PAULO ALEXANDRE DAMASCENO

PROPOSTA DE POLÍTICA DE SEGURANÇA DA INFORMAÇÃO PARA A COMPANHIA DE TRANSMISSÃO PAULISTA (CTEEP)

Monografia apresentada a Escola Politécnica da Universidade de São Paulo para obtenção do Título de MBA - Especialista em Tecnologia da Informação.

São Paulo

2003

PAULO ALEXANDRE DAMASCENO

PROPOSTA DE POLÍTICA DE SEGURANÇA DA INFORMAÇÃO PARA A COMPANHIA DE TRANSMISSÃO PAULISTA (CTEEP)

Monografia apresentada a Escola Politécnica da Universidade de São Paulo para obtenção do Título de MBA - Especialista em Tecnologia da Informação.

Orientador(a)

PROFª. DRª. GRAÇA BRESSAN

São Paulo

2003

AGRADECIMENTOS

Em primeiro lugar a Deus, por me dar forças para lutar e conseguir realizar este trabalho.

A minha querida noiva Maria Lúcia, que me apoiou e me compreendeu nesses momentos tão difíceis.

A minha família, pela ajuda, incentivo e orações, para que eu tivesse forças e sabedoria.

A minha orientadora Professora Drª Graça Bressan, pela ajuda nas orientações e pela paciência, para que meu trabalho ficasse o mais correto possível.

Ao pessoal da CTEEP – colaboradores, gerentes, diretores e presidente – pelo tempo, paciência, auxílio e cooperação, tornando possível a realização deste trabalho.

Ao meu amigo e irmão Christiano H. C. L. Silva, que compartilhou todas as minhas dificuldades, me ajudou e incentivou em todos os momentos.

A todos os professores e colegas do MTI, em especial ao Prof. Moacyr Martucci, que compartilharam seus conhecimentos nesse curso, o qual foi de extrema importância para nossas vidas.

E é claro, ao meu grande amigo Prof. Dib Caran, pois se não fosse a ajuda dele, este trabalho não teria sido entregue.

RESUMO

Este trabalho, em forma de monografia, aborda os principais aspectos relacionados à segurança de redes e sistemas de informação. Serão apresentados conceitos básicos, tecnologias e a importância do planejamento de segurança. Serão, ainda, abordadas algumas das principais ferramentas utilizadas na prevenção de incidentes, como *Firewalls*, Sistemas de detecção de intrusão, Registro de *Logs*, Antivírus e *Backups*. Ao final do trabalho serão apresentadas propostas para definição de uma Política de Segurança da Informação para a Companhia.

O trabalho tem como principal objetivo fornecer uma visão ampla sobre os principais aspectos envolvendo a segurança de redes e das informações.

ÍNDICE

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ANEXOS

LISTA DE SIGLAS

ACC (Ambiente Computacional Complexo) – Representa um ambiente computacional extremamente heterogêneo e distribuído ou, em uma palavra, complexo.

AUP (*Appropriate* – ou *Acceptable* – *Use Policy)* – Uma política de uso apropriado, pode também ser parte de uma política de segurança.

BS 7799 – Norma britânica de segurança da informação constituída de duas partes, sendo a primeira publicada em 1995, também referenciada como BSI (1995), e a segunda, em 1998. A primeira parte deu origem à norma ISO/IEC 17799:2000BS.

CCSC (*Commercial Computer Security Centre*) – Centro de segurança de computação comercial criado pelo Departamento de Indústria e Comércio do Reino Unido (*UK Department of Trade and* Industry – DTI), em 1987, que, dentre as suas atribuições, tinha a tarefa de produzir um código com as melhores práticas de segurança em tecnologia da informação com a finalidade de auxiliar usuários na implantação de sistemas de segurança em seus ACC. Desse esforço, realizado conjuntamente com o Centro de Computação Nacional (*National Computing Centre* – NCC), resultou um "Código de práticas para usuários" (*Users Code of Practice*), que foi publicado em 1989.

CEO (*Chief Executive Officer*) – Diretor executivo, diretor geral ou presidente de uma Companhia.

CERT/CC (*Computer Emergency Response Team)* – Centro de pesquisas em segurança na Internet da Universidade de Carnegie Mellon.

CIO (*Chief Information Officer*) – Cargo com a responsabilidade de análise de sistemas e recursos de tecnologia da informação, que projeta a estrutura tecnológica necessária ao alcance das metas da empresa.

CRO (Centro Regional de Operações) – No comando do Sistema da Transmissão Paulista temos quatro Centros de Operação interligados por uma rede de computadores, os quais têm a responsabilidade de coordenar, supervisionar e controlar as operações realizadas ao longo dos 11.589 km de linhas de transmissão da Companhia.

DNS (*Domain Name Service*) – Serviço de replicação que interpreta os números pelos quais os servidores conectados à internet são identificados e os representa ao usuário como um nome textual.

DOS (*Denial Of Service*) – É uma ameaça em que um *hack*, após ter acessado e dominado um computador alheio, consegue gerar uma grande quantidade de transmissão de dados deste, causando um excesso de pacotes, seja para uma rede, estação ou servidor, com a finalidade de sobrecarregar a vítima, deixando as suas atividades indisponíveis (negação de serviço) ou muito lentas.

DTI (*UK Department of Trade and Industry*) – Departamento de Comércio e Indústria do Reino Unido.

EDI (*Eletronic Data Interchanging*) – Intercâmbio eletrônico de Dados.

GWh (Giga-wats por hora) – Unidade de potência igual a um bilhão de watts, 1000 megawatts ou um milhão de kilowatts.

IEC (*International Electrotechnical Commission*) – Organização que, conjuntamente com a ISO, desenvolve, sugere e define padrões para protocolos de rede.

IP (*Internet Protocol*) – Juntamente com o TCP, é o protocolo em que se baseia o funcionamento da Internet.

ISMS (*Information Security Management System*) – É o resultado de uma ação de gerenciamento explícito, expresso como uma coleção de políticas, princípios, objetivos, medidas, processos, formas, modelos, lista de verificações (*checklist*), etc, que juntos definem como os riscos de segurança de um ACC podem ser reduzidos.

ISO (*International Organization for Standardization*) – Organização internacional que desenvolve, sugere e define padrões.

KV (Quilovolts) – É a unidade de medida da tensão.

LAN (*Local Area Network* = rede local) – É um tipo de rede concentrada em um spaço físico limitado (prédio, empresa, campus universitário, etc).

Mbps (*Mega bits* por segundo) – Medida de velocidade de transmissão de informação entre computadores.

MVA (Megavolts-ampére) – Unidade de medida da potência (Volt Ampére). A unidade VA é obtida pelo produto direto da tensão nominal pela corrente nominal. Este produto determina a potência do equipamento. Este valor é usado para a definição das características da instalação elétrica (cabos, fusíveis, disjuntores etc.

NCC (*National Computing Centre*) – Ver CCSC (*Commercial Computer Security Centre*).

NFS (*Network File System*) – Sistema de arquivos em rede utilizado por sistemas operacionais UNIX. Similar ao compartilhamento das redes Microsoft.

OSI (*Open Systems Interconnection*) – É um modelo de referência de sete camadas para redes, desenvolvido pela *International Standards Organization* (ISO). O modelo de referência OSI é um método formal para descrever os conjuntos de interconexão de *hardware* e *software* de rede usados para oferecer serviços de rede.

RFC (*Request For Comments*) – Documentos utilizados para comunicar idéias para desenvolvimento pela comunidade da Internet e que podem se tornar padrões.

SSC (Sistema de Supervisão e Controle) – Sistema responsável pela supervisão e controle da malha de linhas de transmissão, e suas inter-conexões, da Companhia de Transmissão Paulista.

TCP/IP (*Transmission Control Protocol / Internet Protocol*) – Protocolo (método) de comunicação entre computadores ligados em rede.

TI (Tecnologia da Informação) – Conjunto de tecnologias utilizadas para desenvolver o processo de geração, processamento, disseminação e documentação das informações.

WAN (*Wide Area Network* = rede de longa distância) – é um tipo de rede remota que abrange uma longa distância, podendo ser de metrópoles para metrópoles ou de país para país.

WWW (*World Wide Web*) – Recurso ou serviço oferecido na *Internet* (rede mundial de computadores), e que consiste num sistema distribuído de acesso a informações, as quais são apresentadas na forma de hipertexto, com elos entre documentos e outros objetos (menus, índices), localizados em pontos diversos da Rede.

CAPÍTULO 1 – INTRODUÇÃO

Segundo FONTES (2000), atualmente é fato que somos dependentes do computador e o uso desta tecnologia é hoje, irreversível e cresce a cada dia, fazendo com que as empresas que não aderiram ainda a tudo isso, tornem-se obsoletas, arcaicas e tenham prejuízos.

A rapidez com que surgem novas facilidades e avanços tecnológicos é assustadora, uma empresa termina de atualizar seus *softwares* para uma nova versão e em seguida são lançados *softwares* ainda mais avançados, estes avanços tecnológicos proporcionam grandes facilidades como, por exemplo, agilidade, confiabilidade, rapidez, controle de informações, entre outras.

Mas tudo isso também traz problemas, pois a dependência desta tecnologia faz com que um defeito num computador ou um problema em um *software*, coloque em risco anos de trabalhos e estudos.

Além disso, no momento em que os sistemas passaram a compartilhar os dados e conectar as redes, aumentaram os problemas por falta de segurança, pois quando muitos acessam as informações são necessários cuidados para que não haja acessos indevidos e mau uso do sistema.

De acordo com SEGURANÇA MÁXIMA (2001), antigamente também existiam problemas de segurança, mas eram em proporções muito menores que hoje e mais simples de serem resolvidos. Hoje em dia existem pessoas comuns controlando sistemas importantes da empresa, muitas delas não acompanharam a evolução dos problemas de segurança e não possuem o conhecimento necessário para se prevenir contra novos problemas que aparecem a cada dia.

Segundo estatísticas, sobre os incidentes de segurança registrados no ano de 2003, pelo *Computer Emergency Response Team* – CERT/CC (2003), centro de pesquisas em segurança na *Internet* da Universidade de Carnegie Mellon, os números impressionam, até o terceiro trimestre de

2003, já foram registrados 114.855 incidentes de segurança. Este total representa praticamente a soma dos incidentes registrados em 2001 (52.658) e 2002 (82.094).

FONTES (1999), em um dos seus artigos, diz que segurança da informação não é apenas uma atitude ou um produto ou uma pessoa, são muitas atitudes, que implementadas vão proteger a organização, e tornar a segurança da informação efetiva. Não adianta gastar um valor exorbitante para colocar porta com senha de acesso nas salas onde estão os servidores da empresa, se não existe um procedimento de controle de acessos e a senha é conhecida por todos e não é trocada regularmente. Não adianta ter um perfeito *software* de *backup* e um cofre em outra planta da empresa, para onde as fitas são levadas, se diariamente este *backup* não for conferido se foi realizado corretamente.

É importante salientar que cada empresa tem uma realidade e, devido a isso, uma solução de segurança, proposta para uma empresa, pode não ser a solução ideal para outra empresa, que trate de negócios diferentes.

O estudo, a que se propõe este trabalho, está baseado em uma pesquisa teórica, conforme referências bibliográficas, livros, revistas, jornais e demais mídias atuais, assim como, pelo acompanhamento na prática.

Portanto, este trabalho citará problemas gerais que qualquer tipo de empresa está exposta, as medidas de segurança para prevenção destes problemas, propostas neste trabalho, podem ser usadas por qualquer empresa, mas serão soluções básicas que deverão ser trabalhadas em conjunto para se tornarem efetivas.

