sigla para *Carbon* Copy) da era eletrônica. O endereço eletrônico que estiver nesta linha, receberá uma cópia da mensagem apenas para sua informação.

**Bcc:** Receptor(es) de cópia "cega" *(Bcc é* a sigla para *Blind Carbon Copy).* Para o caso de alguém querer enviar uma cópia para terceiros, sem notificar o(s) outro(s) receptor(es) da mensagem.

**Subject:** Assunto da mensagem. Este é um texto livre. Deve-se escolher um assunto curto e significativo, sem esquecer-se da pontuação. Embora a presença desta linha não seja obrigatória, seu uso é altamente recomendável.

**Date:** Data e hora em que a mensagem foi enviada. Sendo que é importante que a notação da data siga um formato padrão, pois muitos programas podem estar capacitados a classificar mensagens pela data na *mailbox*. A maioria dos sistemas de *e-mail* insere linhas *Date:* corretamente formatadas de modo automático (exemplo: 02 Jun 9716:03:17 -0500). Alguns não permitem a inclusão manual de informações neste campo.

**Message-Id**: Identificador único da mensagem que é fornecido pelo host do emissor. Estes campos são utilizados quando se trabalha com correio eletrônico. Ainda existem várias polêmicas a respeito dos serviços providos pelo correio eletrônico, segurança e privacidade do mesmo.

**Received:** Esta é uma informação relativa a rastreamento e é utilizada para a análise de problemas no envio das mensagens do correio eletrônico. Normalmente ela é composta por múltiplas linhas, que demonstram quando e em que computadores a mensagem passou.

**Resent-From:** Endereço da pessoa ou programa a partir de onde a mensagem se originou. Campos começando com Resent - indicam que a mensagem foi reenviada, ou seja "*forwarded*", No caso do Resent-From:, pela pessoa identificada na linha. Pode haver outras linhas, tais como: Resent-To: e Resent-Cc:.

**Reply-To:** É o endereço da pessoa a quem se deverá responder a mensagem. Em muitos casos, contém o endereço do emissor da mensagem e consiste também numa oportunidade para automaticamente reenviar todas as respostas diretamente para outro lugar ou pessoa, sem precisar perguntar pelo endereço do emissor na própria mensagem. Em adição, podem existir outras linhas, tais como Sender:, que é utilizado para identificar o emissor, caso este seja diferente do autor demonstrado no endereço da mailbox (por exemplo, no caso de From: postmaster). Todos estes comandos são recursos ativos nos principais softwares de correio eletrônico existentes e são reconhecidos mundialmente. Estes recursos padronizados facilitam o uso deste tipo de ferramenta para todos os usuários, que os reconhecem sempre que estão trabalhando.

O corpo da mensagem contém o texto completo da mesma, em um formato *ASCII* que permite sua impressão de 7 bits e as mensagens não-texto, do tipo: vóz, fax,

imagens, *EDI* (Electronic Data Interchange), Código *Binário*, que exigem caracteres de 8 *bits*, precisando ser, de alguma maneira, codificadas em caracteres de 7 *bits*. Numa grande maioria dos sistemas de Correio Eletrônico, não é permitido o envio de códigos *binários* de 8 *bits*, sem antes se executar alguns procedimentos especiais, pois o problema consiste no "oitavo bit" que pode ser perdido quando transferido em formato *ASCII* ou *EBCDIC*. Para que se possa salvar todos os códigos de controle ou caracteres especiais ligados ao oitavo *bit*, é necessário codificar antes os *binários* em 7 *bits ASCII* ou *EBCDIC* e, na seqüência, efetuar a transferência e posteriormente efetuar a decodificação do formato de 7 *bits* para o de 8 *bits* no destino. Na maioria dos sistemas de *e-mail*, existem programas que realizam tais procedimentos de forma transparente ao usuário. Alguns *sites* da *Internet* estipulam o tamanho máximo de uma mensagem em 10.000 *Bytes*. Outros, como por exemplo, os da rede Eunet e CSRG Berkeley LTNIX, estipulam este limite em 100.000 *Bytes*. Existem *Sites* (são espaços ou páginas disponíveis na *Internet* para acesso a informações relativas a empresas ou qualquer entidade que queira apresentar informações suas na *Internet*), que não estipulam limite para o tamanho da mensagem, como os da rede UUNET e, em geral, o limite de 64.000 *Bytes* é um limite seguro a ser observado.

### 5.4.3 FORMATO DA SINTAXE DOS ENDEREÇOS

Segundo Pagliusi (1998), o correio eletrônico tem funções próprias para processamento dos endereços de seus usuários. Um remetente pode enviar simultaneamente várias cópias de uma mensagem, para diferentes destinatários utilizando o conceito de lista de distribuição (é um nome que identifica um grupo de usuários). O formato dos endereços eletrônicos *SMTP* é o seguinte: nome_local@nome_do_domínio , onde o nome_do_domínio identifica o domínio ao qual a máquina de destino pertence, o nome_local identifica a caixa postal do destinatário. O *SMTP* especifica como o sistema de correio eletrônico transfere mensagens de uma máquina para outra. O módulo *interface* com o usuário é a forma como as mensagens são armazenadas não são definidas pelo protocolo *SMTP*. O sistema de correio eletrônico pode também ser utilizado por processos de aplicação para transmitir mensagens contendo textos.

Os serviços de segurança necessários para o correio eletrônico deverão incluir confidencialidade e integridade em transmissões sem conexão, autenticação das origens das mensagens e, impedimento de rejeição pelo destinatário e remetente. O *Sendmail* (Gerenciador de mensagens mais comum no Sistema Operacional *Unix*), tem sido um

dos maiores causadores de problemas de segurança. Recomenda-se sempre manter a versão mais atual do *Sendmail* de maneira a ter as últimas correções. Observa-se abaixo três formas distintas de se montar um endereço hipotético de emissor de correio eletrônico, que geralmente são encontradas no cabeçalho de uma mensagem eletrônica:

From: silva@inf.unitau.br (José da Silva)

From: José da Silva <silva@inf.unitau.br>

From: silva@inf.unitau.br

A cadeia de caracteres *José da Silva,* apesar de fornecer o nome do emissor, não faz parte do endereço utilizado pelo sistema para efetuar o *roteamento* das mensagens. O sistema de *e-mail* interpreta e processa todos os três endereços acima de maneira idêntica, pois ele observa apenas a cadeia de caracteres silva@inf.unitau.br, que na realidade, esta cadeia de caracteres consiste no endereço real de *e-mail.*

No exemplo acima, o nome *José da Silva é* considerado como apenas um comentário que é repassado, sem modificações, pelo sistema de *e-mail*. Existe a possibilidade de se colocar este comentário entre parêntesis, ( ), ou o e-mail entre os sinais < >. Se o comentário incluir caracteres de pontuação, deve-se empregar a forma entre parêntesis, como a seguir:

From: Julio_gonçalves@inf.unitau.br (Prof. Julio Gonçalves)

Para efetuarmos uma análise um pouco mais criteriosa, poderemos nos basear no endereço *de e-mail* acima e dividi-lo em duas partes, ou seja, parte da esquerda e parte da direita do caractere@ (arroba), que deve ser único. A parte da esquerda é chamada de parte local e indica o nome *da mailbox* e a parte da direita é o domínio. O domínio especifica onde uma *mailbox* determinada está localizada. Caso o endereço não tenha um @, como em:

From: Julio

Ele deverá ter um endereço local, que significa uma *mailbox* local na organização, sendo que a maioria dos sistemas de *e-mail* permite a omissão do domínio quando ocorre o envio de mensagem para uma *mailbox* local, porém, o domínio completo precisar ser adicionado pelo sistema antes do envio da mensagem.

A caixa postal de correspondência eletrônica *ou mailbox* pode pertencer a um usuário ou a um grupo de usuários, podendo ser, também, o local para se deixar mensagens para alguém com uma função específica, como o *postmaster* (nome dado a uma área de armazenamento, onde as mensagens permanecem até que o usuário execute uma ação de leitura, arquivamento, eliminação ou de transferência para outra área). *A mailbox é a* versão eletrônica da caixa postal do sistema de correio tradicional.

Existem algumas convenções para a determinação da forma de nomes de *mailboxes,* utilizadas para fins especiais:

X-lovers: Nomes de *mailboxes* com travessões no interior são provavelmente especiais. Se o nome parecer-se com um que pertença a um grupo de pessoas, ele é possivelmente uma lista de distribuição ou de discussão e o envio de uma mensagem para nomes deste tipo redistribui a mensagem para todos aqueles que estiverem inscritos na lista.

*x-lovers-request:* Nomes terminando em *request,* que são endereços administrativos de listas de discussão, que é normalmente o local para onde são enviados os pedidos de inscrição *(subscribe)* ou de cancelamento de inscrição *(unsubscribe) em* listas. No caso da lista ser moderada, é também para endereços deste tipo que são enviadas as sugestões ao Moderador. Um Moderador é um editor voluntário que proporciona uma melhor qualidade à lista de discussão, agindo como um filtro humano para tópicos relevantes.

*Postmaster:* Supõe-se que todo domínio ou *site* possua uma caixa de correspondência central utilizada para comunicações diversas e normalmente é para onde são encaminhadas as dúvidas e são relatados os problemas envolvendo o sistema de mensagens.

*Mailer-daemon:* Este é o agente do sistema de correio amigável propriamente dito e as mensagens vindas dele são, na maioria, relatos de problemas ocorridos com uma mensagem enviada ou notificação do seu envio. Um exemplo de um erro bastante comum é a mensagem de *Host Unknown* ou *User Unknown,* indicando que a mensagem seguiu com um endereço incorreto e indevido.

*Local%domain:* A maioria dos sistemas interpreta nomes de *mailbox* com um caractere % no meio como sendo um endereço completo de *e-mail*, sendo que o primeiro % é substituído por um @ (arroba) *e o e-mail é* redirecionado de acordo com este novo endereço formado.

*Jose.Silva:* Um crescente número de sistemas de correio vem permitindo o endereçamento do usuário pelo seu nome completo e para que este recurso possa ser implementado, o primeiro nome e os nomes seguintes que compõem o sobrenome devem vir separados por um ponto (.) ou por um sinal de sublinhado (_).

*XYZ123AB:* Existem organizações em que a utilização de números ou códigos para nomes de *mailbox,* é utilizado, e este procedimento é comum em redes EARN e BITNET. Para estes casos, é uma boa prática acrescentar um comentário contendo o nome do destinatário no endereço.

*JDS:* Em sistemas Operacionais *Unix*, é bastante comum o uso de partes do nome do usuário para denominar uma *mailbox*, sendo que o uso de apelidos ou as iniciais de nomes também é utilizado, como JDS para José da Silva.

### 5.5 DNS (DOMAIN NAME SYSTEM)

Segundo Soares et al. (1995), o *DNS* (Domain Name System), é um esquema de gerenciamento de nomes, hierárquico e distribuído para computadores interligados e prestando diversos serviços de informações e *Internet* às corporações. O *DNS* define a sintaxe dos nomes usados na *Internet*, regras para delegação de autoridade na definição de nomes, um banco de dados distribuído que associa nomes a atributos (entre eles, o endereço *IP*) e um *algoritmo* distribuído para mapear nomes em endereços. As aplicações normalmente utilizam um endereço *IP* de 32 *bits*, no sentido de abrir uma conexão, ou enviar um *datagrama IP*. Normalmente os usuários preferem identificar as máquinas por meio de nomes, ao invés de números, por ser mais simples de se memorizar e, desta maneira, é necessário um banco de dados que permita a uma aplicação, encontrar um endereço, dado que ela conheça o nome da máquina com a qual deseja se comunicar.

Um exemplo típico é o nome ostra.inf.unitau.br. Esse é o nome de uma máquina que fica no Departamento de informática da Universidade de Taubaté, na cidade de Taubaté, Estado de São Paulo. Para encontrar seu endereço *Internet*, pode ser necessário o acesso a até quatro servidores de nomes. Inicialmente, deve ser consultado um servidor central, denominado servidor raiz, para descobrir onde está o servidor principal. O servidor principal é responsável pela gerência dos nomes das instituições brasileiras ligadas a *Internet*.

O servidor raiz informa, como resultado da consulta, o endereço *IP* de vários servidores de nomes para o nível br. Um servidor do nível br pode então ser consultado, devolvendo o endereço *IP* do servidor unitau. De posse do endereço do servidor unitau, é possível solicitar que ele informe o endereço de um servidor inf, quando, finalmente, pode se consultar o servidor inf sobre o endereço da máquina ostra. O resultado final da busca é o endereço *Internet* correspondente ao nome ostra.inf.unitau.br. O *DNS* não se limita a manter e gerenciar endereço *Internet*.

Cada nome de domínio é um nó em um banco de dados, que pode conter informações definindo várias propriedades. Por exemplo, o tipo da máquina e a lista de serviço oferecido por ela. Também é possível utilizar o *DNS* para armazenar informações

sobre usuários, listas de distribuição ou outros objetos. O *DNS* é particularmente importante para o sistema de correio eletrônico. No *DNS* são definidos registros que identificam a máquina que manipulam as correspondências relativas a um dado nome, identificando assim, onde um determinado usuário recebe suas correspondências.

Além do modelo de serviço de diretório *DNS*, existe um outro bem mais completo, o X.500. Os requisitos de serviços de segurança são bem definidos para o X.500, que incorpora em seu protocolo mecanismos de segurança para implementar estes serviços. Por outro lado, não existe uma definição explícita para os serviços de segurança para o *DNS*, que, conseqüentemente, não possui mecanismo de segurança. Provavelmente, se o *DNS* for aumentado para incorporar recursos de segurança, seus requisitos de segurança serão muito semelhantes aos do X.500. São esses os requisitos:

- Autenticação da origem dos dados.
- Controle de integridade em transmissões de dados para proteger as consultas e respostas ao diretório.
- Controle de acesso para permitir o armazenamento dos dados no diretório, com a confiança que esses dados somente serão modificados por usuários autorizados ou administradores e que dados sensíveis não serão revelados para usuários não autorizados.

Na ausência de mecanismos de segurança específicos no *DNS*, mecanismos de níveis inferiores devem ser empregados para fornecer: autenticação, integridade e controle de acesso, embora a eficácia desse mecanismo não seja a mesma que a do mecanismo do X.500, atuante no nível de aplicação. Segundo McClure (2000), o *DNS* é um banco de dados distribuído utilizado para mapear endereços *IP* para nomes de *hosts* e vice-versa e se um *DNS* for configurado de forma insegura, existe a possibilidade de se obter informações reveladoras sobre uma organização.

A parte da direita do sinal de arroba (@), é chamada de *nome de domínio*. Indica o computador ou o domínio a que pertence o computador onde *a mailbox* está situada. Para descobrir sua localização, existe *DNS*.

Em resumo, o *DNS* é o sistema que resolve problemas de localização de nomes de computadores ou de domínios, numa rede *TCP/IP*, pelo mapeamento destes nomes a endereços *IP* e vice-versa. Uma de suas funções consiste em definir um mecanismo universal para encontrar os computadores destinatários de mensagens endereçadas a um domínio específico. Para isto, divide o nome de domínio onde há pontos, (.), separando-o em segmentos denominados *sub-dominios.*

Normalmente existem, a princípio, de três a seis sub-domínios. O sub-domínio à direita indica sempre um nível superior em relação ao corrente. O da extrema direita,

mais geral, é o primeiro nível ou o *Dominio do nível de topo,* composto normalmente por duas letras indicando o código do país, (por exemplo, br para Brasil) ou uma designação de rede.

Existem várias exceções, por exemplo, nos Estados Unidos e em alguns sites do Canadá , o nível de topo indicando o país é omitido. Utiliza-se, como segmento mais à direita, um código para indicar o tipo de site, ou seja, a natureza da organização a que o computador pertence.

Este código é, normalmente utilizado como segundo nível (sub-domínio 1) nos demais países, conforme Tabela 3.

Tabela 3 – Códigos para Indicar o Tipo do Site

| ***CÓDIGO*** | ***NATUREZA DA ORGANIZAÇÃO DO SITE*** |
|---|---|
| **COM** | Comercial |
| **EDU** | Educacional |
| **GOV** | Governamental |
| **MIL** | Militar |
| **NET** | Organizações de Rede |
| **ORG** | Outras organizações, por exemplo, Organizações Não Governamentais – ONGs. |
| **INT** | Internacional |

Fonte: Pagliusi. (1998, p.19).

Segundo Pagliusi (1998), em alguns países, como a Europa, a notação dos sub-domínios é sujeita a um acordo comum entre as redes de cada país e alguns no Reino Unido, utilizam AC e CO no lugar de EDU e COM, para designar, respectivamente, membros acadêmicos e companhias. No Brasil, há também uma exceção, onde se omite o sub-domínio EDU no caso de sites de natureza educacional e, sendo assim, ao invés *de unitau.edu.br* temos, no exemplo dado, *unitau.br*. Deste modo, o nome da instituição passa para o segundo nível (sub-domínio 1). Em outros países, como a Suíça, há também várias entidades que omitem o segmento apropriado para indicar a natureza da organização. Por exemplo: *who.ch ((*World Health Organization*,* Suíça, o código internacional da Suíça é CH, derivado de "Confederation Helvetica", em Latim), que deveria ser, pela regra geral, *who.org.ch,* porém o nome da organização é freqüentemente utilizado como terceiro nível (subdomínio 2), como em *embratel.net.br* (Empresa Brasileira de Telecomunicações), é a própria organização que sugere o

nome deste sub-domínio que, estando disponível, será concedido e os demais segmentos, à esquerda, detalham ainda mais a informação sobre o receptor. Como quarto nível (sub-domínio 3), é comum empregar-se o nome do computador ou, se houver um quinto nível, o nome da área dentro da organização (nome do Departamento, entre outras áreas) em que se situa o computador, porém este segmento pode ser omitido. O quinto nível (sub-domínio 4), também não obrigatório, indica normalmente o nome da máquina que provê suporte para o site, ou, caso haja um sexto domínio, indicará o nome da sub-área (dentro da área da organização) a que pertence o computador. O sexto nível (sub-domínio 5), se existir, indicará o nome do computador. A sintaxe genérica para os endereços de *e-mail é:* mailbox@sub-domínion...sub-domínio2.sub-domínio1.domínio-nível-de-topo.

### 5.5.1 ARQUITETURA DO CORREIO ELETRÔNICO

Segundo Allman (1995) *apud* Pagliusi (1998), um sistema de correio eletrônico é formado por componentes que interagem para haver envio e recebimento de mensagens e esta atividade pode ocorrer entre usuários de um mesmo equipamento ou entre usuários situados em equipamentos diferentes, ligados em rede. Neste caso, pode haver alguma incompatibilidade entre os sistemas. Desta maneira, um dos maiores problemas com os sistemas de correio eletrônico ocorre quando os sistemas de comunicação processando nos diferentes computadores não são compatíveis quando desempenham atividades semelhantes. Para solucionar este problema, foram desenvolvidos protocolos específicos para suportar as comunicações de correio eletrônico.

Os dois grandes fornecedores de padrões para sistemas de correio eletrônico são: *ISO/ITU-T* (International Standards Organization / International Telecommunications Union - Telecommunications), por meio do protocolo X.400 (X.400 - Recommendations for Message Handling Systems); e a *Internet*, por meio do protocolo *SMTP* .

Os protocolos de transferência de mensagens X.400 e o *SMTP* são considerados, respectivamente, o padrão "de juri" e o padrão "de facto" para protocolos de correio eletrônico, sendo que a *Internet* é também conhecida como a maior rede de computadores do mundo e ela se baseia no conjunto de protocolos *TCP/IP*. Na Arquitetura *TCP/IP,* a transferência de *e-mail* ocorre por meio do protocolo *SMTP,* utilizando toda a infra-estrutura disponível na *Internet*, que é um item importante deste trabalho e é o protocolo de correio eletrônico mais utilizado em todo o mundo.

### 5.5.2 COMPONENTES BÁSICOS DOS SISTEMAS DE *E-MAIL*

Segundo Cavalcanti (1997) apud Pagliusi (1998), os sistemas de *e-mail* são constituídos de duas partes distintas, sendo que uma parte provê *a interface* com o ser humano e é chamada *de Agente Usuário* (ou *UA*, de *User Agent*). O *UA* consiste no programa de correio eletrônico que permite ao usuário confeccionar, enviar, receber e ler mensagens, bem como manipular a caixa de correspondência ou *mailbox*. Equivale à caneta e ao papel utilizados na composição de uma carta convencional.

A outra parte é a que provê o envio da mensagem ao receptor, chamado de Agente de Transferência de Mensagem (ou *MTA*, de Message Transfer Agent). O *MTA* é o programa que encaminha a mensagem para a máquina de destino, utilizando um protocolo de transferência de mensagens. Deste modo, o *MTA* é o equivalente eletrônico de uma agência de correio tradicional. Se o receptor for local (na mesma vizinhança ou na mesma máquina), somente um único *MTA* ou uma única agência estará envolvida.

Se for distante, a mensagem será enviada da agência local (*MTA* local) para outra distante (*MTA* remoto), para ser entregue ao receptor *(mailbox). Um* Sistema de Transferência de Mensagens (ou *STM*) é a denominação dada a um conjunto de *MTAs*, conforme Figura 18.

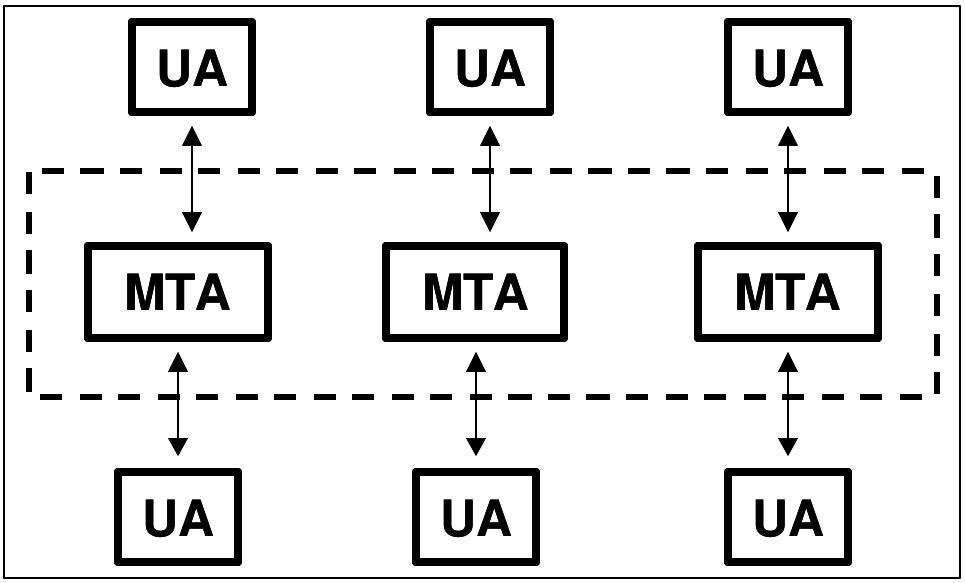


Figura 18 – Modelo Geral dos Sistemas de Correio Eletrônico

Fonte: Cavalcanti (1996) *apud* Pagliusi. (1998, p.22).

Os sistemas de correio eletrônico constituem serviços da Camada de Aplicação do Modelo *OSI/I.S.O,* e o modelo empregado pelos sistemas de correio eletrônico seguem o paradigma cliente/servidor para desenvolvimento de aplicações distribuídas.

### 5.5.3 SMTP (SIMPLE MAIL TRANSFER PROTOCOL)

Segundo Cavalcanti (1997) apud Pagliusi (1998), o *SMTP* (Simple Mail Transfer Protocol) consiste em um protocolo puro da Camada de Aplicação do Modelo *OSI/I.S.O*, não tendo como característica técnica a responsabilidade com os serviços de transporte de dados.

Trata-se de um protocolo simples, orientado a textos e projetado para transferir mensagens de maneira confiável e eficiente. A estrutura de uma máquina que implementa o protocolo de transferência de mensagens *SMTP* se apresenta conforme o esquema da Figura 19:

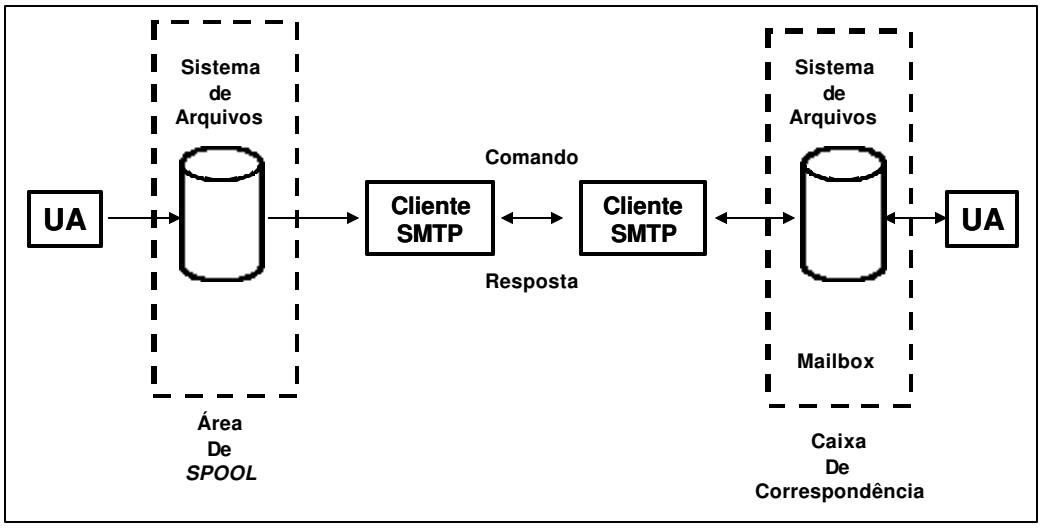



Figura 19 – Modelo Funcional do SMTP

Fonte: Cavalcanti (1997) *apud* Pagliusi (1998, p.23).

Uma ou mais áreas para Enfileiramento de Mensagens, consistem nas áreas *de Spool,*(Simultâneos Peripheral Operation On Line, programa ou equipamento que controla os dados que vão para os dispositivos de saída), ou seja, são as áreas onde as mensagens em trânsito são armazenadas em uma fila de submissão, visando futura transmissão ou remoção para outra área.

Um ou mais *Processos Daemons*, programas executando na retaguarda (em *background* (programas executados na retaguarda, ou seja, em ambiente sem a percepção do usuário do microcomputador)), para a entrega e recebimento de mensagens, de forma a permitir que o usuário continue com suas atividades normais de uso da máquina. Durante o diálogo entre duas máquinas para transferência de uma mensagem, o computador de origem da mensagem *age* como *cliente SMTP.* Por sua vez, o computador de destino age como *servidora SMTP,* aceitando as mensagens que serão colocadas, posteriormente, *na mailbox do* receptor. As *mailboxes* dos usuários, como já exposto, são as áreas de armazenamento onde as mensagens permanecem até que o usuário as elimine ou as transfira para outra área. O *SMTP* normalmente interage com o sistema de correio eletrônico e não diretamente com o usuário. Portanto, ele se posiciona a parte de qualquer transferência local para uma determinada máquina. Deste modo, o *SMTP* somente inicia sua atividade de processamento quando uma mensagem deve ser transferida para uma máquina diferente ou quando do recebimento de uma mensagem remota. Após o usuário escrever uma mensagem e solicitar seu envio por meio do UA, havendo a necessidade de encaminhar uma cópia para alguma máquina remota, este a deposita na área de *Spool* local para mensagens de saída. O *MTA* vasculha periodicamente a área de *Spool* citada em busca de mensagens que ainda não tenham sido despachadas e, quando encontra alguma, ele extrai do seu envelope as informações necessárias para seu envio, via *SMTP*, para a máquina remota destinatária.

No *SMTP*, antes de enviar uma correspondência eletrônica, o processo *cliente* faz a conversão do nome da máquina destino para seu respectivo endereço *IP*, por meio do serviço de diretórios DNS. Dessa forma, é estabelecida uma conexão TCP/IP (aberttura de uma porta conhecida, neste caso, a porta 25) com o processo *servidor em* execução naquela máquina. Se a conexão tiver êxito, o processo *cliente* envia uma cópia da mensagem para *o servidor* remoto. No caminho percorrido por uma mensagem que esteja trafegando na rede, um caminho reverso também é executado, tornando possível a notificação ao emissor original sobre possíveis falhas.

*O servidor* armazena temporariamente a cópia em uma área de *Spool* para mensagens de entrada e quando o *cliente e servidor* concordam com o fato da cópia da mensagem ter sido corretamente transferida e armazenada, *o cliente* remove a cópia local de sua área de *Spool*. *E o servidor* também remove sua cópia transferindo-a normalmente para a *mailbox de* destino. Deste modo, tudo o que o usuário precisa fazer é executar uma *interface* (*UA*) para depositar ou receber mensagens da área de *Spool*. Todas as transferências são executadas por processos em execução na retaguarda (*MTA*), sendo que filas de submissão, tanto de entrada quanto de saída de mensagens, situam-se entre o sistema de *e-mail* local e as partes *cliente e servidor do SMTP*. O processo *cliente SMTP* está relacionado à inicialização da transferência de mensagens para outros sistemas de correio eletrônico. O processo *servidor SMTP* gerencia o recebimento de mensagens oriundas dos sistemas remotos, caso a conexão não tenha sucesso, por não ter sido estabelecida ou devido à falha ocorrida durante a comunicação. Caso a conexão não tenha sucesso, por não ter sido estabelecida ou devido a falha ocorrida durante a comunicação. Uma das funções principais do *SMTP* é a de transferir correio de modo confiável e seguro, sendo que este protocolo é extremamente simples e confiável.

Segundo Soares et al. (1995), os serviços de segurança necessários para o correio eletrônico na *Internet* deverão incluir confidencialidade e integridade em transmissões sem conexão, a autenticação da origem das mensagens e o impedimento da rejeição foram elaborados para permitir esta função adicional ao *SMTP*. A Figura 20 ilustra os componentes usados no sistema de correio.

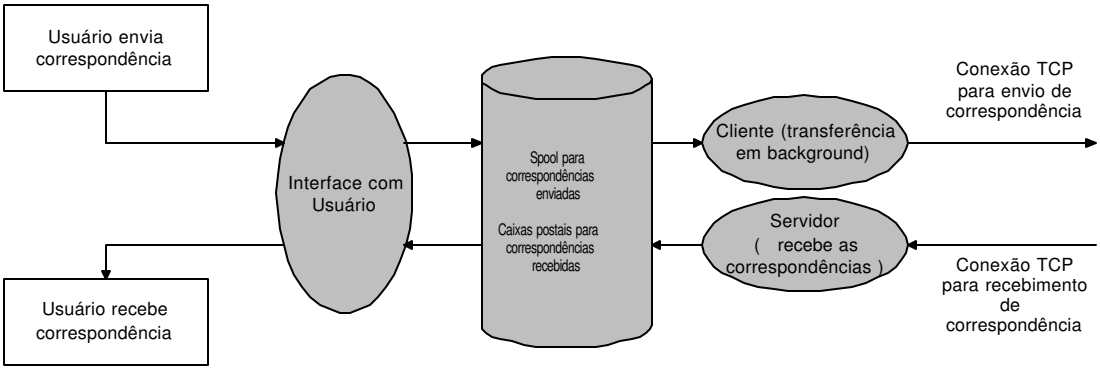



Figura 20 – Funcionamento do SMTP

Fonte: Soares, Luiz F. G., Lemos, Guido, Colcher, Sérgio. (1995, p 414).

Todo o processo de transferência de mensagens, executado em *background*, efetua o mapeamento do nome da máquina de destino em seu endereço *IP*, e tenta estabelecer uma conexão *TCP* com o servidor de correio eletrônico da máquina de destino. Caso haja sucesso e se a conexão for estabelecida, o cliente envia uma cópia da mensagem para o servidor, que a armazena em seu *Spool* e sendo a mensagem transferida com sucesso, o servidor avisa ao cliente que a recebeu e armazenou uma cópia da mesma. Quando recebe a confirmação de recebimento e armazenamento, o cliente retira a cópia da mensagem que mantinha em seu *spool* local. Se a mensagem por algum motivo, não for transmitida com sucesso, o cliente anota o horário da tentativa e suspende sua execução. Periodicamente, o cliente verifica se existem mensagens a serem enviadas em sua área de *spool* e tenta transmití-las. Se uma mensagem não for enviada por um período previamente determinado, o serviço de correio eletrônico devolve a mensagem ao remetente, informando que não conseguiu transmití-la.

### 5.5.4 TRANSFERÊNCIA DE MENSAGENS PELO SMTP

Ainda segundo Soares et al. (1995), a transferência de *e-mails* por meio do *SMTP* envolve uma troca de pacotes especiais *PDZ* (Protocol Data Units), conhecidos por comandos e respostas *SMTP* e, desta forma, a comunicação entre o cliente e o servidor *SMTP* é um diálogo controlado pelo cliente. Este envia um comando ao servidor que lhe retribui com uma resposta e, neste diálogo, todos os comandos são compostos por códigos de quatro caracteres alfabéticos, não importando se maiúsculos ou minúsculos e as respostas aos comandos *SMTP* são compostas por um código numérico de três dígitos transmitidos como três caracteres alfanuméricos, seguido por um texto. A troca de mensagens pelo *SMTP* está baseada no seguinte modelo de comunicação: como resultado de um pedido de envio de mensagem eletrônica feita por um usuário a um *UA*, o cliente *SMTP* da máquina local abre uma conexão de transporte com o servidor *SMTP* da máquina receptora.

Após ter iniciado o canal de transmissão solicitado pelo cliente, o servidor *SMTP* lhe envia o código de resposta 220 (Ready *for mail).* Em seguida, o cliente envia o comando HELO se apresentando e o servidor devolve a resposta 250, seguida de sua identificação. Uma vez estabelecido o canal de comunicação, o cliente *SMTP* envia um comando MAIL indicando o emissor da mensagem eletrônica.

Se o servidor *SMTP* puder receber *e-mails*, ele encaminha uma resposta 250 (Ok). O cliente *SMTP* envia um comando chamado RCPT, identificando o receptor existente no *e-mail*. Se o servidor *SMTP* puder aceitar mensagens para o receptor em pauta, ele devolverá uma resposta 250 *(ok);* caso contrário, o servidor responderá rejeitando aquele receptor, por exemplo, por meio do código 550 (*No such user here*, onde apenas o receptor em pauta é rejeitado e o servidor *SMTP* não rejeita toda a transmissão).

O cliente e o servidor *SMTP* podem negociar vários receptores, tantos quantos estiverem como destinatários nos campos TO:, Cc: e Bcc: que existem no cabeçalho do *e-mail*. Após todos os receptores terem sido negociados, o cliente *SMTP* encaminha o comando DATA, informando ao servidor que está pronto para transferir o conteúdo do *e-mail*.

O servidor envia a resposta *354 (Enter mail, end With.*), informando que está pronto para recebê-lo e o cliente *SMTP* envia, então, o conteúdo da mensagem eletrônica, indicando seu término por meio de uma seqüência especial de caracteres. Se o servidor *SMTP* processar com sucesso os dados do *e-mail*, ele responderá com o código 250 (0k). Para encerrar, o cliente *SMTP* envia um comando QUIT, respondido pelo servidor *SMTP* com um código 221 *(Service closing transmission channel),* concordando com o término. O diálogo ocorre passo a passo, linha após linha e a comunicação se concretiza. Cada comando *SMTP* gera uma resposta. As respostas garantem, deste modo, a sincronização das solicitações e da execução de suas respectivas ações na transferência de um *e-mail*. O primeiro dígito de cada resposta indica se a mesma é boa, ruim ou incompleta. Na Tabela 4 há uma apresentação do significado do primeiro dígito do código de respostas *SMTP*:

Tabela 4 – Significado do Primeiro Dígito do Código de Resposta SMTP

| ***1º DÍGITO DO CÓDIGO RESPOSTA*** | ***SIGNIFICADO*** |
|---|---|
| **1** | Indica que o comando foi aceito, mas requer a confirmação da informação contida na resposta |
| **2** | Comando aceito e ação requisitada complementada com sucesso. |
| **3** | Comando aceito, porém aguarda mais informações para a requisição ser atendida. |
| **4** | Ocorreu um erro e a ação requisitada não será executada, mas poderá ser solicitada outra vez. |
| **5** | Ocorreu um erro e a mesma ação deverá ser novamente solicitada. |

Fonte: Pagliusi. (1998, p.28).

O segundo dígito da resposta indica a categoria da informação. Há quatro valores possíveis, conforme Tabela 5:

Tabela 5 – Significado do Segundo Dígito do Código de Resposta *SMTP*

| ***2º DÍGITO DO CÓDIGO RESPOSTA*** | ***SIGNIFICADO*** |
|---|---|
| **0** | Indica que houve um erro de sintaxe de comando ou comando não especificado ou mesmo um comando supérfluo. |
| **1** | Informação de situação do comando ou de ajuda. |
| **2** | Resposta referente àconexão. |
| **3** | Situação de uma transferência ou de uma ação solicitada. |

Fonte: Pagliusi. (1998, p.28).

Na Tabela 6 são relacionados alguns dos principais comandos *SMTP* utilizados pelos sistemas de correio eletrônico comuns:

Tabela 6 – Os Principais Comandos do *SMTP*.

| ***COMANDO SMTP*** | ***DESCRIÇÃO*** |
|---|---|
| **HELO** | Indica o cliente SMTP para o servidor SMTP. |
| **MAIL** | Inicia uma transação de *e-mail.* |
| **RCPT** | Identifica o receptor (individual) do conteúdo do *e-mail.* |
| **DATA** | O servidor *SMTP* processa as linhas seguintes como sendo o conteúdo do *e-mail* enviado pelo cliente *SMTP*. |

| | |
|---|---|
| **SEND** | Envia o conteúdo do *e-mail* para um ou mais terminais. |
| **SOML** | Envia o *e-mail* para um ou mais terminais, se o usuário receptor estiver ativo, senão, envia para sua *Mailbox*. |
| **SAML** | Envia o conteúdo do *e-mail* para um ou mais terminais e também para as *Mailboxes* dos usuários receptores. |
| **RESET** | Indica que a transação corrente está para ser abortada. |
| **VRFY** | Usuário do correio eletrônico solicita ao servidor *SMTP* para confirmar se o argumento identifica um usuário. |
| **EXPN** | Comando que solicita ao servidor *SMTP* para confirmar se o argumento identifica uma lista de discussão e, caso identifique alguma, solicita a relação dos seus membros. |
| **HELP** | Solicita informação de ajuda ao servidor *SMTP*, pedindo os comandos disponíveis e instruções para utiliza-los. |
| **NOOP** | Não indica nenhuma ação; apenas solicita uma resposta de que está tudo bem ao servidor *SMTP*. |
| **QUIT** | Especifica que o servidor *SMTP* deve enviar uma resposta de que está tudo bem e encerra |
| **TURN** | Especifica uma solicitação de inversão de papéis entre cliente d servidor *SMTP*. O servidor *SMTP* pode negar ou enviar uma resposta de que está tudo bem e assumir o papel do cliente. |

Fonte: Pagliusi. (1998, p.29).

Complementando o funcionamento do Protocolo *SMTP*, na Tabela 7 apresenta os principais códigos de respostas às mensagens do *SMTP*:

Tabela 7 – Os Principais Códigos de Resposta *SMTP* por Grupos de Função

| ***CÓDIGO DE RESPOSTA SMTP*** | ***DESCRIÇÃO*** |
|---|---|
| **500** | Erro de sintaxe, comando não conhecido. |
| **501** | Erro de sintaxe nos parâmetros ou argumentos. |
| **502** | Comando não implementado. |
| **503** | Seqüência incorreta de comandos. |
| **504** | Parâmetro de comando não implementado. |
| **211** | Situação do sistema ou resposta de ajuda do sistema. |
| **214** | Mensagem de ajuda. |
| **220** | (Domínio) serviço pronto |
| **221** | (Domínio) Serviço fechando o canal de transmissão. |
| **421** | (Domínio) Serviço indisponível, fechando canal de transmissão. |
| **250** | Ação solicitada e concluída com sucesso. |
| **251** | Usuário não local. |

| | |
|---|---|
| **450** | Ação não realizada: *Mailbox* não disponível |
| **550** | Ação solicitada e abortada: erro no processamento. |
| **551** | Usuário não local. Necessidade de reenviar a mensagem. |
| **452** | Ação realizada: memória insuficiente. |
| **552** | Ação solicitada abortada: excedeu-se a alocação de memória. |
| **553** | Ação não realizada: nome da *Mailbox* inválida |
| **354** | Existe a necessidade de se iniciar a entrada do conteúdo do *e-mail* e terminar com um ponto. |
| **554** | A transação falhou |

Fonte: Pagliusi. (1998, p.30).

### 5.5.5 EXPANSÃO DE APELIDOS

Segundo Teixeira (1996) *apud* Pagliusi (1998), uma grande maioria de sistemas de correio eletrônico possui um programa para transporte de mensagens que inclui um mecanismo de expansão de apelidos de correspondências, permitindo a conversão de identificadores utilizados em endereços de *e-mail* para novos endereços (um ou mais), sendo que o uso de apelidos aumenta a funcionalidade e conveniência dos sistemas de correio eletrônico, permite que um *Site* associe grupos de usuários por meio de um único identificador, permite também que um usuário possua múltiplos identificadores para correspondência eletrônica, incluindo posições e abreviações, por meio do mapeamento de um conjunto de identificadores para um único indivíduo. O uso destes apelidos também possibilita o estabelecimento de *um expansor de correspondências.* Este programa recebe uma mensagem de entrada e a retransmite para um conjunto de receptores associados a um único identificador, ou seja, para uma lista de correspondência eletrônica.

Após a preparação de uma mensagem pelo usuário e a identificação de cada receptor ter sido estabelecida, geralmente o *UA* consulta os apelidos locais em um banco de dados para substituir o nome do receptor pelo nome mapeado e após esta substituição, ele repassa a mensagem ao *MTA* processando em *background.* Receptores não mapeados, ou seja, sem apelidos, não sofrem alteração e tais apelidos também podem ser utilizados para converter nomes de usuários locais para mensagens recebidas remotamente. Desta maneira, tanto mensagens de entrada quanto de saída passam pelo mecanismo de expansão de apelidos.

Deve-se tomar cuidado com a expansão de apelidos, pois se o apelido especificar um endereço inválido, o emissor irá receber uma mensagem de erro. Ou ainda, se dois *sites* especificarem apelidos conflitantes, os sistemas de correio eletrônico de ambos podem entrar em *loop* (caminho circular total percorrido por um sinal, corrente elétrica ou rotina de um programa de computador.). Por exemplo, o *site* A pode especificar o

endereço estação 1 como sendo o endereço estação 2 no site B. E o site B, por sua vez, pode traduzir o endereço estação 2 para endereço estação 1 no site A.

Na Figura 21 há uma representação de um sistema de correio eletrônico completo:

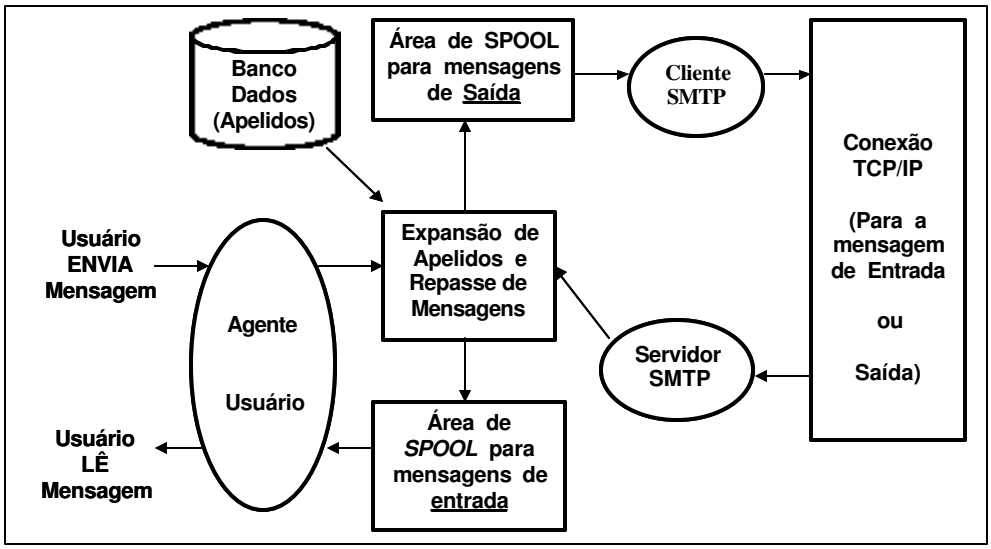



Figura 21 – Exemplo de Um Sistema de Correio Eletrônico Completo

Fonte: Pagliusi. (1998, p.31).

### 5.5.6 ATRIBUTOS TECNOLÓGICOS DO CORREIO ELETRÔNICO

Segundo Sproll (1995) *apud* Pagliusi (1998), analisando-se a tecnologia do correio eletrônico, é possível de concluir que a mesma possui seis características que a diferem de outras tecnologias de comunicação. A primeira delas consiste no fato do correio eletrônico ser *Assíncrono* (denominação dada ao equipamento ou tipo de transmissão de dados na qual os caracteres transmitidos são enviados sem relógio de sincronismo entre o transmissor e o receptor).

Cada caracter é uma unidade autônoma com seu próprio *bit* de parada e de início, utilizados para sincronizar o relógio interno do receptor, ou seja, os emissores e os receptores não precisam estar presentes ao mesmo tempo em um determinado canal de comunicação e ambos podem enviar e receber suas mensagens conforme acharem mais conveniente.

A segunda característica diz respeito ao fato do correio eletrônico ser *rápido*, ou seja, uma mensagem eletrônica pode ser transmitida em segundos ou minutos

atravessando um prédio, um continente ou dando a volta ao mundo e as respostas podem fluir com a mesma rapidez. Esta velocidade não é apenas uma questão de conveniência, pois ela possibilita a conversação de longa distância, tomada de decisões e uma série de outras interações requerendo curto tempo de resposta.

A terceira característica está diretamente ligada ao aspecto do correio eletrônico ser *baseado em texto. As* mensagens, em sua maioria, transmitem caracteres, e não imagens ou sons, embora haja alguns programas de *e-mail* permitindo o envio destes últimos. Além de troca de mensagens, o texto na comunicação eletrônica permite também a troca de documentos. O mais importante desta característica é que as mensagens se parecem muito umas com as outras, não carregam consigo o tom de voz, a inflexão, o sorriso e o olhar de quem as redigiu. Carecem, portanto, de informação social composta de regras e costumes que usualmente regulam as comunicações. Uma tentativa de suprir esta carência consiste no Código de Etiqueta da Rede, desenvolvido pela comunidade da *Internet*: *O Netiquette Code.*

Os Ícones da Emoção (Smileys ou Emoticons) têm também como objetivo introduzir alguma comunicação social no texto escrito, uma outra existente consiste no uso da escrita em letras maiúsculas, indicando que o emissor está "gritando" um certo trecho da mensagem.

Na Tabela 8 estão relacionados alguns dos principais “Emocionícones” utilizados pelos usuários de Correio Eletrônico em geral:

Tabela 8 – Os “Emocionícones” dos Sistemas de *E-mail*

| ***SÍMBOLO*** | ***DESCRIÇÃO*** |
|---|---|
| **: – )** | Quem escreveu está brincando ou sorrindo, não leve a sério |
| **: – I** | O leitor não entendeu a mensagem |
| **: – o** | O leitor ficou surpreso |
| **8 – O** | O leitor ficou chocado |
| **: – (** | Quem escreveu está triste |
| **: – <** | Quem escreveu está irritado |
| **: – #** | Quem escreveu mantém segredo |
| **O: – )** | Quem escreveu não tem culpa |
| **: –** \ | Quem escreveu está indeciso |
| **%– (** | Quem escreveu está confuso |
| **: – D** | Quem escreveu está sorrindo |
| **; – (** | Quem escreveu está com vontade de chorar |
| **; – )** | Quem escreveu está piscando o olho (maliciosamente) |

Fonte: Pagliusi. (1998, p.33).

A quarta característica está diretamente ligada ao fato do *e-mail* poder ser endereçado para múltiplos receptores, sendo que este aspecto indica que, sem depender do tempo ou do espaço, as pessoas podem delegar trabalhos, formar novos grupos, encaminhar contribuições ou até mesmo tomar decisões coletivas.

A quinta característica consiste na memória externa do correio eletrônico, ou seja, o conteúdo das mensagens eletrônicas pode ser armazenado e posteriormente reenviado e esta propriedade é importante para a memória social.

Por exemplo, os participantes de um grupo eletrônico podem armazenar todas as suas interações ocorridas durante meses ou anos e esta memória produzida é processável por computador e pode ser convenientemente organizada, editada, pesquisada e compartilhada com outras pessoas. Este atributo aumenta a força da memória social por permitir análises de tendências, pontos de consenso, padrões de participação e outras questões do gênero.

Outras tecnologias de comunicação possuem algumas destas características, mas somente o correio eletrônico reúne todos estes seis atributos, conforme especificado na Tabela 9:

Tabela 9 – Comparação do Correio eletrônico com Outras Tecnologias

| ***TECNOLOGIA*** | ***ATRIBUTOS TECNOLÓGICOS*** | | | | | |
|---|---|---|---|---|---|---|
| | **ASSÍNCRONO** | **RÁPIDO** | **SOMENTE TEXTO** | **MÚLTIPLOS ENDEREÇOS** | **MEMÓRIA EXTERNA** | **MEMÓRIA PROCESSÁVEL** |
| **REUNIÃO** | NÃO | SIM | NÃO | SIM | NÃO | NÃO |
| **TELEFONE** | NÃO | SIM | NÃO | SIM | NÃO | NÃO |
| **CARTA** | SIM | NÃO | NÃO | NÃO | SIM | NÃO |
| **TELEX** | SIM | SIM | SIM | NÃO | SIM | NÃO |
| **FAX (FACSÍMILE)** | SIM | SIM | NÃO | NÃO | SIM | NÃO |
| **MENSAGEM VÓZ** | SIM | SIM | NÃO | SIM | NÃO | NÃO |
| **CORRÊIO ELETRÔNICO** | SIM | SIM | NÃO | SIM | SIM | SIM |

Fonte: Pagliusi. (1998, p.34).

## 5.6 CONSIDERAÇÕES SOBRE SEGURANÇA EM CORREIO ELETRÔNICO

O assunto segurança do correio eletrônico, com foco na proteção da mensagem ou *e-mail*, faz parte da segurança da informação e abrange vários aspectos importantes, tais como a confidencialidade e a autenticidade de uma mensagem que esteja em trânsito entre a origem e o destinatário.

Segundo Schneier (1995) apud Pagliusi (1998), nos servidores de *e-mail* e no ambiente do correio eletrônico, as mensagens trafegam de uma máquina à outra, por meio de várias linhas de comunicações, abertas e disponíveis, como as mensagens escritas no dorso dos cartões postais, sendo que qualquer indivíduo localizado em uma máquina intermediária poderia capturá-las, do mesmo modo que um carteiro pode ler o verso dos cartões postais manuseados. As pessoas podem optar por não ler, ou podem não possuir os direitos de acesso para ler tão facilmente, mas a única segurança que o usuário do correio eletrônico tem baseia-se na honestidade, ignorância e indiferença daqueles situados nos pontos intermediários e tais pontos podem ser desde universidades até empresas rivais ou governos estrangeiros e o emissor do *e-mail* não tem nenhum controle sobre eles.

As redes de dados que dão suporte aos servidores de *e-mail* são sistemas descentralizados e os diferentes computadores na *Internet* possuem tabelas de roteamento com a finalidade de direcionar as mensagens entre os computadores emissores e seus destinatários. Quando um computador recebe uma mensagem destinada a alguém situado em outro equipamento, ele procura por esta máquina em sua tabela de roteamento e encaminha o *e-mail*. É comum a existência de diversos computadores intermediários entre o *emissor* e o *receptor* da mensagem. Com o intuito de simular uma comunicação via *e-mail* entre duas entidades, num exemplo, o emissor de uma mensagem será chamado de *Alceu* e *o* receptor de *Bernardo*.

Se um espião ou intruso, também por tradição denominado *Everaldo,* sentado em uma destas máquinas intermediárias, desejar ler toda mensagem eletrônica que por este equipamento esteja transitando, ele o fará, não se importando para quem a mensagem se destina, sendo que *Everaldo* também poderá imprimir, mostrar para outro usuário, enviá-la pela rede ou mandar uma cópia imprensa e, caso seja esperto o suficiente, poderá também alterar a mensagem em trânsito. Como espião ou intruso pode ser considerado o administrador do sistema, um *Hacker* habilidoso ou, se a segurança da máquina intermediária for falha o suficiente, um usuário comum qualquer.

Deste modo, *Alceu e Bernardo,* ao trocarem uma mensagem pela *Internet* ou pelas linhas de comunicação disponíveis, são obrigados a confiar na segurança de todos os servidores de rede e de correio eletrônico por onde a mensagem circular. Se as mensagens eletrônicas são como cartões postais, o que se deseja ter acesso são cartas

dentro de envelopes. Da mesma forma que os *e-mails*, as cartas são roteadas por meio de vários pontos intermediários, elas são colocadas em caixas de correspondências ou *mailboxes,* um funcionário do correio faz a coleta e as leva agência de correio local, de onde são roteadas para seu destino por meio de diversas agências de correio e veículos de transporte. Esta rotina acontece até que o carteiro as entrega nas caixas de correspondência ou *mailboxes* dos respectivos receptores. Dezenas de pessoas manuseiam estas cartas durante seu trajeto pelo sistema, mas nenhuma delas pode lê-las, pois elas ficam protegidas dentro de seus envelopes.

Como não é possível a colocação de um *e-mail* dentro de um envelope, utiliza-se uma analogia para representá-lo e, deste modo, pode-se utilizar criptografia como um "envelope" eletrônico. Programas de segurança de correio eletrônico, tais como o *PGP* (Pretty Good Privacy, programa de Criptografia que provê recursos de sigilo e de autenticação para mensagens eletrônicas e arquivos*),* e implementações dos padrões PEM (Privacy Enhanced Mail*,* Conjunto de procedimentos destinados a prover segurança ao correio eletrônico da *Internet)*, *S/MIME* (Secure Multipurpose Internet Mail Extensions) e dos protocolos MOSS (MIME Object Security Services) e *MSP* (Message Security Protocol), fazem exatamente isto, ou seja, cifrando seu *e-mail* para que somente *Bernardo* possa lê-lo, *Alceu* garante que *Everaldo* não poderá ler sua mensagem, mesmo se interceptá-la em trânsito. Adicionando uma assinatura eletrônica em seu *e-mail, Alceu* poderá garantir que *Bernardo* saberá quem enviou a mensagem. *Everaldo* não poderá trocar uma mensagem *de Alceu* por outra e reivindicar que esta outra tenha sido escrita por Alceu. Além disso, *Bernardo* poderá até mesmo provar a terceiros que a mensagem foi enviada por *Alceu,* num processo que seria o equivalente eletrônico do "reconhecimento de firma".

Em resumo, estes programas de segurança de correio eletrônico são melhores do que envelopes físicos, pois *Everaldo* poderá abrir envelopes, velado ou publicamente, e ler seu conteúdo, poderá inclusive interceptar uma carta em trânsito, abrí-la, ler sua mensagem e, em seguida, colocar outra carta em seu lugar dentro de outro envelope, porém, *Everaldo* não poderá fazer isto com facilidade no mundo digital. A combinação do ciframento com uma assinatura digital proporciona um "envelope" que *Everaldo* não conseguirá violar facilmente.

Podemos citar que um dos principais obstáculos encontrados por *Everaldo* na leitura de uma mensagem alheia consiste em localizá-la dentro de um "oceano" de outras mensagens eletrônicas. Em geral, além de *e-mails*, costumam circular em um site mensagens de usuários de grupos de discussão na *Internet*, *e-mails* de propaganda de empresas, acesso remoto efetuado por usuários de diversos sistemas, conversações de

*Chat* (Tipo de interação em rede comum na *Internet*, nos quais duas ou mais pessoas digitam e enviam mensagens umas para as outras em tempo real), em tempo real, *downloads* (transferência de um arquivo de um computador para outro, ou pode ser ainda, a transferência de um arquivo de um servidor da *Internet* para um computador de um determinado usuário. Pode ser executado por meio de comandos *HTTP* (Hypertext Transfer Protocol, protocolo cliente / servidor utilizado para conectar servidores na *Internet*.), ou *Ftp*), de f*tp e* diversas outras mensagens. A ação de se armazenar esta quantidade de dados em um computador, analisá-la e filtrá-la consiste em um grande problema para *Everaldo,* denominado de problema da coleta.

Segundo Pagliusi (1998), todo o processo de filtragem pode basear-se em palavras-chave, tais como, "secreto", "estratégico" ou "criptográfico". Se *Everaldo* for um agente federal, poderá preferir palavras-chave do tipo: "assassinato", "seqüestro", "explosão", "contrabando" ou "sonegação". Existem outras técnicas para a coleta de mensagens, pode-se procurar por mensagens contendo dados com uma determinada estrutura, a de ciframento do seu conteúdo, por exemplo, mas a técnica empregada depende da disposição de tempo e dos recursos *de software ou* de *hardware* utilizados por *Everaldo*. A coleta é inútil sem a análise das mensagens para verificar se realmente são do interesse de *Everaldo*. Existe a necessidade de uma análise pessoal, pois as palavras-chave podem estar sendo utilizadas fora do contexto esperado. As palavras "explosão", "assassinato" e "seqüestro" podem estar relacionadas a um filme policial ou a uma notícia de última hora de um dos principais jornais, ou podem também fazer parte do diálogo eletrônico dos interlocutores *Alceu e Bernardo,* envolvidos com o crime organizado.

A atividade de ciframento torna o trabalho *de Everaldo* mais difícil por vários motivos e o mais óbvio é que *Everaldo* não poderá ler todos os *e-mails*, porém, isto somente será verdade se o método de ciframento for seguro o suficiente para que *Everaldo* não consiga quebrá-lo ou efetuar uma alteração qualquer. Se for desta maneira, restará ainda *a Everaldo* a possibilidade de fazer uma análise de tráfego, que consiste na verificação de quem envia *os e-mails*, para quem são endereçados, que tamanho possuem, de que assunto se relaciona e quando foram despachados. Analisando estes dados, pode-se chegar a conclusão de que existe uma série de informações úteis a *Everaldo* que, dependendo de sua perspicácia e conhecimento técnico, poderá interpretá-los ou não.

Na eventualidade de *Everaldo* conseguir quebrar o método de ciframento, então o problema passa a ser apenas uma questão de quanto tempo e de quantos recursos pretende utilizar para ler as mensagens de *Alceu* ou de *Bernardo*, que pode significar

cinco minutos em um computador com processador tipo *Pentium* (processador da série X86 da empresa Intel caracterizado por apresentar alta velocidade e performance na execução de instruções), ou então muitas horas em um supercomputador paralelo. Durante as tentativas de invasão, se *Everaldo* conseguir quebrar também a assinatura eletrônica de *Alceu* ou de *Bernardo,* ou caso os *e-mails* trocados não sigam assinados eletronicamente, poderá assumir a identidade de um ou de outro. Ele terá condições, por exemplo, de escrever uma mensagem falsa incriminando *Alice e* entregá-la à imprensa. Entretanto, *Everaldo* somente conseguirá ler uma mensagem crucial se conseguir encontrá-la, devido ao problema da coleta já exposto e isto será mais difícil de acontecer se o ciframento for uma prática largamente utilizada pelos interlocutores. Em contrapartida, *se Alceu e Bernardo* somente cifrarem umas poucas mensagens, isto servirá como um sinal de alerta para informar que tais mensagens são interessantes para *Everaldo*, facilitando, deste modo, seu trabalho de coleta, porém se todas as mensagens, inclusive as rotineiras, forem cifradas, *Everaldo* não poderá discernir as mensagens cifradas importantes. Assim, o ciframento das mensagens, mesmo não tendo muitos recursos, poderá rapidamente tornar o problema da coleta algo intransponível para *Everaldo*.

Efetuando-se uma análise sobre a segurança da informação, as ameaças à segurança de sistemas computacionais refletem-se em quatro classes:

Vazamento: a aquisição de informação por usuários ou receptores não autorizados. Um intruso *Everaldo* poderá ser cúmplice de um usuário legítimo *(Alceu ou Bernardo*) que permite o "vazamento" das informações para ele.

Violação*:* é a alteração não autorizada de informação, incluindo programas, dados de bancos de dados, etc.

Furto de Recursos: relaciona-se ao uso de facilidades sem autorização do proprietário.

Vandalismo: trata-se de interferências nas operações próprias de um sistema sem ganhos para o autor.

