**Universidade Federal de Santa Catarina**

**Programa de Pós-Graduação em Engenharia de Produção**

# *Uma Metodologia para Normatização de Correio Eletrônico em Organizações*

Dissertação de Mestrado

Jocênio Marquios Epaminondas

Florianópolis
2001

# *Uma Metodologia para Normatização de Correio Eletrônico em Organizações*

**Universidade Federal de Santa Catarina**

**Programa de Pós-Graduação em Engenharia de Produção**

# *Uma Metodologia para Normatização de Correio Eletrônico em Organizações*

Jocênio Marquios Epaminondas

Dissertação apresentada ao
Programa de Pós-Graduação em
Engenharia de Produção da
Universidade Federal de Santa Catarina
como requisito parcial para obtenção
do título de Mestre em
Engenharia de Produção

Florianópolis
2001

Jocênio Marquios Epaminondas

# *Uma Metodologia para Normatização de Correio Eletrônico em Organizações*

Esta Dissertação foi julgada adequada para obtenção do título de **Mestre em Engenharia de Produção** e aprovada em sua forma final pelo **Programa de Pós-Graduação em Engenharia de Produção da Universidade Federal de Santa Catarina**.

**Florianópolis, 27 de Julho de 2001.**

**Prof. Ricardo Miranda Barcia, Ph.D.**

Coordenador

**Banca Examinadora**

_____

Prof. Edis Mafra Lapolli, Drª .
Orientadora

_____

Prof. Ana Maria Bencciveni Franzoni, Drª .

_____

Prof. Lia Caetano Bastos, Drª .

_____

Prof. José Lucas Pedreira Bueno, M.Eng.

A Deus por guiar meus caminhos e a minha esposa, Graciete, *pelo amor, paciência, compreensão e apoio constante.*

# AGRADECIMENTOS

A todos que estiveram presentes em minha vida acadêmica, participando e contribuindo para o meu desempenho espiritual, pessoal e profissional.

Em particular, gostaria de agradecer:

Aos meus pais (pela educação), minha esposa, irmãos e familiares, pelo amor e apoio que sempre me deram e continuam dando;

A minha orientadora, professora Édis Mafra Lappoli, pelo apoio e confiança.

Aos professores, funcionários e colegas do Programa de Pós Graduação em Engenharia de Produção, pela parcela de contribuição, amizade e estímulos diários.

A UNEB, pelo constante apoio pedagógico ao longo dessa caminhada;

A EMIBM - Engenharia e Comércio Ltda, por confiar em meu potencial;

A meus chefes e colegas da DATAPREV e da UNEB, que tanto me ajudaram no apoio àrealização deste trabalho.

Ao Elisnaldo, Vilmar, Eliane, Prof. Gaspar (UNEB), Marcos Ambrogi e Fernando Benício, que tão bem me acolheram e apoiaram durante a fase mais crítica desta dissertação.

Ao Marcelo, Josélio e Joseney da Excellence Informática pelo apoio, confiança e disponibilização de material técnico.

Finalmente, agradeço a todos os meus colegas e amigos, que de forma direta ou indireta contribuíram para este resultado.

*"A fim de moldar o futuro que se avizinha, precisaremos de novas e poderosas ferramentas intelectuais – novas teorias de mudança e causação – capazes de explicar a nova complexidade social e política; novas categorias e sistemas de classificação e novos modelos que nos ajudem a facilitar a vida e o desenvolvimento humano."*

*Alvin Toffler*

# Sumário

# LISTA DE FIGURAS

# LISTA DE QUADROS

# LISTA DE ABREVIAÇÕES

| | |
|---|---|
| DATAPREV | Empresa de Tecnologia e Informações da Previdência Social |
| MPAS | Ministério da Previdência e Assistência Social |
| WWW | World Wide Web |
| IETF | Internet Engineering Task Force |
| IAB | Internet Architecture Board |
| DARPA | Defense Advanced Research Projects Agency |
| ARPANET | Advanced Research Projects Agency |
| EUA | Estados Unidos da América |
| TCP/IP | Transfere Control Protocol / Internet Protocol |
| FTP | File Transfer Protocol |
| RNP | Rede Nacional de Pacotes |
| POP'S | Point of Presence |
| CTDF.O | Centro de Tratamento de Informações do Distrito Federal |
| SDFS.P | Supervisão de Suporte Técnico |
| SDFU.P | Supervisão de Atendimento ao Usuário |

# Resumo

Epaminondas, Jocênio Marquios. **Uma metodologia para normatização de correio eletrônico em organizações**. Florianópolis, 2001. 147f. Dissertação (Mestrado em Engenharia de Produção com Ênfase em Informática)- Programa de Pós Graduação em Engenharia de Produção, UFSC, 2001.

O serviço de correio eletrônico atualmente é um dos serviços de Internet que mais cresce no ambiente corporativo.

Essa evolução vem trazendo vários problemas para as organizações no que tange principalmente aos tipos de informações que circulam dentro da rede corporativa. Sendo assim, destaca-se que o problema se agrava ainda mais por não existir nenhum tipo de controle dos conteúdos das mensagens enviadas e/ou recebidas. Deixando brechas, ocasionando a má utilização e abuso do serviço.

Neste trabalho é proposta uma normatização para utilização do correio eletrônico corporativo, definindo responsabilidades e sanções (administrativas e/ou penal) a serem aplicadas a quem infligi-la. Também são apresentados alguns softwares para monitoramento eletrônico do serviço de correio eletrônico, tendo como finalidade vigiar quaisquer tipos de arquivos armazenados, recebidos e enviados. Dando ênfase também aos aspectos legais envolvidos no assunto.

Palavras-Chave: monitoramento eletrônico, Correio Eletrônico, normatização, organizações, aspectos legais.

# Abstract

Epaminondas, Jocênio Marquios. **Uma metodologia para normatização de correio eletrônico em organizações**. Florianópolis, 2001. 147f. Dissertação (Mestrado em Engenharia de Produção com Ênfase em Informática)- Programa de Pós Graduação em Engenharia de Produção, UFSC, 2001.

The electronic mail service is now one of the Internet services that more grows in the corporate atmosphere.

That evolution is bringing several problems for the organizations in what plays mainly to the types of information that circulates inside of the corporate net. Being like this, we detached that the problem becomes worse more because does not exist no one type of control in the contents of the sent messages and/or received. Leaving breaches, causing the bad use and abuse of the service.

In this work normalization is proposed for use of the corporate electronic mail, defining responsibilities and sanctions (administrative and/or penal) to be applied at a person that can inflict it. Also are presented some software's to the electronic monitoring of the electronic mail service, having as purpose to watch any type of stored files, sent and received. Giving emphasis also to the legal aspects involved in the subject.

Word-key: electronic monitoring, Electronic mail, normalization, organizations, legal aspects.

# 1 . INTRODUÇÃO

## 1.1 Origem do Trabalho

A Internet permite que milhões de usuários de computadores consultem e partilhem informações. Centenas de milhares de computadores estão permanentemente conectados através de muitas redes de dados, disponibilizando informações e serviços aos milhões de computadores que casualmente a elas se ligam.

As redes eletrônicas de computadores proporcionam a seus usuários comunicação a baixo custo e acesso a fontes inesgotáveis de informação. Uma das principais características da Rede Mundial é ampliar e democratizar o acesso à informação, eliminando barreiras como distância, fronteiras, fuso horário etc.

O número estimado de usuários da Internet é de 40 milhões em mais de cem países. Esta significativa massa de usuários acessa a rede através de computadores e terminais em instituições educacionais, provedores comerciais e outras organizações.

Além dos recursos básicos de correio eletrônico e lista de discussão, a Internet proporciona a seus usuários acesso aos mais variados serviços de informação como, por exemplo: bases de dados especializadas, catálogos de bibliotecas, repositórios de software de domínio público, jornais e revistas

eletrônicas etc. Através da Internet, também, é possível ter acesso a recursos de hardware especializados como computadores de alto desempenho e processadores especializados.

Estes serviços estão normalizados e foram aceitos por organismos que regram de algum modo o funcionamento da Internet, ou, que pela via do mercado ditaram as suas regras e se tornaram populares.

Ao serem aceitos, os serviços e os protocolos de comunicação que os implementam foram sendo sucessivamente utilizados comumentemente por uma vasta gama de programas, a qual é capaz de comunicar-se entre si e entender-se na troca de dados.

As mensagens enviadas através do correio eletrônico podem ser interceptadas, de modo geral, por outras pessoas. Por este motivo, não é aconselhável que se envie mensagens confidenciais, uma vez que o envio de mensagens via correio eletrônico não é totalmente seguro.

Não há garantia de privacidade no uso do correio eletrônico. O ideal é imaginar a mensagem enviada por este meio como um cartão postal, destinado a alguém, mas que pode ser lido no meio do caminho. Uma mensagem de e-mail fica armazenada no computador de quem a enviou, onde pode ser lida por programas de recuperação de dados mesmo que apagada. A mensagem, uma vez enviada, passa por uma série de provedores, numa rota que depende do seu destino, e fica armazenada no servidor até que o destinatário se conecte à rede e baixe a mensagem. Nesse servidor pode facilmente ser lida pelos administradores. Isso não significa que os provedores leiam as mensagens, significa apenas que isso é tecnicamente possível, uma vez que o

administrador da rede tem poder para isso. É importante lembrar também que é muito fácil falsificar o remetente de uma mensagem eletrônica, no que se chama *fake mail*, e que o texto pode ser facilmente editado. Evite, portanto, enviar informações confidenciais por e-mail.

Diante disto, este projeto propõe a implementação de uma metodologia para normatização de correio eletrônico em organizações, o qual orientará sobre quais tipos de mensagens deve ser enviada na rede, segurança, plataforma, infra-estrutura, capacidade de armazenamento, formatação do texto, tipos de mensagens e divulgação de correio para fins de interesse da organização, dentre outros.

Tendo, portanto, como meta o estabelecimento de normas para uma administração de serviços de correio eletrônico mais eficientes em organizações, servindo como fonte de orientação na implementação de políticas internas (procedimentos, padrões, softwares, sanções etc.) para utilização de correio eletrônico.

## 1.2 Objetivos do Trabalho

### 1.2.1 Objetivo Geral

Este trabalho apresenta como objetivo geral à elaboração de procedimentos para utilização de Correio Eletrônico em organizações. Para tanto, a seguir, são delineados os objetivos específicos necessários.

### 1.2.2 Objetivos Específicos

Têm-se como objetivos específicos:

- Definir metodologias para controle de mensagens eletrônicas enviadas via e-mail, analisando os fatores de segurança, acesso remoto, cultura de usuários, dentre outros; e
- Reunir procedimentos implementados por administradores de redes em seu ambiente de Internet, disponibilizando informações padronizadas a qual poderá ser implementada em qualquer organização, independentemente do seu setor de atuação.

## 1.3 Justificativa e Importância do Trabalho

As organizações passam por sérios problemas com relação ao uso de correio eletrônico: invasão da rede corporativa de computadores, recebimentos de arquivos contaminados, tipos de mensagens que trafegam na rede etc.

Uma falta de normatização e procedimentos agrava ainda mais esta situação, pois os administradores criam suas próprias regras e geralmente não as tem documentado, além de não orientar seus usuários de tais processos implementados; no qual esta responsabilidade acaba dependendo do bom senso de cada um.

Os itens abaixo refletem as principais justificativas para a pesquisa proposta:

- A inexistência de um padrão para orientar os usuários de rede interna de uma organização sobre o envio de mensagens eletrônicas;

- A falta de interação dos administradores de redes com os seus usuários, relacionado à utilização de correio eletrônico da corporação, ocasionando assim vários problemas que vai desde o recebimento de e-mails via listas de discussões até uma invasão da rede ou disseminação de vírus na rede, podendo causar danos irreparáveis aos dados corporativos;
- Disponibilizar de forma mais dinâmica padrões para utilização de correio eletrônico, orientando os usuários sobre quais tipos de dados podem ser recebidos via correio, a importância da segurança de seus dados, dentre outros;
- Expor como é formada uma infra-estrutura de correio eletrônico, tipos de equipamentos, especificações de segurança, tipos de softwares/aplicações adotados para a implantação de um serviço de correio eletrônico;
- Orientar as organizações quanto àsegurança de suas informações;
- Alertar as organizações no que tange à observação de alguns requisitos básicos para a segurança de dados: Disponibilidade, Integridade e a confiabilidade dos recursos da informação;
- Oferecer subsídios às organizações de como se deve proceder em caso de roubo/perca de informações organizacionais;
- A importância do monitoramento dos controles de segurança da informação implementados nas organizações;
- Facilitar a implementação de controles de segurança que atendam aos requisitos de sua política interna;
- A garantia de acesso a servidores é importante que se observe à questão de contingência (procedimentos que garantem a funcionalidade dos

serviços de informática), estes vão desde especificações de rotinas de backup's, até definição de utilização de servidores espelhados que tem como objetivo garantir a integridade e funcionamento de todos os serviços, sendo este processo transparente para os usuários que os utilizam;

- A necessidade de padrões para segurança da informação, sendo que , segundo pesquisas realizadas pela Módulo Security Solutions S/A (http://www.modulo.com.br), 41 % das invasões são realizadas a sistemas internos e 35% destas invasões são praticadas por funcionários da organização.

## 1.4 Estrutura do Trabalho

Este trabalho está estruturado em 5 capítulos.

O primeiro capítulo é introdutório e apresenta a origem, os objetivos, justificativas e importância do trabalho.

O segundo capítulo é dedicado a fundamentação teórica e apresenta uma visão geral da *World Wide Web* - WWW, mensagem eletrônica, correio eletrônico, e sua infra-estrutura, segurança da informação, segurança de correio eletrônico, políticas de segurança, os dez mandamentos para utilização correta de correio eletrônico, lista de falsos alarmes de correio eletrônico e responsabilidades dos usuários.

O terceiro capítulo é definido as normas para utilização de correio eletrônico.

No quarto capítulo são apresentados os resultados da aplicação do questionário e palestras apresentadas ao corpo funcional da empresa.

O quinto capítulo é reservado para as conclusões e recomendações para futuros trabalhos.

Finalmente, a Bibliografia consultada e referenciada é listada.

# 2 . FUNDAMENTAÇÃO TEÓRICA

## 2.1 Visão Geral da World Wide Web - WWW

A Internet é um conjunto de redes interligadas por diversas redes de computadores *Internetnetworking* pelo mundo inteiro. Para que estas redes se comuniquem devem-se utilizar uma mesma linguagem (protocolos) e serviços (ferramentas utilizadas para obter informações) em comum.

A tecnologia Internet surgiu com o propósito de ser transparente às conexões físicas, retirando das aplicações a responsabilidade de atuar nos detalhes dos níveis inferiores e ao mesmo tempo fornecendo diversas aplicações para viabilizar a interconectividade de ambientes distintos.

Na Internet, as informações podem ser encontradas em diferentes formatos e sistemas operacionais, rodando em qualquer tipo de máquina.

As redes variam muito de tamanho e complexidade dependendo do número de computadores envolvidos ou da quantidade de dados trocados entre si.

A comunicação pode ocorrer por dados, voz e vídeo, ou seja, utiliza recursos multimídia, exigindo maior velocidade para transmissão de dados. Tal processo é conhecido como *World Wide Web* ou Teia Mundial.

A Internet por ser um conjunto de redes, não possuem dono. Porém, existem organizações que são responsáveis por seu controle, cadastro de usuários, endereçamento de *hosts*; pode-se destacar:

- *Internet Society* – com sede em Virgínia - EUA, sendo responsável pelo direcionamento estratégico da Internet;
- *Internet Engineering Task Force* – IETF tem como atribuição desenvolver novos protocolos e aplicativos para uso na rede mundial;
- *Internet Engineering Sterig Group* – faz a validade dos desenvolvidos pela IETF e os submete para aprovação ao Internet Architecture Board - IAB;
- *Internic* - cadastra todas as redes locais à Internet e oferece serviços de consultoria e assistência técnica;

Resumidamente, o objetivo principal da Internet é a interconexão de ambientes heterogêneos sem distinção de fabricante, tecnologia ou arquitetura.

### 2.1.1 Evolução

Surgiu a partir de um projeto da Defense Advanced Research and Projects Agency - DARPA, tendo como objetivo interligar os computadores de seus órgãos de pesquisa e departamentos oficiais em pesquisas e projetos voltados àdefesa dos EUA, (Cyclades do Brasil, 1996).

Nascida em 1969 nos Estados Unidos da América - EUA, com o nome de Advanced Research Projects Agency - ARPANET, interligavam originalmente os laboratórios de pesquisa e era uma rede do Departamento de Defesa Americano, pois no auge da guerra fria, os cientistas procuravam uma rede que permanecesse conectada, mesmo após um bombardeio. Utilizava uma conexão ponto-a-ponto e passou a interligar a universidade da Califórnia, la Santa Bárbara, instituto de pesquisa Stanford e Universidades.

O crescimento da Internet na década de 70 atraiu pesquisadores e estudiosos que receberam o projeto e colaboraram intensivamente nas definições técnicas do projeto, tendo como principal resultado o conjunto de protocolos Transfer Control Protocol / Internet Protocol - TCP/IP para Internet, que permite regular a comunicação em linguagem de comunicação, (Gasparini, 1999).

No início da década de 80 a Universidade da Califórnia de Berkeley, implementou o protocolo TCP/IP no Unix, possibilitando a interconexão de várias universidades àrede da ARPANET, (Derfler, 1995).

Em 1985, criou-se a rede National Science Fundation - NFSNET, na qual interligava a rede NFS com seus centros de pesquisa. No ano seguinte o conjunto de todos da NFS e ARPANET estavam conectados a esses dois Backbones.

No ano de 1987, a NSFNET passou a ser mantida pela IBM, MCI e MERIT (Instituições educacionais), criando a Advanced Network and Services - ANS.

Em 1990, foi criado o Backbone Defense Research Internet - DRI, desativando o backbone da ARPANET. A partir de 1992, com o surgimento de vários provedores, centenas de milhares de pessoas começaram a colocar informações na rede, tornando-a uma grande mania, (Leiner, 2000).

A exploração comercial no Brasil foi liberada em 1995, o número de usuários no país segundo o comitê Gestor da Internet, está estimado em superior a 3 milhões e mais de 83 milhões, nos Estados Unidos, (RNP1,1995).

### 2.1.2 WORLD WIDE WEB (WWW)

Concebida como linguagem para interligar computadores dentre dos laboratórios e instituições de pesquisa, proporcionando a exibição de documentos científicos de forma simples e fácil, foi criada por Tim Bernners-Lee em 1991 no laboratório CERN (Suíça).

Segundo Tim Bernners-Lee: “A revolução da WEB dependia de uma outra revolução: a da própria Internet”.

Com a criação do programa Mosaic, que permitiu o acesso a Web em um ambiente gráfico tipo windows, em 1993 já era comum nas universidades americanas, que estudantes fizessem suas páginas pessoais.

Na WWW os textos e imagens são interligados por palavras chaves, tornando a navegação simples e agradável. A chave do sucesso é o hipertexto, (Wall, 1996).

A base da WWW é a hipermídia, isto é, uma maneira de conectar mídias como texto, sons, vídeos e imagens gráficas. Através destas conexões hipermídia, você pode navegar pelos assuntos de seu interesse.

Após a entrada de duas gigantes da informática como Microsoft e a Netscape, cada uma com o seu Browser, que evoluíram as tecnologias de apresentação de imagens, dados, sons e multimídia; aumentou-se o interesse por parte dos usuários ao uso da Internet, pela facilidade com que disponibilizava o conteúdo na Internet, (Eager, 1995).

A informação é fornecida através de páginas que possuem ligações com outras (Hiperlinks), o link (alvo) pode ser serviço FTP, imagens, textos, dentre

outros. Para que isso ocorra é necessário que se utilize um Browser (Navegador).

Para que se precise acessar à rede mundial é necessário apenas uma linha telefônica, um modem e um provedor de acesso. A Web faz pela Internet a mesma coisa que o sistema operacional faz pelo computador pessoal (a interação), (Shaffer, 1987).

### 2.1.3 Componentes (Serviços)

Os serviços são disponibilizados na rede de acordo com a necessidade da organização. Mcfedries (1996) examina que: “alguns serviços são disponíveis para que o usuário possa usar para interagir com as diversas partes da Internet”. A seguir são relacionados alguns desses serviços:

- **Correio Eletrônico (E-mail)**

Sistema de transmissão de documentos e mensagens entre pessoas através do uso de computadores.

Este serviço será abordado no tópico 2.3 deste capítulo.

- **FTP (*File Transfer Protocol*)**

Protocolo de Transferência de Arquivos. Ferramenta que permite transferir arquivos e programas de uma máquina para outra remotamente através da Internet. Também é utilizado para designar o programa que realiza a transferência dos arquivos.

- **FAQ’s (*Frequently Asked Questions)***

Lista de perguntas mais freqüentes, realizadas por usuário sobre dúvidas encontradas em sites, grupos de discussões, sistemas etc...

- **WWW**

Literalmente, teia de alcance mundial. A base da WWW é a hipermídia, isto é, uma maneira de conectar mídias como texto, sons, vídeos e imagens gráficas. Através destas conexões hipermídia, você pode navegar pelos assuntos de seu interesse.

Este assunto foi abordado com detalhes no tópico 2.1.2 deste capítulo.

- **Browser**

Programa utilizado para visualizar as páginas da WWW. Muitos deles já são bem populares, em especial o *Netscape Navegator*. Há ainda o *IBM Mosaic*, o *Microsoft Explorer*, o *Hotjava* etc. Neles estão os comandos e as ferramentas que auxiliarão a acessar os sites da rede e a guardá-los para uso futuro.

- **CHAT**

São programas que permitem a conversa e troca de arquivos entre pessoas de todas as partes do mundo em tempo real, sem precisar de equipamentos adicionais aos que você já usa para acessar à Internet. Depois é chamar o programa, escolher a sala e conversar. Estes arquivos podem ser fotos, documentos etc.

- **Fórum**

Mecanismo de comunicação no qual "as pessoas vão até a informação", ou seja, existe no provedor um repositório de “temas em discussão”. Cada tema tem uma “linha de discussão”, com a seqüência das questões, opiniões, réplicas e argumentações. O participante consulta o índice de assuntos,

acompanha a linha da discussão escolhida, acessa as mensagens anteriores e pode responder a qualquer uma, contribuindo assim, para a linha da discussão.

No Fórum, as mensagens residem em um ou mais provedores que hospedam a discussão. Na Lista, as mensagens simplesmente "passam" pelos provedores residindo nas máquinas dos remetentes e destinatários.

- **TELNET**

Permite login remote, tornando, possível um microcomputador atuar como terminal de computadores de qualquer parte do mundo. O Telnet atua no modo texto e permite usar um computador, que está longe, como se o seu próprio micro.

### 2.1.4 Internet no Brasil

Surgiu a partir de uma iniciativa das comunidades acadêmicas FAPESP, UFRJ em 1988. Não podendo de deixar de seguir o exemplo da criação da própria Internet que em seu início teve o grande apoio das comunidades acadêmicas para seu crescimento.

Em 1989, foi criado a Rede Nacional de Pesquisas - RNP, no qual tinha como atribuição iniciar e coordenar a disponibilização de serviços de acesso à Internet no Brasil como vimos no tópico anterior; neste mesmo momento foi criado o Backbone RNP (Espinha Dorsal) interligando inicialmente as Instituições educacionais, com uma velocidade inicial de 64 kbps.

No final do ano de 1994, devido à grande divulgação na mídia sobre a Internet e a venda de serviços de Internet por parte de grupos que acessavam as redes acadêmicas. A Embratel lançou a Internet comercial no Brasil, sendo

inclusive o primeiro Provedor de Serviços de Internet. Inicialmente com acesso à Internet através de linhas dedicadas e posteriormente através de acessos dedicadas via Rede Nacional de Pacotes em linhas E1, (Cyclades do Brasil,1996).

Devido à grande demanda foi realizada a ampliação do BACKBONE RNP no tangente à velocidade e número de POP's ( *Point of Presence*) objetivando suportar o tráfego comercial de futuras redes conectadas a esses POP's (Internet/BR).

A 1ª etapa do Backbone da Internet/BR foi concluída em dezembro de 1995; e é importante ressaltar que em 1996 algumas empresas também inauguravam seus BACKBONES próprios (IBM, Unisys etc.) .

As privatizações das Teles e Embratel em 1998, trouxeram grandes expectativas aos provedores de acesso e aos usuários, oferecendo, outrossim, melhorias dos serviços tanto em níveis de velocidades quanto ao surgimento/disponibilização de novas tecnologias, como por exemplo, a *Assíncrona Delair Services Layer* - ADSL, (Charlab, 1995).

A RNP é responsável pela administração do Backbone Internet/BR, através de centros de operações como, por exemplo, a FAPESP (Responsável pela distribuição de Nomes de Domínios).

É importante ressaltar que no Brasil existe o Comitê Gestor de Internet (criado em junho de 1995), sendo a instância máxima consultiva e tem como objetivo a coordenação da implementação do Acesso à Internet, composto pelo Ministério das Comunicações e da Ciência e Tecnologia e representantes de instituições comerciais e acadêmicas.

Ainda ligado a RNP existe o Centro de Informações da Internet/BR que tem como principal atribuição coletar e disponibilizar informações e produtos de domínio Público; a fim de auxiliar a implantação e conexão à Internet de rede local, (RNP2, 1995).

### 2.1.5 Internet nas Empresas

O crescimento dos setores produtivos tem levado a uma demanda crescente pela utilização da Internet nas organizações. Tal fato ajuda para o surgimento de novos serviços para públicos bastante específicos, contribuindo também para o surgimento da necessidade de novos profissionais qualificados para operacionalizar tal tecnologia. Têm-se como exemplos claros: solicitação de estoque On-Line diretamente com o fornecedor através de uma Internet e/ou Extranet, Sites oferecendo serviços on-line como venda de livros, CD's, acessórios, dentre outros (Zeff, 2000).

Basicamente os serviços mais utilizados nestas organizações são:

- INTRANET

As intranet's são conhecidas como servidores internos de WEB, oferecem uma revolução na comunicação interna da empresa, permitindo o compartilhamento de dispositivos como arquivos e impressoras; possibilitando, outrossim, a troca de mensagem através de correio eletrônico.

A infraestrutura básica para se montar uma intranet é uma estrutura de Rede, os servidores de Web e os clientes e seus browser's (fatores estes já disponíveis na maioria das organizações).

A intranet pode funcionar isoladamente em uma rede ou via Internet, facilitando inclusive o acesso à su as bases de dados de qualquer parte do mundo de clientes ou funcionários.

A seguir são listados alguns motivos que podem levar uma organização a implementar uma intranet (Almeida, 2000):

- Disponibilização de aplicações – a organização tem seus aplicativos e base de dados disponíveis em uma plataforma homogênea; substituindo inclusive os sistemas de informações para executivos.
- Acesso fácil via software's a preços baixos; inclusive dependendo da Plataforma pode ter disponíveis aplicações com licenças gratuitas (como por exemplo, o LINUX);
- Apenas pessoas autorizadas podem ter acesso às informações das organizações;
- Baixo custo em treinamento de usuários, não é necessário gastar com aplicações clientes sendo que já se tem um browser que a ferramenta de Front-End;
- É um canal de comunicação entre clientes e empresas – a partir desse canal à organização pode obter um feedback de seus clientes (sobre como os clientes estão recebendo os seus serviços, sugestões e críticas);
- Baixo custo com divulgação e comercialização de produtos e serviços.