Mas, para que a empresa fique tranqüila, no que diz respeito a segurança, a implantação destas medidas é apenas o começo, sempre será necessário o comprometimento dos funcionários, o apoio da alta direção da empresa e o acompanhamento de novas tecnologias e novos riscos, ou seja, é um trabalho que exige continuidade.

1.1 – OBJETIVO DO TRABALHO

OBJETIVO GERAL

Estudar e propor a elaboração de um documento de política de segurança da informação, que auxilie nos procedimentos para garantir a segurança dos sistemas computacionais e informações neles armazenadas e distribuídas, preservando, de forma íntegra, os recursos e a reputação dos seus proprietários, diante das várias plataformas de *hardware* e *software*, utilizadas hoje pela Transmissão Paulista em suas redes.

OBJETIVO ESPECÍFICO

- Estudar e propor a elaboração de um documento de política de segurança, fornecendo uma visão ampla sobre os principais aspectos envolvendo a segurança de redes e das informações.

1.2 – MOTIVAÇÃO E JUSTIFICATIVA

O desenvolvimento deste trabalho é motivado e justificado pela necessidade de proteção das informações que se armazenam e se publicam nos servidores da Transmissão Paulista, levando em consideração que os mesmos estão ligados à *Internet*. Também pela necessidade da integração de suas duas redes, corporativa e do SSC – Sistema de Supervisão e Controle, garantindo que ambas redes atendam a um nível desejável e confiável de segurança.

Manter a integridade de tais informações requer profissionais adequadamente especializados para esta finalidade, já que se trata de um esforço contínuo, para que a aplicação dos conceitos de segurança não fique desatualizada.

Em complemento, acrescenta-se a notável necessidade de estabelecer políticas de acesso e uso dos recursos computacionais concedidos aos usuários das redes de trabalho, esclarecendo quais serviços podem ser acessados e quais não podem (e sob quais penas), bem como as

rotinas do administrador de sistemas na distribuição e expiração de senhas, criação de usuários, contas de administrador, configuração de sistemas operacionais, geração de relatórios sobre atividades e tentativas de mau uso, estações de trabalho, serviços de rede entre outros.

1.3 – METODOLOGIA UTILIZADA

- Coletar informações sobre os diversos sistemas operacionais utilizados na Transmissão Paulista e que possam contribuir para o desenvolvimento do trabalho;
- Propor a elaboração de um documento para política de segurança da informação na Transmissão Paulista.

1.4 – RESULTADOS ESPERADOS E CONTRIBUIÇÃO DO TRABALHO

O presente trabalho apresenta como resultado final uma Proposta de Política de Segurança da Informação para a Companhia, com medidas básicas de segurança, para os administradores de rede de computadores, visando minimizar ao máximo os problemas que podem afetar os sistemas e redes de computadores, sem, contudo esgotar o assunto.

Também como contribuição para a Companhia, esperamos que seja o comprometimento e a preocupação com o tema Segurança da Informação, fornecendo uma visão sobre a questão, promovendo a conscientização para a alta administração da Companhia para a elaboração de uma Política de Segurança da Informação. Também o comprometimento dos funcionários e o acompanhamento de novas tecnologias e novos riscos, ou seja, todos os resultados e contribuições exigem continuidade.

1.5 – ORGANIZAÇÃO DO TRABALHO

CAPÍTULO 1 – INTRODUÇÃO – Neste capítulo será apresentado uma breve introdução sobre o assunto segurança da informação e também sobre políticas de segurança da informação.

CAPÍTULO 2 – REVISÃO DA LITERATURA – Todo este capítulo apresentará conceitos e definições, coletados das literaturas e bibliografias que foram estudas para o desenvolvimento do trabalho.

CAPÍTULO 3 – A TRANSMISSÃO PAULISTA (CTEEP) – Apresentação da Companhia, fornecendo uma visão política e tecnológica.

CAPÍTULO 4 – PROPOSTA PARA POLÍTICA DE SEGURANÇA – No decorrer deste capítulo será apresentado com base nas pesquisas realizadas, algumas propostas para o planejamento de uma política de segurança da informação para a Companhia.

CAPÍTULO 5 – CONCLUSÃO – Neste capítulo final será apresentado uma conclusão para o trabalho proposto, levando em consideração os benefícios que a proposta poderá trazer a companhia.

CAPÍTULO 2 – REVISÃO DA LITERATURA

2.1 – DEFINIÇÕES SOBRE SEGURANÇA DA INFORMAÇÃO

Os altos índices de informatização, conectividade, negócios pela *Internet* e compartilhamento de dados tornaram a informação um dos bens mais valiosos e mais vulneráveis das empresas. Com isso, incidentes nas redes de computadores passaram a afetar diretamente os resultados do negócio e o valor das empresas.

De acordo com FERREIRA (2002), informação é um dado acerca de alguém ou algo; o conhecimento; segundo a teoria da informação, a medida da redução da incerteza.

A projeção que a segurança das informações obteve no mercado global nos últimos anos foi enorme, o tema alcançou as mais altas e estratégicas camadas das organizações, chegando ao CIO, CEO e aos acionistas.

Segundo a norma ISO/IEC 17799:2000, segurança da informação pode ser definida como a proteção contra um grande número de ameaças às informações, de forma a assegurar a continuidade do negócio, minimizando danos comerciais e maximizando o retorno de possibilidades e investimentos. Ainda segundo a ISO/IEC 17799:2000 a segurança da informação é caracterizada pela preservação dos três atributos básicos da informação: confidencialidade, integridade e disponibilidade.

2.2 – NECESSIDADES DE NEGÓCIOS DA ORGANIZAÇÃO

Segundo o CT-STI (2000), a *Internet* é uma porta aberta da organização para um novo universo de clientes em potencial. A disponibilização de informações sobre produtos e serviços na *Internet* deve ser encarada como uma forma eficaz de ampliar o alcance da organização para o bom atendimento ao público.

Ainda segundo CT-STI (2000), os setores de produção de informação nas organizações, governamentais ou não, estão correndo em direção à exposição na *Internet*, com ânsia crescente para colocar serviços à disposição da população. Esta é uma tendência inquestionável: os *sites* devem passar a oferecer o "serviço público mais público", ou seja, aquele que pode ser usufruído pelos clientes fora da organização, a partir do ambiente residencial ou de trabalho.

Não existem regras para determinar quais são as necessidades de negócios de uma organização. Obviamente, cada organização compreende variáveis específicas. Entretanto, é um erro conectar-se à *Internet* sem identificar claramente as necessidades organizacionais. Isso poderia custar mais do que o necessário, além de resultar no oferecimento de serviços irrelevantes. Também pode revelar-se uma iniciativa que represente apenas um alto consumo de tempo e uma exposição desnecessária frente aos riscos potenciais de segurança.

Para CT-STI (2000), alguns serviços que devem ser definidos de acordo com as necessidades da organização são:

- **Correio Eletrônico:** Permite a troca de mensagens de correio (pedidos, confirmações de pedidos, atendimento a sugestões e reclamações) com clientes e fornecedores em qualquer parte do mundo em apenas poucos minutos.
- **As Páginas na Rede Mundial (WWW):** A organização pode proporcionar ou obter prontamente muitos tipos de informações – financeiras, setoriais, de referência e educacionais, ou proporcionar uma vitrine mundial para seus produtos e serviços.
- **Troca de Informações (transferência de arquivos):** A organização pode trocar informações sob a forma de arquivos de dados, muitas vezes anexados a uma mensagem de correio eletrônico.

- **Comércio Eletrônico:** Cada vez mais organizações estão usando a *Internet* para oferecer e vender seus produtos diretamente aos clientes. Quase tudo pode ser comprado após o exame de um catálogo *on-line*, escolha e encomenda, com a garantia de um pagamento seguro por um boleto bancário ou cartão de crédito.
- ***Intranet*:** Uma *Intranet* é uma rede local – ou um grupo de redes locais – que pode ser acessada somente por aquelas pessoas que tenham sido autorizadas. É uma excelente maneira de compartilhar informações, por exemplo, numa organização que tenha *sites* em diferentes partes de uma cidade, ou cuja rede ultrapasse as fronteiras regionais, nacionais e internacionais.
- ***Extranet*:** A *Extranet* é uma extensão da *Intranet*. Através dela, os usuários podem acessar redes locais, desde que devidamente autorizados. Uma *Extranet* amplia o conceito de *Intranet*, com a inclusão de parceiros de confiança no âmbito das redes. Nela, o acesso também é restrito. A *Extranet* compreende uma linha de ligação exclusiva entre parceiros, fora da *Internet*. Ela só pode ser acessada via linha dedicada ou particular. Um exemplo de *Extranet* é o *homebanking*.
- **Intercâmbio Eletrônico de Dados (EDI):** Para organizações envolvidas no EDI, a *Internet* pode proporcionar uma maneira relativamente barata de intercambiar informações. O governo utiliza sistematicamente o EDI para o tratamento das informações do DARF – Documento de Arrecadação da Receita Federal e também no Siscomex – Sistema de Comércio Exterior.

Também de acordo com CT-STI (2000), para se definir esses serviços é necessário que a organização responda algumas perguntas como:

- Quais são os serviços necessários?
- Em quê eles serão úteis?
- Como e quem usará esses serviços?
- Quais serviços devem ter acesso restrito?
- Se a organização está considerando a criação de uma página WWW, que tipo de informação será publicada, e com que freqüência elas serão atualizadas?
- Quem realizará uma avaliação de riscos e criará uma política de segurança?

2.3 – RISCOS

Todos os dias, os gerentes assumem decisões de risco para proteger suas organizações e ativos. Sob vários aspectos, a *Internet* ainda é um ambiente vulnerável. Há riscos potenciais em seu uso e, portanto, as organizações precisam tomar precauções – implementar controles de segurança apropriados – para minimizar esses riscos.

No entanto, antes de poder implementar os controles adequados para a organização, é preciso entender exatamente quais são esses riscos.

2.3.1 – VULNERABILIDADES

No ambiente da segurança podem-se considerar vulnerabilidades como falhas ou fraquezas que, se exploradas, ensejam na perda ou no vazamento de alguma informação. As vulnerabilidades podem ser encontradas no modo de agir das pessoas (por exemplo, aquelas que emprestam suas senhas a outros usuários), nos equipamentos (facilidade de se abrir um servidor, para ali colocar um equipamento de acompanhamento de teclado, ou falhas nos equipamentos de rede que podem ser exploradas por um DOS, por exemplo), ou nos sistemas ou *softwares* (erros que

permitem a execução remota de aplicativos com privilégios de administrador num *Web Server* ou presença de *software* malicioso, por exemplo).

Pelas razões abordadas é fundamental identificar as vulnerabilidades que podem contribuir para a ocorrência de incidentes de segurança, que é um aspecto importante na identificação de medidas preventivas.

De acordo com MOREIRA (2001), os riscos não podem ser determinados sem o conhecimento de até que ponto onde um sistema é vulnerável, à ação das ameaças. Em um processo de análise de segurança, devem-se identificar os processos críticos vulneráveis e saber se os riscos a ele associados são aceitáveis ou não. O nível de vulnerabilidade decai à medida que são implementados controles e medidas de proteção adequadas, diminuindo também os riscos para o negócio. Pode-se dizer que os riscos estão ligados ao nível de vulnerabilidade que o ambiente possui, pois para se determinar os riscos, as vulnerabilidades precisam ser identificadas.