Em todos os sistemas de *e-mail*, uma boa parte destas ameaças podem ser minimizadas por meio do emprego de um gerenciamento de *chaves* seguro e adequado. O ciframento de uma mensagem baseia-se em dois componentes um *algoritmo* e uma *chave*. No momento em que *Alceu* cifra uma mensagem, ela utiliza um *algoritmo* de ciframento para transformar o conteúdo da mensagem em texto cifrado e, quando *Bernardo* decifra a mensagem, ele utiliza o *algoritmo* de deciframento correspondente para converter o texto cifrado de novo em uma mensagem clara. Há alguns anos a segurança do ciframento estava baseada na manutenção do *algoritmo* em sigilo, ou seja,

se *Everaldo* conhecesse o *algoritmo* sem *chave*, poderia decifrar uma mensagem cifrada tão facilmente quanto *Bernardo* e manter um *algoritmo* sem *chave* em segredo poderia criar uma série de problemas.

Com o objetivo inicial de contornar o problema apresentado utilizando o segundo componente básico da criptografia de mensagens: a *chave*. Cada *chave* individual faz com que o *algoritmo* trabalhe de forma ligeiramente diferente, ou seja, em uma rede utilizando este sistema e cada par de usuários precisa ter seu próprio *algoritmo* e *chave*.

Quando *Alceu* cifra uma mensagem, ela utiliza um *algoritmo* de ciframento e uma *chave* secreta para transformar uma mensagem clara em um texto cifrado. *Bernardo*, por sua vez, ao decifrar uma mensagem, utiliza o *algoritmo* de deciframento correspondente e a mesma *chave* para transformar o texto cifrado em uma mensagem em claro. *Everaldo*, por não possuir a *chave* secreta, mesmo conhecendo o *algoritmo*, não conseguirá decifrar a mensagem. A segurança do sistema passa a residir não mais no *algoritmo* e sim na *chave* empregada, e esta, no lugar do *algoritmo*, deverá ser mantida em segredo por *Alceu e Bernardo*. Este tipo de ciframento utiliza a criptografia denominada *simétrica ou convencional*.

A respeito do gerenciamento das *chaves*, este consiste na parte mais difícil da criptografia de mensagens eletrônicas. É muito fácil escolher um *algoritmo* seguro para ciframento e implementá-lo, é simples cifrar mensagens em uma ponta e decifrá-las em outra e o maior desafio consiste justamente na distribuição segura das *chaves*. Na verdade a *chave* de deciframento ou é a mesma que a utilizada para o ciframento ou é uma *chave* facilmente derivada desta última e ela funciona como a uma fechadura. Mesmo se duas pessoas utilizarem duas fechaduras idênticas, não poderão abrir a porta uma da outra, a não ser que tenham ambas a mesma *chave* e uma rede inteira de usuários pode se comunicar seguramente utilizando-se apenas de um *algoritmo* e muitas *chaves* secretas distintas.

Complementando, no momento antes de *Alceu* enviar uma mensagem cifrada para *Bernardo*, ambos precisam se comunicar e entrar em um acordo quanto ao tipo de *chave* a ser empregada. *Alceu* também pode gerar a *chave* sozinho e enviá-la para *Bernardo* por meio de um mensageiro de confiança. Após esta fase, eles terão duas opções: armazenar a *chave* em algum lugar comum para ambos, correndo risco de furto, até que ela venha a ser utilizada, ou memorizá-la até o momento de sua utilização, correndo o risco de esquecimento.

Os programas de segurança de *e-mail* modernos permitem que *Alceu* envie uma mensagem *a Bernardo* sem ter que convencionar uma *chave* secreta previamente e, não

precisam nem mesmo se conhecer ou sequer confiar um no outro e este fato é possível devido a existência *da criptografia de chave pública* (ou *assimétrica).*

Quando se estuda a criptografia de chave pública, observa-se a existência de duas *chaves* diferentes: uma para ciframento e outra para deciframento. Elas existem e trabalham aos pares. Uma *chave* de ciframento trabalha junto com uma *chave* de deciframento específica. Como não é possível de se derivar uma *chave* a partir da outra, então com apenas a *chave* de ciframento, não será possível conseguir decifrar as mensagens. De modo geral, a sistemática funciona assim: *Bernardo* e todos os que desejam comunicar-se de modo seguro geram uma *chave* de ciframento e sua correspondente *chave* de deciframento. *Bernardo* mantém secreta a *chave* de deciframento, que também é chamada de sua *chave privada*. *Bernardo* torna pública a sua *chave* de ciframento, que passa a receber o nome de *chave pública*.

Analisando as características da *chave* pública, realmente ela condiz com seu nome, pois, qualquer usuário poderá obter uma cópia dela. *Bernardo*, inclusive envia uma cópia para seus amigos, publicando-a em boletins. Desta maneira, *Everaldo* não tem nenhuma dificuldade em obtê-la, e quando *Alceu* deseja enviar uma mensagem a *Bernardo*, precisará inicialmente encontrar a *chave* pública dele, atividade que pode ser feita de várias maneiras, ou seja, obtendo-a diretamente de *Bernardo*, obtê-la por meio de um banco de dados centralizado ou podendo obtê-la do seu próprio banco de dados. Depois de concluído esta etapa, ela cifrará sua mensagem utilizando a *chave* pública *de Bernardo,* despachando-a em seguida. Após *Bernardo* receber a mensagem, ele a decifra facilmente com sua *chave* privada. *Everaldo,* que interceptou a mensagem em trânsito, não conhece a *chave* privada *de Bernardo,* embora conheça sua *chave* pública, mas este conhecimento não ajuda a decifrar a mensagem e mesmo *Alceu,* que foi quem cifrou a mensagem com a *chave* pública *de Bernardo,* não poderá decifrá-la ainda e desta forma, mesmo alguém que nunca tenha encontrado *Bernardo* antes, poderá obter sua *chave* pública de uma banco de dados e enviar-lhe um *e-mail* cifrado sem antes precisar compartilhar um segredo com ele. De todo o processo descrito, pode-se fazer duas analogias para um melhor entendimento deste conceito:

- Formar uma idéia e imaginar este sistema como uma caixa de correspondências, onde qualquer usuário *(Alceu)* poderá inserir uma carta por meio da sua abertura (mensagem cifrada com a *chave* pública) e somente o receptor autorizado (*Bernardo*), aquele com a *chave* da citada caixa (a *chave* privada), poderá abrí-la e ler a carta nela depositada (decifrar a mensagem).
- Tentar formar uma idéia imaginando este sistema como uma caixa de metal onde alguém *(Alceu)* insere uma carta e a tranca, utilizando um cadeado de

combinação colocado na caixa por outra pessoa (mensagem cifrada com a *chave* pública de *Bernardo*). Em seguida, esta outra pessoa (*Bernardo*), portanto, passa a ser a única a poder abrir a caixa de metal, pois somente ela conhece a combinação para a abertura do cadeado (a chave privada de *Bernardo*).

Baseado no estudo até este ponto observa-se que com um sistema de *chave* pública, o gerenciamento de *chaves* passa a ter dois novos aspectos:

- Em primeiro lugar deve-se localizar a chave pública de qualquer pessoa com quem se deseja comunicar.
- Segundo lugar deve-se obter uma garantia de que a chave pública encontrada seja proveniente daquela pessoa *(Bernardo).*

Sem esta garantia, um intruso *Everaldo* poderá convencer os interlocutores *(Alceu e Bernardo)* de que as *chaves* públicas falsas pertencem a eles. Caso seja estabelecido um processo de confiança entre os interlocutores, *Everaldo* poderá se fazer passar por ambos e, desta maneira, quando um interlocutor *(Alceu)* enviar uma mensagem ao outro *(Bernardo)* solicitando sua *chave* pública, o intruso poderá interceptá-la e devolver-lhe uma *chave* pública forjada por ele. Ele também poderá fazer o mesmo com o receptor (*Bernardo*), fazendo com que cada lado pense que está realmente se comunicando com o outro, quando na verdade estão sendo interceptados pelo intruso.

Agindo assim, *Everaldo*, então poderá decifrar todas as mensagens, cifrá-las novamente ou, se preferir, poderá até substituí-las por outras mensagens, dando início ao ataque do tipo *Man-In-The Middle* (O Homem do Meio, tipo de ataque a *e-mail* onde um usuário *se* mascara de um segundo usuário para um terceiro e se faz passar por terceiro perante o segundo, se interpondo na troca de mensagem). Deste ataque, um intruso poderá causar tantos danos ou até mais do que causaria se conseguisse quebrar o *algoritmo* de criptografia empregado pelos interlocutores. É realmente um problema que precisa ser analisado e é necessário que se tenha uma garantia de que exista ferramenta implementada para minimizar estas ações. A garantia para evitar este ataque é representada pelos certificados de *chave* pública. Estes certificados consistem em *chaves* públicas assinadas por uma pessoa de confiança e servem para evitar tentativas de substituição de uma *chave* pública por outra. O certificado de *Bernardo* contém algo mais do que sua chave *pública* e contém informações sobre *Bernardo, o* seu nome, endereço e outros dados pessoais e, assinado por alguém em quem *Alceu* deposita sua confiança: uma *autoridade de certificação ou CA* (Certification Authority).

Por meio da assinatura da *chave* pública e das informações sobre *Bernardo*, a *CA* garante e informa que os dados sobre *Bernardo* estão corretos e que a *chave* pública

em questão realmente pertence *a Bernardo. Alceu,* por sua vez, confere a assinatura da *CA* e então utiliza a *chave* pública em evidência, segura de que esta pertence a *Bernardo* e a ninguém mais. Os certificados desempenham um importante papel em um grande número de protocolos e padrões utilizados na proteção de sistemas de *e-mail*.

### 5.6.1 CONSIDERAÇÕES SOBRE TIPOS DE ATAQUES

Segundo Pagliusi (1998), em todos os sistemas de correio eletrônico existem alguns ataques e tentativas de invasões, que são conhecidas e que estão constantemente pondo em risco as mensagens trafegando pelos servidores do *e-mail.*

Escuta clandestina*:* trata-se da obtenção de cópias de mensagens sem autorização, diretamente de uma rede, canal de comunicação ou pelo exame de informações armazenadas e inadequadamente protegidas na rede.

Mascaramento: trata-se do envio ou da recepção de mensagens utilizando a identidade de outro interlocutor *(Alceu* ou *Bernardo*) sem sua autorização. Provê uma forma de ataque conhecido como *Man-In-The-Middle,* onde *Everaldo se* mascara *de Alceu* para *Bernardo e* se faz passar por *Bernardo* perante *Alceu,* se interpondo na troca de mensagem.

Violação de mensagens: é o tipo de ataque em que se dá a interceptação de mensagens e alteração de seus conteúdos antes de entregá-los para o receptor (*Bernardo*) a que se destinam, sendo que é um tipo de ataque também conhecido como ataque ativo*,* pois Inclui também a inserção e a remoção de mensagens.

Repetição: é o armazenamento de cópias de mensagens e o reenvio das mesmas em uma data posterior, ou seja, após a autorização para o uso de um recurso ter sido revogada, mesmo que não se conheça o conteúdo de algum texto, um intruso pode simplesmente, repetir o cifrado durante um protocolo para ganhar acesso a outras informações, sendo também conhecido como ataque da meia-noite.

Inferência: trata-se da tentativa de se obter algum item de informação por meio de cálculos matemáticos, por meio de *criptoanálise* (ciência que estuda a leitura do tráfego cifrado de mensagens sem conhecer o conteúdo dos textos cifrados sem que se seja o legítimo destinatário). Normalmente o objetivo principal é de se obter os conteúdos somente com o auxílio dos textos cifrados, mas isso pode ser muito difícil, sendo assim, a criptoanálise também pode ser baseada em texto escolhido ou texto conhecido. Para os casos de *algoritmos* de bloco, existem métodos próprios de ataque, tais como a Criptoanálise Diferencial e a Criptoanálise Linear. Podemos citar como exemplo de

inferência por criptoanálise o roubo de informações pela derivação de uma *chave* criptográfica.

Busca exaustiva: é a tentativa de se utilizar todas as *chaves* possíveis conhecidas e não conhecidas. É um ponto de referência para os outros tipos de ataques, também conhecidos como Método da Força Bruta, que é um tipo ataque sempre possível e não há como preveni-lo. Uma alternativa utilizada para desestimulá-lo, é a adoção da tática de torná-lo tão dispendioso em tempo e recursos de modo a não valer a pena sequer iniciá-lo. O número total de *chaves* possíveis para um tamanho de *chave n*, igual a $2^{128}$, por exemplo, uma *chave* de tamanho igual a 128 *Bits* possibilita $2^{128}$ *chaves* distintas, ou seja, cerca de $10^{38}$.

Ataque somente ao texto cifrado: um profissional especialista em criptografia possui alguns *e-mails* cifrados com um *algoritmo* conhecido, porém ele não tem acesso ao respectivo texto original das mensagens ou às *chaves* utilizadas. Este profissional tem como meta encontrar os correspondentes textos em claros trocados por *Alceu* e *Bernardo*.

Ataque do texto plano conhecido: é bastante comum um intruso Everaldo ter, além do algoritmo, um ou mais pares de mensagens de Alceu com um texto cifrado e seu respectivo texto claro, empregando a mesma chave. Estes pares, conhecidos como cribs (nome dado a um ou mais pares de mensagens com um texto cifrado e seu respectivo texto claro, empregando a mesma chave criptográfica), podem prestar auxílio à criptoanálise, pois Everaldo tem como objetivo encontrar a chave utilizada na comunicação.

Ataque do texto plano escolhido: tendo em vista que o suposto intruso *Everaldo* escolhe um ou mais pares de textos claros e cifrados correspondentes, cada par com uma *chave*. Pode ser que os claros escolhidos não estejam presentes em nenhuma mensagem real e desta maneira, neste ataque, *Everaldo* escolhe um pedaço de um texto em claro para ser cifrado com um determinado *algoritmo*. Ele conhece o texto claro que escolheu, seu correspondente texto cifrado e o *algoritmo*, mas não conhece a *chave* e tem como objetivo encontrar esta *chave*, para poder desvendar outras mensagens cifradas por *Alceu ou Bernardo* com o mesmo *algoritmo* e a mesma *chave*.

Corte e cola: trata-se de dadas duas mensagens cifradas com a mesma *chave*, sendo que é possível combinar porções de duas ou mais mensagens para produzir uma nova e é possível que não se conheça exatamente o que elas dizem, mas um intruso *(Everaldo)* poderá utilizá-las para enganar um usuário autorizado *(Alceu ou Bernardo),* de modo a este fazer o que ele deseja.

Qualquer usuário ou invasor, para utilizar um dos ataques citados a um sistema de *e-mail*, deverá ter acesso ao sistema de modo a executar o programa que implementa o ataque. A maioria dos ataques é lançada por um dos usuários legítimos de um sistema que, por abuso de suas autorizações executam programas designados para "carregar" uma das formas de ataque. Para usuários ilegítimos, um simples método de infiltração, por meio de suposição de senhas ou pelo uso de programas "quebra senha" para obter a senha de um usuário conhecido e, em adição a estas formas diretas de ataque, há alguns métodos mais sutis, que incluem Vírus de Computador, Verme *(Worm)* e Cavalo de Tróia *(Trojan Horse).*

Como conclusão a que se pode chegar sobre o assunto dos métodos de ataque com suas respectivas formas de infiltração é que, para se produzir um sistema seguro e, particularmente, um sistema de *e-mail* seguro, deve-se projetar os componentes do sistema (por exemplo, os diretórios) assumindo-se que as outras partes (pessoas ou programas) não são confiáveis até que se prove o contrário.

### 5.6.2 CONSIDERAÇÕES SOBRE SERVIÇOS DE SEGURANÇA

Ainda, segundo Pagliusi (1998), uma grande maioria dos serviços de segurança citados neste tópico não são específicos para *e-mail*, ou seja, qualquer documento confidencial pode ser cifrado e assinado, no entanto, os serviços em análise são, na maior parte das vezes, utilizados para correio eletrônico:

Confidencialidade de Conteúdo: a confidencialidade significa proteger a mensagem contra a divulgação a usuários não autorizados, ou seja, a mensagem não deve ser revelada a ninguém, exceto ao destinatário real. Esta certeza pode ser obtida pelo ciframento da mensagem, utilizando-se de *algoritmos* simétricos e de *chave* secreta, ou assimétricos, com duas *chaves* distintas. A submissão de mensagens a múltiplos receptores exige técnicas simétricas, sozinhas ou combinadas com técnicas assimétricas, sendo que o uso de técnicas assimétricas isoladas para ciframento tem um custo mais elevado em termos computacionais, tornando-o inviável para cifrar mensagens inteiras.

Autenticidade da Origem da Mensagem: o termo autenticidade da origem da mensagem simplesmente fornece uma resposta àseguinte pergunta: "Quem *enviou esta* mensagem?", partindo-se do princípio de que é possível a um receptor de uma mensagem averiguar sua origem. Um invasor, denominado *Everaldo,* não deve ser capaz de se fazer passar pelo emissor legítimo da mensagem, pois ela é tipicamente provida pela integridade do conteúdo e desta maneira, a autenticidade da origem da mensagem, proporcionada pela utilização de assinaturas digitais. Estas assinaturas são muito

semelhantes às assinaturas feitas a mão, por serem não reutilizáveis, inimitáveis, autênticas e poderem provar que o documento não foi alterado, como também, não poderem ser repudiadas pelo emissor. Mensagens com assinaturas digitais não são reutilizáveis de um modo geral, mas, elas podem ser repetidas. Apesar do conteúdo da mensagem não poder ser modificado, as assinaturas digitais não garantem necessariamente que linhas de cabeçalho, tais como Date e Subject, não sejam alteradas. Quanto àassinatura e ao ciframento, podem ser combinados de três maneiras distintas, ou seja:

- Ciframento do documento, depois o assinando.
- Assinando o documento, depois cifrando somente o seu conteúdo, deixando a assinatura em claro.
- Assinando o documento, depois cifrando seu conteúdo junto com a assinatura.

A terceira opção é a melhor, sob o ponto de vista de proteger a identidade do emissor perante intrusos.

Autenticidade da Integridade do Conteúdo: Trata-se de assegurar que o conteúdo da mensagem não foi modificado, ou seja, garantir e possibilitar ao destinatário de uma mensagem *(Bernardo)* verificar que ela não foi modificada em trânsito e um possível invasor *(Everaldo)* não deve ser capaz de substituir uma mensagem legítima por outra falsa, sendo que e a autenticidade da origem da mensagem deverá ser automaticamente provida pela integridade do seu conteúdo. Certamente, ambas devem sempre ser utilizadas em conjunto: a manutenção da integridade não tem qualquer valor se a origem da mensagem não puder ser confirmada. A origem autenticada não possui valor algum se a integridade não puder ser preservada. O fato de se verificar a integridade do conteúdo de uma mensagem muito grande é, uma operação exaustiva. Então, calculado-se um pequeno *Valor Hash* (o mesmo que *Message Digest*. Funciona com uma impressão digital que possibilita a distinção entre uma mensagem e outra, mesmo se ambas diferirem por apenas um *bit*), em separado da mensagem e este valor segue incluso na mesma. Um *Valor Hash* consiste em uma pequena e única quantia de informação, que é associada a uma mensagem em particular, porém muito menor do que a mensagem em si. Como conseqüência, a verificação da autenticidade da origem da mensagem e da integridade do seu conteúdo torna-se uma operação bem mais simples: a autenticidade completa da mensagem a ser averiguada com base na conferência de um pequeno *Valor Hash* previamente assinado.

Não Repúdio: Trata-se do não repúdio da origem e, em sua concepção mais simples, consiste apenas na autenticação da origem da mensagem (e também da integridade do conteúdo) combinada com *algoritmos* de ciframento assimétrico, sendo

que deste modo, um emissor *(Alceu)* não poderia falsamente negar, mais tarde, que teria enviado a mensagem. No entanto, com a utilização do não repúdio do recebimento existem alguns problemas, ou seja, mensagens de trote não podem ser detectadas antecipadamente e para solucionar este caso, o receptor da mensagem, *Bernardo*, poderia primeiro confirmar a impressão digital de uma mensagem, mas neste caso ele poderia rejeitá-la e, portanto, recusar o seu recebimento. Além deste fato, não há nenhuma definição consensual do termo recebimento e, freqüentemente, ele significa leitura, mas não há nada informado sobre o entendimento da mensagem ou sobre tomar alguma ação a respeito dela. Os sistemas *EDI* (Electronic Data Interchange) permitem requisitar que os destinatários não possam ler as mensagens sem uma notificação de recebimento assinada. Isto pode ser obtido pelo uso do *DCMP* (Digital Certified Mail Protocol). Este protocolo, na teoria é válido, porém é complexo e pouco prático, exigindo o envio de aproximadamente 200 (duzentas) mensagens entre o emissor e o receptor e baseando-se na revelação de *chaves* secretas, *bit a bit,* para ambas a parte. Uma outra maneira consiste na utilização de um árbitro, que impediria o receptor de ler uma mensagem antes do envio de um recibo assinado ao emitente.

### 5.6.3 CONSIDERAÇÕES SOBRE PADRÕES E PRODUTOS

O *e-mail* é atualmente uma das formas de comunicações mais comuns, prática e objetiva, tanto quanto o telefone e sua utilização vêm crescendo gradativamente. Com isto o seu gerenciamento, monitoramento e segurança são de extrema importância a fim de garantir a integridade das informações contidas nos servidores dos correios eletrônicos. Embora seja bastante seguro e capaz de transitar por meio de muitas redes até chegar a seu destinatário, o *e-mail* se torna vulnerável em alguns aspectos, como:

- Interceptação e quebra de privacidade.
- Replicação, adulteração, falsificação de seu conteúdo.
- Falsificação de identidade.

Em resumo, com o objetivo de se evitar estas fragilidades, alguns requisitos de segurança são necessários. A utilização de:

- Criptografia para a codificação do seu conteúdo.
- O uso do *Algoritmo* de Hash ou Valor Hasch, Message Digest ou MAC para garantir a integridade da mensagem.
- Assinatura Digital para verificação de remetente.
- Criptografia com *Chave* Pública para verificação de destinatário.

Com relação aos protocolos de *e-mail* seguro existem alguns padrões importantes:

- *PGP*: Pretty Good Privacy & Open PGP
- *S/MINE*: Secure Multipurpose *Internet* Mail Extension
- *PEM*: Privacy-Enhanced Mail
- *MOSS* : MINE Object Security Service
- *MSP*: Message Security Protocol (uso militar)
- Os padrões mais utilizados são o *PGP* e o *S/MINE*.

Segundo Pagliusi (1998), quando analisados na prática, os *algoritmos* criptográficos de *chave* pública são pesados e complicados e, por este motivo, são pouco utilizados para cifrar mensagens eletrônicas inteiras, pois o processo levaria muito tempo, sendo assim, os programas de segurança de correio eletrônico existentes utilizam a criptografia de *chave* pública apenas voltada para o gerenciamento das *chaves*, e não para o ciframento de mensagens inteiras.

O trabalho de ciframento das mensagens é feito utilizando-se *algoritmos* de criptografia convencional ou de *chave* secreta, que são mais rápidos, tais como o *DES* (Data Encryption Standard), e o *IDEA*. Sempre que há um novo ciframento de mensagens, os programas de ciframento de *e-mail* geram uma nova *chave* secreta a ser utilizada pelo *algoritmo* convencional, também conhecida como *chave* de sessão aleatória e, deste modo, somente esta *chave* de sessão é cifrada pela criptografia de *chave* pública. Sendo assim, o *algoritmo* de *chave* pública é utilizado como NÃO no ciframento de mensagens inteiras e SIM na distribuição de *chaves* de sessão aleatória. Abaixo seguem alguns exemplos dos padrões e produtos utilizados no mercado para o ciframento em *e-mail*.

*PGP* (Pretty Good Privacy): a data de sua implementação é de 1991, sendo que é o produto para segurança de *e-mail* com maior utilização e sucesso, tornando-se o padrão para ciframento de *e-mail* na *Internet*. Foi concebido para ser utilizado com todos os sistemas de correio eletrônico existentes e encontra-se disponível em quase todas as plataformas de Sistemas Operacionais, sendo que é considerado um programa completo em termos criptográficos e gerou várias discussões desde que seu criador, Phil Zimmermann, foi indiciado por facilitar sua exportação ilegal dos Estados Unidos, tornando o programa disponível via *Internet*.

Com relação às funcionalidades mais importantes do *PGP*, pode-se citar o modelo de distribuição para o gerenciamento de *chaves*, sendo que não há hierarquia de autoridades para certificação e, ao contrário, o *PGP* provê uma teia de confiança, composta por uma rede distribuída de indivíduos. Para o *PGP* é válida a frase: "Eu conheço quem você é porque eu confio em alguém que acredita que você é quem diz ser". O fato é que todo usuário gera e distribui sua própria *chave* pública por meio do *e-*

*mails*, pela *Internet*, servidores de *chave* ou boletins internos. Cada usuário assina conforme desejarem as *chaves* públicas uns dos outros e criando, desta maneira, grupos de usuários *PGP* interligados e decidem em quem confiam para atestá-los para outros usuários, como um referencial. Cada usuário pode obter as *chaves* diretamente, tornando-se sua própria origem da confiança, e cada terceira pessoa torna-se uma autoridade de certificação ou *CA* (Certification Authority). Este fato apresenta consigo problemas de escala, ligados à administração de *chaves*, como é o caso de uma rede composta por milhares de usuários do *PGP*, onde um usuário não pode verificar a validade de todas as outras *chaves*. Por outro lado, o *PGP* não requer nenhuma infra-estrutura sofisticada para seu funcionamento, ou seja, dois usuários podem começar a utilizá-lo para se comunicarem a todo instante e outros usuários poderão ser adicionados ao primeiro e, deste modo, a rede cresce rapidamente. Outra característica é que o *PGP* também não proporciona autenticação do recebimento. Em resumo, o sucesso do *PGP* se deve a alguns itens, tais como:

- Disponibilidade para uso em várias e difrentes plataformas.
- Aplicável na segurança de *VPN* (Virtual Privacy Network), arquivos e *e-mail*.
- Trabalho com *algoritmos* seguros.
- Não foi desenvolvido e não é totalmente controlado por nenhuma entidade governamental ou privada.
- É uma ferramenta de fácil utilização.

A distribuição do código é pública garantindo sua credibilidade.

*PEM* (Privacy-Enhanced Mail): o *PEM* foi o padrão adotado pela IAB (*Internet* Architecture Board) para prover a segurança do correio eletrônico existente na *Internet*. Foi projetado inicialmente pelo IRTF (Internet Resources Task Force) e PSRG (Privacy and Security Research Group) e foi repassado para o IETF / PEM Working Group, que efetuou a publicação dos documentos finais em 1993. O padrão *PEM* abrange a essência dos serviços de segurança do Modelo de *OSI/I.S.O* de ciframento, autenticação, integridade de mensagens e gerenciamento de *chaves*, sendo esta baseada em uma hierarquia de certificados. Da mesma maneira que o *PGP*, o *PEM* também não proporciona autenticação do recebimento e pode ser executado em quase todos os sistemas de *e-mail* existentes. Todos os protocolos e procedimentos do *PEM* foram projetados para serem compatíveis com uma certa variedade de modelos de gerenciamento de *chaves*, o que faz com que o *PEM* inclua tanto o esquema de criptografia simétrica quanto o de *chave* pública para o ciframento das *chaves* de sessões. O padrão *PEM* permite ainda diferentes combinações entre alguns *algoritmos* que suporta, utilizando também criptografia simétrica para cifrar o conteúdo das

mensagens e *algoritmos Hash* criptográficos para garantir a integridade dos *e-mails*. Não é possível despachar por meio do *PEM* mensagens sem assinatura, o que obriga a assinatura de todas as mensagens, algo um pouco inconveniente e demorado.

Uma das características que mais se destacam no *PEM* é a sua distribuição hierárquica de chaves, o controle centralizado, conseguido por meio de um pequeno número de servidores denominado de *Root* formando a *IPRA (Internet* PCA Registration Authority), sendo *PCA* (Policy Certificatzon Authority), que são as origens de toda a confiança. Esta confiança do *PEM*, é obrigatória e não uma escolha individual de um determinado usuário e, neste caso, é válida a: "Eu conheço quem você é porque seu *CA* assinou por você, seu *PCA* pertinente assinou por seu *CA* e o *IPRA* assinou por seu *PCA*", onde *IPRA, PCA* e *CA* representam entidades organizadas em uma estrutura hierárquica, conforme Figura 22, abaixo.

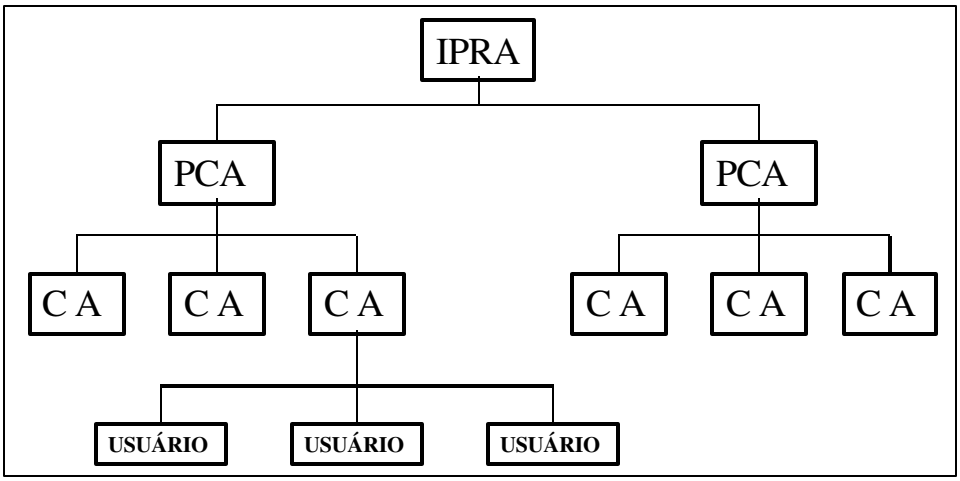



Figura 22 – O Esquema Hierárquico dos Certificados PEM

Fonte: Pagliusi. (1998, p.58).

De acordo com as normas do *PEM*, dois usuários sempre possuirão alguma autoridade hierarquicamente superior em comum que tenha assinado ambas as *chaves* para possibilitar uma comunicação mútua, segura e confiável e, em última análise, esta autoridade poderia ser o *IPRA* raiz. O *IPRA*, que é uma autoridade central e raiz da hierarquia de certificados, efetua a cobrança de uma taxa para o seu funcionamento e todas as *chaves* precisam ser certificadas, demandando suporte e custo adicional. Embora na teoria seja altamente escalável, o padrão *PEM* necessita de infraestrutura e de diretórios públicos para suportar sua escalabilidade. Desta maneira, os produtos desenvolvidos segundo a especificação *PEM*, como o *RIPEM* (Riordan's Internet Privacy-

Enhanced Mail), não implementam a totalidade de suas especificações e o *RIPEM*, não utiliza a certificação para autenticação de *chaves* prevista.

Além do *PGP* e o *PEM*, existem outros padrões e produtos que trabalham como provedores de recursos de segurança para o *e-mail*, por exemplo, o padrão *PGP/MIME*, que adiciona ao *PGP* a habilidade de manusear objetos *MIME* (Multipurpose Internet Mail Extensions). O *PEM* foi adaptado aos objetos *MIME* por meio *do MOSS* (MIME Object Security Services). O *S/*MIME (Secure Multipurpose Internet Mail Extensions) consiste em um esforço em pesquisas de um consórcio de empresas, liderado pela RSADSI e pela Microsoft, para adicionar segurança a mensagens eletrônicas no formato *MIME*. O *S/MINE* foi desenvolvido com tecnologia diferente do *PGP*, que tem seu uso escolhido preferencialmente para a segurança pessoal de *e-mail*, o *S/MINE* surge mais como um padrão para a indústria e para o uso comercial e organizacional e essencialmente tem as mesmas funções de autenticação e confidencialidade do *PGP* embutidas no padrão MINE de seu conteúdo.

### 5.6.4 RECOMENDAÇÕES PARA UM SISTEMA DE *E-MAIL* SEGURO

As organizações, as universidades e as pessoas precisam se comunicar via correio eletrônico, precisam confiar neste serviço e este sistema precisa ser seguro, precisos, objetivos e de fácil utilização, sendo que também é necessário um meticuloso gerenciamento das *chaves*. Alguns pontos também são importantes para esta segurança, ou seja, a Confidencialidade de Conteúdo, a Autenticidade da Origem da Mensagem, a Autenticidade da Integridade do Conteúdo e o Não Repúdio.

Segundo Pagliusi (1998), conforme analisado, o fato de se prover tais características a um sistema de *e-mail* exige um certo conjunto de ferramentas, sendo que do lado do emissor (*Alceu*), é necessário:

O Ciframento de *chave* pública, que é o ponto central de um sistema de segurança de *e-mail* e que consiste na habilidade de se prover comunicação segura com outras pessoas sem haver a necessidade de se trocar *chaves* secretas com elas inicialmente e a criptografia de *chave* pública é uma das possibilidades de se fazer isto.

A Assinatura Digital é um modo de se prover a autenticação e a integridade da mensagem e a criptografia de *chave* pública também é uma maneira de se prover este recurso com eficiência.

Do lado do receptor (*Bernardo*), é preciso:

- Deciframento por *Chave* Pública e
- Verificação de Assinatura Digital.

Em complemento, é necessário a existência de toda uma infra-estrutura de *chaves* públicas, de modo que um emissor qualquer possa enviar uma mensagem cifrada a qualquer receptor, sem terem que se encontrar previamente e, é preciso também gerar e distribuir *chaves*, e às vezes revogar aquelas que tenham sido objeto de furto ou que tenham sido perdidas. Para o sucesso, boa aceitação e confiança no uso, é preciso que todos estes recursos estejam em um único pacote, fácil de utilizar, que possa interagir com todos os sistemas de correio eletrônicos da *Internet* e que possa ser empregado rotineiramente.

Inicialmente, um bom sistema de proteção de *e-mail* tem a necessidade de ser seguro, caso contrário, não há razão para utilizá-lo, pois a segurança é muito mais que escolher um bom par de bons *algoritmos* de criptografia. A segurança é como uma corrente, que é tão resistente quanto o seu elo mais fraco. E em um sistema de segurança de mensagens eletrônicas existem muitos elos fracos com que se preocupar, por exemplo, *algoritmos* convencionais, de *chave* secreta, para o ciframento do conteúdo da mensagem, por exemplo, o *IDEA*, os *algoritmos* de *chave* pública para o gerenciamento de *chaves,* por exemplo, o *RSA*, os *algoritmos* de *chave* pública para assinaturas digitais, por exemplo, o *RSA* e o *DSA*, funções de espalhamento unidirecional para emprego com assinaturas digitais, por exemplo, o SHA e o MD5, a geração de números aleatórios, para utilização na criação de *chaves* de sessão para o *algoritmo* convencional, a geração de números primos, para uso na criação de *chaves* públicas e privadas, o armazenamento de *chaves* públicas e privadas, os procedimentos de gerenciamento de *chaves*, os cuidados ao apagar arquivos e a Interface com o usuário.

A relação citada acima não é exaustiva, se um órgão de inteligência do governo desejar monitorar a comunicação de algum usuário, ele certamente não o fará por meio de quebra do *IDEA* ou do Triplo *DES*, mesmo porque a criptografia é uma disciplina acadêmica há tempos sendo estudada e com vários *algoritmos* na literatura publicada, têm sido analisados por inúmeros usuários e pesquisadores que a têm considerado segura. Provavelmente o órgão de inteligência fará o monitoramento pela exploração de alguma fraqueza em uma seção obscura do programa de segurança de correio eletrônico utilizado na comunicação e com o intuito de se validar a afirmação anterior, o *algoritmo* convencional utilizado deverá possuir um tamanho de *chave* de pelo menos 112 *bits*. O *algoritmo* de *chave* pública deve possuir um tamanho de *chave* de pelo menos 1024 *bits*.

Observa-se que a geração das *chaves* de sessão aleatória é mais difícil do que a escolha e a implementação de um *algoritmo* criptográfico, pois os números realmente aleatórios não podem ser gerados num computador digital, que se pode fazer é gerar

números pseudo-aleatórios isto é, seqüências de números com uma determinada lei de formação, o conhecimento da regra de recorrência permite determinar um elemento da seqüência a partir do anterior.

O gerenciamento de *chaves* também é uma tarefa árdua, sendo que existem uma série de ataques possíveis contra as *chaves*, e um bom sistema deve levar em conta todos eles e, ainda deve se resguardar contra *chaves* falsas substituindo *chaves* legítimas, *chaves* furtadas ou antigas sendo armazenadas para posterior reutilização, entre outros ataques.

Outro objeto de verificação é a análise de tráfego que deve ser dificultada ao máximo, pois se trata de um problema complexo, que não pode ser solucionado, normalmente, apenas por meio de um programa de segurança de *e-mail*.

Deste modo, é muito mais fácil quebrar um programa de segurança do que provar que ele não pode ser quebrado. É possível provar que um certo usuário não possa quebrá-lo com uma determinada quantidade de recursos em um tempo previamente definido, porém este fato não prova nenhuma alternativa sobre outros usuários tentando quebrá-lo com mais recursos, mais tempo e com maior conhecimento técnico.

Em resumo, um aplicativo ou sistema de segurança de *e-mail* tem a necessidade de ser bastante flexível, deve permitir aos usuários o envio de mensagens cifradas não assinadas, assinadas não cifradas e mensagens assinadas e cifradas. Precisa, ainda, ter a característica de cifrar as mensagens que armazena e deve possibilitar o envio de mensagens tanto para um único quanto para múltiplos outros usuários de correio eletrônico.

É importante que este programa tenha adaptabilidade, que também esteja disponível para todo o tipo de plataforma de sistema Operacional de computadores, seja *Unix*, *MS-DOS* ou *Windows.* Usuários que utilizam um sistema operacional devem ser capazes de enviar mensagens seguras para pessoas que utilizam outro sistema e, quanto mais flexível for o programa de segurança, maior utilidade ele terá, quanto maior sua utilidade, maior sua presença nos mais variados ambientes e máquinas, que é o objetivo final de todo programa de segurança de *e-mail*.

É de caráter imprescindível que este sistema aplicativo de segurança de correio eletrônico permita o uso de uma variedade de diferentes *algoritmos*, pois alguns usuários poderão preferir o *DES*, outros o IDEA ou o Triplo *DES* e, caso a comunidade científica descubra que um determinado *algoritmo* criptográfico possa ser quebrado, seria uma simples questão de substituí-lo por outro.

Com relação à interface como usuário final, existe uma pequena estória que se for perguntado a um comandante de um submarino se ele deseja ou não um novo

componente em seu submarino, ele responderia: "somente se ele não provocar nenhum ruído, não ocupar nenhum espaço, não utilizar nenhuma energia de bordo e contribuir para a melhora do desempenho do submarino como um todo". A segurança computacional tem muita relação com esta citação, pois os usuários a desejam, porém somente se ela não exigir nenhuma memória adicional, não afetar o desempenho e a performance do sistema e tiver uma característica totalmente transparente ao usuário final, porém, todas estas observações ainda não são possíveis. Apesar de não conseguir atender todas as objeções citadas, deseja-se que um programa de segurança de *e-mail* chegue o mais próximo possível desta meta e que o envio de uma mensagem eletrônica assinada e cifrada deveria ser a opção rotineira em qualquer programa deste tipo, sendo que o usuário deveria apenas realizar uma tarefa extra para o envio de mensagem sem assinatura e / ou não cifrada.

Outra objeção importante, é que o programa deveria estar apto a produzir mensagens cifradas que passassem por meio de todos os sistemas de *e-mail* sem sofrer qualquer alteração, como também, decifrar mensagens no destino que tivessem passado por meio de uma grande variedade de *gateways* de *e-mails* e sem sofrer qualquer intervenção do usuário final e, além de todos estes fatos conseguir ter mecanismos de proteção contra *Spam, Hoax, Worm, Trojans Horse* (Cavalo de Tróia) e *e-mail* bomba.

Em resumo, um programa que tenha uma boa interface com o usuário final é muito mais complexo e difícil de se conseguir do que ter uma boa segurança, pois a *Internet* está repleta de diferentes computadores, equipamentos de comunicação de dados, sistemas operacionais, programas de *e-mail* e usuários com conhecimento bastante diversificado. Todas estas pessoas têm suas próprias preferências, e é virtualmente impossível fazer um programa que trabalhe bem em todos os ambientes computacionais e que consiga atender a todas as aspirações de todos os usuários.

Até este ponto deste capítulo, foi feita uma abordagem do correio eletrônico com relação à segurança do *e-mail*, principalmente com referencia à criptografia das mensagens. No próximo tópico será feita uma abordagem do problema relacionado aos vírus de computadores, fatores bastante preocupantes e causadores de danos às organizações.

### 5.7 CONSIDERAÇÕES SOBRE ANTIVÍRUS E VÍRUS DE COMPUTADOR

Segundo Shang (1994), a designação Vírus de Computador é bastante comum atualmente, porém muitas pessoas ainda desconhecem do que se trata. Um vírus de computador é um programa que pode ser executado em um computador, mas o que

acontece em seguida, normalmente é imprevisível e depende do vírus. O termo vírus se tornou sinônimo de dificuldade e causador de problemas nos computadores existentes. Todos são programas indesejáveis, não convidados, potencialmente perigosos, porém importantes diferenças existem entre todos eles com relação à manifestação. Um vírus pode infectar arquivos e setores de inicialização de disquetes, discos de armazenamento de dados em microcomputadores pessoais e em servidores de dados, principalmente de correio eletrônico e, neste caso, contaminado por meio de vírus anexados a arquivos que tenham chegado pela *Internet*. O processo de infecção inclui sobregravação, preposição e anexação em arquivos. Um vírus de sobregravação normalmente se instala no início do programa, diretamente sobre o código do programa original, de modo que o programa fica quebrado ou dividido, particionado e quando se tentar executa-lo, nenhuma ação se realiza, com exceção de que o vírus contamina outro arquivo, mais um outro e, deste modo, a infecção se torna completa. Este tipo de vírus é facilmente detectado e removido. Um vírus de preposição pode simplesmente coloca todo seu código sobre o programa original e, quando se opera um programa infectado, primeiro o código do vírus opera e, na seqüência, o programa original é executado. Um vírus de anexação instala o início do programa no final do arquivo é colocada uma marca no início do arquivo e se instala entre o que originalmente foi o final do arquivo. Quando se tentar operar o programa, a marca chama o vírus, que entra em operação sobre o original.

Segundo Schifreen (1992), existem uma infinidade de *softwares* que produzem uma varredura dos discos, memória das máquinas verificando a possibilidade de existência de vírus. Estes programas possuem inofensivos detectores de vírus já conhecidos, que é recomendável sua instalação e pesquisa constantemente nos equipamentos. É importante existir uma sistemática de atualização constante da lista de vírus nos computadores, o que auxilia no processo de prevenção da contaminação por meio de vírus mais novos que tenham surgido no mercado.

O fato de se manter um cuidado especial junto às caixas postais dos usuários de correio eletrônico, efetuando regularmente uma varredura para se eliminar possíveis vírus em arquivos que tenham vindo via *Internet*, garante uma maior segurança da rede de dados, tendo em vista que um vírus que possa se instalar em todos os microcomputadores existentes na rede e que tenha potencial para deflagrar um ataque simultaneamente em todos os microcomputadores, provocaria um prejuízo de enormes proporções.

Um vírus de computador é, ainda um programa que pode infectar outro programa de computador por meio da modificação deste, de forma a incluir uma cópia de si mesmo. A denominação de programa-vírus vem de uma analogia com o vírus biológico, que

transforma a célula numa fábrica de cópias do vírus. Para o público em geral qualquer programa que apague dados, ou atrapalhe o trabalho pode levar a denominação de vírus. Do ponto de vista de um programador, o vírus de computador é algo bastante interessante. Pode ser descrito como um programa altamente sofisticado, capaz de tomar decisões automaticamente, funcionar em diferentes tipos de computadores, e apresentar um índice mínimo de problemas ou mal-funcionamento. Os vírus de computadores, por serem criados por programas de computadores, podem ser considerados como a primeira forma de vida construída pelo homem, tendo em vista o argumento de que a auto-reprodução e a manutenção da vida são –- para alguns cientistas –- o básico para um organismo ser descrito como vivo. De fato, o vírus é capaz de se reproduzir sem a interferência do homem e também de garantir sozinho sua sobrevivência. Por exemplo, o vírus chamado Stoned é um exemplo que resiste até hoje, anos depois da sua criação. Sendo o vírus um programa de computador sofisticado, ainda que use técnicas de inteligência artificial, ele obedece a um conjunto de instruções contidas no seu código. Portanto é possível se prevenir contra seu funcionamento, conhecendo seus hábitos.

Seus efeitos vão desde o simples aumento de alguns *bytes* em arquivos até a formatação do disco rígido. O primeiro vírus foi descoberto em 1983 e a partir de então todos os dias surgem novos. Calcula-se que haja mais de dez mil vírus circulando atualmente, sem contar as variantes, filhotes adulterados dos vírus, que chegam a causar danos maiores que os pais originários. Num mundo de informações globalizadas, ter um programa antivírus instalado no servidor e nas estações de trabalho é fundamental. Um arquivo infectado compartilhado seja via rede, via *e-mail* ou via disquete, pode contaminar toda estrutura e até paralisar o sistema. Não basta apenas instalar o programa, é necessário atualizá-lo constantemente. De acordo com o *NCSA* (National Computer Security Association), consórcio de empresas que tem a função de testar e certificar a qualidade de um programa antivírus, uma contaminação por vírus causa, por ano, uma média de 44 horas de paralisação em um computador, 21.7 dias de trabalho perdidos e um custo adicional de US$8366.00 por máquina. Isto se traduz em bilhões de dólares em prejuízos que poderiam ser evitados pelo uso de antivírus atualizado mensalmente. Todavia devemos acrescentar que nenhum antivírus é 100% seguro e que um bom sistema de *back-up* e a atualização constante do antivírus é imprescindível. Fabricantes de software antivírus, como a Symantec, McAfee, Trend Micro e Cheyenne já desenvolveram produtos que podem ser instalados automaticamente nas estações de trabalho a partir do servidor, reduzindo o tempo de configuração. Além disso, esses produtos podem ter suas bibliotecas de vírus atualizadas sempre que for

feita uma conexão com a *Internet*, sendo esta atualização realizada em *background*, sem mesmo o usuário perceber.

Segundo Oliveira (2001), o vírus de computador é um *software* que inspira fascínio, atenção e estimula a curiosidade de profissionais e estudantes de informática. Em uma última convenção promovida na Argentina sobre *Hackers* e fabricantes de vírus, dentre os vários questionamentos evidenciados, um deles foi o de se saber o motivo pelo qual os vírus são criados. Dentre as várias respostas, algumas podem ser citadas:

- Por diversão e entretenimento.
- Para se estudar as possibilidades relativas à vida artificial, tendo em vista a idéia de que *"Os vírus de computador são as primeiras formas de vida feitas pelo homem". (Stephen Hawking).*
- Para se descobrir se, como *Hackers*, têm a capacidade e competência técnica necessária para a concretização da criação de um vírus, para execução de testes de conhecimento.
- Por motivo de frustração, vingança ou conseguir fama.
- Curiosidade, uma das formas de conhecer sobre vírus é "criando um novo".
- Para punir usuários que copiam programas indevidamente e não pagam pelos direitos autorais.

Finalidades militares com o objetivo de atrapalhar as informações do inimigo.

### 5.7.1 VÍRUS DE MACRO

Segundo Vírus & Cia (2001), quando se utilizam alguns programas, por exemplo, um editor de texto, e necessita-se executar uma tarefa repetidas vezes em seqüência (por exemplo, substituir todos os "eh" por "é"), é possível se editar um comando único para efetuá-las. Este comando é chamado de macro, que pode ser salvo em um modelo para ser aplicado em outros arquivos. A opção de se poder fazer um modelo com os comandos básicos dos editores de texto auxiliam muito na performance de trabalho dos usuários, pois são implementadas facilmente por meio do recurso de criação de macros automatizada dos aplicativos. Os vírus de macro ou macrovírus, atacam justamente estes arquivos –- das macros –- comprometendo o funcionamento do programa. Os alvos principais são programas de uso comum: o editor de texto MS-Word e a planilha de cálculo MS-Excel. Depois de ativos, as macros podem se auto-executar, sorrateiramente e automaticamente, acionando uma série de comandos a todo o momento em que um arquivo for aberto, ou seja, outro documento que continha macros pode, ao ser aberto, infectar um que originalmente não os tinha. Um caso muito interessante é o do vírus Melissa, cuja disseminação foi muito rápida, tendo forçado diversas empresas a

desligarem seus servidores de *e-mail* em 26/03/1999. Ao contrário dos vírus até então existentes, que se limitavam a arquivos executáveis ou afins e áreas de *boot*, os macrovírus infectam e se espalham por arquivos de dados, cuja simples abertura pode ativar o vírus. Segundo Moreira (2001), o vírus Melissa é um vírus que é recebido no microcomputador via *e-mail* anexado a um arquivo do MS-Word e, ao infectar a máquina, ele procura pela lista de endereços do programa de correio eletrônico e envia clones de si mesmo a outros cinqüenta usuários automaticamente, causando uma auto-reprodução, disseminação a outras pessoas e causando congestionamento das redes e provedores. Para que o Melissa possa realmente se alastrar pela máquina, é necessário que o usuário abra o arquivo do MS-Word anexado ao *e-mail* recebido e contendo a macro que dispara a contaminação.

Esta ameaça bastante comum, o vírus de macro, e que normalmente acompanham documentos do Microsoft Word ou Excel, bastando que o documento seja aberto para que o vírus seja executado, também desabilitam funções como salvar, imprimir e transformam arquivos em *templates* (tipo e formato de arquivo característico dos produtos da empresa Microsoft S.A, que são modelos prontos para futuras adaptações). São os únicos que podem migrar de uma plataforma para outra, derrubando um dos vários mitos existentes sobre os vírus. Com a utilização cada vez maior do correio eletrônico, esses vírus são cada vez mais disseminados e são responsáveis por cerca de 80% das infecções Para minimizar os problemas causados por eles, surgiram os *Gateways* antivírus para *Internet*, que verificam todas as mensagens antes de serem passadas para os clientes.

A disseminação deste tipo de vírus é muito mais rápida, pois os documentos são muitos móveis e transitam de máquina em máquina (entre colegas de trabalho, estudantes, amigos). Ao escrever, editar ou, simplesmente, ler arquivos vindos de computadores infectados, a contaminação ocorre como as verdadeiras "epidemias", que podem acontecer em pouco tempo. Além disso, os macrovírus constituem a primeira categoria de vírus multiplataforma, ou seja, não se limitam aos computadores pessoais, podendo infectar também outras plataformas que usem o mesmo programa, como o Macintosh. Quando a macro é ativada (a macro AutoOpen do MS-Word, por exemplo), os comandos nela existentes se autocopiam, juntamente com qualquer outra macro que o vírus necessite. Assim, quando abrimos um documento infectado, automaticamente executamos o código virótico. Esse código altera o ambiente interno do MS-Word de forma que todos os futuros documentos salvos utilizando a função "AutoOpen" sejam infectados com o código virótico. O destino dessas cópias é a memória o Modelo global do MS-Word ou o arquivo Normal.dot, de onde o vírus contaminará qualquer novo

documento que for criado ou, mesmo, qualquer documento que for aberto. Existe um outro agravante em relação a estes vírus, que é a facilidade de lidar com as linguagens de macro, no que diz respeito à edição e criação, dispensando que o criador do vírus seja um especialista em programação, ao contrário da linguagem Assembly, com formato pouco amigável e altamente abstrato. Isso acarretou no desenvolvimento de muitos vírus e inúmeras variantes, em um período curto de tempo.

Cuidados a serem tomados**:**

1. Copiar e instalar os "*viewers*": Os documentos do MS-Word, do MS-Power-Point e do MS-Excel podem transmitir vírus, ativados por macros. Uma das maneiras de conseguir proteção é copiar diretamente do site da Microsoft os programas *freeware* Word-Viewer, PowerPoint-Viewer *e* Excel-Viewer. Como eles são apenas *Viewers*, eles não executam nenhuma instrução macro e permitem visualizar e imprimir todo o documento, com toda a sua formatação sem precisar abrí-lo.

No caso do visualizador do MS-Word, depois de instalado surgirão outras opções, como o MS-WordView, no menu de contexto (o menu que aparece quando se efetua um acesso com o botão direito do mouse sobre o nome do arquivo, dentro do MS-Windows Explorer). Desta maneira, ao se efetuar um acesso em um arquivo tipo .doc, por exemplo, o programa MS-Word-Viewer é que abrirá o arquivo e ele é um *freeware* (software que pode ser usado, copiado ou distribuído sem qualquer custo), que vem no CD das últimas versões do Microsoft Office, mas também pode ser copiado a partir do site da oficial da Microsoft:

### 5.7.2 VÍRUS DE *BOOT*

Segundo a Módulo Security Solutions (3) (2000), uma grande maioria dos vírus de *boot* (nome designado à área do disquete ou do *Hard Disk* (disco rígido), utilizado para armazenamento de dados dos microcomputadores ou servidores de dados, residentes tem a característica de utilizar a mesma técnica para reservar memória do sistema para poder efetuar a sua cópia, ou seja, executar uma redução do tamanho da memória *MS-DOS* (Sistema Operacional desenvolvido pela empresa Microsoft, também conhecido por *MS-DOS*), que pode gravar uma palavra no endereço de memória 0040:0013 e copiar seu código para esta parte da memória. Geralmente, o tamanho da memória reservada para o *MS-DOS* é reduzido em uma única unidade (1 KB) para o caso de se tratar de vírus de *boot* pequenos, que ocupam um único setor do espaço do disco (512 bytes) com seu código. Quando a ação do vírus se inicia, ele manuseia a segunda metade de um KB como um *buffer* de leitura e gravação para o processo de

infecção dos discos. Caso, porém, o vírus possa ocupar mais do que 1 KB, ou utilizar técnica de infecção fora do padrão, exigindo uma área de *buffer* (Segmentos de memória utilizados para armazenamento de dados durante um determinado processamento), de memória de leitura e gravação maior, sendo que para este caso o tamanho da memória *MS-DOS* é reduzido em vários KB (entre os vírus conhecidos, o recorde é do "RDA.Fighter", que chegou a 30 KB). Após esta fase, alguns vírus aguardam que o *MS-DOS* inicialize e restaure o valor original do tamanho da memória original do *MSDOS* e com isto, eles ficam localizados dentro da área reservada para o *MSDOS*, mas como um bloco separado desta memória. Alguns vírus de *boot* não utilizam a memória *MS-DOS* nem modificam o tamanho da memória do sistema, sendo que eles se replicam para alguma área ociosa da memória principal, aguardam a inicialização do *MS-DOS* e, na seqüência instalam o seu código de todas as maneiras possíveis em *MS-DOS*.

Os vírus que se enquadram nesta categoria utilizam diversas maneiras para interceptar o momento da inicialização do *MS-DOS* e uma das maneiras mais “populares” é a de verificar o valor de *INT 21h* (interrupção das funções do *MS-DOS*), caso este valor tenha sido modificado, os vírus pensam que a instalação do *MS-DOS* foi concluída. *INT 21h* é verificado quando *INT 8, 1Ch* (interrupções do cronômetro, para isso os vírus também interceptam as interrupções do cronômetro, além das interrupções dos serviços do disco) ou *INT 13h* são acionados. Um dos tópicos que é menos comum é a verificação dos dados lidos do disco (para tanto, é necessário interceptar apenas *INT 13h*) e para o caso do *buffer* de leitura conter um cabeçalho de arquivo .EXE, os vírus interpretarão que a inicialização do *MS-DOS* foi concluída, devido ao fato de um arquivo EXE ter sido “carregado” na memória para execução. Com o objetivo de se interceptar chamadas de disco, a maioria dos vírus de *boot* intercepta *INT 13h*, que é a principal interrupção para essas operações. Existe uma outra interrupção, a interceptação *INT 40h*, que é utilizada em menos casos e é a interrupção utilizada em operações com discos flexíveis. Existem alguns métodos exóticos de interceptação de chamadas de disquetes do *BIOS* (*Basic* /*Input Output System*) e *MS-DOS* são ainda menos utilizados, porém não vem ao caso efetuar qualquer citação por tratar-se de detalhe bastante técnico. Se *INT 13h/40h* são interceptados, os vírus processam os comandos de leitura e gravação de setores (AH=2,3), verificam se o disco está infectado e gravam seu código no setor de inicialização ou no *MBR (Master Boot Record)* do disco rígido. Outros comandos são interceptados com menos freqüência, do comando de *Reset* (comando para limpar, retornar a uma posição inicial) de Disco (AH=0) ao de leitura/gravação longa (AH=0Ah,0Bh).

Uma grande parte dos vírus de *boot* não efetua uma verificação se a memória do sistema contém "resíduos" de sua cópia *TSR* (Terminate and Stay Resident – programa residente em memória que pode ser acionado com o pressionar de algumas teclas), já instalada, eles empregam a técnica *Stealth* (reservada, para o caso dos vírus polimórficos), tornando impossível repetidas inicializações do vírus, ou se valem do fato de que o código do vírus é carregado uma vez durante a inicialização do *MS-DOS* e após esta etapa, não há como executar os códigos do setor de inicialização do disco. Alguns vírus verificam a presença de sua cópia e para esse fim, utilizam chamadas especiais da *INT 13h* com alguns valores não convencionais, ou marcam alguns bytes ociosos (ou palavra) na tabela de vetores de interrupção ou na área de sistema *BIOS* (0040:00??), porém existem alguma outras formas de se detectar a sua própria cópia *TSR*.

### 5.7.3 VÍRUS POLIMÓRFICOS

Segundo A Módulo Security Solutions (2) (2000), alguns vírus são chamados de polimórficos quando não podem (ou podem, mas com grande dificuldade) ser detectados com as chamadas máscaras de vírus, ou seja, partes do código específico do vírus não modificável. Isto é conseguido principalmente de duas maneiras: a primeira delas é por meio da criptografia do código principal do vírus com uma *chave* não-constante e com conjuntos aleatórios de comandos de descriptografia e a segunda maneira, é pela modificação do código executável do vírus, sendo que existem também outros exemplos um pouco exóticos de polimorfismo. O vírus do MS-DOS "Bomber" não é criptografado, mas a seqüência de instruções que passa o controle para o corpo do vírus é totalmente polimórfica. Segundo pesquisas, existem vírus polimórficos de todos os tipos, desde vírus do *MS-DOS* de arquivo e de *boot*, vírus de Microsoft Windows, e até mesmo vírus polimórfico de macro para o MS-Word. Existem descriptadores polimórficos e o exemplo mais simples de um descriptador parcialmente polimórfico é formado por um conjunto de instruções programáveis. Nem um único *byte* do vírus ou do seu descriptador permanece o mesmo ao infectar diferentes arquivos como resultado do uso desse código.

De acordo com pesquisas realizadas, os vírus polimórficos mais complicados utilizam *algoritmos* muito mais complexos para a geração do seu código descriptador e as instruções ou equivalentes passam de um arquivo infectado para outro, são diluídas com instruções que não produzem quaisquer modificações, como NOP, STI, CLI, STC, CLC, registros DEC não usados, registros XCHG não usados, etc..., porém, os vírus polimórficos de valor inteiro utilizam *algoritmos* ainda mais complicados, resultando em

numerosas instruções aleatórias, como SUB, ADD, XOR, ROR, ROL, em ordem e quantidade aleatórias no descriptador do vírus. Em relação ao carregamento e a modificação de *chaves*, bem como de outros parâmetros de criptografia, também são feitos pela construção de conjuntos aleatórios, que podem conter praticamente todas as instruções dos processadores Intel (Nome da empresa eletrônica que desenvolveu o projeto dos processadores para computadores padrão IBM / PC), (ADD, SUB, TEST, XOR, OR, SHR, SHL, ROR, MOV, XCHG, JNZ, PUSH, POP, etc.), com todos os modos de endereçamento possíveis.

Os vírus polimórficos se desenvolveram muito nos últimos anos e surgiram várias versões utilizando instruções do *Intel* 386 para descriptografar e, em 1997, foi encontrado um vírus polimórfico de 32 *bits* infectando arquivos EXE do MS-Windows95, sendo que, como resultado, no topo do arquivo infectado por um vírus semelhante, surgem um conjunto de instruções aparentemente sem sentido e, além disso, algumas combinações bastante viáveis não são desmontadas por produtos para depuração de algumas empresas (por exemplo, as combinações CS:CS ou CS:NOP). Às vezes, comandos como MOV, XOR, LOOP, JMP, aqueles que estão realmente funcionando, podem ser encontrados.

Níveis de polimorfismo: devido à complexidade e a proporção deste tipo de vírus, existe um sistema de divisão dos mesmos em níveis, ou seja, de acordo com a complexidade do código de seus descriptadores e este sistema foi criado pelo Dr. Alan Solomon e depois aperfeiçoado por Vesselin Bontchev.

Nível 1: é o nome dado ao grupo de vírus cujo conjunto de descriptadores têm um código constante, que escolhe um deles durante a infecção e são os chamados de "semipolimórficos" ou "oligomórficos". Exemplos: "Cheeba", "Slovakia", "Whale".