A intranet oferece diversas vantagens dentro da organização, como pode-se ver a seguir:

- Economia: todos os formulários, brochuras, relatórios, gráficos e planfetos, ou qualquer tipos de papel que circulam na organização podem ser armazenados na intranet, reduzindo custos nos preenchimentos de papéis.
- Banco de Dados: disponibilização de todos os dados da empresa via web, proporcionando agilidade na localização de informações, economizando tempo, agilizando os processos e aumentando a qualidade dos serviços oferecidos.
- Agilidade nos diversos processos através de e-mail, enviando mensagens a vários destinatários com facilidade e economia de tempo e dinheiro. O papel do correio eletrônico nas organizações vem substituindo o papel na comunicação interpessoal.

- EXTRANET

A extranet surgiu como uma ferramenta de apoio à gestão empresarial. A Extranet significa a interligação de intranets corporativas para troca de informações e a realização de transações com clientes e fornecedores via Internet.

A extranet pode tornar mais ágil e eficiente a relação com seus parceiros comerciais, permitindo, por exemplo: melhorar o atendimento ao consumidor, home banking; assim como novos produtos e serviços.

Ela permite a integração de todo o ciclo de planejamento, produção e controle de uma empresa; abrangendo desde o fornecedor da matéria prima até o fabricante do produto final ao consumidor (Pfafferderber, 1998).

No Brasil, o setor financeiro é, o primeiro grande mercado para a implementação de extranet. Como pode-se destacar Home Banking do Banco do Brasil, Banco Real, Bradesco, Itaú, dentre outros.

Outro setor da economia que está de olho para a implementação de extranets é o de serviços.

Apesar das facilidades e das possibilidades oferecidas por esse novo tipo de conceito de rede, as barreiras para sua ampla disseminação no mercado ainda são grandes, pode-se destacar: àexpansão da Internet e a segurança.

É necessário que as organizações tenham maior contato com a Internet para poder entender melhor o que é uma intranet e operá-la melhor, oferecendo melhor os seus produtos e/ou serviços. Estar por dentro das novas tecnologias que estão surgindo, facilitando assim, uma melhor agilidade nos processos organizacionais em um ambiente WEB (Pfaffenderber, 1998).

A segurança é um fator primordial a ser analisada pelas organizações, pois, essas transações comerciais podem trazer riscos. Embora os sistemas de proteção estejam cada vez mais sofisticados, as empresas de modo geral ainda têm receios de ligar as suas bases de dados àInternet (Oppiger, 2000).

- MARKETING

As organizações brasileiras utilizam a Web para divulgação dos dados institucionais: o que é, o que faz, catálogo de produtos, serviços e telefones para contatos.

Porém, a organização pode agir mais agressivamente na WEB, tomando algumas precauções (Cronin, 2000):

- Integre seu negócio principal em sua home page (disponibilize seu negócio on-line);

• Ofereça interatividade: a Internet permite receber informações de cada um de seus clientes. Essa possibilidade não deve ser desperdiçada em páginas mortas, que só oferecem leitura;

• Responda as dúvidas e mantenha uma seção de correspondência pela rede (FAQ's);

• Disponibilize o catálogo de produtos, oferecendo opção de compra pela rede e entrega em domicílio e a mantenha sempre atualizada;

• Divulgue sua home page em sites de outras empresas que tenham seus web Sites muitos visitados, como por exemplo, sites de pesquisas;

• Procure conhecer os sites da concorrência. Um Web site com qualidade inferior ao do seu concorrente, em termos de visual e interatividade, tem um péssimo efeito sobre a imagem da empresa;

• O site deve oferecer informações úteis, programas ou imagens para download, oferecer brindes para atrair as pessoas a visitá-lo;

Seguindo tais dicas, é possível manter-se mais instável na rede frente aos seus concorrentes que com certeza estará sondando seus pontos fracos, objetivando ganhar os seus clientes.

- CORREIO ELETRÔNICO

É o serviço pioneiro da Internet. Dentro da organização representa uma grande economia principalmente no tocante em gastos com correio convencional, além do acúmulo de papéis arquivados na organização.

O e-mail é a combinação do telefone ou da conversa cara-a-cara com a cortesia da palavra escrita.

Esse tópico e suas características serão abordadas no item 2.3 e 2.4 deste capítulo.

Dentre dos fatores observados concluí-se que a Internet proporciona algumas vantagens a seus usuários (Hawkins,1995):

- Interatividade: o usuário pode escolher a forma de como navegar em busca de informações.
- Produtividade: a hipótese de troca de informações entre os usuários aumenta a produtividade.
- Atualidade: os documentos estão permanentemente em construção e atualização.
- Economia: pode-se acessar uma informação de qualquer parte do mundo sem precisar sair de casa e com custo baixíssimo.
- Globalização: podemos acessar uma grande quantidade de informações infinitas e fazer negócios. De qualquer parte do mundo, conhecendo seus costumes, culturas, pensamentos, dentre outros.

Atualmente, encontram-se muitas empresas virtuais na qual faz-se refletir sobre a “Perda do Contato Social”**,** e também, temos restrições ao acesso devido ao custo (equipamentos, linha telefônica, tarifas...).

### 2.1.6 A Internet 2

A Internet 2 tem como missão promover a entrada de novas tecnologias como, ensino a distância, e tratamento de casos de saúde emergenciais à distância com características de gerenciamento e planejamento necessárias

para obter-se qualidade de serviços, e tem como principais objetivos (Tema nº 146, 2000):

- Habilitar uma nova geração de aplicações;
- Recriar a liderança em redes;
- Transferir a capacitação para a Internet Global.

Segundo Itri (1999) “a arquitetura da Internet2 foi escolhida para demonstrar a efetividade de novas tecnologias. O sucesso dela permitirá ao ensino superior e instituições de ensino superior a permanecerem lideres mundiais no desenvolvimento de aplicações avançadas em tecnologia da informação”.

A Internet2 representa um salto quantitativo e será a continuidade natural da evolução tecnológica atual, levando-nos a um novo patamar de softwares, aplicações, padrões e infra-estrutura de comunicações (Itri, 1999).

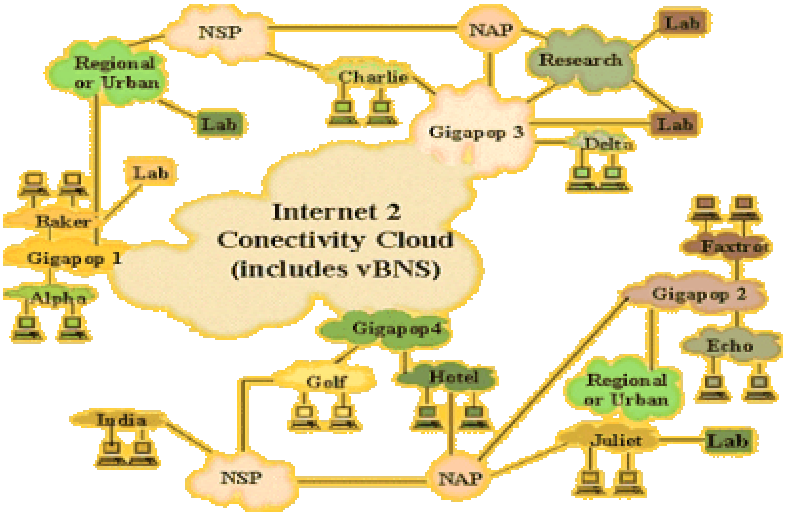
Surgiu em outubro de 1996, com a parceria de 34 universidades americanas formando o Comitê Geral de Trabalho da Internet2. Além do desenvolvimento de novas pesquisas para as áreas acadêmicas, têm o propósito de transferência de tecnologia para o setor comercial, dentre destacamos (RNP, 2000):

- Bibliotecas Digitais – com capacidade de reprodução de imagens de áudio e vídeo de alta fidelidade;;
- Ambientes colaborativos que englobam laboratórios virtuais com instrumentação remota;
- Novas formas de trabalho em grupo, com desenvolvimento de tecnologias de presença virtual e colaboração em 3D;
- Telemedicina, incluindo diagnóstico e monitoração remota de pacientes;

- Projeção de telas de computadores em três dimensões, através da utilização de WEBTV;
- Controle remoto de microscópios eletrônicos para pesquisas médicas.

A arquitetura física (figura 2.1) da rede eletrônica que dá suporte ao Internet2 inclui a implantação de GigaPOPs (pontos de presença com velocidade de tráfego da ordem de Gigabits), que tem como principal função o gerenciamento da troca do tráfego Internet2 de acordo com especificações de velocidade e qualidade de serviços previamente estabelecidos através da rede.

**Figura 2.1: Estrutura Internet 2**




Fonte : http://www.rnp.br

Os principais backbones da Internet2 são o Abilene (University Corporation for Advanced Internet Development - UCAID); e a National Science Foundation - VBNS.

A participação de instituições estrangeiras na Internet2 é estabelecida através de "Memorandos de Entendimento". Em geral, as instituições interessadas são organizações comprometidas em atingir metas similares às

do Projeto I2 em seus respectivos países, além de universidades, centros de pesquisa e instituições sem fins lucrativos (MOU,2000).

Todas as instituições de ensino superior dos Estados Unidos da América podem participar, como membros, do consórcio Internet2. As instituições que não se enquadram neste grupo deverão submeter sua aprovação ao Comitê Geral do Internet2, que poderá ou não aprovar a participação. A RNP (2000), define que os membros da I2 estão divididos em 4 categorias:

1. Universidades

2. Empresas Parceiras (*Instituições que doaram US$ 1 milhão ou mais*)

3. Empresas Patrocinadoras.

4. Membros afiliados

Itri (1999), destaca que a Internet 2 propicia o surgimento de novas tecnologias:

**GigaPops** : Estruturas responsáveis pela comutação e gerenciamento de tráfego entre redes de uma mesma região.

**Protocolos:** implementação do IPv6, aumentando a segurança e a qualidade sobre o serviço (QoS) .

**QoS** : *Quality of Service* – o usuário poderá especificar a qualidade do serviço que deseja obter.

Em 1997 o Brasil e suas instituições de ensino superior e centros de pesquisa foram incluídos no acordo de cooperação em tecnologias para a educação. Dois anos após, o Brasil foi firmado como parceiro do projeto Internet 2 através do acordo Memorandum of Understanding - MoU, assinado entre RNP e a UCAD .

Inicialmente, o backbone RNP2 permitirá a interconexão nacional das Remav's existentes com enlaces de até 155 Mbps de velocidade. Essa infra-estrutura atenderá a demanda por serviços de rede diferenciados e velocidades de conexão compatíveis com as aplicações avançadas que estão em desenvolvimento (Tema nº 146, 2000).

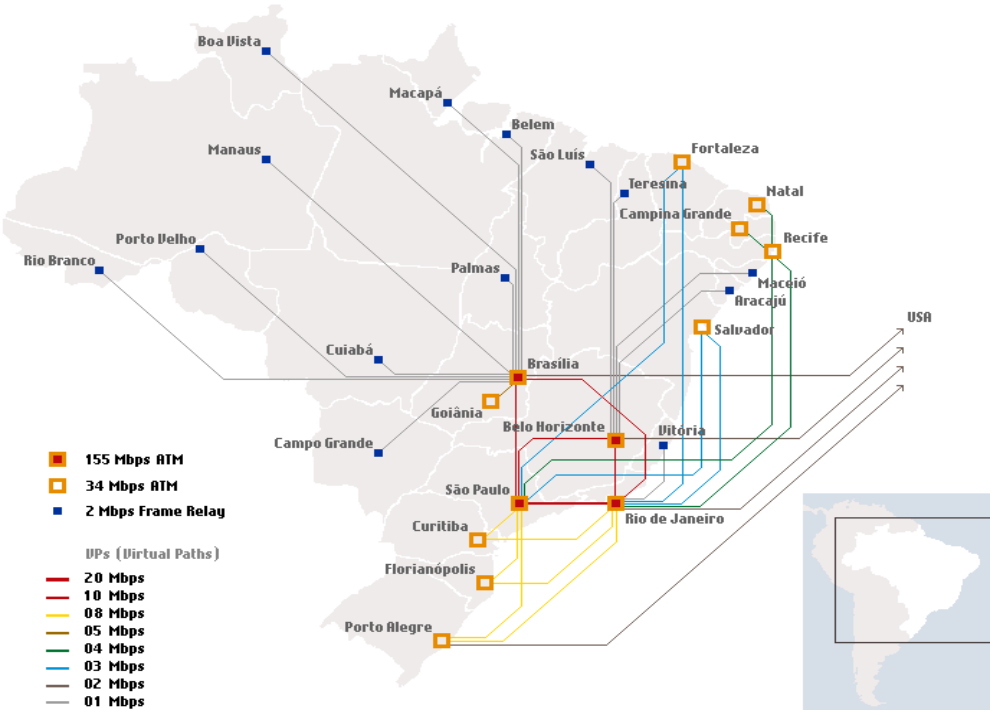
O backbone RNP2 (figura 2.2) foi projetado para atender a requisitos técnicos de aplicações avançadas e começou a ser implementado em julho/2000. Os Pontos de Presença que concentram maior fluxo de tráfego de dados utilizam conexões com tecnologia ATM. Atualmente, quatro conexões internacionais de 2 Mbps e 23 Pontos de Presença instalados nas principais cidades e capitais do país interligando todas as ReMAVs, Instituições Federais de Ensino Superior (IFES), além de novas conexões internacionais e em fim será conectada àrede norte -americana Internet2 (RNP, 2000).

**PoPs já conectados:**

ATM - RJ, SP, DF, MG, PR, SC, RS, PE, CE, RN, BA, GO, PB, FR - AL, AC, AM, MS, SE, RO, MT, ES, PI, PA, TO

Demonstrações dos novos potenciais do Internet2 vêm sendo apresentadas em vários eventos e workshops promovidos com o intuito de sensibilizar não só a comunidade acadêmica, como também diversos setores da indústria e até mesmo o governo.

**Figura 2.2: Backbone RNP 2**




Fonte: http://www.Internet2.edu/international/

## 2.2 Mensagem Eletrônica

É a informação gerada, enviada, recebida ou arquivada eletronicamente, por meio óptico ou por similares incluindo, mas não se limitando a: Eletronic data interchange - EDI, correio eletrônico, telegrama, telex e fax; (Carvalho, 1997).

Cada mensagem consiste de dois componentes: cabeçalho e conteúdo. O **cabeçalho da mensagem** (*header*) contém informação de controle que identifica a mensagem: de onde ela veio (remetente), para onde vai (destinatário), quando foi enviada e o assunto (*subject*). O **conteúdo** é o corpo

da mensagem, é a correspondência propriamente dita que alguém recebeu ou está preparando para enviar.

**Endereçamento**

Quando envia-se uma carta pelo correio, coloca-se no envelope o endereço do remetente e o do destinatário. Esta informação de controle constitui um "padrão de endereçamento" comum a todos os envolvidos (remetente, destinatário e correio) no tratamento da correspondência (Sadler, 1996).

Ao endereçar uma mensagem, é importante observar-se o uso de letras maiúsculas e minúsculas. Normalmente, as mensagens devem ser enviadas em letras minúsculas.

Sadler (1996), diz que "é importante atentar-se a não cometer um erro muito comum entre os usuários ao endereçar uma mensagem", ou seja, a digitação incorreta do nome do usuário do destinatário. Para se resolver é aconselhável que o usuário adquira o hábito de verificar duas vezes a linha do endereço (*address*) antes de enviar a mensagem.

Pode-se exemplificar como seria o cabeçalho da mensagem para um usuário (jocenio. epaminondas). Então, Primeiro a mensagem do usuário tem que chegar ao computador do Diretor (empresa. com.br*)* e, depois, tem que chegar a ele (jocenio.epaminondas).

A forma de endereçar uma mensagem na Internet é apresentada no quadro 2.1:

**Quadro 2.1: Endereçamento da Mensagem**

| | |
|---|---|
| **From**: | *Jocenio.epaminondas@mestradouneb.ufsc.br* |
| **To**: | *usuario@local.do.destinatario* |
| **Subject** | *Defesa de Tese de Mestrado* |

Onde *usuário* é a identificação com a qual a pessoa está cadastrada e *local* é o computador através do qual ela está ligada à Internet. Em nosso exemplo o usuário poderia ser: oriente@*led.ufsc.br* .

A seguir ver-se-a como ficaria a mensagem. Incluir-se-á também os campos opcionais Cc e Bcc, que têm como função remeter uma cópia da mensagem para outro(s) usuário(s). A diferença entre eles (Quadro 2.2) é que CC significa com cópia e BCC *cópia oculta*, conforme explicação a seguir:

- o endereço em CC (*Carbon Copy*) aparece no cabeçalho recebido por todos os destinatários da mensagem (cópia em aberto**).**
- O endereço em BCC (*Blind Carbon Copy*) não aparece no cabeçalho das mensagens dos demais destinatários (no exemplo abaixo, apenas Beltrano sabe que recebeu cópia da mensagem, os demais pensam que apenas José Silva e Fulano receberam a mensagem),

**Quadro 2.2: Corpo da mensagem**

| | |
|---|---|
| **From**: | *Jocenio.epaminondas@mestradouneb.ufsc.br* |
| **To**: | oriente@*led.ufsc.br* |
| **Subject**: | Defesa de tese de Mestrado |
| **Cc**: | *ludimila@uneb.com.br* |
| **Bcc**: | *epaminondas@uneb.com.br* |
| **Mensagem**: | Prezados Senhores;<br>Comunico que a data de defesa de minha tese... |

### 2.2.1 Como Ler ou Compor uma Mensagem

Existem vários programas que podem ser usados para essa finalidade, que fornecem uma série de recursos aos seus usuários, como a possibilidade de se trabalhar com folders (pastas) para organização de suas mensagens.

É possível se organizar, toda a sua árvore criando pastas de acordo com o interesse. Facilitando assim, o armazenamento de todas as mensagens enviadas/recebidas por determinados departamentos ou setores. Seria a sua garantia de defesa. É aconselhável que guarde sempre uma cópia de seus arquivos, gravando uma cópia do arquivo de sua estrutura de correio. Tem-se como exemplo os arquivos com extensão *.PST (utilizado pelos sistemas EXCHANGE).

- O uso de addressbook (agenda de endereços)

Contém uma lista de todos os usuários do sistema. Os sistemas de correio eletrônico oferecem diversos critérios para o usuário configurar sua lista. Entre eles pode-se citar o nome do usuário, a localização da empresa, o número do telefone, dentre outros.

- Criação de lista de endereços

Diariamente, recebe-se também, emails de outros usuários que não fazem parte da agenda de endereços da organização e enviar correspondência para determinados grupos de trabalhos com atribuições específicas. Pode-se criar listas de endereços e enviar mensagens exclusivamente para aqueles grupos desejados. Digitando apenas o nome da lista que você criou no qual está incluso o endereço dos componentes envolvidos no processo. Exemplo: trab_normas.

Entre esses programas encontram-se o Netscape, Eudora, Elm, Mail, o Exchange, Outlook, Pegasus Mail, dentre outros; (Mcfedries, 1996).

## 2.3 Correio Eletrônico

### 2.3.1 Visão Geral

O correio eletrônico foi a primeira aplicação surgida na Internet, com o objetivo de facilitar a comunicação e a troca de idéias e observações entre o grupo de acadêmicos que estava construindo e experimentando a Internet. Os documentos mais antigos da comunidade eram distribuídos via correio tradicional, conseqüentemente, pouco ágil e apresentavam conjuntos de idéias desenvolvidas por pesquisadores de um determinado lugar para o resto da comunidade. Depois que o e-mail ou correio eletrônico começou a ser utilizado, a velocidade da comunicação o padrão de autoria dos trabalhos mudou. Os documentos passaram a ser apresentados por co-autores com uma visão comum, independentemente de suas localizações. E a capacidade e a velocidade de envio da comunicação e da resposta à comunicação aumentaram exponencialmente (De Moraes, 1997).

Então, pode-se concluir que: correio eletrônico é um sistema eletrônico semelhante ao serviço de correios que conhece-se (é necessário que a cidade/País tenha uma agência de correio) e que serve para enviar e receber dados eletrônicos (a cidade precisa estar conectada a uma rede de computadores, linha telefônica ou Linha dedicada). Utiliza-se uma caixa postal eletrônica simbolizada por um endereço eletrônico com nomenclatura vista no tópico do tipo “seunome@nomedoseuprovedor.com.br”. Todas as mensagens enviadas ficam armazenadas nos servidores de e-mail do seu provedor (Institucional ou Governamental) até a hora em que você acesse a Internet

(você precisa estar conectado à Internet para receber seus e-mails) e dê o comando para recebê-las, baixando-as para o seu microcomputador pessoal (USP, 2000).

É um dos recursos mais antigos utilizados pelos usuários da Internet. Através do correio eletrônico pode-se enviar textos, gráficos e arquivos multimídia.

A troca de mensagens é realizada através do protocolo SMTP (Protocolo de Transporte de Simples Postagem) é o protocolo para o envio de mensagens "e-mail", que especifica o conteúdo e o formato de tais mensagens, bem como a seqüência correta das mensagens trocadas.

O SMTP é conhecido como o "servidor de mensagens de saída", ou seja, cuida das mensagens enviadas por uma estação cliente conectada ao servidor (Gasparini, 1999).

As informações de gerenciamento são armazenadas em uma base de dados chamadas Management Information Base - MIS, que contém informações de hosts e Gateways, interfases de redes, tradução de endereços e softwares relacionados ao Internet Protocol - IP, Internet Control Message Protocol - ICMP, Transmission Control Protocol - TCP, User Datagram Protocol - UDP e Exterior Gateways Protocol - EGP, (Sadler, 1996).

### 2.3.2 Funcionamento do Correio Eletrônico

Carvalho (1997) diz que: "O funcionamento do correio eletrônico é baseado no paradigma "*store-and-forward*" (armazenar e enviar)", ou seja, os usuários envolvidos na transferência de uma mensagem não interagem diretamente

entre si, e sim com programas servidores encarregados de executar e gerenciar essa transferência.

Abaixo são relacionados os principais componentes/serviços de um sistema de correio (Cyclades do Brasil, 1996):

- ***User Agent - UA***

Programa cliente que interage com o usuário, este é responsável pela obtenção de mensagens a ser transmitidas e de mensagens recebidas, (PC-EUDORA).

- ***Mail Tranport Agent - MTA***

Programa responsável pelo transporte de mensagem entre pontos envolvidos, locais ou através da Internet (sendmail do UNIX).

- ***Mail Boxes***

Caixas postais onde são armazenadas ou recebidas mensagens.

- ***Mail Box Manager***

Programa responsável pelo gerenciamento das caixas postais, necessários especialmente quando os programas UA e MTA não residem no mesmo equipamento (um programa POP Server).

- ***Listas de Discussão***

Baseado na associação a uma lista de usuários, de forma que uma correspondência enviada a esse endereço seja recebida por todos. Essa lista de discussão pode ser uma lista, moderada ou fechada.

- ***Serviços de Informação via Correio Eletrônico***

Fornecidos por programas que interagem com os usuários através de correspondência direcionada a um dado endereço de correio eletrônico,

normalmente constituída por comandos e palavras chaves que orientam tais programas a transferir as informações solicitadas.

O correio eletrônico trabalha com o princípio de cliente-servidor, ou seja, programa cliente que habilite um usuário a interagir com um servidor, acessando informações e serviços neste computador (servidor). A aplicação cliente é a que permite o usuário ler este e-mail, responder, redirecionar, compor e enviar novas mensagens, (Tanembaum, 1994).

A aplicação básica do correio eletrônico é a "comunicação" entre duas ou mais pessoas. Esta comunicação pode ser de caráter pessoal (entre familiares e amigos) e de caráter profissional (entre funcionários da mesma empresa, parceiros de empresas distintas, clientes e fornecedores ou prestadores de serviços, profissionais e empresa etc). Abaixo, Mcfedries (1996) cita algumas grandes vantagens deste serviço:

- É rápido: toma segundos ou minutos para chegar até à caixa postal do destinatário, em qualquer parte do mundo;
- É barato: não se paga por e-mail enviado ou recebido, mas apenas uma mensalidade ao seu provedor.
- É escrito: facilita o acompanhamento de solicitações;
- Permite o envio de mensagens para muitas pessoas ao mesmo tempo;
- Permite respostas a e-mails recebidos;
- Permite encaminhamentos de e-mails recebidos a terceiros;
- Permite o envio de arquivos de dados anexados: imagine que beleza poder receber um arquivo integral em seu formato original para trabalho ou consulta.

- Muito cômodo - já que as mensagens são recebidas na caixa postal particular do destinatário e lá ficam àespera que ele (a) as acesse;
- É universal, pois milhões de pessoas utilizam correio eletrônico na Internet, assim como qualquer sistema de correio eletrônico pode ler sua mensagem (São homogêneos).
- É menos evasivo – causa um nível mínimo de interrupção nas atividades que estão sendo realizadas pelos destinatários. Ao contrário do telefone, o correio eletrônico quase não interrompe o destinatário;
- Disponibilidade – "o correio eletrônico não dá ocupado", não precisamos nos preocupar se o destinatário de nossa mensagem está ou não disponível naquele momento (ao contrário do telefone).

## 2.4 Infraestrutura de Correio Eletrônico

Este tópico tem como principal meta oferecer informações sobre o ambiente de correio eletrônico, a arquitetura em que está rodando, as ferramentas de correio utilizadas, software, pessoal técnico envolvido no projeto e uma visão geral sobre custos envolvidos.

### 2.4.1 Plataforma Cliente-Servidor

Os sistemas de correio eletrônicos utilizam como arquitetura básica à de Cliente-Servidor, em que há módulos de programa distintos para, de um lado, receber e executar os pedidos de informação (o módulo servidor) e, do outro lado, para capturar os pedidos do usuário e apresentar os resultados da execução desses pedidos (o módulo cliente). Portanto, para usá-las, é

necessário instalar um módulo cliente compatível com o equipamento do usuário, (Soares, 1995).

Nesta plataforma o cliente faz solicitações ao servidor e este após analisa-las as executa de acordo com suas prioridades.

As principais vantagens dessa arquitetura são:

- Como somente o servidor acessa o sistema de arquivos, o nível de segurança oferecido é muito mais alto;
- O Tráfego na rede é inferior devido à divisão do processamento das tarefas entre cliente e servidor e a comunicação é efetuada em cima do protocolo RPC (remote procedure Call) que reduz significamente o tráfego na maioria das vezes;
- Utiliza-se de facilidades de servidores Cliente-Servidor como as implementações de Rollback (volta atrás e não efetua a operação) e Corriet (regista a operação efetuada), que diminuem o fluxo de perda de dados no caso de alguma falha no servidor, ou no cliente;

Como fator relevante deve-se considerar algumas desvantagens:

- A necessidade de máquina com grande poder de processamento, muito espaço em disco disponível e abundância de Memória RAM;
- Aumento da quantidade de tempo dedicada ao gerenciamento do sistema, por possuir um nível de complexidade bem superior.

### 2.4.2 Ferramentas

Com o crescimento das redes de computadores e o aumento das informações armazenadas, foi necessário ao longo do tempo desenvolver

novas formas para facilitar o acesso e a localização das informações disponíveis ”Ferramentas”. O propósito destas, é possibilitar a visita a computadores de todo o mundo, adquirindo assim, as informações disponíveis (Torres, 2001).

**WAIS (Wide Area Information Server)**

É um sistema de informações distribuídas que possibilita ao usuário buscar e recuperar documentos armazenados em bases de dados disponíveis na rede e podem conter tanto textos como figuras, sons ou imagens.

**Whois**

É uma ferramenta voltada para o atendimento de consultas sobre pessoas e organizações presentes na rede. As informações, armazenadas em uma base de dados, são coletadas pela InterNIC - e incluem endereço (postal e eletrônico) de pessoas e organizações usuárias da rede.