Ainda segundo MOREIRA (2001), mencionam-se outras vulnerabilidades, também presentes em muitos ambientes, e que muitas empresas não atentam para determinadas situações:

- Senhas fracas;
- Falhas de implementação de segurança;
- Deficiência na Política de Segurança;
- Manuseio inadequado de informações confidenciais/críticas.

Para BASTOS (1998), as principais vulnerabilidades encontradas costumam ser relativa a erros, acidentes ou desconhecimento dos usuários que, impensadamente alteram configurações de equipamentos, divulgam contas e senhas de acesso, deixam sessões abertas na sua ausência, utilizam senhas frágeis facilmente descobertas (como o próprio nome ou palavras comuns) ou mesmo contaminam seus arquivos e programas com vírus de computadores.

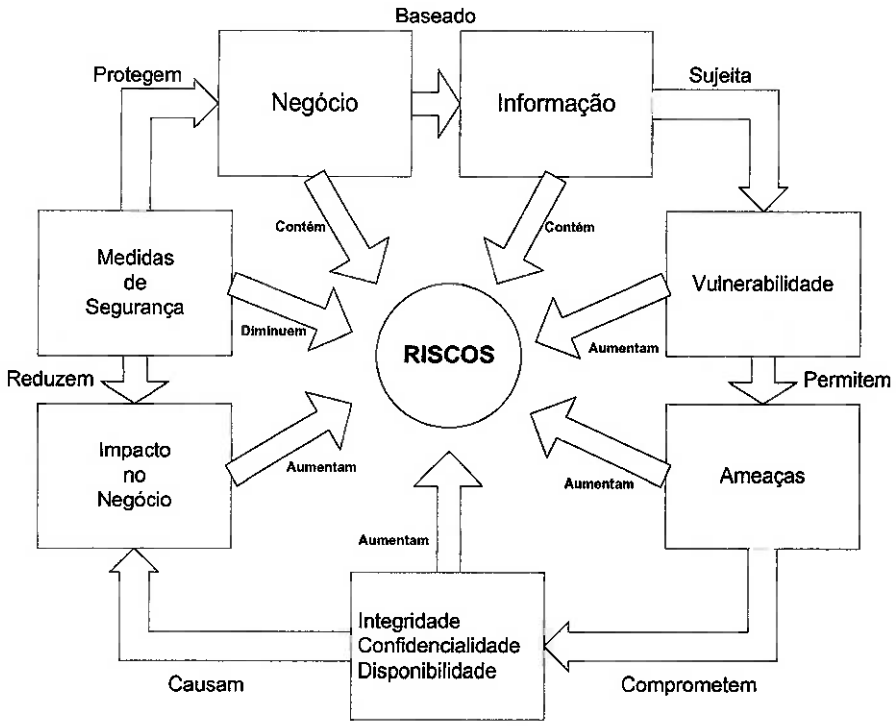

Figura 1 – Ciclo da Segurança da Informação (MOREIRA, 2001)

2.3.2 – A SEGURANÇA NA *INTERNET*

Segundo CT-STI (2000), as ameaças aos computadores e as informações das organizações podem ser assim resumidas:

- A *Internet*, sendo uma rede pública que não tem administração ou controle central é naturalmente insegura;
- Uma organização que utilize a *Internet* é responsável pela segurança de sua própria rede, de seus próprios sistemas e informações;
- Há pessoas na *Internet* – os "*hackers*" – que podem atacar sistemas de computadores e de informações somente pelo desafio de tentar obter acesso não autorizado. Os "*crackers*", por sua vez, são piratas virtuais que violam e roubam informações de bancos de dados;
- Os "*hackers*" e os "*crackers*" estão bem organizados e costumam trocar informações sobre ataques em *Web Sites* especiais. A

organização não pode subestimar a possibilidade de sofrer ataques dessas pessoas;

- Não é possível acompanhar o percurso de uma mensagem enviada pela *Internet*. As organizações não podem controlar o caminho que a mensagem tomará quando atravessa a *Internet*, digamos do Brasil para a Argentina;
- As mensagens podem ser interceptadas, lidas e modificadas;
- Se a organização importar uma informação da *Internet*, inclusive via correio eletrônico (o tratamento dos anexos merece cuidados especiais), ela se tornará vulnerável a ataques por vírus;
- A menos que devidamente cifrados, os pagamentos por cartão de crédito podem ser interceptados e manipulados, ou roubados;
- A importação de material ilegal via *Internet* pode ter conseqüências jurídicas. Existem diversas propostas de leis para tipificar crimes na *Internet* em tramitação no Congresso Nacional.

De acordo com CT-STI (2000), para entender em que medida a organização estará exposta na *Internet*, é preciso avaliar os riscos potenciais levando-se em conta:

- O valor das informações;
- O dano resultante de uma quebra da segurança;
- A probabilidade real de uma quebra de segurança vir a ocorrer, analisando as ameaças e os controles existentes.

Assim, ainda de acordo com CT-STI (2000), uma vez avaliado o nível de risco, é possível então determinar os controles necessários para reduzi-los a um nível aceitável. Os controles de segurança ajudarão a evitar:

- Quebras de confidencialidade;

- Invasão da privacidade – pessoal e organizacional;
- Roubo de informações;
- Vandalismo ou danos a sistemas e/ou informações;
- Perdas financeiras resultantes de fraudes.

2.4 – PRINCIPIOS DA SEGURANÇA DA INFORMAÇÃO

Os princípios da segurança da informação são essenciais para se proteger as organizações e são citados por CT-STI (2000) como sendo:

Disponibilidade – Considera-se este princípio quando um sistema, ou ativo de informação precisa estar disponível para satisfazer os seus requisitos ou evitar perdas financeiras.

Integridade – Considera-se este princípio quando um sistema, ou ativo de informação, contém informação que deve ser protegida contra modificações não autorizadas, imprevistas ou até mesmo não intencionais, incluindo ainda mecanismos que permitam a detecção de tais tipos de alteração.

Confidencialidade – Considera-se este princípio quando um sistema, ou ativo de informação, necessita de proteção contra a divulgação não autorizada dos seus bens de informação.

Autenticidade – Considera-se este princípio para atestar, com exatidão, o originador do dado ou informação, e não permitir o repúdio quanto a transmissão ou recepção do mesmo.

Já a norma ISO/IEC 17799:2000 que está baseada em práticas efetivas de gerenciamento da segurança, propõe que seu conteúdo torna-se uma ferramenta poderosa, e de aceitação internacional, a ser usada na implementação e manutenção de segurança em um Ambiente Computacional Complexo – ACC. A norma define que um ACC, para ser seguro, deve, proporcionar:

- **Confidencialidade** – que é a garantia que a informação só é acessada por quem realmente tem este privilégio;
- **Integridade** – que é a garantia de que a informação só será alterada por quem tem este direito;
- **Disponibilidade** – que é a garantia de que apenas usuários autorizados terão acesso à informação e aos ativos correspondentes.

2.5 – POLÍTICAS DE SEGURANÇA

Segundo a norma ISO/IEC 17799:2000, seus objetivos são descrever a importância de uma política de segurança bem como relacionar os principais assuntos que devem ser abordados nesta política.

A administração deve estabelecer uma política clara e demonstrar apoio e comprometimento com a segurança da informação através da definição e manutenção de uma política que deverá ser seguida por toda a organização.

O documento de política da segurança da informação deve expressar as preocupações da administração com a segurança de suas informações. Deve também ter o poder de estabelecer as diretivas para o gerenciamento da segurança. É importante que a política seja aprovada e apoiada pela administração, publicada e comunicada a todos os funcionários, com o aceite de cada um, de preferência por escrito.

Para a RFC 2196 (2000) uma política de segurança é a expressão formal das regras pelas quais é fornecido acesso aos recursos tecnológicos da empresa.

O principal propósito de uma política de segurança é informar aos usuários, equipe e gerentes, as suas obrigações para a proteção da tecnologia e do acesso à informação. A política deve especificar os

mecanismos através dos quais estes requisitos podem ser alcançados. Outro propósito é oferecer um ponto de referência a partir do qual se possa adquirir, configurar e auditar sistemas computacionais e redes, para que sejam adequados aos requisitos propostos. Portanto, uma tentativa de utilizar um conjunto de ferramentas de segurança na ausência de pelo menos uma política de segurança implícita não faz sentido.

Uma política de uso apropriado (*Appropriate* – ou *Acceptable – Use Policy* – AUP) pode também ser parte de uma política de segurança. Ela deveria expressar o que os usuários devem e não devem fazer em relação aos diversos componentes do sistema, incluindo o tipo de tráfego permitido nas redes. A AUP deve ser tão explícita quanto possível para evitar ambigüidades ou maus entendimentos. Por exemplo, uma AUP pode lista *newsgroups* USENET proibidos.

De acordo com CT-STI (2000), uma política de segurança relativa à *Internet* é uma declaração ampla dos objetivos e intenções da organização com relação à conexão e ao uso.

A política de segurança de uma organização pode ser resumida em uma ou duas páginas. Normalmente, ela deve especificar o seguinte:

- Os serviços que podem ser usados;
- Quem autoriza as conexões;
- Quem é responsável pela segurança;
- As normas, diretrizes e práticas a serem obedecidas;
- As responsabilidades dos usuários.

Isto é necessário para assegurar que as informações e os ativos da organização estarão protegidos contra um ataque através do serviço oferecido na *Internet*.

Uma questão fundamental é decidir quem será responsável pela segurança na organização. Todos os usuários terão um papel a

desempenhar, mas, em última análise, os gerentes de alto escalão são os responsáveis por assegurar a implementação e manutenção dos controles de segurança adequados.

Se todos entenderem a necessidade dos controles de segurança e suas próprias responsabilidades para com eles, haverá menos probabilidade de uma quebra de segurança na organização. Para definir a política da organização é preciso:

- 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.

2.6 – CONTROLES DA SEGURANÇA

Para CT-STI (2000), como ocorre com todos os aspectos da gestão da segurança, serão necessários alguns controles de procedimentos técnicos e de pessoas. A complexidade dos procedimentos dependerá do serviço disponibilizado ou utilizado na *Internet*.

O CT-STI (2000), relaciona abaixo algumas das técnicas específicas de segurança, a serem consideradas juntamente com o tipo de proteção que podem oferecer. É recomendável buscar aconselhamento de especialistas em segurança para a implementação adequada de algumas dessas técnicas. Isso ajudará uma organização a se certificar de que a conexão à *Internet* atende aos seus requisitos de segurança.

Cifração – Usada principalmente para proteger o conteúdo dos arquivos de informações, de mensagens e de transações financeiras durante sua transmissão através da *Internet*. Há, entretanto, regras que cobrem o

licenciamento de alguns produtos criptográficos, especialmente se esses são exportados de um país para outro.

Identificações Digitais – As identificações digitais permitem provar a identidade do usuário no envio de mensagens importantes. Elas também são utilizadas para proteger a integridade da mensagem, de modo a evitar alterações.

"*Firewalls*" – São computadores que ficam entre as redes de computadores da organização e a *Internet*, que colocam em prática a política de segurança definida. Os "*firewalls*" evitam e detectam quaisquer ataques à segurança, controlando quais são as conexões de *Internet* com entradas e saídas permitidas na organização. Como todas as ferramentas de segurança, os "*firewalls*" devem também ser controlado para evitar o acesso ou modificações não autorizadas.

A solução a utilizar deve não apenas atender às necessidades da organização, mas também às estabelecidas pela política de segurança. Para muitas organizações, a conexão com um provedor de serviços terceirizados a partir de um computador pessoal individual poderá ser a melhor solução, em termos da proteção e do gerenciamento da segurança e da relação custo/benefício.