Nível 2: é o nome dado ao grupo de vírus cujo descriptador contém uma ou diversas instruções constantes, sendo que o restante pode ser modificado.

Nível 3: é o caso do descriptador que contém funções não utilizadas - "lixo" como NOP, CLI, STI, etc.

Nível 4: trata-se do descriptador que utiliza instruções intercambiáveis e modifica sua ordem (mistura de instruções), sendo que o *algoritmo* de descriptação permanece inalterado.

Nível 5: é o caso em que todas as técnicas anteriormente mencionadas são utilizadas e o *algoritmo* de descriptação é modificável, a criptografia repetida do código do vírus e mesmo a criptografia parcial do descriptador são possíveis.

Nível 6: são os vírus de permutação, sendo que o código principal do vírus está sujeito a mudanças. Ele é divido em blocos que são posicionados em ordem aleatória

durante a infecção e mesmo assim, o vírus continua a poder trabalhar, porém pode ser decriptografado. Trata-se de um dos mais perigosos vírus desta categoria.

Esta categoria e divisão ainda possui desvantagens, pois o principal critério é a possibilidade de detecção do vírus de acordo com o código do descriptador, com a ajuda da técnica convencional de máscaras de vírus:

Nível um: para se conseguir detectar o vírus basta ter diversas máscaras.

Nível dois: é a detecção do vírus com a ajuda da máscara utilizando "caracteres do tipo curinga".

Nível três: é a característica da detecção do vírus com a ajuda da máscara depois da exclusão de instruções "lixo".

Nível quatro: é o caso da máscara que contém diversas versões de código e se torna um *algoritmo* do nível cinco.

Nível cinco: é a característica da impossibilidade de detecção do vírus utilizando máscaras, pois a deficiências desta divisão é demonstrada em um vírus do terceiro nível de polimorfismo, o qual é chamado, adequadamente, de "Nível 3". De acordo com pesquisas executadas, este é um dos vírus polimórficos mais complicados, e se encaixa na terceira categoria, conforme a divisão atual, porque funciona como um *algoritmo* de decriptação constante, precedido por muitas instruções "lixo" e neste vírus, entretanto, o *algoritmo* de geração de "lixo" é trabalhado até a perfeição e no código do descriptador é possível encontrar praticamente todas as instruções i8086. Caso haja a necessidade de se dividir os vírus em níveis, conforme a teoria dos antivírus, utilizando os sistemas de decriptação automática do código do vírus (emuladores), esta divisão dependerá da complexidade do código do vírus. Existem muitas outras técnicas de detecção de vírus que são possíveis, por exemplo, a descriptação com a ajuda de leis primárias da matemática, desta maneira, a divisão poderia ser mais objetiva caso considerasse outros parâmetros além do critério da máscara do vírus, como por exemplo:

- O grau de complexidade do código polimórfico do vírus, ou seja, um percentual de todas as instruções do processador, que pode ser encontrado no código do descriptador.
- Análise do uso da técnica do antiemulador.
- Análise da constância do *algoritmo* de decriptação.

Verificação do tamanho do *algoritmo* de decriptação.

### 5.7.4 VERMES (*WORMS*)

Segundo Virus & Cia. (2001), os Vermes (*Worms*) são programas autônomos que se propagam, se ativam sozinhos nos sistemas infectados, e procuram outros sistemas na rede que estejam acessíveis. Também é um tipo de vírus de computador, que tem como principal característica a autoduplicação, não necessitam se anexar a outros programas e residem e se multiplicam em ambientes Multitarefa, sendo que têm a característica de explorar as facilidades para executar processos remotamente em sistemas distribuídos.

O uso permanente do antivírus é extremamente fundamental, ele pode ser instalado nas estações de trabalho do usuário, em um servidor ou em um servidor *Gateway* de *e-mail*, para que seja verificada cada mensagem que chegar, seus arquivos anexados e, quando encontrado um arquivo infectado, este arquivo pode ser limpo ou excluído, dependendo da configuração parametrizada. Recomenda-se que o antivírus seja instalado em ambos e configurado para excluir o arquivo infectado somente quando não for possível eliminá-lo. O fato de vários vírus serem criados diariamente faz com que o antivírus tenha de ser atualizado periodicamente, pois os vírus mais recentes, normalmente são mais perigosos, pois são criados com tecnologias novas e são mais fáceis de passar por sistemas de proteção desatualizados. As principais formas de propagação dos vírus são as conexões permanentes, computação móvel, disquetes trazidos de fora da empresa e o maior responsável pelas contaminações, o *e-mail*.

### 5.7.5 VERME (WORM) SIRCAM

Segundo Haical (2001), o Worm Sircam foi descoberto no dia 17 de Julho de 2001 e se apresentou com um altíssimo poder de disseminação, chegando a ser caracterizado como o vírus de maior incidência no Brasil, no México e na Argentina, países que foram considerados os mais atingidos

Além dos três países citados, o Sircam atingiu o *NIPC* (The National Infrastructure Protection Center), a organização de segurança na *Internet* ligada ao FBI, sendo que, na Quarta-feira, a máquina de um investigador foi atingida e, apesar de não ter se disseminado entre outros computadores do órgão, enviou automaticamente documentos oficiais para oito pessoas de fora do *NIPC*. Este *Worm* se dissemina pela rede anexado a mensagens de correio eletrônico, o *e-mails*, por meio do software Microsoft Outlook, onde seleciona uma palavra aleatoriamente para o campo "assunto" e adiciona um arquivo da máquina infectada ao à mensagem, expondo documentos pessoais ou sigilosos do usuário.

Realmente este vírus foi considerado pela crítica especializada como uma praga que também espalha por meio de programas de compartilhamento de rede, sendo que o arquivo anexado pode trazer as extensões .bat, .com, .exe ou .lnk.

Conforme a empresa Trend Micro, o Sircam possui seu próprio mecanismo de *SMTP (Simple Mail Transport Protocol)*, que é o protocolo utilizado na transferência de *e-mails* na *Internet* e se dissemina de modo semelhante ao Magistr.Worm. Como característica de identificação, recomenda-se observar o corpo da mensagem irá sempre conter os textos:

(Inglês)

Primeira frase: Hi! How are you?

Última frase: See you later. Thanks

(Espanhol)

Primeira frase: Hola como estas?

Última frase: Nos vemos pronto, gracias.

Entre as duas frases é escolhida uma das seguintes frases:

(Inglês)

I hope you like the file that I send you

I hope you can help me with this file that I send

This is the file with the information that you ask for

I send you this file in order to have your advice

(Espanhol)

Espero te guste este archivo que te mando

Espero me puedas ayudar con el archivo que te mando

Este es el archivo con la informacion que me pediste

Te mando este archivo para que me des tu punto de vista

Algumas recomendações são importantes para se proteger do Sircam:.

1 – Efetuar o download de arquivos de correção do Microsoft Outlook, fornecido pela Microsoft.

2 - Evitar abrir arquivos anexos sem ter a certeza da origem do mesmo e, apesar de se ter a certeza da origem, é importante ter cuidado e, antes de abrir qualquer arquivo anexado, confirmar com o remetente do que se trata. Recomenda-se ainda, efetuar uma varredura do arquivo como software antivírus. É importante também procurar manter sempre atualizado o antivírus do microcomputador.

3 – Deixar programado para o antivírus para efetuar uma varredura automática do sistema e se atualizar regularmente e automaticamente.

4 – Procurar se manter informado sobre as novas pragas de vírus existentes e atuando no mercado.

### 5.7.6 *TROJAN HORSE* (CAVALO DE TRÓIA)

Segundo Virus & Cia. (2001), a lenda do Cavalo de Tróia (em inglês *"Trojan Horse"*), diz que um grande cavalo de madeira foi presenteado pelos gregos aos troianos, como sinal de que estavam desistindo da guerra, porém o cavalo escondia no seu interior um grupo de soldados gregos, que esperaram a noite, abriram os portões da cidade de Tróia e o exército grego invadiu e dominou a cidade.

Desta maneira, o nome "*Trojan*" um programa que oculta o seu objetivo sob uma camuflagem de outro programa útil ou inofensivo, é um programa que informa que executa uma atividade (que pode fazer ou não), mas na realidade ele realmente executa outra ação, sendo que essa segunda ação pode danificar seriamente o computador. Por exemplo, o *Spoof Login*, que é um programa que se apresenta a usuários com *prompts* (marca de início de linha de comando em Sistemas Operacionais de computadores), que não são distinguíveis de *logins* regulares e diálogos de senhas, mas de fato armazena a entrada inocente do usuário em um arquivo conveniente para posterior uso ilícito.

Diferenças principais entre *TROJAN HORSE* e vírus

Os *Trojan Horse* não possuem instruções para auto-replicação.

São programas autônomos, ou seja, não necessitam infectar outras entidades (programas, setores de *boot* , por exemplo, para serem executados).

Em geral, são ativados por diversos tipos de gatilho, pelo próprio usuário (executando ou abrindo um "Trojan" no microcomputador, seqüências lógicas de eventos (bombas lógicas), ou por uma data ou período de tempo (bombas de tempo).

Não existe uma preocupação de auto-preservação, não objetivam a própria disseminação como os vírus.

Como não são feitos para se replicar, costumam permanecer indefinidamente no microcomputador ou se autodestruir junto com os dados que visa apagar ou corromper.

A sua propagação acontece especialmente por meio de canais de distribuição, como a *Internet*, onde são colocados e oferecidos como programas úteis. São assim, voluntariamente copiados por usuários diversos, enganados quanto aos reais efeitos do

programa. Entretanto, inicialmente, os *Trojans Horses* não se replicavam, mas em janeiro de 1999 surgiu um *Trojan* com capacidade de autodistribuição, o Happy99.

Como os *Trojans* não se limitam às características dos vírus, são potencialmente mais perigosos. Assim, arquivos .exe desconhecidos ou de origem duvidosa, mesmo que passem pelo antivírus, só podem ser executados com cuidado, de preferência em computadores devidamente com um *back-up* de segurança garantido e, se possível, em um computador utilizado para testes, cujo disco rígido não possua nada indispensável. Atualmente há uma grande preocupação com *Trojans*, pois vários *Backdoors* são cavalos de Tróia.

### 5.7.7 *BACKDOORS*

Segundo Virus & Cia. (2001), *Backdoors* são programas que instalam um ambiente de serviço em um computador, tornando-o acessível à distância, permitindo o controle remoto da máquina sem que o usuário tenha conhecimento de tal acontecimento. Desta maneira, o microcomputador poderá ser totalmente controlado à distância por um outro usuário, em outro microcomputador, possibilitando a este invasor executar qualquer atitude, ou seja, acessar os arquivos armazenados, ler *e-mails*, ver todas as senhas existentes, apagar ou trocar os nomes dos arquivos, executar *boot* na máquina, conectar-se via rede a outras máquinas as quais se tenha acesso, executar programas no computador, tais como jogos, capturar todas as teclas digitadas do teclado da máquina para um arquivo (comprometendo acessos a sites seguros - cartão de crédito, *homebanking* etc), e formatar o disco rígido do micro, etc. Dois famosos programas desse tipo são o Back Oriffice e o Netbus e, um grande problema é que a invasão de computadores atualmente não é ação apenas para *Hackers* (maníacos por informática, e também maníacos em entrar em sistemas alheios). Os *backdoors* são programas simples e pequenos que tornaram possível que qualquer pessoa não especializada possa invadir um computador sem dificuldade.

### 5.7.8 CORRENTES, HOAX E SPAM

Segundo Virus & Cia. (2001), as CORRENTES são um tipo de correspondência em que se envia a mesma mensagem para muitas pessoas, semelhante a uma mala direta, e é facilmente identificável. Funciona como uma isca, como objetivo de fazer com que o usuário leia a mensagem até o final.

Às vezes se apresenta como uma ameaça para assustar e penalizar o leitor, outras vezes há uma citação de apoio a uma causa social solicitando que inclua seu endereço

de *e-mail* e retransmita a mensagem para outros usuários, etc. Às vezes tem um pedido para que o leitor retransmita a mensagem (inútil) para um certo número de pessoas, ou para quantas forem possíveis.

Em resumo, uma corrente é uma correspondência em que se envia a mesma mensagem para vários usuários, como malas diretas, pirâmides de enriquecimento fácil e abaixo-assinados. Toda a mensagem ou *e-mail* que tiver o padrão citado acima se trata de uma corrente. O problema mais sério com as correntes, é que se perde tempo e paciência, sendo que um fator agravante da situação, é que o *e-mail* que recebeu a mensagem, automaticamente foi incluído em alguma mala direta eletrônica e sem a devida autorização, sendo que o usuário destinatário é quem tem os maiores prejuízos, pois é responsável pelos custos do tempo de uso do acesso à *Internet* e da conta telefônica para receber lixo ou propaganda e publicidade não solicitada.

Em se tratando de *Internet*, objetivo principal das correntes é o de provocar um congestionamento do tráfego de dados e mensagens em trânsito nos servidores de correio eletrônico e nas redes de comunicação de dados das organizações. Os usuários reproduzem a mensagem com o intuito de estarem fazendo uma ação benéfica, enquanto que na verdade, estão prejudicando o sistema, independentemente da procedência e dos objetivos, sejam eles humanitários, de protesto ou de apoio e o que realmente acontece de prático é o prejuízo para os usuários de microcomputadores e das organizações do mundo todo, pois o envio indiscriminado de centenas e até milhares de mensagens gera um imenso volume de dados em trânsito, inútil e desnecessário na *Internet* e demonstra a desinformação dos *Internautas* (nome dado ao usuário da *Internet*).

A atividade de se redistribuir mensagens de correntes somente contribuem para multiplicar geometricamente este tráfego e, em conseqüência, o tempo de resposta dos servidores é cada vez mais lento, sendo que há perda de tempo útil, produtividade e degradação do tempo de resposta do ambiente de correio eletrônico e da comunicação entre as redes.

No caso do *SPAM*, trata-se do ato de se enviar mensagens não solicitadas a muitos usuários destinatários com um conteúdo comercial. Um caso de exemplo característico foi o do Spam enviado pela CyberPromotions à AOL, onde 1,8 milhão de mensagens diárias estavam sendo enviadas até o final de um processo judicial. Tendo em vista que um usuário da AOL demore cinco segundos para identificar e descartar a mensagem, foram desperdiçadas cinco mil horas de conexão por dia, apenas neste caso e o *Spammer* (usuário responsável pelo envio de uma mensagem *Spam*),não teve um custo de R$ 100,00 por dia para enviar a mensagem. Uma das versões mais reais sobre

o *Spam*, é que é um vírus social, que se utiliza da boa fé e boa vontade das pessoas para se reproduzir e atingir os seus objetivos. A legislação brasileira está trabalhando para regulamentar leis que irão regulamentar o uso do correio eletrônico, principalmente no que tange ao envio de propaganda comercial indiscriminadamente por parte de empresas. Um exemplo é sobre a possibilidade do usuário efetuar uma solicitação para sua exclusão da lista de receptores do *e-mail*, havendo a citação de frase no final das mensagens com os dizeres semelhantes a: "Esta mensagem é enviada em acordo à nova legislação sobre o correio eletrônico, Seção 301, Parágrafo (2), Decreto S.1618, Título Terceiro aprovado pelo "105 Congresso Base das Normativas Internacionais Sobre o SPAM". Este *e-mail* não poderá ser considerado um Spam quando inclua uma forma de ser removido. Caso não queira receber este *e-mail* outras vezes, gentileza responder-nos como título "REMOVER" e será excluído da lista de correspondência imediatamente".

*HOAX* é o nome dado à mensagem que tem um conteúdo "alarmante", como por exemplo, o alarme de ataque de um vírus perigoso que tenha sido detectado. Normalmente estas mensagens informam que não se deve abrir um determinado arquivo de correio eletrônico que possua alguma determinação de assunto como "Good Times", "Join The Crew", "Penpal Greetings" e "Win a Holiday" ou caso não obedeça, seu microcomputador será contaminado por vírus, ou o disco rígido será formatado e etc...

Em resumo, um Spam é uma mensagem não solicitada, como uma propaganda publicitária normal, enquanto que o Hoax também é uma mensagem que conta estórias falsas como a infecção por vírus.

### 5.7.9 ANTIVÍRUS

Segundo Virus & Cia. (2001), os *softwares* antivírus são os responsáveis por verificar a existência de vírus em um computador, disco rígido, pastas ou diretórios, arquivos e, quando da detecção de um vírus, este programa inicia uma operação de eliminação do vírus ou exclusão do arquivo contaminado, conforme configurações prévias executadas pelo usuário ou Administrador da rede. Normalmente os *softwares* antivírus analisam o "comportamento" dos programas que estejam residentes na memória do microcomputador com o objetivo de detectar uma ação de vírus. Dentre as várias formas de manifestação dos vírus, por exemplo, caso algum destes programas esteja iniciando uma ação de tentativa de mudar o nome, aumentar de tamanho ou transferir algum arquivo de uma área gravada para outra, estas são típicas características de ação virótica, que o *software* antivírus detecta e inicia sua ação de proteção. Após a instalação do antivírus em um computador, inicia-se o processo de otimização do mesmo,

ou seja, passa-se a uma configuração mais refinada onde serão informadas as ações que o antivírus deverão desencadear automaticamente para os casos de encontrar arquivos contaminados. É nesta fase, também que, dependendo do antivírus, o mesmo poderá ser configurado para estar sempre ativo analisando todos os arquivos que forem abertos no computador, ou que cheguem via *e-mail* e, caso surja algum vírus, será efetuada uma ação imediata de proteção. Em todos os momentos surgem novos tipos de vírus, novas versões de vírus antigos, sendo assim, é necessário uma constante atualização da lista de vírus existente no antivírus instalado no computador de trabalho do usuário final, como também nos servidores da rede.

## 5.8 PRIVACIDADE E MONITORAMENTO DO CORREIO ELETRÔNICO

O correio eletrônico é formado por um sistema cuja função é prover a funcionalidade de se redigir uma mensagem, anexar ou não um arquivo e encaminhá-la para um outro destinatário interno ou externo à empresa. Existem correios eletrônicos profissionais e com excelentes recursos, como o *Lotus Notes*, da *IBM*, e o Microsoft Exchange, da Microsoft. Os serviços de segurança necessários para o correio eletrônico na *Internet* deverão incluir confidencialidade e integridade em transmissões sem conexão, autenticação da origem das mensagens e impedimento da rejeição pelo destinatário ou remetente. O protocolo *PEM* foi elaborado para fornecer estes serviços ao *SMTP*.

Este recurso da Informática, o correio eletrônico, provê uma fragilidade às redes, que é a possibilidade de grande congestionamento de mensagens trafegando pelas linhas de comunicação e o recebimento de arquivos contaminados com vírus de computador. O correio eletrônico é uma das maiores fontes destes vírus de computador em trânsito, pois os arquivos contaminados são recebidos pelos usuários vindos de várias origens, com grandes possibilidades de contaminação e são enviados a mais outros usuários da rede disseminando uma contaminação generalizada.

A privacidade do uso de informação também inclui questões de utilização de recursos da organização, gerenciamento de pessoal e de responsabilidade profissional. Quando esses pontos estão bem definidos para todos, é mais fácil e efetivo tratar a questão da privacidade do usuário e da segurança da informação da empresa. Uma não deve ser inimiga da outra, principalmente no que tange aos dados contidos e recebidos por correio eletrônico. Segundo Oliveira (2001), todos os provedores da *Internet* são capazes de ler as correspondências eletrônicas de seus usuários, sendo que as caixas postais ficam à disposição dos Administradores dos servidores. Existe uma ética

profissional, no entanto, que dita a regra de que os provedores jamais devem acessar as caixas postais dos seus usuários sem o consentimento dos mesmos.

O serviço de monitoramento consiste em se estar constantemente analisando o tráfego de mensagens no segmento da rede, verificando as mensagens de alerta referente a possíveis falhas dos sistemas ou tentativa de invasão por intrusos e usuários não autorizados, internos ou externos. O monitoramento tem o objetivo de se antecipar aos problemas com o intuito de evitá-los, mesmo antes que ocorram, e de manter um controle da rede em caráter preventivo. Todo endereço de correio eletrônico necessita ser configurado segundo normas e padrões de denominação característico e próprio. Existe a necessidade de se ter um *DNS*, onde é feita esta padronização de nomes.

Até este ponto do trabalho foram analisados vários aspectos relacionados à segurança da informação, à segurança nas redes de computadores e no correio eletrônico. No capítulo seguinte serão apresentados os critérios relativos àMetodologia a ser empregada no desenvolvimento do estudo de Caso, foco desta pesquisa.

## 5.9 A PROTEÇÃO DAS INFORMAÇÕES NAS ORGANIZAÇÕES

Segundo a Módulo Security Solutions (1) (2000), os altos índices de informatização, conectividade, negócios pela *Internet* e compartilhamento de dados tornaram a informação um dos bens mais valiosos e mais vulneráveis das empresas. Com isso, incidentes nas redes de computadores passaram a afetar diretamente os resultados do negócio e o valor das empresas. Além da projeção que a segurança das informações obteve no mercado global, o tema alcançou as mais altas e estratégicas camadas das organizações, chegando ao diretor de informática, ao presidente da organização aos acionistas. Seis em cada dez executivos entrevistados acreditam que os problemas de segurança irão aumentar em 2001; 94% reconhecem a grande importância da proteção dos dados para o ambiente corporativo, sendo que 56% consideram vital.

Em uma pesquisa executada pela empresa Módulo Security Solutions no ano de 1999, os vírus respondem por 75% das maiores ameaças àsegurança da informação nas empresas. Apesar de 93% das corporações afirmarem já terem adotado sistemas de prevenção contra vírus, 48% sofreram contaminação nos últimos seis meses e apenas 11% das empresas entrevistadas declararam nunca ter sido infectadas.

Segundo leite (2002), os vírus da categoria Cavalos de Tróia são os que mais provocam problemas. Eles são capazes de tirar do ar o sistema de correio eletrônico e até as redes internas, estão sendo distribuídos globalmente numa velocidade avassaladora. Os fornecedores de sistemas antivírus não conseguem evitar muitos dos novos vírus, por demandarem certo espaço de tempo para a disseminação das

necessárias vacinas eletrônicas. E é um fato que o *e-mail* vem se tornando o maior veículo para disseminação de vírus e instalação de Cavalos de Tróia.

Segundo Plachta (2001), diferentemente do que se pensava no passado sobre a definição de Continuidade de Negócio Empresarial, quando o conceito estava associado à sobrevivência das empresas –- principalmente por meio das suas estratégias comerciais, redução de custos com produtividade e fortalecimento da marca, da patente –-, observa-se nos dias atuais uma mudança que cria um novo conceito associado a um modelo de gestão mais abrangente, diversificado e apoiado pelo tecnicismo da Tecnologia da Informação, onde todos os componentes e processos essenciais ao negócio tenham os seus riscos de inoperância ou paralisação minimizados por Planos de Continuidade de Negócios atualizados, documentados e divulgados corretamente. Conforme pesquisa efetuada pela empresa Módulo Security Solutions (1) (2001), das 165 empresas pesquisadas no ano de 2001, 31% delas têm um Plano de Continuidade do Negócio em Casos de Ataques ou Invasões de seus servidores de dados, 46% das empresa não têm um plano específico ou colocado em prática e 23% sequer souberam responder se existe uma ação formalizada na empresa para esta eventualidade crítica, conforme Figura 23 abaixo:

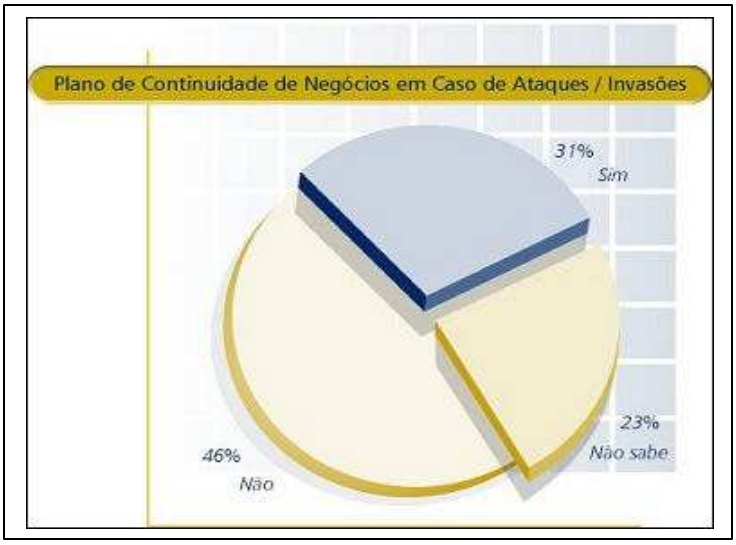



Figura 23 – Plano de Continuidade de Negócios em Caso de Ataques/Invasão

Fonte: Módulo Security Solutions (1). (2001).

Na época em que o antigo conceito era usado, todas as preocupações referentes à inoperabilidade dos componentes (sejam estes de suporte à tecnologia ou aos processos), eram analisadas isoladamente por cada gestor ou técnico responsável que, como não possuíam uma visualização –- a nível macro e necessária –- de todas as

interdependências existentes, não orientavam a implementação às atividades fins da empresa. Seria necessário então criar uma solução onde todas as áreas pudessem ter uma visão global dos seus inter-relacionamentos e, com isto, seria possível definir critérios referentes ao custo de recuperação, de inoperância ou de impacto refletidos na atividade fim da empresa.

Quando se iniciava a procura ou enumeravam-se os grandes vilões responsáveis pela indisponibilidade e o caos nas empresas, pensava-se em furtos, explosões, desastres como as ameaças naturais, terremotos, inundações e outros similares. Porém, estes fatores perderam terreno para as vulnerabilidades herdadas pelas empresas em decorrência do aumento desenfreado, e necessário, das novas tecnologias, principalmente relacionadas à Tecnologia da Informação. Com isso, o conceito de desastre, antes atrelado ao caos gerado por fatores naturais, vem sendo substituído pelo conceito de evento, que é a concretização de uma ameaça previamente identificada, podendo ser seguido ou não de um desastre.

Um exemplo clássico e ativo nas organizações atualmente é o recebimento de um vírus por um usuário de *e-mail.* Este fato identifica-se como um evento até que o programa seja executado, resultando na perda de dados, caso não seja tomado uma ação imediata de proteção, o vírus poderá se disseminar para todos os microcomputadores e servidores da rede da empresa, o que seria um desastre, considerando o valor das informações atingidas.

Nos dias de hoje, após os atentados nos Estados Unidos, intensifica-se um conceito de estado de alerta para o Plano de Continuidade de Negócios denominado Plano de Administração de Crise onde, segundo a British Standard 7799–1 (1999), todas as medidas para o estado de vigilância e ações de resposta emergenciais devem estar documentadas e destinadas às equipes de plantão responsáveis pela sua execução. Por meio destas medidas, observa-se cada vez mais que a continuidade dos processos e negócios está atrelada não somente à recuperação ou à contingência dos processos vitais, mas também à vigilância contínua dos eventos. Desta maneira, quando é possível a identificação imediata da probabilidade da ocorrência de um evento que ocasionará a indisponibilidade de um processo crítico ou vital, este deverá ser tratado como uma situação de crise, aplicando-se o plano de controle e administração para a redução do risco desta ocorrência.

Segundo Gonçalves (2001), conforme pesquisas atuais, são inúmeras as possibilidades de lucro ou, ao menos, de grande redução nas despesas das empresas que entendem e aplicam a Internet de modo adequado aos seus negócios e à sua estrutura. Baseando-se neste raciocínio inicial, não se pensa apenas no comércio

eletrônico, mas sim na integração interna da empresa por meio de seus computadores, a *Intranet*, com as outras empresas e pessoas fora de sua e estrutura física, a *Internet*. As oportunidades de negócios, de comercialização de produtos e as possibilidades de sucesso são muitas, porém as vulnerabilidades relacionadas àTecnologia da Informação aumentam na mesma proporção ou maior. O número de empresa que têm redes de computadores, comércio eletrônico ligado à *Internet* e funcionários o tempo todo acessando vários *Sites* pelo mundo todo –- mesmo a trabalho –-, na maioria das vezes não estão preparados para enfrentar este problema.

Atualmente, para que as organizações consigam manter sua competitividade e liderança em seu ramo de atividade, a informação é a mais valiosa das ferramentas que pode possuir, isto é indiscutível. Sendo assim, se não houver uma proteção para estas informações nestas empresas, cedo ou tarde, haverá um prejuízo, seja ele moral ou material, pequeno ou de imensas proporções. Conforme recente pesquisa da empresa Módulo Security Solutions (1) (2001), executada com 165 empresas de grande porte (18% das quais com mais de 5.000 terminais), revelou que 40% delas já sofreu invasão em seus sistemas, enquanto 31% não souberam dizer se foram alvo de ataque aos seus dados e 29% negaram qualquer tipo de ocorrência. Estes números, embora assustadores, podem ser ainda maiores, uma vez que as empresas não têm interesse em assumir este tipo de violação aos seus dados. Cerca de 8% das companhias pesquisadas calcularam seus prejuízos entre quinhentos mil e um milhão de reais.

Uma análise nos dados divulgados revela um quadro que, embora bastante conhecido, continua a ser desconsiderado pela grande maioria dos empresários: mais da metade dos ataques aos sistemas ocorrem dentro das próprias empresas e são praticados por empregados insatisfeitos ou simplesmente infiéis. Os usuários mais perigosos são os denominados e tão temidos *Hackers*, responsáveis por pouco mais de um terço das ocorrências e outros 18% delas foram fruto de espionagem industrial. Se coibir a espionagem industrial e os *hackers* parece um trabalho árduo e muito longo, a criação de Políticas de Segurança da Informação pode eliminar mais da metade das ameaças, pois mesmo os *Hackers* se utilizam, em geral, de uma falha interna dos sistemas computacionais das empresas para agir.

O aspecto técnico de uma Política de Segurança da Informação empresarial, entretanto, não pode ser implementada de modo eficaz sem um acompanhamento de medidas jurídicas capazes de garantir a efetividade dos resultados. Os limites da proteção serão medidos pela interação destas duas variáveis. Não haverá qualquer bom aproveitamento e produtividade com apenas a colocação de equipamentos modernos se os funcionários puderem acessar os dados de modo indiscriminado, por exemplo. O

problema existe, é atuante e necessita de ação imediata, pois há pouco tempo, uma empresa instalada em São Paulo descobriu que dados e até projetos seus estavam sendo indevidamente enviados para fora das suas dependências por um funcionário que, simplesmente, todos os dias enviava (via *e-mail*), arquivos com até 10Mb de dados da empresa para sua residência por meio de uma conta de *e-mail* particular e pessoal. Este problema, aparentemente simples, ocorre diariamente na maioria das empresas e escritórios comerciais no mundo inteiro e conduz à reflexão, à busca de alternativas de coibição e busca por uma saída técnica, a filtragem de *e-mails*, que é viável e uma outra opção que é a jurídica. Quando se passa para a área Jurídica, esbarra-se em outro fator que é o de responder à pergunta: Pode-se barrar ou monitorar os *e-mails* dos funcionários de uma organização? O assunto é bastante polêmico e merece considerações extensas. Porém, em síntese, diversos países do mundo já aplicam este tipo de controle nas empresas e 54% dos norte-americanos o aceitam como justo, havendo até um projeto específico sobre o tema, o "Notice of Eletronic Monitoring Act". No Brasil, não há nada específico sobre este tema, nem na lei atual nem em projetos, como o dos EUA. Cerca de 83% das empresas usam o *e-mail* como ferramenta de seus negócios e o tráfego na rede é estimado em mais de 10 bilhões de mensagens diárias.

Devido a estes números, vê-se que monitorar as mensagens de modo manual não é uma opção nem possível, seja pelo volume de trabalho, seja pela invasão na privacidade dos empregados e outros fatores diversos adicionais. Neste caso específico, o problema é resolvido no campo técnico da área de Tecnologia da Informação pela criação de um filtro, via *software*, que é instalado no servidor do correio eletrônico principal das caixas postais dos usuários, impedindo uso de contas particulares nos servidores da empresa, regulando o tamanho máximo dos *e-mails* que saem e chegam e identificando somente os arquivos anexados que podem trafegar pela rede ou correio eletrônico. Este tipo de *software* tem a característica de identificar ainda, se for o caso, mensagens que contenham frases, termos ou expressões consideradas estratégicas pela empresa. No campo jurídico, deve-se criar um termo específico sobre os limites para o uso do *e-mail* da empresa, incluindo um compromisso de confidencialidade sobre os assuntos internos e deixando claro que as mensagens serão monitoradas tecnicamente. Além disso, por se tratar de *e-mail* profissional e pertencente à organização, o nome do usuário e senha devem ser providos pela empresa, afastando o caráter de privacidade da conta, que deve ser usada apenas para assuntos de trabalho, sendo um canal da empresa e não do empregado.

Segundo Pereira (2001), a segurança sempre foi tratada como uma ferramenta para proteção das informações nas empresas, porém existe uma grande dúvida sobre se

ao serem implementadas as configurações de segurança nos ativos se realmente a organização está protegida. Alguns pesquisadores ao analisar o assunto, tendem a vincular a configuração de determinada ferramenta, *software* ou *hardware* da topologia de sua rede como uma segurança implantada. Pode-se dizer que existe fundamento verdadeiro nesta observação. Realmente houve um passo em direção à implantação da segurança da informação, mas para que uma segurança seja realmente efetiva em uma organização, são necessárias a avaliação e a determinação de medidas de segurança que passem pela tecnologia, processos e pessoas. Somente a tecnologia não garante a segurança das informações de uma organização. O *firewall* é um bom exemplo, ou seja, ao se contratar uma empresa especializada em instalar e configurar, da melhor maneira possível, um *firewall,* no parque tecnológico de uma organização, não é possível garantir a segurança desta organização, visto que, após a saída da empresa contratada, a empresa poderá não possuir a capacitação técnica necessária para dar continuidade ao processo de configuração durante uma mudança desta ferramenta adotada. Até mesmo uma mudança tecnológica do parque disponibilizado nesta rede que poderá carecer de uma mudança na configuração deste *firewall* instalado. A empresa poderia contratar um especialista nesta ferramenta como objetivo de amenizar os problemas, visto que haveria sempre alguém disponível e com a responsabilidade para efetuar as atualizações de software do *firewall* necessárias para o pleno funcionamento de suas funções de proteção.

Esta atitude, porém não é suficiente. Ao se adquirir uma determinada ferramenta para qualquer área de uma organização, é necessário provar em números, que esta compra trará retorno para a empresa e que o benefício é mensurável, pois só assim os gestores desta organização poderão acreditar no investimento realizado. É necessário sempre manter atualizada a documentação, além dos processos estarem bem definidos para que não haja retrabalho, erro ou omissões.

Quanto às pessoas, os usuários que trabalham na empresa, quando se implanta determinada medida de segurança, geralmente sofre-se um pouco com a reatividade ou resistência às mudanças implementadas por parte dos usuários, sendo que a fase de transição e implementação é a mais crítica e trabalhosa. Para se minimizar este problema, o importante é sempre vincular uma nova implementação no tratamento das pessoas, abrindo espaços para que possam tirar suas dúvidas, falar de seus anseios, além de obter as informações necessárias sobre a nova mudança. Todos estes fatores podem ser um tanto complicados, mas a implantação de uma Política de Segurança da informação é muito mais do que uma simples implementação de ferramentas e configurações. Na verdade, é necessário a existência de um controle do parque

tecnológico disponibilizado, tanto internamente quanto externamente. Internamente, quando se está monitorando os *logs*, verifica-se se "as máquinas estão com o coração batendo", se não há riscos de danos físicos aos equipamentos, dentre outros. Externamente quando se está acompanhando a mudança tecnológica, novas atualizações dos *softwares*, novas vulnerabilidades que estão sendo exploradas por pesquisadores e fabricantes em geral e tudo isto é controle.

É preciso possuir também o controle da gestão do negócio, definição dos processos e investimento nos colaboradores, pois é necessário justificar aos diretores, gerentes e superiores em geral os gastos realizados. Para tanto, apresenta-se números, índices e indicadores de segurança para fazer com que estes líderes sintam no "bolso" da organização o problema da disponibilidade, integridade e confidencialidade de uma informação que torna o negócio competitivo, ativo e, muitas vezes, líder do mercado no seu ramo de atividade.

A palavra Controle, de acordo com o dicionário Aurélio, é: "ato ou poder de controlar, domínio, governo, fiscalização exercida sobre as atividades de pessoas, órgãos departamentos ou sob produto, para que tais atividades ou produtos não se desviem das normas pré-estabelecidas". Portanto, hoje a segurança da informação está com o foco nos controles, pois as tecnologias mudam, e com estas mudanças os processos poderão passar por algumas alterações, devendo, assim, existir incentivo e orçamento previsto para investir nas pessoas que irão manipular e realizar os processos.

Realmente não existe uma fórmula mágica que possa indicar 100% de segurança e, por isto, é sempre necessário o controle, entendendo controle como gestão da segurança, para que se tenha um mínimo da proteção implantada.

Segundo a empresa Módulo Security Solutions (2) (2001), os ataques a servidores da *Internet* dobraram no ano de 2001 quando comparados ao ano de 2000, (de 24 para 48%) e cerca de 90% das empresas americanas foram infectadas por vírus no de 2001. É o que revelou uma pesquisa pela revista Information Security, em Julho e Agosto/2001, com 2,5 mil funcionários da área de segurança de companhias dos EUA.

Os incidentes internos ocorreram com maior freqüência em 2001, segundo o relatório. Em 78% das organizações, os empregados instalaram programas sem autorização e 60% utilizaram os computadores do trabalho para fins ilegais. Além disso, 22% enfrentaram problemas com roubo de dados ou sabotagem realizada por funcionários, sendo que 9% disseram que os empregados estiveram envolvidos em fraudes. Códigos maliciosos, privacidade, questões de confidencialidade e proteção contra *exploits* (ferramentas de ataques automáticos e métodos de explorar vulnerabilidades não corrigidas), encabeçaram a lista das maiores preocupações para o

final do ano de 2001 e início de 2002. Para combater os problemas, as empresas estão analisando a possibilidade de se contratar serviços e tecnologias relacionadas à criptografia, *Wireless* e *ESM* (Enterprise Security Management) em 2002.

Apesar das descobertas de ameaças internas, a prioridade número um dos profissionais de segurança é proteger as redes contra invasões externas, garantindo a disponibilidade dos *Sites*. Entre os obstáculos para a implementação de uma segurança forte, estão a falta ou o baixo orçamento destinado à área, a ausência de treinamento dos funcionários e a dificuldade em encontrar profissionais competentes.

Segundo a empresa Módulo Security Solutions (3) (2001), as principais empresas de antivírus efetuaram uma divulgação de alertas sobre um novo vírus com grande poder de disseminação, trata-se do Scherzo, também conhecido como Sheer, um vírus que surgiu na Itália e ataca computadores apenas com a leitura da mensagem de *e-mail*. Ou seja, não é preciso abrir o arquivo anexado para que o vírus entre em ação. Esta praga virtual explora uma vulnerabilidade de algumas versões do Internet Explorer e segundo a MessageLabs, empresa que monitora o tráfego de *e-mails* para várias outras empresas, mais de 6,5 mil mensagens com vírus já foram identificadas em 92 países.

Conforme nota da empresa Americana McAfee, este vírus utiliza um site (http://banners.interfree.it), para efetuar o *download* das informações que serão utilizadas no *e-mail* que será enviado automaticamente pelo computador infectado, como o assunto e o corpo da mensagem. Deste modo, permite ao seu criador alterá-lo, acrescentando novas funções. Geralmente, ele chega com a seguinte mensagem abaixo, em italiano, que cita sobre uma corrente de sorte, inicialmente deixando a impressão de ser apenas mais uma mensagem na rede para gerar tráfego nos servidores. Segue o trecho na íntegra da mensagem:

*"Con questa mail ti e stata spedita la FortUna; non la fortuna e basta, e neanche la Fortuna con la F maiuscola, ma addirittura la FortUna con la F e la U maiuscole. Qui non badiamo a spese. Da oggi avrai buona fortuna, ma solo ed esclusivamente se ti liberi di questa mail e la spedisci a tutti quelli che conosci. Se lo farai potrai: - produrti in prestazioni sessuali degne di King Kong per il resto della tua vita - beccherai sempre il verde o al massimo il giallo ai semafori - catturerai tutti e centocinquantuno i Pokemon incluso l'elusivo Mew - (per lui) quando andrai a pescare, invece della solita trota tirerai su una sirena tettona nata per sbaglio con gambe umane - (per lei) lui sara talmente innamorato di te che ti come una sirena tettona nata per sbaglio con le gambe Se invece non mandi questa mail a tutta la tua list entro quaranta secondi,allora la tua esistenza diventera una grottesca sequela di eventi tragicomici, una colossale barzelletta che suscitera il riso del resto del pianeta, e ticondurra ad una morte orribile, precoce e solitaria... No, dai, ho esagerato: hai sessanta secondi. Cascaci: e' tutto vero. Puddu Polipu, un grossista di aurore boreali cagliaritano, spedi' questa mail a tutta la sua lista ed il giorno dopo vinse il Potere Temporale della Chiesa alla lotteria della parrocchia. Ciccillo Pizzapasta, un cosmonauta campano che soffriva di calcoli, si preoccupo di diffondere questa mail: quando fu operato si scopri' che i suoi calcoli erano in realta diamanti grezzi.*

*GianMarco Minaccia, un domatore d fiumi del Molise che non aveva fatto circolare questa mail, perse entrambe le mani in un incidente subito dopo aver comprato un paio di guanti. Erode Scannabelve, un pediatra mannaro di Trieste,non spedi a nessuno questa mail: dei suoi tre figli uno comincio a drogarsi, il secondo entro in Forza Italia e il terzo si iscrisse a Ingegneria".* Módulo Security Solutions (3) (2001).

Esta mensagem apresenta anexado o arquivo Javascript.exe, que até então, não foi identificado alguma carga destrutiva, porém, ele pode ser alterado remotamente pelo *Hacker*, além de contribuir para o congestionamento dos servidores de *e-mail*. Para minimizar os problemas da vulnerabilidade utilizada pelo invasor, o *internauta* deve instalar um arquivo oferecido pela Microsoft para o Internet Explorer, como também um bom programa de antivírus.

### 5.9.1 EQUACIONANDO A GESTÃO DOS RISCOS DA INFORMAÇÃO

Segundo Sêmola (2001), não é tarefa fácil encontrar uma resposta padrão que equacione e solucione definitivamente o problema da gestão dos riscos da informação, pois segurança total inexiste. Atualmente, as organizações não têm conseguido fugir das premissas há muito validadas, que hoje sustentam –- com sucesso –- as iniciativas corporativas de segurança da informação. Sabe-se que cada tipo de negócio, independentemente de seu segmento de mercado, possui dezenas, talvez centenas de variáveis que se relacionam direta e indiretamente com a definição do seu nível de segurança mais adequado.

Identificar estas variáveis passa a ser a primeira etapa do desafio e, adotando-se analogicamente o exemplo do médico, a empresa deve passar por uma análise contextualizada antes que se possa especificar um tratamento medicamentoso com a finalidade de solucionar sua enfermidade. É justamente a fase do diagnóstico que será capaz de identificar as ameaças internas e externas, as vulnerabilidades físicas, tecnológicas, humanas, e os possíveis impactos financeiros, operacionais e morais. Baseado na análise anterior é possível esboçar a equação abaixo:

**Risco = Ameaças x Vulnerabilidades x Impactos**.

É possível de se executar uma breve análise de cada termo que compõe a fórmula citada, antes de se voltar a discutir o desafio da segurança agora equacionado.

Ameaça: é a atitude ou dispositivo com potencialidade para explorar e provocar danos à segurança da informação, atingindo seus conceitos: Confidencialidade, Integridade e Disponibilidade. Consultando a definição no dicionário, encontra-se: "Ameaça: palavra, gesto ou sinal indicativo do mau que se quer fazer a alguém; prenúncio de um mau ou doença; advertência". Exemplos: concorrente, sabotador, especulador, *Hacker*, erro humano (exclusão de arquivos digitais acidentalmente, etc.),

acidentes naturais (inundação, etc.), funcionário insatisfeito, técnicas (engenharia social, etc.), ferramentas de *software* (vírus, *Trojan Horse*, etc.).

O fato de se identificar as ameaças é fator crítico de sucesso para a correta dimensão do risco e principalmente para a modelagem de uma solução de segurança corporativa personalizada, sendo que, é difícil se defender de algo que não se conhece.

Vulnerabilidade: evidência ou fragilidade que eleva o grau de exposição dos ativos que sustentam o negócio (infra-estrutura física, tecnologia, aplicações, pessoas e a própria informação), aumentando a probabilidade de sucesso pela investida de uma ameaça. Verificando o termo em dicionário, encontraremos: "Vulnerabilidade: qualidade de vulnerável. Vulnerável: que, ou por onde, pode ser ferido; diz-se do ponto fraco de uma pessoa, coisa ou questão". Exemplos: falhas de infra-estrutura física (carência de mecanismos de controle de acesso físico na sala dos servidores, etc.), falhas tecnológicas (configuração inadequada do *firewall*, erros em projeto de software básico, sistemas operacionais, etc.), falhas de meios de armazenamento da informação (fitas de *back-up* impróprias para restauração por deterioração, etc.); falhas humanas (ausência de conscientização provocando displicência ao criar e manter em sigilo a senha pessoal, etc.).

Impacto: resultado da ação bem sucedida de uma ameaça ao explorar as vulnerabilidades de um ativo, atingindo assim um ou mais conceitos da segurança da informação. Em mais uma consulta ao dicionário, encontra-se que impacto é um choque; embate; encontrão; colisão entre dois corpos, com a existência de forças relativamente grandes durante um intervalo de tempo muito pequeno; abalo moral por um acontecimento doloroso ou chocante; impressão profunda provocada por ocorrência grave ou inesperada". Exemplos: prejuízo financeiro, perda de competitividade, perda de mercado, danos à imagem, depreciação da marca, descontinuidade, etc.

Neste ponto tem-se equacionado o risco com a identificação das variáveis citadas. É preciso ratificar que a gestão corporativa da segurança da informação deve estar sempre orientada a considerar as particularidades de cada negócio, em busca da implementação de controles que reduzam os riscos — fazendo-o tender a zero — e da eliminação e administração das vulnerabilidades dos ativos, evitando-se assim que as ameaças as explorem gerando impactos e comprometendo o negócio.

A análise de risco está intimamente relacionada à segurança de redes de dados corporativas. Ela visa detectar agressões e falhas, identificar e priorizar valores, identificar vulnerabilidades, ameaças e suas probabilidades, suas contra-medidas ou respostas, e planejar políticas e procedimentos de segurança. Os itens política e procedimentos de segurança visam políticas gerais, com foco nas necessidades e o

porquê destas necessidades e procedimentos detalhados e específicos enfatizando quem, quando e como algo pode ser previsto ou solucionado.

Diante do suposto acima, antes mesmo de se traçar a estratégia de segurança e os planos de ação, é importante se dedicar um bom tempo para analisar o contexto em que a empresa está operando, identificar as variáveis internas e externas, os aspectos físicos, os tecnológicos e humanos e sua sensibilidade diante de possíveis impactos, para que a partir desta análise possa, então, iniciar a modelagem de uma solução corporativa de segurança da informação sob medida, eficiente e capaz de proporcionar o melhor retorno sobre o investimento.

### 5.9.2 PANORAMA ATUAL SOBRE A SEGURANÇA NAS EMPRESAS

A segurança da informação e a proteção contra vírus de computador estão presentes em todas as organizações e a cada novo dia mais preocupantes.

Segundo Sêmola (2002), o investimento será uma palavra de grande atuação para o ano de 2002. A segurança deixará de ser vista como uma despesa dentro das empresas, que sempre a trataram com poucas chances de ser justificada, e passará a ser viabilizada por análises e estudos do *ROI* (Retorno sobre o Investimento), que serão considerados e valorizados pelos sócios, investidores e pelo próprio mercado, provocando reflexos no fortalecimento da imagem da empresa e a sua conseqüente valorização.

Uma realidade que está sendo observada é que as grandes corporações estão deixando de buscar soluções de segurança pontuais e isoladas que cumprem um papel limitado e auxiliam paliativamente a empresa no objetivo maior de reduzir seu risco operacional. Estarão com isso organizando o departamento de segurança corporativa, liderado pela figura do *Security Officer* (profissional com conhecimento de Informática e que representará um grupo de usuários ou um departamento da empresa para os assuntos de segurança da informação), e posicionando-o com maior autonomia no organograma. O reflexo disto será o tratamento integrado das demandas de segurança orientadas pelas necessidades do negócio, e não necessariamente as perspectivas do departamento de Tecnologia da Informação. Foco é outra palavra de ordem.

A competitividade do mercado, mais visível nos segmentos financeiro, telecomunicações e energia farão com que as empresas não gastem seus esforços em atividades que não fazem parte de seu segmento de atuação no mercado empresarial, ou seja, estarão organizando melhor sua área de segurança sob o ponto de vista de

gestão, mas contarão com apoio externo de empresas especializadas que possam servir de retaguarda.

Desta forma, terão os processos de segurança sob controle, mas interferirão apenas na organização, coordenação e acompanhamento dos trabalhos terceirizados que envolvem tecnologias heterogêneas e extremamente perecíveis e dinâmicas que obrigam altos investimentos em capacitação.

A complexidade crescente dos processos de negócio, a heterogeneidade de tecnologias, o alto grau de conectividade e compartilhamento de informações, e ainda os novos planos de negócio da empresa serão fatores ainda mais relevantes para a gestão do *Security Officer*. Diante disto, possuir um Plano Diretor de Segurança será condição necessária para a orientação do profissional de segurança na relação com os executivos principais da empresa, investidores e conseqüentemente com a empresa especialista que atuará como retaguarda de segurança. Os planos de continuidade de negócio, divididos em plano de recuperação de desastres, plano de administração de crises e plano de continuidade operacional, receberão grande destaque na primeira metade do ano de 2002, principalmente em empresas que dependerem de operações críticas cujo prejuízo é proporcional ao tempo de indisponibilidade.

Este estudo de caso tem como objetivo propor, para a empresa em estudo, uma Política de Segurança da Informação, o gerenciamento da informação e sua segurança contra ataques de vírus de computador recebidos por meio de correio eletrônico e seus recursos, observando os aspectos existentes atualmente, como também, considerando as futuras expansões que poderão surgir no que se refere ao ambiente de redes e do correio eletrônico.

A administração da segurança de uma rede é um trabalho contínuo, que visa manter o sistema livre de ameaças de grandes perdas e da busca de novas medidas para impedir que elas aconteçam. Manter uma rede segura requer organização, porque um planejamento que não tenha sido bem feito resultará inevitavelmente em falhas na segurança, favorecerá também o surgimento de riscos imprevistos e que poderão deixar a empresa em sérias dificuldades.

Para garantir que a segurança da rede seja efetiva, as empresas estão buscando a elaboração de Políticas de Segurança da Informação, que possam garantir um aumento do controle dos processos envolvidos e, conseqüentemente, da proteção das informações.

Analisando as observações citadas, constatamos a preocupação dos dirigentes empresariais, expressa claramente no resultado da 7ª Pesquisa Nacional sobre Segurança da Informação, executada pela empresa especializada em segurança da

informação, a Módulo Security Solutions S/A no ano de 2001, onde o volume de investimento para a implementação de Políticas de Segurança da Informação têm sido uma das principais metas de dispêndio de divisas.

A Tabela 10, a seguir, relaciona os principais itens relativos aos investimentos previstos para o ano de 2001, com o intuito de se evitar prejuízos gerados por problemas de segurança da informação. Cerca de 80% das empresas brasileiras pretendem aumentar seus investimentos nesta área, 19% irão manter o mesmo do ano anterior e apenas 1% afirma que irá diminuir. Dentre as empresas que declararam os investimentos para este ano, 14% reservam mais de um quinto do orçamento da Área de Tecnologia da Informação para Segurança da Informação.

Tabela 10 – Investimentos em Segurança para 2001

| **INVESTIMENTOS EM SEGURANÇA PARA 2001** | | |
|---|---|---|
| **POSIÇÃO** | **ITEM** | **%** |
| 1º | Política de Segurança | 71 |
| 2º | Capacitação da Equipe Técnica | 65 |
| 3º | Criptografia | 41 |
| 4º | Virtual Private Network (VPN) | 38 |
| 5º | Testes de Invasão | 38 |
| 6º | Análise de Riscos | 35 |
| 7º | Sistema de detecção de Intrusos | 34 |
| 8º | Contratação de Empresas Especializadas | 30 |
| 9º | Aquisição de Software de Controle de Acesso | 29 |
| 10º | Autoridade Certificadora | 29 |
| 11º | Certificado Digital | 28 |
| 12º | Implementação de *Firewall* | 26 |
| 13º | Sistemas de Gestão de Segurança Centralizada | 19 |
| 14º | *Smartcard* | 12 |
| 15º | *Biométrica* | 11 |
| 16º | Controle de Conteúdo | 1 |

Fonte: Módulo Security Solutions (1). (2001).

Segundo a empresa Módulo Security Solution (1) (2001), aproximadamente 53% das empresas apontaram para funcionários insatisfeitos como a maior ameaça à segurança da informação nas organizações. Cerca de 40% das empresas afirmaram terem sido vítimas de algum tipo de invasão, enquanto que 31% não sabiam se tinham sido invadidas, 29% afirmaram nunca ter sofrido qualquer tipo de ataque.

Estes dados revelam o grande risco em que as corporações sofrem por desconhecerem as vulnerabilidades das suas redes de dados. Em 22 casos de ataques,

as organizações não conseguiram detectar a causa e 85% não souberam quantificar o prejuízo.

Cerca de 84% dos ataques foram registrados no último ano, sendo que 43% nos últimos seis meses e 46% das empresas pesquisadas afirmaram não possuir um plano de ação formalizado em caso de ataque.

A Tabela 11 apresenta algumas das principais ameaças às informações que as organizações enfrentam na atualidade.

Tabela 11 – Principais Ameaças às informações da Empresa

| **PRINCIPAIS AMEAÇAS ÀS INFORMAÇÕES DA EMPRESA** | | |
|---|---|---|
| **POSIÇÃO** | **ÍTEM** | **%** |
| 1º | Funcionário Insatisfeito | 53 |
| 2º | Acessos Indevidos | 45 |
| 3º | Vírus | 42 |
| 4º | Divulgação Indevida | 39 |
| 5º | *Hackers* | 36 |
| 6º | Uso de *NoteBook* | 33 |
| 7º | Vazamento de Informações | 30 |
| 8º | Divulgação de Senhas | 30 |
| 9º | Fraudes, Erros e Acidentes | 29 |
| 10º | Pirataria | 27 |
| 11º | Falhas na Segurança Física | 27 |
| 12º | Roubo de Senhas | 25 |
| 13º | Roubo / Furto | 24 |
| 14º | Super Poderes de Acesso | 23 |
| 15º | Alteração Indevida | 21 |
| 16º | Uso Indevido de Recursos | 21 |
| 17º | Alterações Indevidas de Configurações | 21 |
| 18º | Fraudes em *E-mail* | 19 |
| 19º | Lixo Informático | 19 |
| 20º | Acessos Remotos Indevidos | 19 |
| 21º | Concorrentes | 18 |
| 22º | Espionagem Industrial | 18 |
| 23º | Incêndio / Desastre | 16 |
| 24º | Falhas de Energia | 15 |
| 25º | Sabotagens | 12 |

Fonte: Módulo Security Solutions (1). (2001).

Todos os itens citados acima estão presentes nas empresas e é necessária a implementação de uma Política de Segurança que tenha uma abrangência aos principais itens citados, para que a mesma seja eficiente na proteção da Informação.

Segundo a empresa Módulo Security Solution (1998), apesar da Política de Segurança ser o item de maior investimento no ano de 1998, na mesma pesquisa realizada no ano seguinte, foi apresentado que apenas 65% das corporações apresentavam políticas estruturadas, que na metade dos casos está desatualizada e não integrada ao negócio da organização, conforme observado na Tabela 12, com isto, é possível de se ter uma noção de que além da necessidade de se ter um investimento em Política de Segurança, é de vital importância o comprometimento de todos os profissionais da organização para a manutenção e a atualização da mesma, com o intuito de que se consiga prover os objetivos esperados em relação àsegurança da informação e dos recursos disponíveis.

TABELA 12 – Empresas que possuem uma política de segurança

| | |
|---|---|
| Não possui uma política de segurança formalizada | 35% |
| Possui, mas está desatualizada. | 30% |
| Possui e está atualizada | 35% |
| **TOTAL** | **100%** |

Fonte: Módulo Security Solutions. (1998).

Além do fato descrito anteriormente, o pior caso é o índice de empresas que não possuem uma Política de Segurança formalizada (35%), empresas que estão sujeitas a qualquer momento sofrer perdas irreparáveis e que esta situação pode prejudicar sensivelmente a mesma no seu mercado de atuação, por meio da perda de confiabilidade e credibilidade. Uma Política de Segurança é um conjunto de princípios relativos à disponibilidade da rede para os usuários de modo que os dados da organização e recursos computacionais sejam utilizados com segurança, além de possuir um conjunto de procedimentos que serão utilizados na administração da rede para salvo guardar os dados e recursos da organização.

Este documento deve ser claramente descrito, e deve estar de acordo com o objetivo da empresa, pois o ideal é que o mesmo faça parte de um grande planejamento, relacionado com assuntos relativos a segurança incluindo itens como: segurança do próprio prédio, sistema telefônico e outros aspectos diversos da organização. A Política de Segurança proposta neste trabalho tem como objetivo, procurar descrever os aspectos relacionados com a segurança interna/externa da companhia, principalmente

focando a segurança do correio eletrônico (*e-mail)*. Os tópicos abordados procuram tratar dos problemas relacionados à comunicação existente com o correio eletrônico, seus riscos e precauções.

A empresa demonstrou estar preocupada com a segurança da informação, tanto que identificou a necessidade e emitiu um ofício expressando esta preocupação, interesse, apoio e convocando seus Superintendentes e responsáveis pelo projeto, para tomarem as devidas providências sobre o assunto, conforme ANEXO 22.

# CAPÍTULO VI

# PROCEDIMENTOS METODOLÓGICOS

## 6.1 INTRODUÇÃO

Conforme Lakatos e Marconi (1985, p. 81) *"..o método é o conjunto das atividades sistemáticas e racionais que, com maior segurança e economia, permite alcançar o objetivo".*

Nas áreas de Ciências Sociais e Humanas são comuns as pesquisas descritivas, nas quais se registra e analisa fatos ou fenômenos que não podem ser diretamente manipulados quer pelo custo envolvido quer pela própria natureza do fenômeno.

Segundo Cervo (1983), a pesquisa descritiva pode assumir diversas formas, tais como estudos exploratórios, descritivos, documentais e estudos de caso. Para este trabalho escolheu-se o estudo de caso. Assim, após uma pesquisa bibliográfica detalhada, onde a conceituação teórica do problema pode ser apresentada, passou-se ao estudo de uma grande empresa do Vale do Paraíba, procurando analisar os problemas enfrentados e as soluções adotadas em termos de segurança informática, particularmente os problemas relativos à *Internet*, correio eletrônico e vírus de computador.

Buscou-se, assim, uma descrição do contexto da empresa, seu histórico, situação atual e perspectivas futuras, onde a problemática que nos interessa pudesse ser inserida.

## 6.2 O ESTUDO DE CASO

Um estudo de caso pode ser entendido como um questionamento empírico sobre um fenômeno contemporâneo, delimitado por seu contexto real. Embora normalmente o estudo de caso seja proposto e se aplique a situações onde um evento singular deva ser investigado e apreendido por seu valor intrínseco, a situação que se interessa investigar propicia um resultado distinto e suplementar. Além do conhecimento obtido sobre o caso estudado *per si*, a análise feita permite constatar a eficácia de uma política de segurança em informática e sua contribuição para a continuidade do negócio, permitindo, assim, um certo grau de generalização nas conclusões obtidas.

Quanto ao método em si, pode-se dizer que são muitas as vantagens e desvantagens do estudo de caso, fazendo-o se tornar o delineamento mais adequado em várias situações. Uma das principais vantagens é a de que os pesquisadores podem se envolver com o assunto com rapidez, e conseguir sentir o que está acontecendo. O estímulo às novas descobertas é vantajoso, pois em virtude da flexibilidade do planejamento do estudo de caso, o pesquisador durante o seu processo fica atento às novas descobertas, sendo freqüente o mesmo mudar o plano inicial, por conta de ter seu interesse despertado por outros aspectos não previstos anteriormente.

Outra vantagem diz respeito àsimplicidade dos procedimentos de coleta e análise de dados, principalmente quando comparados com os exigidos por outros tipos de delineamento. A linguagem e a forma dos relatórios dos estudos de caso são mais acessíveis do que de outros relatórios de pesquisa. O estudo de caso deve evitar palavras ou frases longas, devendo ser objetivo, não introduzir julgamento do autor e ter poucos adjetivos. Deve relatar a ordem cronológica dos acontecimentos, sempre que possível e utilizar citações diretas de fontes e documentos.