**IRC (*Internet Relay Chat*)**

É uma ferramenta que permite estabelecer uma conversação simultânea entre dois ou mais usuários da rede, as discussões através de IRC fazem uso do conceito de canal (trilha de conversação), podendo ser públicas ou privadas quanto àparticipação de novos membros.

**Finger**

Esta ferramenta permite verificar se outros usuários da rede estão usando seus computadores no momento. É mais utilizada quando o computador é do tipo que aceita grande número de usuários (*mainframe*).

Computadores pessoais também podem responder a consultas feitas com *finger*, desde que o seu dono instale o programa apropriado.

### 2.4.3 Softwares

A escolha de softwares para sua rede local de correio eletrônico dever ser cuidadosamente adequada às necessidades da empresa. O avanço da funcionalidade dos softwares de correio eletrônico (licenças de calendário, planejamento, opções de personalização de mensagens, dentre outros) é constantemente atualizado por seus fornecedores: wordperfect, Microsoft, Lótus, Pegasus, etc.

Outro fator importante a ser observado, além da praticidade, é a questão de custo. Diante disso deve-se observar dois fatores principais (Sadler, 1996):

Licenças de Adicionais

É o valor que se paga a cada usuário que tenha acesso ao aplicativo de correio eletrônico baseado no servidor. Esses valores adicionais às licenças existentes geralmente estão disponíveis através de requerimentos via suporte on-line ao usuário, WWW, Fax ou serviços de FTP. Normalmente existe um equilíbrio competitivo entre os fornecedores.

**Possibilidades de UPGRADE**

É importante observar no contrato de fornecimento de Software como o fabricante de software de correio eletrônico trata a questão de *UPGrad*e de Software, quais os custos envolvidos, verificar se o fabricante cobra por cada versão atualizada do aplicativo adquirido ou se existe uma taxa adicional que inclui o custo de upgrades gratuitos no futuro.

Quando se trata de aquisição de licença de software de correio eletrônico ou qualquer outro aplicativo é aconselhado que se leve em conta à reputação

do fornecedor de quem está se adquirindo o software. Deve-se verificar se esta organização é bem estabelecida se existe um serviço de atendimento ao usuário. Pois, caso tal organização venha a falir, sua instituição estará sem suporte técnico.

Outro fator a se observar ao adquirir uma licença de software de correio eletrônico é considerar a compatibilidade do pacote com sistemas operacionais de rede e estações de trabalho que deseja ou já é utilizado na organização.

### 2.4.4 Pessoal Técnico

Para que um ambiente esteja realmente capaz de prestar bons serviços aos seus usuários é importante ter uma equipe especialista para tal.

Geralmente esta equipe é formada por: analista de suporte, administradores de rede, pessoas especialistas aptas a esclarecerem as dúvidas de usuários e configurar estações de trabalho.

A empresa deverá ter pelo menos:

- 1 (um) analista de Suporte
- 2 (dois) administradores de rede (para acompanhar as tarefas diárias de rede, que vai desde configuração/manutenção dos servidores até configurações e/ou implementações de serviços adicionais).
- 3 (três) técnicos especialistas para central de atendimento, capacitados para orientar os usuários e os técnicos de atendimento sobre dúvidas relacionadas a correio eletrônico.
- 2 (dois) técnicos de atendimento, tendo como atribuição realizar manutenção, configuração e instalação de PC’s na rede, assim como todos os

sistemas corporativos, aplicativos e inclusive instalação/configuração de novas contas de correio eletrônico corporativo.

A relação de pessoal técnico envolvido poderá ser alterada de acordo com o porte da organização.

### 2.4.5 Custos

Esta planilha de custos (quadro 2.3) foi realizada com bases no pessoal técnico envolvido e abrange também relação de equipamentos e de softwares.

**Quadro 2.3: Custo Mensal com Pessoal Técnico**

Pessoal Técnico (Mensal)

| | Quantidade | Vrl.Unitário | Vrl Total |
|---|---|---|---|
| Analista de Suporte | 01 | R$ 2.800,00 | R$ 2.800,00 |
| Administrador de Rede | 02 | R$ 2.000,00 | R$ 4.000,00 |
| Técnicos Especialistas | 03 | R$ 1.100,00 | R$ 3.300,00 |
| Técnicos de Atendimento | 02 | R$ 600,00 | R$ 1.200,00 |
| | | Subtotal=> | R$ 11.000,00 |

Equipamentos / Hardware

| | Quant. | Vrl.Unit | Vrl Total |
|---|---|---|---|
| Servidor de Rede (Hardware) | 01 | R$ 5.300,00 | R$ 5.300,00 |
| Sistema Operacional de Rede | 01 | R$ 5.068,00 | R$ 5.068,00 |
| No Break 2.0 KVA | 01 | R$ 2.000,00 | R$ 2.000,00 |
| Soft.Adm correio eletrônico(Server) | 01 | R$ 2.000,00 | R$ 2.000,00 |
| Soft. correio eletrônico ( Cliente ) | ** | *** | * |
| | | Subtotal=> | 14.368,00 |

* Já vem incluso nos pacotes de *Backoffice* da Microsoft.

Estes custos podem ser reduzidos se a organização optar por sistemas operacionais de rede abertos (Linux), que tem aplicações de gerenciamento fazendo parte do pacote.

## 2.5 Segurança da Informação

A possibilidade de funcionar em rede, assegurando a prestação de serviços de forma rápida e descentralizada, é um privilégio que a Era da Informação concede às organizações. O grau de eficiência dessas organizações depende

de sua capacidade de processar informação e de uma estrutura capaz de assimilar um modo de funcionamento mais flexível e interativo.

As transações comerciais via Internet permite o acesso direto a um mercado realmente global. Atributos como tamanho físico e uma enorme população de usuários finais tornam a Internet o maior mercado que existe. Características como velocidade intrínseca e baixo custo a tornam um dos meios mais interessantes para a realização de transformações comerciais.

Além de ser o maior mercado, a Internet é o maior provedor de informações. Os usuários podem se conectar a bibliotecas, agências, instituições, empresas, serviços de news ou a outros usuários para trocar informações. A única exigência é conhecer o endereço na Internet (http://www.ceilandiaweb.net), que pode ser facilmente obtido através dos inúmeros índices e dispositivos de pesquisa disponíveis. Na Internet, é possível ter acesso gratuito a um incrível volume de informações.

A Tecnologia da informação só se torna uma ferramenta capaz de alavancar os negócios, quando seu uso está vinculado à medidas de proteção dos dados Corporativos.

A segurança nos sistemas e redes constrói-se em torno de diversas técnicas (criptografia, controle de acesso etc.) e de políticas de utilização adequadas. No entanto, a utilização isolada, em sistemas/empresas de alguma dimensão, arrisca-se a fugir ao controle do realizador, e produzir entorses face ao efeito desejado: buracos não previstos, níveis de segurança inadequados, em excesso ou por defeito; conflitos.

Para que as empresas possam ser competitivas, é imperativo que elas possam contar com um trabalho de profissionais especializados e qualificados que saibam como alinhar segurança à tecnologia da informação (Berntein, 1997).

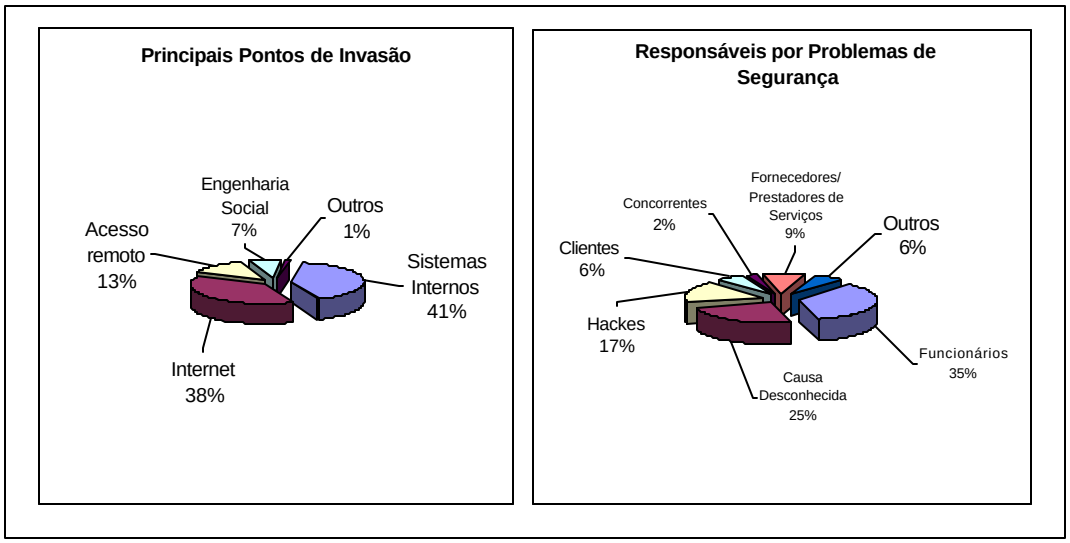
Em 1999, a Módulo Security Solutions S/A, realizou pesquisa nacional sobre Segurança da Informação. A pesquisa abrangeu 148 organizações, sendo 42% empresas privadas de capital nacional, 21% privadas de capital estrangeiro, 15% de órgãos Governamentais, 14% sociedades de economia mista e 8 % empresas estatais (Módulo Security Solutions S/A, 1999).

Dados desta pesquisa mostra que a maioria (35%) dos problemas de segurança dentro da organização são dos seus próprios funcionários, seguindo como principal ponto de invasão os sistemas corporativos (figura 2.3).

Outro fator importante é a empresa realmente prezar por suas informações, valor da informação e qual a relação direta dos sistemas de informação com o negócio final da empresa, é uma nova exigência que recai principalmente sobre os administradores de sistemas de redes.

Diariamente ouvimos notícias de ataques a sites deixando-os fora do ar por horas como, por exemplo: Yahoo, E-trade, Datatek, ZDNet, CNN, Amazon, Buy.com e E-Bay e no Brasil o UOL, o IG e o Zip.Net. Diante destes fatos é importante refletir-se sobre a fragilidade da estrutura da Internet, para poder-se garantir a maior segurança dos dados corporativos.

**Figura 2.3: Principais pontos de Invasão e Responsáveis por problemas de segurança**




Fonte: 5ª Pesquisa Nacional sobre Segurança da Informação– Módulo Security Solutions S/ A

Um fator crítico a ser avaliado é a questão de falta de legislação para punir os criminosos digitais, enquadrando-os em outros delitos como: estelionato, falsidade ideológica ou crime contra a segurança nacional, fator em que a legislação americana é muito dura: prisão de 5 a 10 anos e multa de até US$ 250 mil.

A aplicação de respostas e tecnologias adequadas ao alto índice de evolução e complexidade das ferramentas de segurança disponível é um desafio ainda maior para o profissional que administra o ambiente de tecnologia da informação. Tais soluções definidas por essa equipe demandam complexidade de segurança e previsão/análise de vulnerabilidades, devendo-se numa abordagem e visão completas, cobrir os diversos níveis de segurança exigido em cada caso, garantindo soluções com níveis de segurança sob medida e a melhor solução de custo total em um projeto de segurança.

Na medida em que as redes são conectadas, as empresas começam a sofrer ameaças em suas redes. Abaixo são listadas as categorias de ameaças mais comuns (Starling, 1999):

- **Ameaças à Rede Corporativa**: a disponibilidade de serviços da Internet pode abrir furos na segurança que permitem o acesso de intrusos a outros componentes da rede de computadores;
- **Ameaças aos Servidores da Internet:** intrusos podem entrar em um servidor de Internet; com isso, eles têm a possibilidade de ler ou até mesmo modificar arquivos armazenados no servidor.
- **Ameaças à Transmissão de Dados**: a confidencialidade e a integridade das informações podem ser violadas se alguém interceptar a comunicação com a rede da empresa (correio eletrônico, transações WEB, download de arquivos etc.);
- **Ameaças à Disponibilidade dos Serviços**: um intruso mal-intencionado poderia utilizar um ataque que interromperia a disponibilidade de sistemas, ou até mesmo da rede inteira, para seus legítimos usuários;
- **Ameaças de Repudiação**: um participante de uma transação on-line pode negar que a transação realmente tenha acontecido.

As fraquezas tecnológicas se referem a deficiências nos produtos de software e hardware e utiliza as falhas no material de comunicação. As fraquezas na política de operação se referem às regras pelas quais operam os sistemas de computador.

Implementar procedimentos de segurança sem uma Política definida é equivalente a navegar sem saber aonde se quer chegar. É imprescindível que

se levante todas as informações relevantes à segurança dos dados corporativos.

### 2.5.1 Princípios Básicos

Medidas de segurança visam a probabilidade de ocorrência de eventos causadores de dados, e minimizar os efeitos caso venha a acontecer. A ausência de uma política de segurança gera vulnerabilidade nos recursos e nas informações da organização.

Segundo Soares (1995), “A ameaça é qualquer violação de segurança de um sistema, e dá como exemplo: destruição, roubo, remoção ou perda da informação ou de outros recursos, modificação, deturpação ou revelação e interrupção de serviços”.

### 2.5.2 Agentes Envolvidos em Segurança da Informação

A seguir são descritos os agentes envolvidos em segurança da informação (Fonte, 2000):

- GESTOR DA INFORMAÇÃO: O indivíduo responsável para fazer decisões em nome da organização no que diz respeito ao uso, à identificação, àclassificação, e àproteção de um recurso específico da informação.
- CUSTODIANTE: Agente responsável pelo processamento, organização e guarda da informação.
- USUÁRIO: Alguma pessoa que interage diretamente com o sistema computadorizado. Um usuário autorizado com poderes de adicionar ou

atualizar a informação. Em alguns ambientes, o usuário pode ser o proprietário da informação.

### 2.5.3 Classificação das Informações

Segundo Gil (1994), todas as informações críticas segundo o seu grau de criticidade e teor podem ser classificados em:

- Informações confidenciais: devem ser disseminadas somente para empregados nomeados.
- Informações Corporativas: devem ser disseminadas somente dentro da empresas.
- Informações Públicas: podem ser disseminadas dentro e fora da empresa.

### 2.5.4 Trilhas de Auditoria

É importante que a organização tenha especialistas na área de segurança da informação, utilizando produtos, que ofereçam serviços com uma abrangência muito ampla, permitindo apontar problemas e brechas na segurança dos sistemas de informação (Cheswick, 1994).

O Serviço deverá verificar a segurança dos servidores, bem como de outros dispositivos IP (endereço que identifica o seu computador na Internet) à escolha dos administradores de sistema.

Tal serviço deverá dispor de módulo que permita ativar remotamente os testes de segurança da instituição, através da Internet, por chamada telefônica e modem; os especialistas de segurança poderão também efetuar os testes

nas instalações do Cliente, em conjunto com os técnicos responsáveis pela segurança da empresa.

De mãos dos dados recolhidos na auditoria de segurança, serão criados relatórios com a lista das falhas de segurança, podendo os especialistas e os responsáveis pela segurança da rede indicar prioridades por nível de risco e recomendações para a sua eliminação.

### 2.5.5 Política de Backup

É muito importante que a organização tenha segurança sobre os dados que circulam em seus servidores. A realização de backup's dos dados em fitas ou outra mídia de armazenamento removível deverá atender aos seguintes propósitos (Jennings, 1997):

- Evitar a perda irreparável de dados;
- Oferecer uma cópia offline dos dados que podem ser recuperados qualquer instante;
- Fornecer um arquivo de dados que pode ser preservado para fins históricos ou legais.
- Fornecer cópia dos dados corporativos, em servidores situados em outras localidades.
- Realização de cópia de segurança, inclusive quais os servidores que deverão ter prioridade de backup.

Toda organização deverá ter pré-definido o tipo de tecnologia e mídia a serem adotadas para se efetuar backup (cópia de segurança) é necessário hardware específico.

A cada dia que se passa os fabricantes oferecem mídia e métodos de gravação diversos. Sendo que podemos destacar: as Fitas DAT (Digital Áudio Tape), e drivers óticos:

**Fitas DAT** (Digital Áudio Tape)

Tais fitas têm capacidade de armazenamento de 1,2GB a 12GB, os sistemas de fita DAT de 4mm e 8 mm oferecem maior produtividade e confiabilidade, assim com um formato compacto e conveniente.

**Drivers Óticos**

Essa família inclui o Compact Disk –Ready only medias - CD-ROM , o Write once ready many - Worm e o Magnect optical - MO, ou seja, discos óticos que podem ser apagados, também proporcionam rapidez de acesso aos dados e um formato confiável se for implementadas corretamente.

CD-ROM - é utilizado para armazenamento de grandes bancos de dados não alteráveis, mas que sejam utilizados freqüentemente como referência.

Worm - é semelhante à tecnologia do CD -ROM, depois de gravados os dados não podem ser apagados, também não sofrem degeneração por motivos de distúrbios elétricos e magnéticos.

MO - consiste em duas tecnologias que são usadas em conjunto para propiciar um disco ótico que pode ser apagado, com o desempenho de um driver de disco rígido de ponta.

Para maior segurança das informações, as organizações podem dispor de uma “SALA COFRE” (ambiente é capaz de proteger, fisicamente, os equipamentos e materiais ali acondicionados, contra desastres, tais como: incêndio, roubo, radiações, poeira, umidade, vandalismo etc ..). possuem

câmara refratária, sistemas de proteção contra alta umidade, dotadas contra água, e também protegem o ambiente de gases corrosivos e pulsos eletromagnéticos, freqüência de rádio- agentes altamente nocivos para a informação armazenada. O acesso é restrito às pessoas autorizadas.

### 2.5.6 Política de Uso de Software

"É responsável por criar controles de utilização de softwares na organização. Softwares que não sejam homologados pela equipe de informática devem ser desinstalados imediatamente e informados aos chefes imediatos para a aplicação das sanções cabíveis:".

- **Controle Antipirataria**

Há empresas que não dão muita importância a este aspecto. Funcionários podem copiar em sua máquina programas e softwares sem licença da organização.

É importante que se tenha um controle de todos os aplicativos e/ou softwares utilizados na organização evitando com isso multas por utilização de cópias não autorizadas.

- **Definição da linha mestra dos softwares utilizados por ambiente computacional.**

Tais softwares e/ou aplicativos institucionais devem ser adquiridos ou desenvolvidos de acordo com a necessidade da organização.

É aconselhável que se faça um estudo sobre o software a ser adquirido (se é compatível com a plataforma utilizada na instituição); e um outro fator relevante é a questão custo benefício. Atualmente tem-se sistemas de

plataforma aberta (Linux) que pode baixar consideravelmente os custos com aquisição de softwares principalmente no que tange à aplicações para se rvidor de arquivos e Internet.

### 2.5.7 Conscientização dos Usuários

"O usuário á a parte mais importante de uma rede, pois é o maior utilizador. Sendo assim é também a parte mais delicada para se tratar. Grande parte dos problemas como: acesso não autorizado, alteração indevida de arquivos, roubos, dano intencional ou acidental, ocorrem por culpa de usuários mal intencionados ou desavisados. Boa parte dos problemas pode ser evitada com planos de conscientização e treinamentos".

Todos os usuários devem estar familiarizados com os procedimentos operacionais e de segurança. Para isso se faz necessário um guia claro e conciso, para explicar aos usuários sobre o funcionamento da rede e sobre os serviços por ela disponibilizados, como por exemplo, e-mail, Internet e intranet.

- Segurança Física
  - Controle de acesso físico: são usados para garantir que o acesso a um recurso somente a usuários autorizados;
  - Definição de ambientes físicos de alta criticidade: hardwares e equipamentos de conectividades responsáveis pela funcionalidade das comunicações;
  - Monitoração de ambientes: garantir que o acesso a um recurso somente a usuários autorizados. Objetiva Coletar e tabular informação; permite detecção automática da topologia e da configuração de rede, gerência por domínios.

Esses serviços de gerenciamento permitirão Backup “On-line”, Distribuição e instalação de softwares nas estações, Geração de “log”, inventário de “software” e “hardware”, geração de relatórios e gráficos estatísticos da rede.

- Segurança Lógica
  - Backup

Realização de uma cópia de segurança dos dados para evitar a perda irreparável resultante de falhas, tendo em vista a grande quantidade de informações de armazenamento de dados pelos usuários.

- Pirataria

Pode ser controlado através dos controles e auditoria através das soluções de Gerenciamento implementadas na organização.

- Vírus

A quantidade leva a organização a ter um controle mais efetivo prevenida das informações copiadas na rede local. Em se tratando de vírus na corporação é responsabilidade do usuário:

- Manter o antivírus das estações de trabalho residente em memória, após a instalação e configuração do mesmo pelo pessoal de informática;
- Todo E-mail e arquivos recebidos a partir da rede devem ser passados antivírus;
- Informar ao administrador do sistema sobre a existência de vírus, como também o comportamento do mesmo no ambiente;
- Se a estação infectada estiver conectada à rede, o usuário deve fazer a desconexão da mesma da rede corporativa;

No mesmo tocante é responsabilidade do administrador da rede:

1. Verificar e testar os novos softwares a serem instalados nos servidores corporativos para que estes não introduzam vírus na rede;

2. Verificar a presença de vírus (passar antivírus) nos servidores de arquivos da rede;

3. Manter disponível e atualizada a cópia do antivírus na rede para utilização pelos usuários;

4. Divulgar aos usuários sempre que tiver nova versão do anti-vírus;

- Intranet / Extranet

"É importante que os usuários da rede tenham consciência sobre os procedimentos de utilização da intranet / extranet. Deve-se divulgar amplamente na organização a importância das informações que circulam na rede e sobre os processos de segurança e sanções aplicadas quanto à má utilização".

Os clientes que acessam a rede privada da organização via Internet (Extranet) deve ter a mesma visão sobre utilização dos serviços oferecidos pela organização.

### 2.5.8 Plano de Contingência

"Em uma organização existem produtos finais, que utilizam recursos e serviços. Que utilizam uso de redes de computadores, computadores, programas e que são, por sua vez, suportados pela infra-estrutura básica e serviços essenciais. Para dar suporte a tais processos são criados procedimentos alternativos para a continuidade às operações vitais e integridade das informações processadas sob sua responsabilidade e em

interfaces com sistemas de terceiros. Essencialmente, deve garantir a operação do negócio em casos de catástrofes, eventualmente causado por uma possível pane nos sistemas de computadores ou em equipamentos".

Gil (1994) descreve que os objetivos de um plano de contingência são:

- Proteção de vidas;
- Estabelecer uma cadeia de comando;
- Identificar as atividades afetadas e seu grau de criticidade;
- Minimizar dados e perdas imediatas;
- Retomar as funções críticas;
- Recuperar para o estado normal;

A seguir serão citados alguns processos que não podem ser deixados de ser apreciado em um plano de contingência (Gil, 1994):

- Análise de riscos do ambiente computacional;
- Definição da criticidade dos sistemas corporativos;
- Definição da criticidade dos módulos críticos dentro dos sistemas considerados críticos;
- Definição da Infra-estrutura básica para processamento em caso de contingência;
- Definição dos recursos de softwares e hardware necessários para processamento dos sistemas;
- Definição das equipes de contingência.

A necessidade de um plano de contingência tem como principal característica à definição de profissionais que tenham conhecimentos de todos

os serviços básicos: Elétrica, Equipamentos, funcionamento de Serviços básicos de acessos, Segurança Física e Lógica etc.

## 2.6 Segurança em Correio Eletrônico

Como sabe-se qualquer correspondência pode ser enviada pela Internet. Assim como qualquer pessoa que tenha um bom conhecimento técnico pode intercepta-la.

Conforme explanado em tópicos anteriores, o correio eletrônico é comparado a uma agência de correios convencional, na qual uma carta vai de um bairro a outro através de ruas e avenidas, existindo pontos de verificação e aí pode facilmente interceptar sua carta , lê-la e enviá-la novamente para o seu destino.

Sadler (1996) indaga que “há várias opções e questões básicas, que se pode utilizar para minimizar a chance de os dados confidenciais da empresa serem interceptados e lidos por convidados inesperados e elas incluem”:

- Qual o grau de confidencialidade dos dados que meus usuários estão enviando;
- A criptografia de mensagens e arquivos é uma opção viável?
- Por qual caminho de roteamento as mensagens dos meus usuários estão trafegando antes de serem recebidas pelo receptor pretendido?

Antes de entrar em pânico é necessário realizar um levantamento sobre os tipos de informações que são enviadas por seus usuários. A partir daí deve-se realizar um trabalho sobre qual tipo de segurança precisa ser implementada (Sadler, 1996).

O e-mail, recurso mais usado da Internet, é pratico e rápido. Mas não é seguro. Ao enviar uma mensagem, nos conectamos a um servidor SMTP, que a retransmite entre vários roteadores, até ficar armazenada num provedor, esperando que o destinatário se conecte e leia. Em qualquer ponto deste trajeto, o administrador de sistemas (ou um hacker, se o sistema não for suficientemente seguro) pode bisbilhotar ou até mesmo alterar o conteúdo da mensagem. Se alguém conseguir descobrir sua senha de acesso, também pode ler o e-mail no seu provedor antes de você. Por fim, qualquer pessoa pode enviar uma mensagem com a identidade de outra, bastando configurar a identidade no programa de e-mail.

Existem softwares de criptografia tanto para mensagens quanto para arquivos (anexos), com um agravante: o software deve estar instalado na rede do transmissor e receptor para que a mensagem seja bloqueada e/ou desbloqueada.

A criptografia é uma arte: a arte de escrever ocultamente. Talvez tão antiga, quanto à escrita. Hoje um dos métodos mais eficientes de se transmitir informações, sem que haja a possibilidade de comprometimento do sigilo. Baseada em chaves, uma informação pode ser codificada através de algum algoritmo de criptografia, de modo que, tendo conhecimento do algoritmo utilizado e da chave utilizada, é possível recuperar a informação original fazendo o percurso contrário da encriptação, a desencriptação. O programa de criptografia mais famoso é o Pretty Good Privacy - Ótima Privacidade - PGP. É também um dos programas mais polêmicos da Internet. O seu autor, Phil Zimmermann, sofreu uma série de investigações por parte do FBI e teve de

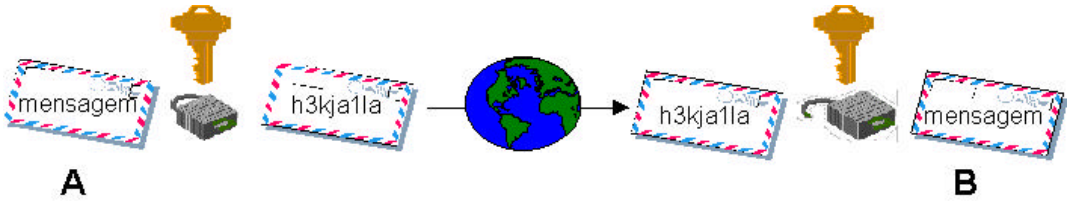
recorrer a grupos de apoio que se formaram na Internet para conseguir pagar seus advogados (Mcfedries, 1996).

É importante destacar que um bom método de criptografia deve garantir pelo menos que um intruso recupere a partir do texto criptografado e do conhecimento sobre o método de criptografia, o valor das chaves. Ou seja, enquanto as chaves mantiverem-se secretas, a confiabilidade do texto transmitido está garantido.

- **Encriptação por chave privada (Simétrica)**

É o método de encriptação que utiliza uma mesma chave para encriptar e desencriptar a mensagem; esta chave pode ser uma palavra, uma frase ou uma seqüência aleatória de números. O tamanho da chave é medido em bits e, via de regra, quanto maior a chave, mais seguro será o documento encriptado. A encriptação por chave privada (figura 2.4). Funciona muito bem quando o usuário que encripta á o mesmo que desencripta o arquivo (por exemplo, para proteger arquivos que ficam armazenados no próprio disco rígido). Mas quando se trata de uma mensagem que vai ser transmitida, surge um problema. O receptor e o transmissor precisam antes combinar uma senha, e usar algum meio seguro para transmitir esta informação (isso só ocorre quando se cria apenas uma chave).