Ainda SELEGUIM (2002), cita algumas outras técnicas para controle da segurança como sendo:

Sistemas de Detecção de Intrusos – São sistemas inteligentes, capazes de detectar tentativas de invasão em tempo real. Estes sistemas podem apenas alertar sobre a invasão, como, também, aplicar ações necessárias contra o ataque. Eles podem ser sistemas baseados em regras ou adaptáveis, no primeiro as regras de tipos de invasões e a ação a ser tomada são previamente cadastradas. O problema é que a cada dia surgem novos tipos de ataques e estas regras precisam estar sempre atualizadas para o sistema ser realmente eficaz. No segundo tipo, são empregadas

técnicas mais avançadas, inclusive de inteligência artificial, para detectarem novos ataques, sempre que surgirem.

Logs – *Logs* são registros gerados pelos sistemas ou aplicações, sobre informações de eventos ocorridos. É considerado uma medida básica de segurança, mas muitas vezes não é utilizado pelos administradores, ou porque está desativado, pois dependendo do sistema e do *hardware*, a geração do *Log* pode se tornar lenta, ou porque esquecem ou não querem analisá-lo, já que os *Logs* geralmente são relatórios enormes. Mas é uma ferramenta útil para auditorias de acesso, verificação do que está sendo utilizado, possível falha nos sistemas, entre outros.

Antivírus – *Software* que verifica a existência de vírus em uma máquina, pasta, arquivo e ao encontrá-lo, executa a limpeza. A maneira como ele fará isso pode ser totalmente configurada pelo usuário. O padrão é o antivírus analisar e quando encontrar algum vírus, tentar eliminar apenas o vírus, caso não consiga, se o usuário autorizar, ele removerá o arquivo também. Uma vez instalado o antivírus em um micro, ele pode ser configurado, dependendo da sua característica, para ficar ativo e analisar tudo o que for aberto no micro, caso apareça algum vírus, ele avisa imediatamente. Mas como diariamente surgem novos tipos de vírus, é importante o usuário ficar atento e atualizar o seu antivírus sempre que possível.

Backup – Uma das ferramentas existentes para segurança dos dados são os *softwares* de *backup* e *restore*, que servem para fazer cópias de segurança das informações e de sistemas de uma empresa e recuperar as informações quando necessário. Todos os dados e sistemas de uma empresa devem possuir cópias de segurança íntegras, atuais e armazenadas em local seguro. Em geral, o *backup* é feito em fita, disquete ou outra mídia portátil que pode ser armazenado para futura utilização, como no caso de algum desastre ou perda de informações. As informações podem ser perdidas por causa de acidentes, desastres, ataques, erros de sistema ou *hardware* ou falha humana, entre outros motivos. Com as informações

atualizadas copiadas através de *backups* para alguma mídia, quando houver uma perda de dados, basta restaurar estas informações.

Em geral as técnicas apresentadas, utilizadas em conjunto, garantem um certo nível de proteção para as informações da empresa, mas como dito anteriormente nenhuma proteção funciona 100%.

2.7 – MONITORAÇÃO DA SEGURANÇA

De acordo com CT-STI (2000), é necessário examinar regularmente os controles implementados pela organização. Isso deve ser feito para assegurar que os controles estão sendo usados de forma adequada e que ainda proporcionam um nível de proteção que atenda às necessidades da organização. A configuração técnica de algumas soluções – em especial os *firewalls* – é vital para a proteção das informações da organização. Modificações não autorizadas podem causar uma falha de segurança que pode ser explorada.

É importante que a conexão à *Internet* seja continuamente monitorada para registrar todos os eventos ligados à segurança: todos os alarmes e todos os incidentes. Esses registros devem ser examinados regularmente. Isso é necessário para detectar se alguém tentou quebrar os controles de segurança estabelecidos.

Diversas organizações percebem que, com o uso da *Internet*, suas razões iniciais para utilizar o serviço se modificam – especialmente quando a conexão inicial fornece somente serviços básicos. Muitas das que começaram a usar a *Internet* simplesmente para fins de correio eletrônico, evoluíram os conceitos, desenvolveram *Web Sites* e agora estão passando a adotar o *e-business* ou aprimorando seus *call-centers* com as modernas práticas de CRM – *Customer Relationship Management*, ou Gerenciamento de Relacionamento com o Cliente. Com a confiança e a experiência no uso dos serviços da *Internet*, as necessidades da organização também podem

mudar. Se isso ocorrer, a organização precisará percorrer todo o ciclo novamente – desde a definição das necessidades do negócio até a implementação dos controles de segurança.

Para CT-STI (2000), isto é necessário para assegurar a segurança adequada para a organização, que atenda às necessidades específicas da sua área de atuação ou negócio. As etapas necessárias estão ilustradas abaixo:

- Revisar o caso da organização para incorporar as necessidades modificadas do negócio (*e-business*);
- Avaliar os riscos;
- Rever a política de segurança para atender a quaisquer mudanças nos níveis de risco;
- Implementar os controles de segurança que atendam aos requisitos da política;
- Monitorar e manter a eficácia dos controles de segurança.

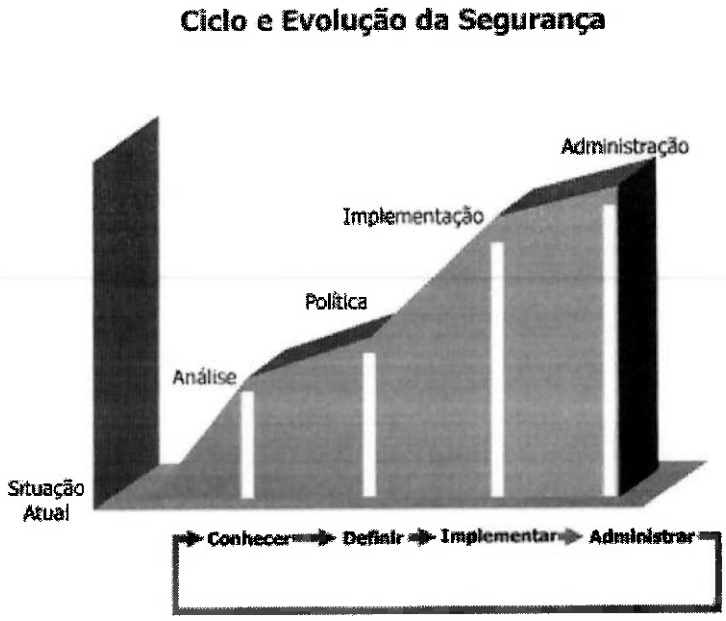

Figura 2 – Ciclo e Evolução da Segurança (CT-STI, 2000)

CAPÍTULO 3 – A TRANSMISSÃO PAULISTA (CTEEP)

3.1 – INTRODUÇÃO

"A reestruturação do setor elétrico brasileiro induziu à desverticalização das antigas concessionárias, promovendo a separação das áreas de geração, transmissão e distribuição de energia elétrica.

Dentro desse novo cenário, o Estado de São Paulo, pela Lei Estadual nº 9361, de 5 de julho de 1996, criou o Programa Estadual de Desestatização – PED, responsável pela reestruturação societária e patrimonial do setor energético paulista. Essa Lei mantém assegurado o controle acionário das empresas de transmissão pelo Governo Estadual, com a propriedade de, no mínimo, 51% das ações com direito a voto.

Ainda em conformidade com essa Lei, houve a cisão parcial da CESP Companhia Energética de São Paulo e da Eletropaulo – Eletricidade de São Paulo S.A., as principais concessionárias paulistas do setor elétrico à época, dando origem a empresas de geração, transmissão e distribuição.

As empresas de transmissão oriundas desse processo de cisão foram, na CESP, a Transmissão Paulista (CTEEP) e, na Eletropaulo, a EPTE – Empresa Paulista de Transmissão de Energia Elétrica S/A." CTEEP (2002).

3.1.1 – A CTEEP

"A empresa CTEEP, criada em abril de 1999, dispõe de 11.000 quilômetros de linhas de transmissão, com as seguintes classes de tensão: 88, 138, 230, 345 e 440 quilovolts (kV). São mais de 17.000 quilômetros de circuitos e 75 subestações, distribuídas praticamente por todo o território do Estado de São Paulo. Um sistema que soma uma capacidade de transformação de 18.000 megavolts-ampére (MVA).

A competência da CTEEP já conta com aval internacionalmente reconhecido. A gestão do Centro de Operação do Sistema São Paulo (COS–

SP), localizado no município de Jundiaí, está inteiramente dentro dos padrões da norma ISO 9002. A conquista dessa certificação é exemplo inequívoco da seriedade do trabalho da companhia. Em novembro de 1999 este Centro recebeu um novo Sistema de Supervisão e Controle – SSC, o mais moderno do País, que em seguida foi instalado nos Centros Regionais de Operação (CRO) de Bauru e Cabreúva para que, com uma atuação integrada, fossem ampliadas a confiabilidade e a qualidade da coordenação, supervisão e controle em tempo real do sistema elétrico." CTEEP (2002).

3.1.2 – A EPTE

"A empresa EPTE – primeira empresa brasileira voltada exclusivamente para a prestação do serviço de transmissão de eletricidade – iniciou suas atividades em janeiro de 1998, tendo sob sua responsabilidade o transporte de energia do sistema interligado Sul/Sudeste/Centro–Oeste para as distribuidoras Eletropaulo Metropolitana e Bandeirante, concessionárias também oriundas da cisão da antiga Eletropaulo, numa região onde se concentram mais de 20 milhões de habitantes, com uma atividade econômica correspondente a cerca de 27% da formação da renda nacional. O Centro Regional de Operação São Paulo (CRO) da EPTE recebeu nova versão do Sistema de Supervisão e Controle – SSC, passando a atuar de forma integrada com o Centro de Operação do Sistema São Paulo (COS-SP), assim como com os CROs da CTEEP.

Este Centro Regional conta com certificação ISO 9002, obtida em junho de 2001, sinônimo de reconhecimento internacional da sua capacitação." CTEEP (2002).

3.1.3 – A UNIFICAÇÃO CTEEP/EPTE

"Como CTEEP e EPTE executam as mesmas atividades para a transmissão de energia elétrica, em áreas geograficamente complementares

dentro do Estado, em outubro de 1999 uma diretoria única assumiu a administração das duas empresas.

O primeiro reflexo dessa administração unificada foi a possibilidade de se integrar a operação dos sistemas CTEEP/EPTE, trazendo benefícios que foram sentidos no dia-a-dia das empresas, com troca de experiências, melhoria da qualidade dos serviços e confiabilidade da supervisão, controle e operação dos serviços de transmissão de energia elétrica.

Desde aquela data, estudos foram iniciados para a unificação das transmissoras de energia elétrica paulistas. Esses estudos, autorizados pelo Conselho Diretor do PED, levavam em conta o aproveitamento de sinergias da CTEEP e da EPTE, ganhos de escala, otimização de recursos e redução de despesas, culminando com a proposta de incorporação da EPTE pela CTEEP.

Os Conselhos de Administração das duas empresas referendaram esta proposta, que, apreciada e aprovada pelas Assembléias Gerais de Acionistas, resultou numa única empresa de transmissão – a CTEEP – maior e mais eficiente.

O controle acionário, conforme determina a Lei Estadual nº 9361, continua com o Governo do Estado de São Paulo, detentor da maioria do capital votante – 65% das ações ordinárias (ON).

Com um ativo total superior a R$ 4 bilhões, a "nova" CTEEP tem a tarefa de operar 99 subestações, com capacidade de transformação acima de 35.000 MVA, e mais de 18.000 quilômetros de linhas de transmissão, transportando cerca de 136.000 GWh de energia, além de contar com um sistema integrado de coordenação, supervisão e controle do sistema elétrico.