Um aspecto interessante é que o estudo de caso não fecha a questão com uma solução somente, mas apresenta várias opções. Refere-se a um método de ensino bastante popular em comportamento organizacional e administração. Não é um meio adequado para apoiar ou desmentir uma hipótese, sendo mais útil para a pesquisa exploratória.

Segundo Gil (1996), o estudo de caso é preferido quando:

- A questão de pesquisa é do tipo "como?" e "por quê?";
- O controle que o investigador tem sobre os eventos é bastante reduzido;
- O foco temporal se apresenta em fenômenos contemporâneos dentro do contexto de vida real.

A tendência central dos tipos de estudo de caso é que eles tentam esclarecer uma decisão ou conjunto de decisões, tipo "por quê elas foram tomadas?", "como foram

implementadas? " e "quais resultados foram alcançados?". O estudo de caso se aplica quando tentamos:

- Explicar ligações causais em intervenções ou situações da vida real que são complexas demais para tratamento por meio de estratégias experimentais ou de levantamento de dados.
    - Descrever um contexto de vida real no qual uma intervenção ocorreu.
- Avaliar uma intervenção em curso e modificá-la com base em um estudo de caso ilustrativo.
- Explorar aquelas situações nas quais a intervenção não tem clareza no conjunto de resultados.

Exigem-se muita habilidade e esforço de redação para o estudo de caso. Um bom relato começa a ser montado bem antes da efetiva coleta de dados, ou seja, várias decisões envolvendo a redação devem ser tomadas nas fases anteriores para que se aumentem as chances de produção de um estudo de qualidade. A presente dissertação, por se restringir ao âmbito de uma empresa específica, assume as características de um Estudo de Caso, porquanto tem por objetivo efetuar uma análise das ameaças e riscos em que a organização possa se encontrar vulnerável com relação à segurança da informação do *e-mail*. O estudo de caso é caracterizado pelo estudo profundo e exaustivo de um ou de poucos objetos, de maneira que permita o seu amplo e detalhado conhecimento, tarefa praticamente impossível para outros delineamentos.

Em resumo, o trabalho será direcionado seguindo-se os critérios:

- Pesquisa bibliográfica referenciando o assunto;
- Avaliação crítica do problema para as organizações;
- Análise da documentação da empresa no estudo de caso;
- Implementação do estudo de caso;
- Avaliação dos resultados obtidos com a implementação das ferramentas propostas no estudo de caso.

Após a finalização da pesquisa teórica sobre a Política de Segurança da Informação, com foco na proteção das mensagens eletrônicas que chegarem com vírus de computador, será criada uma proposta de uma política de segurança para a empresa em estudo. Esta Política de Segurança a ser criada será implementada e, durante um período de aproximadamente um mês, serão analisadas todas as mensagens de *e-mail* que chegarem ao servidor do correio eletrônico, com o intuito de se identificar se os critérios e diretrizes propostas na política implantada, como também se a intervenção das ferramentas instaladas, estarão sendo eficientes no tocante à proteção das informações, embasada na teoria estudada.

# CAPÍTULO VII

# ESTUDO DE CASO

## 7.1 A EMPRESA FOCO DA PESQUISA

A empresa em estudo é uma Multinacional, pertencente ao ramo de atividade Metalúrgico, presente em 70 países, atuando no Brasil desde 1956, organizada em cinco setores principais denominados Power, Transport, Transmission & Distribution, Power Conversion e Marine, empregando mais de 140.000 profissionais no mundo todo, com ações cotadas nas Bolsas de Valores de Paris, Londres e New York, com um faturamento estimado em 24,6 Bilhões de Euros anuais e seu lema é *"Projetamos Hoje O Que Será Qualidade De Vida Amanhã".*

### 7.1.1 SEGMENTOS DE ATUAÇÃO NO MERCADO MUNDIAL

A empresa atua no mercado mundial no ramo de construção especialista de equipamentos para Infra-Estrutura de Energia e Transporte, conforme detalhamento das atividades abaixo, dividida por Setores:

Power: este segmento detém 20% do mercado mundial, é responsável pela construção de Usinas Hidrelétricas, Termelétrica, Turbinas Industriais, Turbinas a Gás e a Vapor, Caldeiras, Geradores, Irrigação e Saneamento, Controle Ambiental e Customer Services.

Transport: este setor detém 18% do mercado mundial, é responsável pela Construção de Infra-Estrutura, Projeto e Fabricação Metrô-Ferrovário de Carros de Passageiros e de Cargas, Sistemas de Sinalização de Bordo e de Linhas, Centro de Controle Operacional, Equipamentos de Tração, Information Solutions, Trens de Alta Velocidade tipo "Trem Bala", com velocidade aproximada de 345 Km/h.

Transmission & Distribution: esta ramificação detém 13% do mercado mundial, é responsável pela construção de Sistemas de Transmissão e Distribuição de Energia, Fabricação de Equipamentos de Alta, Média e Baixa Tensão, Proteção e Controle, Serviços de Manutenção e Assistência Técnica e Serviços.

Power Conversion: este segmento detém 10% do mercado mundial e é responsável pela construção de equipamentos de Automação de Processos nos Mercados de Mineração, Cimento, Siderurgia, Metalúrgica e Outros, também atuando no desenvolvimento de dispositivos de Acionamento Automático, Geração, Conversão de Energia Elétrica em Energia Produto e Inversores de Alta Velocidade.

Marine: este setor detém 32% do mercado mundial na construção de Grandes Navios de Passageiros, Tanques de Gás Natural Liquefeito, Balsas de Alta Velocidade, Fragatas de patrulha, Navios de Pesquisas Especiais e Navios de Guerra.

### 7.1.2 BREVE HISTÓRICO DA EMPRESA

O nascimento da companhia deu-se no ano de 1782, numa pequena aldeia da cidade de Creusot, na França, dedicada à fundição de vidro. Os Irmãos Adolphe e Joseph Eugéne S. compraram a Usina de Creusot em 1836 e formaram a *Sociedade S. Freres & Cie.* Após a criação da nova Sociedade passaram a diversificar a sua atuação no mercado e a desenvolver o que seria sua principal atividade: a construção mecânica acrescentando-se à Indústria Metalúrgica. Em 1942, os irmãos Charles e Jean sucederam ao pai, concentrando esforços para preservar o potencial industrial do Creusot. Na Segunda Guerra Mundial, um acidente de avião provocou o falecimento de Jean e deixou Charles sozinho àfrente da companhia. Charles reestruturou o Grupo S. e criou a *Societé de Forges et Ateliers du Creusot (SFAC)*, período em que chegou a ser o principal acionista das usinas *SKODA*, na Tchecoslováquia.

### 7.1.3 A ATUAÇÃO NO BRASIL

Com a nacionalização das empresas, o Grupo S. procurou um país propício para sua expansão internacional e assim, em 1948, o casal Charles e Liliane S. se desembarcaram no Rio de Janeiro. Em 1951, Charles S., conquistado pelo Brasil, decidiu investir em vários empreendimentos no Estado de Minas Gerais. Em 1955 o Grupo S. adquiriu uma velha fazenda de café, com uma área de 860.000 $m^2$, situada na cidade de Taubaté, Estado de São Paulo, local onde foi instalada a seda da empresa no Brasil. A pedra fundamental foi lançada em 1956, na presença de ilustres cidadãos, Ilmo. Sr. Presidente da República do Brasil Sr. Juscelino Kubitschek de Oliveira, que saudou a nova empresa com um breve discurso:

*"Os votos que eu formulo nesta hora, são para que capitais estrangeiros, técnicos estrangeiros e, sobretudo, mestres de indústrias – como Charles S.– venham para o Brasil colaborar conosco e ajudar-nos no nosso desenvolvimento que fará desta Nação,*

*em poucos anos, uma das maiores expressões da riqueza mundial". (Juscelino K. de Oliveira).*

No ano de 1957 suas operações fabris são efetivamente iniciadas, com 203 funcionários, inclusive 25 especialistas vindos da França, na maioria soldadores que utilizavam recursos de tecnologia avançada, tanto em usinagem mecânica como também em caldeiraria.

Desde então o Grupo Empresarial tem evoluído, construindo e mantendo uma liderança no seu ramo de atuação no mercado, evoluindo não somente no Brasil, como também nos outros 70 países, efetuando uma diversificação de suas atividades e produtos, associando-se a outros conglomerados industriais, seja em tecnologia, pesquisa, desenvolvimento de novas soluções tecnológicas e buscando uma excelência na qualidade e competitividade dos seus produtos para um melhor atendimento dos seus clientes.

### 7.2 O AMBIENTE DA PESQUISA NA EMPRESA

A unidade da empresa que é foco desta pesquisa é a fábrica principal do Setor Power de atuação do Grupo Empresarial na América Latina, localizada na cidade de Taubaté São Paulo. Uma empresa com o porte e influência mundial semelhante à que está em estudo, necessita ter implementado uma sistemática de Segurança da Informação, também denominada Política de Segurança da Informação e a empresa em estudo investe neste sentido. A companhia tem, como caráter imprescindível frente ao seu mercado de atuação, a preocupação em manter ativa a sua *Rede de Computadores* interligando todos os recursos computacionais existentes nas unidades espalhadas pelo mundo ininterruptamente. É uma atividade complexa e frágil, porém provê toda uma operação de estratégia, competitividade, agressividade frente ao mercado concorrente e também no apoio à tomada de decisão. Esta rede tem o objetivo de possibilitar o intercâmbio das informações rapidamente entre os diversos usuários e unidades da empresa com segurança, integridade, confiança e de fácil acesso. Com relação ao fluxo das informações em trânsito, a empresa tem uma preocupação elevada –- a nível mundial –- com referência às pessoas que têm acesso aos seus sistemas de Informática e às suas bases de dados, que contribuem diretamente para manter sua competitividade. Deste modo, a Gestão dos Processos e da Informação, acompanhamento evolutivo do ciclo de fabricação, controle, cronogramas técnicos e toda a documentação relacionada aos assuntos da empresa no tocante à sua divulgação aos seus funcionários, é classificada como Confidencial, Restrita e Irrestrita e a divulgação é limitada aos profissionais autorizados.

### 7.2.1 A EVOLUÇÃO TECNOLÓGICA DOS COMPUTADORES NA EMPRESA

A automação e os recursos de Informática da empresa evoluíram seguindo uma perspectiva semelhante à adotada por companhias multinacionais existentes no Brasil do porte semelhante à empresa em estudo. Quando do início da fase de automação, todos os recursos de *hardware* foram adquiridos de um único fabricante, geralmente um grande fornecedor de soluções para as empresas, que garantia qualidade, segurança dos dados, rapidez e presteza no atendimento em casos de quebra ou problema técnico no *hardware* ou seus *periféricos*. Esta sistemática esteve presente e atuante até o momento da migração para os equipamentos de plataformas menores, ou seja, para os microcomputadores e servidores de rede de menor porte.

#### 7.2.1.1 O COMPUTADOR *MAINFRAME* DO PASSADO

Inicialmente, na década de 1980, houve a implementação do Centro de Processamento de Dados, com todas as informações centralizadas num único local, em uma única máquina do tipo *Mainframe* modelo serie *IBM* /370, substituído em 1987 pelo equipamento da série *IBM* 4381, também da *IBM*. Todos os sistemas de Gestão Empresarial, Financeiro, Contábil, Controle de Estoques, Métodos e Processos, Planejamento, Controles de Obras de Engenharia e de Recursos Humanos foram desenvolvidos internamente, por profissionais especializados e contratados como funcionários. A linguagem de desenvolvimento adotada na época foi o *COBOL* integrado com a ferramenta *GENER / OL* e o banco de dados *DL/1* com estrutura e método de armazenamento de dados Hierárquico. Esta estrutura de Informática detinha um processamento de dados centralizado e com um alto custo para se manter, ou seja, existiam vários contratos de manutenção tanto de *hardware* quanto de *softwares* assinados com a *IBM*, além dos custos com folha de pagamento da equipe de desenvolvimento, que na realidade funcionava como uma pequena *Software House* para atender às necessidades de desenvolvimento de serviços internos da empresa.

#### 7.2.1.2 O PROCESSO DE *DOWN-SIZE* DOS COMPUTADORES

Com a evolução tecnológica dos recursos de Microinformática, a empresa percebeu a necessidade de acompanhar as novas tendências e facilidades emergentes, ou seja, adquiriu vários microcomputadores de última geração para uso dos usuários de diversas áreas (atualmente existem 930 microcomputadores ativos na rede), em substituição aos antigos terminais *IBM*, iniciou o seu processo de *Down-Size* do

computador *Mainframe*, reestruturou toda a sua Rede de Computadores com tecnologias atuais tipo *Giga-Bit Ethernet* de velocidade com todos os dispositivos necessários para a distribuição do sinal de comunicação e acesso, adquiriu vinte e um servidores também de última geração e de alto desempenho, configurados com o Sistema Operacional Windows NT Server 4, da empresa Microsoft S.A, para suportar o novo Sistema de Gestão Integrada tipo *ERP SAP / R3* da empresa alemã *SAP*, implantou o Sistema de Correio eletrônico *Lotus Notes*, adotou o banco de dados *Oracle* e *SQL Server* para suas aplicações críticas, efetuou uma padronização dos *softwares* da área Administrativa utilizando as ferramentas desenvolvidas pela empresa Microsoft S.A, tais como MS-Office, MS-Project e o Sistema Operacional Windows NT Workstation 4. Para a área de Engenharia, padronizou as ferramentas utilizando os produtos desenvolvidos e comercializados mundialmente pela empresa AutoDesk S.A, ou seja o software Mechanical Desktop e Auto Cad Mechanical e para projetos envolvendo a Teoria de Elementos Finitos, utiliza-se o *software* Ansys.

Nestes vinte e um servidores, estão distribuídos todos os dados e informações pertinentes à operação da empresa, ou seja, todos os seus projetos, obras, pesquisas desenvolvidas, acordos com clientes e fornecedores, informações corporativas, legados históricos de projetos, abrigam ainda o sistema de Gestão integrada SAP / R3, o correio eletrônico Lotus Notes e uma infinidade de outras informações imprescindíveis para a sobrevivência da empresa e que contribuem para a tomada decisão gerencial, inclusive os dados os dados de histórico corporativo e de contratos com clientes, antes existentes no *mainframe*, que foram adaptados ao novo ambiente.

A Tabela 13 apresenta uma relação contendo todos os servidores de dados, dos sistemas de gestão do negócio, do correio eletrônico, dos bancos de dados e de aplicações diversas, com suas características específicas:

Tabela 13 – Servidores de Rede e Aplicações Diversas

| Utilização | **Denominação** | **Aplicação** | **Características Atuais** |
|---|---|---|---|
| **SAP TAUBATÉ** | **SAPX01** | • Servidor de Banco de Dados da Produção | • WINDOWS NT SERVER 4<br>• COMPAQ Proliant 6500<br>• 02 processadores Pentium PRO 200 Mhz<br>• 1.917 Gb RAM<br>• 184.7 Gb<br>• DLT 35 / 70 |
| **SAP TAUBATÉ** | **SAPXA1** | • Servidor de Aplicações da Produção | • WINDOWS NT SERVER 4<br>• COMPAQ Proliant 6500<br>• 03 processadores Pentium 800 Mhz<br>• 3.8 Gb RAM |

| | | | |
|---|---|---|---|
| | | | • 29.1 Gb |
| **SAP TAUBATÉ** | **SAPXA2** | • Servidor de Aplicações da Produção | • WINDOWS NT SERVER 4<br>• COMPAQ Proliant 6500<br>• 03 processadores Pentium 800 Mhz<br>• 1.917 Gb RAM<br>• 29.1 Gb |
| **SAP TAUBATÉ** | **SAPY01** | • Servidor de Banco de Dados e Aplicações para Desenvolvimento | • WINDOWS NT SERVER 4<br>• COMPAQ Proliant 6000<br>• 02 processadores Pentium 800 Mhz<br>• 1.917 Gb RAM<br>• 137 Gb<br>• DLT 15 / 30 |
| **SAP TAUBATÉ** | **SAPZ01** | • Servidor de Banco de Dados e Aplicações para Testes | • WINDOWS NT SERVER 4<br>• COMPAQ Proliant 6000<br>• 02 processadores Pentium 800 Mhz<br>• 1.917 Mb RAM<br>• 184.7 Gb<br>• DLT 15 / 30 |
| **Rede – TAUBATÉ** | **K-682** | • Servidor PDC (Controlador Primário do Domínio), responsável pelo acesso dos usuários à rede.<br>• Servidor de controle dos serviços TCP/IP (DHCP e WINS) | • WINDOWS NT SERVER 4<br>• COMPAQ Proliant 2500<br>• 01 processador Pentium 800 Mhz<br>• 256 Mb RAM<br>• 15 Gb |
| **Aplicativos SQL SERVER Taubaté** | **K-0765** | • Servidor Member Server do Domínio<br>• Netexprex<br>• Conversão IBM<br>• Sistema de Folha de Pagamento<br>• MS-SQLSERVER | • WINDOWS NT SERVER 4<br>• COMPAQ Proliant 3000<br>• 01 processador Pentium II 800 Mhz<br>• 256 Mb RAM<br>• 54 Gb |
| **LOTUS NOTES** | **BR01YH (K-0345)** | • Servidor do Correio Eletrônico Lotus Notes | • WINDOWS NT SERVER 4<br>• COMPAQ Proliant 3000<br>• 02 processadores Pentium II 800 Mhz<br>• 256 Mb RAM<br>• 15 Gb<br>• DLT 20 / 40 |

**(...)**

***Nota: Por tratar-se de um documento com informações confidenciais da empresa, esta relação não poderá ser apresentada na íntegra.***

Todos os servidores citados acima estão localizados em local isolado da área fabril, restrito para o acesso de somente pessoas autorizadas, sala em ambiente com toda infra-estrutura de proteção contra incêndio, provida de ar-condicionado para manter a temperatura constante em torno de 20º C, servida por rede de alimentação elétrica totalmente independente e aterrada, dependências de salas monitoradas em sistema de vigília durante vinte e quatro horas pela equipe de profissionais da Segurança Patrimonial, provida por equipamento *nobreak* com autonomia para quinze horas, sendo

que este *nobreak* está ligado a um gerador de energia elétrica, movido a óleo combustível, para funcionamento ininterrupto quando em momentos de falta de energia.

### 7.3.2 A INFRA-ESTRUTURA DE INFORMÁTICA EXISTENTE

A rede *LAN* (Local Area Netowrk) e *WAN* (Wide Area Network) no Brasil são interligadas por meio de linhas de comunicações contratadas das empresas provedoras públicas, tais como a Telefonica. Devido ao fato destas informações estarem transitando de uma filial para a outra por meio de comunicação provida pelas empresas citadas acima, é um desafio manter toda esta infra-estrutura de rede segura, disponível e os computadores em funcionamento constantemente. O bom desempenho da companhia, como também dos seus profissionais, depende desta comunicação. Na Figura 24, são detalhadas todas as linhas de comunicação entre as principais unidades atuantes no Brasil.

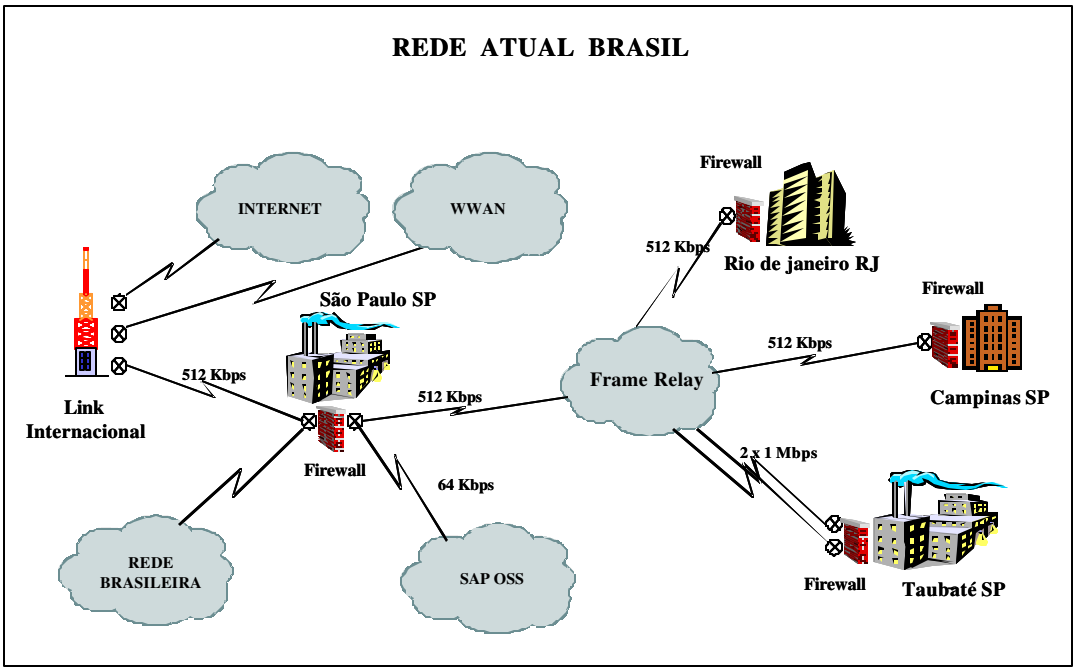



Figura 24 – Esquema da Rede LAN e WAN no Brasil

Sobre o esquema acima, há atualmente um conjunto de linhas privadas de comunicação de dados e contratadas das prestadoras de serviços telefônicos, a Telefonica, onde uma das unidades da empresa em estudo localizada na cidade de São Paulo, é a sede de concentração de toda a comunicação e fluxo de informações tanto de chegada, como também de saída, para outras filiais dentro do Brasil ou no exterior. Na

Tabela 14 apresenta-se um detalhamento das linhas de comunicação existentes dentro do Brasil e com as respectivas características.

Tabela 14 – Descritivo das Linhas de Comunicação de dados

| UNIDADE ORIGEM | UNIDADE DESTINO | COMUNICAÇÃO | PRESTADORA |
|---|---|---|---|
| Taubaté - SP | Nuvem Frame Relay | 02 de 01 Mbps | Telefonica |
| Rio de Janeiro RJ<br>Campinas - SP | Nuvem Frame Relay<br>Nuvem Frame Relay | 512 Kbps<br>512 Kbps | Telefonica<br>Telefonica |
| Empresa SAP Brasil | São Paulo - SP | 64 Kbps | Telefonica |
| Nuvem Frame Relay | São Paulo - SP | 512 Kbps | Telefonica |
| São Paulo - SP | Link Internacional | 512 Kbps | Provedor Internacional |

Cada filial tem a sua proteção independente e efetuada por meio de um *Firewall* da marca *Check Point* (denominação de um *software Firewall* distribuído pela empresa Computer Associate), onde são filtrados todos os dados que chegam e que saem, além de executar proteção contra invasores indesejáveis, por exemplo, *Hackers*.

A preocupação com este assunto tem sido comprovada tomando-se como base os altos investimentos feitos em infra-estrutura de Informática, ou seja, a reformulação das salas onde se concentram os servidores principais dos Sistemas Integrados de Gestão Integrada, Servidores dos Bancos de Dados, Servidores do Correio Eletrônico, dispositivos de *Back-up* e *Restore* de dados, bem como todo um conjunto de equipamentos de ar-condicionado, *nobreaks* para os servidores, gerador de energia elétrica, alarmes contra incêndio, cofre de segurança imune a fogo e portas cancelas de segurança. A preocupação com a Segurança da Informação ao nível Físico e Lógico é uma constante e exigida dos responsáveis, sendo constatado pelo investimento efetuado anualmente na modernização de dispositivos de *Hardware* e *Software*, geradores de energia elétrica e *nobreaks*, como também no investimento em treinamento dos profissionais da área de Informática e usuários de diversas áreas. No Brasil existem aproximadamente cinco mil funcionários e quatro mil computadores interligados em rede acessando os servidores de dados e enviando, como também recebendo, mensagens por meio do correio eletrônico. Somente na unidade de Taubaté, local desta pesquisa, existe um mil e duzentos usuários e novecentos e trinta microcomputadores e um mil trezentos e quarenta e um pontos de rede disponíveis para ligação de um microcomputador utilizando a tecnologia *Giga-Bit Ethernet* (tecnologia que adapta o modelo *Ethernet* para transmissão de dados a 1 *Gbps* ou maior). O padrão de roteadores utilizados são os modelos da série 25XX da empresa Cisco, e existem 5 operando na interligação das redes. Com referência aos Swiches, existem trinta e quatro

do fabricante 3COM e o meio físico formado por cabo tipo Par Trançado categoria 5e da marca Furukawa e Panduit..

Os arquivos de trabalho, projetos de obras, pesquisas desenvolvidas, gerenciamento de contratos com fornecedores e clientes, estratégia de *Marketing*, lançamento de novos produtos, propostas comerciais, estratégias de incorporação de novas empresas, acordos mundiais de prestação de serviços, enfim, tudo que se relaciona às atividades da empresa — ligados à unidade de Taubaté — estão armazenados em alguns dos servidores citados na Tabela 13 e que são considerados o "Coração da Empresa".

A companhia se preocupa com a preparação e capacitação do seu quadro de funcionários com as competências necessárias para o bom desempenho de suas funções, investe, portanto, em treinamento e pesquisa. O objetivo principal a ser conseguido com o treinamento é a busca do conhecimento das ferramentas adequadas do trabalho, para se evitar enganos com o mau uso e, sobretudo, com o uso indevido. A empresa concluiu que existe a necessidade de criar uma Política de Segurança da Informação, que provê um Plano de Ação e investe neste sentido.

## 7.4 DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO EXISTENTES

A empresa não tem uma Política de Segurança da Informação com os requisitos necessários citados em um documento oficial aprovado pela alta direção e que tenha sido divulgado internamente. Existe, porém, algumas normas sobre segurança que são utilizadas baseando-se em cuidados postos em prática pelo "bom senso" e que são recomendados pela experiência de profissionais do ramo de informática. Todas estas ações e observações são decididas e acordadas em reuniões com os dirigentes responsáveis de cada setor, juntamente com o responsável pela Área de Informática, como também um representante da alta direção da empresa. Existe uma consciência de que a responsabilidade pela integridade do sistema de informação é do Departamento de Informática e algumas regras básicas são observadas:

- Nenhum usuário pode se conectar a rede de dados da empresa, exceto os homologados, autorizados e monitorados pela Área de Informática.
- É proibido o uso de equipamentos de *hardware* ou *software* de propriedade de funcionários na rede da empresa.
- Um novo UserID (identificação do usuário na rede) ou uma nova "conta" para acesso à rede para um novo usuário somente poderá ser criada mediante

solicitação por escrito validada pelo gerente responsável pela área solicitante.

- Todos os acessos à rede de dados e correio eletrônico e servidores devem ser bem definidos e documentados para todos os usuários.
- Para o Sistema de Gestão Integrada, SAP e BAAN, todos os usuários devem ter um perfil de acesso às transações restritas às funcionalidades para as quais foram autorizados por suas respectivas gerências.
- Todas as senhas para acesso à rede ou qualquer aplicativo da empresa devem ter –- no mínimo –- oito dígitos e com a obrigatoriedade de mudança automática forçada a cada três meses.
- As últimas seis senhas não poderão ser repetidas e o sistema deverá efetuar o bloqueio automático da conta de acesso após três tentativas inválidas.
- Após três tentativas sem sucesso de digitação da senha para acesso aos sistemas informatizados ou à rede, a conta do usuário é bloqueada automaticamente.
- O desbloqueio da conta travada somente será possível mediante a intervenção do Administrador da Rede, após a abertura de um chamado técnico junto à central de gerenciamento do *Help-Desk* (grupo de profissionais responsáveis por todo o suporte técnico de hardware e software para a microinformática dentro das dependências da organização) e envio do formulário conforme ANEXO 13.
- A temperatura da sala onde se encontram os servidores deve ser constantemente monitorada pelos profissionais de plantão e o termômetro interno deve estar sempre em perfeitas condições operacionais para acionamento automático em caso de qualquer variação da temperatura que esteja fora da faixa aceitável de 18º C até 23º C.
- A carga da bateria do *nobreak* principal deve ser monitorada todos os dias para verificação de sua capacidade de atendimento sempre que solicitado, por meio de pane elétrica da rede principal.
- O tanque de óleo combustível, bem como os testes de funcionamento do gerador de energia elétrica devem ser monitorados todos os dias, com o objetivo de o mesmo estar disponível e em sua plena funcionalidade operacional tão logo seja solicitado.
- Rotinas de teste de *back-up* e *Restore* de dados devem ser executadas semanalmente com o objetivo de verificação da boa funcionalidade das unidades de cartuchos de fitas.

- Os cartuchos de fitas de *back-up* de dados devem ser armazenados em sala cofre ou ambiente totalmente vedado, protegido contra incêndio, umidade e o local deve ser o mais longe possível da sala dos servidores da rede.
- Somente é permitido o acesso às salas dos servidores por funcionários ou profissionais devidamente identificados e autorizados pela Gerência do Departamento de Informática.
- Nenhum microcomputador da empresa deve possuir *modem* interno ou externo instalado para acessar a *Internet* ou qualquer serviço por meio de linha discada.
- Toda e qualquer comunicação com a *Internet* ou com serviços ligados à telecomunicações deve ser por meio da rede de dados da empresa, para se ter garantido a proteção do *Firewall* disponível.
- Todos os microcomputadores da empresa que estão conectados à rede de dados devem estar com o software antivírus McAfee instalado e garantindo proteção contra vírus indesejáveis.

### 7.4.1 IDENTIFICAÇÃO DAS VULNERABILIDADES DO AMBIENTE

A identificação e o registro dos pontos vulneráveis de uma rede é de fundamental importância para a implementação de um procedimento de segurança. As vulnerabilidades são relativamente fáceis de se identificar em uma rede, a maioria possui como característica comum à espera por um pedido de conexão que eles respondem de algum modo permitindo acesso a informações.

Abaixo é apresentada uma lista das principais vulnerabilidades encontradas no ambiente da empresa em estudo:

- Necessidade de se instalar um software antivírus nos servidores de dados que possa efetuar um rastreamento automático sempre que um determinado arquivo for gravado na rede.
- Necessidade de se instalar um software antivírus no servidor do correio eletrônico que possa efetuar um rastreamento automático de vírus em todos os *e-mails* que estejam chegando para as caixas postais dos usuários.
- Necessidade de se instalar um software que possa executar um inventário automático das estações de trabalho dos usuários e que o mesmo informe aos administradores da rede sempre que houver qualquer alteração das configurações –- tanto de hardware como também de software –- existente nestas estações.

- Necessidade da execução de uma diretriz de que todos os softwares em uso nas dependências da empresa sejam adquiridos, testados e homologados antes de ser disponibilizados para uso na rede.
- Necessidade de se proibir o uso de softwares tipo *Shareware* (*software* distribuído para demonstração em *BBS´s* (Bulletin Board Service), provedores de *Internet*, *Home Page* (página inicial da *Internet* de fabricantes e organizações diversas) e *Freeware* (*software* que pode ser usado, copiado ou distribuído sem qualquer custo).
- Necessidade bloqueio da área do Painel de Controle do Sistema Operacional Windows da estação de trabalho dos usuários, com o objetivo de não permitir que o mesmo possa executar a instalação de qualquer *software* que tenha a intenção.
- Necessidade de proteção para o Servidor do Correio Eletrônico *Lotus Notes*.
- Necessidade de proteção para o Servidor do *DNS*.
- Necessidade de proteção para o Servidor do *DHCP*
- Necessidade de proteção para o Servidor do Controle do Acesso Remoto.
- Necessidade de padronização de formulários para cadastramento de novos usuários na rede, no correio eletrônico e no Sistema de Gestão Integrada.
- Necessidade de padronização es formulários para controle de cartuchos de *back-up* dos servidores.
- Necessidade de definição de procedimentos para uso de estações de trabalho ligadas àrede e em redes independentes.

### 7.4.2 CONSIDERAÇÕES SOBRE A IMPLANTAÇÃO DE UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO NA EMPRESA EM ESTUDO

Segundo Luz (1999), a implantação de uma Política de Segurança apresenta vários benefícios conforme abaixo:

- A padronização das redes *LAN* e *WAN*, centralizando as definições, seus componentes de *Hardware* e *Software*, linhas ou sistema de comunicação.
- Compartilhar das decisões e experiências com os gestores e membros da Alta administração.
- Avaliação dos riscos existentes.
- Visão estratégica da empresa como um negócio.
- Implementar uma arquitetura de segurança da informação com visão

corporativa.

- Pesquisar novas tecnologias para implementação na corporação.
- Atuar em conjunto com as auditorias internas da empresa.
- Desenvolver programas de conscientização de usuários, bem como treinamento.
- Definir as expectativas da organização quanto ao uso dos seus computadores e rede e estabelecer procedimentos visando prevenir e responder a incidentes relativos àsegurança.
- Assegurar a legalidade, confidencialidade, integridade e disponibilidade da informação.
- Fazer com que os usuários utilizem os recursos de informática com maior intensidade para fins do negócio da empresa.
- Disciplinar a circulação de informação dentro da empresa.
- Monitorar os Sistemas de Informações.

Segundo Fontes (2000), o processo de segurança da informação na empresa, como também nas organizações em geral, envolve aspectos técnicos, humanos e organizacionais. Em relação a estes dois últimos é fundamental a definição e a existência de uma Política de Segurança de proteção da informação. Esta Política deve explicitar para todos os usuários que acessam e usam a informação, qual é a filosofia da empresa sobre este recurso. Ela deve considerar as características operacionais e culturais da empresa, bem como o relacionamento entre as pessoas.

A Política de Segurança dará o direcionamento para as implementações técnicas. Implementar procedimentos de segurança sem uma Política definida é equivalente a navegar sem saber o destino a que se quer chegar. A Política deve ser um elemento de um conjunto de ações que compõem o Processo de Segurança da empresa, independente da informação estar no ambiente computacional ou no ambiente convencional.

O cuidado com a informação deve ser o mesmo e a Política precisa ter vida e chegar a todas as pessoas. Uma das formas de dar vida àPolítica é a conscientização de todos os usuários, mostrando a estes o valor da informação e quais são suas responsabilidades. As empresas que investem na conscientização dos seus usuários têm mais chance de ter sucesso no seu Processo de Segurança.

No estudo das viabilidades para que a implantação de uma Política de Segurança se torne apropriada e efetiva em qualquer empresa ou organização, é de suma importância o envolvimento de profissionais de todos os níveis, inclusive da alta direção, para que se possa alcançar os objetivos almejados. É de caráter imprescindível que os

líderes e gerentes corporativos suportem de forma completa o processo da Política de Segurança da Informação, caso contrário, haverá poucas chances de que ela obtenha o impacto desejado.

Existem alguns profissionais que precisam estar envolvidos com todo o processo de criação e revisão de procedimentos da Política:

- O Administrador da Segurança do Site e dos Sistemas de Informação.
- Os profissionais da área de suporte técnico da área de Tecnologia da Informação.
- Os Administradores ou disseminadores de diretrizes dentro dos grupos de usuários dentro da corporação.
- A equipe de reação a incidentes de segurança da organização.
- Os representantes dos grupos de usuários diretamente afetados pela Política de Segurança da Informação.
- O Conselho Jurídico Legal da corporação.

A lista relacionada acima tem caráter representativo, podendo sofrer variações de acordo com a empresa na qual será criada a Política. No entanto, o envolvimento deste grupo de profissionais é importante para que a Política resultante consiga atingir uma maior aceitabilidade possível.

Um dos objetivos principais é o envolvimento de representantes dos membros, gerentes e dirigentes com autoridade sobre o orçamento a ser gasto com a implementação da Política, pessoal técnico com conhecimento suficiente para delimitar os limites a serem suportados pelas soluções a serem implantadas, e o conselho legal que conheça as decorrências legais das várias Políticas.

Em algumas empresas, pode ser conveniente e apropriado a inclusão de profissionais responsáveis pela Auditoria Interna. O comprometimento e o envolvimento deste grupo é importante para que a política resultante consiga alcançar uma maior aceitabilidade possível dentro da corporação. Com relação à área Jurídica, também é importante mencionar que o seu papel do conselho legal irá variar de país para país, conforme as leis vigentes.

Em conformidade aos fatores descritos acima, uma Política de Segurança demonstra ser um documento que exige para sua formulação e pesquisa, um trabalho extenso e complexo, envolvendo um grupo de pessoas. Sendo assim, a seguir é apresentada uma proposta de Política de Segurança, de forma que a mesma possa servir como base para as futuras discussões e consulta.

## 7.5 PROPOSTA DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Com base no estudo desenvolvido até esta fase do trabalho, na seqüência serão apresentados alguns dos principais critérios importantes para a implementação da Política de Segurança da Informação, o gerenciamento da informação e sua segurança contra ataques de vírus de computador recebidos por meio de correio eletrônico, na empresa em estudo.

Com a implementação da Política de Segurança da Informação, espera-se obter maior segurança quanto às mensagens e arquivos que chegarem à empresa contaminados por vírus de computador via correio eletrônico, eliminação de *softwares* considerados ilegais –- "Piratas" –-, padronização dos aplicativos utilizados, conscientização dos usuários e uma garantia de que as informações armazenadas nos servidores estarão íntegras e confiáveis.

O tema em estudo estará sendo pesquisado em uma vasta teoria e literatura publicada por revistas especializadas, portais da *Internet* mantidos por empresas especializadas e governamentais no trato do assunto e que será a base do estudo de caso em evidência. A informação pode ser o diferencial e o poder existente no competitivo meio organizacional. A abordagem sobre a segurança da informação é como uma corrente na empresa, cujo "elo fraco" são as pessoas que fazem uso inadequado do correio eletrônico e dos sistemas de informação. A comunicação da empresa com o mundo interior e o exterior com segurança é o fascínio e o desafio de se conseguir garantir que a informação --- tão preciosa para a continuidade do negócio --- se mantenha íntegra, disponível, confidencial e autêntica.

### 7.5.1 PRINCIPAIS METAS

As principais metas a serem atingidas com a criação desta política são:

- Garantir aos usuários da informação um ambiente seguro, estável e bem configurado.
- Conscientizar os usuários do valor da informação.
- Permitir acesso seguro às informações.
- Garantir a segurança das informações armazenadas e em trânsito.
- Estabelecer controle sobre o ambiente.
- Proteger os negócios da empresa.
- Reduzir os riscos existentes.
- Proteger as informações contra ameaças externas.
- Garantir confiabilidade e alta disponibilidade dos recursos.

### 7.5.2 PRINCÍPIOS BÁSICOS DA INFORMAÇÃO

Segundo Akiyama (1999), A informação tem quatro princípios básicos conforme citados abaixo:

- Integridade: A condição na qual a informação ou os recursos da informação são protegidos contra modificações não autorizadas.
- Confidencialidade: Propriedade de certas informações que não podem ser disponibilizadas ou divulgadas sem autorização prévia dos responsáveis pelas mesmas.
- Disponibilidade: Característica da informação que se relaciona diretamente à possibilidade de acesso por parte daqueles que a necessitam para o desempenho de suas atividades.
- Legalidade: Estado legal da informação, em conformidade com os preceitos da legislação em vigor.
- A informação deve ser classificada, avaliada e, se necessário, atualizada anualmente pela área geradora e detentora da informação e relacionada no documento denominado “Classificação de Documentos”, conforme ANEXO 01. Quanto a sua confidencialidade poderá se enquadrar em uma das três classes abaixo, classificadas com base no seu nível de impacto potencial e probabilidade de ocorrência:
- Confidencial: Informação geralmente de caráter sigiloso que se divulgada fora do ambiente (externo ou interno) onde a informação deva ser utilizada causa um alto impacto no negócio da empresa.
- Confidencial de Alto Impacto: Informação importante e de alto risco que, se não for controlado apropriadamente, poderá ter um significante impacto com relação às demonstrações financeiras, operação do negócio, e / ou segurança geral da operação. Esta informação geralmente não existe no concorrente e neste caso, poderia ser utilizada para modificação ou melhoria do seu processo, ficando em condições superiores de competitividade.
- Restrita: Informação que se divulgada fora do ambiente (externo ou interno) onde a informação deva ser utilizada causa um impacto médio no negócio da empresa.
- Restrita Médio Impacto: Informação importante e de alto risco que, se não for controlado apropriadamente, poderá em conjunto com outros pontos de atenção, comprometer a integridade e segurança dos sistemas e das informações por ele processadas. A falta de controle sobre este risco pode, com o passar do tempo, gerar um impacto desfavorável relacionado às demonstrações financeiras,

operação do negócio, e/ou segurança geral da operação. Existe informação de conhecimento semelhante no concorrente e, neste caso, poderia ser utilizada como *benchmark*.

- Irrestrita: Todas as informações não classificadas nas classes acima e, conseqüentemente, não causam nenhum impacto aos negócios da empresa, caso sejam divulgadas fora do ambiente onde a informação deva ser utilizada.

### 7.5.3 PRINCIPAIS AMEAÇAS

As principais ameaças à segurança da informação, muitas vezes são executadas por pessoas não autorizadas, por meio de falha humana, imperícia ou por fenômenos da natureza.

Com referência à Integridade da Informação:

- Ameaças de Ambiente (fogo, enchente, tempestade, etc.)
- Erros humanos
- Fraudes
- Erros de processamento
- Erro Dados em: *back-ups*, *logs*, bases de dados.

Com referência à Indisponibilidade da Informação:

- Falha em sistemas ou nos diversos ambientes computacionais
- Indisponibilidade de Serviço

Com referência à Divulgação da informação:

- Divulgação de informações premeditada
- Divulgação de informações acidental.

Com referência a Alterações Não Autorizadas da informação:

- Alteração premeditada das informações
- Alteração acidental das informações

Com referência a Acessos Não Autorizados da informação:

- Acessos internos às informações
- Acessos externos às informações

### 7.5.4 ABRANGÊNCIA DA POLÍTICA A SER IMPLEMENTADA

A seguir, um escopo da abrangência da Política a ser implementada:

- Documentos impressos.
- *Back-up* das informações.
- Gravação de CD Rom, discos Zip Drive (discos semelhante a um disquete, porém com capacidade de armazenamento entre 100 ou 250 Mega Bytes de dados).
- *Internet*, *Intranet* e *Extranet*.
- Controle de acesso aos equipamentos e informações.
- Segurança física dos equipamentos.
- Pirataria de *software*.
- Conscientização dos usuários.
- Entrada e saída de informação.
- Correio eletrônico (*e-mail*).
- Proteção antivírus.

#### 7.5.4.1 DOCUMENTOS IMPRESSOS

Com referência a todo o tipo de documentos, formulários e papéis diversos relacionados à empresa, deverão seguir as diretrizes que se seguem:

- Todos os documentos relacionados aos assuntos de interesse da organização sejam confidenciais ou não, não poderão permanecer sobre a mesa dos usuários, expostos, exceto aqueles que estejam sendo utilizados no trabalho atual.
- No horário do almoço, à saída do expediente e no caso do funcionário ausentar-se do local de trabalho por períodos prolongados, os documentos deverão ser guardados em locais apropriados.
- Nas áreas produtivas, os desenhos, ordens de produção, instruções específicas e outros documentos necessários à fabricação dos componentes também deverão ser guardados em locais protegidos. Ao término da fabricação dos componentes, os documentos deverão ser prontamente destruídos, com respectiva baixa nos sistemas.
- As cópias de documentos deverão ser feitas de acordo com normas internas da empresa e com as devidas autorizações dos responsáveis. Cópias avulsas deverão ser inutilizadas após a sua utilização.
- As áreas serão providas de fragmentadoras de papel para destruição de qualquer documento que contenha informações relevantes.

- Todos os armários que contenham documentos impressos deverão possuir chaves e serem trancados ao final do expediente. Cópias das chaves, devidamente identificadas deverão ficar em poder da segurança patrimonial e somente entregues mediante autorização da gerência específica.
- Durante o horário de expediente, os supervisores e gerentes das áreas deverão verificar se os procedimentos estão sendo cumpridos, orientando os funcionários para tal. Fora do horário de expediente, a segurança patrimonial durante as rondas diárias verificará o cumprimento das normas.
- Os documentos encontrados sobre as mesas fora do horário de trabalho serão recolhidos pela segurança patrimonial e entregues à gerência do funcionário no dia seguinte.
- Em cada departamento haverá uma fragmentadora de papel que deverá ser utilizada para destruição de documentos confidenciais.

#### 7.5.4.2 *BACK-UP* DAS INFORMAÇÕES

Adota-se como premissa básica de que todas as informações relacionadas a trabalho e ligadas à empresa são armazenadas nos servidores de dados da rede, portanto, todas as diretrizes de *back-up* adotadas estarão com foco para estes servidores. A empresa criou um procedimento específico para gerenciamento da rotina específica de *back-up* para todos os servidores, conforme ANEXO 21.

##### 7.5.4.2.1 *BACK-UP* DOS SERVIDORES DE DADOS

Todos os servidores da rede são munidos de dispositivos de *hardware* e *software* para a execução das rotinas de *back-up,* segundo as características da sistemática abaixo. Diariamente as ocorrências de problemas relacionados ao *hardware* que são detectadas, são anotadas no documento conforme ANEXO 24 e ANEXO 25, que contribui para uma constante verificação dos equipamentos se estão trabalhando a plena capacidade de uso e de disponibilidade.

Com o intuito de se manter um controle do rodízio de fitas, utiliza-se um controle dos cartuchos de *back-up* diariamente, conforme formulário do ANEXO 23.

- Unidades de fita DLT 15/30, 20/40, 35/70 e 40/80 Gbytes.
- *Softwares* – Arcserve – Computer Associates / SAPDBA – SAP.
- Periodicidade – diária.
- Ciclo de retenção do *back-up* diário – 30 dias.
- Ciclo de retenção do *back-up* semanal – 8 semanas.

- Ciclo de retenção do *back-up* mensal – 6 meses.
- Teste de recuperação (*Restore*) – mensal.
- Guarda da mídia – prédio distinto em cofre de alta segurança.
- Responsabilidade da execução e orientação – Área de Tecnologia da Informação.
- Para armazenamento das informações pertinentes a trabalho da empresa, deve-se seguir o procedimento modelo conforme ANEXO 02 deste documento, no qual determina como estas informações devem ser armazenadas nos servidores.

#### 7.5.4.2.2 *BACK-UP* DOS MICROCOMPUTADORES DOS USUÁRIOS

Nenhum tipo ou sistemática formalizada de *back-up* será destinada aos documentos armazenados nos microcomputadores pessoais de trabalho dos usuários, porém as informações contidas nestes equipamentos deverão seguir os procedimentos abaixo:

- A empresa não se responsabilizará pelas informações armazenadas nos discos dos microcomputadores pessoais, caso haja algum problema a nível de *hardware* ou *software* e que provoque a perda destas informações.
- Todas informações importantes para o usuário deverão ser armazenadas no diretório "C:\Dados" do microcomputador pessoal, pois, caso haja algum problema no equipamento, o suporte técnico tentará recuperar as informações contidas neste diretório, porém não se responsabilizando pela integridade das mesmas.

#### 7.5.4.2.3 CONSIDERAÇÕES GERAIS

Como considerações gerais sobre a implementação da Política de Segurança da Informação neste estudo de caso, é possível de se citar:

- Nenhuma informação confidencial deve ser armazenada nos microcomputadores pessoais e sim nos servidores. Toda área que necessitar de espaço nos servidores para guardar informações confidenciais deve fazer a solicitação à área de informática mediante preenchimento do formulário do ANEXO 05 e apresentar a instrução técnica da utilização da rede do departamento, conforme modelo do ANEXO 02.
- Informações não pertinentes aos interesses da empresa jamais devem ser armazenadas nos servidores e microcomputadores pessoais.

- A responsabilidade pelas informações armazenadas nos servidores é da área de Tecnologia da Informação e as informações armazenadas nos microcomputadores pessoais é do usuário. É vedada a prática de cópia dos arquivos armazenados nos computadores pessoais para as pastas de trabalho da redes, mesmo que compactados, com o intuito de execução de *back-ups* pessoais diários. Tais arquivos quando encontrados serão prontamente eliminados e a devidas gerências informadas.
- É expressamente proibido o armazenamento de informações não ligadas à atividade profissional do usuário. Qualquer informação deliberadamente inadequada (jogos, vídeos e figuras pornográficas, softwares piratas, etc.) armazenada nos servidores serão automaticamente eliminadas e o usuário responsável terá o seu acesso à rede bloqueado e receberá uma notificação conforme formulário do ANEX0 06.

#### 7.5.4.3 GRAVAÇÃO DE CD ROM E ZIP DRIVE

Nenhuma área da empresa está autorizada a ter em suas dependências unidades gravadoras de CD Rom ou de Zip Drive. A responsabilidade pela gravação de qualquer informação digital relacionada às atividades profissionais realizadas na empresa para CDR/CRRW ou ZIP Drive é da Central de Cópias (CEC), determinação estabelecida na Instrução de trabalho "Gravação de CD e ZIP Drive", conforme ANEXO 03 e utilizando-se do formulário para solicitação do serviço que consta no ANEXO 04.

#### 7.5.4.4 *INTERNET*, *INTRANET* E *EXTRANET*

- Para a utilização da Internet na Unidade de Taubaté, será disponibilizado um *link* de acesso a um provedor a ser definido, um *Proxy Server*, *softwares* (inclusive antivírus) e equipamentos de proteção *Firewall* (do provedor e da própria empresa).
- A *Internet* poderá ser disponibilizada para todo usuário que necessitarem do acesso para desenvolver suas atividades profissionais.
- Somente a Gerência da área poderá solicitar o acesso à *Internet* para seus funcionários, conforme formulário do ANEXO 07.
- Somente a área de Tecnologia da Informação poderá liberar o acesso à Internet para os usuários da empresa, sendo responsável pelo bloqueio de acessos aos Sites considerados inadequados às atividades profissionais.

- Cada usuário é responsável pela utilização correta dos recursos da Internet oferecidos pela empresa. O funcionário que utilizar os recursos de forma inadequada terá o seu acesso automaticamente bloqueado e somente poderá reavê-lo mediante uma solicitação formal da respectiva Gerência, a qual deverá justificar o acesso ou conscientizar o referido usuário sobre a correta utilização da Internet enviando uma solicitação de desbloqueio desta conta. Entende-se por utilização inadequada qualquer tentativa ou acesso a Sites não ligados à atividade profissional, sendo que a inadequação dos Sites obedece a critérios pré-definidos pela área de Tecnologia da Informação e pela respectiva Gerência do usuário.
- Somente a *Internet* disponível pela empresa poderá ser utilizada. Nenhum funcionário, terceiro ou qualquer prestador de serviços poderá utilizar os serviços de outro provedor para obter acesso à *Internet* dentro das dependências da empresa.
- É terminantemente proibido o uso de qualquer placa de fax-modem interno ou modem externo conectado a qualquer microcomputador ligado à rede de dados.
- As aplicações a serem utilizadas pelos usuários devem ser definidas de acordo com critérios próprios da área e obedecendo a critérios básicos pré-definidos pela área de Tecnologia da Informação. A definição dos critérios da área deve ser realizada pela respectiva Gerência.
- O controle de acesso aos *Sites* é de responsabilidade da área de Tecnologia da Informação, em conjunto com a Gerência de cada área. Devem ser estabelecidas quais os tipos de informações poderão ser acessados, de acordo com as necessidades profissionais de cada área.
- Será fornecida mensalmente às Gerências, uma relação contendo os *Sites* mais visitados pelos respectivos usuários.
- A liberação e o cancelamento da utilização da *Internet* é de responsabilidade de cada Gerência ou Supervisão. A área de Tecnologia da Informação deverá cancelar automaticamente o acesso de funcionários que não obedecerem às regras estabelecidas, conforme formulário do ANEXO 08 e comunicar o responsável da área que permitirá ou não o recadastramento, conforme formulário do ANEXO 09.
- *E-Mail* via *Internet* não deve ser utilizado visto que cada usuário já possui um endereço eletrônico via *Lotus Notes.* Eventuais necessidades deverão ser analisadas quando oportuno.

- O profissional deve ter a preocupação e a disciplina de utilizar a *Internet* somente para assuntos relacionados ao trabalho, tendo em vista o tempo que se mantém "navegando" pelos diversos *Sites* disponíveis e tornando sua produtividade profissional baixa.
- O *Firewall* a ser instalado será um equipamento Nokia IP 440 com o *software* Check Point, onde dentre algumas das diretrizes a serem implementadas, estará em evidência a de que todo e qualquer Site da *Internet* relacionado a sexo, assuntos sobre *Hackers*, fabricação de bombas caseiras, mensagens de *Spam* e etc. serão bloqueados. Os Protocolos que estarão liberados para trânsito de dados serão o *FTP* (Transferência de arquivos), *Telnet* (Terminal), *SMTP* (Envio de *e-mail*) e *POP3* (Post Office Protocol 3, Protocolo de Agência de Correio 3, relacionado à recepção e armazenamento de *e-mail*), porém todos eles com regras de proteção ativa.
- A *Intranet* e *Extranet* deverão seguir os princípios básicos de segurança utilizados na implementação da *Internet* e deverão ser analisados quando da implementação após a obtenção dos resultados obtidos com a implantação da *Internet*.

#### 7.5.4.5 CONTROLE DE ACESSO AOS EQUIPAMENTOS E INFORMAÇÕES

O controle de acesso é uma tarefa de responsabilidade do Administrador de Redes que deve desenvolver procedimentos para a administração dos usuários e senhas. Periodicamente deve rever as autoridades de acesso e coordenar os relatórios de verificação de trabalhos para novos projetos antes de criar e disponibilizar novos usuários. Membros de gerenciamento de sistemas de todos os níveis são orientados para informar as pessoas sobre a sua supervisão, dos procedimentos existentes. Os membros do gerenciamento são responsáveis pelas ações das pessoas que estão subordinadas àsua supervisão.

- Nenhum usuário pode se conectar a rede de dados da empresa, exceto os homologados, autorizados e monitorados pela Área de Informática.
- Todas as atividades de suporte efetuado pelos administradores dos sistemas e da rede deverão ser contabilizadas e registradas em arquivos de *logs* para futuras consultas quando se fizer necessário.
- É proibido o uso de equipamentos de *hardware* ou *software* de propriedade de funcionários na rede da empresa.

- Um novo UserID (identificação do usuário na rede) ou uma nova "conta" para acesso à rede para um novo usuário, somente poderá ser criada mediante solicitação por escrito validada pelo gerente responsável pela área solicitante, conforme ANEXO 09.
- Todos os acessos à rede de dados e correio eletrônico e servidores devem ser bem definidos e documentados para todos os usuários, conforme ANEXO 09.
- Somente os usuários homologados e monitorados pela área de informática podem ter acesso a rede de dados e aos demais sistemas de informação – SAP, BAAN, LOTUS NOTES, etc, conforme ANEXO 12.
- Para o Sistema de Gestão Integrada, SAP e BAAN, todos os usuários devem ter um perfil de acesso às transações restritas às funcionalidades para as quais foram autorizados por suas respectivas gerências, conforme ANEXO 12.
- Todas as senhas para acesso à rede ou qualquer aplicativo da empresa devem ter –- no mínimo –- oito dígitos e com a obrigatoriedade de mudança automática forçada a cada três meses.
- Bloqueio do acesso após 3 tentativas erradas (o usuário deverá abrir um chamado técnico no Help-Desk, encaminhar o formulário de "Solicitação de Desbloqueio de Acesso", conforme ANEXO 13, devidamente preenchido e a equipe de administração da rede efetuará o desbloqueio).
- As últimas seis senhas não poderão ser repetidas e o sistema deverá efetuar o bloqueio automático da conta de acesso após três tentativas inválidas.
- Após três tentativas sem sucesso de digitação da senha para acesso aos sistemas informatizados ou à rede, a conta do usuário é bloqueada automaticamente.
- As senhas para servidores devem ser trocadas, no mínimo, a cada três meses.
- O desbloqueio da conta travada somente será possível mediante o envio do formulário específico, conforme ANEXO 13, e a intervenção do Administrador da Rede, após a abertura de um chamado técnico junto à central de gerenciamento do *Help-Desk* (grupo de profissionais responsáveis por todo o suporte técnico de hardware e software para a microinformática dentro das dependências da organização).
- Somente é permitido o acesso às salas dos servidores por funcionários ou profissionais devidamente identificados e autorizados pela Gerência do Departamento de Informática.

- Cada usuário quando contratado deverá possuir uma ficha de cadastro, conforme ANEXO 09 e uma outra conforme anexo 10, a ser preenchida pela respectiva Gerência. Esta ficha deve possuir informações sobre o horário de acesso permitido ao usuário, sistemas que terá acesso – SAP, BAAN, Lotus Notes, Rede de dados, etc., período de acesso quando for o caso ou se contratado por empresa de *Outsourcing*, qual o equipamento que irá utilizar, etc. O acesso aos sistemas de informação deverá ser individual, não podendo ser compartilhados entre os usuários. Casos isolados serão analisados pela área de informática e a Gerência interessada.
- Todo usuário que, por qualquer motivo, se ausentar do seu posto de trabalho deverá se desconectar da rede, ou bloquear a estação.
- A empresa deverá providenciar a configuração dos recursos do Policy Editor, do Sistema Operacional Windows 2000, em todas as estações de trabalho do usuário, com a finalidade de desabilitar a função de "Instalar" qualquer novo aplicativo ou software, não permitir a alteração das impressoras configuradas ou efetuar qualquer mudança dos detalhes da tela do microcomputador de trabalho.
- A empresa deverá providenciar a instalação, em todos os microcomputadores de trabalho dos usuários, de um *software* para gerenciamento de rede que possa permitir efetuar um Inventário dos componentes de *hardware* e *software* existentes em cada microcomputador, e que possa também executar uma auditoria de equipamentos e produtos de rede e Identificação de duplicidade de arquivos armazenados, conforme formulário do ANEXO 11.
- Nenhum usuário deverá ter autorização para efetuar substituições de equipamentos (monitores, teclados, etc.) e/ou abrir equipamentos. Caso seja detectada uma substituição indevida, o equipamento será bloqueado e a Gerência será comunicada. A substituição de mouses, *tonner (*produto semelhante a um pó na cor preto que é utilizado em equipamentos de impressão a laser ou em máquinas copiadoras que, quando aquecido a uma temperatura ideal pelo equipamento, o mesmo torna-se afixado em folhas de papel ou transparência e gerando a imagem ou texto desejado) e cartuchos de tintas, que são consideradas exceções e, obviamente, deverão ser efetuadas pelos próprios usuários.
- Os servidores serão preparados para exigir a identificação do usuário a qualquer tempo e não apenas na entrada do sistema. Este procedimento visa

garantir que quem esteja utilizando a máquina seja realmente o usuário definido.

- O UserID é um código de identificação que será associado diretamente ao usuário, (ex.: nome) e refletirá sua ligação com a organização. Geralmente o UserID é formado pela primeira letra do primeiro nome e mais sete letras do sobrenome, resultando um código que é a "Conta para acesso" à Rede de dados, SAP, BAAN ou Lotus Notes. Sempre que um usuário for transferido para um novo trabalho, departamento, ou cargo, as autoridades de acesso para o usuário devem ser modificadas para refletir o acesso requerido pelo seu novo trabalho. UserIDs pessoais devem ser usados quando forem necessários para modificação de seus dados.
- Após o login do usuário em qualquer um dos nossos sistemas de informação (Notes, SAP e Rede) deverá haver uma mensagem citando que o usuário está acessando uma rede de informação privada, que é regida por uma norma de utilização e que, caso aceite as normas poderá prosseguir, caso contrario deverá se desconectar imediatamente. Na eventualidade de que o usuário prossiga ao acesso da rede, a partir deste momento toda a ação do mesmo poderá estar sendo monitorada e registrada.
- O acesso remoto aos recursos de informática (rede, correio eletrônico e/ou *Internet*) somente poderá ser disponibilizado aos usuários que obtiverem a autorização expressa do Comitê Executivo, conforme formulário contido no ANEXO12.
- Todos os acessos remotos serão registrados por meio de um sistema personalizado de identificação (UserID), contendo: usuário que efetuou o acesso, data e hora do acesso, telefone que originou a chamada.
- Os usuários que possuírem *notebook* como computador pessoal, deverão ser cadastrados e receberão um cartão contendo sua identificação e a do *notebook,* para ter acesso liberado nas portarias da empresa.
- Os funcionários ou contratados da empresa deverão zelar pela conservação e utilizar corretamente os equipamentos de informática que estiverem disponíveis para o exercício de suas atividades profissionais. Caso um equipamento seja danificado por mau uso ou imperícia, seus usuários serão advertidos conforme a gravidade da situação. Para os casos de funcionários, os mesmos estarão também sujeitos à rescisão do contrato de trabalho por Justa Causa, com base no artigo 482 da C.L.T.

- As senhas para servidores devem ser trocadas, no mínimo, a cada três meses.
- Mensalmente a equipe de administração de rede deverá atualizar a lista de usuários (NT, SAP, BAAN, Lotus Notes, etc.) a partir da lista de funcionários que foram desligados da empresa, recebida do GRH.
- Deverá ser adquirido um *software* para controle do inventário dos equipamentos de *hardware* e *software* pertencentes a toda a unidade da empresa em Taubaté. Este *software* deverá efetuar automaticamente o inventário, como também contribuir para a instalação automática de softwares nos microcomputadores e prover suporte para o gerenciamento da rede de dados.