**Figura 2.4: Criptografia Por Chave Privada**

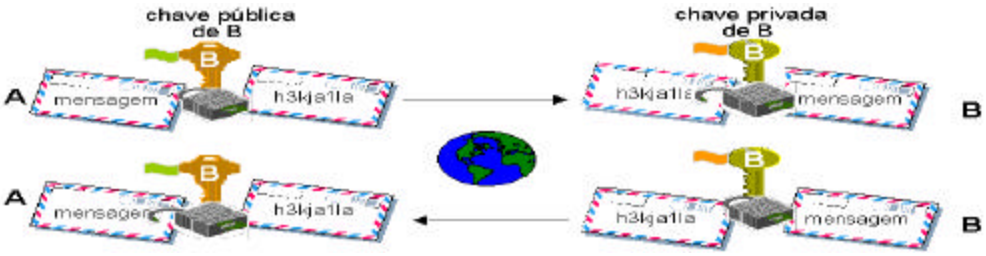



Fonte: Tema: a revista do serpro, ano XXIV – Nº 146.

- **Encriptação por chave pública (Assimétrica)**

O método de encriptação por chave pública (figura 2.5), proposto em 1976 por Diffie e Hellman (1976), resolve o problema de transmitir uma mensagem totalmente segura através de um canal inseguro (sujeito à observação, "grampo" etc.). O receptor da mensagem cria duas chaves que são relacionadas entre si, uma pública e uma privada. A chave pública pode e deve ser distribuída livremente. Quem envia a mensagem tem que utilizar a chave pública do receptor para encriptá-la. Uma vez encriptada, esta mensagem só pode ser desencriptada pela chave do receptor.

**Figura 2.5: Criptografia por Chave Pública**




Fonte: Tema : a revista do serpro, ano XXIV – Nº 146

- **Assinatura eletrônica de documento**

A assinatura eletrônica de documentos representa um aspecto importante para garantir privacidade. Ao assinar um documento, o usuário garante que ele é realmente o autor e que seu conteúdo não foi modificado (figura 2.6).

O mecanismo de uma assinatura digital envolve basicamente dois procedimentos: assinatura de uma unidade de dados e verificação da assinatura em uma unidade de dados para reconhecer a assinatura.

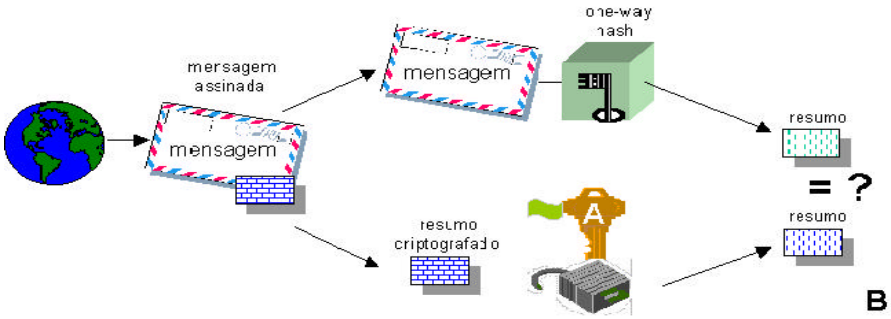
O processo de assinatura envolve a codificação da unidade de dados completa ou parcial de uma parte.

**Figura 2.6: Geração de uma mensagem com assinatura digital**


Fonte: Tema : a revista do serpro, ano XXIV – Nº 146

Já o processo de verificação envolve a utilização de um método e uma chave publica para determinar se a assinatura foi produzida com a informação privada do signatário (com sua chave primária), utilizando a chave pública do signatário para decodificar a mensagem (figura 2.7).

**Figura 2.7: Verificação de uma mensagem com assinatura digital**




Fonte: Tema : a revista do serpro, ano XXIV – Nº 146

## 2.7 Políticas de Segurança

É um conjunto de leis, regras e práticas que regulam como uma organização gerencia, protege e distribui suas informações e recursos (Soares, 1997).

Um conjunto de critérios e soluções para problemas tecnológicos e humanos criados para evitar ou minimizar a vulnerabilidade das informações, é tão importante quanto investir em sofistificados sistemas de proteção.

As regras são as funções das responsabilidades de sensibilidade, associadas aos recursos e informações (confidencial, secreto), do grau de autorização das entidades e das formas de acesso suportadas por um sistema.

A política deve ter o jeito da organização, porém alguns assuntos devem ser tratados em comum por todas as organizações:

- Os serviços que podem ser utilizados (uso profissional);
- Quem autoriza as conexões;
- Quem é responsável pela segurança;
- As normas, diretrizes e práticas a serem obedecidas;
- As responsabilidades dos usuários;
- Preparação para situações de contingência (continuidade operacional);
- Privacidade do usuário – arquivos pessoais, correio eletrônicos;
- Medidas disciplinares que serão utilizadas caso a Política não seja cumprida.

Para definir tal política na organização é necessário (Gil, 1994):

- Pesquisar o conteúdo que terá a política;
- Minutar o texto que descreve a política;
- Obter a aprovação dos altos escalões da administração da organização;
- Disseminar a política de segurança em todos os escalões da organização.

Um exemplo dos principais pontos vulneráveis em um sistema é a relativa facilidade de acesso a eles (Cheswick, 1994). Mesmo com senhas tornam-se ineficientes quando não há controle rigoroso sobre o uso delas. É preciso instituir regras na empresa que combatam a divulgação de uma senha para colegas de trabalho ou aquelas que sejam de fácil dedução.

Como sabe-se a maior função de uma senha é garantir que o usuário tenha acesso a sistemas onde está autorizado.A senha deve ser bem escolhida, não deve ser óbvia, porém deve ser lembrada sem dificuldades. Algumas dicas para escolher uma boa senha (Mcfedries, 1996):

- Nunca utilize seu nome, data de nascimento, telefone ou qualquer outro dado eu esteja ligado a pessoas de rotina;
- Misture letras com números (utilize símbolos $,^, % e *);
- Se o sistema aceitar letras maiúsculas e minúsculas, utilize ambos em sua senha.
- Nunca use menos de seis caracteres;
- Utilize senhas que possam ser digitadas rapidamente, evitando olhar para o teclado;
- Memorize sua senha;
- Mude sua senha pelo menos de 3 em 3 meses;
- Utilize senhas diferentes para cada tipo de serviço que esteja cadastrado.

Diante disso concluímos que uma política de segurança é uma declaração ampla dos objetivos e intenções da organização com relação aos dados que estão circulando em seu ambiente organizacional, na qual inclui regras, define as informações e recursos da organização que devem ser utilizados.

## 2.8 Os 10 Mandamentos

A utilização da rede é um privilégio e não um direito, ou seja, poderá ser recusado em qualquer altura devido a comportamento abusivo (colocação de informação ilegal num sistema, linguagem incorreta que possa afetar terceiros)

em mensagens públicas ou privadas, o envio de *chain-letters* (cartas correntes), o envio de mensagens em larga escala para grupos de indivíduos que não as solicitaram, ou outro tipo de abusos que possam interferir no trabalho de terceiros ou provoquem a congestão das redes.

Ao se comunicar na rede, depara-se com diversos tipos de usuários: usuários novatos e usuários antigos. Também encontra-se diversos tipos de culturas e povos. Este tópico tem como principal objetivo, descrever os 10 mandamentos básicos a se seguir ao utilizar a Internet, assim como descrever modos de como se tratar na rede (ao se escrever ou receber uma mensagem eletrônica).

Os dez mandamentos do instituto de ética na Internet definidos são (etiquete, 2000):

1. Não utilize o computador para prejudicar as pessoas;
2. Não interfira no trabalho de outras pessoas;
3. Não se intrometa nos arquivos alheios;
4. Não use o computador para roubar;
5. Não use o computador para obter falsos testemunhos;
6. Não use nem copie softwares pelos quais você não pagou;
7. Não use os recursos de computadores alheios sem pedir permissão;
8. Não se aproprie de idéias que não são suas;
9. Pense nas conseqüências sociais causadas pelo que você escreve;
10. Use o computador de modo que demonstre consideração e respeito.

Como já sabe-se a comunicação por e-mails é prática e muito rápida mas nem sempre é a solução adequada. O fazer parte do Ciberespaço (espaço

cibernético) é necessário que se utilize padrões de comportamento On-line. Ou seja, cada espaço que você navega tem sua própria cultura, se não se utilizar um padrão para conversação você pode ofender pessoas intencionalmente, este conjunto de regras é chamado de “Netiquetas”, este assunto é explanado com maiores detalhes no próximo tópico.

## 2.9 Netiquetas

Netiqueta é a forma aportuguesada do termo inglês "netiquette", que significa "etiqueta (bons modos) na Internet". A Netiqueta é um conjunto de regras não-oficiais, passadas de boca em boca e site em site que tenta estabelecer um padrão de comportamento considerável "desejável" pelos internautas e para os internautas (Computing Services, 1987).

As regras da netiqueta todas elas visam tornar a Internet um lugar menos caótico e mais sadio, ensinando as pessoas que certas atitudes aparentemente inofensivas podem aborrecer, atrapalhar ou agredir outros usuários.O usuário que desrespeita a netiqueta, propositalmente ou não, prejudica também a si mesmo, porque é "deixado de lado" pelos outros internautas (Shapiro, 1985).

Esse conjunto de regras pode ser empregado em correio eletrônico, listas de discussões, Netnews, informações genéricas (WWW, FTP, Telnet), sendo que muitas destas são baseadas nas regras que nos permitem viver em sociedade. Este tópico tratará apenas no que tange a e-mails. Dentre destacamos (Varho, 1995):

- Considere que as mensagens na Internet não são seguras. Nunca escreva numa mensagem qualquer coisa que não pudesse ser escrita num cartão postal.

- Respeite o direito autoral do material o que você utiliza numa mensagem. Quase todos os países têm leis sobre o assunto.
- Se você está retransmitindo uma mensagem recebida, não mude o texto. Copie as partes importantes e retransmita-o.
- Nunca envie “corrente" por e-mail. Notifique o administrador local sobre o recebimento de correntes;
- Não envie arquivos atachados com vírus em seus e-mails. Não faça com os outros o que não gostaria que fizesse com você;
- Seja moderado nas mensagens que manda e liberal com as que recebem. Você não deve mandar mensagens "Grosseiras" mesmo quando provocado.
- Antes de responder as mensagens cheque o assunto (Subject) de todas as mensagens antes de responder, às vezes uma pessoa que pede ajuda (ou explicações) manda outra mensagem que diz, efetivamente, "esqueça a primeira mensagem". Certifique-se de que a mensagem que seja realmente dirigida à você (você pode estar recebendo somente uma cópia da mensagem para conhecimento, e não para "participar da discussão");
- Não use e-mail de outras pessoas, respeito a privacidade de cada um;
- Seja cuidadoso ao enviar mensagens. Existem endereços que podem enviar a mensagem para muitas pessoas envie apenas para os endereços que você conhece.
- Preste atenção no campo de cópias da mensagem (CC - "carbon copy"), informações gerais devem ser enviadas para o seu superior imediato com cópia para os demais interessados.

- Em geral a maioria das pessoas que usa a Internet não tem tempo para responder a questões gerais a respeito da Internet e de seu funcionamento. Não envie mensagens não solicitadas pedindo informações a pessoas cujo e-mail você viu "por aí".
- Lembre-se de que as pessoas com as quais trocas mensagens podem estar em qualquer parte do mundo. Ao Enviar uma mensagem, dê um tempo real de resposta; não envie mensagens de reforço perguntando se recebeu a anterior é uma pressão desnecessária e desagradável;
- Tenha atenção com o conteúdo de suas mensagens-escreva o que tem certeza ou faça perguntas. Porém, evite enviar informação incorreta, pois, ela pode gerar atingir um número imprevisto de pessoas e deixa-lo em situação constrangedora;
- Ao sair de férias, informe ao administrador para que ele possa fechar sua caixa postal ou redirecione-o para a caixa postal de outra pessoa (Se você assume uma função de chefia solicite que redirecione sua caixa postal para o seu substituto);
- Verifique todos os endereços para os quais está mandando mensagens longas ou pessoais. É de bom tom colocar a palavra LONGO ("*Long*") na linha do assunto da mensagem ("subject") para que o destinatário saiba que a mensagem exigirá algum tempo para ler e responder (Uma mensagem com mais de 100 linhas de texto é considerada muito longa);
- Nunca coloque mais de 65 caracteres numa linha e termine toda linha com um <ENTER> ("retorno de carro").

- Saiba quem contactar para pedir ajuda. Normalmente há muitos recursos por perto. Check com pessoas próximas quem pode ajudá-lo com problemas de software e de sistema. Também saiba a quem recorrer no caso de qualquer coisa questionável ou ilegal.
- Lembre-se de que os destinatários são seres humanos cuja cultura, língua e senso de humor podem ter pontos de referência distintos dos seus. Lembre-se de que o formato de datas, as medidas e os idiomas não "viajam bem". Seja especialmente cuidadoso com sarcasmo!
- Use letras maiúsculas e minúsculas normalmente. ESCREVER TUDO EM MAIÚSCULAS É COMO SE ESTIVESSE GRITANDO!
- Limpe sua lixeira constantemente, liberando mais espaço de sua caixa posta e agilizando a comunicação;
- Use alguns símbolos para dar ênfase. Por exemplo, *assim*. Para sublinhar palavras faça assim. Ex*:* Caro amigo, sabe se já _*efetuaram o Pagamento*.
- (Não utilize “smileys” Ex::-) é um exemplo de "smiley" (olhe de lado), pois a maioria dos usuários não está habituada a utiliza-los até mesmo porque a cada dia surge novos na rede;
- Não envie arquivos pornográficos e/ou engraçadinhos por e-mail, na maioria das organizações é motivo para demissão (aplicado de acordo com a lei vigente);
- Não responda de "cabeça quente". Quando receber uma mensagem que o perturbou muito, primeiro esfrie a cabeça antes de responde-la;

- Não use acentos, caracteres de controle ou anexos que não sejam ASCII. Seja breve sem ser telegráfico. Quando responder a uma mensagem, inclua pequenas partes da mensagem original para ser entendido. É extremamente indelicado responder a uma mensagem simplesmente incluindo todo o texto original: retire as partes que não são importantes;
- Jamais assina o seu e-mail organizacional em lojas virtuais e/ou listas de discussões;
- O assunto da mensagem ("subject") deve refletir, fielmente, o conteúdo da mesma;
- Se você usa uma assinatura faça-a curta. Regra prática: não mais do que 04 linhas. É importante que se coloque o nome completo, cargo, setor e telefone para futuros contatos;
- Mensagens de e-mail não são seguras. Mensagens (e notícias em news) estão sujeitas à falsificações mais ou menos sofisticadas. Use o bom senso antes de concluir pela autenticidade de uma mensagem.
- Se uma mensagem recebida for muito importante responda imediatamente para que o emitente saiba que você a recebeu e, depois, mande uma resposta mais elaborada;
- Convites por E-mail – se o evento for uma reunião informal em sua casa ou em eventos comerciais, não há problemas em enviar um e-mail. Porém, antes deve-se envia-lo com antecedência; enviar na véspera denota falta de organização. Convites para casamento e outros encontros formais não devem ser enviados por e-mail;

- Padrões de conduta via e-mail dependem do seu relacionamento pessoal com o destinatário e do contexto da comunicação. Seja cuidadoso com gírias, palavrões e siglas locais;
- O custo de "entrega" de uma mensagem é, em média, page igualmente pelo emitente e pelo destinatário (ou por suas empresas).
- Conheça o tamanho das mensagens que manda. Incluir arquivos grandes (tais como figuras, textos formatados, programas etc) Regra prática: não mande arquivos anexados maiores do que 50 kb (Kilobytes).
- Não envie mensagens com grandes quantidades de informações não solicitadas.

Estes conjuntos de regras, lista alguns comportamentos para auxiliar que os usuários possam se adaptar às suas necessidades pessoais e organizacionais (Matarazzo, 2000).

Os usuários devem estar atentos ao que não lhes interessa, devem seguir os padrões definidos sobre a propriedade de serviços de correio eletrônico, como e o que pode ser enviado e recebido em sua caixa postal.

## 2.10 Lista de Falsos Alarmes

Geralmente quem utiliza serviços de correio eletrônico, seja corporativo, gratuito ou pessoal está sujeito a recebimento de mensagens eletrônicas alarmantes sendo na maioria das vezes correntes e/ou Vírus.

Chama-se SPAM o uso abusivo do correio eletrônico para envio de mensagens não solicitadas para uma grande quantidade de usuários, como malas diretas, pirâmides de enriquecimento fácil, abaixo assinado e as

correntes (estas que aumentam a cada dia de forma espantadora). Tais mensagens geram uma grande quantidade de tráfego, congestionando a rede e difamando instituições sérias (SPAM, 2000).

Em geral o usuário pode ter entrado em algum tipo de site e permitiu o envio de notícias por e-mail, mas na maioria das vezes o seu endereço de e-mail foi incluído nestas listas sem autorização prévia.

As razões que levam o escritor inicial a divulgar via e-mail carta de corrente, Lista de Vírus etc. só ele pode dizer, mas pode-se fazer algumas deduções:

- Ver até onde sua mensagem pode trafegar na rede;
- Molestar outra pessoa (direcionando as mensagens para uma determinada pessoa);
- Quebrar alguma outra corrente de e-mail;
- Prejudicar a reputação de uma pessoa ou organização.

No Brasil existe o Movimento Brasileiro Anti-SPAM, onde você pode fazer dentre outras coisas denúncias e consultar listas-negras de SPAMMERS (abuse@antispam.org.br). Segundo estudos de alguns pesquisadores até hoje nenhuma veracidade destas “Lendas Urbanas” como é chamada na Internet foi comprovada. Estas lendas estão distribuídas em 3 categorias: Lendas, Falsos Vírus e correntes (SPAM, 2000).

**Lendas**

A primeira coisa que se deve observar neste tipo de mensagens é a advertência solicitando para que você envie para todo o mundo, fique atento, pois, nenhuma mensagem de fonte acreditável deve ser divulgada para que todos saibam seu conteúdo.

Existem dois fatores que contribui para a aceitação de tal mensagem: utilização de termos técnicos (levando a acreditar que a advertência é real) e credibilidade através de associações.

Geralmente utiliza-se o prestígio de grandes companhias, fazendo com que a história seja verdadeira, apoiada pela reputação da companhia e o gerente.

Diariamente muitas pessoas recebem vários tipos de lendas, no qual tem como: Bill Gates, Walt Disney & AOL, Brasil dividido ou Enquanto é tempo, O, Garotinha com câncer: vamos salvar uma criança, O garoto com tumor no cérebro. Ericsson e Nokia distribuem telefones celulares gratuitamente, Greve na Internet contra as empresas telefônicas, assim como outras inúmeras.

**Falsos Vírus**

A maioria dos vírus sobre os quais as mensagens alertam não existem, e as que existem não contaminarão seu computador a menos que você abra os arquivos.

Alguns dos e-mails mais comuns sobre alerta de vírus, só que na realidade não são verdadeiros são: Pokénmon, Good Times, Telefone Celular Digital, cartão virtual para você, dentre outros.

**Correntes**

São conhecidas na Internet como (*chain letters*). Existem as inofensivas (felicidade e amor), as que intimidam os que quebram as correntes prometendo maus momentos e dias nefastos e as que oferecem muito dinheiro fácil (estes podem ser enquadrados no artigo 171- Estelionatário)

Pode-se reconhecer uma história, atente pelos padrões utilizados, geralmente são semelhantes. É formado por 3 partes comuns:

- O Aviso: sempre tem um gancho para ter seu interesse e conseguir sua atenção para que continue lendo o resto da carta “Ganhe dinheiro sem fazer esforço”;
- A Ameaça: A maioria das mensagens adverte sobre coisas terríveis que poderão acontecer se você não continuar enviando a mensagem, já outros jogam com a ganância para conseguir que envie a mensagem para frente. Contém freqüentemente informações ou idiomas técnicos para conseguir fazer com que você pense que é real;
- Um Pedido: O mais antigo é aquele que pede que você envie $1,00 para uma lista de 10 pessoas, sempre informando para distribuir o e-mail para quantas pessoas forem possível. Nunca informam sobre o gargalho da largura da banda ou que a mensagem á uma fraude.

É importante que os usuários antes de abrir uma mensagem recebida observe alguns pontos:

1. Se receber um e-mail com arquivo anexado de alguém que não conheça, não abra, simplesmente apague.
2. Vírus e programas de Trojans têm que ser executado para infectar os arquivos. Se você "clicar duas vezes" em um arquivo anexado de e-mail, você está executando código e pode infetar sua máquina.

## 2.11 Responsabilidades dos Usuários

A corporação após ter orientado os usuários de sua rede sobre regras para a utilização de e-mail, aplicações, recursos tecnológicos disponíveis, informa-

lhes sobre suas responsabilidades para que mantenham sua caixa postal sempre disponível para comunicação dentro da organização.

"Abaixo são citadas algumas responsabilidades dos usuários para com os conteúdos e as manutenções da caixa de correio eletrônico:"

- Consulte a sua caixa postal periodicamente para que esta não ocupe demasiado espaço em disco no servidor.
- Evite receber mensagens excessivamente grandes (> 1 ou 2 MB, por exemplo).
- As mensagens, logo que transferidas para o seu computador, poderão ser apagadas do servidor (realizada automaticamente pela maior parte dos programas de correio eletrônico).
- Nunca assuma que o seu correio eletrônico só pode ser lido por si, enquanto permanece no servidor. Outros poderão ter acesso à sua caixa por meios ilícitos (e que são normalmente impedidos por mecanismos de segurança).
- Para o envio/recepção de uma mensagem privada de conteúdo crítico, considere a utilização de meios de criptação ou codificação de mensagens.

Deve-se considerar que algumas corporações, disponibilizam para usuários especiais um espaço reservado no servidor corporativo de E-mail, para maior segurança das correspondências recebidas, até mesmo pelo fato de que estes equipamentos têm um plano de contingência pré-estabelecido, esses devem observar aos seguintes aspectos:

- Mantenha o tamanho das mensagens no mínimo possível. Caso não sejam necessários no servidor, as mensagens deverão ser transferidas para o seu computador pessoal.

- Por precaução, verifique, com a ajuda de um anti-virus, as mensagens que transferiu ou recebeu de outros sistemas, para que se possam evitar eventuais ataques de vírus.
- As mensagens de conteúdo crítico não deverão ser guardadas no servidor, ou então deverão ser considerados meios para codificação dos mesmos.

# 3 .PESQUISA SOBRE “UTILIZAÇÃO DE CORREIO ELETRÔNICO”

O correio eletrônico atualmente propicia uma agilidade e comunicação entre os diversos departamentos organizacionais.

Como já citado, o correio eletrônico é uma ferramenta essencial para as organizações modernas, transmitindo e enviando documentos, imagens, gráficos, dentre outros. Facilitando a comunicação entre funcionários da organização, seus clientes, fornecedores etc.

Este trabalho investiga e fornece questões para orientar as organizações a avaliarem o nível de aceitação do serviço de correio eletrônico, tendo como premissa a utilização das informações para correções e implementação de uma norma de utilização de correio eletrônico corporativo. Esta pesquisa, objetiva buscar:

- Informações sobre utilização de algum procedimento para envio de mensagem eletrônica (norma, orientação etc.);
- Acesso àferramenta;
- Tipo de mensagens que trafegam no serviço de correio eletrônico corporativo;
- Índice de aceitação para monitoramento do serviço de correio eletrônico;
- Central de atendimento;
- Utilização dos recursos da ferramenta;
- Treinamento para utilização da ferramenta.

Para se atingir o objetivo desta pesquisa, foi utilizado um questionário disponibilizado através da WEB para usuários do serviço de correio eletrônico da previdência social no Distrito Federal (DATAPREV, MPAS e INSS).

A pesquisa foi executada no período de 04 a 08 de Maio de 2001. Foram realizadas 50 entrevistas, usuários do serviço de correio eletrônico da Previdência Social no Distrito Federal, o mesmo é oferecido e administrado pela DATAPREV.

## 3.1 Objetivo

A pesquisa sobre utilização de correio eletrônico tem como objetivo produzir indicadores que permitam avaliar a satisfação dos usuários quanto à utilização dos serviços de correio eletrônico. Facilitando com isso a implementação de uma norma interna para utilização do correio eletrônico e soluções para um controle efetivo dos conteúdos de mensagens que trafegam nesta corporação.

## 3.2 Universo

A pesquisa sobre utilização de correio eletrônico abrange todos os usuários da Previdência Social, no qual atende a três públicos: MPAS, DATAPREV e INSS.

**A Dataprev**

É uma empresa pública, vinculada ao MPAS, instituída em 04 de novembro de 1974.

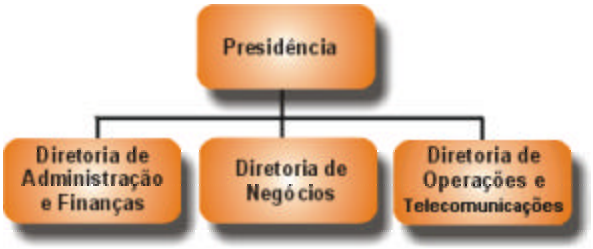
Além do edifício-sede, no bairro de Botafogo, no Rio de Janeiro, e de três Centros de Processamento de Dados, a DATAPREV possui Escritórios

Estaduais em vinte e três (23) estados do país. Atualmente, a empresa conta com cerca de 3.000 empregados.

Conhecer melhor a Dataprev significa saber a importância do trabalho que ela desenvolve para a Previdência Social brasileira, informatizando os diversos órgãos previdenciários e contribuindo para que o segurado receba um atendimento de qualidade.

A Dataprev está estruturada em três diretorias, conforme (figura 3.1).

**Figura 3.1: Estrutura Organizacional da Dataprev**




Fonte: http://www.dataprev.gov.br

A empresa conta, atualmente, com três Centros de Processamento de Dados: o do Rio de Janeiro (Centro de Tratamento de Informações do Rio de Janeiro - CTRJ. O), o de São Paulo (Centro de Tratamento de Informações de São Paulo - CTSP. O) e o de Brasília (Centro de Tratamento de Informações do Distrito Federal - CTDF. O).

Preocupado com a utilização do serviço de correio eletrônico corporativo o CTDF.O tomou a iniciativa de montar um piloto, para o tratamento das informações que trafegam nele. A partir dos resultados obtidos serão adotadas medidas corretivas para sanar os problemas identificados.

### 3.3 Número de Entrevistados

Com base nos usuários cadastrados no serviço de mensagem eletrônica e no âmbito previamente definido, foram selecionados cerca de 50 usuários, distribuídos nos referidos órgãos.

### 3.4 Critérios de Amostragem

A amostra é representativa dos usuários da área pesquisada, selecionada em 3 estágios. No primeiro estágio os usuários da DATAPREV**,** em segundo os usuários do INSS e por último os usuários do MPAS.

### 3.5 Coleta de Dados

Entrevistas pessoais com utilização de questionário elaborado de acordo com os objetivos da pesquisa. Para coleta desses dados foram realizadas as seguintes premissas:

- Aplicação por amostragem de um questionário através da WEB, procurando avaliar a utilização do correio eletrônico.
- Diagnóstico do questionário respondido pelos usuários, visando levantar dados sobre a utilização do serviço de correio eletrônico.