No comando desse complexo eletro-energético que dispõe ainda de sistema próprio de telecomunicações, está um quadro de empregados de alto nível, preparado para atender as demandas de um mercado cujas exigências avançam continuamente." CTEEP (2002).

3.1.4 – ALGUNS DADOS SOBRE A EMPRESA

RECURSOS HUMANOS	DADOS TÉCNICOS
3.164 empregados (1.559 na capital e 1.605 no Interior) 2.794 homens e 370 mulheres Idade média de 40 anos Escolaridade: ensino fundamental – 647; médio – 1.431; superior – 974 e pós-graduados – 122. Funções: administrativas, técnicas e operacionais – 2.307; universitários – 754 e executivos – 103.	35.604 MVA de capacidade instalada de transformação 18.022 km de circuitos de transmissão 11.515 km de linhas de transmissão 99 subestações em operação 326 transformadores 145 estações de microondas 891 km de cabos de fibra ópticas 135.580 GWh de energia transportada em 2000
ADMINISTRAÇÃO	**RETRATO ECONÔMICO**
Frota: 500 veículos Fornecedores: 8.000 Acervo imobiliário: 18.930 imóveis de servidão de passagem e de Domínio.	Ativo: cerca de R$ 4,1 bilhões Patrimônio: cerca de R$ 3,3 bilhões Faturamento: R$ 711 milhões Total de ações: 150 bilhões (aproximadamente) OBS: O estado continua no controle da Empresa com 65% das Ações Ordinárias (ON) e 16% das Preferenciais (PN).

Tabela 1 – Dados sobre a CTEEP (JORNAL INTERLIG, 2001)

3.2 – A ARQUITETURA COMPUTACIONAL DA CTEEP

A CTEEP conta, hoje, com uma plataforma tecnológica atualizada, provida de equipamentos de informática (*hardwares*) e ainda vários programas (*softwares*) mais adequados às necessidades da empresa, trabalhando com sistemas operacionais de última geração, interligados a uma estrutura atual de comunicação de Rede Lógica, representando uma melhoria e incremento em seu parque de informática.

3.2.1 – O PARQUE COMPUTACIONAL

A empresa conta hoje com um vasto parque computacional, composto principalmente pelas plataformas de *hardware* SUN e Intel, e pelas plataformas Windows, Solaris, Oracle e Lotus Notes como *software*, que possibilitam sua utilização como servidores *Web*, tornando disponíveis informações na rede corporativa que, através de ferramentas de consultas diversas, permitem explorar com maior eficiência as informações corporativas localizadas em Servidores *Web*, atendendo a diretriz que define a interface *Web* padrão na companhia.

Todas as máquinas estão interligadas por uma rede interna hierárquica, padrão *Ethernet* a 10 e 100 Mbps, utilizando protocolo TCP/IP. A essa rede estão ligadas diversas estações de trabalho e centenas de microcomputadores.

Também está conectado a essa rede um servidor de comunicações, com várias linhas de acesso discado, para permitir aos usuários da rede a utilização dos recursos a partir de casa.

Cada Gerência da empresa, espalhada pelo interior do estado, conta com seu parque computacional próprio, que estão interligados ao *backbone* da CTEEP via *Frame Relay* (alugado) ou Rádio (próprio).

A CTEEP conta ainda com impressoras matriciais, jato de tinta e *laser*, câmeras e monitores de alta resolução.

Para atender as necessidades das empresas está sendo desenvolvido estudo para redimensionamento do parque computacional, com características de disponibilidade e performance capazes de atender a demanda que será gerada a partir de todo este processo de reorganização empresarial.

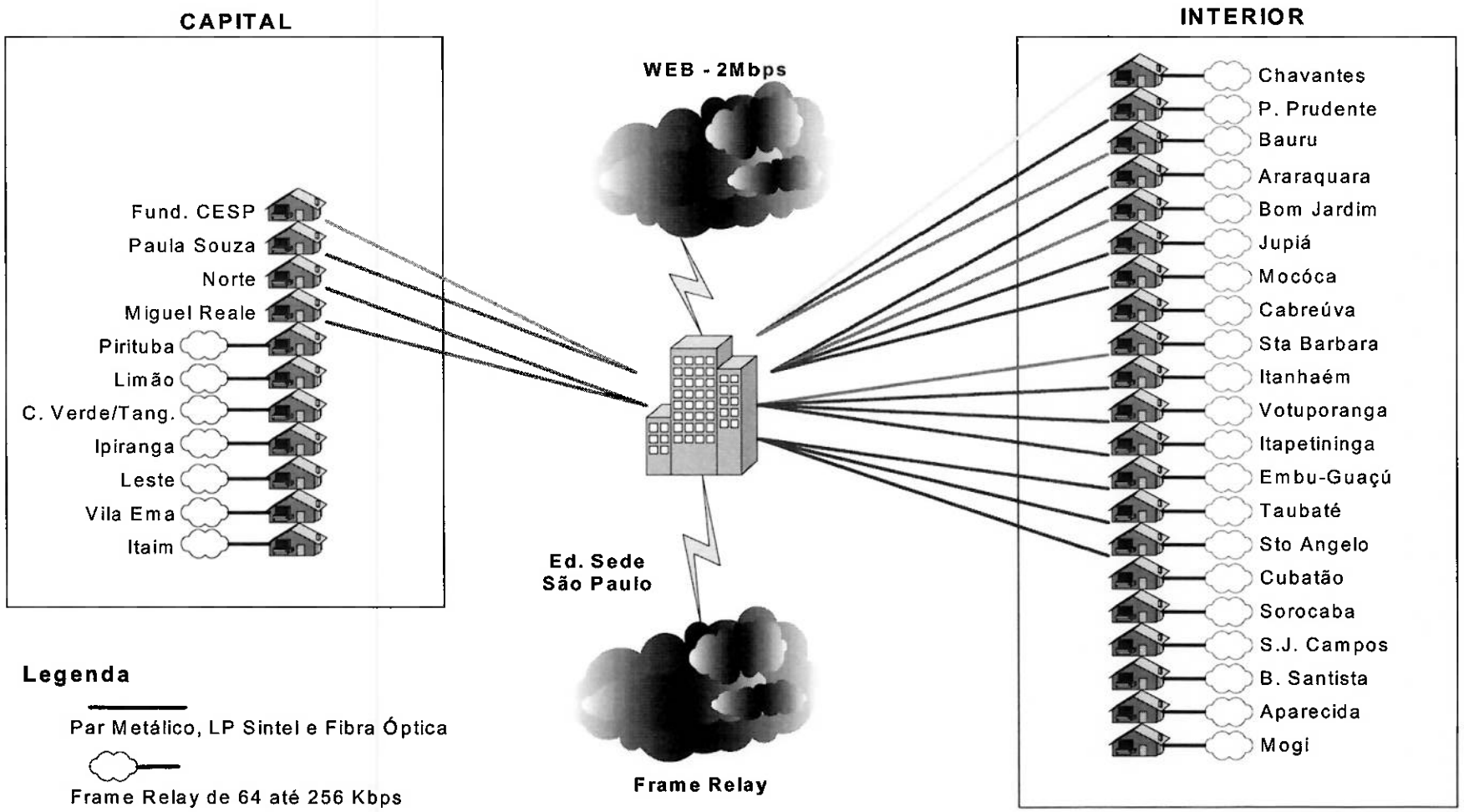

Figura 3 – Mapa da rede corporativa (CTEEP, 2002)

3.2.2 – SERVIDORES DE BANCO DE DADOS

Os Servidores de Banco de Dados tem como característica principal a divisão de tarefas entre o cliente, a estação de trabalho que ordena através das aplicações o acesso aos bancos de dados, e o servidor, que executa tarefas, tais como: atualizações, supressões, procura de dados e todas as outras tarefas próprias do gerenciamento de banco de dados, porém, sob as ordens da estação de trabalho (Cliente).

A vantagem é evidente: dividindo o processamento em dois sistemas, temos de saída a diminuição do tráfego de dados na rede. Com isto, o desempenho aumenta pois é evitado de se processar os dados, fazendo-os transitar pela rede, entre a estação de trabalho e o servidor, pelo menos duas vezes. Ao invés disso, os dados são armazenados em variáveis do processo em alguns parâmetros e são enviados ao servidor. Estes ao chegarem são recepcionados pelo Oracle que os envia para *Stored Procedure*, que então inicia o processamento desejado até seu final de dentro do servidor, limitando-se a avisar a estação de trabalho o término do processo, com sucesso ou não.

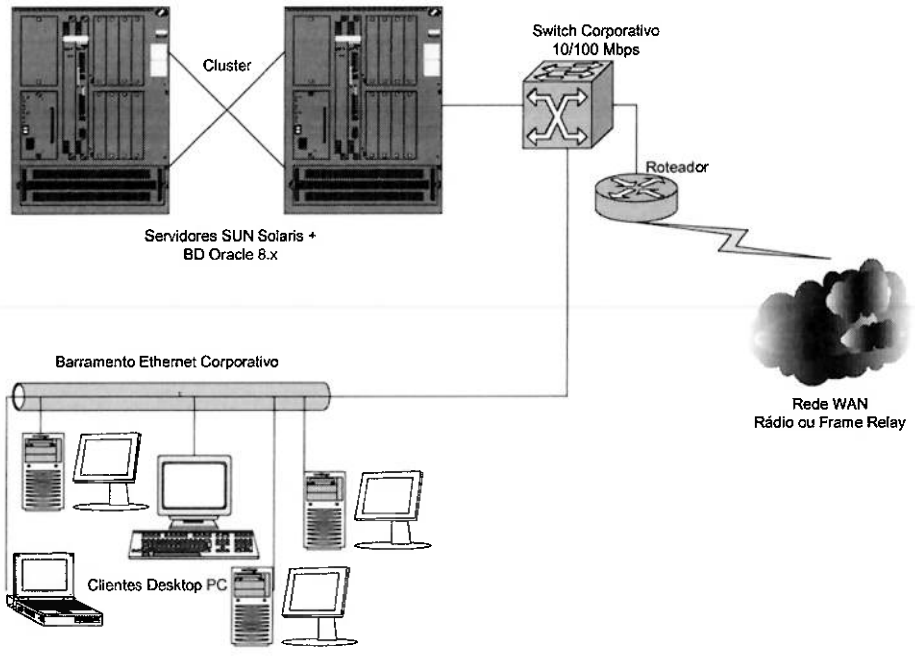

Figura 4 – Ambiente de Banco de Dados

3.2.3 – SERVIDORES DE ARQUIVOS E IMPRESSORAS

O *Novell NetWare* é uma solução de *software* de serviços que oferece um acesso aos principais recursos de rede. Ele permite que acesse arquivos, impressoras e outros serviços em qualquer tipo de rede, plataforma de armazenamento e *desktop* cliente, também é realizado neste ambiente a autenticação de todos os usuários da rede corporativa.