#### 7.5.4.6 SEGURANÇA FÍSICA DOS EQUIPAMENTOS

- A empresa deverá prover uma sistemática de contingência para o restabelecimento dos servidores de produção, do Lotus Notes e de arquivos de projetos, em caso de desastre total, por meio de um contrato com fornecedores que permitam o retorno das funcionalidades dos equipamentos em um tempo mínimo de vinte e quatro horas.
- É proibido o uso de equipamentos de *hardware* ou *software* de propriedade de funcionários na rede da empresa.
- O local reservado para armazenamento dos cartuchos de fitas do *back-up* deverá ser localizado em um prédio geograficamente distante do local em que se encontram instalados os Servidores. Esta área deverá possuir todas as garantias possíveis de segurança (fogo, água, umidade, poeira, furto, panes elétricas, acesso restrito, etc.).
- A temperatura da sala onde se encontram os servidores deverá ser constantemente monitorada pelos profissionais de plantão e o termômetro interno deve estar sempre em perfeitas condições operacionais para acionamento automático em caso de qualquer variação da temperatura que esteja fora da faixa aceitável de 18º C até 23º C.
- A carga da bateria do *nobreak* principal deverá ser monitorada todos os dias para verificação de sua capacidade de atendimento sempre que solicitado, por meio de pane elétrica da rede principal.
- O tanque de óleo combustível, bem como os testes de funcionamento do gerador de energia elétrica devem ser monitorados todos os dias, com o

objetivo de o mesmo estar disponível e em sua plena funcionalidade operacional tão logo seja solicitado.

- Os cartuchos de fitas de *back-up* de dados deverão ser armazenados em sala cofre ou ambiente totalmente vedado, protegido contra incêndio, umidade e o local deve ser o mais longe possível da sala dos servidores.
- Nenhum microcomputador da empresa deverá possuir modem interno ou externo instalado para acessar a Internet ou qualquer serviço por meio de linha discada.
- Toda e qualquer manutenção possível de ser programada em que haja a necessidade de se tornar os sistemas computacionais indisponíveis para uso por parte dos usuários, deverá –- na medida do possível –-, ser agendada para o período noturno, finais de semanas ou feriados, com o objetivo de se minimizar os prejuízos da empresa com as paralisações necessárias.
- Todo e qualquer trabalho de manutenção ou melhoria do *hardware* ou *software* a ser executado nos equipamentos servidores da rede, deverão ser iniciados após a finalização da rotina de *back-up* completo do equipamento.
- Toda e qualquer comunicação com a *Internet* ou com serviços ligados a telecomunicações deverá ser por meio da rede de dados da empresa, para se ter garantido a proteção por meio do *Firewall* disponível.
- Os dispositivos de rede (roteadores, switches, modems, etc.) que estabelecem a comunicação entre as outras unidades da empresa deverão estar localizados na Área de Tecnologia da Informação e na Central do PABX, que também deverá estar protegida com *nobreak* e gerador de energia elétrica.
- As instalações da sala dos servidores e o local de segurança de armazenamento dos cartuchos de *back-up* deverão ser providos de um sistema de controle de acesso por serem locais restritos à equipe de suporte técnico e à Gerência da área de informática. Qualquer outro profissional somente poderá ter acesso a estas dependências com a devida autorização ou acompanhado por um dos profissionais citados.
- Como medida emergencial para suporte em caso de desastre na área de informática, a empresa mantém um contrato de segurança de *hardware* com um representante dos fabricantes de computadores, cujas cláusulas contratuais garantem o fornecimento de máquinas e possíveis consertos dos equipamentos em caráter de emergência. Nas dependências da empresa, existe uma sala com dimensões apropriadas, infra-estrutura de energia elétrica, conexões para linhas de comunicação e ar-condicionado onde será

possível a transferência dos principais equipamentos e restabelecimento em vinte e quatro horas de todas as máquinas, *restore* de dados e adequação de linhas de comunicação. Como medida extrema de segurança, caso não seja possível efetuar a montagem desta sala no tempo estimado, todos os cartuchos de fitas de *back-up* poderão ser transferidos para o Centro de Competência de Informática, localizado na unidade da empresa situada no bairro da Lapa, em São Paulo, onde estes dados serão restaurados nos servidores e todos os usuários poderão estar efetuando seus acessos remotamente.

- Todos os casos de tentativas de invasão ou comprovações de ataques à informação deverão ser relatados ao grupo gestor da segurança da informação na empresa, para que sejam executadas uma análise e verificação de penalidades ou ações cabíveis.

#### 7.5.4.7 PIRATARIA DE *SOFTWARE*

Segundo Moreira (2001), a pirataria de *software* é uma prática ilícita caracterizada pela reprodução e/ou o uso indevido de programas de computador, o *software*, que sejam legalmente protegidos, sem autorização expressa do titular da obra e sem a devida licença de uso. Cada pacote de software adquirido tem uma única licença de usuário e somente pode ser instalado em uma máquina, sendo que o ato de se copiá-lo para outro equipamento, mesmo que para uso do mesmo usuário, sem a devida licença adicional, trata-se de caso de pirataria de *software*. A pirataria individual ocorre quando há o compartilhamento de *software* entre colegas de trabalho. A pirataria corporativa ocorre quando há execução de cópias não autorizadas de *softwares* em computadores dentro da organização. A lei vigente contra pirataria de software é válida para todas as modalidades de transgressões, inclusive para a individual.

- Somente a área de Tecnologia da Informação terá autorização para a instalação de *softwares* nos microcomputadores. São considerados piratas quaisquer softwares não instalados pela área de Informática (ou por pessoas autorizadas por ela) e estes, se detectados, serão automaticamente desinstalados sem nenhum comunicado prévio. O microcomputador envolvido terá seus recursos bloqueados e chefia da área será comunicada sobre o fato, conforme formulário ANEXO 06.

- A empresa possui licenças para uso de *softwares* diversos, provenientes de fornecedores legalmente estabelecidos. Nenhum funcionário ou contratado da empresa poderá reproduzir estes *softwares* sem autorização expressa da área de Tecnologia da Informação.
- É expressamente proibido qualquer tipo de jogo nos microcomputadores.
- Os funcionários ou contratados da empresa que tomarem conhecimento do uso inadequado, de *software* ou de sua respectiva documentação que seja de propriedade da empresa, dentro ou fora de suas instalações, deverão notificar a área de Tecnologia da Informação, por meio de sua respectiva Gerência.
- De acordo com a Lei de *Software* (nº 9609/98 de 20 de Fevereiro de 1998), conforme ANEXO 31, as pessoas envolvidas em reprodução ou instalação ilegal de programas de computador ficarão sujeitas ao pagamento de indenizações por perdas e danos, correspondentes a até três mil vezes o valor de cada cópia ilegal, além de sanções penais como multas e prisões. Caso seja encontrado algum *software* irregular em um equipamento de informática da empresa, o usuário deste equipamento será considerado responsável pelo programa, inclusive perante aos órgãos fiscalizadores.
- Os funcionários ou contratados da empresa que fizerem, adquirirem, instalarem ou usarem cópias ilegais e não autorizadas, serão punidos de acordo com as circunstâncias, sendo inteiramente responsáveis pela reparação dos danos resultantes de tais atos. Quando empregados, estarão também sujeitos à rescisão do contrato de tabalho por Justa Causa, com base no artigo 482 da C.L.T.

#### 7.5.4.8 CONSCIENTIZAÇÃO DOS USUÁRIOS

- A conscientização e o treinamento dos usuários sobre a Política de Segurança da informação e suas diretrizes e critérios deverá fazer parte do processo de admissão de um novo funcionário ou contratação de prestadores de serviços. É um processo que deverá sofrer auditorias periodicamente, quando da realização das auditorias internas da área de Garantia da Qualidade. Todos os funcionários ou prestadores de serviço recém contratados deverão receber um manual (cartilha) sobre os princípios básicos da política de segurança implementada na empresa, conforme

ANEXO 15, e assinar o aditivo ao contrato de trabalho referente ao "Termo de Confidencialidade da Informação", conforme o ANEXO 14.

- É de responsabilidade do departamento de compras da empresa garantir que todas as empresas prestadoras de qualquer tipo de serviço assinarão o "Termo de Compromisso de Confidencialidade e Responsabilidade - Empresas" conforme o ANEXO 16 e seus funcionários, que prestam serviço para a empresa, também assinarão o "Termo de Compromisso de Confidencialidade da Informação - Parceiros", conforme ANEXO 18.
- Para os casos de encerramento de contrato de prestação de serviços com empresas de Terceiros, as mesmas deverão assinar o documento "Comunicado de Encerramento de Contrato de Prestador de Serviço", conforme ANEXO 19.
- Para os casos de demissões de funcionários, é necessário que o mesmo preencha o formulário específico "Comunicado de Encerramento de Conta e Demissão de Funcionário", conforme ANEXO 20 .
- É de responsabilidade do departamento de informática a confecção de material de divulgação e conscientizações periódicas desta política, "Cartilha Uma Questão de Segurança", conforme ANEXO 15.
- É de responsabilidade do *"Security Officer"* (profissional com conhecimento de Informática e que representará um grupo de usuários ou um departamento da empresa para os assuntos de segurança da informação), de cada área a conscientizar os novos funcionários e prestadores de serviço por meio do detalhamento dos princípios básicos da Política de Segurança da empresa, bem como auxiliar a área de Tecnologia da Informação enviando informações sobre novas contratações de profissionais e desligamento de outros.
- A verificação da utilização dos recursos disponibilizados pela empresa deve sofrer periodicamente uma auditoria pela área de informática mediante um comunicado prévio à Gerência da área, "Comunicado de Auditoria", conforme formulário do ANEXO 11. Esta auditoria poderá ser realizada por meio de *Softwares* de Gerenciamento de rede.
- É responsabilidade da área de Recursos Humanos a comunicação imediata à área de informática sobre a demissão de qualquer funcionário da empresa utilizando-se do formulário "Comunicado de Encerramento de Conta e Demissão de Funcionário", conforme ANEXO 20.
- É responsabilidade da Gerência do departamento contratante a comunicação imediata à área de informática sobre o encerramento do contrato do prestador

de serviços utilizando-se do formulário “Comunicado de Encerramento de Contrato de Prestador de Serviço”, conforme ANEXO 19.

- É responsabilidade dos departamentos elaborarem a sua instrução técnica de utilização da rede de dados, a conscientização e a correta utilização desta, bem como da organização das pastas de suas respectivas áreas de trabalho. Esta instrução técnica deve conter quais os níveis de acessos de seus usuários e os departamentos externos que possam ter algum tipo de acesso, utilizando-se do formulário “Modelo de Organização da Rede”, conforme ANEXO 02.
- Todos os profissionais contratados da empresa deverão também ser conscientizados pelo departamento de informática e pelos departamentos onde irão prestar serviço.
- Após o recebimento, pela área de informática, do comunicado sobre o desligamento de funcionários e/ou encerramento de contratos de serviços, todos os acessos dos envolvidos serão imediatamente bloqueados e após 15 dias do bloqueio, todos os acessos como também a conta dos usuários serão eliminados.
- Para os casos de problemas relacionados a dúvidas ou suposições de quaisquer assuntos que possam ser caracterizados como possível furto ou tentativa de invasão ou quebra da segurança da informação apresentada nesta Política de Segurança, ou mesmo para verificação de queixas por parte de funcionários que possam acusar a empresa de qualquer tentativa de invasão da privacidade da sua caixa postal do correio eletrônico, fica eleito o grupo de profissionais responsáveis pela implementação da Política de Segurança da Informação, apoiado para pela área Jurídica da empresa para analisarem e arbitrarem sobre o assunto. Caso haja a necessidade de movimentações de ações legais junto à justiça local, fica estipulado o Fórum da cidade de Taubaté para análise dos processos e julgamentos que se fizerem necessários.

#### 7.5.4.9 ENTRADA E SAÍDA DA INFORMAÇÃO

- A portaria da empresa poderá aleatoriamente solicitar que lhe seja identificado qualquer tipo de documentação, escrita ou em meio magnético, que possa retratar uma suspeita de saída de informação, no momento em que qualquer profissional estiver se ausentando empresa. Em caso de ser

escolhido, o profissional deverá se dirigir a uma sala e abrir sua bagagem, deixando à vista do vigilante o conteúdo interno. Todas as vezes que um determinado profissional estiver que sair das dependências da empresa levando consigo alguma informação da empresa em papel ou meio magnético, seu superior imediato deverá enviar um *e-mail* à portaria informando da permissão para porte de tais objetos. Caso o profissional não tenha este documento, o mesmo somente poderá se ausentar da empresa, com as informações, mediante autorização por *e-mail* de um dos seus superiores a serem acionados na ocasião.

- Todos os visitantes e funcionários (com exceção dos funcionários que já tenham cadastrado o *notebook*), que entrarem à empresa com qualquer tipo de equipamento de informática, *notebook*, disquetes, CD rom e outros, deverão registrá-los na portaria. Os usuários não cadastrados, que necessitarem sair da empresa com algum equipamento de informática, deverão encaminhar autorização formal via *e-mail* à Segurança Patrimonial, por meio da sua Gerência, detalhando a identificação do portador, características e identificação do equipamento e as datas de saída e retorno.
- Todo documento impresso oficial para saída da empresa, somente será confeccionado pela Central de Cópias e deverá ser solicitado pelo controle de documento do SAP.

#### 7.5.4.10 POLÍTICA DE SEGURANÇA NO CORREIO ELETRÔNICO (*E-MAIL*)

Segundo Overly (1999), muitos dos problemas existentes nas empresas, principalmente relacionados com as leis e penalidades, computadores e funcionários estão ligados ao uso do correio eletrônico, o *e-mail*. O correio eletrônico é uma revolução no meio de comunicação entre as pessoas, entre as empresas e organizações em geral. Devido a sua influência, atuação em uma maioria das companhias, universidades, órgãos governamentais e a seu dinamismo, como também à sua rapidez na comunicação, facilidade de uso e baixo custo, o *e-mail* pode ser considerado o maior foco de atuação para a difusão de vírus de computador, como também para a atuação de mensagens com a intenção de se provocar lentidão na Internet e nas redes das corporações em geral. O número de mensagens de *e-mail* circulando por hora na Internet é alarmante, ultrapassando a média de um milhão de mensagens. Estimativas efetuadas apontaram para um total aproximado de 2,7 trilhões de mensagens enviadas no ano de 1997, cerca de sete trilhões no ano 2000 e, numa grande parte destas

mensagens, o assunto não tinha ligação aos negócios das empresas e sim com pornografia, correntes de mensagens e mensagens do tipo *Spam* e *Hoax*, com o único objetivo de tornar mais lenta a comunicação das redes. Como vantagem do uso do e-mail nas organizações, pode-se citar a eficiência, a velocidade e a economia que se consegue com a comunicação entre os profissionais –- na tomada de decisão –- e na agilidade do fluxo das informações. O fato de o profissional ter acesso à sua caixa postal do correio eletrônico na empresa, como também de sua residência, criou no indivíduo um hábito de estar sempre conectado à Internet, verificando se recebeu alguma mensagem nova, respondendo aos e-mails recebidos e tomando ações e decisões particulares, como também relacionadas ao trabalho, em nome do negócio da empresa em qualquer momento e sem barreiras geográficas.

Desta maneira, o e-mail é um item tão importante, frágil e merecedor de atenção quanto à implementação de recursos de segurança da informação, como qualquer outro dispositivo da rede de dados. Ele é uma porta de entrada para vírus dos mais diversos tipos e ameaçadores da segurança da informação corporativa. O e-mail é, sem sombra de dúvida, uma ferramenta estratégica da empresa no tocante à sua agilidade de comunicação e de apoio à tomada de decisão, com característica de ser rápido, preciso e eficiente. As mensagens que saem do ambiente de uma empresa até chegarem a uma filial localizada em outro município, estado ou país utilizam as redes e recursos de comunicação e telefonia fornecidos pelas provedoras existentes no mercado, tais como Embratel, Intelig e Telefônica, ou seja, num determinado momento um *e-mail* com arquivo anexado está trafegando pelas linhas públicas juntamente com dados de outras empresas e, apesar da existência de toda uma tecnologia própria para segurança da informação fornecido por estas provedoras, como, por exemplo, o *Firewall*, é de caráter imprescindível que as empresas tenham suas próprias Políticas de Segurança implementadas, para garantir que uma possível falha na segurança da provedora não desencadeie um processo de invasão e destruição de seus dados internamente.

Segundo Pimenta (2001), em poucos anos, o *e-mail* tornou-se um dos mais eficazes meios de comunicação mundial entre as empresas e as pessoas, ultrapassando uma série de limitações e trazendo inúmeros benefícios, principalmente quando se refere aos gastos expressivos em correio convencional e em contas telefônicas. Seguindo os princípios de qualquer tecnologia, existem aspectos que precisam ser avaliados. No caso desta pesquisa, o foco está diretamente no aspecto de segurança, ou seja, na proteção das informações trafegadas, no *e-mail* com arquivo anexado, no comportamento dos usuários e na criação de mecanismos utilizados para minimizar os riscos envolvidos no processo de comunicação via *e-mail*.

O correio eletrônico tanto pode ser um processo de comunicação com alto poder construtivo, encurtando as distâncias e facilitando a interação entre as empresas, as universidades e as pessoas, quanto pode ser destrutivo, quando o ambiente computacional se encontra vulnerável a ação de pragas eletrônicas, comprometendo os três pilares da segurança da informação: confidencialidade, integridade e disponibilidade. Atualmente, qualquer negócio que tenha por objetivo alcançar resultados positivos, visando lucro ou sucesso e progresso no seu ramo de atuação, seja em pesquisas ou fabricação de qualquer produto, está apoiado em informações, muitas vezes estratégicas, que trafegam em sua maior parte por meio eletrônico. Sendo assim, a criação de uma Política de Segurança deve seguir alguns critérios. Alguns resultados das 6ª e 7ª pesquisas nacionais de segurança da informação realizadas pela empresa Módulo (www.modulo.com.br), mostraram que:

- O fator consciência é considerado por 58% dos entrevistados como principal obstáculo para implementação de segurança num ambiente corporativo.
- Aproximadamente 53% das empresas apontam os funcionários insatisfeitos como a maior ameaça àsegurança da informação nas empresas.
- A falta de orçamento necessário é responsável por cerca de 32% dos obstáculos àimplantação da Política de Segurança.
- Cerca de 21% dos problemas estão relacionados à escassez de recursos humanos especializados, além da falta de ferramentas adequadas e de apoio especializado, ambos citados por 13% dos entrevistados.
- Cerca de 31% dos funcionários são responsáveis pelos problemas de segurança.
- Os principais pontos de invasão são os sistemas internos (41%) e a *Internet* (38%).
- **Vírus propagados via *e-mail* atingiram mais de meio bilhão de computadores no mundo inteiro em tempo recorde.**
- Aumento de incidência de vírus do tipo de *Trojan Horses* (Cavalo de Tróia), programas maliciosos que se disfarçam como partes de sistemas para roubar senhas e outras informações.
- Aproximadamente 66% das empresas pesquisadas afirmaram possuir uma Política de Segurança da Informação implantada, porém em 19% a Política está desatualizada.

É necessário definir alguns critérios a serem aplicados –- como precaução e ação –- para que se possa proteger as informações com eficiência. O uso inadequado do *e-mail* no ambiente corporativo traz conseqüências muitas vezes catastróficas, ocasionando ações predatórias aos sistemas e às informações. Como pensar em segurança aplicável ao uso do *e-mail* se sua proteção está ligada diretamente ao comportamento do usuário? Como diferenciar um *e-mail* contendo um arquivo em anexo (*attach*) comum de um *e-mail* contendo um arquivo anexado com um vírus altamente destrutivo?

O usuário, ao qual se deve confiar todas as informações corporativas, muitas vezes está inconsciente dos riscos, das ameaças e das vulnerabilidades inerentes a este ambiente. Para que a Política de Segurança em *e-mail* tenha eficiência, é necessário observar-se alguns cuidados quando da sua criação. Quando se pensa em Política de Segurança, deve-se atentar para que não falte o que pode ser considerado como o mínimo para que se possa criar a espinha dorsal que irá dar subsídios na elaboração, tanto da estratégia quanto da tática, e também da sistemática operacional a serem aplicadas, conforme referenciado na Figura 25.

**a) O que é obrigatório na elaboração do conteúdo?**

- Ser simples e objetivo.
- Definir que todo e qualquer recurso disponibilizado para trabalho é de propriedade da organização, inclusive o *e-mail*.
- A informação trafegada, ou seja, em trânsito pela organização é patrimônio da empresa.

**b) Qual será o alvo?**

Figura 25 – Esquema Alvo da Política de Segurança em *E-mail*

Fonte: Pimenta, Cristiano. (2001).

É necessário avaliar sob os aspectos estratégico, tático e operacional, quais serão as ações que deverão ser aplicadas na elaboração da Política da Segurança, para que esta possa atingir todos os níveis da organização. O alvo a ser protegido é a informação, que deve estar protegida por recursos e sistemáticas implementadas na Política, com responsabilidade, baseada em ferramentas implementadas via *software,* que seja baseada nas leis vigentes do estado, do país e que tenha um caráter internacional, contudo ela deve ser restritiva com relação aos acessos e se basear fortemente na conscientização do usuário, conforme esquema da Figura 26.

**c) O que deve ser abordado?**


Figura 26 – A Abordagem da Política de Segurança em *E-mail*

Fonte: Pimenta, Cristiano. (2001).

Um conjunto de elementos devem ser considerado para uma efetiva utilização e controle do *e-mail* corporativo, como: legalidade, responsabilidades, restrições de acesso, implementação de software e conscientização dos usuários.

**d) Qual estrutura básica a ser utilizada na criação da política?**

- Introdução
  - Objetivos Principais
  - Uso da mensagem do *e-mail*
  - Condições para configuração, manutenção e uso do *e-mail*
    - Identificação do usuário
    - Conta, senha e segurança
    - Comunicação externa
    - Conduta do usuário
      - Diretrizes Gerais
      - Diretrizes Específicas
      - Diretrizes Especiais
    - Análise de incidentes de segurança observados
- Responsabilidades

**e) Quais são as regras básicas a serem aplicadas?**

- Aspectos Gerais

  Caso o *e-mail* seja a principal ferramenta de comunicação da organização, seu uso deve estar baseado nas premissas de cordialidade, civilidade, eficiência e agilidade, sempre objetivando aumentar a produtividade nos trabalhos diários.
- Recomenda-se proibir o uso do *e-mail* corporativo para a divulgação de boatos, informações não confirmadas, campanhas políticas, venda de produtos de terceiros, oferecimento de vantagens ou divulgação de software não oficial da organização.
- O usuário deve ser o único responsável pelo conteúdo das transmissões feitas por meio do *e-mail* a partir de sua senha ou conta.
- Aspectos Específicos
  - Não utilizar o *e-mail* para fins ilegais.
  - Não interferir ou interromper o serviço de *e-mail* dos servidores ou redes conectadas.
  - Cumprir todos os requerimentos, procedimentos, políticas e regulamentos.
  - Não transmitir quaisquer materiais ilegais ou de qualquer forma censuráveis por meio do serviço.

- Não transmitir qualquer material que viole direitos de terceiros, incluindo, mas sem limitação, direitos de propriedade intelectual.
- Não transmitir qualquer material que viole qualquer lei ou regulamentos locais, estaduais, nacionais ou internacionais aplicáveis.
- Não obter ou tentar obter acesso não-autorizado a outros sistemas ou redes de computadores conectados ao serviço.
- Não utilizar os serviços para transmitir quaisquer materiais que contenham vírus, arquivos do tipo "Cavalo de Tróia", ou outro programa prejudicial à informação.
- Não transmitir mensagens não-solicitadas, conhecidas como *Spam* (mensagens não solicitadas, tipo propaganda), *Hoax* (mensagem que conta uma estória mentirosa, como por exemplo, vírus por *e-mail*) ou *Junk Mail* (*e-mail* não autorizado e enviado em larga escala), correntes *Chain Letters* (cartas e mensagens normalmente longas enviadas a um grande número de usuários e sempre solicitando que a mesma seja enviada a um outro grupo de usuários com o intuito de congestionar as redes de dados), ou distribuição em massa de mensagens não-solicitadas.

**e) Alguns Cuidados Especiais**

- O *e-mail* deve estar ativo e disponível sempre que o usuário estiver trabalhando no microcomputador. Quando se afastar deverá encerrar a sessão ou acionar recurso de proteção de tela com senha pessoal.
- As mensagens do *e-mail* são confidenciais, portanto, somente podem ser acessadas pelo remetente e seu(s) destinatário(s). Deve-se proibir a leitura de mensagens de outros usuários, mesmo que estejam abertas na tela. Quaisquer leituras indevidas e injustificadas de mensagens de outros usuários serão tratadas conforme as normas da empresa e a legislação em vigor.
- Mensagens com assuntos confidenciais não deverão ser impressos em equipamentos corporativos utilizados por vários usuários.
- As mensagens já lidas, ou sem utilidade, devem ser apagadas regularmente.
- Deve ser terminantemente proibido aos administradores de rede ou do correio eletrônico acessar ou ler as mensagens de qualquer usuário, mesmo em serviços de manutenção e suporte.

#### 7.5.4.10.1 TÓPICOS ABORDADOS PELA POLÍTICA (*E-MAIL*)

Tendo ciência dos problemas citados acima a empresa tomou a decisão de implementar sua Política de Segurança da Informação abordando os tópicos abaixo –- em complemento aos tópicos anteriores –-, específicos para o correio eletrônico (*e-mail*):

- O correio eletrônico é uma ferramenta fornecida pela empresa para uso dos funcionários em caráter profissional, sendo que todas as informações contidas nas caixas postais dos usuários são de propriedade intelectual da empresa.
- Toda informação eletrônica que circular na empresa deverá ter relação com a atividade profissional do usuário e, desta forma, toda a utilização destes recursos estará sendo monitorada pela Área de Tecnologia da Informação por meio de software específico e da análise dos administradores de rede.
- Ao receber informações não relacionadas à sua atividade profissional, o usuário não deve, em hipótese alguma, arquivar esta informação nos equipamentos e/ou dispositivos da empresa (Servidores, Microcomputadores, CD Rom, disquetes, etc.).
- Mensagens contendo correntes, piadas ou material pornográfico de qualquer espécie, que possam ser interpretadas como ofensivas, obscenas ou em desacordo com as normas da empresa ou, ainda, que possam ferir a ética profissional, são terminantemente proibidas. Caso o usuário receba algum *e-mail* desta espécie, deverá excluí-lo imediatamente. Em hipótese alguma, o usuário deverá arquivá-lo ou retransmitir para outras pessoas.
- A responsabilidade pelo arquivamento das informações divulgadas entre os funcionários da empresa é do usuário que gerou a documentação. Sempre que possível, o usuário deve evitar arquivar informações recebidas, eliminando assim, duplicidade de arquivos. Este item não se aplica às informações recebidas de pessoas externas à empresa, cabendo ao destinatário analisar a necessidade ou não do arquivamento. Todo arquivamento deve ser realizado de acordo com a necessidade ou não de *back-up* e conforme a confidencialidade das informações.
- O usuário não deve abrir arquivos anexados a um *e-mail* que tenham sido recebidos de fonte desconhecida, não confiável, que tenham título suspeito

ou com as extensões .exe, .com, .wav. ou .avi. Normalmente arquivos com estas extensões são contaminados facilmente por vírus.

- Após receber e analisar informações recebidas, o usuário deve eliminá-las ou arquivá-las, não as deixando acessíveis em seu local de trabalho ou disponíveis em sua caixa postal. Arquivos anexados e recebidos via *e-mail* não devem permanecer na caixa postal do usuário e sim desanexados e arquivados conforme a necessidade. O processo de arquivamento das informações deve ser realizado de acordo com o grau de confidencialidade da informação e conforme as considerações colocadas no item sobre *back-up*.
- As informações ou arquivos anexados recebidos não poderão ser copiados e/ou alterados sem a prévia autorização do emitente. Desta maneira, para informações sigilosas, recomenda-se utilizar os recursos de criptografia e proteção para a mensagem, recurso do correio eletrônico.
- A distribuição das informações deve ser efetuada de forma criteriosa e somente para os usuários envolvidos no assunto, ou seja, deve ser evitado o envio de *e-mails* de forma genérica para todos os usuários da empresa.
- As informações armazenadas em qualquer equipamento e/ou dispositivo somente podem ser acessadas e/ou distribuídas pelo responsável das informações e seus respectivos superiores hierárquicos.
- Caso algum usuário contrarie os princípios de segurança previstos neste documento, imediatamente e automaticamente serão bloqueados todos os recursos computacionais que o mesmo possuir e será comunicado à sua respectiva Gerência, conforme ANEXO 06. Somente a Gerência do usuário poderá autorizar o desbloqueio dos recursos, conforme ANEXO 13, ou caso necessário, solicitar uma auditoria nas informações do usuário conforme ANEXO 11.
- Toda informação confidencial distribuída por meio eletrônico deverá ser previamente protegida (senhas, criptografia e proteção contra cópias). A execução desta proteção é de responsabilidade do usuário com orientação da área de informática. Os recursos para realizar esta proteção estão disponíveis para todos os usuários que necessitarem. Quaisquer necessidades de orientação sobre a utilização destes recursos podem ser obtidas mediante a abertura de um chamado técnico junto àequipe de suporte técnico para a Microinformática, o *Help-Desk*.
- A confidencialidade das informações deve ser analisada pela área detentora da informação quanto ao impacto da mesma ser obtida por outros usuários,

seja internamente à área, externamente e/ou externamente à empresa. A distribuição de informações confidenciais somente poderão ser feitas mediante autorização prévia do responsável pelas informações e seus respectivos superiores hierárquicos

- O arquivamento das mensagens enviadas ou recebidas será efetuado em um servidor específico para esta função, tendo como limite máximo de 120 Mb por usuário, impedindo o arquivamento de novas mensagens que excedam o limite máximo de arquivamento.
- No servidor de correio eletrônico da empresa está instalado o *software* antivírus Groupshield, da empresa McAfee que verifica a existência de vírus nas mensagens recebidas, assim como monitora e impede o recebimento de arquivos anexados cujo conteúdo não seja de utilização exclusivamente profissional.
- O correio eletrônico deverá ser configurado e otimizado, ao nível de *software*, para que toda e qualquer mensagem que tenha arquivo anexado cujo tamanho esteja entre 2 Mb e 4 Mb, fique bloqueada em modo de espera e somente posa continuar trafegando pela rede durante o período compreendido entre 22:00 horas e 05:00 horas. Arquivos com tamanho que exceda 4 Mb não serão transmitidos, ficando na caixa postal de saída do servidor pelo tempo de uma hora em modo de espera, aguardando uma ação do Administrador do correio eletrônico, após o mesmo ter recebido uma mensagem de alerta sobre o fato. Após uma hora, a mensagem é excluída automaticamente da caixa postal de saída do servidor, sendo que tanto o Administrador quanto o usuário emitente da mensagem são informados desta exclusão.
- O *e-mail* deve estar ativo e disponível sempre que o usuário estiver trabalhando no microcomputador. Quando se afastar deverá encerrar a sessão ou acionar recurso de proteção de tela com senha pessoal.
- As mensagens do *e-mail* são confidenciais, portanto, somente podem ser acessadas pelo remetente e seu(s) destinatário(s). Deve-se proibir a leitura de mensagens de outros usuários, mesmo que estejam abertas na tela. Quaisquer leituras indevidas e injustificadas de mensagens de outros usuários serão tratadas conforme as normas da empresa e a legislação em vigor.
- Mensagens com assuntos confidenciais não deverão ser impressas em equipamentos corporativos utilizados por vários usuários.

- Deve ser terminantemente proibido aos administradores de rede ou do correio eletrônico acessar ou ler as mensagens de qualquer usuário, mesmo em serviços de manutenção e suporte.
- É estritamente proibido o uso dos computadores da empresa para:
    - Enviar, receber, efetuar *download*, visualizar, imprimir, distribuir ou disseminar qualquer material pornográfico, profano, obsceno, fraudulento, de racialmente ofensivo, difamatório ou contrário às leis vigentes.
    - Disseminar ou armazenar assuntos pessoais do tipo propaganda comercial, promoções de lojas, programas destrutivos, principalmente que contenham vírus ou código de replicação automática, material de propaganda política ou qualquer outro material não autorizado.
    - Efetuar assinatura de qualquer lista de *e-mail* com recepção automática, ficar um tempo excessivo conectado à *Internet* sem necessidade de se estar a trabalho, utilizar-se de jogos de computador, fazer parte de grupos de discussão da *Internet*, imprimir várias cópias de um mesmo documento e criar tráfego desnecessário na rede.
    - Uso de licença ou instalação de *softwares* que tenham sido copiados de algum *Site* da *Internet*, que tenha sido recebido por *e-mail* ou que possa violar os acordos de utilização.
    - Violação de leis estaduais, federais ou internacionais sobre *e-mail*.
    - A divulgação de boatos, informações não confirmadas, campanhas políticas, venda de produtos de terceiros, oferecimento de vantagens ou divulgação de *software* não oficial da organização.
    - Disponibilizar sua senha de acesso a outros, ou seja, o usuário deve ser o único responsável pelo conteúdo das transmissões feitas por meio do *e-mail* a partir de sua senha ou conta.
    - Utilizar o *e-mail* para fins ilegais.
    - Ao usuário interferir ou interromper o serviço de *e-mail* dos servidores ou redes conectadas.
    - Não respeitar o limite máximo para se anexar um arquivo a um *e-mail* a ser enviado é de 4 Mb e este limite é necessário para se evitar mensagens de grande porte provocando lentidão ao sistema de correio eletrônico corporativo.

- Não cumprir as normas, requerimentos, procedimentos, políticas e regulamentos adotados sobre as normas do correio eletrônico.
- Enviar quaisquer materiais ilegais ou de qualquer forma censuráveis por meio do serviço disponibilizado pela empresa.
- Transmitir qualquer material que viole qualquer lei ou regulamentos locais, estaduais, nacionais ou internacionais aplicáveis a *e-mail*.
- Obter ou tentar obter acesso não-autorizado a outros sistemas ou redes de computadores conectados ao serviço.
- Utilizar os serviços para transmitir quaisquer materiais que contenham vírus, arquivos do tipo "Cavalo de Tróia", ou outro programa prejudicial àinformação.
- Transmitir mensagens não-solicitadas, conhecidas como *Spam*, *Hoax* ou *Junk Mail*, correntes *Chain Letters*, ou distribuição em massa de mensagens não-solicitadas.
- Deve-se desconfiar de quaisquer arquivos anexados a mensagens de *e-mail* que não estejam sendo esperados, mesmo que provenientes de pessoas ou organizações de sua confiança. Havendo qualquer dúvida de que o arquivo possa conter vírus, assuma que ele o contém e adote as medidas necessárias, tanto entrando em contato com a pessoa que supostamente enviou a mensagem para se certificar do motivo do envio do arquivo anexado, quanto executando *software* antivírus para se assegurar do não contágio.
- Não se deve dar seqüência a quaisquer correntes de alerta contra novos vírus. Em geral, tais correntes servem apenas para atemorizar pessoas que, inocentemente, propagam a mensagem de alerta para inúmeras outras pessoas, causando perda de produtividade e congestionamento das redes. No ambiente corporativo, envie tal mensagem de alerta tão somente para o departamento de suporte, que avaliará as medidas que, eventualmente, tenham que ser tomadas.

#### 7.5.4.11 PROTEÇÃO CONTRA VÍRUS DE COMPUTADOR

A preocupação das organizações e empresas em geral com a perda de dados provocados por contaminações de vírus tem sido uma constante.

Abaixo se apresenta a Tabela 15 com o Ranking dos Vírus Mais Ativos no mês de Outubro /2001.

Tabela 15 – Ranking dos Vírus Mais Ativos no mês de Outubro/2001

| **RANKING DOS VÍRUS MAIS ATIVOS (OUTUBRO/2001)** | | |
|---|---|---|
| **POSIÇÃO** | **NOME DO VÍRUS** | **AÇÃO** |
| 1º | W32 / SIRCAM – A | 21,7 % |
| 2º | W32 / NIMDA – A | 17,8 % |
| 3º | W32 / MAGISTR – B | 16,1 % |
| 4º | W32 / MAGISTR – A | 9,2 % |
| 5º | W32 / HYBRIS – B | 6,6 % |
| 6º | VBS / MTX | 1,3 % |
| 7º | SADMIND / IIS | 1,9 % |
| 8º | W32 / MTX | 1,3 % |
| 9º | W32 / VERONA - B | 1,2 % |
| 10 | VBS / HAPTIME - A | 1,0 % |
| -- | OUTROS | 20,7 % |

Fonte: *Ranking dos Vírus Mais Ativos*. (2001).

Segundo Vírus E Cia. (2001), o que normalmente são chamados de "vírus de computador" são programas que possuem algumas características em comum com os vírus biológicos, ou seja, são pequenos. Um vírus, por definição, não funciona por si só, ele deve infectar um arquivo executável ou arquivos que utilizam macros, ou seja, em geral fica escondido dentro da série de comandos de um programa maior, contém instruções para parasitar e criar cópias de si mesmo de forma autônoma, automática e sem autorização específica e, na maioria das vezes, sem o conhecimento do usuário para isso, e eles são, portanto, auto-replicantes.

Com relação à infecção, há várias manifestações visíveis da atividade dos vírus, ou seja, mostrar mensagens, alterar ou excluir determinados tipos de arquivos, corromper a tabela de alocação, diminuir a performance do sistema ou até formatar o disco rígido. Muitas vezes a ação de um vírus só se inicia a partir de eventos ou condições que seu criador pré-estipulou, que normalmente se manifesta quando atingir uma certa data, um número de vezes que um programa é processado, quando um comando específico é executado, etc. Um vírus pode

atingir um computador a partir de diferentes "vetores" todos previamente infectados: documentos, programas, disquetes, arquivos de sistema, etc. Arquivos executáveis (com extensões do tipo .exe, .bat, .com) são particularmente perigosos e deve-se evitar enviá-los ou recebê-los. Após infectar o computador, eles podem passar a atacar outros arquivos. Se um destes arquivos infectados for transferido para outro computador, o vírus vai junto e, quando for executado irá contaminar a segunda máquina e, desta maneira, o processo se repete indefinidamente. Arquivos de dados, de som (.wav, .mid), de imagem (.bmp, .pcx, .gif, .jpg), de vídeo (.avi, .mov) e os de texto que não contenham macros (.txt, .wri) podem ser abertos sem problemas, mas tanto o processo de *download,* como o serviço de correio eletrônico *e-mail* possibilitam a entrada de arquivos no computador. Desta maneira, a *Internet* se tornou um grande foco de disseminação de vírus, *Worms*, *Trojans* e outros programas maliciosos, por facilitar em muito o envio e recepção de arquivos, fato que no passado era feito basicamente por meio de disquetes.

Como um dos mais populares serviços da *Internet* é o correio eletrônico, o envio de programas invasores por *e-mail* é preocupante. Como regra geral pode-se assumir que não se deve executar arquivos recebidos por *e-mail*, especialmente os arquivos que são executáveis (.exe, .com), a menos que se conheça o remetente e que se tenha certeza que ele é cuidadoso e usa antivírus atualizado, mas na quase totalidade dos casos pode-se admitir que a simples recepção e a visualização de uma mensagem não contamina o computador receptor. Recentemente surgiu um novo tipo de *Worm*, que se propaga por *e-mail* e não necessita de arquivos anexados. É o *Bubbleboy,* que efetua acontaminação apenas pela abertura da mensagem de correio eletrônico, que felizmente, tem ação restrita a alguns programas.

Para auxiliar e para minimizar os problemas de contaminação por vírus, a alternativa existente no mercado é o uso de ferramentas antivírus, que são softwares desenvolvidos com o objetivo de rastrear, proteger de contaminação e eliminar possíveis contaminações de vírus existentes em arquivos de dados ou em computadores. Atualmente, muitos desses programas não são apenas antivírus, mas também tem atividade antitrojan, antiworm e antibackdoors. É absolutamente necessário instalar um deles, ou mais que um no computador, e atualizá-lo freqüentemente. Felizmente existem vários programas antivírus bons e gratuitos disponíveis na *Internet*, sendo que o importante é notar que o uso de antivírus exige sempre algumas outras medidas de prevenções e cuidados.

Segundo Corrêa (1001), sobre o vírus “I LOVE YOU’, recentemente divulgado, ele foi criativo e grande "marqueteiro". Esses são os primeiros adjetivos que definem o inventor da carta de amor mais lida do mundo nos últimos tempos. O autor, que assina Spyder, fez com que um vírus muito parecido com diversos outros já distribuídos pela *Internet* tivesse uma velocidade de propagação estrondosa, nunca antes conseguida. E não foi pelo poder letal do vírus, mas sim pelo *marketing* do "I love You". O dia após a infecção, já chamado "Bug do Amor" proporcionou oportunidade para que as pessoas brincassem umas com as outras, afinal as equipes de Tecnologia da Informação e de segurança agiram, na maioria dos locais, com rapidez. O mundo não acabou e os microcomputadores atacados já estavam desinfectados. A mídia trouxe diversas histórias hilariantes de pessoas que receberam a carta do amor. Quem esteve no centro do furacão não teve muitos motivos para achar graça. Diversas organizações privadas e governamentais pelo mundo todo tiveram seus correios eletrônicos paralisados durante a onda de contaminação. Uns como opção de defesa, outros pelo volume gigantesco de *e-mails* circulando em seus servidores. Segundo estimativas, o valor do prejuízo causado pelo Vírus do Amor pode chegar a dez bilhões de dólares. Este valor é pequeno quando comparado com as verdadeiras conseqüências que esse vírus ainda poderá trazer para toda a *Internet*. O vírus I Love You é um vírus didático. O código está em texto claro, ou seja, é legível por qualquer pessoa. Com um pouco de conhecimento, novas variantes serão produzidas. Já existem inclusive, três variantes em português.

Apesar de ter deixado de ser o foco de atenções dos problemas da *Internet*, os vírus (incluindo *Worms* e *Trojan Horses*) nunca deixaram de ser um problema constante para os administradores de rede e de segurança de informação. Pesquisa recém publicada pelo CSI (Computer Security Institute) em conjunto com o FBI (San Francisco Federal Bureau of Investigation"s Computer Intrusion Squad) mostra que, apesar de 100% das empresas entrevistadas usarem antivírus, 70% delas foram contaminadas no último ano. A média de perdas financeiras por cada contaminação foi de US$ 61.729. Algumas empresas reportaram prejuízos de até dez milhões de dólares numa única contaminação. Apesar de perdas financeiras tão altas e problemas de segurança significativos, o combate aos vírus é um dos mais fáceis e baratos de serem feitos. É fácil perceber pelo resultado da pesquisa CSI/FBI que não basta adquirir um antivírus. Como qualquer outra tecnologia de segurança, os antivírus são somente o elemento de reforço de uma Política de Segurança.

A solução não pode ser pontual. Os vírus sempre andaram na frente dos antivírus. A velocidade com que se propagam hoje torna essa dianteira extremamente perigosa, já que, em qualquer lugar do mundo, eles chegam antes do antídoto. É preciso definir o

modelo de gestão de segurança no combate a vírus. Além do tradicional modelo de ter o antivírus habilitado nas estações de trabalho e buscar as atualizações com o fornecedor do software, é preciso dar um tratamento melhor para o que é hoje a principal porta de acesso dos vírus –- *o e-mail* –- definindo uma Política de uso claros para os usuários e administradores. Não é difícil nem tem um custo elevado manter o ambiente corporativo livre de vírus, *Worms* e *Trojan Horses*. Para tanto, basta uma definição clara do modelo de gestão da segurança, sustentada por uma Política de Segurança antivírus e por *softwares* que garantam e reforcem essa Política, somadas a campanhas de conscientização devem ser uma constante para formar uma cultura nos usuários.

Existe um outro vírus agindo atacando as contas de correio eletrônico com grande poder de atuação e dissemi nação, o *Worm* Gone, também conhecido como Goner, que continua se disseminando com grande velocidade pela *Internet*. Este Worm foi descoberto na Terça-feira 04/12/2001 e já infectou mais de 100 mil computadores. No ambiente corporativo, atingiu mais de 160 empresas em todo o mundo. Os países mais atingidos são França, Alemanha, Reino Unido e Estados Unidos. No Brasil, as empresas de antivírus já contabilizam pelo menos 4 mil estações de trabalho contaminadas.

A praga chega por *e-mail* em uma mensagem que fala sobre um *screensaver* (pequenos programas com animações e que são utilizados com proteção de tela para microcomputadores), e vem com o arquivo Gone.scr anexado. Ao ser executado, o vírus mostra uma janela com informações sobre os autores do vírus e cria uma chave de registro com o arquivo Gone.scr, para que ele seja ativado toda vez que o usuário ligar o microcomputador. Segundo a empresa Symantec, o Goner –- além de enviar mensagens infectadas para todos os usuários cadastrados no catálogo de endereços do Microsoft Outlook –-, também apaga o *software* Norton Antivirus, deixando o equipamento vulnerável. As empresas de antivírus também descobriram que a praga danifica diversos outros arquivos –- incluindo programas de *firewall* –- e instala um programa de *backdoor*, destinado a abrir o computador da vítima para ataques de *Hackers*.

O Goner está sendo considerado pelos especialistas das empresas antivírus, como o vírus com maior velocidade de disseminação até o momento. O laboratório de pesquisa da McAfee, por exemplo, identificou cerca de 50 mil *e-mails* infectados em apenas 25 minutos. O Nimda, outra praga que se espalhou rapidamente, demorou 24 horas para gerar 100 mil mensagens contaminadas, segundo a companhia. No Brasil, a McAfee já recebeu comunicados de contaminação em 81 empresas. Para combater ou remover o Goner, as principais companhias de antivírus disponibilizaram vacinas e instruções para ajudar os usuários. Uma das maneiras de se evitar a contaminação pelo Goner, é

executar a recomendação de que, em ambiente corporativo, sejam bloqueadas as mensagens com extensão .scr.

Segundo a empresa Módulo Security Solutions (2) (2001), a contaminação por vírus de computador estava em terceiro lugar dentre as principais ameaças às informações da empresa e o ano de 2001 foi considerado pelos especialistas em segurança de redes de computadores como o pior ano em matéria de vírus , sendo que o mês de Dezembro foi o pior mês, o que se pode esperar para 2002? A previsão de especialistas é que surjam novos vírus, com uma capacidade destrutiva ainda maior do que vista neste ano. Os criadores de vírus já descobriram que é fácil ter sucesso em anexos de *e-mails* que prometem, por exemplo, fotos sensuais da tenista russa Anna Kournikova, ou em anexos que se disfarçam de pesquisas sobre a guerra do Afeganistão. O ano de 2001 também foi marcado por vírus de ação múltipla, como o Nimda, que se espalha por *e-mail* e também ataca *Sites* e servidores do correio eletrônico. Para Vincent Gullotto, diretor da divisão antivírus da Network Associates, o ano novo trará mais vírus que atacam páginas da *Internet*, infectando os visitantes. Já George Samenuk, o presidente-executivo da Network Associates, acredita que a próxima onda de ataques ocorrerá em aparelhos sem fio e não em microcomputadores comuns. "Menos de cinco por cento dos aparelhos sem fio possuem software antivírus, enquanto os administradores das redes tradicionais estão realmente se protegendo", afirmou Samenuk. Gullotto diz que os vírus de "scripts", que são trechos de códigos de programação, serão muito comuns e se espalharão pelos sistemas de mensagens instantâneas de telefones celulares. "Você pode tirar um telefone do ar enviando um “script” “ desses, afirmou o especialista.

#### 7.5.4.11.1 TÓPICOS ABORDADOS PELA POLÍTICA (VÍRUS)

Alguns tópicos são importantes e devem ser abordados quando da criação de uma Política de Segurança da Informação em uma organização, conforme abaixo:

- A empresa deverá utilizar o *software* antivírus da empresa McAfee Viruscan, americana, módulo para servidores, instalado em todos os seus servidores de dados de projetos, dos sistemas corporativos e banco de dados. No servidor do correio eletrônico deverá ter o módulo denominado GroupShield e nas estações de trabalho o módulo McAfee para estações de usuário final. A cada nova versão da lista de vírus, o fornecedor do *software* automaticamente a envia para os Administradores providenciarem a devida atualização em todos os equipamentos. A atualização das estações deverá ser feita

automaticamente a partir do servidor de rede no momento do primeiro acesso após a referida atualização.

- Apesar de possuir um *software* altamente confiável (McAfee), deve-se estar sempre precavidos e jamais abrir um arquivo (principalmente se for um executável) se a fonte não for confiável. Em caso de dúvida da procedência do arquivo, deve-se excluí-lo.
- Qualquer *e-mail* alertando sobre o aparecimento ou existência de vírus deve ser imediatamente encaminhado para análise da área de informática e jamais divulgado para outros usuários. A maioria dos *e-mails* alertando sobre vírus não passa de boatos e tem como única intenção apavorar os usuários e congestionar a Internet e redes locais.
- É de responsabilidade do usuário executar a opção de rastreamento e eliminação de vírus no diretório de armazenamento das informações do micro computador (C:\dados) mensalmente.
- É de responsabilidade do usuário executar a opção de rastreamento e eliminação de vírus em qualquer arquivo recebido de fontes externas, mesmo que a origem seja conhecida.
- Em todos os equipamentos da empresa, o antivírus deve sempre estar ativo e com a opção de verificação automática para todos os arquivos que chegarem ou que forem acessados serem verificados.
- Jamais se deve abrir um arquivo anexado por duplo clique (ou procedimento correspondente) sobre o ícone do anexo (em geral, um clips), no momento em que recebe a mensagem. É importante que se efetue um clique com o botão direito do mouse sobre ele (ou procedimento correspondente) para gravá-lo no *Hard Disk* (Dispositivo componente interno dos computadores cuja função é a de armazenar os dados de trabalho), ou em disquete. Após salvá-lo, não é recomendável abri-lo imediatamente, o melhor a fazer é visualizá-lo utilizando-se um bom visualizador de arquivos, que permita ver e imprimir todo o documento, com toda a sua formatação sem precisar abrí-lo.
- A melhor saída para uma infecção por programas maliciosos é a prevenção, portanto, é de caráter imprescindível que todo cuidado possível seja tomado quando se tratar de conseguir arquivos com origem desconhecida.
- Deve-se desconfiar de quaisquer arquivos anexados a mensagens de *e-mail* que não estejam sendo esperados, mesmo que provenientes de pessoas ou organizações de sua confiança. Havendo qualquer dúvida de que o arquivo possa conter vírus, é recomendável assumir que ele o contém e adotar as

medidas necessárias, tanto entrando em contato com a pessoa que supostamente enviou a mensagem para se certificar do porque do envio do arquivo anexado, quanto executando *software* antivírus para se assegurar do não contágio.

- Deve-se desconfiar muito de quaisquer arquivos anexados a mensagens de *e-mail* que tenham extensões duplas. Em geral, programas Cavalo de Tróia são enviados como inofensivos arquivos contendo textos simples ou imagens interessantes. Arquivos tais como LOVELETTER.TXT.VBS ou ANNAKOURNIKOVA.JPG.VBS nada têm de inocentes, tratando-se de perigosos Cavalos de Tróia.
- Para os casos de se desconfiar que um vírus possa ter contaminado qualquer arquivo em sua máquina, no ambiente corporativo, entre em contato com o departamento de suporte técnico, imediatamente, não tomando qualquer outra providência por sua conta, inclusive não gerando pânico entre seus colegas de trabalho.
- É necessário fazer cópias de segurança, *backu-ps,* de dados e arquivos importantes regularmente, tendo o cuidado de testar se as cópias foram realizadas com sucesso. No caso de um contágio por vírus que venha a destruir um determinado arquivo, a existência da cópia de segurança pode ser o seu único meio de recuperação.
- Deve-se utilizar o formato *RTF (Rich Text Format),* em vez de DOC, ao produzir documentos no processador de textos MS-Word. Este formato não porta vírus de macro.
- Deve-se tomar todo o cuidado com qualquer arquivo levado do escritório para o equipamento em sua casa e vice-versa, submetendo-o a uma inspeção por sistema antivírus antes de ser aberto, utilizado ou executado.

#### 7.5.4.11.2 PROTEÇÃO DO *E-MAIL* CONTRA VÍRUS

A empresa em estudo oficializou o uso do módulo denominado Groupshield, componente do software antivírus McAfee, por ser um dos pacotes mais seguros e eficientes do mercado utilizados para a proteção de servidores de correio eletrônico, cuja função é desempenhar a atividade de filtrar de todas as mensagens que chegam no servidor de *e-mail*, como também proteger os servidores do correio eletrônico e as caixas postais dos usuários contra vírus. O Groupshield identifica se são mensagens com vírus ou pertencentes a um grupo previamente configurado para que determinado tipo de

arquivo anexado em um *e-mail* não seja encaminhado ao destinatário, sendo que o mesmo irá receber apenas uma mensagem de notificação do ocorrido. Quando se tratar de um *e-mail* que contenha qualquer dos vírus reconhecidos pela lista de atualização do aplicativo, o Groupshield estará otimizado para automaticamente eliminar o vírus e, caso não consiga, será enviado uma mensagem de alerta ao Administrador da rede e do correio eletrônico, como também ao usuário de destino da mensagem e, tanto o *e-mail* quanto o arquivo anexado serão excluídos.

O software Groupshield possui recursos que possibilitam a criação de filtros para bloqueio de *e-mails*, evitando o uso indevido do correio eletrônico.

Por meio da criação de regras Rules (regras para configuração ou otimização de software), as mensagens podem ser bloqueadas de acordo com os tipos de arquivo anexados, ou pela presença de palavras consideradas inadequadas em seu conteúdo. Quando um *e-mail* for filtrado, ele será movido para a base de "Quarantine", que mantém a mensagem bloqueada.

O Groupshield, então, enviará um alerta para seu remetente, ao destinatário e também para os administradores do servidor. Deve-se criar uma regra para cada tipo de arquivo, como por exemplo, músicas (.mp2, .mp3), vídeos (.avi, .mpg), apresentações animadas (.pps), protetores de tela (.scr), etc, conforme mostrado na Figura 27. Todos os arquivos que chegarem a qualquer caixa postal do servidor do correio eletrônico e que tenham as extensões citadas acima serão bloqueados e não irão para as caixas postais dos usuários.

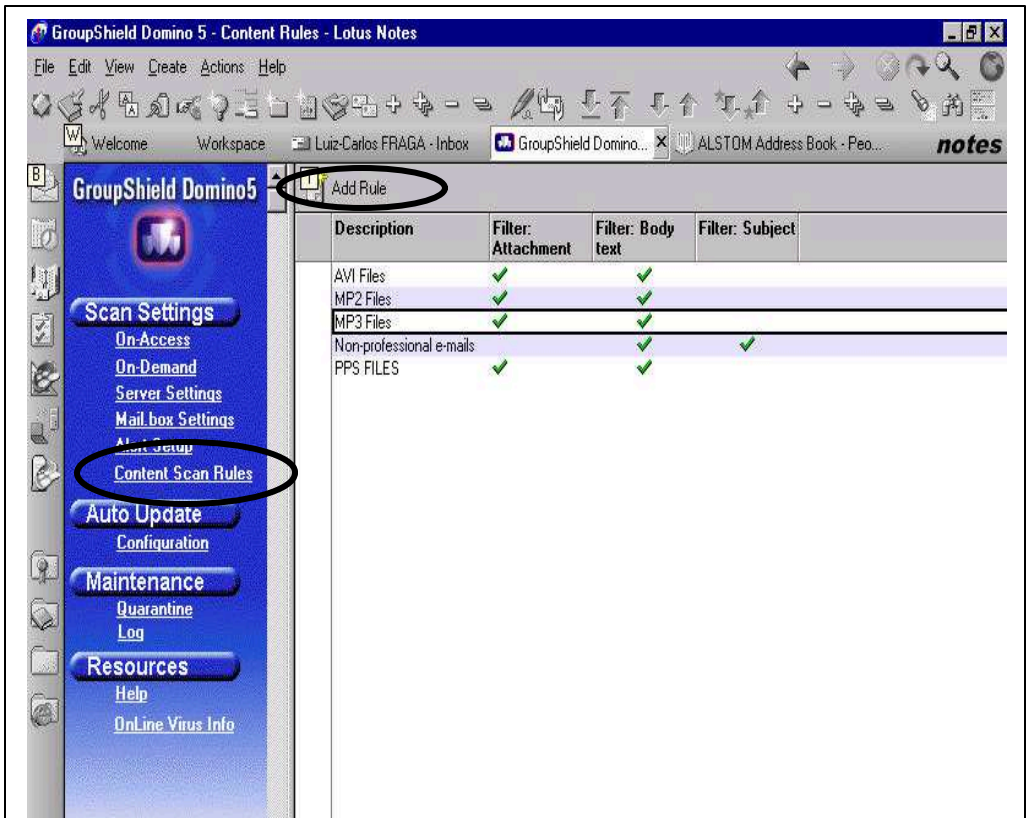


Figura 27 – Configurações do Groupshield para Filtro de Arquivos

Para se criar uma outra regra contendo *strings* (conjunto de caracteres que podem ser utilizados para uma determinada pesquisa por programas de computadores), que sirvam de parâmetro para filtragem das mensagens.

Abaixo, na Figura 28, pode-se observar uma configuração típica para bloqueio de qualquer *e-mail* que tenha assunto não relacionados a trabalho profissionais ou que tenha qualquer assunto relacionado a sexo:

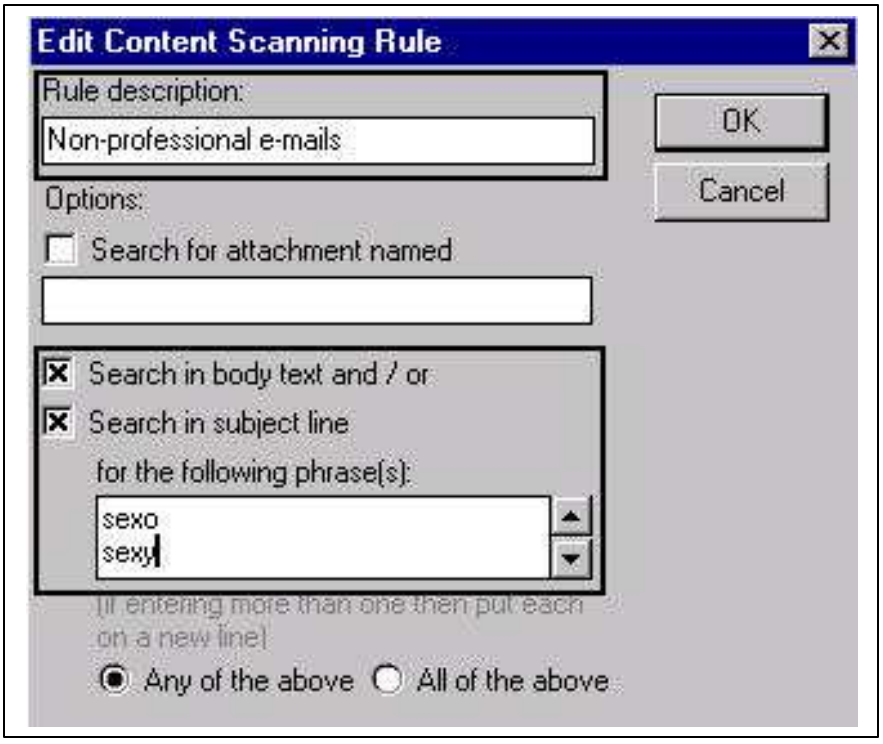



Figura 28 – Configuração do Groupshield para Assuntos não Profissionais

Alguns cuidados, no entanto, devem ser tomados, como por exemplo, o Groupshield não filtra automaticamente arquivos inseridos dentro de arquivos

compactados por softwares semelhantes ao *Winzip*, sendo que é necessária uma parametrização especial.

Quando se elaborar regras com *strings*, uma mensagem que contenha a palavra "Sexta-feira" poderá ser bloqueada caso haja alguma regra com a *string* "sex".

O Groupshield é uma ferramenta eficiente e que tem contribuído para evitar o fluxo de mensagens indesejáveis circulando pela empresa, congestionando o meio físico da rede e o servidor do correio eletrônico, como também contribuindo para minimizar a perda de produtividade de cada usuário lendo mensagens não relacionadas aos assuntos de trabalho.