### 3.6 Desenvolvimento do Questionário

O questionário foi desenvolvido a partir de reclamações recebidas pela supervisão de suporte (SDFS. P), e também pela grande quantidade de informações indesejáveis que são distribuídos através do serviço de correio

eletrônico. No qual tais mensagens utilizam em média 30% da largura da banda de rede WAN.

### 3.6.1 Controle de Qualidade

- Filtragem: 100 % dos questionários foram filtrados após a realização das entrevistas.
- Fiscalização: 10 % dos questionários executados foram fiscalizados para verificação de cuidado na aplicação do questionário e adequação do entrevistado às variáveis das quotas da amostra.

## 3.7 Características da Pesquisa

### 3.7.1 Âmbito

Na pesquisa são investigados os tipos de mensagens eletrônicas que os usuários enviam e recebem através do serviço de mensagem eletrônica corporativa:

- Fins de utilização do correio eletrônico
- Arquivos provenientes de outras organizações
- Conteúdos impróprios, correntes, vírus, etc ..
- Suporte para utilização de correio eletrônico
- Utilização dos recursos oferecidos pela ferramenta

### 3.7.2 Variável Investigada

Serviço de correio eletrônico, o suporte ao correio eletrônico e avaliação geral do serviço por seus usuários.

### 3.7.3 Construção de Indicadores

A partir dos dados levantados serão construídos, três índices :

- Índice de Satisfação de usuários da previdência Social;
- Atuação do suporte técnico e
- Tipos de mensagens que são recebidas e/ou enviadas.

## 3.8 Interpretação dos Resultados

Nesta fase procurou-se identificar as necessidades, falhas e opiniões dos usuários do serviço de correio eletrônico da Previdência Social.

A estratégia implementada foi selecionar usuários aleatórios dos referidos órgãos para a validação da pesquisa intitulada como “Pesquisa de Utilização de correio eletrônico”.

A pesquisa buscou, colher informações seguindo as seguintes premissas:

- Um Público que apresentasse opiniões de usuários do corpo técnico;
- Gerentes;
- Administrativa Operacional;
- Operacional

Para colher os dados, para análise do ambiente, foram enviados através do correio eletrônico o informativo do link para 50 usuários, responderem o questionário eletrônico (Anexo 3) a fim de avaliar a utilização do correio eletrônico corporativo a ser respondido no prazo de três dias. A seguir são apresentados os resultados da pesquisa. Tais resultados representam a interpretação dos dados coletados através do questionário eletrônico.

## 3.9 Estudo da Demanda

Ao final deste prazo 42 usuários (84%) do total estimado responderam ao questionário eletrônico (Anexo III), as respostas foram armazenadas em um Banco de Dados para análise da demanda que será apresentada mais ao final deste capítulo.

As principais razões para o envio do questionário eram avaliar o índice de satisfação do usuário e obter subsídios para implementação futura de uma norma interna de utilização de correio eletrônico e monitoramento das mesmas. Dos entrevistados 63 % afirmam utilizar alguma norma para utilização de correio eletrônico, sendo que não existe um regulamento pré-definido e sim recomendação solta pelo Ministério do Planejamento e Medida Provisória do Ministério da Previdência Social - MPAS, sendo estas muito superficiais e genéricas, não especificando responsabilidades e sanções quanto à utilização do serviço.

Outro fator avaliado é que 67% dos usuários concordam com o monitoramento do serviço de correio eletrônico, garantindo assim o recebimento de mensagens indesejáveis. Além do mais, a organização teria um controle mais efetivo das mensagens que circulam no serviço de correio eletrônico, gerenciando o recebimento e envio de mensagens com conteúdos difamatórios, racistas, correntes religiosas, pirâmides de enriquecimento, arquivos impróprios, vírus através de arquivos atachados, anúncios ou ofertas de bens e serviços.

## 3.10 Divulgação dos Resultados

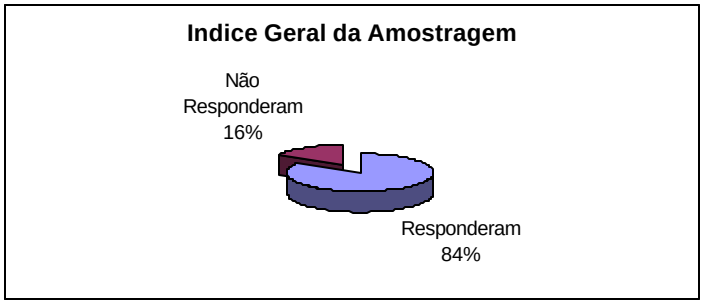
### 3.10.1 Análise Geral

Os dados levantados apresentam um panorama bastante interessante, relacionados a várias funções e órgãos. O índice de satisfação dos usuários que utilizam o serviço de correio eletrônico corporativo confronta a análise de índices genéricos e indicadores individual.

Em primeiro momento a pesquisa buscou informações sobre a satisfação dos usuários quanto ao serviço de correio eletrônico, abrangendo questões como: fins de utilização de correio, opinião sobre o monitoramento eletrônico, segurança, arquivo com conteúdos difamatórios, impróprios, suporte ao usuário, capacitação técnica, dentre outros. No segundo momento, avaliou-se o suporte técnico ao usuário e por último uma avaliação geral do serviço.

Vale destacar que, do total da amostragem 16% dos entrevistados não responderam ao questionário da pesquisa.

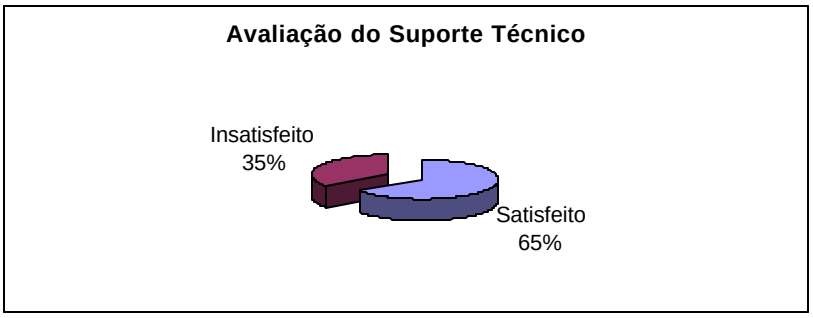
**Gráfico 3.1: Analise Geral da Amostragem**




Na avaliação do suporte ao serviço de correio eletrônico, constatou-se que 65% dos usuários estão satisfeitos com o suporte ao serviço, e 35% dos usuários apresentaram insatisfação quanto à disponibilização de informações

sobre o serviço de correio eletrônico (intranet, revistas eletrônicas, pastas públicas), conforme apresentado no gráfico 3.2.

**Gráfico 3.2: Índice de Satisfação quanto ao suporte ao serviço de E-mail**



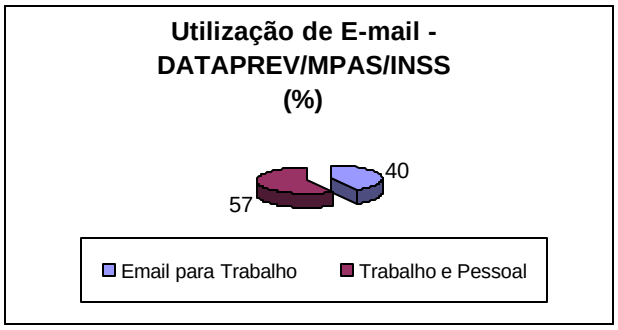

A maioria do entrevistados considera que o serviço de correio eletrônico atende suas necessidades e que ele é importante para o desempenho de suas atividades funcionais.

3.10.2 Avaliação do serviço de Correio Eletrônico

Nesta etapa, foi perguntado sobre a utilização do serviço de correio eletrônico. Podendo a partir desta análise permitir que o CTDF.O possa tomar medidas de segurança quanto à utilização do serviço. A pesquisa mostra que 57% dos entrevistados utilizam o serviço de correio eletrônico para fins de trabalho e Pessoal (gráfico 3.3). Vale destacar um fato curioso quanto aos usuários do INSS, no qual 69% do entrevistados afirmam que só utilizam o correio eletrônico apenas para fins de atividades funcionais (sendo que, na CAC -Central de Atendimento ao Cliente, tem registrado um índice muito grande de reclamações quanto ao recebimento de e-mails com correntes, pirâmides de enriquecimento, e reclamações e chamados técnicos de máquinas infectadas com vírus provenientes de arquivos anexos de

mensagens eletrônicas). Também são gerados reclamações e chamados técnicos para manutenção de máquinas infectadas com vírus.

**Gráfico 3.3: Utilização de E-mail: DATAPREV,MPAS e INSS**

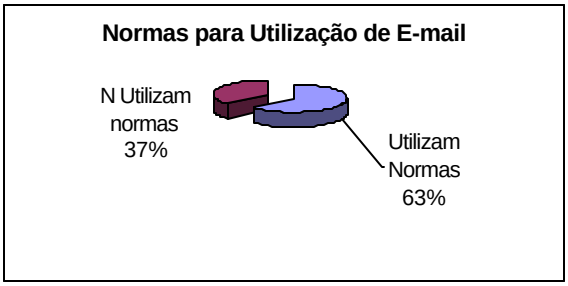



Um dos principais interesses da DATAPREV é criar uma norma para utilização do correio eletrônico, a qual tem como objetivo principal definir as responsabilidades dos usuários e sanções para aqueles que descumprí-las. Um fato interessante é que 63% dos entrevistados afirmam utilizar alguma norma para utilização de correio eletrônico (gráfico 3.4), fator este mascarado, sendo que existem apenas duas publicações no âmbito da organização referente ao assunto:

1. Recomendação nº 1, de 22 de setembro de 1999 -Ministério do Planejamento, que faz recomendações quanto a utilização do serviço de mensageria de extremo interesse da administração pública;

2. Portaria do MPAS Nº 862, de 23 de Março de 2001, publicada no Diário Oficial da União de 26 de março de 2001 (Seção I).Dispõe sobre o controle de acesso a dados, informações e sistemas informatizados da Previdência e Assistência Social.

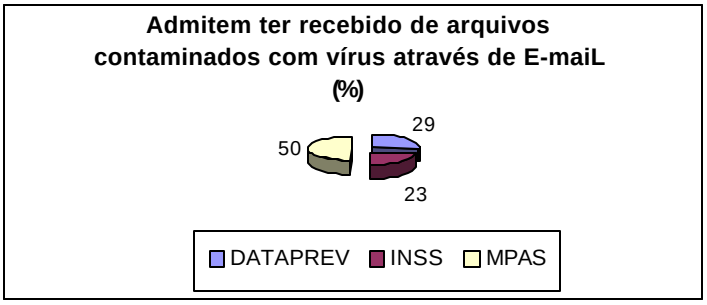
**Gráfico 3.4: Utilização de Normas de E-mail**




Dos entrevistados 100% afirmam efetuar logout antes de sair da máquina, garantindo assim, com que outros usuários não utilizem seu e-mail para outros fins, e que, já receberam mensagens com correntes religiosas, pirâmides de enriquec imento, arquivos impróprios,correntes.

A metade da amostragem do MPAS (50%) admite ter recebido arquivos com vírus através do correio eletrônico, contra 29 % da DATAPREV e 23% do INSS. Porém, como explanado anteriormente, as estatísticas da supervisão de atendimento ao usuário - SDFU.P indicam que a maioria das reclamações quanto à abertura de chamados para retirada de vírus é do INSS e em média 80% deste chamados é proveniente de vírus oriundos de arquivos baixados do correio eletrônico (gráfico 3.5)

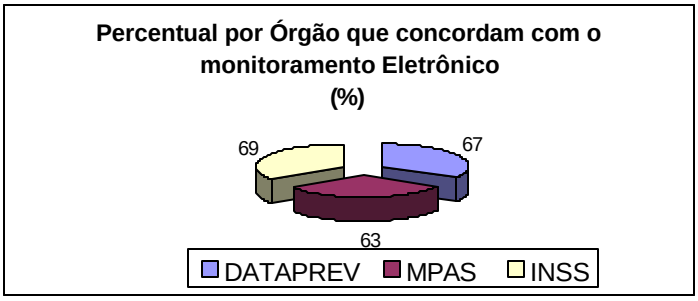
**Gráfico 3.5: Admitem receber arquivos contaminados com vírus**




De forma geral a maioria dos usuários do serviço (67%) aceitam que a DATAPREV (provedor de serviços) monitore o conteúdo das mensagens do

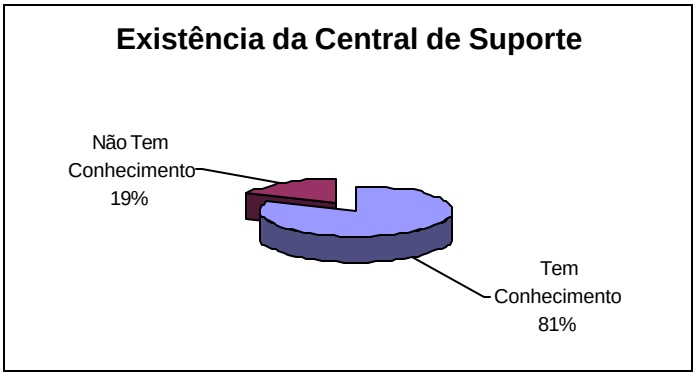
correio eletrônico, pois assim, eles terão maior segurança de seus dados e haverá um controle mais efetivo dos arquivos indesejáveis (gráfico 3.6).

**Gráfico 3.6: Concordam com o Monitoramento Eletrônico do Serviço**



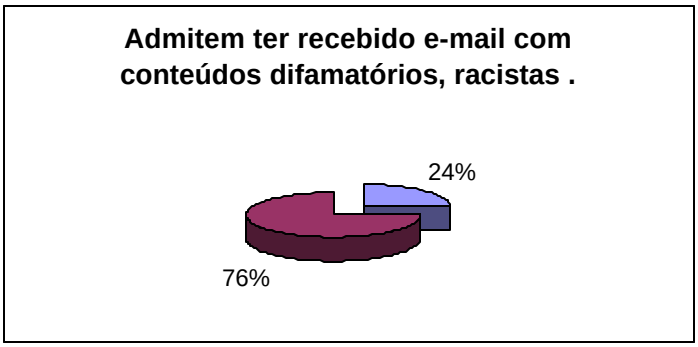

Os usuários entrevistados (81%) afirmam conhecer o suporte ao serviço de correio eletrônico, sobre administração do CTDF.O, o qual fornece orientações sobre instalação, configuração e esclarecimentos sobre a utilização (gráfico 3.7).

**Gráfico 3.7: Tem conhecimento da existência da Central de Suporte**



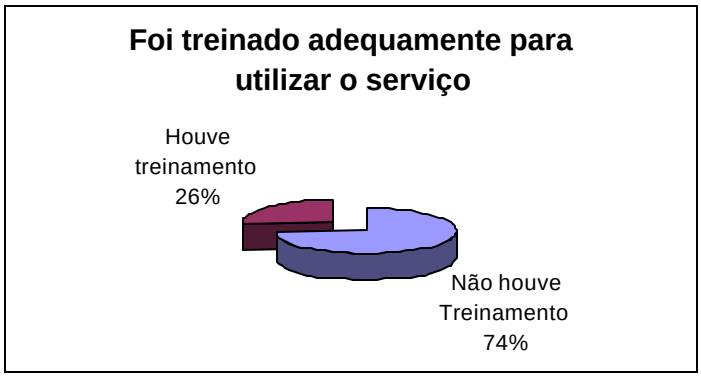

Outro item avaliado de extrema importância foi à questão do recebimento de mensagens com conteúdos difamatórios, racistas etc. 76 % dos usuários admitem já ter recebido mensagens dessa natureza (gráfico 3.8). Esta, assim como todas as variáveis abordadas, são de extrema importância. Porém, a organização deve tratar tal questão com muita atenção, pois qualquer usuário pode processa-la por ter recebido conteúdos difamatórios, que venham a denegrir a imagem da organização.

**Gráfico 3.8: Receberam e-mail com conteúdos difamatórios, racistas**



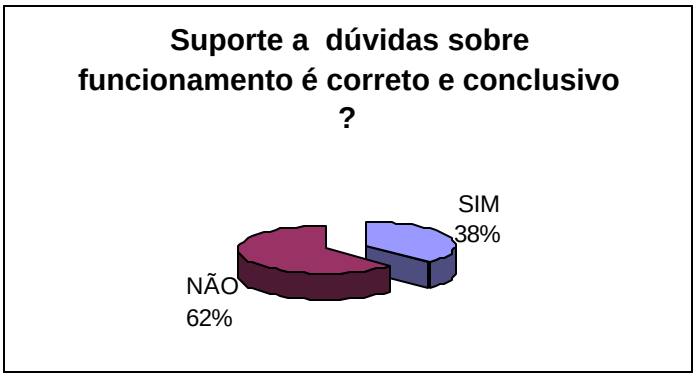

A maioria dos usuários do serviço (74%) admite que não receberam nenhum tipo de treinamento ou orientação para utilização da ferramenta (gráfico 3.9). Sendo que o crescimento de acesso ao serviço ocorreu sobre demanda de acordo com a necessidade dos órgãos utilizadores.

**Gráfico 3.9: Recebeu treinamento para utilização do serviço de correio eletrônico**



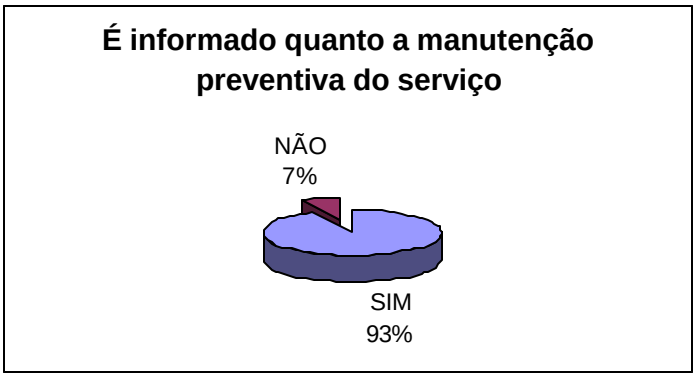

A pesquisa abrange o nível de satisfação quanto à atuação do suporte de correio eletrônico. 38% dos entrevistados afirmam ter suas dúvidas sanadas. Um fato curioso a se destacar, é que 62 % dos entrevistados do MPAS afirmam que o suporte não é conclusivo e correto, pois, tal suporte é realizado pelo próprio MPAS. No qual possui sua equipe própria de suporte (gráfico 3.10).

**Gráfico 3.10: Suporte a dúvidas sobre o funcionamento é correto**



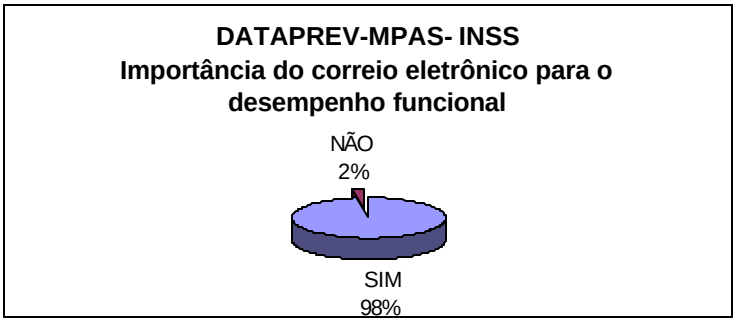

Dos usuários entrevistados (93%) admitem que é informado quanto à manutenção preventiva do serviço de correio eletrônico, garantindo assim, maior segurança de suas informações e melhor desempenho em suas atividades funcionais (gráfico 3.11).

**Gráfico 3.11: É informado quanto à manutenção preventiva do serviço**




A maioria dos usuários (98%) considera o serviço de correio eletrônico importante para bom desempenho de suas atividades funcionais, agilizando assim despacho de documentos, reduzindo papéis e minimizando a burocracia (gráfico 3.12).

**Gráfico 3.12: Importância do Correio Eletrônico para o desempenho funcional**




Essa pesquisa é de supra importância para a DATAPREV, a fim de avaliar o nível de satisfação quanto à utilização do serviço eletrônico, detectando as falhas e propondo ações corretivas para implementação de novos serviços na intenção de garantir uma melhor utilização, e integridade dos dados e informações nelas contidas. Além disso, pode-se também ter como ponto de partida, o estudo de implementar uma rotina de monitoramento das mensagens, garantindo com isso o envio apenas de informações de interesse da corporação e punir os usuários que por alguma razão venham a descumprir uma norma interna.

# 4 .NORMATIZAÇÃO PARA UTILIZAÇÃO DE CORREIO ELETRÔNICO

## 4.1 Metodologia para Normatização

A utilização de correio eletrônico vem crescendo consideravelmente nas organizações, agilizando a comunicação interna, reduzindo custos com materiais de expediente, otimizando e controlando o tráfego dos dados transmitidos através do correio eletrônico, impedindo com isso o vazamento das informações corporativas, dentre outros.

Porém, seus usuários não recebem nenhum tipo de orientação sobre o que é permitido ser recebido ou enviado, ocorrendo assim uma utilização indevida do serviço.

Pode-se citar como exemplo: envio e/ou recebimento de arquivos com conteúdos obscenos, piadas, correntes, roubo de informações de propriedade intelectual da organização, recebimento de arquivos com vírus (contaminando outrossim a LAN- Rede Local de computadores).

Um dos fatores que contribui, é a falta de uma legislação específica, ocasionando com isso uma visão errônea dos usuários com relação à propriedade dos serviços disponíveis, ou seja, utilizam recursos e ferramentas corporativas como sendo de uso público, obtendo direito de confidencialidade das correspondências eletrônicas contidas em sua caixa postal.

Devido a tais fatores, surge a necessidade da implementação de normas administrativas que visam inibir a utilização abusiva de tal serviço, limitando

com isso, o tamanho da banda de rede a ser utilizada, exclusão de sites de conteúdos pornográficos, gerenciamento da utilização dos serviços para negócios particulares em horário de expediente, envio de mensagens molestando colegas de trabalho, dentre outros.

Os principais motivos para o controle rígido das correspondências arquivadas, com informações sobre conteúdo, data, remetente e destinatário são:

- Segurança de informações corporativas
- Agilidade do sistema
- Produtividade dos empregados

Para conseguir tais controles, existem ferramentas de apoio como: softwares para gerenciamento de correio eletrônico.

É válido destacar que um dos pontos cruciais para o sucesso deste trabalho, é a conscientização do corpo funcional sobre as normas de uso e a aplicabilidade de sanções administrativas relacionadas a possíveis danos morais a terceiros e/ou à organização, sendo que, tais políticas devem ser entregues aos usuários por meio de orientações (palestras, capacitação técnica, folders, dentre outros) e o mesmo tendo que assinar um termo de responsabilidade sobre a utilização dos serviços. Nos módulos são expostos os principais critérios a serem observados ao se criar uma norma para utilização do correio eletrônico. Todos os fatores descritos são importantes para se conter os tipos de informações que trafegam no serviço de correio eletrônico corporativo, a importância da informação, o acesso, as responsabilidades na utilização do serviço, as sanções e penalidades a que estão sujeitos.

### 4.1.1 Propósito

As organizações estão demonstrando grande preocupação devido ao aumento na utilização dos serviços de correio eletrônico, assim como a falta de controle e os abusos detectados.

O propósito deste trabalho é estabelecer regras de conduta a todos os usuários do serviço de correio eletrônico (empregados, contratados, consultores, estagiários etc...), além de oferecer subsídios ao empregador para que possa aplicar penalidades, a quem descumpra.

Neste mesmo contexto, é importante que as políticas de correio eletrônico sejam comunicadas pelos gerentes dos funcionários ou pelo departamento de recursos humanos. É válido destacar que as organizações devem cumprir um papel muito importante delineando ações estratégicas para estruturação deste projeto e enfatizar os principais objetivos em presariais para o monitoramento de correio eletrônico. Tais ações refletem em:

- Elaboração de uma normatização de correio eletrônico formal;
- Definição do envio de mensagens corporativas com destino externo da corporação, que deverá seguir um padrão de segurança (criptografia de dados) para que a informação não caia em mãos erradas (por exemplo, seu concorrente direto);
- Definir critérios relacionados aos conteúdos e informações que devem ser enviadas;

- Definir critérios relacionados às políticas de utilização de correio eletrônico e termo de responsabilidade aos seus usuários (eliminando assim “Expectativa de Privacidade”);

- Esclarecer que tipo de violações de normas pode acarretar punições disciplinares, que podem ir desde uma advertência verbal a escrita; e dependendo da gravidade até mesmo a demissão;

- Disponibilizar ferramentas para segurança contra vírus dentro da rede corporativa;

- Aplicar com rigor as penalidades necessárias em caso de violação das normas (após as devidas apurações);

- Publicar, distribuir cópias e obter aceitação das normas de utilização de correio eletrônico organizacional a todos os usuários no ato de sua admissão;

- Designar um departamento para gerenciar, controlar e monitorar todo o acesso e recursos computacionais (normalmente esta atribuição é realizada pela gerência e segurança de rede);

- Criar dispositivos para que, em caso de violação desta norma, os privilégios de acesso à caixa postal do usuário sejam suspensos, sendo informado confidencialmente aos seus chefes imediatos para aplicabilidade de punições disciplinares;

- Assegurar que as mensagens eletrônicas enviadas através dos serviços de correio eletrônico sejam recebidas pelo usuário correto, sem interferências de qualquer natureza;

- Limitar o espaço de armazenamento em disco reservado a cada usuário para envio e recebimento de mensagens de correio eletrônico;

- Informar e realizar campanhas de conscientização aos usuários sobre a utilização dos serviços de correio eletrônico e monitorar as atividades realizadas na rede corporativa para avaliação do nível de comprometimento dos funcionários com a normatização em vigor.

### 4.1.2 Política Específica

Uma política bem definida deverá esclarecer todas as questões que possam estar dificultando o bom andamento do processo: O que é um "correio eletrônico apropriado"? Que conseqüências os funcionários podem esperar caso desrespeitem esta normatização? Uma política clara pode ajudar a eliminar os receios dos funcionários sobre o monitoramento de correio eletrônico e esclarecer as expectativas.

A organização reserva-se do direito de propriedade exclusiva das máquinas e domínios para ter acesso às correspondências dos empregados, podendo esta suspender tais serviços sem notificação prévia. observando-se alguns critérios:

- Os endereços eletrônicos devem ser de propriedade do empregador;
- Caso haja suspeita de um crime de vazamento de informações sigilosas da empresa, esta dispõe do poder de investigação, para confirmar o delito e aplicação das sanções disciplinares conforme legislação apresentadas no item 4.1.10.

Para que a organização se proteja contra a falta de legislação específica quanto ao processo disciplinar à utilização inadequada do correio eletrônico

estão definindo normas disciplinares no qual os funcionários devem estar adeptos àutilização deste ser viço.

Este tópico aborda as formas de utilização do correio eletrônico organizacional, abrangendo aspectos operacionais que devem ser pré-definidos. Tais como:

1. Definição da quantidade de destinatários que deverão receber a mensagem enviada (evitando assim grandes listas);

2. Qualquer tipo de avisos, convites, mensagens, advertências de alertas; devem ser enviados para o endereço eletrônico do setor responsável pela comunicação social da organização (comunicado@led.ufsc.br – Depto de Comunicação Social);

3. Informar a todos os colaboradores recém contratados sobre as políticas e sanções relacionadas ànorma em questão (treinamento do corpo funcional);

4. Estabelecer os privilégios padrões (logon à rede corporativa, senhas, permissões de acesso etc.) para usuários dos serviços de correio eletrônico;

5. Criar critérios para que, ao ser enviado uma correspondência eletrônica, o ID's (identificação do usuário) seja diferenciado (por exemplo: Ludmila. Uneb – Coordenação de Mestrado);

6. Estabelecer uma área pública no qual os usuários possam adquirir cópia de formulários padrões, Boletins informativos, dentre outros. Visando assim uma padronização nos serviços corporativos; sendo que:

a) Áreas Públicas: São áreas onde é permitido acesso para o público em geral;

b) Este serviço será de responsabilidade da administração do serviço;

c) Os conteúdos disponíveis não poderão ser modificados, adaptados ou publicados, sendo que estes estão disponíveis apenas com a finalidade de divulgar, distribuir e promover os serviços organizacionais.