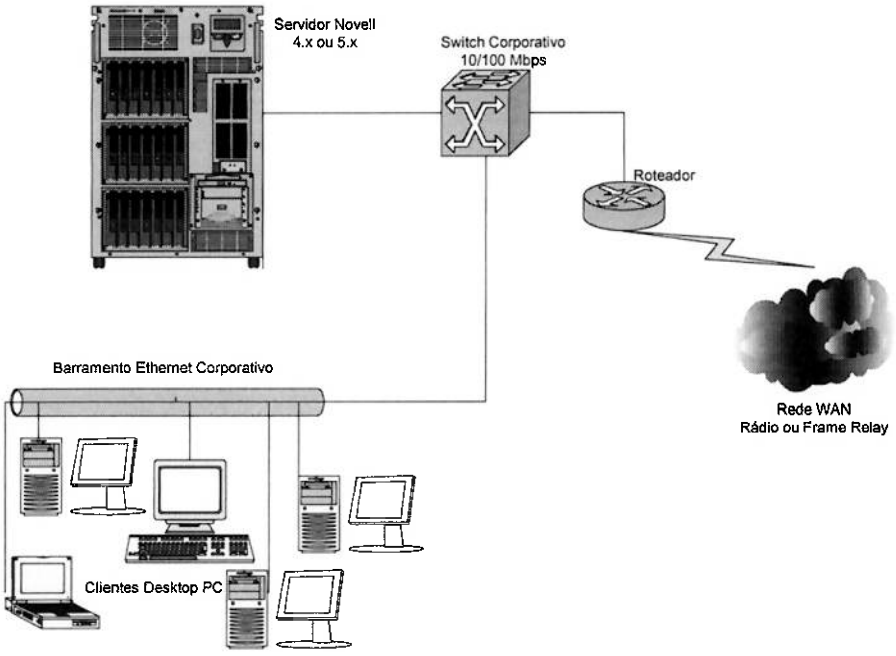

Figura 5 – Ambiente de Autenticação, Arquivos e Impressoras

3.2.4 – SERVIDORES DE *E-MAIL* E APLICAÇÕES PARA COLABORAÇÃO

Prove troca de mensagens, e aplicações de colaboração, por uma plataforma integrada para interações *on-line* seguras entre empregados ou com os clientes, sócios e provedores.

Redefinindo assim o conceito de administrar o negócio com *workplaces* dinâmico e outros modos inovadores de conectar idéias, pensadores, compradores, vendedores e comunidades em um em mundo de demanda.

Sendo assim, aumenta a produtividade humana unindo as pessoas através de troca de mensagens, agendas & programações e aplicações colaboradoras - diminuindo o custo total de sua troca de seu serviço de mensagens e infra-estrutura de colaboração.

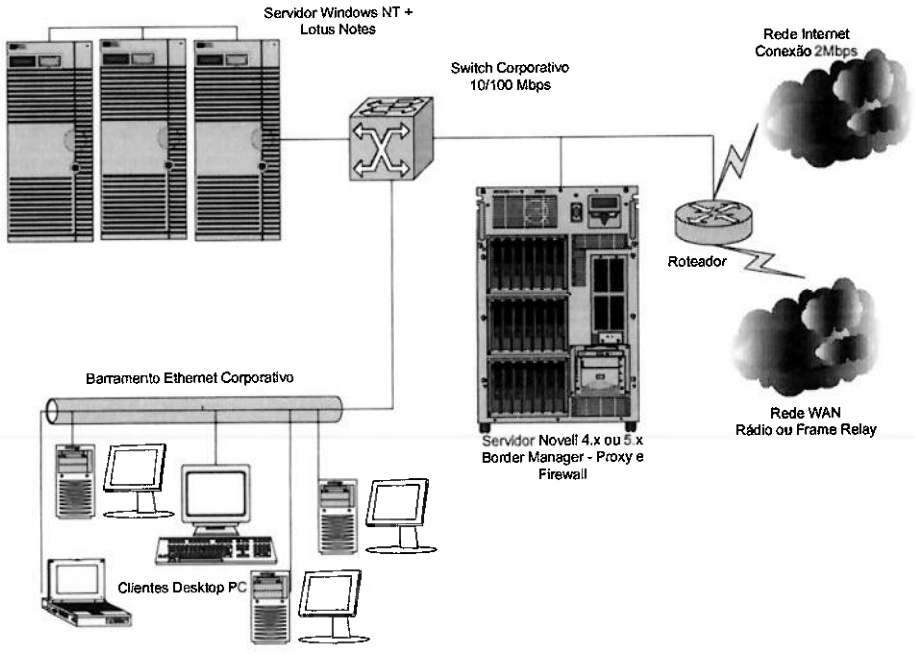

Figura 6 – Ambiente de Colaboração

3.2.5 – SERVIDORES *WEB* E *PROXY*

O *Novell BorderManager* é uma das principais soluções de acesso e segurança da *Novell*. Com seus recursos integrados a diretórios, é possível controlar, acelerar e monitorar as atividades dos usuários na *Internet*. Como o *Novell BorderManager* se beneficia do controle de acesso baseado em identidades e dos *proxies* de encaminhamento, protegendo assim a rede contra conteúdo indesejável da *Internet*, ao mesmo tempo em que mantém níveis de desempenho.

O *Web Server* oferece excelente performance e robustez para comunicação interna e externa da empresa. Dados, produtos e serviços podem ser disponibilizados de forma segura na *Internet* ou na *intranet*. A solução suporta altos volumes de tráfego e possibilita a hospedagem de múltiplos domínios virtuais, utilizando o *software* mais confiável da sua categoria.

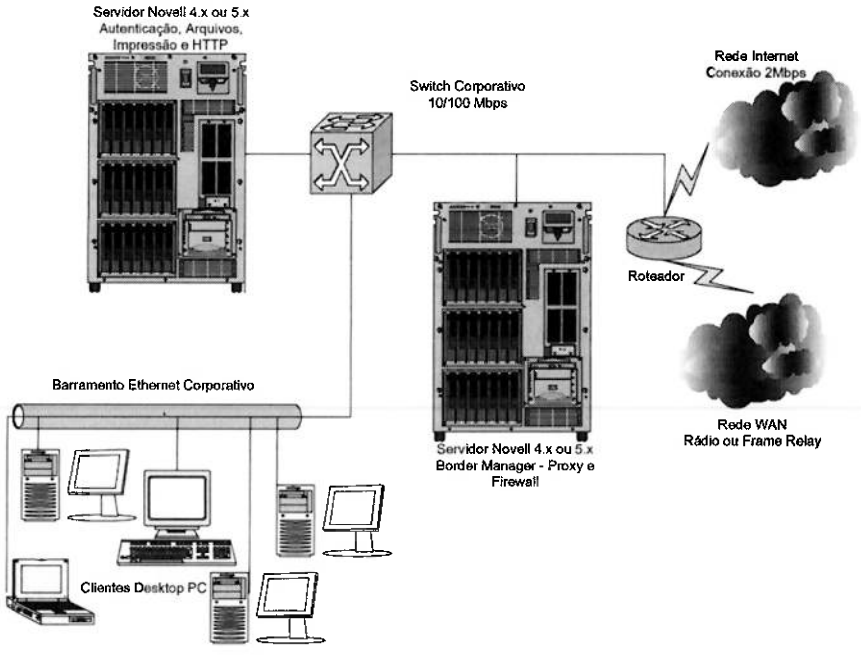

Figura 7 – Ambiente *WEB* e *Proxy*

3.2.6 – SERVIDOR *DNS*

O *DNS – Domain Name System* é o serviço para resolução de endereços para ambientes *Internet* e *Intranet*. A solução padroniza o endereçamento, facilitando a utilização pelo usuário e as modificações e atualizações na estrutura da rede. Com recurso de *cache*, agiliza o atendimento de novas requisições de tradução de endereços. Tem características que permitem níveis de segurança adequados ao ambiente de *Internet*.

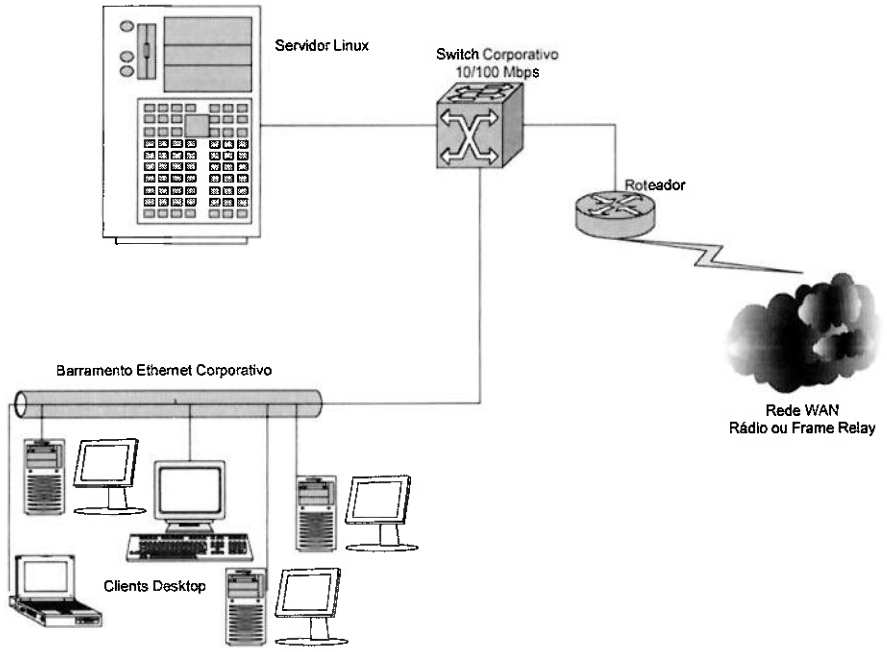

Figura 8 – Ambiente *DNS*

3.2.7 – SERVIDORES DE APLICATIVOS

O *Citrix Metaframe* é uma solução combinada de h*ardware* e *software* que faz com que aplicativos corporativos desenvolvidos para plataformas Windows (como *Visual Basic*, *Delphi* e outros) e produtos de automação de escritórios como *Word*, *Excel*, *PowerPoint*, *Access*, Correio Eletrônico, *CorelDraw*, etc, possam ser disponibilizados a todas as unidades da organização com um alta performance. É valido lembrar que esses aplicativos foram desenvolvidos objetivando um ambiente de rede local (*LAN*), não considerando as dificuldades e limitações de um ambiente distribuído (*WAN*).

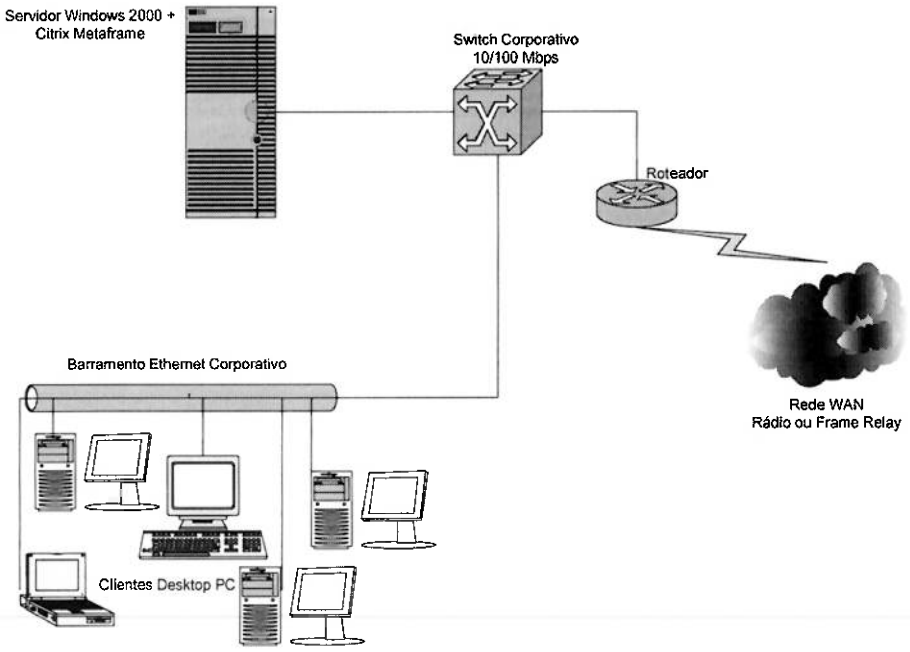

Figura 9 – Ambiente de Aplicações

3.2.8 – SERVIDORES ADMINISTRATIVOS DIVERSOS

Neste ambiente contamos com vários serviços de grande utilidade para o dia-a-dia da empresa, pois reduzem a necessidade de intervenção humana nos *desktops* e também automatizam tarefas do cotidiano.