A Figura 29 apresenta as configurações do Groupshield com referência àproteção do servidor do correio eletrônico contra vírus de computador que possam estar vindo via *e-mail* tanto para o próprio servidor como também para as caixas postais dos usuários existentes:

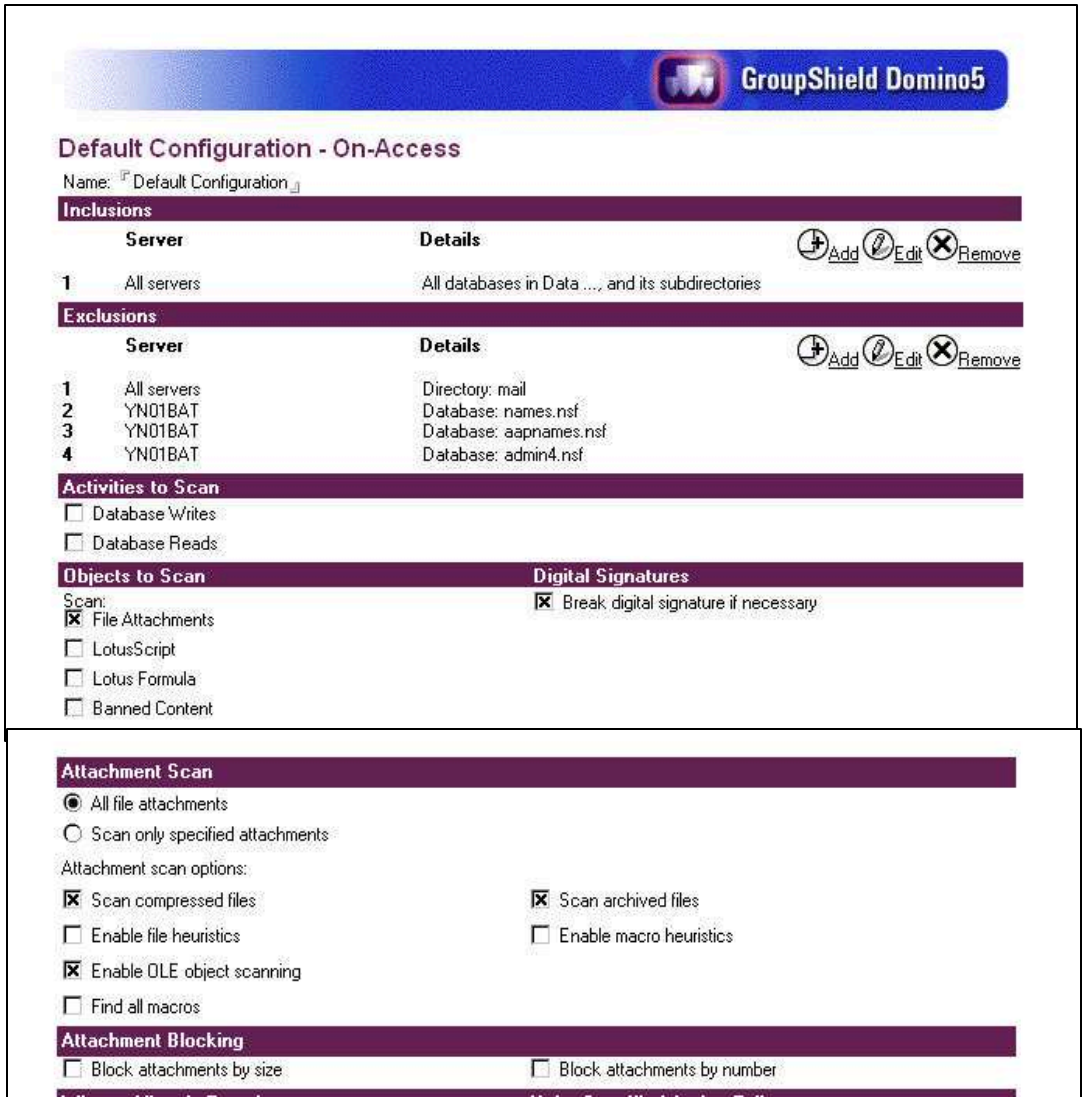


Figura 29 – Configurações do Groupshield para Proteções contra Vírus

As configurações acima são importantes para que o software Groupshield possa efetuar com eficiência o trabalho de pesquisa e proteção.

#### 7.5.4.12 O CORREIO ELETRÔNICO LOTUS NOTES

O software do correio eletrônico adotado pela empresa chama-se LOTUS NOTES DOMINO, da empresa Lotus,adquirida pela *IBM* (International Business Machine). É uma ferramenta considerada completa e robusta no que tange àcomunicação entre diferentes organizações, replicação de suas bases de dados de controles, bem como dos seus livros de usuários cadastrados, e suportada por vários recursos de segurança, tais como criptografia e assinatura digital. Além dos recursos de correio eletrônico, dispõe de funções:

- Correio Eletrônico: aplicativo com a funcionalidade de enviar e receber informações, mensagens e arquivos anexados a *e-mail*.
- *Workflow:* aplicativo com funções customizadas para distribuir tarefas e padronizar o método de trabalho das áreas envolvidas em um processo.
- *Workgroup:* recurso que permite que diferentes áreas trabalhem mais próximas e em conjunto.
- Broadcast: disponibilizando manuais e procedimentos para que seus funcionários tenham um grau de conhecimento maior sobre a organização.
- Integração: possibilidade de integração e conexão com a maioria das ferramentas de desenvolvimento e armazenamento (banco de dados) diksponíveis no mercado.
- *Internet / Intranet*: permite compatibilidade com linguagens de desenvolvimento de páginas para a *Internet* / *Intranet*.

O *Lotus Notes* oferece uma segurança por camadas, cuja segurança pode ser executada a partir de um usuário, por grupos de usuários e por todo o ambiente do correio eletrônico do servidor, ou seja, por todo o Domínio do Lotus Notes. O controle da segurança nos Servidores é de responsabilidade dos administradores da rede. Para os

casos em que o servidor instalado pertença a um domínio de proporções mundiais, é necessário que os Gerentes mundiais atribuam perfis e direitos de acesso a determinadas funções existentes para os Administradores Locais. Seus recursos vão além de uma ferramenta completa que permite a manipulação de suas bases de dados, como também de desenvolvimento de aplicações específicas para trabalho, sendo que as configurações de segurança poderão ser atribuídas por usuário ou grupos de usuários.

A Criptografia permite proteção ao nível de campo, ou seja, pode-se codificar o conteúdo de qualquer campo de forma que somente leitores que têm a chave de criptografia poderão acessar a mensagem ou campo. Gerentes de banco de dados podem codificar um banco de dados inteiro, inclusive cada campo pertencente a este banco de dados.

Assinaturas Eletrônicas confirmam a segurança de que um documento ou seções de documento são remetidos de um usuário a outro e não há falsificação antes de alcançar o destinatário. Para se obter uma segurança extra, existe a possibilidade do *Lotus Notes* incluir uma assinatura eletrônica adicional ao arquivo anexado ou à mensagem, pois esta ação assegura aos usuários que a identidade do remetente é genuína e que a informação não mudou desde que foi remetida até o destinatário.

Todo banco de dados tem uma lista de controle de acesso denominada *ACL* (Access Control List), que define quem terá acesso ao banco de dados e descreve as atividades que podem ser executadas tanto para um usuário como também para um grupo de usuários. Os documentos codificados contêm um ou mais campos que são habilitados para criptografia, que são unidos a chaves para codificação dos dados do campo. O processo de criptografia acontece automaticamente ou manualmente sendo acionado pelos usuários autores ou editores das mensagens. Associando-se criptografia múltipla automaticamente a um documento, a codificação é estendida a todos os campos do mesmo com as mesmas chaves.

A criptografia pode ser secreta, sendo que as chaves precisam ser enviadas aos usuários para que eles decifrem e consigam ter acesso ao conteúdo da mensagem, ou pública, sendo que neste caso, as chaves são associadas com o identificador do usuário no Livro Principal de Endereço Público, a *PAB* (Public Address Book) do Lotus Notes.

Devido aos seus recursos de segurança, como também às suas funcionalidades, o *Lotus Notes* tem sido um dos *softwares* de correio eletrônico mais utilizados corporativamente pelas empresas, pois seu processo de replicação e atualização de banco de dados pode ser feito automaticamente e para todas as unidades pertencentes à organização a nível mundial.

### 7.5.4.13 A ESTRATÉGIA DE IMPLANTAÇÃO DA POLÍTICA DE SEGURANÇA

Para que a implantação de uma Política de Segurança da Informação em qualquer organização possa ter sucesso é necessário a criação de algumas atividades de apoio, grupos de solução e responsável pela criação dos procedimentos cabíveis, como também a aquisição e investimento em *hardware* e *software*.

#### 7.5.4.13.1 O GSI – GRUPO DE SEGURANÇA DA INFORMAÇÃO

Para a implementação da política de segurança estudada nesta proposta, foi criado um grupo de trabalho denominado GSI – Grupo de Segurança da Informação, contendo representantes de cada uma das principais áreas da empresa. Este grupo está ligado diretamente a todos os membros do Comitê Executivo da organização, como também tem autonomia para buscar recursos que viabilizem o sucesso do projeto.

Funções do GSI:

- O GSI, Grupo de Segurança da Informação, tem como função definir a política de segurança da informação para toda a unidade da empresa localizada na cidade de Taubaté, como um projeto piloto que, após sua implementação deverá ser estendido também para todas as unidades da empresa.
- Efetuar a implantação, treinamento e conscientização dos usuários.
- Providenciar cronograma das auditorias internas nas diversas áreas.
- Buscar o desenvolvimento, modernização e análise de novas tecnologias voltadas àsegurança da informação.

A Figura 30 apresenta o organograma do GSI – Grupo de Segurança da Informação:

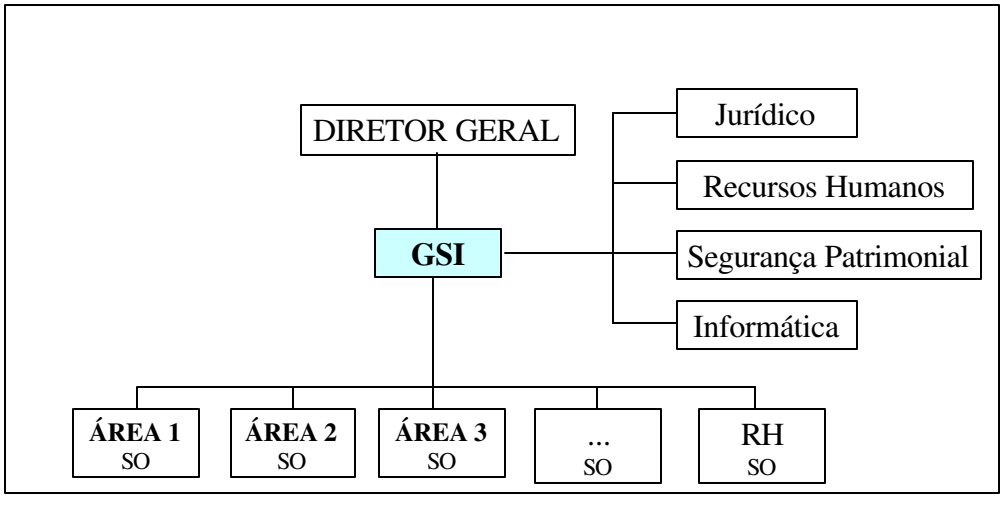


Figura 30 – Organograma do GSI – Grupo de Segurança da Informação

Todo o trabalho do GSI está diretamente ligado e em comunicação com a área Jurídica, Recursos Humanos, Segurança Patrimonial e Informática às quais provêm consultorias e suporte sobre as leis vigentes no país, normas da companhia, acordos com sindicatos e sobre os recursos computacionais.

O GSI deverá receber informações e interagir com os representantes de cada uma das áreas principais da empresa –- os *Security Officer* –-, no tocante às definições e implementações da sistemáticas de proteção e segurança na empresa.

Generalidades:

- Todos os departamentos deverão escolher *um Security Officer* (S.O) que terá o representante desta área para os assuntos de segurança da informação.
- Durante o transcorrer do projeto, caso haja a necessidade poderão ser contratados profissionais específicos e especialistas.
- A responsabilidade pela monitoração, auditoria, aplicação de penalidades cabíveis e acompanhamento da Política de Segurança implementada é de responsabilidade do grupo GSI, juntamente com o responsável pela área de Tecnologia da Informação, pois deste acompanhamento serão minimizados os problemas de acessos indevidos, contaminação por meio de vírus, pirataria de software, desconfiguração da estação de trabalho e falta de cultura do usuário com a não preocupação com a segurança da informação.

Recursos relacionados à Informática:

- Deverá efetuar monitorar e emitir relatórios do uso e dos recursos dos sistemas de Informação (*Lotus Notes* e SAP).
- Implementar todas as diretrizes para segurança na *Internet*, *Intranet*, na rede, nos servidores e nas estações de trabalho dos usuários.
- Deverá efetuar a validação das novas tecnologias.
- Deverá prover a instalação e manutenção sistemas computacionais.
- Deverá efetuar a administração das contas e direitos de acessos dos usuários aos sistemas de informação.
- Deverá prover suporte técnico na elaboração de procedimentos e políticas.

Recursos relacionados à área de Recursos Humanos:

- Fornecer informações antecipadas de funcionários em missão, em licença médica e admissão de funcionários para o GSI e Informática.
- Prover suporte na elaboração de procedimentos e políticas.
- Executar as penalidades previstas e cabíveis.
- A Política de Segurança da Informação, bem como a assinatura dos formulários cabíveis, deverão fazer parte da rotina de contratação de novos profissionais, juntamente como contrato de trabalho.

Recursos relacionados àárea Jurídica:

- Fornecer suporte na elaboração de procedimentos e políticas
- Executar as penalidades previstas e cabíveis.

Recursos relacionados àárea de Segurança Patrimonial:

- Promover e exercer a segurança física dos equipamentos e mídias de *back-up* (servidores, microcomputadores dos usuários, cartuchos de fitas magnéticas, *notebooks*).
- Suporte na elaboração de procedimentos e políticas
- Promover e exercer a segurança nas portarias da empresa, tanto para entrada e saída de equipamentos de informática, *notebooks*, papéis e cd rom.

Recursos relacionados aos *Security Officer:*

- São os responsáveis pela segurança da informação nos departamentos em que estarão alocados.
- Deverão assessorar o GSI nas tarefas do dia-a-dia e orientar os usuários dos departamentos.
- Definir junto aos gerentes dos departamentos quais serão os direitos de acesso aos sistemas computacionais da empresa.
- Treinar, assessorar, conscientizar e orientar os usuários dos diversos departamentos.

Divulgação da Implantação Política de Segurança Implementada:

- Cartilha “Uma Questão de Segurança”.
- Faixas ilustrativas em locais estratégicos da empresa.
- Reuniões de conscientizações.
- Treinamento direcionado a todos os profissionais envolvidos.
- Peça teatral evidenciando assuntos relacionados àPolítica de Segurança.

Auditorias Permanentes:

- Após a implementação da Política de Segurança da Informação, é importante a divulgação de um calendário constando as datas para a execução das auditorias permanentes em cada departamento da empresa.
- Quando da implantação de uma Política de Segurança devem existir mecanismos de controle, para assegurar que a mesma seja seguida, sendo que uma das maneiras de se poder executar este controle é por meio de auditorias permanentes. O objetivo é de se evitar as incidências de desvios no cumprimento da Política, pois, Infelizmente, uma grande parte dos usuários somente a respeitam quando têm ciência de que serão punidos caso não a obedeçam.
- Para a execução de auditorias deverão ser envolvidos profissionais especializados da área de informática, juntamente com os membros do Grupo GSI, que irão planejar as áreas, os usuários a serem auditados e as datas das auditorias.
- Deve-se ter bem claro o que será auditado e as punições para cada tipo de não conformidade com as diretrizes da Política. A auditoria também irá se basear na utilização do correio eletrônico, quanto aos acessos à *Internet*, aos arquivos gravados na rede e nas pastas locais das estações dos usuários, se os perfis de direitos para acessos que o usuário possui estão de acordo com a função desempenhada na empresa.
- O profissional responsável pela auditoria deverá fazê-la da maneira o mais sigilosa possível, registrando todos os detalhes dos problemas encontrados e tomando o cuidado para não divulgar qualquer resultado encontrado durante a auditoria. Este auditor desempenha uma tarefa difícil, pois sua atividade o expõe como um espião ou "dedo duro" da empresa, fato que o poderá fazê-lo sofrer ameaças ou indiferenças por parte dos colegas. Normalmente os auditores se tornam consultores e utilizam suas habilidades tradicionais para reconhecer e solucionar problemas.
- Quando do término da auditoria deve ser elaborado um relatório contendo as não conformidades encontradas e demais informações importantes, sendo que o mesmo deverá ser entregue aos líderes responsáveis pela segurança da informação da empresa. O usuário ao qual tenham sido encontradas irregularidades –- quanto às diretrizes da Política de Segurança –-, deverá ser notificado para que redirecione suas atitudes dentro da empresa e que nos casos de reincidência, poderá receber uma punição mais grave.

### 7.5.4.13.2 RECURSOS PARA A IMPLANTAÇÃO DA POLÍTICA

Sobre o tópico relativo aos recursos a serem utilizados para a implementação da política de segurança, segue na Tabela 16 um resumo do Plano de Ação para implementação da Política de Segurança.

Existem algumas das atividades que se apresentam com percentual baixo, em virtude de, na data do estudo, estes itens ainda estarem em fase de implementação.

Tabela 16 – Plano de Ação Para Implantação da Política de Segurança

| AÇÃO | PRAZO | RESP | STATUS |
|---|---|---|---|
| Definição da Política | jan/01 | VP / DG | 85% |
| Classificação dos documentos | jan/01 | GSI, Gerentes | 30% |
| Definição / treinamento Security Officer | fev/01 | GSI, Gerentes | 25% |
| Cartilha e Termos de compromisso | fev/01 | GSI, TI, RH | 50% |
| Treinamento / Conscientização usuários | mar/01 | GSI, TI, RH | 5% |
| Mensagem nos sistemas de informação | mar/01 | TI | 10% |
| Gerenciamento de rede | mar/01 | TI | 20% |
| Adesão ao Grupo de Segurança - GSI | abr/01 | GSI | 10% |
| Monitoramento e Logs | abr/01 | TI | 25% |
| Procedimentos e Instruções Técnicas | mai/01 | GSI, TI, Gerentes | 20% |
| Alta disponibilidade | jul/01 | TI, Seg. Patrim. | 5% |
| Controle e Administração de acesso | jul/01 | TI | 20% |
| Proteção do ambiente | ago/01 | TI | 20% |

A Tabela 17, a seguir, apresenta um resumo dos valores a serem gastos com as implementações da Política de Segurança, como também uma estimativa do tempo gasto para sua finalização.

O investimento expresso é alto, pois como a empresa praticamente não possuía nenhuma política real implementada, muitas das sistemáticas tiveram que se iniciar adquirindo-se todos os recursos necessários, inclusive contratando suporte de consultorias externas para as definições dos procedimentos necessários.

Quanto à somatória do tempo, o total de 170 dias estimado, foi em virtude de que muitas ações poderem ser conduzidas em paralelo a outras.

Todo o projeto foi concluído com sucesso no mês de Agosto/2001.

Tabela 17 – Custos Relativos a Implantação da Política de Segurança

| POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - INVESTIMENTOS |
|---|

| Necessidade | Custo Inicial (KUS$) | Custo Mensal (KUS$) | Tempo p/ Implementação (Dias) |
|---|---|---|---|
| Fragmentadoras de Papel | 4,0 | - | 30 |
| Gerenciamento de rede | 95,5 | 2,0 | 50 |
| Acesso àInternet | 27,0 | 4,2 | 50 |
| Proteção do ambiente (Firewall) | 131,0 | 2,6 | 80 |
| Controle de acesso e proteção dos equipamentos | 200,0 | - | 90 |
| Sistema de alta disponibilidade | 72,7 | - | 60 |
| Proteção antivírus | 20,0 | - | 0 |
| Administração da Segurança | 14,0 | - | 40 |
| Suprimentos | 10,0 | - | 15 |
| **TOTAL** | **574,2** | **8,8** | **170** |

A Figura 31, abaixo, apresenta o Ciclo de Vida da Política de Segurança da Informação, esquema seguido no tocante àimplementação da Política de Segurança em estudo. A fase em que a empresa se encontra neste momento é a de AVALIAÇÃO da Política implementada como um todo junto ao GSI e os *Security Officer*.

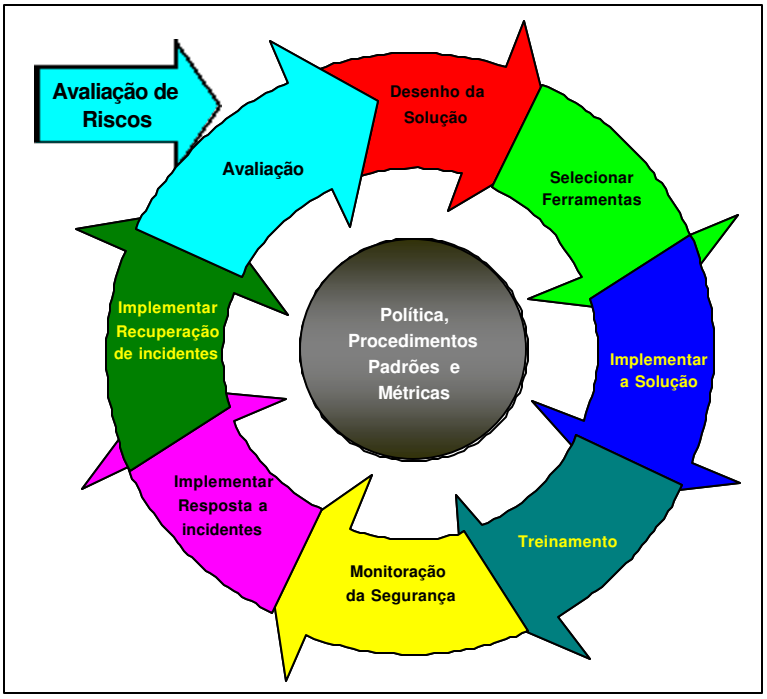



Figura 31– O Cido de Vida da Política de Segurança da Informação

Fonte: *Case Solectron* (2000).

A fase em que a empresa se encontra neste momento é a de Avaliação da Política implementada como um todo junto ao GSI e os *Security Officer*.

Para este ano de 2002, está previsto a finalização desta fase de Avaliação de todo o projeto, momento de reflexão e crítica, onde após esta fase, estará concluído o documento da Avaliação da Política de Segurança implementada.

Caso neste estudo seja detectada a necessidade de mudanças, será efetuado um redirecionamento de algum item que, por ventura, não esteja se adequando àrealidade –- tanto da empresa quanto do mercado –-, tendo em vista as evoluções tecnológicas das ferramentas como também das necessidades de novas implementações de segurança.

Ao nível da empresa e da Gestão da Informação, a Política da Informação implantada, por ser generalizada e estar baseada em conceitos e normas, não sofre qualquer alteração, porém, ela se apóia em ferramentas, em *software* e *hardware,* que estão em constante evolução natural e tecnológica e que, para seu sucesso contínuo, ano após ano, é imprescindível uma reavaliação destes dispositivos, com o intuito de se verificar se ainda estão eficientes e cumprindo os propósitos previstos.

No capítulo seguinte serão apresentados os resultados obtidos com pesquisa efetuada colocando-se em prática a Política de Segurança da Informação implementada.

# CAPÍTULO VIII

# RESULTADOS

## 8.1 FOCO DA PESQUISA

O objetivo principal desta pesquisa está citado no início deste trabalho:

*"... procura efetuar inicialmente um estudo do conceito Informação e as suas aplicações nas organizações, refletindo tópicos como estratégia, sistemas de informação e a importância para a competitividade frente ao mercado empresarial, evidenciando a fragilidade da informação existente nas corporações –- armazenada nos servidores de dados dos Centros de Informática –- e vulneráveis a ataques de vírus de computador que possam ter como meio de transmissão o correio eletrônico. O objetivo deste trabalho é propor a implantação de uma Política de Segurança da Informação em uma indústria, dando ênfase àproteção contra ataques de vírus recebidos por meio de e-mail ...".*

O projeto de implantação da Política de Segurança da Informação na empresa em estudo foi finalizado no mês de Agosto de 2001. A partir da data da divulgação da sua atuação, muitas reuniões foram efetuadas com os membros do GSI, com os *Security Officers*, como também com a alta direção da empresa. Um dos objetivos principais destas reuniões estava sempre em evidência o acompanhamento de cada fase do processo, verificando-se as dificuldades encontradas, analisando-se os *softwares* e *hardwares* em implantação, suas limitações e as otimizações em andamento, conforme a Política especificada.

Nas avaliações que foram feitas nestes últimos quatro meses de atuação da Política, percebeu-se claramente que a o projeto contribuiu para que a companhia pudesse garantir a segurança da informação em sua rede de dados, provendo qualidade e confiança aos usuários na tomada de decisão baseada na informação existente, como também protegendo os microcomputadores de trabalho.

### 8.2 EVIDENCIAS ENCONTRADAS

Com relação às evidências encontradas, trata-se de fatos que aconteceram e que refletiram a necessidade da ação de alguma diretriz estipulada e prevista na Política de Segurança implantada.

#### 8.2.1 BLOQUEIO DE *E-MAIL* COM ARQUIVO DE TAMANHO INADEQUADO

Um dos tópicos da Política em evidência na empresa retrata a preocupação em se manter uma boa performance dos *links* de comunicação da rede de dados corporativa e, para tanto, ficou estipulado um limite máximo no tamanho de arquivo anexado de 4 Mb para uma mensagem ser enviada por meio do *Lotus Notes*. Este limite foi estipulado tomando-se como base um tamanho médio de arquivos gravados nos servidores de dados da rede, como também no tamanho permitido pelo provedor local da *Internet* para envio deste tipo de *e-mail*. A empresa mantém um contrato com um provedor de conta na *Internet* local, onde são disponibilizadas sete contas para o envio de mensagens

emergenciais nesta categoria alternativa. Tal fato se faz necessário, como contingência, para o caso de qualquer problema com o servidor do correio eletrônico e a empresa ter que receber ou enviar mensagens urgentes.

Dentre alguns casos que foram evidenciados, na Figura 32, a seguir apresenta-se a tela de gerenciamento de mensagens enviadas pelos usuários, que é uma ferramenta de monitoramento da caixa postal de saída do servidor do correio eletrônico, onde encontrava-se bloqueada uma mensagem de tamanho de 25 Mb que foi detectada e, tanto os Administradores do servidor de *e-mail* como também o usuário responsável pela mesma foram notificados. Esta mensagem foi destruída na seqüência após sua detecção, fato que contribuiu para se evitar congestionamento das linhas de comunicação de dados da companhia.

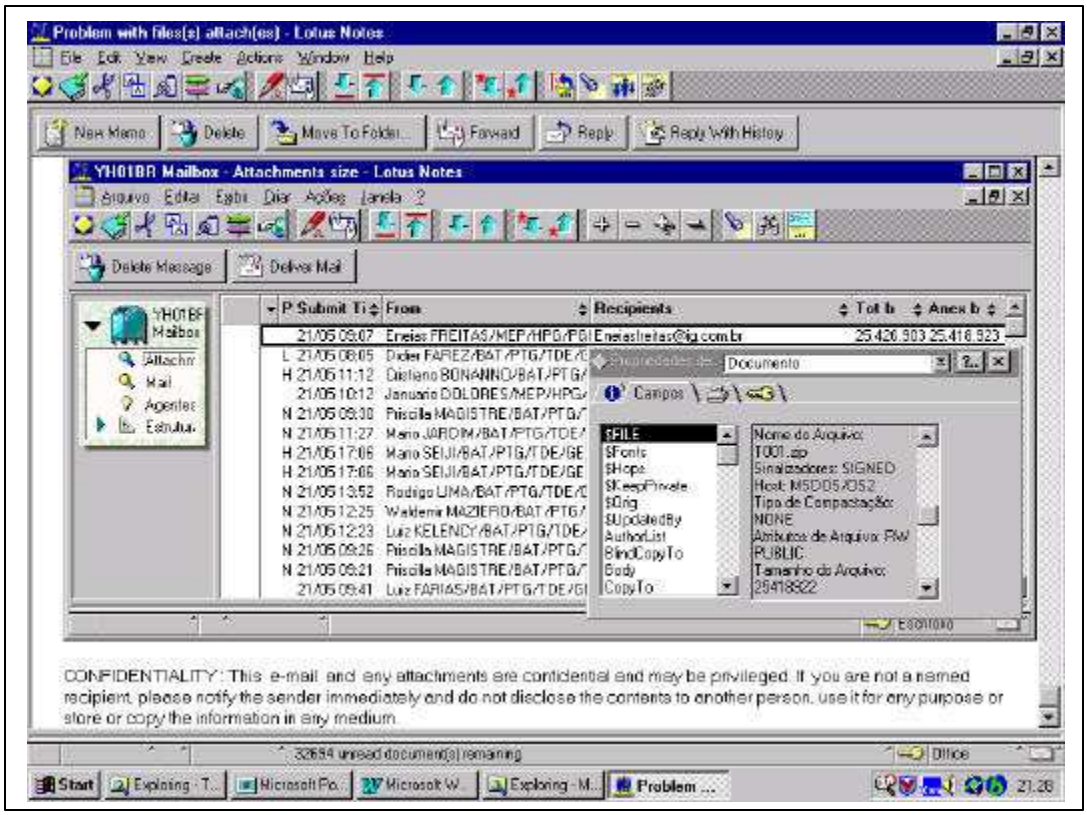



Figura 32 - Alerta Sobre *E-mail* com Arquivo de Tamanho Inadequado

### 8.2.2 BLOQUEIO DE *E-MAIL* COM MENSAGENS INADEQUADAS

Um dos maiores problemas existentes nas empresas está relacionado àqueda de produtividade dos funcionários com relação a mensagens pornográficas ou não relacionadas a trabalho (extensões do tipo .bmp, .pps, .avi, .scr, etc...), arquivos de música (tipo .mp3 ou .avi) e uma série de outras que se enquadram nesta categoria. O

perigo torna-se real –- e vai além da perda de produtividade do funcionário –-, quando estes arquivos são portadores de vírus de computador e que podem gerar problemas maiores, tanto nos servidores de dados, como também no servidor do correio eletrônico e nas estações de trabalho dos usuários. De acordo com a Política em evidência na empresa, este assunto também é retratado e a ação implementada é que o *software* Groupshield efetua um bloqueio a todas as mensagens com arquivos pertencentes a esta categoria, como também executa uma ação de eliminação dos vírus existentes.

A seguir serão apresentadas algumas informações relativas à observação efetuada sobre o recebimento de mensagens com arquivos não relacionados a trabalho e contaminados por vírus. Na Figura 33 tem-se a impressão da tela de gerenciamento dos arquivos inadequados que foram recebidos classificados por data, autor e servidor do correio eletrônico. Cada uma das linhas existentes representa um evento recebido e, editando-se cada um deles, obtém-se o detalhe da ocorrência:

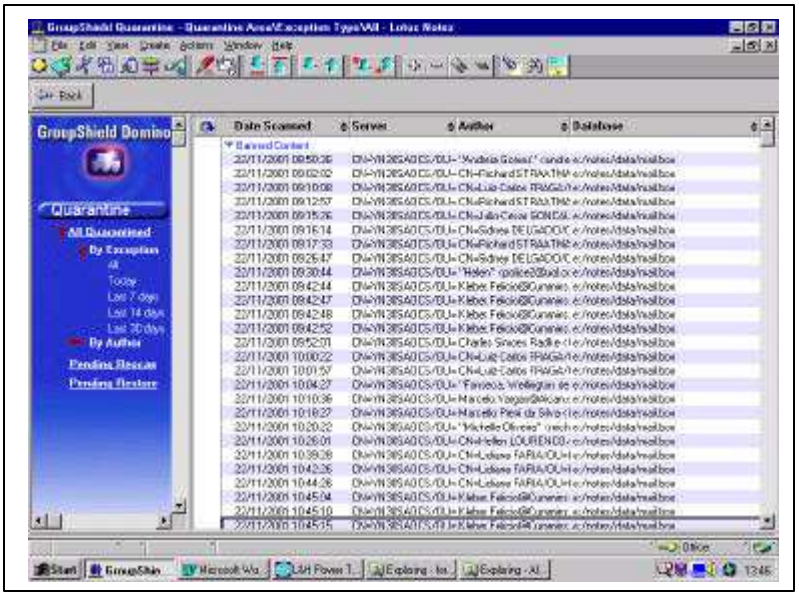



Figura 33 – Tela de Gerenciamento do Groupshield – Arquivos Inadequados

Tomando-se como base e editando a primeira ocorrência desta relação, onde se encontra o item do dia 22/11/01 às 08:50:36 horas, é possível de se obter a informação detalhada de que se trata de uma evidência de arquivo anexado no *e-mail* com característica pornográfica, conforme Figura 34:

Figura 34 – Tela de Gerenciamento do Groupshield – Detalhe de Evento

Esta informação relata o fato de que realmente é um arquivo inadequado ao trabalho e, conforme diretriz da Política implementada e configurada no *software* Groupshield, este *e-mail* foi bloqueado automaticamente, sendo que um alerta citando o ocorrido foi encaminhado para os Administradores do Correio eletrônico, ao remetente da mensagem, como também para os destinatários da mesma.

Para verificação das ocorrências, foi selecionado no software Groupshield para efetuar um levantamento durante o período de 22/11/2001 até 28/12/2001, registrando-se todas as evidências relativas a *e-mails* com arquivos anexados e não relacionados a trabalho, como também contendo vírus, que fossem encontrados.

O Resultado desta pesquisa está resumido na Tabela 18 e a listagem contendo a pesquisa completa, citando as ocorrências diariamente, poderão ser consultadas no ANEXO 35.

Tabela 18 – Pesquisa das Mensagens de *E-mail*

| ***E-MAIL* COM VÍRUS E ARQUIVOS INADEQUADOS AO TRABALHO** | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | | | | |
| **PERÍODO: DE 22 DE NOVEMBRO DE 2001 À 28 DE DEZEMBRO DE 2001** | | | | | | | | |
| | | | | | | | | |
| | **TIPO DE ARQUIVO ENCONTRADO** | | | | | | ***E-MAIL*** | **QTD.** |
| **ARQS.** | **.MP3** | **.AVI** | **.PPS** | **PORNOG.** | **NÃO PROFIS.** | **VÍRUS** | **BLOQS** | ***E-MAIL*** |
| | | | | | | | | |
| **TOTAL** | **26** | **11** | **1114** | **13** | **1106** | **47** | **2317** | **499.500** |

Na seqüência, a Figura 35 ilustra graficamente o resultado obtido com a pesquisa:

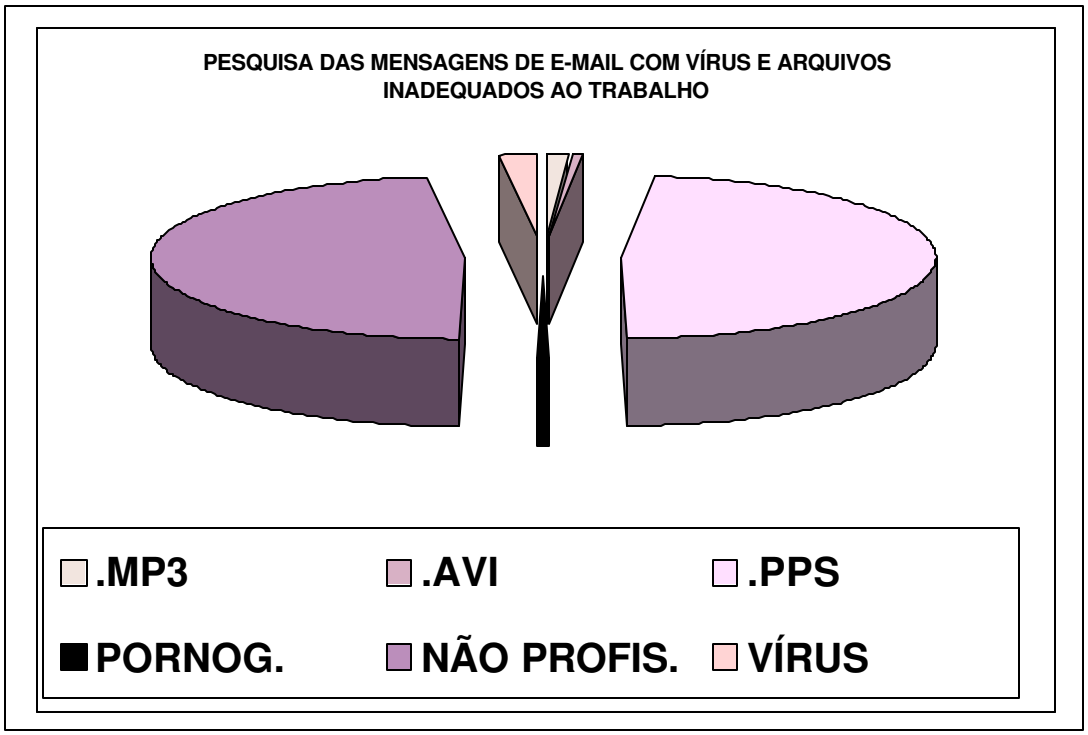



Figura 35 – Gráfico Pesquisas das Mensagens de *E-mail*

Durante o período analisado, a empresa recebeu um total de 499.500 *e-mails*, sendo que deste total, 2.317 mensagens foram bloqueadas por estarem contra os princípios estipulados na Política de Segurança implementada na empresa e 499.183 foram utilizados como úteis para trabalho.

O maior número de arquivos que foram bloqueados se caracterizaram como arquivos do tipo .pps, ou seja, geralmente animações geradas pelo *software* MS-Powerpoint, que normalmente são arquivos de tamanho grande, gráficos e que, além de fazer com que o usuário faça uma pausa em suas atividades profissionais para "assistir" a mensagem recebida, provoca uma lentidão no fluxo das mensagens trafegando pela rede devido ao seu tamanho. Em muitos casos semelhantes, o usuário envia esta mensagem para um grupo de amigos e, inicia-se desta maneira, mais uma quantidade de dados transitando pelas redes e gerando um congestionamento adicional nos servidores de *e-mail* e nas linhas de comunicação.

Em segundo lugar, destacam-se os arquivos com assuntos não profissionais, ou seja, correntes, mensagens tipo *Spam*, *Hoax* e demais mensagens que apresentam trechos do texto contendo palavras que sugerem arquivos não terem relacionamento com trabalho, por exemplo, Sexo, Play Boy, World Trade Center, Afeganistão, Osama B. Laden, palavrões diversos e uma série de palavras obscenas.

Sobre esta grande quantidade de arquivos em trânsito pela rede, via correio eletrônico, do tipo .pps e não relacionados a trabalho, é possível de se concluir que a empresa está necessitando efetuar urgentemente um treinamento e redirecionamento das responsabilidades dos seus colaboradores, para um melhor aproveitamento do tempo e das ferramentas disponibilizadas pela empresa para trabalho e atividades profissionais.

Arquivos pornográficos, de filmes e música foram as menores quantidades recebidas.

Mensagens contendo contaminações por vírus de computador foram exatamente 47 recebidas. Um número relativamente pequeno quando comparado àquantidade total de *e-mails* recebidos, porém quando se trata de vírus de computador, a quantidade é um fator preocupante, mas não tão grave.

O problema maior está em que tipo de vírus foi recebido e qual o seu poder de disseminação e destruição. Na Tabela 19, estão relacionados os vírus encontrados e suas características de contaminação:

Tabela 19 – Relação dos Vírus Encontrados

| VÍRUS | QUANTIDADE | CARACTERÍSTICA |
|---|---|---|
| MELISSA | 2 | Risco Médio. Envia automaticamente *e-mail* para usuários do livro de endereços do correio eletrônico. |
| SIRCAM | 4 | Risco Médio. Envia automaticamente mensagens para todos os usuários do livro de endereços. |
| W32 / BAD TRANS | 29 | Risco Médio. Alto índice de contaminação e tem a característica de enviar *e-mails* não lidos da caixa postal. |
| W32 / MAGISTR.A | 1 | Risco Médio. Alto índice de disseminação e mesmo efetua a criação de arquivos .DAT. |
| W32 / MAGISTR.B | 6 | Risco Médio. Efetua a criação de um novo arquivo System.ini, danificando a inicialização do equipamento. |

| | | |
|---|---|---|
| W97M / ANTIV | 2 | Risco Baixo. É um vírus de macro e apresenta mensagens na tela do usuário. |
| W97M / IPID.GEN | 2 | Risco Baixo. É um vírus de macro e apresenta mensagens na tela do usuário e torna invisível a barra de ferramentas do MS-Word. |
| W97M / MDMAK | 1 | Risco Baixo. É um vírus de macro e apresenta mensagens na tela do usuário. |
| **TOTAL** | **47** | |

### 8.3 DISCUSSÕES E BENEFÍCIOS

Analisando-se os vírus encontrados, os piores foram o Melissa e o Sircam, devido a sua grande eficiência em se reproduzir pela rede de computadores via correio eletrônico, além de enviar mensagens automáticas para todos os usuários. O congestionamento do servidor de *e-mail* torna-se tão grande que é necessário desligá-lo. Caso um vírus deste se espalhe na rede de computadores em estudo, atingindo todos os 930 microcomputadores somente da unidade de Taubaté, efetuando-se um cálculo rápido dos valores que a empresa teria que desembolsar de imediato para análise, tem-se:

O tempo médio necessário para a desinfecção de um microcomputador e instalação do *software* antivírus é de aproximadamente 20 minutos de trabalho, sendo que o valor médio cobrado por um técnico para a execução desta atividade é de aproximadamente R$12,00 para cada equipamento. Para um total de 930 máquinas, resultaria em R$11.160,00. O tempo total que um técnico levaria para finalizar o trabalho seria de: 20 minutos x 930 máquinas. = 18.600 minutos, ou 310 horas ou 31 dias, trabalhando 10 horas diárias, que é um tempo de paralisação impraticável para uma empresa de ponta no mercado.

Contratando-se uma equipe de dez técnicos, este tempo poderia cair para 1.860 minutos ou 31 horas ou 3,1 dias, trabalhando 10 horas diárias, tempo que poderia até ser tolerável, porém a um custo de R$111.600,00 e, levando-se em conta que não haja a necessidade de se apagar todos os dados do microcomputador nem de haver a necessidade de reinstalação total de *softwares*.

Não se pode esquecer do fato de que três dias em que a empresa se encontra inativa o prejuízo torna-se um alto valor. Na linha de produção da fábrica principal existem dois equipamentos, pertencentes ao processo de automação, em que o valor da hora de trabalho da máquina está avaliado em U$300 (trezentos dólares). Convertendo-se ao câmbio do Dólar atual aproximado a R$2,48, chegaríamos a um total de

R$1.488,00 para as duas máquina para cada hora. No final de 31 horas paradas, o valor estaria próximo de R$46.128,00. Até este momento, com um cálculo aproximado, a empresa estaria perdendo R$157.728,00, ou seja, R$111.600,00 somados a R$ 46.128,00.

Caso haja a necessidade de se analisar o valor do salário por hora de cada funcionário parado (aproximadamente 1.200 colaboradores), atrasos nos prazos de entrega de encomendas (que normalmente têm multas contratuais), a incerteza e o risco de que o vírus não tenha sido enviado –- por ignorância dos fatos –- para algum cliente, danos causados em servidores de dados e do correio eletrônico, tempo de *Restore* de dados de *back-up´s* etc... Enfim, as cifras de prejuízos iriam tomando um "vulto faraônico".

Portanto, tomando-se com premissa as evidências encontradas neste estudo, a Política de Segurança da Informação implementada obteve resultado positivo, transformando a segurança da informação em ganho real de divisas que se repercutiu em continuidade do negócio, credibilidade, permanência da empresa no mercado e confiança para seus funcionários –- no tocante à tomada de decisão –-, baseada na informação existente nos sistemas informatizados.

Baseado nos resultados apresentados segundo a empresa Módulo Security Solutions (1) (2001), relativo à 7ª Pesquisa Nacional Sobre Segurança da Informação 2001, é possível de se detectar que a maioria das proposições de segurança da informação que as empresas estão implementando atualmente, também foram abordadas pela Política de Segurança estudo, evidenciando que a empresa estudada está atenta aos perigos, às necessidades e aos meios de se manter uma informação segura, confiável, íntegra, confidencial, disponível e rapidamente acessível aos usuários com permissão. Conforme Tabela 20, a seguir, na Política de Segurança implementada, todos os tópicos contidos na mesma foram abordados, o que mostra que a empresa está bastante sintonizada com o que está acontecendo nas outras empresas sobre o assunto.

Tabela 20 – Medidas Implementadas

| **POSIÇÃO** | MEDIDAS IMPLEMENTADAS | **2000 (%)** | **2001 (%)** |
|---|---|---|---|
| 1º | **Firewall** | 89 | 83 |
| 2º | Prevenção Contra Vírus | 93 | 78 |
| 3º | Proxy Server | 69 | 71 |
| 4º | Segurança na Sala dos Servidores da Rede | 72 | 62 |
| 5º | Sistema de Back-up | 91 | 61 |
| 6º | Software de Controle de Acesso | 65 | 61 |
| 7º | Monitoração de Log | 58 | 56 |
| 8º | Cofre Anti-incêndio | 62 | 43 |

| | | | |
|---|---|---|---|
| 9º | Fragmentadoras de Papel | 60 | 41 |
| 10º | Plano de Contingência | 59 | 41 |
| 11º | Capacitação e Treinamento | 52 | 40 |
| 12º | Termo de Responsabilidade | 49 | 40 |
| 13º | Contratação de Empresas Especializadas | 35 | 40 |
| 14º | Prevenção Contra Pirataria de Software | 54 | 39 |
| 15º | Sistema de Detecção de Intrusos | - | 37 |
| 16º | Sistema de Criptografia | 48 | 35 |
| 17º | Procedimentos Formalizados | 34 | 33 |

## 8.4 DIFICULDADES ENCONTRADAS NA IMPLEMENTAÇÃO

Em relação às dificuldades encontradas, pode-se citar:

- Dificuldades para se criar o grupo GSI com os integrantes disponíveis para que além de executarem suas atividades normais, ainda terem que assumir o trabalho adicional da segurança da informação.
- Dificuldade de conseguir conciliar as diretrizes que deveriam atender às filias da empresa, pois pertencem a outras diretorias, em outros estados e com costumes diferentes.
- Disponibilidade de equipamento (servidor de correio eletrônico) para a execução de testes com a ferramenta Groupshield.
- Disponibilidade de recursos financeiros para a implementação dos recursos necessários da Política.
- Houve uma grande dificuldade no momento da implementação da Política, pois os profissionais se mostraram resistentes a assinar os termos de confidencialidade da informação, acreditando que a empresa não os estava conscientizando e sim desconfiando de que os mesmos estariam enviando as informações para terceiros.
- Houve resistência também para assinatura dos termos por parte das empresas de Terceiros, pois os mesmos ficaram receosos de que a empresa pudesse no futuro, tendo posse dos termos de compromisso assinado por elas, poderia acioná-las judicialmente por qualquer problema que houvesse de perda de informação ou de algum dado encontrado em outras empresas que elas também prestavam serviços.
- Quanto a pirataria de *software*, houve uma preocupação muito grande também quanto ao funcionário e ao microcomputador utilizado pelo mesmo para trabalho, ou seja, enquanto a empresa não apresentou uma relação contendo todos os *softwares* que compunham cada microcomputador, mostrando claramente que todos os aplicativos existentes estavam legalizados

e que, a partir daquele instante se iniciaria o processo de auditoria com a responsabilidade daquele usuário, o usuário não se mostrou confiante e receptivo àPolítica.

- Antes da instalação da Política de Segurança da Informação, arquivos de pornografia e jogos eram encontrados em toda a rede e nos microcomputadores utilizados pelos usuários. A empresa não tinha qualquer documento assinado pelos usuários dando ciência de que os mesmos poderiam ser demitidos por Justa Causa devido a tais atitudes. A partir do compromisso assinado, a empresa passou a ter um documento no qual o funcionário assinou, deu sua ciência sobre as normas da mesma e o seu consentimento para que tanto seu microcomputador, como também sua área da rede, pudesse ser monitorada e sofrer auditorias.

Foram necessárias muitas reuniões e conscientizações, divulgações das cartilhas explicativas, bem como alguns exemplos práticos, deixando bem evidente que a intenção da empresa não era punitiva, num primeiro momento, e sim de orientação para se resolver os problemas de pirataria que estivessem sendo detectados e que as punições contra pirataria de software somente viria numa etapa posterior, após toda a exclusão de aplicativos indevidos, inclusive do tipo *freeware*, que é de livre uso e também disponível na *internet*.

## CAPÍTULO IX

## CONCLUSÃO

A presente pesquisa representou um estudo das principais teorias desenvolvidas no tocante à segurança da informação, aos fatores que colocam em risco as organizações e os negócios na atualidade. Com a evolução tecnológica da computação, o uso da *Internet* e do correio eletrônico, os problemas evoluíram a ponto de a comunicação informatizada ser ameaçada por um dos principais fatores que causam perigo àdisponibilidade da informação das empresas: o Vírus de Computador.

O objetivo principal desta pesquisa foi o de se efetuar um estudo do conceito da Informação nas organizações, refletindo tópicos como estratégia, sistemas informatizados, competitividade provida pela informação correta, acessível, íntegra e rápida. Uma das maneiras de atingir tal segurança é a implementação de uma Política de Segurança da Informação, que pode contribuir para a melhoria da segurança

necessária à continuidade do negócio das empresas e, neste caso em particular, com o foco para o problema do *e-mail* com arquivo contaminado por vírus de computador.

Com o estudo de caso e a aplicações de princípios baseados na literatura estudada sobre o assunto, ficou evidente uma considerável melhoria nas condições de proteção das informações existentes na empresa, pois na mesma não havia qualquer norma, diretriz ou procedimento escrito, aprovado e que estivesse sendo seguido pelos usuários. Foi graças à Política de Segurança da Informação implementada que se observou a melhoria na segurança dos dados armazenados nos servidores da empresa, bem como a proteção contra vírus de computadores. Os termos de compromisso assinados por todos os profissionais, que evidenciaram a confidencialidade da informação e penalidades em caso de instalação de softwares ilegais, proporcionaram uma maior preocupação e comprometimento de todos os funcionários em não instalar softwares inadequados, como também em não divulgar projetos e dados da empresa para terceiros. As auditorias periódicas internas efetuadas nos microcomputadores dos usuários fortaleceram o processo de conscientização e eliminação de softwares considerados ilegais existentes. Este processo também foi auxiliado pela adoção da sistemática de eliminação das opções para instalação de aplicativos e desconfiguração dos microcomputadores por parte dos usuários, houve uma contribuição considerável na padronização dos aplicativos utilizados, sempre baseada em um completo inventário de hardware e software efetuado anteriormente. O processo como um todo por um lado trouxe uma melhoria na confiança dos usuários com relação às informações armazenadas nos servidores e uma certeza de que as mesmas estariam íntegras para desempenho de suas funções profissionais e para apoio sua tomada de decisões.

A implementação da Política, no entanto, não foi de todo simples. Existiram momentos delicados e polêmicos, principalmente no instante da apresentação e divulgação da Política. Apesar de se ter aprovação por parte da alta direção da empresa, houve resistência e insegurança por parte dos profissionais quanto às novidades que estariam sendo observadas a partir daquela data. As dificuldades para se conseguir formar um grupo de profissionais que concordassem com a determinação de que além de terem sua carga de trabalho normal, também deveriam assumir novas funções junto ao Grupo de Segurança da Informação, o GSI, pois efetuar contratação de mão-de-obra externa não traria solução imediata, pois seriam necessários profissionais que conhecessem do negócio para conseguirem obter sucesso. Surgiram problemas imprevistos, por exemplo, a dificuldade de se conseguir conciliar as mesmas diretrizes para atender às filiais da empresa, pois apesar de pertencerem à mesma organização,

encontravam-se em locais pertencentes a outras diretorias, em outros estados, com costumes e hábitos diferentes.

Um fator que também gerou dificuldade no início do projeto foi a necessidade de se ter um equipamento para ser utilizado como servidor de correio eletrônico quando da execução de testes com a ferramenta *Groupshield*. A disponibilidade de recursos financeiros para a aquisição das ferramentas e *softwares* para a implementação dos recursos necessários da Política também causou problema. Com relação aos profissionais da organização, houve uma grande resistência a assinar os termos de confidencialidade da informação. Estas pessoas acreditavam que a empresa não mais estava confiando nelas. Pensavam que a organização iria penaliza-los na primeira oportunidade que tivesse comprovação, gerando motivo para uma demissão por Justa Causa. Os documentos dos termos para assinatura foram vistos como objetos punitivos e não apenas de conscientização para o problema. Tal fato também se mostrou evidente com os parceiros terceirizados, pois os mesmos passaram a acreditar que a empresa poderia acioná-los juridicamente e culpando-os por qualquer problema que pudesse ser constatado –- de desvio de informação –- para empresas também parceiras deles.

Quanto ao assunto da pirataria de *software,* os funcionários se mostraram bastante preocupados. Alegavam que não poderiam se responsabilizar pelos aplicativos instalados em seus microcomputadores de trabalho, tendo em vista que tal equipamento também era compartilhado para uso por outras pessoas em seu departamento. A solução adotada foi a de se apresentar um relatório fruto de um detalhado inventário de *software* e *hardware* existente em cada equipamento e, a partir daquele instante o usuário seria o responsável por manter aquelas configurações e, caso houvesse a necessidade de instalação de qualquer novo aplicativo, o mesmo seria adquirido e instalado pelos profissionais do departamento de Informática. As auditorias que viriam a ser realizadas no futuro serviriam apenas para constatar algo firmado e assinado e, caso houvesse qualquer divergência, seria o momento de se efetuar uma análise mais criteriosa.

Houve a necessidade de treinamento, conscientização e divulgação de exemplos práticos, simulações diversas, bem como várias orientações aos funcionários para que entendessem que o objetivo da empresa era o de garantir a segurança de suas informações e não de iniciar um processo punitivo e de demissões por Justa Causa. Esta diretriz foi um fato observado numa primeira etapa, na qual deu-se ênfase à conscientização e orientação para se resolver os problemas de pirataria que estivessem sendo detectados e que as punições contra qualquer distorção da Política somente viria num momento posterior, após as auditorias e de toda a regularização dos aplicativos

indevidos, inclusive na eliminação dos *softwares* do tipo *freeware* e de livre disponibilidade na *internet*.

A pesquisa abordou inicialmente os conceitos relacionados à sociedade, à informação, à comunicação a distância entre as pessoas, às universidades e às organizações por meio de sinais elétricos, o crescimento dos recursos informatizados, o armazenamento das informações e à fragilidade dos dados armazenados nas empresas frente a possíveis ataques por meio de vírus de computadores. Procurou-se ressaltar a importância dos sistemas de informação e a informação íntegra, disponível e confidencial como fator estratégico para a tomada de decisões pelos executivos das empresas.

Efetuou-se uma abordagem teórica sobre os conceitos de Redes de Computadores, Protocolos, Segurança nos Centro de Processamento de Dados, bem como dos conceitos de Política de Segurança da Informação. Houve uma ênfase às teorias relacionadas ao Correio Eletrônico, sua fragilidade e a citação de algumas ferramentas utilizadas para sua proteção, como também sobre vírus de computador e os riscos que os mesmos apresentam às empresas. Ao final apresentou-se o resultado obtido com o estudo de caso como um exemplo prático da aplicação da teoria pesquisada.

Esta pesquisa não teve o objetivo de efetuar uma abordagem profunda do assunto segurança da informação com foco em medidas de proteção das empresas contra ataques de *Hackers*, pois para tratar deste assunto seria necessário um aprofundamento muito maior nos conceitos e ferramentas relacionadas à segurança em Redes de Computadores e nas estações de trabalho dos usuários. Também não foi abordado com profundidade sobre as leis de software e que estão tramitando no Congresso Nacional Brasileiro, bem como das penalidades para cada caso existente.

Houve sim, conforme observado no estudo de caso, uma preocupação com o fator humano e que o mesmo pudesse ser conscientizado da importância da sua contribuição para a melhoria contínua da proteção das informações da empresa, bem como que acatasse as determinações e normas aprovadas pelo Comitê Executivo. A empresa acredita que somente desta maneira, seria possível adotar uma ação preventiva e não corretiva –- sob o aspecto segurança da informação –-, para se basear com um pouco mais de segurança nas informações armazenadas nos servidores para trabalho e tomada de decisão.

O assunto sobre segurança da informação é bastante vasto e a cada novo dia surgem novas necessidades de proteção e ação de Políticas de Segurança, desta forma,

abaixo estão relacionadas algumas sugestões para novas pesquisas abordando o mesmo tópico, ou seja:

Existe uma carência muito grande sobre uma Política de Segurança da Informação para Hospitais, Centros de Saúde, Centros Cirúrgicos, Hemonúcleos, Creches e entidades que trabalham o tempo todo com a saúde e a vida humana, como também, uma Política voltada para assuntos Jurídicos e controles Administrativos das Delegacias de Polícia, Processos Judiciais e Órgãos Governamentais de controle carcerário.

Como foco mais voltado para a área de Tecnologia da Informação, seria interessante uma Política desenvolvida e voltada para *Firewall* de rede, específica para a segurança de um Provedor de Internet, bem como uma Política voltada para o controle de Veículos, documentações relativas a Multas, Processos e furtos de veículos, como também para todas as informações relacionadas a veículos e impostos relacionados aos mesmos.

Com relação ao Social e aos Órgãos Governamentais, aos assuntos do governo, servindo como auditoria segura em caso de fraudes e escândalos, seria importante uma Política de Segurança da Informação para o Controle do Cadastro de Funcionários das Empresas para a Geração da *RAIS* (Relação Anual de Informações Sociais), Cadastros dos Profissionais Pensionistas Aposentados, como também um controle da Informação Imóveis existentes nos Estados e nas cidades.

Existe uma área extremamente delicada e que exige segurança máxima, que é o Sistema de Informação para Aeroportos, incluindo todo o processo de triagem de passageiros, saída e chegada de aeronaves e controle do tráfego aéreo, como também para o Sistema Metroviário, controle do tráfego de trens e desvios de linhas.

Enfim, toda Política de Segurança da Informação é semelhante no tocante à proteção de dados, dos equipamentos de informática ao nível de *software* e *hardware*, porém, quando se trata do controle do fluxo da informação, para cada negócio e segmento do mercado em que a mesma deverá ser aplicada, são necessárias especificações criteriosas e detalhadas para que se obtenha o resultado esperado.

Baseando-se nos resultados apresentados e na melhoria da segurança das informações obtida pela empresa, conclui-se que a Política implementada foi válida. Os resultados foram obtidos com sucesso. Garantiram a proteção da informação existente no correio eletrônico, como também disponibilizou segurança às bases de dados dos usuários localizadas no servidor de *e-mail*, o que gerou credibilidade nas informações utilizadas para a tomada de decisões na empresa. Um fator importante também a ser ressaltado, é que a empresa recebe e envia um total de aproximadamente vinte e um mil

*e-mails* diariamente. A Companhia conseguiu ficar imune aos ataques de vírus provenientes do correio eletrônico, como também não disseminou mensagens com arquivos contaminados com vírus para fornecedores, clientes e demais parceiros de trabalho.

## REFERÊNCIAS BIBLIOGRÁFICAS

AKIYAMA, Erika M., CUSTÓDIO, Alvina M. *Proposta de Política de Segurança Interna para a Universidade de Taubaté*. Monografia de Graduação no Curso de Bacharelado em Computação, Departamento de Informática da Universidade de Taubaté – UNITAU. Taubaté: UNITAU, 1999.

AMERICANO, Tatiana. *Cuidado Com As Invasões*. Revista Network Computing Brasil, São Paulo: it.midia, ano 2, n. 20, p. 36, out. 2000.

ARONSON, Jules P., BROWNLEE, Nevil. *Redes de Computadores e suas Aplicações na Educação – Política de Segurança*. Universidade Federal do Rio Grande do Sul. Rio Grande do Sul: UFRGS, 1997. Consultado na INTERNET, em 25/11/01.http://penta.ufrgs.br/gereseg/rfc2196/.

BAKER, Richard H. *Network Security: How to plan for it and achieve it*. New York: McGraw-Hill, 1995.

BEUREN, Ilse M. *Gerenciamento da Informação: Um Recurso Estratégico no Processo de Gestão Empresarial*. São Paulo: Atlas, 1998.

CARUSO, Carlos A. A., STEFFEN, Flavio D. *Segurança em Informática e de Informações*. São Paulo: Senac, 1999.

CERVO, A.L. *Metodologia Científica: para uso dos estudantes universitários*, 3ª ed. São Paulo, McGraw-Hill, 1983.

CHAMON, Marco A. *Gerenciamento de Risco em Projetos Espaciais: O Caso Brasileiro*. São José dos Campos: INPE, 2001.

CORRÊA, Nelson. *Amor ou Falta Dele Custou ao Mundo Alguns Bilhões de Dólares*. Consultado na INTERNET em 20 de Dezembro de 2001. www.modulo.com.br/, Novembro 2001.