7. Definir procedimentos de segurança (encriptografia) para envio /recebimento de mensagens eletrônicas, sendo que, internamente não se deva utilizar nenhum tipo;

8. Informar aos colaboradores que os acessos a qualquer serviço de correio eletrônico deverão ser relevantes para finalidades do trabalho;

9. Definir e divulgar aos usuários que a organização reserva para si o direito de monitorar quaisquer arquivos armazenados, recebidos e enviados através de correio eletrônico, tendo como finalidade avaliar o cumprimento da norma;

10. Divulgar aos seus usuários que a administração dos serviços de correio eletrônico poderá cancelar senha, conta ou utilização do serviço a qualquer momento sem aviso prévio.

### 4.1.3 A informação Organizacional

Para que a organização estabeleça expectativas claras sobre privacidade, de acordo, com a norma, o correio eletrônico do funcionário é considerado propriedade da empresa e pode ser lido por qualquer motivo. Entretanto, a sua empresa pode tratar a questão da privacidade de outra maneira. É importante que as pessoas saibam como o monitoramento de correio eletrônico pode afetar a sua privacidade.

As empresas além de se preocupar com a proteção de seus recursos de infra-estrutura, se preocupam com a sua reputação, propriedades e

funcionários. As vantagens das soluções de filtragem de conteúdo de correio eletrônico são:

- Proteção contra perda de propriedade intelectual.

A perda de propriedade intelectual é uma séria ameaça à empresa. Sendo necessário uma preocupação maior com as informações de propriedade intelectual (internas ou forma do ambiente corporativo).

- Limitando responsabilidades

Utilização de monitoramento para controlar e provar a utilização de materiais de assédio sexual e discriminação racial.

- Garantindo a credibilidade do cliente e a reputação da empresa.

A empresa deve preocupar-se com a proteção da informação, principalmente quando se tratar de comunicação com o fornecedor. Podendo causar, por exemplo, um questionamento no recebimento de vírus via transmissão eletrônica de dados, através do serviço de correio eletrônico, causando com isso desconfortos relacionado à credibilidade e reputação da organização em caso de operações comerciais mais sólidas.

- Mantendo a produtividade dos funcionários.

Os funcionários não são relapsos, mas o custo de enviar mensagens eletrônicas para os amigos e a família durante o expediente de trabalho pode ser cumulativo.

- Melhorando o desempenho da rede.

Mensagens eletrônicas não relacionadas ao trabalho podem consumir a largura de banda. Vírus e outros códigos maléficos podem se infiltrar na rede através de sistemas de correio eletrônicos não monitorados.

### 4.1.4 Proteção da Informação

Diariamente, ocorrem interceptações de informações via correio eletrônico, portanto, deve-se proteger os dados corporativos como segredos, propriedades ou informações privadas.

Informações como: números de Cartões de Crédito de clientes, números telefônicos, senhas de acesso, informações confidencias, dentre outros; não devem ser enviados para fora do ambiente corporativo, salvo em situações excepcionais e com autorização prévia do chefe imediato (através de utilização do método de segurança aprovado pela organização).

Um dos métodos de privacidade mais utilizados é o *Pretty Good Privacy* - PGP, algoritmo de criptografia ou outro meio de transmissão com segurança de dados através da Internet.

Esta norma não prevê definição de utilização de criptografia de dados, sendo que de acordo com o termo de responsabilidade de utilização do serviço de correio eletrônico organizacional, os usuários estão cientes de que quaisquer tipos de informação contidos nos servidores de correio eletrônicos estão sendo gerenciados por um software de monitoramento eletrônico.

Para tanto é valido destacar que:

- Todo o usuário é responsável pelo armazenamento de suas informações e mensagens corporativas;

- O usuário deverá armazenar e manter cópias de backup de todas as mensagens enviadas e recebidas e/ou armazenadas em seu poder;

- Qualquer troca de informações com clientes externos, não é autorizada, a não ser com autorização prévia do supervisor imediato e liberação pelos administradores dos serviços de correio eletrônico;

- É expressamente proibido o recebimento e a instalação de softwares a não ser os homologados pela organização;

- O administrador do serviço de correio eletrônico é responsável pela segurança e privacidade dos servidores corporativos, conforme termos contratuais estabelecidas com o usuário (funcionários);

-Qualquer tipo de problema relacionado à segurança de correio eletrônico deverá o usuário informar àadministração dos serviços de correio eletrônico;

-As mensagens de correio eletrônico que contém materiais fraudulentos, ou obscenos, serão filtradas pelo software de monitoramento e no qual será realizada apuração do emitente, assim como aplicação de sanção disciplinar;

-As mensagens que não forem mais de interesse da organização deverão ser apagadas das caixas postais periodicamente pelos usuários, devendo para isto realizar backup antes de tal procedimento.

### 4.1.5 Uma Questão de Privacidade

As mensagens eletrônicas organizacionais são de propriedade exclusiva da organização, não podendo o usuário do serviço deter a privacidade de sua conta, ou seja, qualquer informação armazenada em sua conta, ficará disponível ao administrador de correio eletrônico da organização ou setor com esta atribuição para o devido monitoramento, devendo ser aplicadas:

-Em casos de danos morais e/ou materiais causados por usuários de correio eletrônicos a terceiros ou à organização, os conteúdos das contas de correio eletrônico organizacional poderão estar disponíveis a uma investigação policial;

- Os usuários não devem interceptar ou abrir qualquer tipo de mensagem eletrônica a não ser a sua própria;

- A utilização de correio eletrônico para envio de correspondência, além dos domínios corporativos, será permitido apenas os que defendem o interesse da organização;

-Os usuários de correio eletrônico não devem revelar ou tornar públicas as informações confidenciais, tais como: informações financeiras, novas idéias de produtos, planos estratégicos, banco de dados ou partes, senhas de acesso à rede de computadores, dentre outros;

-O *logon* aos serviços de correio eletrônico é de propriedade exclusiva do usuário, devendo este não revelar a nenhum outro empregado.

### 4.1.6 A Utilização dos Recursos Computacionais

Os recursos computacionais deverão ser utilizados para uso exclusivo dos interesses da organização.

Nesta mesma linha de raciocínio não é permitida a utilização de correio eletrônico para: jogos (download de jogos e jogo contra oponentes através da rede), participação em grupos de notícias, ou outras atividades relacionadas ao interesse pessoal do usuário.

Diante de tais fatores é justo que a organização queira saber como os seus recursos estão sendo utilizados.

É importante ressaltar que o uso de quaisquer recursos computacionais da organização para fins ilegais; está o funcionário sujeito a demissão sem prejuízo de medidas cíveis e criminais cabíveis.

### 4.1.7 Controle de Acesso

Todo o usuário do serviço de correio eletrônico tem que se autenticar a um servidor de correio eletrônico. Essa autenticação dever ser realizada através de uma senha, a qual identificará todas as suas permissões de acesso, inclusive para acesso a serviço de correio eletrônico via web quando disponível pela organização.

Ao ser efetivado no quadro funcional da organização, o usuário receberá uma senha e uma identificação de conta, devendo o mesmo estar ciente que:

- Uma conta de correio eletrônico não deve ser utilizada por outro usuário, sendo este responsável pelo uso de sua conta, inclusive sua proteção;
- Qualquer tentativa de utilização dos serviços de correio eletrônico com intenção ilegal ou ato doloso, ou qualquer outra tentativa de privar que outros usuários a utilizem pode ser aplicada a sanção disciplinar;
- É responsável por manter a confiabilidade da senha e da conta e além de todas as atividades realizadas com elas;
- Concorda em notificar a administração do serviço de correio eletrônico sobre qualquer uso não autorizado de sua senha ou conta;

- Ao sair de sua conta, ao final de cada sessão deverá garantir que a mesma não seja acessada por pessoa não autorizada;

- Reconhece que os critérios, práticas gerais e limites relacionados à utilização do serviço são exclusivos da organização, tais como:

a) número máximo de dias que os conteúdos estarão disponibilizados no serviço de correio eletrônico;

b) Número máximo de mensagens que podem ser enviadas ou recebidas pelo usuário;

c) Quanto àutilização de espaço no servidor organizacional, definir a cota máxima de armazenamento a ser utilizada por caixa postal.

- O usuário reconhece que as letras a,b e c do parágrafo anterior poderão ser modificadas pela organização a qualquer momento, a seu exclusivo critério com ou sem notificação.

### 4.1.8 Responsabilidades

Neste tópico serão expostos os deveres que os usuários dos serviços de correio eletrônico devem seguir:

- Realizar prevenção com software de antivírus de qualquer arquivo recebido através de sua caixa postal;

- Não enviar mensagens de interesse particular através do serviço de correio eletrônico institucional, exceto com autorização prévia;

- Não enviar ou divulgar o seu endereço de correio eletrônico institucional, em listas de discussões, chat, news, sites de compras, dentre outros;

- No envio de mensagens externas (quando autorizado) utilizar os meios corretos para o envio seguro de dados homologados pela organização;

- Zelar pela integridade dos dados organizacionais de sua responsabilidade (memorandos internos, contratos, planilhas gerenciais, dentre outros.);

- Manter o controle e uso exclusivo de suas senhas; e não a revelar para outras pessoas;

- Não baixar através de correio eletrônico, arquivos anexos oriundos de redes externas;

- Não divulgar através de correio eletrônico corporativo qualquer tipo de software aos usuários, a não ser aqueles homologados pela organização;

- Não enviar através do serviço de correio eletrônico, alertas de vírus, cavalos de tróia ou qualquer outro código, arquivo ou programa de computador com a intenção de limitar, interromper ou destruir a funcionalidade de qualquer computador ou equipamento de software, hardware ou telecomunicações; caso haja suspeitas remeter mensagem apenas para o responsável do mesmo para que sejam tomadas as devidas averiguações;

- É proibida qualquer tentativa de teste ou de burla dos dispositivos de segurança adotada pela organização;

- Não divulgar, enviar, transmitir ou de qualquer outra forma disponibilizar qualquer conteúdo que seja ilegal, vexatório, difamatório, invasivo à privacidade, abusivo, ameaçador, prejudicial, vulgar, obsceno, injurioso, preconceituoso ou de qualquer forma censurável através do serviço;

- Não forjar “Headers” ou de qualquer outra forma manipular identificadores com objetivo de disfarçar a origem de qualquer conteúdo transmitido, através do correio organizacional;

- Não divulgar, enviar, transmitir ou de qualquer outra forma disponibilizar qualquer conteúdo, seja em virtude de compromisso legal, contratual ou de confiança (informações internas, exclusivas ou confidenciais);

- Não divulgar, enviar, transmitir ou disponibilizar qualquer tipo de propaganda ou material não autorizado ou solicitado (“junk mail” ou “SPAN”), correntes, esquemas pirâmides ou qualquer outra forma de apelo;

- Não interferir ou interromper, servidores ou redes conectadas ao serviço de correio eletrônico organizacional;

- Não obter ou tentar obter acesso não autorizado a outros sistemas ou redes de computadores conectados ao serviço de correio eletrônico;

- Não desobedecer qualquer regra, procedimento, política ou regulamento de sistemas ou redes conectadas ao serviço de correio eletrônico organizacional;

- Não violar, intencionalmente ou não, qualquer lei ou regulamento aplicado para utilização do correio eletrônico organizacional;

- Não assediar terceiros através de correio eletrônico organizacional;

- Não obter ou armazenar dados pessoais de outros usuários, inclusive informações financeiras;

- Não divulgar informações sobre produtos ou serviços de natureza particular ou de outras empresas;

- Não divulgar material de natureza político-partidária ou sindical.

### 4.1.9 Termo de Responsabilidade para Utilização de Correio Eletrônico

O propósito do termo de responsabilidade é adquirir do empregado após orientação sobre a norma de utilização de correio eletrônico da organização (Anexo 2) seu conhecimento através de uma assinatura de punho, no qual o mesmo reconhece e concorda que:

- A qualquer hora e sem aviso prévio a corporação tem direito de monitorar as informações das mensagens eletrônicas das caixas postais corporativa;
- Têm conhecimento que os serviços de correio eletrônico são de propriedade exclusiva da organização, e que deve utiliza-lo apenas para os seus propósitos;
- Em qualquer caso de violação dos procedimentos pré-estabelecidas nesta norma, estando sujeito às penalidades disciplinares e até demissão;
- Recebeu cópia, leu e obteve todos os esclarecimentos sobre as normas de utilização de correio eletrônico desta organização;
- Utilizará etiquetas de rede ao envio de correio eletrônico no ambiente corporativo, conforme material disponibilizado por esta organização ;
- Não utilizar os recursos de correio eletrônico para qualquer propósito legal;
- Não receberá arquivos ou mensagens de rede externas e que a administração de correio eletrônico terá direito de retirar do serviço qualquer conteúdo que viole esta norma;

- A organização monitore os conteúdos da caixa postal e que também poderá divulga-lo em casos de:

- Cumprimento de disposição legal

- Fazer cumprir os termos desta norma

- Responder a reclamações de conteúdos que viole direitos de terceiros.

- Proteger direitos, propriedades, interesses ou manter a segurança da organização ou terceiros.

- A organização não será responsável de forma alguma por qualquer conteúdo, perda ou dano de qualquer espécie resultante de conteúdos recebidos ou de qualquer outra forma disponibilizada através do serviço de correio eletrônico, cabendo-lhe sim apuração dos fatos e aplicação de medidas disciplinares;

- Em indenizar e insentar a organização, diretores e empregados, de qualquer perda, despesas, danos, reclamações, ou reivindicações, incluindo custos judiciais e honorários advocatícios:

- Quanto àutilização dos conteúdos fornecidos pelo usuário
- Má Utilização do serviço de correio eletrônico pelo usuário
- Conexão do usuário ao serviço
- Violação do termo de utilização do serviço de correio eletrônico

- A organização poderá cancelar a senha, conta ou utilização do serviço de correio eletrônico. Remover ou apagar qualquer conteúdo do serviço nos seguintes casos:

- A qualquer instante e por qualquer motivo, a critério exclusivo da organização, sendo que o serviço é de propriedade exclusiva dela

- Se a organização identificar qualquer tipo de violação ou uso imprudente com os termos desta norma de utilização de correio eletrônico
- Se o usuário tiver violado os direitos da organização e seus usuários
- Caso o usuário seja desligado da organização.

### 4.1.10 Aspectos Legais

Uma legislação deve evoluir de acordo com as necessidades da sociedade. Porém a legislação atual aparentemente é elaborada para que o país não evolua. As leis não são criadas para amarrar o país à época de sua edição, mas para orientar o presente e o futuro da nação, dentro de princípios fundamentais para o bem da pátria e da sociedade.

Tais leis estão muito defasadas e não conseguem atender a determinadas necessidades no que refere a novas tecnologias.

O poder judiciário quando se depara com situações inusitadas, oriundas das conseqüências da informática e da atual tecnologia no direito e na sociedade, pode na maioria das vezes, utilizar-se de aplicação de regra e utilização de pareceres técnicos fornecidos por peritos da área de informática no auxílio da resolução de um fato criminoso.

As legislações sobre proteção do consumidor e de direitos de propriedade intelectual devem ser aperfeiçoadas. O avanço tecnológico tem papel decisivo a desempenhar neste sentido. Este aperfeiçoamento pode ser alcançado através de programas que:

- Bloqueie conteúdos impróprios e lesivos;
- Garantam a segurança na transmissão de dados;

- Sistemas inteligentes que localizem e identifiquem o banditismo;

Utilizando normas legais já existentes há muito tempo ou pertinentes e adaptável aos novos casos que vem surgindo em razão da informática quer através de analogia e do incentivo ao trabalho legislativo específico, quando inevitáveis utilizando-se de “equivalentes jurisdicionais”.

As organizações podem justificar a monitoração de correio eletrônico de seus funcionários protegidos pelos artigos do código penal: 151, 153, 154, 171, 325 e Lei 6.538 art 41 (Anexo II).

As organizações podem responsabilizar o funcionário pela divulgação de qualquer tipo de material obsceno, incitante ao crime ou de conteúdo discriminatório através do correio eletrônico, podendo este material eletrônico comprometer a imagem e integridade da empresa ou terceiros. Estando as mesmas protegidas pelos artigos do código penal : 234, 286, 287 e Lei 4.117/62 art 53-h (Anexo II).

Caso o funcionário venha a utilizar os recursos da empresa (correio eletrônico, energia elétrica, tráfego de rede, espaço em servidores, dentre outros), a não ser para os interesses da empresa estão os mesmos sujeitos às penalidades previstas pelos artigos do código penal: 155, 163, decreto lei 3.688/41 art 65, Lei 8.069/90 art 241, Lei 5.520/67- art 17 e 21, Código Tributário Nacional art 138, CLT art 482, portaria 862/2001, e das penalidades cabíveis pela não observância dos compromissos assumidos, Lei 9.983/2000 art 1º , partes do Decreto Lei 2.848/40. (Anexo II)

## 4.2 Documentação a ser Disponibilizada para o Usuário

### 4.2.1 Introdução

O correio eletrônico é um sistema eletrônico semelhante ao serviço de correios que conhecemos e que serve para enviar e receber dados eletrônicos. Utiliza-se uma caixa postal eletrônica simbolizada por um endereço eletrônico fornecido pela organização (comunicacao@df.previdenciasocial.gov.br), sendo que todas as mensagens enviadas/recebidas ficam armazenadas nos servidores de e-mail até o momento em que você acesse sua caixa postal para baixa-lo para sua estação de trabalho ( utilizando o Outlook).

Através deste serviço você poderá enviar ou receber textos, arquivos, gráficos, som, vídeo, imagens. Agilizando com isso suas rotinas operacionais, processos e controles gerenciais.

### 4.2.2 Objetivo

Estabelecer critérios para a utilização de correio eletrônico corporativo.

### 4.2.3 Aplicação

Esta norma aplica-se a todos os funcionários cadastrados no serviço de correio eletrônico.

### 4.2.4 Finalidade do Serviço

#### 4.2.4.1 Associação com a atividade fim da empresa

Este serviço visa propor ao corpo funcional uma maior agilização na comunicação interdepartamental e clientes internos e externos. Sendo este reservado para uso exclusivo de interesse da organização.

Só poderão trafegar neste canal informações relevantes ao bom desempenho da atividade funcional de cada colaborador. Tendo estes que atentar às normas de utilização deste serviço.

### 4.2.5 Regras de Utilização

Todos os usuários deste serviço deverão usar procedimentos de utilização para que usufruam ao máximo os recursos disponíveis para melhorar suas atividades fins.

Os mesmos deverão estar cientes e adeptos aos subitens 4.2.5.1, 4.2.5.2, 4.2.5.3 e 4.2.5.4.

#### 4.2.5.1 Recomendações a serem aplicadas durante o uso

O usuário do serviço de correio eletrônico deverá ter bons modos, utilizando comportamento sadio, para o envio de mensagens eletrônicas.

Ao transmitir mensagens os usuários não deverão incomodar, atrapalhar ou agredir outros usuários. Para tal aconselha-se utilizar algumas precauções ao enviar ou receber mensagens eletrônicas:

I. Considere que as mensagens na Internet não são seguras - nunca escreva numa mensagem qualquer coisa que não pode ser escrita num cartão postal. Caso contrário utilize algum dispositivo de encriptação (por software ou hardware);

II. Se você está retransmitindo uma mensagem recebida - não mude o texto. Se a mensagem foi endereçada pessoalmente a você e deseja retransmiti-la, você pode "encurtar" a mensagem e copiar passagens importantes;

III. Nunca envie “corrente" por e-mail - de acordo com a política da empresa seus privilégios de acesso ao serviço de correio eletrônico podem ser suspensos;

IV. Não envie arquivos atachados com vírus em seus e-mails;

V. Não deve enviar mensagens "Grosseiras" mesmo quando provocado. Por outro lado, não se surpreenda se você for "atacado" e, mesmo assim, é prudente que não responda àmensagem;

VI. Cheque o assunto - de todas as mensagens antes de responder, às vezes uma pessoa que pede ajuda (ou explicações) manda outra mensagem que diz, efetivamente, "esqueça a primeira mensagem";

VII. Não use e-mail de outras pessoas - respeito a privacidade de cada um;

VIII. Seja cuidadoso ao enviar mensagens - envie mensagens para endereços que você conhece;

IX. Preste atenção no campo de cópias da mensagem (CC - "carbon copy")- informações gerais devem ser enviadas para o seu superior imediato com cópia para os demais interessados;

X. Não envie mensagens não solicitadas - pedindo informações a pessoas cujo e-mail você viu "por aí". Procure os administradores do serviço de Correio para esclarecimentos;

XI. Ao sair de férias - informe ao administrador para que ele possa fechar sua caixa postal ou redirecione-o para a caixa postal de outra pessoa (Se você assume uma função de chefia solicite que redirecione sua caixa postal para o seu substituto);

XII. Verifique todos os endereços para os quais está mandando mensagens longas ou pessoais - é de bom tom colocar a palavra LONGO ("Long") na linha do assunto da mensagem ("subject") para que o destinatário saiba que a mensagem exigirá algum tempo para ler e responder (Uma mensagem com mais de 100 linhas de texto é considerada muito longa);

XIII. Nunca coloque mais de **65** caracteres numa linha - termine toda linha com um <ENTER> ("retorno de carro").

XIV. Quando com problemas de software e sistemas - Cheque com pessoas próximas quem pode ajudá-lo. Também saiba a quem recorrer no caso de qualquer material questionável ou ilegal.

XV. Use letras maiúsculas e minúsculas normalmente - ESCREVER TUDO EM MAIÚSCULAS É COMO SE ESTIVESSE GRITANDO!

XVI. Limpe sua lixeira constantemente - liberando mais espaço de sua caixa postal e agilizando a comunicação;

XVII. Use alguns símbolos para dar ênfase. Por exemplo, *assim*.

XVIII. Não utilize “smileys” :-) - é um exemplo de "smiley" (olhe de lado),

XIX. Não envie arquivos pornográficos e/ou engraçadinhos

XX. Quando receber uma mensagem que o perturbou muito, primeiro esfrie a cabeça antes de responde-la;

XXI. Não utilize acentos, caracteres de controle ou anexos que não sejam ASCII;

XXII. Ao responder a uma mensagem - inclua pequenas partes da mensagem original para ser entendido. Retire as partes que não são importantes;

XXIII. Jamais assine o seu e-mail organizacional - em lojas virtuais e/ou listas de discussões;

XXIV. Se você usa uma assinatura faça-a curta - regra prática: não mais do que 04 linhas. É importante que se coloque o nome completo, cargo, setor e telefone para futuros contatos;

XXV. Mensagens de e-mail não são seguras - Mensagens (e notícias em news) estão sujeitas à falsificações mais ou menos sofisticadas. Use o bom senso antes de concluir pela autenticidade de uma mensagem.

XXVI. Se uma mensagem recebida for muito importante - responda imediatamente para que o emitente saiba que você a recebeu e, depois, mande uma resposta mais elaborada;

XXVII. Seja cuidadoso com gírias - palavrões e siglas locais;

4.2.5.2 Regras gerais e responsabilidades

**Das Regras Gerais**

1. A Coordenação de Informática ou setor responsável pelo serviço de correio eletrônico atuarão como Supervisores de Segurança de Acesso, com as seguintes atribuições no seu âmbito de atuação:

I orientar a execução das atividades de cadastramento e habilitação, assim como os usuários nos aspectos relativos àsegurança de acesso ao serviço;

II fiscalizar o cumprimento das normas de utilização do serviço, através de ferramentas específicas;

III apurar irregularidades envolvendo acesso não-autorizado e violação de informação no âmbito corporativo e relatá-las à administração do serviço de correio eletrônico.

2. A administração do serviço de correio eletrônico deverá:

I propor diretrizes para a norma de utilização de correio eletrônico

II coordenar a implantação de ferramentas de monitoramento eletrônico, evitando assim evasão de dados corporativos;

III avaliar, propor e acompanhar a adoção de medidas corretivas nos casos de violação da informação organizacional.

IV promover programas visando à divulgação das normas de utilização de correio eletrônico, principalmente no que tange à propriedade e responsabilidade dos usuários;

V Realizar prevenção com software de antivírus de qualquer arquivo recebido através de sua caixa postal;

VI monitorar os conteúdos da caixa postal e que também poderá divulga-lo em casos de:

1. Cumprimento de disposição legal
2. Fazer cumprir os termos desta norma
3. Responder às reclamações de conteúdos que viole direitos de terceiros.

4. Proteger direitos, propriedades, interesses ou manter a segurança da organização ou terceiros.

**Das Responsabilidades**

É responsabilidade de todos os usuários dos serviços de correio eletrônico:

I - cuidar da integridade, confidencialidade e disponibilidade de dados e informações, devendo comunicar por escrito aos gestores de sistema quaisquer irregularidades, desvios ou falhas identificadas.

II - É proibido enviar dados ou informações a pessoas não-autorizadas ou que, legalmente, não tenham direito ao seu conhecimento.

III - Os usuários devem manter suas senhas de acesso secretas e intransferíveis, devendo trocar ou providenciar a troca de sua senha quando houver suspeita, indício ou conhecimento de que a mesma foi violada ou revelada a terceiros.

IV - O titular da senha é obrigado a:

a) Zelar pelo seu sigilo absoluto;

b) Utilizar os serviços de correio eletrônico apenas para necessidade de serviço;

c) Manter a necessária cautela quando da exibição de dados em tela, impressora, na gravação em meios eletrônicos ou em qualquer outra circunstância, a fim de evitar que pessoas não autorizadas deles possam tomar ciência;

d) Não abandonar ou afastar-se do microcomputador sem que antes tenha encerrado a sessão de sua caixa postal, de modo a evitar que terceiros não autorizados a ele tenham acesso.