Dentre os serviços disponíveis podemos citar:

- **Servidor para geração de *PDFs*:** Este servidor realiza a conversão de documentos em qualquer formato para o formato *PDF*, de maneira simples para o usuário;
- **Servidor para atualização do Antivírus:** Este servidor é responsável pela instalação e atualização das versões de antivírus nas estações *desktop*;
- **Servidor de licenças do *Autocad*:** Neste servidor é realizada a distribuição de licenças do aplicativo *Autocad*, permitindo assim um controle central das licenças;
- **Servidor *Infocast*:** Este serviço é responsável em transformar e distribuir as informações que chegam diariamente ao Grupo Estado em incomparáveis ferramentas de trabalho e negócios para os executivos da Companhia.

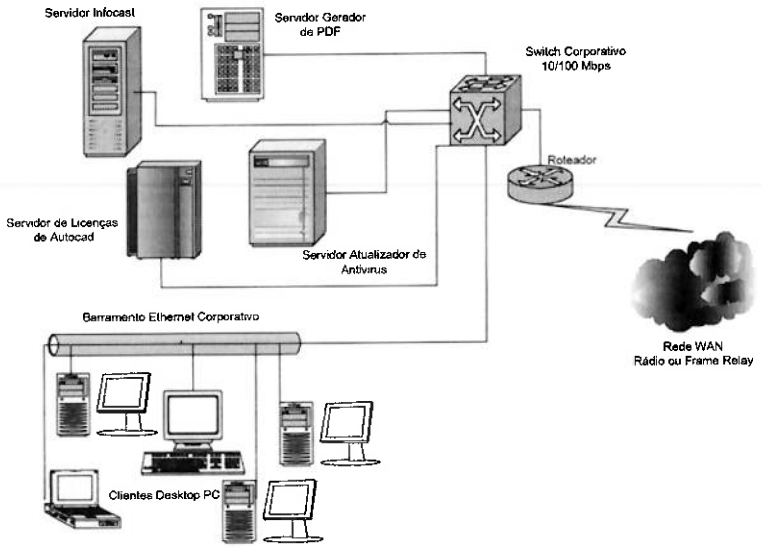

Figura 10 – Ambiente Administrativo

3.2.9 – CLIENTE *DESKTOP*

O ambiente *desktop* é composto por estações do tipo IBM PC, padrão *Intel* e contam com sistema operacional que variam entre *Windows* 95, *Windows* 98 e *Windows* 2000 *professional*.

Como padrão para o *Backoffice*, são utilizados o pacote *Microsoft Office*, que também pode ser encontrado nas versões MS *Office* 95, MS *Office* 97 e MS *Office* XP.

Alem dos aplicativos padrões como *Adobe Acrobat Reader* e *Winzip*, todas as estações contam com sistema antivírus da *Symantec*, que é atualizado toda vez em que usuário realiza sua autenticação na rede.

O *Browser* padrão utilizado pela companhia é o *Internet Explorer* 5.x.

3.4 – O DEPARTAMENTO DE TI

A Divisão de Tecnologia da Informação conta com 52 empregados e está, subordinada à Diretoria Administrativa.

Esta equipe é responsável pela implantação e manutenção, do seguinte parque computacional:

- 1.700 estações;
- 50 servidores;
- 700 impressoras;

Esta equipe ainda realiza o atendimento de suporte a cerca de 3.200 usuários.

Anteriormente à adoção do ERP a empresa contava com sistemas desenvolvidos internamente para as funções, Financeira, Suprimentos, Recursos Humanos e Folha de Pagamento, em um Ambiente Computacional constituído por *Mainframe*, Banco de Dados *ADABAS* e linguagem *Natural*.

CAPÍTULO 4 – PROPOSTA PARA POLÍTICA DE SEGURANÇA

Com base nas informações fornecidas por ZWICKY et al. (2001) e por NIC BR *SECURITY OFICE* (2003), formulou-se linhas mestras para a elaboração de um documento de política de segurança. O objetivo é encontrar o melhor modelo considerando:

- Custo da segurança;

Em ambientes conectados à *Internet*, não se pode assumir segurança absoluta, mesmo que se tenha a disposição recursos financeiros ilimitados.

- Funcionalidade;

As pessoas não gostam de trabalhar ou estudar em ambientes hostis, então, por um lado se perde em segurança e por outro se perde em funcionalidade, sempre.

- Compatibilidade cultural;

Regulamentar o comportamento do usuário de acordo com o que está dentro de seus costumes é fator decisivo no sucesso da implantação da política de segurança.

- Aspectos legais.

É importante que haja conformidade entre as penalidades impostas no documento de política de segurança e a lei vigente no País.

4.1 – CONTEÚDO

A política de segurança deve ser vista como um canal de comunicação entre usuários e administradores da rede. Precisa explicar a importância da segurança para motivar o usuário a praticá-la.

É importante incluir no documento a mensagem de que a responsabilidade por atos prejudiciais é de todos. É hostil e injusto distribuir um documento que especifica apenas as obrigações dos usuários.

A maioria das pessoas não convive com textos jurídicos nem são especialistas em computação. É preferível portanto, utilizar uma linguagem casual para formular o documento de política de segurança mesmo que ele não ganhe toda aparência oficial que se deseja.

Mais do que escrever o documento, é necessário usa-lo como regra todos os dias. Isto significa que se a política não é seguida, algo deve ser feito para consertar a situação. O profissional de segurança da informação deve ser responsável por fazer tais correções acontecerem e esta afirmação também deve estar contida no documento, assim como outras:

- Gerentes de certos serviços têm autoridade para revogar acesso de usuários subordinados a ele;
- Gerentes terão como responsabilidade avaliar transgressões ocorridas em seus setores;
- O administrador da rede, em conjunto com a diretoria pode cessar recursos que não se enquadram nos padrões da empresa.

A política deve especificar quem decide e dar indícios de quais penalidades estão previstas para cada caso descrito. Porém não deve apontar o que acontecerá em seguida com muita exatidão, já que não se tratam de sentenças de lei, mas sim de políticas.

- Nenhuma política atinge a perfeição;
- Não é possível prever cada caso e documenta-los;
- Entretanto, é preciso especificar as exceções que podem ocorrer em cada processo.

Prever que a política sofrerá revisões é necessário. Nunca se pode dar por encerrada a formulação do documento. Com o passar do tempo novas necessidades precisam ser documentadas e o lançamento destas, é importante para a continuidade efetiva da política.

No momento em que se precisa aprofundar o detalhamento técnico que descreve os sistemas do qual a rede é formada, algumas questões são relevantes para o processo de formulação do documento de política de segurança. Entre elas:

- A quem é permitido ter conta no sistema?
- Existem contas temporárias para visitantes?
- Como tratar fornecedores, parceiros e clientes?
- As contas podem ser compartilhadas entre mais de um usuário?
- Secretárias e auxiliares podem receber permissão para ler correspondência eletrônica de seus superiores?
- De que forma disponibilizar informações de projeto para os parceiros da organização?
- Membros das famílias dos funcionários recebem algum privilégio no sistema?
- Como tratar os empréstimos informais de credenciais de acesso ao sistema?
- Em que circunstâncias um funcionário perde sua credencial de acesso? E quando a recebe de volta?
- Os funcionários podem servir conteúdo em seus computadores?
- Quais procedimentos os usuários devem tomar quando necessitarem ligar um computador pessoal (ou externo) na rede?
- Informações financeiras da corporação precisam tratamento especial? (criptografia, *backups* extra etc...)
- Como deve ser a formulação das senhas dos usuários e com que freqüências devem ser renovadas?
- Quais são os limites de uso da *Internet*? Quais as penalidades para os infratores?

- Que precauções devem ser seguidas em ordem de se evitar infecções por vírus na rede?
- Quais procedimentos devem os usuários tomar para manter seus computadores domésticos tão seguros quanto os da empresa?
- Devem existir recursos/privilégios especiais para funcionários viajantes?
- Quais pré-requisitos devem-se atender antes de se projetar *sites* de comércio eletrônico dentro da empresa?
- Quais informações são confidenciais? Como serão protegidas? Podem ser transmitidas por meios não criptografados?
- Quais as responsabilidades com relação à equipamentos móveis e computadores pessoais?

Informações que não são importantes para o usuário não devem ser inclusas no documento de política de segurança. É importante enfatizar o que está se tentando proteger e porque estes procedimentos são feitos, entretanto, não se deve detalhar no nível técnico estas instruções. Em resumo, é de maior utilidade ter a política toda documentada em uma página de texto descrevendo o quê e o porquê das medidas de segurança a ter um documento formal e altamente técnico ocupando 10 folhas de papel para detalhar procedimentos que os usuários não conseguem compreender.

4.2 – PLANEJAMENTO

O item planejamento diz respeito às ações que devem ser tomadas antes de colocar os sistemas computacionais em funcionamento. Nem sempre isto é possível, pois na maioria das vezes a preocupação com segurança surge após os incidentes da rede já em funcionamento. Em todos os casos, deve-se avaliar a segurança como um processo cíclico revendo cada ponto crítico de tempos em tempos.

- Identificar o que é necessário proteger;
- Definir quais são as prioridades de proteção do ambiente;
- Especificar normas sobre como proceder diante de cada emergência;
- Educar os usuários da rede interna.

4.3 – USUÁRIOS E SENHAS

Algumas práticas com relação aos usuários e senhas são muito eficientes na prevenção de incidentes. Uma prática é instruir os usuários a usar senhas formadas por combinações relativamente complexas que inviabilizem o uso de *password crackers*. Outra é estudar o funcionamento dos programas que atacam com força bruta as contas do sistema. Assim o próprio administrador faz o trabalho de tentar "quebrar" senhas detectando combinações fracas antes do atacante.

Outro ponto importante é o elo de ligação entre os setores de informática e recursos humanos.

O administrador da rede deve ser sempre a primeira pessoa a saber da demissão de qualquer usuário/cliente da rede, para invalidar tentativas de destruição das informações que ele possa ter acesso.

- Auditar todas as alterações de usuários (inclusão, troca e exclusão de arquivos ou diretório, falha de *login* ou *logoff* do sistema, etc);
- Certificar-se que as permissões do arquivo de contas de usuários não possa ser lido por ninguém além do administrador e do sistema de autenticação;
- Certificar-se que cada usuário possui uma conta individual no sistema;
- Certificar-se que o sistema não aceita senhas mal formuladas;
- Certificar-se que todas as contas possuem senha;

- Considerar a possibilidade de expirar as senhas dos usuários em intervalos curtos e regulares;
- Estabelecer critérios para controlar o uso de senhas e criar métodos para que a mesma se torne uma senha forte;
- Executar *password crackers* contra o próprio sistema à procura de senhas fracas;
- Limitar a quantidade de contas existentes para o mínimo possível e estas contas deverão ser controladas e auditadas periodicamente. E os operadores e quaisquer usuários que não tenham o papel de administrador devem receber apenas os direitos mínimos e necessários para executar as suas funções;
- Não transmitir senhas por meios de fácil captura, como telefone e *e-mail*.