DAVENPORT, Thomas H., PRUSAK, Laurence. *Ecologia da Informação: Por Que só a Tecnologia não Basta Para o Sucesso na Era da Informação*. Tradução Bernadete Siqueira Abrão. São Paulo: Futura, 1998.

DREYFUSS, Cássio. *Como se Proteger?* Revista Network Computing Brasil, São Paulo: it.midia, ano 2, n. 16, p. 53, Junho 2000.

FONTES, Edison. *Os Dez Mandamentos*. Revista Network Computing Brasil, São Paulo: it.midia, ano 2, n. 18, p. 18, Agosto 2000.

FONTES, Edison. *Política de Segurança da Informação*. Consultado na INTERNET em 20 de Dezembro de 2001. www.pobox.com/. Agosto 2000.

GIL, Antonio C. *Como Elaborar Projetos de Pesquisa*. 3ª ed. São Paulo: Atlas, 1996.

GONÇALVES, Sérgio R.M. *A Internet, o e-mail e a (In)Segurança das Empresas*. Consultado na INTERNET em 18 de Dezembro de 2001.www.modulo.com.br/. Novembro 2001.

GRAÇA, Antonio. *Sem Segurança Não Tem Negócio*. Revista Network Computing Brasil, São Paulo: it.midia, ano 2, n. 16, p. 47, Junho 2000.

GRIMBERG, Marcelo. *e-mail,30*. Jornal Folha de São Paulo – Caderno Folha Informática, São Paulo: Folha de São Paulo, ano 2001, p.1, Outubro 2001.

HAICAL, Cristiane. *Worm Sircam*. Consultado na INTERNET em 26 de Julho de 2001.www.modulo.com.br/. Julho 2001.

HASHIOKA, Mauro H., SALGADO, Antonio E. *Apostila de Redes de Computadores*, Taubaté: Universidade de Taubaté – UNITAU,1995.

HITECH IND. COML. LTDA. *Apostila de Introdução àSegurança da Informação* , São Paulo: Hitech, 1998.

LAKATOS, E.M. MARCONI, M.A. *Fundamentos de Metodologia Científica*. São Paulo: Atlas, 1985.

LEITE, Celso H. *Vírus de Computador: Inimigo Número Um*. Consultado na INTERNET em 27 de Dezembro de 2001. www.modulo.com.br/. Agosto 2001.

LOPES, Fábio. *A Fortaleza Dos Negócios*. Revista Network Computing Brasil, São Paulo: it.midia, ano 1, n. 12, p. 30, Fevereiro 2000.

LUZ, Giovani A ., REIS, Gutierres B. *Proposta de Política de Segurança e de Arquiteturas de Firewall para a Universidade de Taubaté*. Monografia de Graduação no Curso de Bacharelado em Computação, Departamento de Informática da Universidade de Taubaté – UNITAU. Taubaté: UNITAU, 1999.

McCLURE, Stuart, SCAMBRAY, Joel, KURTZ, George. *Hackers Expostos – Segredos e Soluções Para a Segurança de Redes*. São Paulo: MAKRON Books, 2000.

MÓDULO SECURITY SOLUTIONS. *4ª Pesquisa Nacional Sobre Segurança da Informação 1998*. Consultado na INTERNET em 01 de Dezembro de 1999.www.modulo.com.br/, 1998.

MÓDULO SECURITY SOLUTIONS. *5ª Pesquisa Nacional Sobre Segurança da Informação 1999*. Consultado na INTERNET em 10 de Novembro de 2001.www.modulo.com.br/, 1999.

MÓDULO SECURITY SOLUTIONS (1). *6ª Pesquisa Nacional Sobre Segurança da Informação 2000*. Consultado na INTERNET em 29 de Junho de 2000.www.modulo.com.br/, 2000.

MÓDULO SECURITY SOLUTIONS (2). *Vírus Polimórficos*. Consultado na INTERNET em 20 de Julho de 2000.www.modulo.com.br/, 2000.

MÓDULO SECURITY SOLUTIONS (3). *Vírus de Boot*. Consultado na INTERNET em 26 de Julho de 2000.www.modulo.com.br/, 2000.

MÓDULO SECURITY SOLUTIONS (1). *7ª Pesquisa Nacional Sobre Segurança da Informação 2001*. Consultado na INTERNET em 30 de Julho de 2001.www.modulo.com.br/, 2001.

MÓDULO SECURITY SOLUTIONS (2). *Novos e Perigosos Vírus Atacarão em 2002. (O que Podemos Esperar no Próximo Ano?)*. Consultado na INTERNET em 29 de Dezembro de 2001.www.modulo.com.br/, 2001.

MÓDULO SECURITY SOLUTIONS (3). *Vírus Scherzo Atinge 92 Países*. Consultado na INTERNET em 27 de Dezembro de 2001.www.modulo.com.br/, 2001.

MOURA, Adriana C. *Esquema de Fire Wall para Segurança de Redes*. Monografia de Graduação no Curso de Bacharelado em Computação, Departamento de Informática da Universidade de Taubaté – UNITAU. Taubaté: UNITAU, 1996.

MOREIRA, Nilton S. *Segurança Mínima Uma Visão Corporativa da Segurança de Informações*. Rio de Janeiro: Axcel Books, 2001.

OLIVEIRA, Djalma de P. R. *Sistemas de Informações Gerenciais: Estratégicas, Tática Operacionais*. São Paulo: Atlas, 1993.

OLIVEIRA, Wilson J. de. *Segurança da Informação Técnicas e Soluções*. Florianópolis: Visual Books, 2001.

OVERLY, Michael R. *e-policy: How to develop computer , E-mail and Internet guidelines to protect your company and its assets*. New York: Amacom, 1999.

PAGLIUSI, Paulo S. *Introdução de Mecanismos de Segurança em Sistemas de Correio Eletrônico*. Dissertação de Mestrado em Ciência da Computação, Instituto de de Computação da Universidade de Campinas, UNICAMP. Campinas: UNICAMP, 1998.

PENTEADO, Sônia, MARINO, Silvia. *A Hora De Tomar Medidas Drásticas*. Revista InformationWeek Brasil, São Paulo: it.midia, ano 2, n. 27, p. 38, Agosto 2000.

PENTEADO, Sônia. *De Olho Na Segurança*. Revista Network Computing Brasil, São Paulo : it.midia, ano 1, n. 6, p. 26, Julho 1999.

PIMENTA, Cristiano. *Política de Segurança no e-mail Corporativo*. Consultado na INTERNET em 20 de Dezembro de 2001.www.modulo.com.br/, Novembro 2001.

PEREIRA, Cristiane. *Proteção ou Controle*. Consultado na INTERNET em 22 de Dezembro de 2001. www.modulo.com.br/, Outubro 2001.

PLACHTA, Claudio. *Plano de Continuidade de Negócios – Garantindo a Sobrevivência*. Consultado na INTERNET em 23 de Dezembro de 2001. www.modulo.com.br/, Novembro 2001.

SCHIFREEN, Robert. *Data Protection and Security for Persoinal Computers*. London: TTK, 1992.

SÊMOLA, Marcos. *Equacionando a Gestão de Riscos*. Consultado na INTERNET em 23 de Janeiro de 2002.www.modulo.com.br/, Janeiro 2002.

SÊMOLA, Marcos. *2002: Perspectivas para a Segurança da Informação no Brasil*. Consultado na INTERNET em 29 de Dezembro de 2001. www.infoguerra.com.br/, Julho 2001.

SETTE, Adriana A. *Um Guia Para Implantação de Segurança Básica em Sistemas*. Monografia de Graduação no Curso de Tecnologia em Informática. Centro de Ciências Naturais e Exatas da Universidade Luterana do Brasil. Canoas: Universidade Luterana do Brasil, 2001.

SHAFFER, Steven L., SIMON, Alan R. *Network Security.* London: AP Professional, 1994.

SHANG, David J., MOON, Sylvia. *Segredos de Segurança em Rede.* Rio de Janeiro: Berkeley, 1994.

SILVA Jr., Ovídio F.P. da. *Avaliando os Sistemas de Informações Executivas nos processos decisórios das Instituições Universitárias Brasileiras*. Florianópolis, 2000. Dissertação de Mestrado em Engenharia de Produção da Universidade Federal de Santa Catarina.

SOARES, Luiz F. G., LEMOS, Guido, COLCHER, Sérgio. *Redes de Computadores Das LANS, MANS e WANS às Redes ATM* . Rio de Janeiro: Campus, 1995.

SWANSON, Marianne, GUTTMAN, Bárbara. *Generally Accepted Principles abd Practices for Securing Information Technology Systems*. Consultado na INTERNET em 20 de Agosto de 2001. www.nist.gov/, Agosto 2001.

TANENBAUM, Andrew S. *Redes de Computadores*. Rio de Janeiro: Campus, 1994.

WLADLOW, Thomas A. *Segurança de Redes*. Rio de Janeiro: Campus, 2000.

_____. *British Standard 7799 – 1*. London: 1999. 44p.

_____. *Case Solectron – Segurança da Informação. Apostila da Apresentação do Projeto de Segurança da Informação*. São José dos Campos: Solectron, Outubro/2000.

_____. *Ranking dos Vírus Mais Ativos*. Consultado na INTERNET em 24 de Dezembro de 2001. www.infoguerra.com.br/, Dezembro 2001.

_____. *Segurança Máxima*. São Paulo: Campus, 1998.

_____. *Vírus & Cia*. Consultado na INTERNET em 24 de Dezembro de 2001. www.ufpa.br/dicas/, Dezembro 2001.

# GLOSSÁRIO DE TERMOS TÉCNICOS

**ABNT**
Associação Brasileira de Normas Técnicas.

**ACL**
Accsses Control List.

**ALGORÍTMO**
Uma expressão lógica que resolve uma fórmula Matemática complexa ou instruções de um programa. Normalmente são utilizados como “Chaves” para criptografia de dados.

**APPLE TALK**
Uma arquitetura de rede da Apple que suporta o acesso proprietário da Apple, Ethernet e Token Ring.

**ARP**
Address Resolution Protocol. Protocolo TCP/IP de baixo nível, utilizado para obter o endereço físico de um ponto de rede quando se conhece apenas seu endereço lógico IP.

**ARPANET**
Advanced Research Projects Agency Network, tecnologia de comutação de pacotes precursora da atual Internet, “nascida” nos EUA.

**ARRAY PROCESSOR**
São conjuntos de processadores de Matrizes.

**ASCII**
American Standard Code for Information Interchange.

**ASSÍNCRONO**
Denominação dada ao equipamento ou tipo de transmissão de dados na qual os caracteres transmitidos são enviados sem relógio de sincronismo entre o transmissor e o receptor. Cada caracter é uma unidade autônoma com seu próprio bit de parada e de início, utilizados para sincronizar o relógio interno do receptor.

**ATTACH**
Nome dado a um arquivo anexado a um e-mail.

**BCC**
Bind Carbon Copy, é a sigla identificando o envio de uma cópia da mensagem a uma terceira pessoa, sendo que o destinatário principal não toma conhecimento deste envio.

**BACKDOORS**
São programas que instalam um ambiente de serviço em um computador, tornando-o acessível àdistância, permitindo o controle remoto da máquina sem que o usuário saiba. É um tipo de vírus.

**BACKGROUND**
Programas executados na retaguarda, ou seja, em ambiente sem a percepção do usuário do microcomputador.

**BACK-UP**
Processo de se executar cópias de segurança de dados em discos ou fitas magnéticas.

**BBS**
Bulletin Board Service.

**BENCHMARK**
Padrão contra o qual o desempenho ou qualidade é comparado.

**BINÁRIO**
Sistema de informação com dois símbolos. Todos os dados que entram em um computador são codificados em dois símbolos representados por zero (0) e um (1).

**BIOMÉTRICA**
Tecnologia de segurança da informação, onde a identificação do usuário para acesso físico a um determinado local ou sistema é feito pela identificação biológica, ou seja, utilizando-se a íris do olho ou as impressões digitais.

**BIOS**
Basic Input Output System.

**BIT**
Binary DigIT, é a menor unidade de informação de um sistema binário, podendo ser representado por Zero e 1.

**BOOT**
Nome designado àárea do disquete ou do disco rígido (Hard Disk) armazenamento de dados dos microcomputadores ou servidores de dados.

**BRIDGES**
São equipamentos conectados a redes de dados que servem como pontes utilizadas para conexão de redes de um

mesmo tipo, segmentando tráfego de dados.

**BROADCAST**

Processo pelo qual se consegue enviar uma mensagem partindo de um único emissor para todos os computadores conectados àrede de dados.

**BUFFER**
Segmentos de memória utilizados para armazenamento de dados durante um determinado processamento.

**BUG**
Nome dado a um problema ou falha em um software, geralmente desenvolvido e comercializado por um fabricante potencial.

**BUG DO MILÊNO**
Nome dado àvirada do ano 1999 para 2000, em que houve centenas de boatos citando que os computadores iriam ficar inativos ou descontrolados.

**BUSINESS**
Termo técnico em Inglês que significa o Negócio das empresas.

**BUSINESS INTELLIGENCE (BI)**
São os sistemas inteligentes voltados aos processos de negócios das corporações empresariais.

**BYTE**
Unidade de armazenamento de informação em computadores.

**CA**
Certification Authority.

**CAPABILITIES**
Capacidade de execução de um determinado processamento.

**Cc**
Carbon Copy, cópia carbono, sigla referenciando o envio de uma cópia da mensagem a uma outra pessoa.

**CCIR**
Comitê Consultatif International des Radiocommunications.

**CCITT**
Comité Consultatif de Télégraphique et Téléphonique.

**CD-ROM**
Compact Disk Read Only Memory, um formato de disco compacto utilizado para armazenar texto, figuras e som estéreo com capacidade de mais de 650 Mega byte, equivalente a aproximadamente 650.000 páginas de texto ou 20.000 páginas de média resolução.

**CHAIN LETTER**

Cartas e mensagens normalmente longas enviadas a um grande número de usuários e sempre solicitando que a mesma seja retransmitida a um outro grupo de usuários, com o intuito de congestionar as redes de dados.

**CHAT**
Tipo de interação em rede comum na Internet, nos quais duas ou mais pessoas digitam e enviam mensagens umas para as outras em tempo real.

**CHAVE**
É uma cadeia aleatória de *bits* utilizada em conjunto com um algoritmo.

**CHAVE PÚBLICA**
Campo existente em um banco de dados para acesso às informaç ões armazenadas.

**CHECK POINT**
Denominação de um *software Firewall* distribuído pela empresa Computer Associate.

**CHECKSUM**
Valor usado para assegurar que os dados sejam transmitidos sem erro.

**COBOL**
Common Business-Oriented Language. Linguagem de programação em computador compilada e de alto nível utilizada principalmente em aplicações comerciais executadas em computadores tipo *Mainframes*. Caracterizada por grande volume de dados de entrada, pouco processamento da CPU do computador e grande volume de saída de resultados em forma de listagens.

**COMUTAÇÃO**
Processo de troca de conexões entre circuitos e direcionamento de pacotes entre equipamentos de rede.

**CPD**
Centro de Processamento de Dados.

**CRIBS**
Nome dado a um ou mais pares de mensagens com um texto cifrado e seu respectivo texto claro, empregando a mesma chave criptográfica.

**CRIPTOANÁLISE**
Ciência que estuda a leitura do tráfego cifrado de mensagens sem conhecer o conteúdo dos textos cifrados sem que se seja o legítimo destinatário.

**CRIPTOGRAFIA**
Processo pelo qual um arquivo ou informação é codificado por meio da ação de um programa de computador para armazenamento ou envio por correio eletrônico.

**CSI**
Computer Security Institute.

**DARPA**
Defense Advanced Research Projects Agency.

**DATAGRAMA**
Mensagem do protocolo TCP/IP que contém os dados, o endereço do remetente e do destinatário na Internet.

**DCMP**
*Digital Certified Mail Protocol.*

**DECRIPTOGRAFIA**
Processo pelo qual um arquivo ou informação é decodificado por meio da ação de um programa de computador.

**DEMULTIPLEXAR**
Desmontar um sinal agregado em seus vários canais componentes.

**DES**
Data Encryption Standard.

**DHCP**
Dynamic Host Configuration Protocol. Software incluso nos Sistemas Operacionais Windows 2000, Windows NT 4.0 Server, Windows NT 4.0 Workstation, Windows 98 e Windows 95, da empresa Microsoft, e que atribui automaticamente endereços IP (TCP / IP) às estações conectadas àrede de dados.

**DISKLESS**
Característica que informa que o equipamento (microcomputador) não possui disco rígido para armazenamento de dados.

**DL/1**
Tipo de banco de dados utilizado em computadores *Maninframes*, cuja característica principal de armazenamento de dados é o Método Hierárquico.

**DNS**
Domain Name System.

**DoD**
Nome genérico dado ao conjunto de protocolos pertencentes àfamília TCP/IP.

**DOS**
Sistema Operacional desenvolvido pela empresa Microsoft, também conhecido por MS-DOS.

**DoS**
Denial of Service (Interrupção de Serviço).

**DOWNLOAD**
Transferência de um arquivo de um computador para outro, ou pode ser ainda, a transferência de um arquivo de um servidor da Internet para um computador de um determinado usuário. Pode ser executado por meio de comandos http ou Ftp.

**DOWN-SIZE**
Nome dado ao processo de efetuar uma migração do uso dos recursos de Informática providos por plataformas tipo *Mainframe* para outras plataformas menores, menos robustas e com um custo de manutenção relativamente também menor.

**DUPLEX**
Transmissão de dados em duas direções, porém uma em cada sentido de cada vez.

**E-MAIL**
Electronic Mail, o mesmo que Correio eletrônico.

**EBCDIC**
Extended Binary-Coded Decimal Interchange Code, código binário da IBM para textos.

**EDI**
Electronic Data Interchange.

**EIA**
Electronic Industries Association

**EMBRATEL**
Empresa Brasileira de Telecomunicações.

**ERP**
Enterprise Resource Planning.

**ESM**
Enterprise Security Management.

**ETHERNET**
Rede local desenvolvida pela empresa Xerox, Digital e Intel.

**EXPLOITS**
Ferramentas de ataques automáticos e métodos de explorar vulnerabilidades não corrigidas.

**EXTRANET**
É o nome dado àrede formada inter ligando a Intranet entre as diversas empresas, facilitando a comercialização entre elas.

**EUA**
Estados Unidos da América.

**E-MAIL**
Electronic Mail.

**FAC-SIMILE (FAX)**
Originalmente chamado de Telecópia, é a comunicação de uma página impressa entre localidades remotas pelo processo de codificação da imagem sobre o papel e a transmissão por linhas telefônicas. A máquina na recepção imprime um fac-símile do original.

**FILE SYSTEM**
Sistema de arquivos.

**FIREWALL**
Sistemática que promove a segurança em rede por meio de *software* e *hardware*.

**FORWARD**
Processo de se retransmitir um e-mail recebido a outras pessoas.

**FRAME RELAY**
Rede de comutação de pacotes semelhante ao X.25, mas sem verificação de erros e com altas taxas de transmissões de Pacotes de dados.

**FREEWARE**
Software que pode ser usado, copiado ou distribuído sem qualquer custo.

**FTP**
File Transfer Protocol. Conjunto de comandos usados para acessar diretórios e copiar arquivos em rede TCP/IP (Internet, Unix, etc...).

**FULL-DUPLEX**
Transmissão de dados em duas direções simultaneamente.

**GATEWAY**
Equipamento físico (*hardware*) que permite a interligação entre duas redes de dados.

**GBPS**
Giga-Bit por segundo.

**GENER / OL**
Linguagem de programação em computador compilada e de alto nível utilizada principalmente em aplicações comerciais executadas em computadores tipo *Mainframes*. Especializada em operações de transações do tipo *On-Line*.

**GIGA**
Prefixo que designa um bilhão.

**GIGA-BIT ETHETNET**
Tecnologia que adapta o modelo Ethernet para transmissão de dados a 1 *Gbps* ou maior.

**HACKER**
São técnicos altamente especializados em computadores e que por prazer ou desafio, acessam e invadem computadores de outras pessoas, universidades, empresas, bancos e órgãos governamentais.

**HALF-DUPLEX**
Transmissão de dados em duas direções, porém em uma direção de cada vez.

**HANDSHAKE**
Sinais de Controle enviados entre as partes envolvidas na comunicação para o estabelecimento de uma conexão válida.

**HARD DISK**
Dispositivo componente interno dos computadores cuja função é a de armazenar os dados de trabalho.

**HDLC**
High-Level Data Link Control, protocolo de comunicação do Modelo I.S.O utilizado em redes de Comutação de pacotes do tipo X.25 com correção de erros na Camada de Enlace.

**HELP-DESK**
Grupo de profissionais responsáveis por todo o suporte técnico de hardware e software para a microinformática dentro das dependências da organização.

**HOME PAGE**
Página inicial da *Internet* de fabricantes e organizações diversas.

**HOT PLUGABLE**
Tecnologia existente nos computadores servidores de dados fabricados pela IBM, Compaq, HP e DELL, na qual é possível remover um disco danificado, mesmo com o equipamento ligado e em funcionamento, e instalar um disco novo sem que haja qualquer dano físico ao *hardware*.

**HOT SWAP**
Tecnologia existente nos computadores servidores de dados fabricados pela IBM, Compaq, HP e DELL, na qual é possível a reconstituição dos dados gravados em um novo disco – a partir dos outros discos existentes –, após a remoção de um disco danificado, mesmo com o equipamento ligado e em funcionamento, sem que haja qualquer dano físico ao *hardware*.

**HTML**
Hypertext Markup Language, linguagem utilizada para desenvolvimento de páginas na Internet.

**HARDWARE**
Qualquer dispositivo elétrico ou eletrônico componente de computadores ou dispositivo componente dos mesmos.

**HOAX**
Mensagem que conta uma estória mentirosa, como por exemplo, vírus por *e-mail*.

**HOMEBANKING**
Nome dado à sistemática de se poder efetuar ações bancárias da própria residência, por meio de um computador conectado à Internet e ao banco.

**HOME PAGE**
Página Inicial da Internet de fabricantes ou empresa.

**HOSPEDEIRO**
Pode ser considerado como um computador principal em uma rede e que efetua a comunicação com as outras redes externas.

**HOSTS**
Computador ou servidor central em uma rede que, normalmente pode efetuar a comunicação à rede interna com as redes externas à organização.

**HOST UNKNOWN**
Computador ou servidor central em uma rede não reconhecido.

**HTTP**
Hypertext Transfer Protocol, protocolo cliente / servidor utilizado para conectar servidores na *Internet*.

**IAB**
Internet Architecture Board.

**IBM**
Sigla característica da empresa IBM - International Business Machine.

**IDS**
Intrusion Detection Systems.

**ICMP**
Internet Control Message Protocol.

**IEC**
International Electrotechnical Commision.

**IEEE**
Institute os electrical and Electronics Engineers

**IETF**
Internet Engineering Task Force, que é um Comitê especial que define os padrões para o protocolo TCP / IP.

**INT 8, 1Ch**
Interrupções do cronômetro, para isso os vírus também interceptam estas interrupções, além das ligadas aos dos serviços do disco.

**INT 13h**

Interrupção da verificação dos dados lidos do disco dos computadores.

**INT 21h**
Interrupção das funções do DOS.

**INT 40 h**
É a interrupção utilizada em operações com discos flexíveis.

**INTEL**
Nome da empresa eletrônica que desenvolveu o projeto dos processadores para computadores padrão IBM / PC.

**INTERFACE**
Fronteira compartilhada, ponto físico de demarcação entre dois dispositivos, procedimentos, códigos e protocolos que permitem que duas entidades troquem informações.

**INTERNAUTA**
Nome dado ao usuário da Internet.

**INTERNET**
É a maior rede de comunicação entre computadores, empresas, residências, universidades, órgãos governamentais, bancos e etc..., Também é conhecida como WWW (World Wide Web).

**INTRANET**
É o nome dado à rede Internet formada internamente nas empresas e universidades, interligando os vários departamentos.

**IP (INTERNET PROTOCOL)**
É o protocolo (conjunto de regras gerenciadas via software) da Internet, com o qual todos os computadores e dispositivos de rede se comunicam.

**IP ADDRESS SPOOFING**
Falsificação de endereço IP.

**IPRA**
Internet PCA Registration Authority.

**IRTF**
Internet Resources Task Force.

**I.S.O**
International Organization for Standardization.

**ITU-T**
International Telecommunications Union – Telecommunications.

**JOBS**
Tarefa a ser cumprida por um processador ou computador.

**JUNK MAIL**
Também é um tipo de SPAM, e-mail não autorizado e enviado em larga escala.

**LAN**
Local Área Network, é uma rede local.

**LINK**
Formato de uma rede permanente ou um elo temporário de comunicação entre computadores.

**LOG**
Arquivo contendo informações relacionadas a uma execução de rotina ou de software, onde são registrados todos os detalhes quanto à data de início e término, como também problemas que possam ter acontecido durante o processamento.

**LOGIN**
Processo de se conseguir obter acesso a uma rede de computadores.

**LOGOUT**
Processo de se encerrar o acesso a uma rede de computadores.

**LOOP**
Caminho circular total percorrido por um sinal, corrente elétrica ou rotina de um programa de computador.

**LOOPBACK**
Condição de um canal de comunicações em que a interface de transmissão conectada à da recepção para fins de teste ou de manutenção de uma topologia de Anel redundante.

**LOTUS NOTES**
Software de Correio Eletrônico desenvolvido pela empresa Lotus, atualmente adquirida pela empresa IBM.

**MAIL**
Mensagem de Correio Eletrônico, o mesmo que E-Mail.

**MAIL BOMB**
Mensagem-Bomba: consiste em enviar e-mails gigantescos com o intuito de causar sobrecarga nos servidores ou no usuário final.

**MAILBOX**
Localidade de armazenamento de mensagens de correio eletrônico ou de voz.

**MAINFRAMES**
Sistema de computador de grande porte que pode abrigar software abrangente, vários periféricos e uma rede de computadores com múltiplos usuários.

**MAN-IN-THE-MIDDLE**
(O Homem do Meio). Tipo de ataque a e-mail onde um usuário se mascara de um segundo usuário para um terceiro e se faz passar por terceiro perante o segundo, se interpondo na troca de mensagem.

**MARKETING**
Área da empresa com enfoque comercial dos produtos para vendas e promoções.

**MBPS**
Mega Bits por Segundo. Padrão de medida da taxa de dados e capacidade de transmissão. 1 Mbps equivale a 1.000.000 Bits por segundo.

**MBR**
Master Boot Record.

MESSAGE DIGEST
O mesmo que Valor Hash. Funciona como uma impressão digital que possibilita a distinção entre uma mensagem e outra, mesmo se ambas se diferirem por apenas um bit.

**MIB**
Management Information Base.

**MICROSOFT**
Uma das maiores empresas fabricantes de software voltado para plataforma de microcomputadores pessoais.

**MIME**
Multipurpose Internet Mail Extensions.

**MODELO DE REFERÊNCIA OSI**
Reference Model Open Systems Interconnection.

**MODEM**
MOdulator-DEModulator, é um dispositivo que adapta os sinais digitais de um computador ou terminal para os sinais de áudio de uma linha telefônica e vice-versa.

**MODERADOR**
É um editor voluntário que proporciona uma melhor qualidade àlista de discussão, agindo como um filtro humano para tópicos relevantes.

**MOSS**
MIME Object Security Services.

**MOTIS**
O protocolo de correio eletrônico da I.S.O .

**MSP**
Message Security Protocol.

**MTA**
Message Transfer Agent, também conhecido como máquinas servidoras de E-mail.

**MUA**
Mail User Agent, também conhecido como UA User Agent.

**MULTIPLEXAR**
Transmitir vários sinais utilizando uma única via de comunicação ou canal.

**NCSA**
National Computer Security Association.

**NETBEUI**
Protocolo para redes Microsoft.

**NETWARE**
Família de Sistemas Operacionais da empresa Novell.

**NETIQUETTE CODE**
Código de Etiqueta da Rede, desenvolvido pela comunidade da Internet. São os também chamados de Emocionícones, Ícones da Emoção (Smiles ou Emoticons).

**NFS**
Network File System

**NIPC**
The National Infrastructure Protection Center, organização de segurança na Internet ligada ao FBI.

**NÓ DE REDE**
Ponto de conexão ou junção de uma rede.

**NOBREAK**
Nome comercial consagrado no Brasil para designar fonte de alimentação que fornecem energia elétrica mesmo após a interrupção por parte das companhias energéticas.

**NOTEBOOK**
Computador portátil contendo teclado, mouse, tela e entradas e saídas padrões de conexões.

**NSCA**
National Computer Security Association. Consórcio de empresas que tem a função de testar e certificar a qualidade de um programa antivírus.

**NVT**
Network Virtual Terminal. Terminal Virtual de Rede.

**ON-LINE**
Condição em que um usuário, terminal ou outro dispositivo está em comunicação ativa com um computador ou recurso de rede.

**OCTETOS**
Em redes de Comutação de Pacotes de dados é um grupo de 8 Bits.

**ORACLE**
Tipo de banco de dados utilizado em computadores servidores atuais, cuja característica principal de armazenamento de dados é o Método Relacional.

**OSI**
Open System Interconnection.

**OUTSOURCING**
Processo de delegação de atividades e funções a empresas que são enquadradas como Terceiros, sem vínculo empregatício.

**PAB**
Public Address Book.

**PASSWORD**
Senha para acesso a algum sistema lógico.

**PACOTES**
Conjunto de bits organizados segundo uma estrutura chamada quadro (frame),contendo informações de controle e dados úteis para a transmissão.

**PCA**
Policy Certification Authority.

**PDZ**
Protocol Data Units.

**PEM**
Privacy Enhanced Mail. Conjunto de procedimentos destinados a prover segurança ao correio eletrônico da Internet.

**PENTIUM**
Processador da série X86 da empresa Intel caracterizado por apresentar alta velocidade e performance na execução de instruções.

**PERIFÉRICOS**

Nome característico de todo equipamento que funciona agregado à CPU de um computador, por exemplo, uma impressora e um Scanner.

**PGP**
Pretty Good Privacy. Programa de Criptografia que provê recursos de sigilo e de autenticação para mensagens eletrônicas e arquivos.

**PING**
Packet Internet Groper, recurso utilizado para determinar quais dispositivos estão ativos em uma rede ou Site da Internet.

**PLANO DE CONTINGÊNCIA**
Plano estratégico para se manter as operações de rede funcionando após uma catástrofe.

**POP3**
Post Office Protocol 3, Protocolo de Agência de Correio 3, relacionado àrecepção e armazenamento de e-mail,

**PORT SCANNING**
Varredura de Portas.

**POSTMASTER**
É o nome dado a uma área de armazenamento, onde as mensagens permanecem até que o usuário execute uma ação de leitura, arquivamento, eliminação ou de transferência para outra área).

**PROCESSOS DAEMONS**
Programas sendo executados na retaguarda, ou seja, em modo background em computadores.

**PROMPT**
Marca de início de linha de comando em Sistemas operacionais de computadores.

**PROTOCOLOS**
Regras que governam a transmissão de dados implementadas via software.

**PROXY SERVER**
Servidor de acesso àInternet.

**PSRG**
Privacy and Security Research Group.

**RAIS**
Relação Anual de Informações Sociais.

**REPLAY**
Segunda ou mais uma tentativa de execução de uma atividade ou procedimento, reprodução.

**RESET**
Comando para limpar, retornar a uma posição inicial, inicializar.

**RESTORE**
Processo de se executar o retorno dos dados gravados em cópias de segurança de dados em discos ou fitas magnéticas.

**RFC**
Request for comments.

**RIP**
Routing Information Protocol.

**RIPEM**
Riordan´s Internet Privacy Enhanced Mail. Implementação assimétrica do padrão PEM. Trata-se de um programa de proteção de e-mail escrito por Mark Riordan.

**ROI**
Retorno sobre o Investimento.

**ROM**
Read Only Memory. Chip de memória que armazena instruções se dados permanentemente.

**ROOT**
Nome dado ao usuário principal de um sistema Unix.

**ROTEAMENTO**
Processo de seleção de rotas para uma mensagem.

**ROUTER (ROTEADOR)**
Equipamento físico (hardware) que permite a interligação de duas redes, uma local e uma externa, dentro da empresa (comunicação entre LAN e WAN).

**RPC**
Remote Procedure Call. Chamadas a Procedimentos Remotos,

**RSA**
Rivest, Shamir e Adleman.

**RS-232**
Padrão recomendado pela EIA (Electronic Data Interchange), para interface mecânica e elétrica, especificando conector tipo DB25)

**RTF**
Rich Text Format. Formato de texto do MS-Word que não é possível àcontaminação por vírus de macro.

**RULES**
Regras de configuração ou otimização de software.

**SAP/R3**
Sistema Integrado de Gestão empresarial desenvolvido pela empresa SAP Alemã.

**SCANNER**
Dispositivo utilizado para ler uma superfície escrita ou com desenhos e figuras e gerar um arquivo digital para ser trabalhado em microcomputadores.

**SCREENSAVER**
São pequenos programas com animações e que são utilizados com proteção de tela para microcomputadores.

**SCRIPTS**
São trechos de códigos de programação.

**SDLC**
Synchronous Data Link Control, protocolo síncrono utilizado pelas redes SNA da IBM.

**S/MIME**
Secure Multipurpose Internet Mail Extensions.

**SECURITY OFFICER**

Profissional com conhecimento de Informática e que representa um grupo de usuários ou um departamento da empresa para os assuntos de segurança da informação.

**SENDMAIL**
Gerenciador de mensagens mais comum no Sistema Operacional UNIX.

**SEQUENCE NUMBER SPOOFING**
Falsificação de números Seqüenciais.

**SHAREWARE**
Software distribuído para demonstração em BBS´s (Bulletin Board Service), provedores de Internet e Home Page (Página Inicial da Internet) de fabricantes.

**SLIP**
Serial Line Interface Protocol.

**SIMPLEX**
Transmissão de dados em uma única direção.

**SISTEMAS DISTRIBUÍDOS**
São sistemas que se localizam em áreas geograficamente distantes e podem se comunicar por meio de linhas de comunicação de dados, sendo que seu processamento tem a característica de ser descentralizado.

**SITES**
São espaços ou páginas disponíveis na Internet para acesso a informações relativas a empresas ou qualquer entidade que queira apresentar informações suas na Internet.

**SMARTCARD**
Tecnologia de segurança da informação, geralmente utilizada para acesso remoto, onde um código temporário é gerado pelo Smartcard que, somado a um número fixo de identificação, forma a senha para acesso a um sistema informatizado e acessando remotamente.

**SMTP**
Simple Mail Transfer Protocol.

**SMURF**
O atacante envia um ECHO_REQUEST ICMP (solicitação de respostas) geral, fazendo um spoof do endereço de origem como endereço IP da máquina alvo solicitando uma resposta (ECO) ICMP a toda a máquina de uma rede, fingindo ser a máquina alvo. Todas as máquinas conectadas respondem as pedido enviando a resposta para a máquina alvo real, sobrecarregando a rede e principalmente o sistema alvo.

**SNA**
Systems Network Architeture. Descrição total da IBM para estrutura lógica, formatos, protocolos e seqüências operacionais para transmissão de unidades de informação entre programas e equipamentos da IBM.

**SND-MSG**
Contração da expressão "send message", ou "envie mensagem".

**SNIFFING**
Grampo ou monitoração de um segmento de rede de dados.

**SNMP**
Simple Network Management Protocol.

**SOCKET**
Identificação de um usuário em uma inter-rede.

**SOFTWARE**

Programa de computador desenvolvido com a finalidade de executar algum procedimento previamente programado.

**SOFTWARE-HOUSE**
Nome característico de empresa do ramo de informática cuja especialidade é a de desenvolvimento de sistemas especialistas.

**SPAM**
Mensagens não solicitadas, especialmente propagandas, que chegam ao computador via e-mail.

**SPAMMER**
Usuário da Internet e de correio eletrônico responsável pelo envio de uma mensagem do tipo Spam.

**SPOOF**
Simulação de endereço em uma rede. Falsificação ou disfarce de identidade.

**SPOOF LOGIN**
Um programa que se apresenta a usuários com prompts, que não são distinguíveis de login regulares e diálogos de senhas, mas de fato armazena a entrada inocente do usuário em um arquivo conveniente para posterior uso ilícito.

**SPOOL**
Simultâneos Peripheral Operation On Line, programa ou equipamento que controla os dados que vão para os dispositivos de saída.

**SQL SERVER**
Tipo de banco de dados utilizado em computadores servidores atuais, cuja característica principal de armazenamento de dados é o Método Relacional.

**STACK OVERFLOW**
Estouro de Pilha.

**STEALTH**
Técnica reservada e para o caso dos vírus polimórficos.

**STM**
Sistema de Transferência de Mensagens.

**STREAM**
Conjunto de estruturas tais como bit, campos e registros.

**STRING**
Conjunto de caracteres que podem ser utilizados para uma determinada pesquisa por programas de computadores.

**SUBSCRIBE**
Pedidos de inclusão em listas de discussão de correio eletrônico.

**SYN**
Synchronous Idle, ou Synchronize sequence number, é o caracter de controle utilizado para manter o sincronismo na ausência de dados trafegando pela rede.

**SYN ACK**
(SYN-ACKNOWLEDGMENT) - Código de comunicação enviado por uma estação receptora para uma estação transmissora, (reconhecendo que os dados transmitidos foram recebidos sem erros ou que a estação receptora está pronta para receber mais dados).

**SYN FLOODIN**
Grande volume de SYN (Synchronize sequence number).

**TCP**
Transmission Control Protocol.

**TDM**
Time Division Multiplexor. Tecnologia de concentração de canais em que o trem de pulsos agregados contém uma amostra da informação de cada canal tributário.

**TELNET**
Protocolo de emulação de terminal normalmente utilizado em aplicações que usam de linha de comando na Internet e que fornece serviços de terminal virtual.

**TEMPLATES**
Tipo e formato de arquivo característico dos produtos da empresa Microsoft S.A, que são modelos prontos para futuras adaptações.

**TFTP**
Trivial File Transfer Protocol. Restringe sua operação simplesmente a transferências de arquivos, não implementando mecanismos de autenticação e operando em uma única conexão

**TICKET**
Cartão ou local onde se encontra armazenado algum dado que possa ser processado por computadores.

**TIMESTAMP**
Controle de tempo.

**TOKEN RING**
Mecanismo de acesso àrede de dados e topologia de Anel em que um pacote de supervisão ou Token trafega de estação em estação procurando quem queira transmitir dados.

**TOKENS**
Frame que busca transmissões em uma rede Token Ring (IBM) ou semelhante.

**TONNER**
Produto semelhante a um pó na cor preto ou colorido que é utilizado em equipamentos de impressão a laser ou em máquinas copiadoras que, quando aquecido a uma temperatura ideal pelo equipamento, o mesmo torna-se afixado em folhas de papel ou transparência e gerando a imagem ou texto desejado.

**TOPOLOGIA**
Relação lógica e física dos pontos dentro de uma rede de dados, sendo que as redes normalmente têm uma topologia em Estrela, Anel, Árvore, Barramento ou uma combinação delas.

**TRANSMISSÃO SÍNCRONA**
É a transmissão na qual os bits de dados são enviados a uma taxa fixa com o transmissor e o receptor, trabalhando exatamente na mesma freqüência.

**TRAP DOOR**
Armadilha.

**TROJAN HORSE**
Nome dado a um tipo de Vírus de computador. Programa ou fragmento de código que se esconde dentro de um programa ou se disfarça de programa legitima, mas atua de forma maléfica.

**TSR**
Terminate and Stay Resident – programa residente em memória que pode ser acionado com o pressionar de algumas teclas.

**UA**
User Agent, também conhecido como MUA Mail User Agent.

**UCP**
Unidade Central de Processamento.

**UDP**
User Datagram Protocol.

**USERID**
Identificação do usuário na rede.

**UNIX**
Sistema Operacional projetado pela AT&T para aplicações Multiusuário.

**UNSUBSCRIBE**
Pedidos de exclusão em listas de discussão de correio eletrônico.

**UPGRADE**
Melhoria de um equipamento, onde são adicionadas novas ampliações.

**USER UNKNOWN**
Usuário de uma rede não reconhecido.

**VALOR HASH**
O mesmo que Message Digest. Funciona com uma impressão digital que possibilita a distinção entre uma mensagem e outra, mesmo se ambas diferirem por apenas um Bit.

**VIEWERS**
Denominação dada a programas cuja função é de apenas permitir a visualização dos dados de um determinado arquivo.

**VPN**
Virtual Private Network.

**XWINDOWS SYSTEM**
É uma característica de comunicação por meio de janelas entre os Sistemas Operacionais.

**WAN**
Rede para grandes distâncias geográficas.

**WAR DIALING**
Método "força-bruta" para encontra uma conexão discada ou um sistema de rede conectado via modem, normalmente autorizada, utilizando uma faixa de um prefixo de telefone associado a uma grande empresa para fazer a invasão.

**WEB SITE DEFACEMENT**
Protestos, avisos, ridicularizações diversas na Internet.

**WIRELESS**
Transmissão de dados via rádio. Satélite ou infravermelho.

**WINDOWS NT SERVER 4**
Software Sistema Operacional de Rede de Computadores desenvolvido pela empresa Microsoft S.A .

**WINZIP**
Nome dado a um dos softwares de compactação mais utilizados na área de Informática.

**WORLD WIDE WEB**

Rede interligando computadores existentes no mundo todo e também conhecida como Internet.

**WORKFLOW**
Aplicativos com funções customizadas para distribuir tarefas e padronizar o método de trabalho das áreas envolvidas em um processo.

**WORKGROUP**
Recurso que permite que diferentes áreas trabalhem mais próximas e em conjunto.

**WORKSTATIONS**
Computadores com grande capacidade de processamento, robustez, processamento gráfico e de armazenamento de dados. Geralmente utilizam o Sistema Operacional UNIX.

**WORMS**
É um tipo de vírus de computador, também chamado de Vermes, que tem como principal característica a autoduplicação, não necessitam se anexar a outros programas e residem e se multiplicam em ambientes Multitarefa.

**WORKSTATIONS DISKLESS**
Computadores com grande capacidade de processamento, robustez e de armazenamento de dados. Geralmente utilizam o Sistema Operacional UNIX, porém sem discos para armazenamento de dados.

**WWW**
World Wide Web, que é a Internet.

**XDR**
External Data Representation.

**X.400**
Recommendations for Message Handling Systems.

**XWINDOWS SYSTEM**
Característica de visualização de comandos do Sistema Operacional por meio de janelas.

**ZIP DRIVE**
Discos semelhantes a um disquete, porém com capacidade de armazenamento entre 100 e 250 Mega Bytes de dados.

# APÊNDICE

## ARQUITETURA DE REDES DE COMPUTADORES

Segundo Soares et al. (1995), a maioria dos computadores projetados até a década de 80, teve sua idéia baseada no modelo de Von Neumann (brilhante Matemático (1903-1957), pesquisador, sintetizador e que promoveu o conceito de

programa armazenado cujo projeto lógico se transformou no protótipo para a maioria de seus sucessores com a denominação a Arquitetura de Von Neumann). A arquitetura oferece um mecanismo simples e bastante eficiente, desde que a computação seja puramente seqüencial. A forma pela qual os programas são desenvolvidos e a maneira como são interpretados, proporcionaram para este modelo grande sucesso.

Com o avanço da tecnologia de integração de circuitos, os custos foram reduzidos de maneira significativa. Várias arquiteturas foram então propostas, dentro das restrições de tecnologia de cada época, tentando contornar as limitações do modelo de Von Neumann, no que diz respeito ao custo, confiabilidade e desempenho. Por exemplo, citamos Sistemas de *UCP (Unidade Central de Processamento)* única com múltiplas unidades funcionais, as máquinas PIPELINE e os *Array Processor* (processadores de matrizes). A idéia de seqüências múltiplas de instruções em um sistema composto por vários elementos de processamento compartilhando um espaço comum de memória, aparece como uma outra arquitetura, contornando a restrição de controle centralizado do modelo de Von Neumann. As principais características destes sistemas são:

- Dois ou mais processadores de capacidades aproximadamente iguais.
- Todos os processadores dividem o acesso a uma memória comum.
- Todos os processadores compartilham os canais de entrada / saída, as unidades de controle e dispositivos periféricos.
- O sistema total é controlado por um único sistema operacional.

Uma máquina de arquitetura distribuída é composta por um número finito de módulos autônomos de processamento interconectados para formar um único sistema, no qual o controle executivo global é implementado por meio da cooperação de elementos descentralizados. Não é suficiente que os processadores apareçam para o usuário como um sistema virtual único, é necessário que apareçam como um sistema real único em todos os níveis de abstração. Conceitualmente, um único sistema operacional controla todos os recursos físicos e lógicos, de maneira integrada, tendo, no entanto, seu núcleo e suas estruturas de dados distribuídos pelos vários processadores e memórias.

Ainda, segundo Soares et al. (1995), uma Rede de Computadores também é formada por um número finito de módulos autônomos de processamento interconectados. No entanto, a independência de vários módulos de processamento é preservada na sua tarefa de compartilhamento de recursos e trocas de informações. Não existe nestes sistemas a necessidade de um sistema operacional único, mas sim a cooperação entre os vários sistemas operacionais na realização das tarefas de compartilhamento de recursos e de troca de informação. As Redes de Computadores

surgiram para viabilizar o compartilhamento eficiente de recursos computacionais (*hardware*, *software* e dados) pelos usuários. Em geral esses recursos são sistemas heterogêneos: equipamentos de fabricantes diferentes e com características próprias que utilizam e processam *softwares* com características específicas e distintas para as aplicações desejadas para os usuários, manipulam e produzem dados incompatíveis. Até mesmo quando equipamentos idênticos de um só fabricante são empregados em aplicações distintas, eles podem apresentar características heterogêneas.

Esta heterogeneidade de sistemas beneficia o usuário, que não é restrito a um único tipo de sistema para as suas várias aplicações. Assim, pode-se selecionar um sistema que melhor se adapte às condições da aplicação de interesse e do orçamento disponível. Por outro lado, tal heterogeneidade dificulta consideravelmente a interconexão de equipamentos de fabricantes diferentes. Para garantir a homogeneidade na troca de informações entre os equipamentos e compartilhamento de seus recursos, estes são interligados por um Sistema de Comunicação. O Sistema de Comunicação é constituído de um conjunto de normas e regras, a fim de organizar a comunicação entre os recursos da rede. Este conjunto de regras é chamado de Protocolo (regras que governam a transmissão de dados implementadas via software). Um Nó de comunicação em uma rede é um ponto de conexão ou junção da rede. O Sistema de Comunicação é responsável por oferecer comunicações entre os diversos Nós existentes em um Sistema Distribuído (são sistemas que se localizam em áreas geograficamente distantes e podem se comunicar por meio de linhas de comunicação de dados, sendo que seu processamento tem a característica de ser descentralizado). Este tipo de sistema permite que qualquer Nó de rede transmita informações para outro Nó conectado com a rede de comunicação.

A arquitetura da rede de computadores é formada por Níveis (Camadas), Interfaces e Protocolos que facilitam a interconectividade entre sistemas homogêneos e, especialmente em um ambiente de sistemas abertos, heterogêneos. Cada Nível oferece um conjunto de serviços ao Nível superior, utilizando funções realizadas no próprio Nível e serviços disponíveis nos Níveis inferiores. Um protocolo de Nível N é um conjunto de regras e formatos de semântica e sintaxe, por meio do qual as informações ou dados deste nível são trocados entre as entidades do Nível N, localizadas em sistemas distintos. Um ou mais protocolos podem ser definidos em um Nível. Como os sistemas de comunicações são complexos, é comum dividi-los em camadas. O projeto de Protocolos em Níveis é a maneira mais eficiente de se estruturar uma rede de computadores. Tendo-se definido claramente a interface entre os diversos Níveis, uma alteração na implementação de um Nível pode ser realizada sem causar impacto na estrutura global.

Para permitir um intercâmbio de informações entre computadores de diversos fabricantes, tornou-se necessário definir uma arquitetura única, e para garantir que nenhum fabricante levasse vantagem em relação aos outros, a arquitetura teria que ser aberta e pública. Foi por este motivo que a *I.S.O* (*International Organization for Standardization*) definiu o modelo denominado Modelo de Referência *OSI* (*Reference Model Open Systems Interconnection*), que propõe uma estrutura em sete Níveis como referência para a arquitetura dos protocolos de Redes de Computadores. A arquitetura em camadas oferece muitas vantagens:

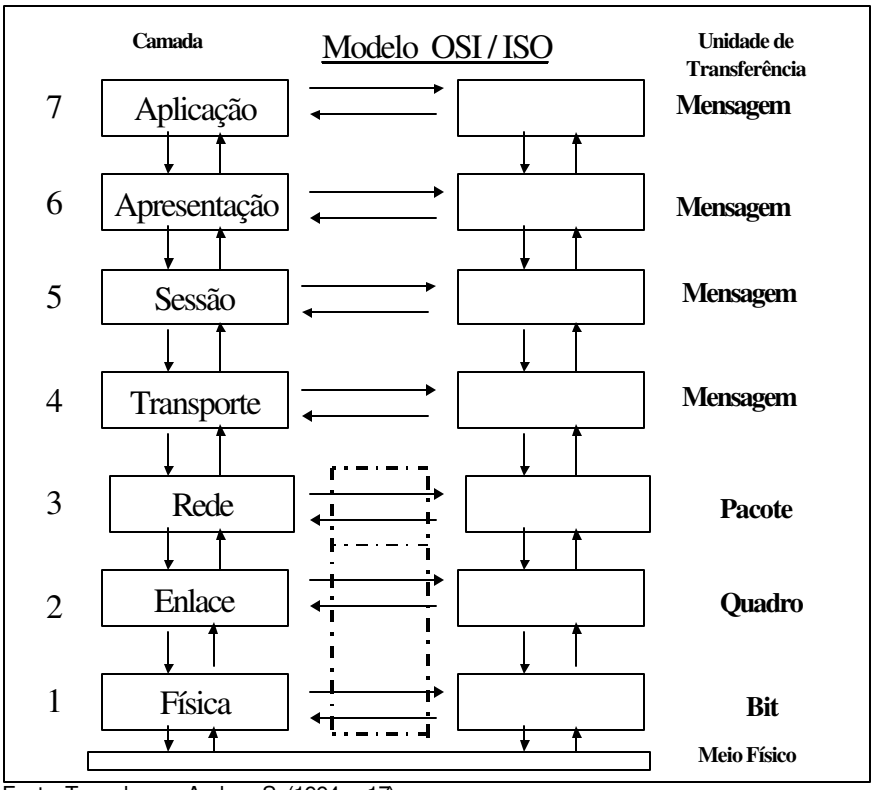
- Independência entre camadas: Cada camada tem conhecimento apenas dos serviços oferecidos pela camada que está imediatamente abaixo.
- Flexibilidade: Qualquer mudança de implementação que aconteça em uma camada, não afetará as camadas abaixo ou acima.
- Implementação simplificada e serviços de manutenção: O recurso de um projeto em camadas modulares e uma de composição arquitetada de toda a funcionalidade de um sistema em unidades mais simples e menores.
- Padronização: O encapsulamento da funcionalidade da camada, dos serviços e das interfaces em entidades arquitetadas cuidadosamente, facilita o desenvolvimento de padrões.

**MODELO OSI / I.S.O**

Segundo Tanenbaum (1994), as organizações internacionais de padronização podem ser classificadas pelo seu enfoque técnico e por sua estrutura geográfica e política, sendo que as organizações internacionais importantes para o tópico de Redes de Computadores são: *I.S.O* (*International Organization for Standardization*), a *IEC* (*International Electrotechnical Commision*), e o *ITU-T* (*International Telecommunications Union*) que corresponde ao antigo *CCITT* (*Comité Consultatif de télégraphique et Téléphonique*), o qual mantém uma relação estreita com o *CCIR (Comitê Consultatif International des Radiocommunications)*. A *I.S.O* é uma organização internacional fundada em 1946 que tem por objetivo a elaboração de padrões internacionais, seus membros são órgãos de padronização nacionais dos 89 países membros. O representante no Brasil é *a ABNT (Associação Brasileira de Normas Técnicas).*

Segundo Hashioka (1995), o modelo OSI / I.S.O se baseia em sete camadas e a camada de nível mais baixo é constituída pela ligação física entre os equipamentos da rede e a partir deste nível, as camadas sucessivas utilizam o serviço oferecido pela camada imediatamente inferior, acrescentando novas funções que são oferecidas no nível imediatamente superior, na forma de um serviço mais sofisticado. Houve uma

preocupação em não se criar um número excessivo de camadas que não tornassem difícil a tarefa de construir e integrar os sistemas. A abrangência criada foi tal que minimizou o número de interações entre os níveis. Os níveis foram separados para facilitar a manipulação de funções realmente diferenciadas com relação ao processo envolvido ou à tecnologia empregada. Funções similares foram agrupadas num mesmo nível. A Figura 6 apresenta um esquema das camadas do Modelo *OSI / I.S.O*, segundo Tanenbaum (1994):




Fonte: Tanenbaum, Andrew S. (1994, p.17).

**CAMADA FÍSICA**

Segundo Tanenbaum (1994), a Camada Física gera os pulsos físicos, as correntes elétricas e os pulsos óticos envolvidos no deslocamento de dados. O padrão *RS-232* (padrão recomendado pela *EIA - Electronic Data Interchange*, para interface mecânica e elétrica), é um exemplo de padrão da camada Física. Essa camada não inclui os sistemas de comunicações, somente a conexão com este sistema. Ela trata dos períodos longos e das durações dos pulsos. Regula a transmissão pura de *bits* (*Binary DigIT*, é a menor unidade de informação de um sistema binário, por meio de um canal de comunicação.

**CAMADA DE ENLACE DE DADOS**

Ainda, conforme Tanenbaum (1994), a Camada de Enlace de dados é o primeiro nível que reúne os bits e trata os dados como pacotes (conjunto de *bits* organizados segundo uma estrutura chamada quadro (*frame*), contendo informações de controle e dados úteis para a transmissão). Este nível executa o agrupamento final dos pacotes que estão sendo enviados e realiza a primeira inspeção no recebimento dos pacotes. Ela adiciona uma correção de erros para os pacotes que estão saindo e uma verificação nos pacotes que estão chegando. Os pacotes incompletos ou com defeitos são descartados. Se a Camada de Enlace conseguir determinar a origem deste pacote, ela retornará um pacote de erro. *SDLC* (*Synchronous Data Link Control*, protocolo síncrono utilizado pelas redes *SNA* (*Systems Network Architeture*, descrição total da *IBM* para estrutura lógica, formatos, protocolos e seqüências operacionais para transmissão de unidades de informação entre programas e equipamentos da *IBM*), e *HDLC* (*High-Level Data Link Control*, protocolo de comunicação *I.S.O* utilizado em redes de Comutação de pacotes tipo X.25 com correção de erros na Camada de Enlace), são dois exemplos de protocolos que operam neste nível. Os *bits* são divididos em quadros e estes são confirmados pelo receptor. Esta camada também é responsável pelo controle de fluxo para regular a velocidade relativa dos dois processos.

**CAMADA DE REDE**

Segundo Tanenbaum (1994), a Camada de Rede provê os meios para estabelecer, manter e terminar conexões de rede entre sistemas contendo entidades de aplicação que se comunicam. Provê também os meios funcionais e de procedimento para a troca de informação, por meio de conexões de rede, entre duas entidades da camada de transporte. Possibilita ainda a escolha de caminhos (rotas) por meio de sistemas intermediários, para uma conexão entre dois endereços ao nível de rede, que é uma das funções básicas da Camada de Rede, a função de encaminhamento ou roteamento de informação.

Esta camada também controla a operação interna da rede. O protocolo da *Internet IP* (*Internet Protocol*) e o *IPX* (*Internetworking Packet Exchange*) do *NetWare* (família de Sistemas Operacionais de Redes de Computadores, cujo fabricante é a empresa Novell), operam neste nível.

**CAMADA DE TRANSPORTE**

Segundo Tanenbaum (1994), a Camada de Transporte é de transição, ou seja, é o último dos níveis que gerenciam os pacotes de roteamento e a geração de erros. Ela

adapta qualquer deficiência que não possa ser resolvida no nível de rede. Se os pacotes forem recebidos de maneira confiável naquele nível, o trabalho do nível de transporte será muito simples. Por outro lado, se o sistema de comunicação não puder fornecer uma transmissão de pacotes segura, esse nível fará uma compensação realizando um trabalho mais complexo.

Um exemplo de protocolo da camada de transporte é o *TCP* (*Transmission Control Protocol*). Ela permite a transferência de dados entre computadores *Hospedeiros* (pode ser considerado como um computador principal em uma rede e que efetua a comunicação com as outras redes externas), utilizando-se do serviço de transmissão oferecido pela Camada de Rede.

**CAMADA DE SESSÃO**

Segundo Tanenbaum (1994), em muitas definições de rede, procura-se estabelecer uma conexão formal entre as entidades de comunicação. Essa conexão garante que as mensagens serão enviadas e recebidas com um alto grau de segurança. Essas preocupações tornam-se necessárias quando a confiabilidade de uma rede é duvidosa, o que ocorre na maioria dos casos de uso das telecomunicações. Por isso, a orientação de Sessão é norma na maioria das comunicações de *mainframe*.

A Camada de Sessão é o nível que mantém as transmissões "orientadas à conexão". O processo de estruturação e rompimento de uma conexão neste nível é um processo de vinculação e de desvinculação. Nesta Camada, assume-se que os pacotes sejam seguros, por isso, a verificação de erro não faz parte deste nível.

**CAMADA DE APRESENTAÇÃO**

De acordo com Tanenbaum (1994), a Camada de Apresentação realiza qualquer conversão de dados contidos em arquivos que possa ser exigida pela camada de aplicação, para tornar os dados utilizáveis. Os processos de compactação / descompactação e criptografia / decriptografia podem ser implementados no nível de apresentação. Um exemplo de uma função nesta camada seria conversão de codificação *ASCII (American Standard Code for Information Interchange)*, em *EBCDIC (Extended Binary-Coded Decimal Interchange Code*, código binário da *IBM* para textos), ou de *EBCDIC* para *ASCII.*

**CAMADA DE APLICAÇÃO**

Ela trata dos assuntos de segurança e disponibilidade de recursos e tende a lidar com a transferência de arquivos e de *jobs* (tarefa a ser cumprida por um processador ou computador), e com protocolos de terminais virtuais. São os programas de aplicações, do tipo bancos de dados distribuídos. Segundo Tanenbaum (1994), esta camada contém os programas do usuário que fazem o verdadeiro trabalho para o qual os computadores foram adquiridos, que utilizam os serviços oferecidos pela camada de aplicações para suas necessidades de comunicação, todas baseadas nos protocolos que estão interagindo e trabalhando em cada nível.

**PROTOCOLOS**

Segundo Tanenbaum (1994), os protocolos de comunicação de dados são utilizados para coordenar a troca de informações entre dispositivos de redes de computadores. Eles estabelecem o mecanismo pelo qual cada dispositivo reconhece as informações úteis de qualquer componente destes dispositivos. No mundo atual das comunicações, existem muitos protocolos em uso, junto com estruturas básicas que tratam de vários aspectos de comunicação de dados.

Atualmente, na área de redes, os protocolos mais usuais são:

- *IPX/SPX* ⇒ Protocolo para rede local da *Novell*;
- *SNA* ⇒ Protocolo utilizado pela *IBM*, para sistemas de médio porte (AS/400, por exemplo);
- X.25 / *Frame Relay* ⇒ Protocolos para comunicação entre computadores e redes públicas ou redes privadas;
- *NETBEUI* ⇒ Protocolo para redes *Microsoft*;
- *TCP/IP* ⇒ Protocolo para *LAN's (Local Área Network)* e *WAN's (Wide Área Network)*, utilizado em ambiente *Unix*, *Internet* e redes privadas *TCP/IP*.

**PROTOCOLO TCP/IP**

Segundo Soares et al. (1995), o *TCP/IP* é uma família de protocolo utilizada nas comunicações de computador. TCP/IP significa *Transmission Control Protocol / Internet Protocol*, mas ao contrário do que acontece na imprensa, o nome completo raramente é utilizado. O *TCP* e o *IP* são protocolos individuais que podem ser discutidos isoladamente, mas eles não são os únicos protocolos que compõem esta família. Pode acontecer de um usuário do *TCP/IP* não utilizá-lo, mas sim, alguns outros protocolos da família. A utilização do *TCP/IP* nessa situação não deixa de ser apropriada porque o nome se aplica de modo genérico ao uso de qualquer protocolo da família *TCP/IP*.

Como o *TCP/IP* foi desenvolvido pelo departamento de defesa norte-americano, esta família de protocolo é, algumas vezes, denominada conjunto *DoD* (nome genérico dado ao conjunto de protocolos pertencentes à família *TCP/IP*), mas ela não tem um nome de divulgação como, por exemplo, o conjunto de protocolos *AppleTalk* (uma arquitetura de rede da empresa Apple que suporta o acesso proprietário da Apple, Ethernet (rede local desenvolvida pelas empresas Xerox, Digital e Intel), e *Token Ring* (mecanismo de acesso à rede de dados e topologia de Anel em que um pacote de supervisão ou Token trafega de estação em estação procurando quem queira transmitir dados), da *Apple*.