V - Não enviar mensagens de interesse particular através do serviço de correio eletrônico institucional, exceto com autorização prévia;

VI - Não revelar fato ou informação de qualquer natureza de que tenha conhecimento por força de suas atribuições, salvo em razão de serviço ou em decorrência de decisão de autoridade competente;

VII - Não enviar ou divulgar o seu endereço de correio eletrônico institucional, em listas de discussões, chat, news, sites de compras, dentre outros;

VIII - No envio de mensagens externas (quando autorizado) utilizar os meios corretos para o envio seguro de dados homologados pela organização;

IX - Zelar pela integridade dos dados organizacionais de sua responsabilidade (memorandos internos, contratos, planilhas gerenciais, dentre outros.);

X - Manter o controle e uso exclusivo de suas senhas; e não a revelar para outras pessoas;

XI - Não baixar através de correio eletrônico, arquivos anexos oriundos de redes externas;

XII - Não divulgar através de correio eletrônico corporativo qualquer tipo de software aos usuários, a não ser aqueles homologados pela organização;

XIII - Não enviar através do serviço de correio eletrônico, alertas de vírus, cavalos de tróia ou qualquer outro código, arquivo ou programa de computador com a intenção de limitar, interromper ou destruir a funcionalidade de qualquer computador ou equipamento de software, hardware ou telecomunicações; caso

haja suspeitas remeter mensagem apenas para o responsável do mesmo para que sejam tomadas as devidas averiguações;

XIV - É proibida qualquer tentativa de teste ou de burla dos dispositivos de segurança adotada pela organização;

XV - Não divulgar, enviar, transmitir ou de qualquer outra forma disponibilizar qualquer conteúdo que seja ilegal, vexatório, difamatório, invasivo à privacidade, abusivo, ameaçador, prejudicial, vulgar, obsceno, injurioso, preconceituoso ou de qualquer forma censurável através do serviço;

XVI - Não forjar “Headers” ou de qualquer outra forma manipular identificadores com objetivo de disfarçar a origem de qualquer conteúdo transmitido, através do correio organizacional;

XVII - Não divulgar, enviar, transmitir ou de qualquer outra forma disponibilizar qualquer conteúdo, seja em virtude de compromisso legal, contratual ou de confiança (informações internas, exclusivas ou confidenciais);

XVIII - Não divulgar, enviar, transmitir ou disponibilizar qualquer tipo de propaganda ou material não autorizado ou solicitado (“junk mail” ou “SPAN”), correntes, esquemas pirâmides ou qualquer outra forma de apelo;

XIX - Não interferir ou interromper, servidores ou redes conectadas ao serviço de correio eletrônico organizacional;

XX - Não obter ou tentar obter acesso não autorizado a outros sistemas ou redes de computadores conectados ao serviço de correio eletrônico;

XXI - Não desobedecer qualquer regra, procedimento, política ou regulamento de sistemas ou redes conectadas ao serviço de correio eletrônico organizacional;

XXII - Não violar, intencionalmente ou não, qualquer lei ou regulamento aplicado para utilização do correio eletrônico organizacional;

XXIII - Não assediar terceiros através de correio eletrônico organizacional;

XXIV - Não obter ou armazenar dados pessoais de outros usuários, inclusive informações financeiras;

XXV - Não divulgar informações sobre produtos ou serviços de natureza particular ou de outras empresas;

XXVI - Não divulgar material de natureza político-partidária ou sindical.

**Parágrafo Único:** O não-cumprimento às disposições destas regras caracterizará infração funcional, a ser apurada em processo administrativo disciplinar, sem prejuízo da responsabilidade penal e civil.

4.2.5.3 Termo de Responsabilidade

Esta norma é passada a todos os funcionários recém contratados, junto com todas as informações de acesso ao serviço de correio eletrônico. Após esclarecimentos de todas as dúvidas o funcionário assina o um termo para utilização do serviço eletrônico, no qual este se compromete a seguir todas as normas e que também está sujeito a penalidades administrativas, penal e civil em caso de descumprimento (anexo II).

4.2.5.4 Penalidades Previstas

Os usuários do serviço de correio eletrônico, que não cumprirem o expresso nesta norma, ou por qualquer outro motivo causar prejuízos, materiais ou

morais, a organização ou a terceiros estarão sujeitos a aplicação das leis descritas no (Anexo II).

### 4.2.6 Dicas de Uso

#### 4.2.6.1 Descrição dos procedimentos para acesso as informações necessárias para melhor aproveitamento da ferramenta

Os usuários do serviço de correio eletrônico poderão esclarecer suas dúvidas da seguinte forma:

1. através da documentação disponível no site da Intranet da organização (http://www.correio-eletrônico );
2. Através do suporte da área responsável pela administração do serviço.
3. Através da central de atendimento ao usuário.

#### 4.2.6.2 Tráfego de Dados

Só poderão trafegar neste canal informações relevantes ao bom desempenho da atividade funcional.

### 4.2.7 Propriedades do correio eletrônico

#### 4.2.7.1 Dos recursos e Utilização

Os recursos informáticos disponibilizados são de uso e direito exclusivo da organização, assim como a utilização dos recursos para monitoramento de todas as informações que trafegam neste ambiente.

4.2.7.2 Definição das cotas de envio, recebimento e armazenamento de mensagens.

A quota definida para o armazenamento de utilização dos serviços de correio eletrônico é de 1,5 MB tanto para envio, quanto para recebimento de mensagens. Dentro deste aspecto, os executivos, gerentes e supervisores terão suas capacidades de armazenamento definida de acordo com o fluxo de informações.

O usuário caso usufrua o Webmail corporativo, deverá ter acesso a partir do mesmo controle de acesso corporativo.

4.2.8 Do Monitoramento do Serviço de Correio Eletrônico

I – Será utilizado para monitorar os dados corporativos que trafegam dentro do ambiente corporativo, evitando assim, a evasão de dados corporativos;

II – Gerenciamento das informações que trafegam na rede corporativa seja pública dentro do ambiente corporativo e de propriedade exclusiva da organização, garantindo que o interesse particular não se sobressaia sobre o público.

## 4.3 Monitoramento Eletrônico

Para que as organizações garantam o gerenciamento das normas pré-definidas neste trabalho, devem utilizar software para a monitoração de correio eletrônico, garantindo a integridade da informação dentro do ambiente corporativo, ou seja, o funcionário utiliza o serviço de correio eletrônico organizacional e seus recursos, porém, não detêm a privacidade de sua caixa

postal. A mesma só deve ser utilizada para fins de interesse da organização e para melhor desempenhar suas atividades funcionais.

Segundo pesquisa realizada pela A.M.A (American Management Association), publicada em abril/2000, 38% das organizações americanas entrevistadas monitoram as atividades de funcionários, envolvendo comunicações por correio eletrônico. Sendo que dentre as que não utilizam, 21% planejam implementar esta ferramenta durante o ano de 2000/2001.

Recentemente, no Brasil está havendo um crescimento na utilização desta ferramenta, porém, a grande preocupação dos empregadores é a falta de ética e violação de leis devido a maus hábitos de seus funcionários, tendo como agravante a falta de legislações específicas para tratar o assunto.aa

A partir do monitoramento eletrônico pode-se ter o controle de um grande problema encontrado na maioria das organizações “Perda de produtividade”:

- Correios eletrônicos indesejáveis (Spam), contendo:
    - Propagandas, piadas, filosofia de vida/amor/amizade;
- Fotos, arquivos de áudio e vídeo;
- Correntes, pirâmides, receitas de riqueza;
- Notícias falsas de vírus;
- Incitação àdiscriminação;
- Utilização de correio eletrônico para interesses pessoais:
    - Correspondências com amigos e familiares;
    - Envio de mensagens relativas a negócios paralelos;
    - Envio de currículos para agências de emprego;
    - Dentre outros.

Além da grande perda com produtividade, isso ocasiona também a degradação na performance na rede local e perda monetária.

Em geral, a maior barreira para se monitorar correio eletrônico são os próprios funcionários. O Departamento de informática tem como objetivo aprimorar as operações. Desenvolver e comunicar uma política de uso de correio eletrônico na empresa é essencial para conseguir o suporte dos funcionários.

O Departamento de Informática e os representantes dos departamentos de recursos humanos e jurídicos devem estar envolvidos no desenvolvimento de uma política de correio eletrônico.

### 4.3.1 Protegendo sua Organização

A maioria das organizações não tem nenhum tipo de controle das informações corporativas. O monitoramento visa oferecer exclusão de arquivos pornográficos, jogos, materiais difamatórios etc.

A maioria delas estão tendo a necessidade de criar alternativas para se prevenir quanto ao abuso da utilização deste serviço, inclusive quanto à utilização do serviço para interesses pessoais e não corporativos.

O primeiro passo a ser tomado para proteger a organização contra perda de informação ou produtividade é definir uma norma de utilização do serviço de correio eletrônico, reservando inclusive o direito de revisar qualquer tipo de material enviado e/ou recebidos através dos recursos de correio eletrônico a qualquer hora através de monitoramento.

Tal monitoramento transmite aos usuários responsabilidades quanto à proteção das informações corporativas, direitos autorais, software e propriedade intelectual conforme acordado no item 4.1.9; assim como o cumprimento do item 4.1.8 contida nesta norma.

### 4.3.2 O que Monitorar?

O monitoramento de correio eletrônico é realizado para garantir a aplicabilidade das normas de utilização definidas no item 4.1.

Todas organizações têm seus próprios protocolos, mas geralmente, o interesse comum é monitorar situações como:

1. Mensagem com arquivos executáveis, que possam conter vírus, cavalos de tróia etc...
2. Mensagens com arquivos grandes que possam causar lentidão na rede;
3. Linhas com assuntos de designação “Encaminhar” (*FORWARDED*) que provavelmente aparecem várias vezes em uma mensagem remetendo ou recebendo piadas, correntes, Spams etc.
4. Arquivos confidenciais que não devem sair do ambiente corporativo;
5. Número de mensagens que o usuário envia e recebe que não sejam de interesse da organização;
6. Palavras que sugestionam a perda de produtividade intelectual como, por exemplo: “confidencial” ou “proprietária”;
7. Calúnias racistas ou palavras como “Sexo” ou “Negro”.

Para que o setor responsável pela segurança possa garantir a disciplina é necessário que esteja equipada com recursos necessários para tais fins.

O primeiro passo para um bom monitoramento é ter uma norma escrita e o segundo; e que haja o comprometimento do departamento de recursos humanos no processo disciplinar através de projeto de conscientização, treinamentos, palestras, informativos etc.

Além dos fatores acima, o controle do segredo organizacional e outras propriedades intelectuais levam ao monitoramento de conteúdos.

### 4.3.3 Softwares de Monitoramento Eletrônico

O monitoramento é realizado para garantir a aplicabilidade das normas de utilização dos serviços de correio eletrônico, definidas no item 4.1.

A principal função dos softwares de monitoramento é gerenciar o fluxo de mensagens de correio eletrônico e disciplinar o seu uso pelos funcionários. Estes fazem inspeção nas mensagens eliminando ou limitando o conteúdo que podem ser enviados por e-mail ou FTP, tornar o sistema sensível a palavras-chaves relacionadas ao sigilo e à segurança da empresa ou ao uso não profissional da rede, possibilitando com que o administrador tenha relatórios sobre o conteúdo que está trafegando pela sua rede.

A seguir são descritas as principais características encontradas nos softwares de gerenciamento de correio eletrônico:

1. Controlar o tráfego excessivo na rede;
2. Não permitir o envio de mensagens de conteúdo inadequado;
3. Gerenciamento de informações sigilosas;
4. Garante a prioridade a mensagens estratégicas;
5. Protege contra violações na segurança e ataques de spams;

6. Garante o bom andamento do trabalho na empresa;

7. Filtra conteúdo de e-mail inadequado, reduzindo a exposição a processos jurídicos.

As principais características dos softwares de Gerenciamentos propostas às organizações são:

1. Proteger as informações e preserva a largura de banda e a produtividade

- Verificação e filtragem abrangentes de mensagens eletrônicas e anexas baseadas em políticas para proteger as empresas de processos de responsabilização judicial;
- Examina os anexos das mensagens eletrônicas, até mesmo os compactados, em todos os formatos conhecidos, incluindo Microsoft®Word, Microsoft Excel, PowerPoint®,texto e Adobe® PDF;
- Protege as informações, aumenta a produtividade do usuário e preserva a largura de banda da rede.

2. Proteger a organização contra processos de responsabilidade civil

- Verifica o conteúdo à procura de palavras e frases inadequadas como, por exemplo, linguagem que indique preconceito sexual ou racial, ou de cunho obsceno. Protegendo a organização caso, por exemplo, uma funcionária seja molestada, através de mensagens enviadas a partir do serviço de correio eletrônico.

3 - Controlar o acesso dos usuários e o conteúdo das mensagens

- Os administradores podem definir permissões de acesso por usuário, por computador e por grupo, verificações de conteúdo personalizadas e políticas de filtro para todo o sistema;

- Criar dicionários ilimitados e listas de acesso permitido/negado para controlar a transmissão ou a recepção de mensagens eletrônicas nas caixas postais.

4 - Apresenta desempenho superior para empresas de qualquer porte

- Permite que os administradores limitem o número de conexões simultâneas à rede;
- O servidor pode ser configurado para atuar como gateway para filtrar mensagens, utilizando o filtro de modo conveniente, sem precisar reestruturar todo o sistema existente;
- Aplicar os filtros apropriados às mensagens recebidas e enviadas;
- Existem diversas ferramentas para monitorar os conteúdos de mensagens eletrônicas, conforme (quadro 4.1).

**Quadro 4.1: Softwares para monitoramento de correio eletrônico**

| | | | |
|---|---|---|---|
| Aspeon Software Inc.<br>*Exchange Plus* | Content Technologies Inc.<br>*MailSweeper* | Elron Software Inc.<br>*Elron CommandView*<br>*Message Inspector* | Marshal Software<br>*MailMarshal* |
| SRA International<br>*Assentor* | SurfWatch Software<br>*SurfWatch* | Tumbleweed<br>Communications Corp.<br>*- WorldSecure Mail* | Symantec Corp.<br>*MailGear* |
| Trend Micro Inc.<br>*ScanMail* | | | |

Recentemente, no Brasil, estão sendo oferecidos dois softwares de monitoramento: o Message Inspector (Elron software) e symantec mail gear (Symantec), veremos agora detalhes sobre as ferramentas de monitoramento de conteúdos mais utilizadas.

4.3.3.1 Message Inspector (Elron Software Inc)

Representada e distribuída no Brasil pela CLM Informática.

Em Brasília, o representante autorizado a Elron software é a Contrix informática Ltda.

O software está dividido em duas partes: uma que funciona em um computador cliente e outro no servidor.

**Requisitos**

**Servidor**

-Pentium II 350 MHz - 128 MB de memória RAM

-Windows NT (Server ou Workstation) com o service pack 5

-Endereço IP estático

-Duas placas de redes (10 Mbps, 10/100 Mbps ou 100 Mbps do tipo Ethernet)

**Estações**

-Pentium de 133 MHz e 32 MB de memória RAM

-Sistemas Operacionais Windows 9X ou NT Workstation ou o 2000 Professional.

**Compatibilidade**

- Lotus Notes, Novell ou Microsoft NT/2000, com o Exchange Server ou com servidores de mensagens que suportem o padrão SMTP.

**Pontos Fortes**

- Variedade de filtros.
- Gerenciamento por browser.
- Assegura política

- Vários tipos de varredura no conteúdo.

**Pontos Fracos** :

- Necessita de duas placas de rede no servidor.
- Não suporta dicionário em português.

4.3.3.2 Mail-Gear (Symantec Corporation)

Em Brasília, o representante autorizado a Symantec Corporation da revenda do Mail Gear é a Trueaccess Segurança corporativa.

**Requisitos de Sistema**

- **Navegadores Recomendados para Interface na Web:**
  - Netscape Navigator ® 4.0 ou posterior
  - Microsoft ® Internet Explorer 4.0 ou posterior
- **Clientes de e-mail**
  - Nenhum software de cliente exigido
  - Compatível com software Cliente de e-mail que aceite POP3 e SMTP (Eudora, Messenger etc).
- **Sistemas Operacionais**

1. Solaris - SPACR - baseado em servidor executando Solaris 2.6 ou posterior
2. Windows NT/2000
3. Red Hat Linux*

- **Hardware**

1. Intel ® Pentium ®
2. Memória de 128 MB, mínima

3. Unidade de CD ROM
4. Conexão àInternet TCP/IP
5. Mínimo de 25 MB para instalação.

É importante ressaltar que os requisitos de velocidade do processador, memória e espaço no disco variam conforme o volume de correio eletrônico a ser gerenciado pelo servidor.

# 5 .CONCLUSÕES E RECOMENDAÇÕES PARA FUTUROS TRABALHOS

## 5.1 Conclusões

Ao longo deste documento foram apresentados alguns conceitos que provavelmente deverão ser comuns a quem trabalha ou trabalhará com administração de serviços de correio eletrônico, e até mesmo, usuários leigos que buscam mais informações sobre o assunto.

Para realizar a implementação de um modelo piloto no que tange a normatização do serviço de correio eletrônico no âmbito institucional, a organização deverá iniciar primeiramente um trabalho de conscientização dos empregados para ficarem cientes das normas internas a serem implementadas promovendo:

- Seminários de conscientização objetivando esclarecer a importância do uso correto da tecnologia, o âmbito de trabalho e o impacto que o mau uso pode acarretar àorganização;
- Apresentação de orientações quanto às formas de envio de uma mensagem eletrônica (netiquetas) ver item 4.2.5.1.
- Divulgação do questionário da pesquisa a todo os usuários do serviço de correio eletrônico corporativo;
- Apresentação de palestras e elaboração de cartilhas que tratem a questão “Monitoramento Eletrônico” na organização;

- Elaboração de palestras sobre a norma de utilização do serviço , no qual são apresentadas as responsabilidades e sanções a que os usuários estão sujeitos;
- Divulgação da norma de utilização de correio eletrônico através da intranet e da administração do serviço;
- Colher assinaturas de ciência da norma de utilização de correio eletrônico, inclusive, o termo de responsabilidade de utilização;
- Disponibilização de conteúdos informativos e da própria norma de utilização em pastas públicas no serviço de correio eletrônico corporativo;

Propostas para capacitação dos usuários no que diz respeito a operacionalização da ferramenta, conhecendo melhor os recursos disponíveis e agilizando suas atividades funcionais. Necessidade esta mostrada pela pesquisa de utilização de correio eletrônico, nos quais 74% dos usuários informaram que não foram treinados para operacionalizar a ferramenta.

Em paralelo, a organização deverá realizar um trabalho para validação de uma ferramenta (ver item 4.2.4) que seja capaz de monitorar as mensagens enviadas e recebidas através do serviço de correio eletrônico. Visando assim, garantir a eficácia da norma e a proteção da propriedade (material e intelectual) da organização.

Como citadas no item 4.2.4 deste trabalho, as ferramentas de monitoramento eletrônicas têm a finalidade de gerenciar o fluxo de mensagens e disciplinar seu uso:

- Controlar o tráfego excessivo de dados;
- Não permitir o envio/recebimento de conteúdos impróprios;
- Gerenciamento das informações estratégicas;

- Proteger contra violação de segurança e SPAM e
- Filtrar e-mails inadequados.

É válido destacar, que a organização deve observar a questão de monitoramento com muita atenção, pois existe uma grande polêmica no que se diz respeito a direitos constitucionalmente garantidos.

De um lado a empresa tem garantido pela Constituição Federal o “Direito à propriedade” (CF,art.5º, XXII) e do outro garante ao cidadão o direito à intimidade e àprivacidade (CF, art. 5º , X,XII).

Como não existe uma lei específica a respeito do monitoramento eletrônico pelas organizações, assim como não há legislação para reger todos os novos tipos de relações jurídicas criadas com o advento e o progresso da informática. A organização pode resolver o conflito desses direitos constitucionalmente garantidos (propriedade X privacidade e intimidade), com um controle parcial do tráfego de informações e conscientização dos usuários, no objetivo de trazer maior segurança as suas informações.

Seguindo esta linha de raciocínio, a empresa pode corrigir as falhas detectadas através da pesquisa aplicada aos usuários do serviço, atuando dentro dos limites legais e constitucionais atualmente vigentes :

Através de uma normatização interna, abrangendo as formas de utilização do correio eletrônico permitidas, as proibidas; as penalidades administrativas aplicáveis aos infratores; os direitos e deveres dos usuários (ver item 4.2.5.2); as infrações que poderão vir a ensejar, além da responsabilização administrativa, a civil e/ou a penal.(Anexo I);

Do monitoramento generalizado, para fins estatísticos (e posterior campanha de conscientização dos empregados) e de futuras auditorias, caso necessário;

Obtenção do Termo de Responsabilidade de Utilização do serviço (Anexo II), assinado pelo funcionário, comprometendo-o a somente utilizar os recursos a ele disponibilizados para o exercício da sua atividade, com pena de multa e/ou demissão por descumprimento;

De Software de controle do uso do correio eletrônico nas estações de trabalho, atuando como Firewall Pessoal, protegendo as máquinas e, ao mesmo tempo, coletando dados que irão subsidiar a auditoria;

Monitoramento generalizado e impessoal dos acessos aos recursos do serviço de correio eletrônico e da própria Internet, gerando estatísticas de utilização veiculadas em uma campanha de divulgação interna;

Regras e critérios técnicos de uso, como: o volume máximo permitido para o tráfego de informações por e-mail, a inibição de acesso a determinados serviços da rede/Internet e ou endereços Web;

Todas essas ações são ótimos exemplos para iniciar o controle e potencializar o uso dos recursos do serviço de correio eletrônico, sem pôr em risco as valiosas informações que sustentam o negócio. E o mais importante, sem esquecer de garantir o direito do principal bem das empresas modernas: o capital intelectual.

Dentro da sistemática, legal e constitucional, vigente, de inviolabilidade da intimidade e de dados, não se vislumbra a possibilidade de monitoramento, por parte da empresa, de forma individual e irrestrita dos e-mails enviados e/ou

recebidos pelo empregado, sob pena de infringência de direitos fundamentais garantidos pela Constituição. Ademais, em caso de violação, por parte do empregado, das normas da empresa, existem os meios legais para que ele seja devidamente responsabilizado.

Diante deste quadro só pode-se aguardar que nossos legisladores disciplinem e regulamentem o monitoramento, com todas as suas particularidades e variantes, a fim de que sejam equilibradas as regras mestras para utilização de e-mails (Internet) na relação de emprego (e de forma geral), nivelando com ponderação e racionalidade os imprescindíveis e relevantes fatores: segurança e privacidade.

## 5.2 Recomendações para Futuros Trabalhos

Diante dos resultados obtidos e para melhor implementação da norma proposta pode-se sugerir:

1. Investigar os resultados decorrentes dos seminários de conscientização sobre o uso correto do correio eletrônico corporativo;

2. Analisar as implicações do monitoramento de serviço de correio eletrônico, filtrando assim, os fatores relevantes quanto àsegurança e privacidade;

3. Analisar o processo normativo do correio eletrônico corporativo;

4. Identificar o grau de satisfação quanto à implementação da norma de utilização, avaliando com isso, o nível de comprometimento do funcionário.

5. Criar uma legislação específica que trate o monitoramento eletrônico, garantindo assim, o direito de propriedade, definida na Constituição Federal.

## Referências Bibliográficas


Abranet. **Leia mais aqui sobre o "decreto" que os SPAMMERS brasileiros dizem**. Acessado em 05/12/200. Disponível em <http://portal.abranetrj.org.br/link.php3?cod_entidade=1&link=http://noticias.abranetrj.org.br/noticia.php3?chave=5>.

ALENCAR, Edgard; GOMES, Marcos Affonso Ortiz, **Metodologia de Pesquisa Social e Diagnóstico Participativo**, Editora: UFLA/FAEPE; 1998.

ALMEIDA, Marcus Garcia de. **Internet, Intranet e Redes Corporativas**. Editora: Brasport, 2000.

BERNSTEIN, Terry. **Segurança na Internet**. Rio de Janeiro: Campus, 1997.

BRASIL, Constituição (1988). **Constituição: República Federativa do Brasil**. Brasília: Senado Federal, Centro Gráfico, 1988.

BRASIL, Lei nº 2.572, de 20 de Julho de 2000. Dispõe sobre a prevenção das entidades públicas do Distrito Federal com relação aos procedimentos praticados na área de informática. **Câmara legislativo do Distrito Federal**. Disponível em <http://www.cl.df.gov.br/legislacao/legisoriginais/leisordinarias/2000/ldf-2000-02572.html> . Acesso em 21/10/2000.

BRASIL, Lei nº 9.983, de 14 de julho de 2000. Altera o Decreto-Lei nº 2.848, de 07 de dezembro de 1940 – Código Penal e dá outras providências. Publicada no **DOU** de 17.7.2000. Disponível em <http://www.presidencia.gov.br/ccivil_03/Leis/L9983.htm> . Acesso em 29/03/2001.

BRASIL. Decreto - Lei Nº 3.689, De 3 De Outubro De 1941**. Código de Processo Penal.** Acesso em 22/02/2001. Disponível em <http://www.presidencia.gov.br/ccivil_03/Decreto-Lei/Del3688.htm>.

BRASIL. Decreto Lei nº 2.848, de 7 de dezembro de 1940, regulamenta o art. 180 da Constituição Federal. Trata dos crimes contra a pessoa. **Código Penal Brasileiro**.

BRASIL. Lei 4.117/62. **Institui o código Brasileiro de Telecomunicações, estabelecendo preceitos para os serviços de telecomunicações no**

**Território Nacional**.art 53-h. Acesso em 16/03/2001. Disponível em <http://www.presidencia.gov.br/ccivil_03/Leis/L4117.htm>.

BRASIL. Lei 5.250, de 09 de Fevereiro de 1967, art 17 e 21. **Regula a liberdade de manifestação do pensamento e de informação**. Publicada no **DOU** de 10.2.67 E Retificado no DOU de 10.3.67. Disponível em: <http://www.planalto.gov.br/ccivil_03/Leis/L5250.htm >. Acesso em 07/01/2001.

BRASIL. Lei 5.988 de 14 de Dezembro de 1973. **Regula os direitos autorais**, Art.4º , V (contrafação a reprografia não autorizada).

BRASIL. Lei 6.538**,** De 22 De Junho De 1978. Rege sobre os serviços postais. Art. 41º "Violar segredo profissional, indispensável à manutenção do sigilo da correspondência mediante". Publicada no **DOU** de 23.6.78. Disponível em < http://www.presidencia.gov.br/ccivil_03/Leis/L6538.htm>. Acesso em 13/03/2001.

BRASIL. Lei 8.069/90. **Dispõe sobre o Estatuto da Criança e do Adolescente** e dá outras providências - art 241. Disponível em <http://www.planalto.gov.br/ccivil_03/Leis/Referencia_Legislativa/L8069ref_leg.html > .Acesso em 14/08/2000.

BRASIL. Lei 8.112, de 11 de dezembro de 1990. Dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais. Publicada no **DOU** de 12.12.90 e Republicada em 18.3.98. Disponível em <http://www.planalto.gov.br/ccivil_03/Leis/L8112orig.htm. Acesso em 05/01/2001>.

BRASIL. LEI Nº 5.172, DE 25 DE OUTUBRO DE 1966. Dispõe sobre o **Sistema Tributário Nacional** e institui normas gerais de direito tributário aplicável à União, Estados e Municípios. Disponível em <http://www.presidencia.gov.br/ccivil_03/Leis/L5172.htm> . Acesso em 21/03/2001.

BRASIL. Portaria do MPAS Nº 862, de 23 de Março de 2001. Dispõe sobre o controle de acesso a dados, informações e sistemas informatizados da Previdência e Assistência Social. **MPAS**. Disponível em <http://www.previdenciasocial.gov.br/inss/links/legislacaoconsultaportariasmpas862de23032001.html>. Acesso em 26/03/2001.

BRASIL. Projeto de Lei nº 1.713/96. Dispõe sobre o acesso, a responsabilidade e os crimes cometidos nas redes integradas de computadores e dá outras providências. **Câmara dos Deputados**. Disponível em <http://www.modulo.com.br/linksfaqs/legislação/lei1713.htm>, acesso em 30/11/2000.

BRASIL. Recomendação nº 1, de 22 de setembro de 1999. Recomendação para utilização do serviço de Mensageria (correio eletrônico). **Ministério do Planejamento, Orçamento e Gestão.** Disponível em <http://www.planejamento.gov.br >. Acesso em 20/01/2001.

CANAL WEB DIGITAL. **Unesp no combate aos Hackers**. Disponível em <http://www.ibusiness.com.br/noticias.asp?id=4471&patro=o>. Acesso em 17/10/2000.

CANARIE. **Acordo de Cooperação Internacional**. Disponível em <http://www.rnp.br/rnp2/rnp2-i2-canarie.html>. Acesso em 18/09/2000.

CARVALHO, Tereza Cristina Melo de Brito. **Arquiteturas de Redes de Computadores – OSI e TCP/IP**. 2ª Edição. Rev.Ampl. São Paulo: Makron Books. Brisa; Rio de Janeiro: Embratel. Brasília-DF: SGA, 1997.