Os protocolos costumam ser agrupados em "famílias" (às vezes, denominados grupos ou pilhas). Os implementadores de protocolos determinam quais protocolos serão agrupados em uma mesma família. Muitas dessas famílias são desenvolvidas por organizações comerciais. Cada protocolo em uma família permite a utilização em um determinado recurso da rede, porém ele sozinho não oferece muita utilidade, precisando ser combinado com outros protocolos de sua família. As famílias de protocolos tentam resolver os mesmos problemas da rede utilizando conjuntos de protocolos ligeiramente diferentes entre si, mas existem muitas semelhanças entre essas famílias.

As famílias de protocolos *TCP/IP* incluem protocolos como o *IP (Internet Protocol)*, *ARP* (*Address Resolution Protocol*), *ICMP* (*Internet Control Message Protocol*), *UDP* (*User Datagram Protocol*), *TCP (Transmission Control Protocol)*, *RIP* (*Routing Information Protocol*), Telnet, *SMTP* (*Simple Mail Transfer Protocol*), *DNS* (*Domain Name System*) e muitos outros que também são utilizados por outros protocolos. Saber exatamente quais são os protocolos que compõem uma determinada família não é pré-requisito para compreender o funcionamento básico da rede. A Figura 7, abaixo, apresenta um esquema contendo a estrutura das camadas do Protocolo TCP / IP com todos os seus protocolos por Níveis.

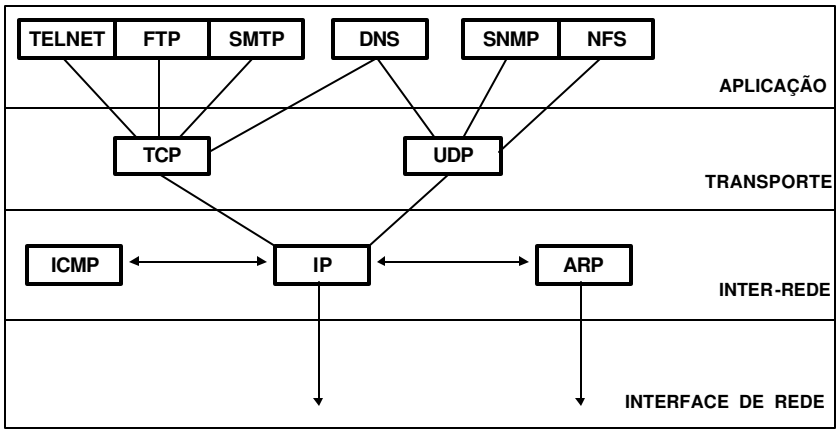


Figura 7 – Configuração do Protoloco TCP / IP

Fonte: Hashioka, Mauro H., Salgado, Antonio E. (1995, p. 27).

**ARQUITETURA TCP/IP**

Segundo Soares et al. (1995), todo o projeto de desenvolvimento da arquitetura *TCP/IP* foi patrocinado pela *DARPA* (*Defense Advanced Research Projects Agency).* Esta arquitetura baseia-se principalmente em um serviço de transporte orientado a conexão, fornecido pelo *TCP*, e um serviço de rede não orientado à conexão (*Datagrama* não confiável), fornecido pelo *IP*. A arquitetura *TCP/IP* dá uma ênfase toda especial a uma interligação de diferentes tecnologias de rede. A idéia baseia-se na seguinte constatação: não existe nenhuma tecnologia de rede que atenda aos anseios de toda a comunidade de usuários. Alguns usuários precisam de redes de alta velocidade que normalmente cobrem uma área geograficamente restrita. Já outros, se contentam com redes de baixa velocidade, que conectam equipamentos distantes milhares de quilômetros uns dos outros. Portanto, a única forma de permitir que um grande número de usuários possa trocar informações é interligar as redes às quais eles estão conectados, formando assim uma inter-rede. Nas ocasiões em que houver a necessidade de se interligar duas redes distintas é necessário conectar uma máquina a ambas as redes envolvidas no processo. Uma das máquinas torna-se responsável pela tarefa de transferir uma mensagem de uma rede para outra. Uma máquina, computador ou dispositivo que conecta duas ou mais redes é denominada *Gateway* (equipamento físico (*hardware*) que permite a interligação entre duas redes de dados), ou *Router* (equipamento físico (*hardware*) que permite a interligação de duas redes, uma local e uma externa, dentro da empresa (comunicação entre *LAN* e *WAN*)). Para ser capaz de "rotear" corretamente as mensagens, os *routers* precisam conhecer a topologia da inter-rede, ou seja, precisam saber como as diversas redes estão interconectadas. Já os usuários vêem a inter-rede como uma rede virtual única, a qual todas as máquinas estão conectadas, não importando a forma física de interconexão, conforme apresentado na Figura 8.

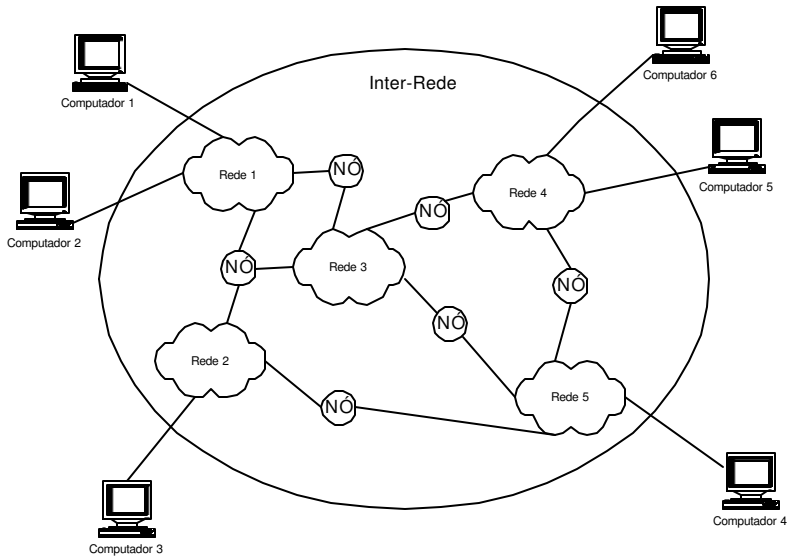



Figura 8 – Conceito de Inter-Rede

Fonte: Soares, Luiz F. G., Lemos, Guido, Colcher, Sérgio. (1995, p.143).

A arquitetura *TCP/IP* é organizada em quatro camadas conceituais definidas sobre uma quinta camada que não faz parte do modelo, a Camada de Inter-Rede. A Figura 9 apresenta as camadas e os tipos de dados passados por elas.

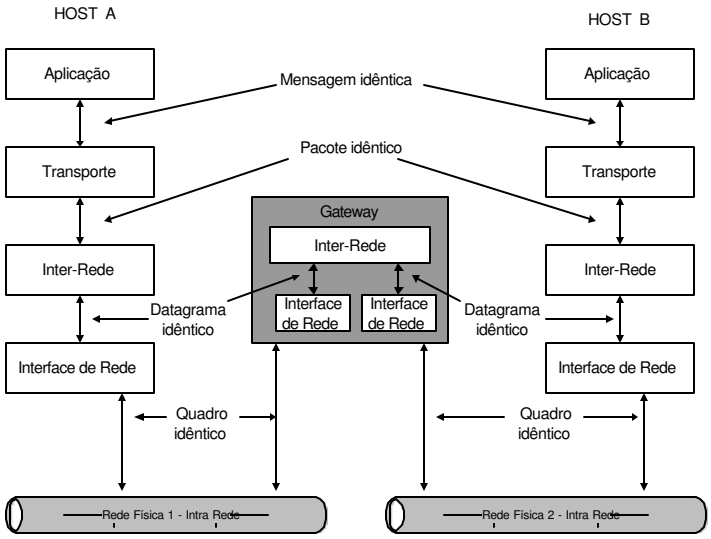



Figura 9 – Camadas conceituais da arquitetura TCP / IP

Fonte: Soares, Luiz F. G., Lemos, Guido, Colcher, Sérgio. (1995, p.144).

**NÍVEL DE APLICAÇÃO**

Segundo Soares et al. (1995), quando os usuários estão utilizando programas de aplicação para acessar os serviços disponíveis na inter-rede, as aplicações interagem com o nível abaixo (Nível de Transporte) para enviar e receber dados. Estas aplicações podem usar serviços orientados a conexão, fornecidos pelo *TCP* (serviço de circuito virtual), ou serviço não orientado à conexão fornecido pelo *UDP* (serviço de *datagrama* não confiável). Algumas aplicações disponíveis na camada de aplicação do *TCP/IP* são:

- *Simple Mail Transfer Protocol* (*SMTP*): que oferece o serviço *Stored And Forward* para mensagens que carregam correspondência contendo textos.

- *File Transfer Protocol* (*FTP*): que fornece serviços de transferência de arquivos.

- *Telnet*: Protocolo de emulação de terminal normalmente utilizado em aplicações que usam de linha de comando na *Internet* que fornece serviços de terminal virtual.

- *Domain Name System* (*DNS*): que fornece serviços de mapeamento de nomes e endereços de rede.

**NÍVEL DE TRANSPORTE**

Segundo Tanenbaum (1994), a função principal desta camada é a de permitir a comunicação fim-a-fim entre as aplicações. As funções do nível de transporte na *Internet* são semelhantes às do mesmo nível no modelo *OSI* da *I.S.O.* Se o protocolo utilizado é o *TCP*, os serviços fornecidos são: controle de erro, controle de fluxo, sequenciação e multiplexação do acesso ao nível inter-rede. O *UDP* é um protocolo bem mais simples e o serviço por ele fornecido é a multiplexação / demultiplexação do acesso ao nível Inter-rede.

**NÍVEL INTER-REDE**

Segundo Tanenbaum (1994), este nível é responsável pela transferência dos dados na inter-rede, desde a máquina de origem até a máquina de destino. Esta camada recebe pedidos do nível de transporte para transmitir pacotes que, ao solicitar a transmissão, fornece o endereço da máquina onde o pacote deverá ser entregue, o

destinatário. O pacote é encapsulado em *datagrama IP* e o *algoritmo* (uma expressão lógica que resolve uma fórmula Matemática complexa ou instruções de um programa), roteamento é executado para determinar se o *datagrama* pode ser entregue diretamente ou deve ser repassado para um *router*. Após a análise do resultado da avaliação do *algoritmo* do roteamento, o *datagrama* é passado para uma Interface de Rede apropriada para então ser transmitido.

O Nível Inter-rede também processa pacotes recebidos das Interfaces de Rede. Nesse caso, o *algoritmo* de roteamento é utilizado para decidir se o *datagrama* deve ser passado para um Nível de Transporte local, ou se deve ser passado adiante por meio de uma das interfaces de rede.

**NÍVEL DE INTERFACE DE REDE**

Segundo Tanenbaum (1994), para a execução dos trabalhos nesta camada não existe nenhuma restrição por parte da arquitetura *TCP/IP* às redes que são interligadas para formar a Inter-rede. Desta maneira, qualquer tipo de rede pode ser ligada, bastando para isso que seja desenvolvida uma interface que compatibilize a tecnologia específica de rede com o protocolo *IP*. Esta compatibilização é a função do nível de interface de rede, que recebe os *datagramas IP* do nível de inter-rede e os transmite por meio de uma rede específica. Para realizar esta tarefa, nesse nível, os endereços *IP* que são os endereços lógicos, são traduzidos para endereços físicos dos *hosts* (computador ou servidor central em uma rede que, normalmente pode efetuar a comunicação a rede interna com as redes externas àorganização) ou *routers* conectados àrede.

**NÍVEL FÍSICO**

Segundo Soares et al. (1995), a função principal deste nível é permitir a transmissão de bits por meio de um canal de comunicação. Cabe a esta camada definir tensões e tempos de duração de bits, se a transmissão é *Simplex* (transmissão de dados em uma única direção), ou *Duplex* (transmissão de dados em duas direções, porém uma em cada sentido de cada vez.), etc. Esta camada pode ser implementada, por exemplo, pelo padrão *Ethernet* na *LAN* ou *SLIP* (*Serial Line Interface Protocol*) na *WAN*. Um exemplo comparativo entre as Arquiteturas *OSI / I.S.O* é apresentado na Figura 10.

**COMPARAÇÃO ENTRE AS ARQUITETURAS OSI / ISO E TCP/IP**

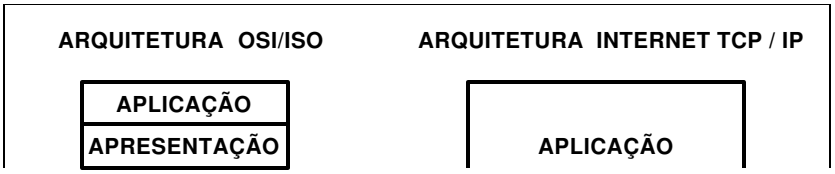


Figura 10 – Arquiteturas OSI e *Internet* TCP / IP

Fonte: Soares, Luiz F. G., Lemos, Guido, Colcher, Sérgio. (1995, p.146).

Segundo Soares et al. (1995), no modelo *OSI / I.S.O* são descritos formalmente os serviços de cada camada, sendo que a interface usada pelas camadas adjacentes para a troca de informações é o protocolo que define regras de comunicação para cada uma das camadas. Os níveis de Enlace, Rede e Transporte podem oferecer serviços orientados à conexão (circuito virtual) ou não orientados à conexão ( *datagrama*). Esta flexibilidade tem aspectos positivos, mas, por outro lado, pode levar a situações em que dois sistemas em conformidade com a arquitetura *OSI / I.S.O* não consigam se comunicar, bastando para tal que implementem perfis funcionais incompatíveis. O processo de interligação de redes com tecnologias distintas é o objetivo pelo qual foi desenvolvida a arquitetura *TCP/IP*. Neste desenvolvimento há um conjunto específico de protocolos que resolveu o problema de forma bastante simples e satisfatória. Os níveis Físico, Enlace e rede do modelo *OSI / I.S.O*, relativos a transmissão de dados em uma única rede, não são abordados na arquitetura *TCP/IP*, que agrupa todos estes serviços na Camada Intra-rede. A arquitetura *TCP/IP* se limita a definir uma interface entre o Nível Inter-rede e o Nível Intra-rede.

Os serviços existentes do nível de rede *OSI / I.S.O*, relativos à interconexão de redes distintas, são implementados na arquitetura *TCP/IP* pelo protocolo *IP* e nesta arquitetura só existe uma opção de protocolo e serviço: o protocolo *IP*, cujo serviço é *datagrama* não confiável. Esta imposição de protocolo no nível inter-rede é uma das principais razões do sucesso da arquitetura *TCP/IP*. No nível de transporte, a arquitetura *TCP/IP* oferece duas opções: o *TCP* e o *UDP*. Estes protocolos são equivalentes aos protocolos orientados e não orientados a conexão no nível de transporte *OSI*. Os Níveis de Sessão, Apresentação e Aplicação da *OSI* são implementados na arquitetura *TCP/IP* no nível de aplicação.

A abordagem da *ISO*, na criação de Camadas Sessão, Apresentação e Aplicação, é mais razoável, no sentido em que permite uma maior reutilização de esforços durante o desenvolvimento de aplicações distribuídas. Os protocolos de arquitetura *TCP/IP* oferecem uma solução simples, porém, bastante funcional, para o problema de interconexão de sistemas abertos. Devido aos seus protocolos terem sido a primeira opção de solução para implementação não proprietária para interconexão de sistemas, fez com que a arquitetura se tornasse um padrão.

**PROTOCOLO IP**

Ainda, segundo Soares et al. (1995), o protocolo IP foi projetado para permitir a interconexão de redes de computadores que utilizam a tecnologia de comutação de pacotes, conforme Figura 11, sendo que um ambiente inter-rede consiste em *hosts* conectados a rede que, por sua vez, são interligados por meio de de *routers*. As redes que fazem partes da inter-rede variam de redes locais (*Ethernet*) até redes de grande porte, do tipo da *ARPANET (Advanced Research Projects Agency Network*, tecnologia de comutação de pacotes precursora da atual *Internet*, "nascida" nos EUA).

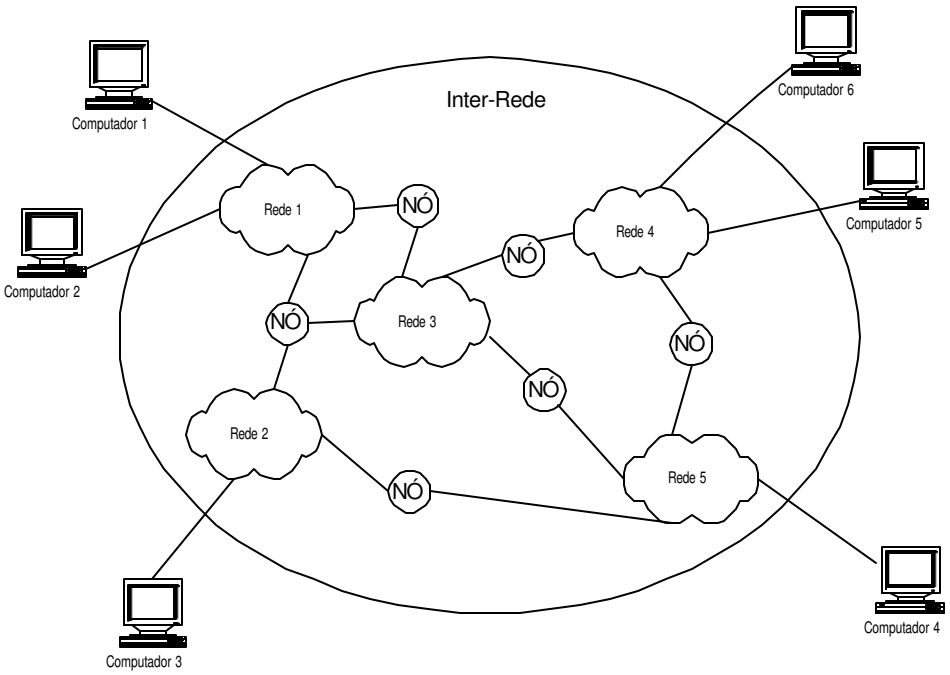



Figura 11 - Interligação dos componentes de uma rede

Fonte: Soares, Luiz F. G., Lemos, Guido, Colcher, Sérgio. (1995, p.143).

Todo o serviço oferecido pelo IP é sem conexão e cada *datagrama* IP é tratado como uma unidade independente que não possui nenhuma relação com qualquer outro *datagrama*. A comunicação é não confiável, não sendo usados reconhecimentos fim-a-fim ou entre nós intermediários. Nenhum mecanismo de controle de erros nos dados transmitidos é utilizado, exceto um *checksum* (valor usado para assegurar que os dados sejam transmitidos sem erro), do cabeçalho que garante que as informações nele contidas, que são usadas pelos *routers* para encaminhar os *datagramas* que estão corretos. Nenhum mecanismo de controle de fluxo é utilizado. Algumas das principais características desse protocolo são:

- Endereçamento hierárquico.
- Facilidades de fragmentação e remontagem de pacotes.
- Identificação da importância do *datagrama* e do nível de confiabilidade exigida.
- Campo especial indicando qual protocolo de transporte a ser utilizado no nível superior.
- Roteamento adaptativo distribuído nos roteadores.
- Descarte e controle de tempo de vida dos pacotes inter-redes no roteador.

**ENDEREÇAMENTO IP**

Segundo Tanenbaum (1994), existe uma sistemática própria para a configuração dos endereços IP que é formada por números com 32 bits, normalmente escritos como quatro *octetos* (em redes de Comutação de pacotes é um grupo de oito bits de dados). Em decimal, por exemplo, 56.36.78.21. O endereçamento IP é dividido em duas partes: uma parte que identifica a rede e outra parte que identifica os *hosts* desta rede. Deve-se observar que um endereço *IP* não identifica uma máquina individual, mas uma conexão à inter-rede. Assim, um roteador conectado em n redes tem n endereços *IP* diferentes, um para cada conexão.

Os endereços *IP* podem ser usados para que se possa referenciar tanto as redes quanto a um *host* individual. Por convenção, um endereço de rede tem um campo identificador de *host* com todos os bits iguais a 0 (zero), pode-se também se referir a todos os *hosts* de uma rede por meio de de um endereço por difusão, desta forma deve-se colocar no campo identificador de *hosts* todos os bits iguais a 1. O endereço 127.0.0.0 é reservado para teste de *loopback* (condição de um canal de comunicações em que a interface de transmissão conectada à da recepção para fins de teste ou de manutenção

de uma topologia de Anel redundante), e comunicação entre processos da mesma máquina.

O *IP* utiliza três classes diferentes de endereços e a definição de classes de endereços deve-se ao fato do tamanho das redes que compõem a Inter-rede variar muito, indo desde redes locais de computadores de pequeno porte, até redes públicas interligando milhares de *hosts*.

Na primeira classe de endereços, Classe A, o bit mais significativo é o 0 (zero) e os outros sete bits do *octeto*, identificam a rede. E os vinte e quatro *bits* restantes, identificam o endereço local. Essa classe de endereços é usada para redes de grande porte, os endereços de rede variam de 1 a 126, e cada rede tem capacidade de endereçar cerca de 16 milhões de *hosts*. O exemplo deste tipo de rede é a *ARPANET*. A Classe B de endereços usa dois octetos para o número de rede e dois *octetos* para o endereço de *host*. Os endereços de rede Classe B variam na faixa de 128.1 até 191.255, e cada rede pode interligar cerca de 65.000 *hosts*. Os endereços Classe C utilizam três *octetos* para identificar a rede e um para identificar o host.

Os endereços de rede situam-se na faixa de 192.1.1 até 233.254.254 e cada rede pode endereçar até 254 hosts. Os endereços acima de 233 do primeiro *octeto* foram reservados para uso futuro. Outras exceções são as Classe D e a Classe E, que são reservadas para transmissão pública e desenvolvimentos futuros.

**DESVANTAGENS DO ENDEREÇAMENTO IP**

Segundo Tanenbaum (1994), existe uma grande desvantagem do endereço *IP* no que se refere à conexão com o *host* e não ao *host*, ou seja, quando necessitamos remanejar um *host* de uma para outra rede, deve-se alterar seu endereço *IP*. É possível citar um exemplo de um computador portátil (*notebook*) que possui um endereço que o identifica na sua rede. Quando este é conectado em outra localidade, o endereço de rede é outro.

Desta forma, este computador não acessará nenhum recurso da rede. A menos que seja fornecido um novo endereço para o computador nesta localidade e as configurações relativas ànova rede sejam efetuadas novamente no equipamento.

Existe ainda uma outra desvantagem no endereçamento *IP* que se refere a escolha da classe de endereçamento. Pode-se observar o fato por meio do exemplo em que em um projeto de rede foi adotado a Classe C de endereçamento *IP*, sendo assim, cada rede não pode ter um número maior que 253 *hosts*, mas com o crescimento da rede, houve necessidade de superar este número.

Desta forma, a única solução é desfazer todo o projeto de endereçamento da Classe C e configurar toda a rede para um endereçamento Classe B ou Classe A, onde se permitiria um aumento do número de *hosts*.

**ROTEAMENTO**

De acordo com Soares et al. (1995), o termo roteamento Inter-redes é a principal função do protocolo *IP*. O roteamento é a função que o protocolo possui de encaminhar pacotes para qualquer outro nó da rede. O protocolo assume que os *hosts* sabem enviar *datagramas* para qualquer outro *host* conectado a mesma rede. A função de roteamento torna-se mais complexa quando uma entidade *IP* deve transmitir um *datagrama* cujo destinatário não está ligado à mesma rede que ela. Neste caso, parte da função de roteamento é transferida para os roteadores, cabendo ao modo *IP* no *host* apenas o envio do *datagrama* a um dos roteadores conectados a sua rede, conforme Figura 12.

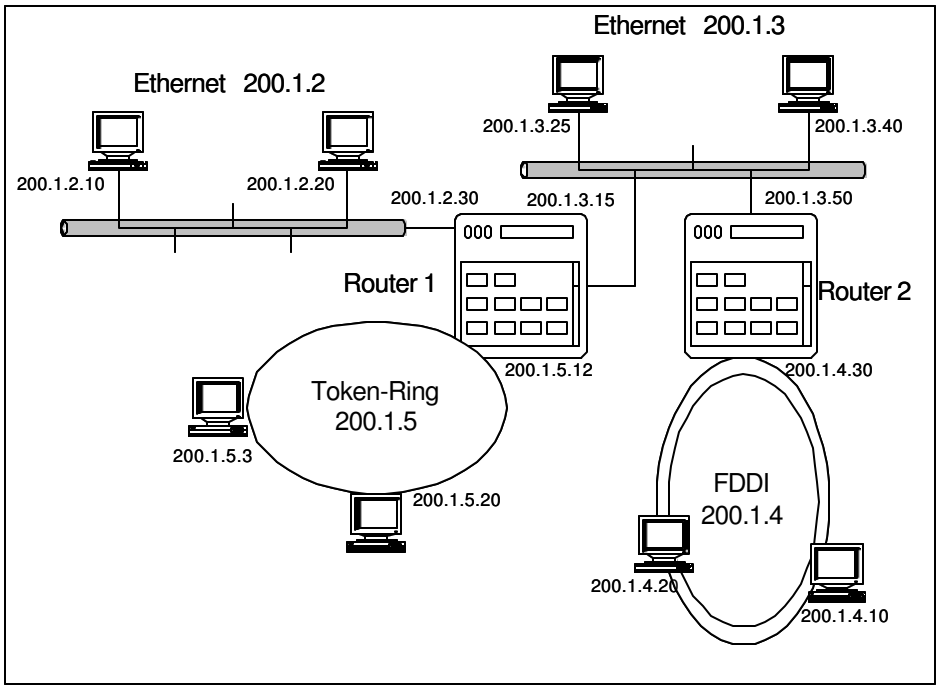



Figura 12 – Esquema de Roteamento em Redes de Computadores

Fonte: Soares, Luiz F. G., Lemos, Guido, Colcher, Sérgio. (1995, p.333).

Os dispositivos físicos envolvidos no processo, chamados de roteadores são freqüentemente computadores normais que possuem mais de uma interface de rede. Nesse caso, a função de roteamento é executada por um *software*, mas em casos onde o tráfego inter-redes é muito alto, com grande volume de dados em trânsito na rede, são

utilizados equipamentos projetados especificamente para executar a tarefa de roteamento.

O roteamento por meio do protocolo *IP* baseia-se exclusivamente no identificador de rede do endereço de destino, onde cada computador possui uma tabela cujas entradas são pares: endereço de rede / endereço de roteador. Esta tabela é denominada Tabela de Roteamento *IP*. Quando o módulo *IP*, no roteador, tem que encaminhar um *datagrama*, ele inicialmente identifica se o destino do *datagrama* é um host conectado a mesma rede que seu *hospedeiro*. Se este for o caso, o *datagrama* é entregue a interface da rede que se encarrega de mapear o endereço *IP* do endereço físico do host, encapsular o *datagrama IP* em um quadro da rede, e, finalmente transmiti-lo ao destinatário.

Existe uma alternativa para se dar seqüência ao envio da mensagem que se manifesta se a rede identificada no endereço de destino do *datagrama* for diferente da rede onde está o módulo *IP:* ele procura em sua tabela de roteamento uma entrada com o endereço de rede igual ao endereço de destino do *datagrama*, recuperando assim o endereço do roteador que deve ser usado para alcançar a rede onde está conectado o destinatário do *datagrama*.

O roteador recuperado da tabela pode não estar conectado diretamente a rede de destino, porém, se este for o caso, ele deve fazer parte do caminho a ser percorrido para encontrá-lo.

**PROTOCOLO TCP**

Dando seqüência às informações relativas a protocolos, segundo Soares et al. (1995), o *TCP* é um protocolo orientado à conexão que fornece um serviço confiável de transferência de dados fim-a-fim e foi projetado para funcionar com base em um serviço de rede sem conexão e sem confirmação. A Figura 13 ilustra a localização do *TCP* na arquitetura *TCP/IP*.

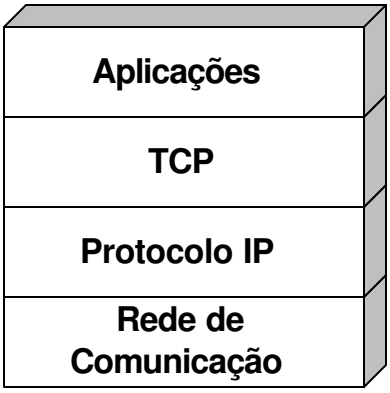



Figura 13 – Camadas de protocolos da arquitetura *Internet* do TCP / IP

Fonte: Soares, Luiz F. G., Lemos, Guido, Colcher, Sérgio. (1995, p.349).

Segundo Soares et al. (1995), o protocolo *TCP* mantém uma interação por um lado com processos das aplicações e por outro com o protocolo da Camada Inter-rede da arquitetura de *Internet*. Existe uma interface entre os processos de aplicação e o *TCP* que consiste em um conjunto de chamadas semelhantes às que os sistemas operacionais fornecem aos processos de aplicação para manipulação de arquivos em computadores. Pode-se citar como exemplo a existência de chamadas para abrir e fechar conexões e para enviar e receber dados em conexões previamente estabelecidas.

O protocolo *TCP* tem a capacidade de transferir uma cadeia *stream* (conjunto de estruturas tais como *bit*, campos e registros), contínua de octetos em duas direções existentes entre seus usuários. Este protocolo tem por função decidir o momento de parar de agrupar os octetos e de, conseqüentemente, transmitir o segmento formado por este agrupamento.

Existe ainda um mecanismo de controle do fluxo de dados que se baseia no envio, junto com o reconhecimento, do número de octetos que o receptor tem condições de receber (tamanho da janela de recepção), contados a partir de último octeto da cadeia de dados recebidos com sucesso. Com base nessa informação, o transmissor atualiza a sua janela de transmissão, ou seja, calcula o número de octetos que pode enviar antes de receber outra liberação.

**CONCEITO DE PORTA, SOCKET E CONEXÃO NO TCP**

Ainda, de acordo com Soares et al. (1995), com o intuito de que se possa permitir que vários processos em um único *host* possam simultaneamente transmitir cadeias de dados, ou seja, possam usar seus serviços, o *TCP* utiliza o conceito de porta. Cada um

dos usuários (processos de aplicação) que o *TCP* esteja atendendo em um dado momento, é identificado por uma porta diferente.

Como os identificadores de portas são selecionados isoladamente por cada entidade *TCP*, eles podem não ser únicos na Inter-rede. Para obter um endereço que identifique univocamente um usuário *TCP*, o identificador da porta é concatenado ao endereço *IP* onde a entidade *TCP* está sendo executada, definindo um *socket* (identificação de um usuário em uma inter-rede).

A associação de portas e processos é tratada independentemente por cada entidade *TCP*. Entretanto, processos servidores que são muito usados (*FTP*, *Telnet*, *SMTP*, etc.) são associados a portas fixas, que são então divulgadas para os usuários.

Uma conexão é identificada pelo par de *sockets* de suas extremidades. Um *socket* local pode participar de várias conexões diferentes com *sockets* remotos. Uma conexão pode ser usada para transportar dados, em ambas as direções simultaneamente, ou seja, as conexões *TCP* são *Full-duplex* (transmissão de dados em duas direções simultaneamente).

Os mecanismos utilizados nas funções de controle de erros e de fluxo exigem que o *TCP* inicie e mantenha informações de estado para cada conexão estabelecida. O conjunto dessas informações, os *sockets*, os números de seqüência, o tamanho das janelas, etc. definem uma conexão.

**PROTOCOLO UDP**

Dentro da tecnologia *TCP/IP*, segundo Soares et al. (1995), o protocolo *UDP* opera no modo sem conexão e fornece um serviço *datagrama* não-confiável, sendo uma simples extensão do protocolo *IP*. O protocolo *UDP* tem como função principal receber os pedidos de transmissão de mensagens entregues pelos processos de aplicação da estação de origem, e os encaminha ao *IP* que é o responsável pela transmissão, sendo que na estação destino acontece o processo exatamente ao contrário.

O protocolo *IP* entrega as mensagens (*datagramas*) recebidas ao *UDP* que as entrega aos processos de aplicação e a principal função do *UDP* é *multiplexar* (transmitir vários sinais utilizando uma única via de comunicação ou canal.), na origem, e *demultiplexar* (desmontar um sinal agregado em seus vários canais componentes), no destino, o acesso ao Nível Inter-rede.

O trabalho conjunto de todos os protocolos contribui para um processo de segurança na rede que, somado ao *hardware* e *softwares* existentes, promovem uma melhor garantia de que havendo uma Política de Segurança da Informação

implementada, o controle e a segurança da informação em trânsito pela rede estarão monitorados e administrados.

## PROTOCOLOS, APLICAÇÕES TCP/IP E OS ASPECTOS DE SEGURANÇA

Ainda segundo Soares et al. (1995), na arquitetura *TCP/IP* as aplicações são implementadas de forma isolada. Não existe um padrão que defina como deve ser estruturada uma aplicação, como no modelo da *OSI*. As aplicações trocam dados visando diretamente a Camada de Transporte, por meio de camadas padronizadas, por onde os dados iniciarão o processo de transferência por meio do meio de transmissão destes dados.

Além de compartilhar o mesmo conjunto de primitivas de transportes, muitas das aplicações *Internet TCP/IP* adotam o modelo Cliente / Servidor. Neste modelo, a denominação servidor refere-se a qualquer aplicação que ofereça um serviço a outra aplicação, serviço que pode ser requisitado por meio de da Inter-rede. Uma aplicação torna-se cliente quando envia uma solicitação a um servidor e espera por uma resposta. Para cada aplicação, são caracterizados os requisitos de segurança e uma tecnologia de segurança específica. Por exemplo, um conjunto de protocolos e uma infra-estrutura de suporte, são identificados como apropriados para fornecer os serviços de segurança requisitados.

O mapeamento entre mecanismos de segurança e aplicações, em alguns casos, baseia-se no exame de um protocolo de aplicação específico, porém, na maior parte dos casos, baseia-se nos requisitos percebidos em qualquer protocolo que forneça um determinado serviço de rede. Em alguns casos, protocolos específicos podem ser citados como apropriados para fornecer um mecanismo de segurança necessário. Em outros, é identificado um vazio em termos de funcionalidade de segurança disponível, indicando que é preciso desenvolver a tecnologia necessária.

A Tabela 3, abaixo, apresenta um relacionamento entre as aplicações e os serviços de segurança.

Tabela 3 – Relacionamento entre Aplicações *Internet* e os Serviços de Segurança

| | **Aplicação** | | | | | | |
|---|---|---|---|---|---|---|---|
| **Serviços** | **Correio Eletrônico** | **Serviço de Diretório** | **Gerencia-mento** | **Terminal Virtual** | **Transf. De Arquivo** | **Servidores Arquivo** | **Roteamento** |
| **Autenticação de Parceiro** | | | | **S** | **S** | **S** | **S** |
| **Autenticação da Origem** | **S** | **S** | **S** | | | | |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Controle de Acesso Confiabilidade com conexão** | | **S** | **S** | **S S** | **S S** | **S** | |
| **Confiabilidade sem conexão** | **S** | **S** | **S** | | | **S** | **S** |
| **Confiabilidade em campos selecionados** | | | | | | | |
| **Confiabilidade do Fluxo de tráfego** | | | | | | | **S** |
| **Integridade c/conexão e com recuperação** | | | | **S** | **S** | | |
| **Integridade c/conexão e sem recuperação** | | | | | | | |
| **Integridade c/ conexão e com recuperação em campos selecionados** | | | | | | | |
| **Integridade s/ conexão Integridade s/ conexão em campos selecionados.** | **S** | **S** | **S** | | | **S** | **S** |
| **Impedimento de Rejeição da origem** | **S** | | | | | | |
| **Impedimento de rejeição do destino** | **S** | | | | | | |

Fonte: Soares, Luiz F. G., Lemos, Guido, Colcher, Sérgio. (1995, p.482).

## SERVIÇOS DO PROTOCOLO TCP

Segundo Soares et al. (1995), o protocolo *TCP* fornece seguramente dois caminhos de fluxo de transmissão de dados, entre dois programas que são processados no mesmo ou em diferentes computadores. Os meios em que os dados são transmitidos são seguros e garantem a chegada de cada *Byte* (unidade de armazenamento de informação em computadores), ao seu destino, na ordem em que fora transmitido. Caso a conexão física seja interrompida, os *Bytes* que ainda não foram transmitidos deixam de alcançar seus destinos, a menos que as rotas sejam alteradas. Se isto ocorrer, o computador com implementação *TCP* envia uma mensagem de erro para o processo que é responsável para enviar ou receber caracteres, isto ocorre sem que o usuário perceba. Cada conexão é dedicada para a extremidade de uma porta. As portas são identificadas por números de 16 *bits*. Todas as conexões *TCP/IP* podem ser identificadas por um conjunto de números de 32 e 16 *bits*, podendo ser:

- Endereço do *host* de origem da conexão.
- Número da porta origem da conexão.
- Endereço do host do destino da conexão.

- Número da porta destino da conexão.

O *TCP* utiliza dois *Bits* especiais no cabeçalho do pacote, o *SYN* e o *ACK*, para negociar a criação de novas conexões. Para abrir uma conexão, o *host* pede para que seja enviado um pacote que tenha o *Bit SYN* configurado, mas não tenha o *Bit ACK*. Recebendo, o servidor reconhece o pedido, enviando de volta um pacote com os dois *Bits* configurados. Finalmente, o host envia um terceiro pacote, novamente com o *Bit ACK* configurado, e o *SYN* desligado. Este processo é conhecido como "*TCP* three way handshake". Com este procedimento, o *TCP* consegue distinguir pacotes requisitados por uma nova conexão de pacotes que já foram enviados como resposta de uma conexão já criada. Esta distinção é útil quando se constrói *Firewalls* baseados em filtro de pacotes.

O *TCP* é utilizado por muitos serviços que requerem o sustento de uma *transmissão Síncrona* (é a transmissão na qual os *bits* de dados são enviados a uma taxa fixa com o transmissor e o receptor, trabalhando exatamente na mesma freqüência), de fluxos de dados em uma ou mais direções. Por exemplo, o *TCP* é usado para serviço de terminal remoto, transferência de arquivos e correios eletrônicos. O *TCP* também é utilizado para enviar comandos de display usando o *Xwindows System* (que é uma característica de comunicação por meio de janelas entre os Sistemas Operacionais).

**SERVIÇOS DO PROTOCOLO UDP**

Tendo em vista que o protocolo *UDP* provê um sistema de enviar pacotes de dados entre dois ou mais programas executados na mesma ou em diferentes máquinas, este protocolo utiliza métodos não confiáveis para a transmissão de pacotes, por isso, não garante que o pacote será entregue para a máquina destino na ordem em que foi transmitido. A vantagem do *UDP* é que ele não é inferior ao *TCP*, e possui um controle de erro menos criterioso, possibilitando desta forma, uma maior velocidade. Os pacotes *UDP's* são enviados de uma porta da máquina origem para uma porta da máquina destino. Como o *TCP*, as portas *UDP* são identificadas por números de 16 *Bits*.

**PROTOCOLO FTP (FILE TRANSFER PROTOCOL)**

Ainda, segundo Soares et al. (1995), o *FTP* permite que, um usuário em um computador, transfira, efetue uma substituição de nomes de arquivos ou remoção dos mesmos existentes em diretórios remotos. O *FTP* só permite a transferência de arquivos completos. Antes de executar qualquer operação o usuário solicitante (cliente) envia sua

identificação (*login*) e sua senha para o servidor, que impede a execução de qualquer operação, caso o usuário não tenha sido registrado. A operação de *FTP* baseia-se no estabelecimento de duas conexões entre o cliente e o servidor. Uma conexão, denominada conexão de controle, é usada para transferência de comandos, e a outra, denominada conexão de transferência de dados. A conexão de controle permanece aberta enquanto durar a sessão *FTP*. Durante uma sessão podem ser transferidos vários arquivos, cada um deles em uma conexão de transferência de dados estabelecida especificamente para tal. Na Figura 24 temos um exemplo do funcionamento do *FTP*:

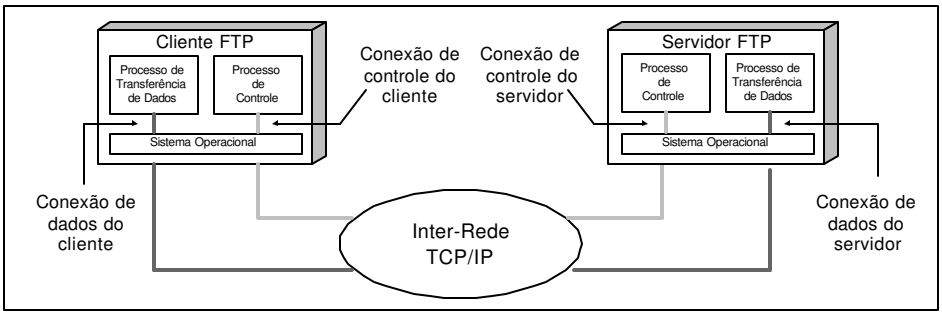



Figura 24 – Funcionamento do FTP

Fonte: Soares, Luiz F. G., Lemos, Guido, Colcher, Sérgio. (1995, p.409).

O *FTP* permite que sejam transferidos arquivos do tipo texto ou binários. Os arquivos do tipo texto são manipulados como sendo compostos por uma cadeia de caracteres *ASCII* ou *EBCDIC*. Os arquivos do tipo *binário* (sistema de informação com dois símbolos). Todos os dados que entram em um computador são codificados em dois símbolos representados por zero (0) e um (1)), são vistos como sendo formados por uma seqüência de *octetos*, que são transferidos sem qualquer conversão. O *FTP* toma providências para compatibilizar o código de caracteres, os delimitadores de fim de linha, etc., quando transfere arquivos entre máquinas onde os dados têm representações diferentes.

Os requisitos de segurança no *FTP* devem incluir integridade e confidencialidade em conexões, autenticação de parceiros e controle de acesso baseado em identidade. Algumas restrições devem ser consideradas, quando da disponibilidade do serviço *FTP*, tais como:

- Não permitir que *hosts* externos àrede acessem as máquinas usando *FTP*.
- Se houver necessidade de liberar o uso do *FTP* para hosts remotos, utilizar um *FTP* server.
- Excluir o direito de escrita no diretório utilizado pelo *FTP*.

**PROTOCOLO TFTP (TRIVIAL FILE TRANSFER PROTOCOL)**

De acordo com Soares et al. (1995), a arquitetura *TCP/IP* define, adicionalmente, um outro protocolo que fornece um serviço simplificado de transferência de arquivos, o *TFTP* (*Trivial File Transfer Protocol*). O *TFTP* restringe sua operação simplesmente a transferências de arquivos, não implementando mecanismos de autenticação e operando em uma única conexão. O *TFTP* utiliza o *UDP* para o transporte de blocos de dados de tamanho fixo. Como o serviço fornecido pelo *UDP* não garante a entrega dos blocos ao destinatário, o *TFTP* utiliza o protocolo de *bit* alternado para transmitir seus blocos.

*TFTP* é uma simplificação do protocolo de transferência de arquivos, padrão do *Unix* (*FTP*). Ele é projetado para ser implementado em *ROM* de sistema *Diskless* (sem disco) como terminal, W*orkstations Diskless* (computadores com grande capacidade de processamento, robustez e de armazenamento de dados. Geralmente utilizam o Sistema Operacional *Unix*, porém sem discos para armazenamento de dados), e roteadores. Não existe autenticação com o *TFTP:* um cliente *TFTP* simplesmente efetua a conexão com o servidor e questiona por um arquivo, sem dizer para quem é o arquivo. Se o arquivo pode ser acessado pelo servidor, então o arquivo é enviado ao cliente. Por este motivo, existe a necessidade de ter muito cuidado sobre quem acessa o servidor por meio do comando *TFTP*. Não é recomendado que se tenha tráfego do protocolo *TFTP* pelo seu *Firewall*, por se tratar de um serviço que pode ser usado sem autenticação e, em conseqüência, sem mecanismos confiáveis de segurança em rede.

**NFS (NETWORK FILE SYSTEM)**

Segundo Soares et al. (1995), o *NFS (Network File System),* permite que um sistema tenha acesso a arquivos localizados remotamente, de um modo integrado e transparente, fornece, ainda, a ilusão de que os discos, impressoras, ou outros dispositivos fisicamente localizados em um sistema remoto, estão diretamente conectados ao sistema local. As aplicações que executam em uma máquina onde é instalado um cliente *NFS*, simplesmente "acreditam" que a máquina possui alguns dispositivos adicionais. Esses dispositivos virtuais adicionais são associados em dispositivos fisicamente localizados em outras máquinas. O *NFS* permite, por exemplo, que estações que não possuam dispositivos de armazenamento, ou que possuam dispositivos com pouca capacidade, armazenem informações de modo transparente em equipamentos que possuam espaços disponíveis. Outro benefício é permitir o compartilhamento a arquivos comuns por diversos usuários.

Quando é executada uma operação para abrir, ler ou gravar dados em um arquivo, o mecanismo que controla o acesso ao sistema de arquivos intercepta a operação e verifica se o acesso é local ou remoto. Se o acesso for local, o redirecionador transfere a execução para o sistema de arquivos local. Se o acesso é remoto, o redirecionador entrega sua solicitação ao cliente *NFS*, que a envia, utilizando o protocolo de transporte *UDP*, ao servidor *NFS*. Os requisitos de segurança nestes sistemas incluem: a integridade e confiabilidade no intercâmbio de *datagramas*, a autenticação de parceiros e o controle de acesso (baseado em identidade). Alguns desses serviços (confiabilidade e integridade) podem ser fornecidos por protocolos do Nível de Rede e de Transporte. Entretanto, a granularidade necessária para o controle de acesso, por exemplo, ao nível de arquivo ou diretório, é obviamente mais fina do que a que pode ser fornecida no Nível de Rede e de Transporte. Como até o momento, não foram definidos padrões para o protocolo de segurança que suportam esta aplicação, ainda não há recomendação para os servidores de arquivos na arquitetura de segurança da *Internet*.

Os principais problemas de segurança são:

- O servidor NFS "confia" em um endereço IP para autenticar máquinas clientes, tornando-se vulneráveis para endereços forjados;
- O servidor *NFS* "confia" no cliente para autenticar o usuário, tornando-se vulnerável para qualquer usuário que utiliza aquela máquina;
- O servidor *NFS* não verifica novamente a autenticação de um cliente, em toda solicitação. O servidor assume que, se um cliente utiliza um cabeçalho de arquivo válido, o cliente é autorizado a usar o *File* System. (Sistema de Arquivos). Um *Hacker* pode acessar o *File System*, forjando ou capturando o cabeçalho de um arquivo válido.

Sendo assim, é aconselhável que o protocolo *NFS* não seja acessado externamente àrede. A Figura 25 apresenta um esquema de uma arquitetura do *NFS*.

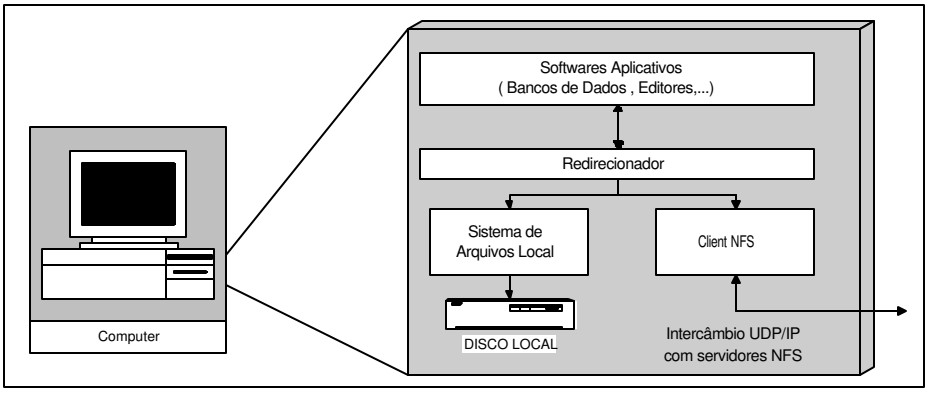



Figura 25 – Arquitetura de um Cliente NFS

Fonte: Soares, Luiz F. G., Lemos, Guido, Colcher, Sérgio. (1995, p.410).

**RPC (REMOTE PROCEDURE CALL)**

O mecanismo *RPC (Remote Procedure Call)*, foi projetado para facilitar o desenvolvimento de aplicações distribuídas, baseadas no modelo de interação Cliente / Servidor. Quando o programa cliente faz uma chamada a um procedimento remoto, os argumentos da chamada são entregues ao cliente *RPC*, que compõe uma mensagem e a envia ao servidor, passando então a aguardar o retorno do resultado. O servidor *RPC*, ao receber uma mensagem, invocando a execução de um procedimento, inicia sua execução e ao seu término envia os resultados obtidos de volta para o cliente *RPC*. O cliente *RPC*, ao receber de volta a mensagem com o resultado da execução do procedimento remoto, entrega esse resultado ao processo de aplicação, colocando-os nos respectivos argumentos da chamada de procedimento.

**XDR (EXTERNAL DATA REPRESENTATION)**

A ferramenta *XDR (EXTERNAL DATA REPRESENTATION),* permite aos programadores escreverem aplicações distribuídas onde são intercambiados dados entre máquinas que os representam de forma distinta, sem que seja necessário escrever procedimentos para compatibilizar as representações. A solução adotada na ferramenta *XDR* foi a definição de uma representação independente de qualquer máquina que é usada para codificar os dados intercambiados.

Quando se deseja transmitir dados, um programa de aplicação chama os procedimentos *XDR*, que converte a representação local para a representação de transferência e, em seguida, transmite os dados convertidos. O programa que recebe os dados chama os procedimentos *XDR*, que convertem a representação de transferência para a representação local específica.

**PROTOCOLO TELNET**

Segundo Soares et al. (1995), o protocolo *Telnet* (protocolo de emulação de terminal normalmente utilizado em aplicações que usam de linha de comando na *Internet* e que fornece serviços de terminal virtual), permite que um usuário que esteja utilizando uma máquina H estabeleça uma sessão interativa na máquina J, na rede. A partir deste momento, todas as teclas pressionadas na máquina H, são repassadas para a máquina J, como se o usuário estivesse utilizando um terminal ligado diretamente a ela. Os comandos digitados na máquina H são processados na máquina J, e o resultado de sua

execução é enviado de volta para ser exibido no monitor da máquina H. O módulo cliente do *Telnet* permite que o usuário identifique a máquina a qual deseja se conectar pelo nome ou por seu endereço *IP*.

A segunda opção torna possível o estabelecimento de conexões remotas em ambientes onde não seja possível fazer associação entre nomes e endereços *IP*.

O protocolo *Telnet* é construído com base em três idéias:

- Conceito de terminal virtual de rede: assume-se que ambas as extremidades estão ligadas a um terminal virtual de rede *NVT* (*Network Virtual Terminal*). Um *NVT* é um dispositivo lógico que fornece uma representação padronizada de um terminal. Com esse conceito, é eliminada a necessidade das máquinas participantes da conexão conhecerem as características do terminal utilizado por seus parceiros. Tanto o servidor quanto o cliente, obedecem a características e convenções de seus terminais locais nas características do *NVT*.
- Princípio de negociação de opções: permite que os usuários envolvidos em uma conexão negociem opções que definem o comportamento do terminal virtual. Dentre as opções negociadas, estão o formato de representação dos caracteres utilizados, e o modo de operação (*Half- Duplex* (transmissão de dados em duas direções, porém em uma direção de cada vez.), ou *Full-Duplex* (transmissão de dados em duas direções simultaneamente.).
- Tratamento equivalente de terminais e processos: o cliente não precisa ser necessariamente um terminal, podendo ser um processo de aplicação qualquer. Uma outra implicação da simetria da conexão é que ambas as extremidades da conexão podem tomar a iniciativa da negociação de opções, o que não seria possível em uma arquitetura cliente / servidor básica, onde o servidor é passivo, ou seja, só entra em funcionamento em resposta a solicitações feitas pelo cliente.

Os requisitos de segurança no *Telnet* se assemelham muito ao do *FTP* e definem o seguinte: inclusão de integridade e confidencialidade em conexões, autenticação de parceiros e controle de acesso baseado em identidade. Esses serviços podem ser implementados por mecanismos nos próprios protocolos de aplicação, ou por meio do uso de mecanismos de camadas inferiores, por exemplo, Transporte e Rede.

A Figura 26 apresenta um exemplo de conexão TELNET:

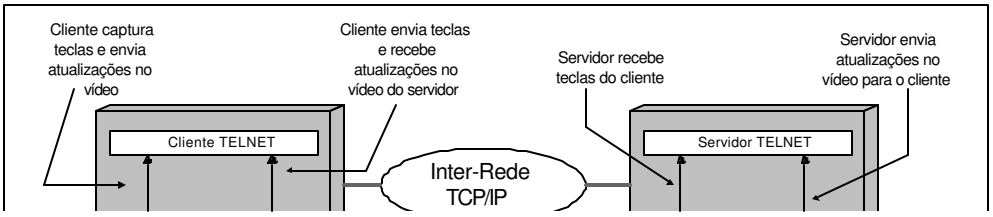


Figura 26 – Conexão TELNET

Fonte: Soares, Luiz F. G., Lemos, Guido, Colcher, Sérgio. (1995, p.414).

**SERVIÇOS DHCP (DYNAMIC HOST CONFIGURATION PROTOCOL)**

Todo computador conectado a redes *IP* precisa, para se comunicar, de uma identificação numérica. Esta identificação é conhecida como endereço *IP*. O endereço *IP* pode ser atribuído de forma estática ou dinâmica.

Endereços *IP* atribuídos estaticamente possuem algumas desvantagens. Sempre que um equipamento for movido de uma rede para outra o endereço *IP* tem que ser alterado manualmente, o que pode envolver uma consulta ao administrador de redes. Adicionalmente, cada rede *IP* possui um *Gateway* distinto, que também precisa ser indicado na configuração do equipamento.

Endereços atribuídos dinamicamente oferecem uma flexibilidade maior. Libertam o usuário de conhecer detalhes sobre a configuração de sua máquina, permitindo-lhes uma maior mobilidade dentro da rede. Tudo o que é necessário é desconectar o equipamento de um ponto e ligá-lo em outro e tudo continuará funcionando normalmente. Usuários de computadores portáteis se beneficiam ainda mais, pois ficam livres de constantemente terem que identificar endereços *IP* livres nas redes em que irão trabalhar.

A atribuição dinâmica de endereços *IP* é feita por meio do protocolo *DHCP (Dynamic Host Configuration Protocol).* Seu uso e configuração, tanto do lado do cliente como do servidor, é extremamente simples.

**PROTOCOLO SNMP (SIMPLE NETWORK MANAGEMENT PROTOCOL)**

O sistema de gerenciamento de redes da arquitetura *Internet TCP/*IP, ainda segundo Soares et al. (1995), opera na camada de aplicação e baseia-se no protocolo *SNMP (Simple Network Management Protocol*). Como no esquema gerenciamento *OSI*,

também para o *TCP/IP*, os processos que implementam as funções de gerenciamento atuam como agentes ou gerentes. Os agentes coletam junto aos objetos gerenciados as informações relevantes para o gerenciamento da rede, o gerente processa as informações recolhidas pelos clientes, com o objetivo de detectar a presença de falhas no funcionamento dos componentes da rede (*Hosts*, *Router*, processos executando os protocolos de comunicação, etc.), para que possam ser tomadas providências no sentido de contornar os problemas que possam ocorrer como conseqüência de falhas.

O software gerenciador envia comandos aos agentes, solicitando uma leitura no valor das variáveis dos objetos gerenciados (get e response), ou modificando seu valor (put). A modificação do valor de uma variável pode ser usada para disparar indiretamente a execução de operações nos recursos associados aos objetos gerenciados (por exemplo, uma reinicialização). Na troca de informações entre o gerente e o agente, são aplicados mecanismos de autenticação para evitar que usuários não autorizados interfiram no funcionamento da rede. A troca de mensagens entre o gerente e o agente é definida pelo protocolo *SNMP*. O *SNMP* define o formato e a ordem que deve ser seguida no intercâmbio de informações de gerenciamento. As informações sobre os objetos gerenciados são armazenados na *MIB (Management Information Base)*, que contém as informações sobre o funcionamento dos *Hosts*, dos *Routers*, dos processos que executam os protocolos de comunicação (*IP*, *TCP*, *ARP (Address Resolution Protocol)*, etc.).

O funcionamento do *SNMP* mostrado na figura abaixo se baseia na troca de operações que permite que o gerente solicite e que o agente lhe informe, ou modifique, o valor de uma variável de um objeto na *MIB*. O *SNMP* define também uma operação, (TRAP), que permite que um agente informe ao gerente a ocorrência de um evento específico. Melhoramentos recentes no *SNMP* (*SNMP* versão 2) provê suporte a um conjunto de requisitos de segurança. Os serviços de segurança que passaram a ser fornecidos foram: confidencialidade e integridade (com proteção contra reenvio postergado - replay) na transmissão de *datagramas*, autenticação na origem de dados e controle de acesso baseado na identidade. Esses serviços são empregados na proteção contra violações do intercâmbio de informações de gerenciamento, e para proteger os objetos gerenciados contra tentativas de manipulação não autorizada. Todos esses serviços foram implementados no *SNMP* no nível de aplicação, incluindo um esquema de distribuição de *chave*s simétricas. A Figura 27 apresenta um esquema de funcionamento do Protocolo *SNMP*.

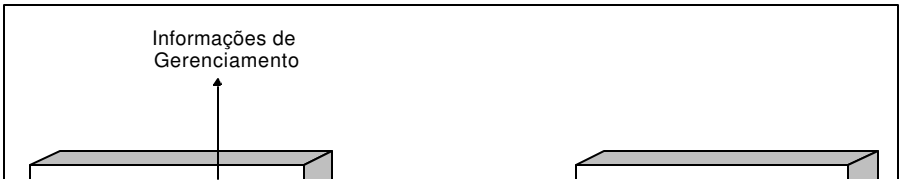


Figura 27 – Funcionamento do SNMP

Fonte: Soares, Luiz F. G., Lemos, Guido, Colcher, Sérgio. (1995, p.420).

Toda esta tecnologia de redes de computadores transmite os dados por Redes *LAN (Local Area Network),* que é uma rede cuja dimensão é de curta distância, num raio de poucos quilômetros, como também por uma Rede *WAN (Wide Área Network),* que é uma rede para longas distâncias, sendo necessário o uso de roteadores, linhas de comunicação privadas e fornecidas por provedoras de serviços de comunicação como a Telefônica, Intelig ou Embratel. Como tecnologia que está sendo utilizada em grande escala atualmente para a comunicação de dados em uma WAN, pode-se citar o *Frame Relay*. O *Frame Relay* é uma tecnologia de transmissão de dados em alta velocidade, sem verificação de erro, utilizando a Comutação por Pacotes, ou seja, o dado a ser transmitido é segmentado em pequenas partes denominadas Pacotes e são transmitidas pelos canais de dados do *Frame Relay*.

**A UTILIZAÇÃO DE REDES INDEPENDENTES**

Em redes de computadores podem existir em uma única *LAN*, em um único local, mais de um servidor, servindo a propósitos diferentes e que podem ser independentes na sua funcionalidade, ou pode-se ter várias redes distribuídas em diversas localidades enviando e recebendo informações, cuja denominação técnica é interconexão de redes.

A interconexão de rede visa a formação de uma rede corporativa, e pode ser feita por equipamentos como:

- Multiplexadores (*TDM (Time Division Multiplexor)* ou estáticos);
- Roteadores (para encaminhar os dados ao seu destino, conectar redes com diferentes protocolos, efetuando inclusive verificação e correção de erros);
- Bridges (pontes utilizadas para conexão de redes de um mesmo tipo, segmentando tráfego);
- Gateways (para converter protocolos no nível de aplicação, visando àconexão de redes diferentes);

- Switches (para a comutação de células e pacotes);
- Estações de satélite;
- Sistemas de microondas, soluções W*ireless* (transmissão de dados via rádio. Satélite ou infravermelho), e demais equipamentos.

O uso de redes interconectadas numa instituição é viável quando se tem um grande volume de dados trafegando entre as filiais, escritórios ou agências e a sua matriz central e um computador central armazena as bases de dados, liberando acesso às filiais.

Todas as tecnologias e recursos citados quando implementados corretamente promovem uma maior garantia da segurança na rede e, em conseqüência, aos dados armazenados e principalmente ao correio eletrônico, que precisa garantir a confiança dos usuários neste serviço e na tecnologia. Caso uma mensagem recebida pelo usuário, que contenha arquivos anexados e contaminados por vírus de computador, seja distribuída no ambiente de rede, o problema causado terá proporções grandes o bastante para provocar até uma paralisação das operações principais do negócio, sendo assim, a segurança do correio eletrônico tem uma importância estratégica para a sobrevivência do negócio, assunto que será abordado no próximo capítulo.