CORREA, Gustavo Testa. **Aspectos Jurídicos da Internet**. Editora: Saraiva, 2000.

CHARLAB, Sérgio. **Você e a Internet no Brasil**. Objetiva, 1995.

CHESWICK, W. R; BELLOVIN, S. M. **Firewalls and Internet Security**: Repelling the wily hacker. Addison-Wesley, 1994

CRONIN, Mary Jr. **Fazendo Business via Internet**. Editora: Érica, 1995.

CICLADES DO BRASIL INC. **Guia Internet de Conectividade**. 2ª Edição, 1996.

COMPUTING SERVICES - University of California Davis. **A Guide to Electronic Communication & Network Etiquette**, revised and submitted by Joan Gargano, edited by Ivars Balkits, 1987.

DE CASTRO, Maria Alice Soares**. Netiqueta - Guia de Boas Maneiras na Internet**. Editora Novatec, 1997.

DE MORAES, Altair Dias Caldas. **Microsoft Exchange 4 Passo a Passo**. Catapult Inc. Tradução. São Paulo: Makron Books, 1997.

DE PAULA, Mario Antonio Lobato. **A informatização da demissão**. Disponível em <http://www.lazaro.guimaraes.nom.br/infodem.htm>. Acesso em 15/01/2001.

DERFLER, Jr; FRANK, Jr. **Guia de Conectividade**. Tradução da 3ª Edição Americana. ARX Publicações. Rio de Janeiro: Campus, 1995.

DIFFIE, W. **New Directions in Cryptography. IEEE Transf. Of Inform**. Theory. Vol IT-22, 1976

DONOVAN, John J. **The Second Industrial Revolution: Business Strategy and Internet Technology**. Published by Prentice Hall Computer Books, 1997.

EAGER, Bill. **Usando a Internet** - O Guia Amigável. Tradução de AXR Publicações. Rio de Janeiro: Campus, 1995.

EDDINGS, Joshua. **Como Funciona a Internet**. Editora: Quark. 2ª Edição, 1994.

ELIAS, Paulo Sá. In: Alguns aspectos da informática e suas conseqüências no direito (RT 766/491). São Paulo: **Revista dos Tribunais**, 1999.

Elron Software Inc. **Internet Usage Police Guide**, Disponibilizado em <http://www.Internetmanager.com.br>, acessado em 17/02/2001.

ETIQUETE. Os 10 Mandamentos do Instituto da Ética da Internet. Disponível em < http://www.goelton.com/Brasil/Etiqueta/etiquenet.html. Acesso em 02/09/2000.

FBI. Cybercrime. **Congressional Statement Federal Bureau of investigation**. 2000. Disponível em <www.fbi.gov/pressrm/congress00/gonza042100.htm.> Acesso em 30/01/2001.

FONTE, Edison. **Política de Segurança da Informação. Modulo Security**. 03/11/2000. Acesso em 30/11/2000. Disponível em <http://www.modulo.com.br/noticias/artigo_entrevista/a-política.htm>.

GASPARINI, Anteu Fabiano L. **TCP/IP solução para conectividade**. Editoria Érica – 10ª Edição,1999.

GIL, Antonio de Loureiro. **Segurança em Informática**. Editora: Atlas, São Paulo,1994.

HAWKINS, Jan. **O Uso de Novas Tecnologias na Educação**. Revista TB, Rio de Janeiro, 120:57-70, Jan-Mar, 1995.

HOESCHL**,** Hugo Cezar; **A legislação Brasileira sobre Telemática**, Disponível em <http://digesto.net/ddigital/dt/leg.htm> - acessado em 20/01/2001.

HOESCHL, Hugo Cezar; **A liberdade de expressão e comunicação na Internet III- Censura Moral na Internet**, Disponível em <http://digesto.net/ddigital/Internet/liberdade3.htm> - acessado em 23/03/2001.

HONEYCUTT, Jerry. **Usando a Internet**. Editora: Campus. 1998.

ITRI, Maurício P. **Internet 2: A próxima Geração**. Market Books, 1999.

JENNINGS, Roger. **Usando Windows NT Server**. Editora: Campus, 1997.

KADOR, John. **Internet content management : A necessary Evil ?**, disponível em <http://www.techrepublic.com/article.jhtml>, acesso em 26/10/2001.

KENT, Peter**. Guia incrível da Internet.** MAKRON BOOKS, 1995.

LEINER, Barry M. **A Brief History of the Internet,** revisado em 04/08/2000. Disponível em http://www.isoc.org/Internet/history/brief.html#leiner, acesso em 23/09/2000.

LOPES, Mauricio Antonio Ribeiro. **Código Penal**. 3ª Edição. Revisada, Atualizada e aumentada. São Paulo, Editora revista dos tribunais, 1998 (RT Códigos).

MARCONI, Marina de Andrade, **Técnicas de pesquisa**: **Planejamento e execução de pesquisas, amostragens e técnicas de pesquisas e elaboração, análise e interpretação dos dados**; São Paulo, Editora Atlas, 1982.

MARZOCHI, Marcelo de Luca. **Direito.BR – Aspectos Jurídicos da Internet no Brasil**. Editora: LTR, 2000.

MATARAZZO, Cláudia. **Como ser bem educado com seus e-mails**. Disponível em <http://www.ig.com.br/ignetqueta_texto.html>. Acesso em 12/09/2000.

MCCLURE, Stuart. **Hackers Expostos: Segredos e Soluções para a Segurança de Redes**. São Paulo: Makron Books, 2000.

MCFEDRIES, Paul. **Guia incrível do Correio Eletrônico**. Editora: Makron Books, 1996.

MCGRATH, Michael. Product Strategy for High-Technology Companies: How to Achieve Growth. Competitive Advantage, and Increased Profits. **Published by Irwin Professional**, 1994.

Ministério do planejamento, orçamento e gestão. **Segurança da Informação: a segurança das informações e a Internet**, Brasília, 2000, pág: 09-16. Também disponível <http://www.redegoverno.gov.br>,

MORAES, Denis de. **A ética comunicacional na Internet**. Universidade Federal Fluminense, Julho/2000, Rio de Janeiro, Brasil. Disponível em <http://bocc.ubi.pt/pg/moraes-denis-etica-Internet.html> . Acessado em 10/05/2000.

MOU. **Memorando de Entendimento I2**. Disponível em <http://www.rnp.br/noticias/2000/not-00040400.html>. Acesso em 26/09/200.

Newsite Internet Provider Netiqueta. **Etiqueta da** Internet. Disponível em <http://www.newsite.com.br/help-netiqueta.htm>, acessado em 26/11/2001.

NUNES, Ângelo. **Empresas adotam regras e combatem desperdício de energia de funcionários com correio eletrônico**. Publicado em 28/10/2000. Disponível em <http://www.veja.com.br>, Acessado em 01/02/2001.

OSBORN, Matthen. **Corporate e-mail polices**. Disponível em <http://www.techrepublic.com/article.jhtml>. Acesso em 10/11/200.

OPPIGER. **Internet & Intranet Security**. Editora: Ernesto Reichmann, 2000.

PFAFFENDERBER, Bryan. **Estratégias de Extranet**. Editora: Berkeley, 1998.

REA, Louis M. **Metodologia de Pesquisa: Do Planejamento à Execução. Editora Pioneira**, ISBN: 85-221-0216-3 2000.

RNP. O projeto Internet 2. acessado em 08/11/2001. Disponível em http://www.rnp.br/rnp2/rnp2-Internet2.html.

RNP1. **Guia do usuário Internet/Brasil**. Atualizado em 15/04/2000. Disponível em http://www.fapeal.br/rnp/ci/doc/rpu0013b.html. Acessado em 18/11/2000.

RNP2. **Guia do Empreendedor Internet** Atualizado em 03/07/1995. Disponível em http://www.fapeal.br/rnp/ci/doc/rpu0013b.html. Acessado em 18/11/2000.

SAAD, Eduardo Gabriel. **CLT – Comentada**, 31ª edição.LTR Editora ,1992.

SADLER, Will. **Usando e-mail na Internet**. Editora Campus, 1996.

SHAFFER, Deborah. **Exploring Internet Training Series**. Module 2- Mail-based Information Delivery: Alamanac and Listservs. ES-USDA, CIT and Pennsylvanian State University; Henry DeVries, Extension Electronic Technology Group, Cornell University; Gregory Parham, ES_USDA, CIT,1987

SHAPIRO, Norman, et al. **Towards an Ethics and Etiquette for Electronic Mail**, Santa Monica, CA: Rand Corporation (publication R-3283-NSF/RC), 1985.

SISNEMA. **Message inspector vigia e-mail**. Disponível em <http://www.sisnema.com.br/news/noticias/meses /2000 /dezembro /message.htm >, acessado em 26/02/01.

SOARES, Luiz Fernando Gomes. **Redes de Computadores.** Editora: CAMPUS, 1995.

SPAM. **O que é SPAM?** Acessado em 12/12/2000. Disponível em http://www.antispam.org.br/oquee.html.

SPYMAN, Hacking. **Manual Completo do Hacker como ser e evita-los**. 4ª edição especial ampliada. Book Express, 2001.

STARLING, Gorky; NOVO Rafael. **Segurança na Internet**. Editora: Books Express, 1999.

SYMANTEC. **Symantec Mail-Gear**. Acesso em 03/03/2001. Disponível em <http://www.symantec.com/region/br/product/mailgear>.

TANEMBAUM, Andrew S. **Rede de Computadores**. Rio de Janeiro: Campus. 1994.

Tema: a revista do serpro, ano XXIV – Nº 146 **– Internet 2 na reta Final**,2000,

Tema: a revista do serpro, ano XXV – Nº 153 – **Governo Eletrônico**, 2000.

TORRES, Gabriel. **Redes de computadores - curso completo**. Rio de Janeiro: campus, 2001.

True Access Consulting, **Segurança da Informação e Gerenciamento de Rede**. Disponível em <http://www.trueaccess.com.br>. Acessado em 06/12/2001.

USP. **E-mail para iniciantes**. Disponível em <http://www.icmsc.sc.usp.br/manual/BigDummy/Email.html>. Acesso em 18/09/2000.

USP1. **Introdução a Netiqueta**. Acessado em 13/11/2000. Disponível em <http://www.icmc.sc.usp.br/manuals/BigDummy/netiqueta.html>.

VARHOL, Peter D. **E-mail: Archiving Local and Global Communications**. Computer Technology Research Corp. Edition 1995.

WALL, Stephen J. **Usando a World Wide Web**. Editora: Campus, 1996.

ZEFF, Robbin. **Publicidade na Internet**. Editora: Campus, 2000.

# ANEXO I

## Penalidades Previstas para o uso indevido

**I - Divulgação de Segredo**

Art 153 CP - *"Divulgar alguém, sem justa causa, conteúdo de documento particular ou de correspondência confidencial, de que é destinatário ou detentor e cuja divulgação possa produzir dano a outrem"*

Pena: Detenção de 1(um) a (seis) meses ou multa.

Art 154 CP - "*Revelar a alguém, sem justa causa, segredo de que tem ciência em razão de função, mistério, ofício ou profissão e cuja revelação pode produzir dano a outrem".*

Pena: Detenção de 3(três) meses a 1(um) ano ou multa.

LEI 6.538 (rege sobre os serviços postais)

Art 41 - *"Violar segredo profissional, indispensável à manutenção do sigilo da correspondência"*

Pena: Detenção de 3(três) meses a 1(um) ano ou multa.

Art 325 CP (Violação de sigilo funcional)- "*Revelar fato de que tem ciência em razão de cargo e que deva permanecer em segredo, ou facilitar-lhe a revelação".*

Pena: Detenção de 6 (seis) meses a 2 (dois) ano ou multa, se o fato não se constituir crime mais grave.

Art 151 CP (Violação de correspondência) – "D*evassar indevidamente o conteúdo de correspondência fechada, dirigida a outrem".*

Pena: Detenção de 1(um) a 6 (seis) meses ou multa

Parágrafo 1º - Na mesma pena incorre: (Sonegação ou destruição de correspondência)

I- Quem se apossa indevidamente de correspondência alheia, embora não fechada, no tudo ou em partes, a sonega ou a destrói.

**II - Estelionato (Crimes contra o Patrimônio)**

Art 171 CP – *"Obter para si ou para outrem vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil ou qualquer outro meio fraudulento".*

Pena: Reclusão de 1(um) a 5(cinco) anos e multa.

**III - Crimes contra o Costumes**

Art 234 CP - *"Fazer, importar, exportar, adquirir ou ter sob sua guarda, para fim de comércio, de distribuição ou de exposição pública, escrita, desenho, pintura, estampa ou qualquer outro objeto obsceno"*

Vender, distribuir, ou expor à ven da ou ao público qualquer dos materiais referidos neste artigo.

Pena: detenção de 6 (seis) meses a 2 (dois) anos ou multa.

**IV - Crimes contra a paz pública**

Art 286 CP - *"Incitar publicamente a prática de crime."*

Pena: detenção de 3 (três) meses a 6 (seis) meses ou multa.

Art 287 CP - *"Fazer publicamente apologia de fato criminoso ou de autor de crime."*

Pena: detenção de 3 (três) meses a 6 (seis) meses ou multa.

LEI 4.117/62 – Código Brasileiro de Telecomunicações

Art 53 - *"Constitui abuso, no exercício da liberdade de radiodifusão, o emprego desse meio de comunicação:"*

h – Ofender a moral familiar pública ou dos bons costumes.

Pena: detenção de 3 (três) meses a 6 (seis) meses ou multa.

**V - Do Furto**

Art 155 CP - *"Subtrair, para si ou para outrem, coisa alheia móvel"*

Parágrafo 3º - "equipara-se à coisa alheia móvel a energia ou qualquer outro bem que tenha valor econômico".

Pena: reclusão de 1 (um) a 4 (quatro) anos e multa.

**VI - DO Dano**

Art 163 CP - *"Destruir, inutilizar ou deteriorar coisa alheia"*

Dano qualificado:

Parágrafo único: "se o crime é cometido"

Inciso IV – "por motivo egoístico ou com prejuízo considerável para a vítima".

Pena: detenção de 6 (seis) meses a 3 (três) anos e multa, além da pena correspondente àviolência

**VII - Decreto LEI 3.688/ 41 (Dispõe das Contravenções Penais)**

Art 65 – Perturbação da tranqüilidade -*"Molestar alguém, pertubar-lhe a tranqüilidade por acidente ou por motivo reprovável".*

Pena: Prisão simples, de 15 (quinze) dias a 2 (dois) meses ou multa.

**VIII - LEI 8.069/ 90( Dispõe sobre o estatuto da Criança e do Adolescente)**

Art 241 – *"Fotografar ou publicar cena de sexo explícito ou pornográfico envolvendo criança ou adolescente".*

Pena: Reclusão de 1 (um) a 4 (quatro) anos

**IX - LEI 5.520/67(Regula o manifesto do pensamento e da informação)**

Art 17 – *"Ofender a moral pública e os bons costumes"*

Pena: Detenção de 3 (três) meses a 1 (um) ano e multa

Art 21 – *"Difamar alguém, impultando-lhe fato ofensivo à sua reputação"*

Pena: Detenção de 3 (três) a 18(dezoito) meses e multa

**X - Código Tributário Nacional**

Art 138 – "*Divulgar informações obtidas em razão do ofício, sobre a situação econômica ou financeira aos sujeitos passivos ou de terceiros e sobre a natureza e o estado dos seus negócios ou atividades".*

Pena: Prisão simples, de 15 (quinze) dias a 2 (dois) meses ou multa.

**XI - Do Código Legislação Trabalhista – CLT**

Artigo 482 – "*Constituem justa causa para rescisão do contrato de trabalho pelo empregador:"*

**Ato de improbidade** - Jurisprudência registrada no TRT (11ª região, proc.RO-172/85,julg.6.8.85, rel. Juiz Geraldo L. Silva): "A improbidade fere os padrões morais de uma sociedade. É um ato que corresponde sempre a uma lesão do patrimônio da empresa. O reclamante não só se apropriou de valores da reclamada, como permitiu que outros se apropriassem".

g- Violação de segredo da empresa - "quando o empregado divulgar fato, de que teve conhecimento em virtude do contrato de trabalho, suscetível de causar prejuízos ao empregador"

Para efeito de esclarecimentos Justa Causa: " é todo ato, doloso ou culposo, de natureza grave e de responsabilidade do empregado, que leva o

empregador à conclusão de que ele não pode continuar a prestar-lhe serviços", texto retirado do original.

# ANEXO II

## TERMO DE RESPONSABILIDADE

Declaro estar ciente da habilitação que me foi conferida e das disposições referentes a utilização e acesso do correio eletrônico da organização contidas na norma de utilização de correio eletrônico corporativo; e a aplicação das penalidades cabíveis pela não observância dos cumprimentos assumidos contidas nos artigos do Código Penal 151, 153, 154, 155, 163, 171, 234, 286, 287, 325; da Lei 6.538 art 41, Lei 4.117/62 art 53-h, decreto lei 3.688/41 art 65, lei 8.069/90 art 241, lei 5.520/67 art 17 e 21, Código Tributário Nacional art 138, e CLT art 482(trata da improbidade e violação de segredo da empresa);para o funcionalismo público agrega-se os dispositivos da Portaria nº 862/2001 e das penalidades cabíveis pela não-observância dos compromissos assumidos. Lei nº 9.983, de 14 de julho de 2000 "Art 1º São acrescidos à Parte Especial do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 * Código Penal:

.....

Comprometo-me a:

a)zelar pelo sigilo absoluto de minha senha;

b)acessar o serviço de correio eletrônico, somente por necessidade de serviço;

c)não enviar, para fora do âmbito corporativo, fato ou informação de qualquer natureza de que tenha conhecimento por força de minhas atribuições, salvo em decorrência de decisão competente na esfera legal ou judicial, bem como de autoridade superior;

d) manter a absoluta cautela quando da exibição de dados em tela, impressora ou, ainda, na gravação em meios eletrônicos, a fim de evitar que deles venham a tomar ciência pessoas não autorizadas;

e) não me ausentar do microcomputador sem encerrar a sessão de uso da caixa postal, garantindo assim a impossibilidade de acesso indevido por pessoas não autorizadas;

f) responder, em todas as instâncias, pelas conseqüências das ações ou omissões de minha parte que possam por em risco ou comprometer a exclusividade de conhecimento da minha senha ou das transações as quais esteja habilitado;

g) estar sujeito a qualquer hora e sem aviso prévio que a corporação monitore as informações de minha caixa postal;

h) a utilizar apenas os serviços de correio eletrônico para os seus propósitos e estou ciente de que são de propriedade exclusiva da organização;

i) cumprir as normas de utilização de correio eletrônico desta organização, conforme cópia e esclarecimento de dúvida após lê-la;

j) Utilizar bons costumes ao envio de correio eletrônico no ambiente corporativo, conforme descrito no item (3.2.3.1. Recomendações a serem aplicadas durante o uso);

k) Não utilizar os recursos de correio eletrônico para qualquer propósito ilegal;

l) Não receber arquivos ou mensagens de rede externas, e que a administração de correio eletrônico terá direito de retirar do serviço qualquer conteúdo que viole esta norma;

m) A organização não será responsável de forma alguma por qualquer conteúdo, perda ou dano de qualquer espécie resultante de conteúdos recebidos ou de qualquer outra forma disponibilizada através do serviço de correio eletrônico, cabendo-lhe sim apuração dos fatos e aplicação de medidas disciplinares;

n) indenizar e insentar a organização, diretores e empregados, de qualquer perda, despesas, danos, reclamações, ou reivindicações, incluindo custos judiciais e honorários advocatícios:

1. Quanto à utilização dos conteúdos fornecidos por outros usuários;
2. Má Utilização do serviço de correio eletrônico;
3. Conexão ao serviço de correio eletrônico;
4. Violação do termo de utilização do serviço de correio eletrônico

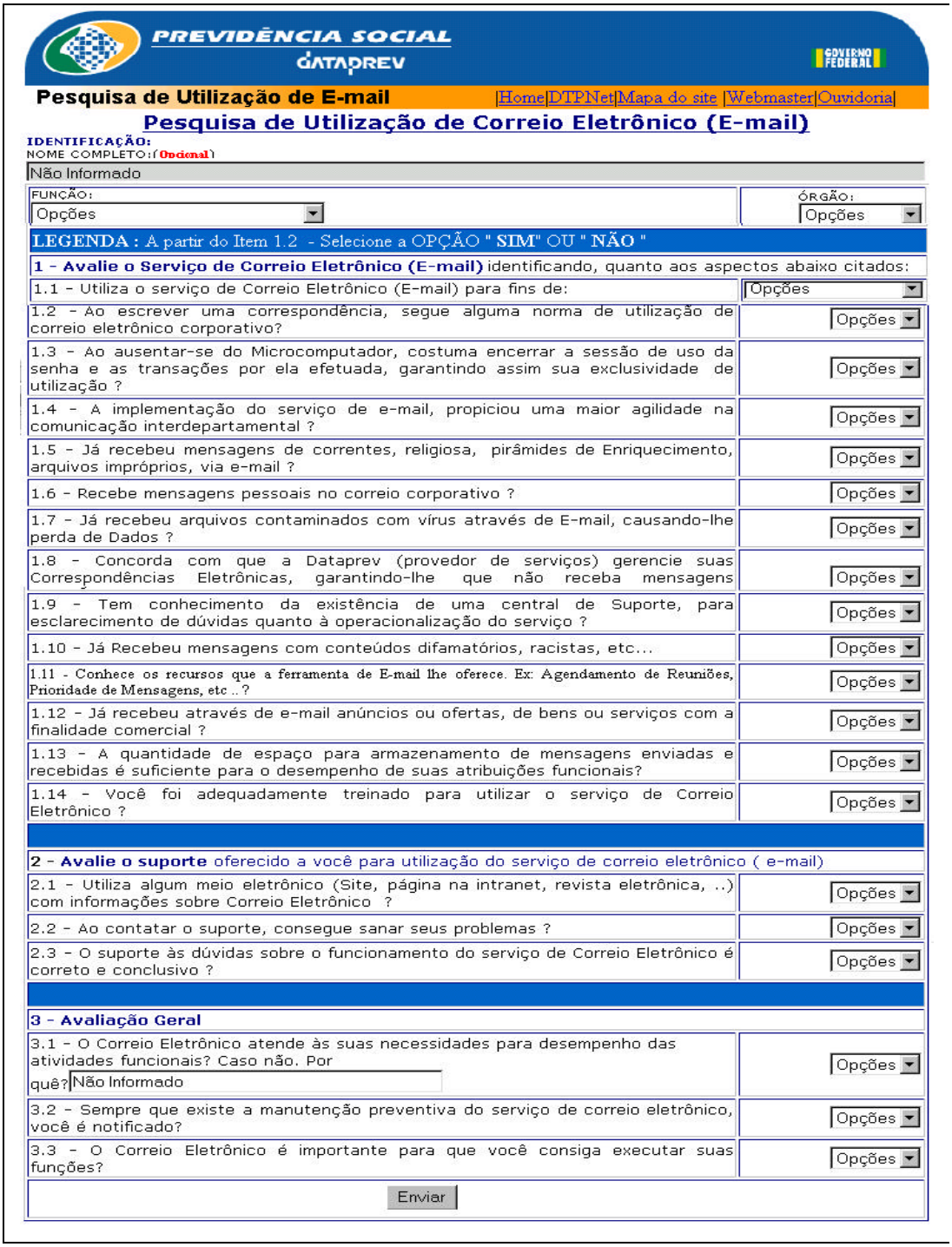
o) A organização poderá cancelar a senha, conta ou utilização do serviço de correio eletrônico. Remover ou apagar qualquer conteúdo do serviço nos seguintes casos:

1. A qualquer instante e por qualquer motivo, a critério exclusivo, sendo que o serviço é de sua propriedade exclusiva;
2. Se a organização identificar qualquer tipo de violação ou uso imprudente com os termos desta norma de utilização de correio eletrônico
3. Se o usuário tiver violado os direitos da organização e de terceiros;
4. Em circunstância de desligamento da organização.

_____

Data/Assinatura

# ANEXO III
# Questionário



PREVIDÊNCIA SOCIAL
DATAPREV
GOVERNO FEDERAL

**Pesquisa de Utilização de E-mail** |Home|DTPNet|Mapa do site |Webmaster|Ouvidoria|

## Pesquisa de Utilização de Correio Eletrônico (E-mail)

**IDENTIFICAÇÃO:**
NOME COMPLETO:(Opcional)
Não Informado

FUNÇÃO: Opções
ÓRGÃO: Opções

**LEGENDA :** A partir do Item 1.2 - Selecione a OPÇÃO " **SIM**" OU " **NÃO** "

**1 - Avalie o Serviço de Correio Eletrônico (E-mail)** identificando, quanto aos aspectos abaixo citados:

| | |
|---|---|
| 1.1 - Utiliza o serviço de Correio Eletrônico (E-mail) para fins de: | Opções |
| 1.2 - Ao escrever uma correspondência, segue alguma norma de utilização de correio eletrônico corporativo? | Opções |
| 1.3 - Ao ausentar-se do Microcomputador, costuma encerrar a sessão de uso da senha e as transações por ela efetuada, garantindo assim sua exclusividade de utilização ? | Opções |
| 1.4 - A implementação do serviço de e-mail, propiciou uma maior agilidade na comunicação interdepartamental ? | Opções |
| 1.5 - Já recebeu mensagens de correntes, religiosa, pirâmides de Enriquecimento, arquivos impróprios, via e-mail ? | Opções |
| 1.6 - Recebe mensagens pessoais no correio corporativo ? | Opções |
| 1.7 - Já recebeu arquivos contaminados com vírus através de E-mail, causando-lhe perda de Dados ? | Opções |
| 1.8 - Concorda com que a Dataprev (provedor de serviços) gerencie suas Correspondências Eletrônicas, garantindo-lhe que não receba mensagens | Opções |
| 1.9 - Tem conhecimento da existência de uma central de Suporte, para esclarecimento de dúvidas quanto à operacionalização do serviço ? | Opções |
| 1.10 - Já Recebeu mensagens com conteúdos difamatórios, racistas, etc... | Opções |
| 1.11 - Conhece os recursos que a ferramenta de E-mail lhe oferece. Ex: Agendamento de Reuniões, Prioridade de Mensagens, etc .. ? | Opções |
| 1.12 - Já recebeu através de e-mail anúncios ou ofertas, de bens ou serviços com a finalidade comercial ? | Opções |
| 1.13 - A quantidade de espaço para armazenamento de mensagens enviadas e recebidas é suficiente para o desempenho de suas atribuições funcionais? | Opções |
| 1.14 - Você foi adequadamente treinado para utilizar o serviço de Correio Eletrônico ? | Opções |

**2 - Avalie o suporte** oferecido a você para utilização do serviço de correio eletrônico ( e-mail)

| | |
|---|---|
| 2.1 - Utiliza algum meio eletrônico (Site, página na intranet, revista eletrônica, ..) com informações sobre Correio Eletrônico ? | Opções |
| 2.2 - Ao contatar o suporte, consegue sanar seus problemas ? | Opções |
| 2.3 - O suporte às dúvidas sobre o funcionamento do serviço de Correio Eletrônico é correto e conclusivo ? | Opções |

**3 - Avaliação Geral**

| | |
|---|---|
| 3.1 - O Correio Eletrônico atende às suas necessidades para desempenho das atividades funcionais? Caso não. Por quê? Não Informado | Opções |
| 3.2 - Sempre que existe a manutenção preventiva do serviço de correio eletrônico, você é notificado? | Opções |
| 3.3 - O Correio Eletrônico é importante para que você consiga executar suas funções? | Opções |

Enviar