4.4 – CONTAS NO SISTEMA

Em um aspecto mais interno do sistema operacional, é importante haver um tratamento especial para as contas do administrador e dos *softwares* servidores. Não se deve atribuir por exemplo a mesma conta para mais de um serviço.

- Criar contas separadas para cada *software* servidor existente no *host*, evitando atribuir serviços à conta padrão *nobody:nogroup* comum em ambientes que seguem o padrão POSIX;
- Inibir a possibilidade de *login* da conta de administrador a partir de terminais remotos;
- Quando existir mais de um administrador, a senha (root ou administrator) de acesso à conta administrativa não deverá ser compartilhada;
- Remover periodicamente contas que ficaram inativas;
- Ter cuidado com os arquivos de senha, eles devem ser protegidos contra acesso indevido e serem constantemente monitorados.

4.5 – CONFIGURAÇÕES DO SISTEMA OPERACIONAL

Arquivos do sistema operacional que são vitais para seu funcionamento. São os principais alvos de ataque, pois neles estão todas as regras de comportamento do computador. Deve ser dada atenção máxima a este ambiente. Algumas recomendações:

- Criar um *logbook* (diário de bordo) que detalhe os componentes instalados no sistema e *todas as modificações* na sua configuração global, relatando quem, data, justificativa e a descrição;
- Efetuar *backups* dos arquivos de sistema e arquivos de usuário regularmente;
- Eliminar possibilidade de gravação nos dispositivos de terminais e pseudoterminais;
- Estar atento quanto aos *service packs ou patches* (pacotes de correção) para garantir os sistemas atualizados;
- Examinar o sistema de arquivos regularmente;
- Executar testes de restauração das mídias de armazenamento dos *backups*;
- Realizar a instalação mínima necessária para a operação dos seus sistemas operacionais e aplicativos;
- Remover *shells* desnecessárias;
- Remover utilitários que não sejam necessários mas são instalados com o sistema operacional;
- Ter o cuidado ao realizar compartilhamento de diretório/arquivos;
- Verificar quais as portas que estão abertas para estabelecer um número mínimo de portas que garanta o funcionamento do sistema.

4.6 – REGISTRO DE LOGS

Nos arquivos de *log* estão todas as atividades que o administrador precisa saber sobre o sistema. Entender o funcionamento e conteúdo de cada um deles ajuda o administrador a detectar anomalias.

- Checar se a sincronização dos horários dos equipamentos da rede está de acordo;
- Criar procedimentos de registro de logs e alocar um *loghost* (servidor) central, separado da rede, para armazenar os logs;
- Estudar e entender a configuração e a saída gerada pelo servidor de logs, para saber quais atividades ele reporta e onde encontrá-las quando necessário;
- Executar os utilitários de verificação de atividades do sistema operacional regularmente.

4.7 – AMEAÇAS LOCAIS

A maioria das falhas relatadas por BUGTRAQ (2001) só podem ser exploradas quando se obtém acesso local ao computador alvo. Algumas recomendações são:

- Incluir e examinar a variável de ambiente $PATH nos scripts de administração de sistema;
- Manter atualizado o programa de anti-vírus nas estações e nos servidores;
- Não incluir o diretório atual (".") na variável de ambiente $PATH;
- Não instalar *softwares* que não forneçam código-fonte e que não sejam homologados.
- Observar a segurança física do local onde se encontram os equipamentos de informática;

- Proibir o uso de modens nas estações de trabalho sem o conhecimento da gerência ou do pessoal da área de segurança.

4.8 – AMEAÇAS NOS SERVIÇOS DE REDE

Falhas nos serviços de rede são as que dão acesso ao sistema sem a necessidade de presença ou conta local no *host*. Apesar de serem difíceis de se explorar são as que mais servem como porta de entrada para intrusos.

- Desabilitar recursos de rede que não são necessários. Entre eles NFS, UUCP, Finger, TFTP e TELNET;
- Desativar serviços rlogin, rsh, rexec, rcp e demais serviços "r", substituindo-os pelo *secure shell*;
- Identificar os servidores de acesso público (SMTP, HTTP, DNS) e isolá-los da rede interna;
- Não instalar os SDK (kits de desenvolvimento com compiladores e outras ferramentas) nos servidores;
- O administrador deverá estabelecer procedimentos de *backup* de dados, arquivos de configuração e logs. E também deverá providenciar meios para armazenagem fora da organização, porém realizando a criptografia e o *checksum* no *backup* para garantir a confidencialidade e integridade;
- Os servidores de acesso público não deverão iniciar sessões com os servidores da rede interna;
- Remover programas de teste que acompanham *softwares* servidores, como o test-cgi, printenv, phf do serviço HTTPD;
- Substituição de POP3 e IMAP sem criptografia por solucões de *email* com criptografia (POP3 ou IMAP sobre SSL, *Webmail* sobre HTTPS);
- Todos os serviços TCP não utilizados ou não necessários deverão ser desabilitados nos equipamentos.

4.9 – RESPONDENDO A INCIDENTES DE SEGURANÇA

O primeiro passo para responder a um incidente de segurança é decidir qual é a natureza da resposta, se houver alguma, que deve ser feita imediatamente. Questões como "O atacante obteve sucesso em seu ataque?" ou "O ataque ainda está em progresso?" são extremamente relevantes, pois se o atacante obteve sucesso então o administrador de redes se encontra realmente em uma emergência porque é necessário antes de tudo, descobrir quais os danos que ocorreram para depois saber qual serviço/recurso que deu entrada para o intruso. Se o ataque ainda está em progresso pode-se tomar decisões como desligar os equipamentos que fazem conexão com a *Internet*.

Uma vez determinado que se está realmente em situação de emergência e que é necessário responder, é importante iniciar a documentação de tudo que está ocorrendo. Mesmo não sendo um momento apropriado, escrever um relatório simples em papel, no formato de *log* ajuda a evitar novos problemas como este e é uma oportunidade de se obter uma compreensão sobre o fato.

Uma vez de posse do material necessário para a documentação, é hora de decidir pelo desligamento do sistema. Para avaliar esta necessidade, deve-se considerar conseqüências como:

- Perda de dados que podem ser necessários para os usuários legítimos da rede;
- Perda de dados que evidenciem o ataque;
- Impossibilidade de analisar os equipamentos porque eles estarão desligados/desconectados;

A próxima prioridade é reparar os danos. Manter a tranqüilidade nesta situação pode ser essencial para resolução de problemas, pois o administrador terá que se autenticar no sistema com privilégios máximos e novos erros por causa da tensão podem comprometer ainda mais o sistema.

A presença de um colega de trabalho ou administrador de rede de outra organização pode ajudar muito.

Dependendo da natureza da organização pode ser necessário relatar o incidente ao corpo jurídico, auditores, relações públicas e departamento de segurança interno se:

- for necessário acusar judicialmente o atacante;
- houver suspeita que há colaboração de internos no incidente;
- houver suspeita de que houve acesso físico por parte do atacante.

O Anexo III descreve as atribuições do Comitê Gestor (COMITÊ GESTOR, 2003) da *Internet* no Brasil, para respostas legais a incidentes de segurança de redes.

4.10 – NORMAS DE SEGURANÇA DA INFORMAÇÃO PARA A COMPANHIA

Com base nas informações fornecidas pela norma ISO/IEC 17799:2000 e pela RFC 2196, podemos também formular algumas Normas de Segurança, que farão parte do documento de Política de Segurança da Informação.

A formalização das normas, necessárias para salvaguardar o negócio da Companhia, é considerada ponto fundamental para todo o processo de Segurança da Informação.

Normas de Segurança da Informação para Acesso ao Ambiente Computacional – Estabelecer requisitos para acesso físico e características dos ambientes de rede da Companhia, preservando a mesma quanto à ocorrência de acessos não autorizados.

Normas de Segurança da Informação para Administração de Estação de Trabalho – Manter a integridade e a disponibilidade das estações de trabalho e assegurar a devida proteção das informações nelas armazenadas.

Normas de Segurança da Informação para Operação de Estação de Trabalho – Estabelecer padrões de segurança para utilização das estações de trabalho.

Normas de Segurança da Informação para Desenvolvimento de Sistemas – Possibilitar o desenvolvimento de aplicações com nível de segurança e padronização visando a melhor execução das atividades do trabalho e a retenção da informação.

Normas de Segurança da Informação para Banco de Dados – Estas normas descrevem as condições para a correta configuração, proteção e uso do Banco de Dados, sua inter-relação com os sistemas, devendo ser obedecidas por toda força de trabalho da Instituição que utilize tais recursos.

Normas de Segurança da Informação para Cópia de Segurança – Definir critérios de segurança para execução e utilização das cópias de segurança das informações e das configurações dos equipamentos de rede da Companhia.

Normas de Segurança da Informação para Contas e Senhas – Estabelecer critérios para a disponibilização e administração dos acessos à rede corporativa da Companhia e aos equipamentos de rede, preservando estes contra acessos indevidos.

Normas de Segurança da Informação de Critérios para Classificação das Informações – Definir critérios para a classificação das informações e seus recursos, visando a adequada proteção.

Normas de Segurança da Informação para Auditoria, Geração e Análise de Registros – Estabelecer critérios para registro dos eventos ocorridos, que facilitem a rastreabilidade e a avaliação destas ocorrências.

Normas de Segurança da Informação para Acesso à *Internet*, *Intranet* e *Extranet* – Definir critérios para administração e utilização dos serviços de *Internet*, *Intranet* e *Extranet*.

Normas de Segurança da Informação para Acesso Remoto – Definir critérios para a disponibilização do serviço de acesso remoto à Companhia, bem como as regras a serem obedecidas pelos usuários, visando à prevenção do acesso não autorizado às informações dos Companhia.

Normas de Segurança da Informação para Transmissão de Informações – Definir requisitos tecnológicos e aspectos a serem obedecidos pelos usuários para a transmissão de dados entre as unidades da Companhia e destas com os clientes externos e parceiros, garantindo que não haja perda, modificação ou acesso indevido às informações transmitidas através da rede corporativa da Companhia e redes públicas, ou qualquer outro meio de comunicação.

Normas Gerais de Segurança da Informação para Técnicos – Agregar segurança às atividades desempenhadas pelos técnicos, orientando-os para auxílio nas ações de segurança e definindo critérios para manipulação e disponibilização dos recursos de tecnologia da informação da Companhia.

Normas Gerais de Segurança da Informação para Usuários – Agregar segurança às atividades desempenhadas pela Comunidade da Companhia, definindo critérios para manipulação e disponibilização das informações e dos recursos de informação.

4.11 – PROPOSTA DE UM CICLO DE MANUTENÇÃO DA SEGURANÇA DA INFORMAÇÃO

Para que a política de segurança esteja sempre em concordância com as melhores práticas adotadas pelo mercado, podemos assim definir um ciclo de vida para a manutenção da mesma e também de seus produtos.

01 – Desenvolver uma nova aplicação ou sistema utilizando uma metodologia de segurança das melhores práticas;

02 – Testar a aplicação ou sistema para detectar falhas na segurança utilizando rastreadores de vulnerabilidades e sistemas de injeção de falhas;

02a – Manutenção da vulnerabilidade: retornar para o processo de desenvolvimento a fim de corrigir as falhas detectadas;

03 – Disponibilizar a nova aplicação ou sistema para a produção;

04 – Utilizar processos de monitoramento da segurança interna e externa, para encontrar novas brechas e possíveis arrombamentos;

04a – Manutenção da vulnerabilidade: modificação da aplicação ou sistema para remoção das brechas e redisponibilização;

04b – Enviar o sistema em produção para mudanças no processo de desenvolvimento.

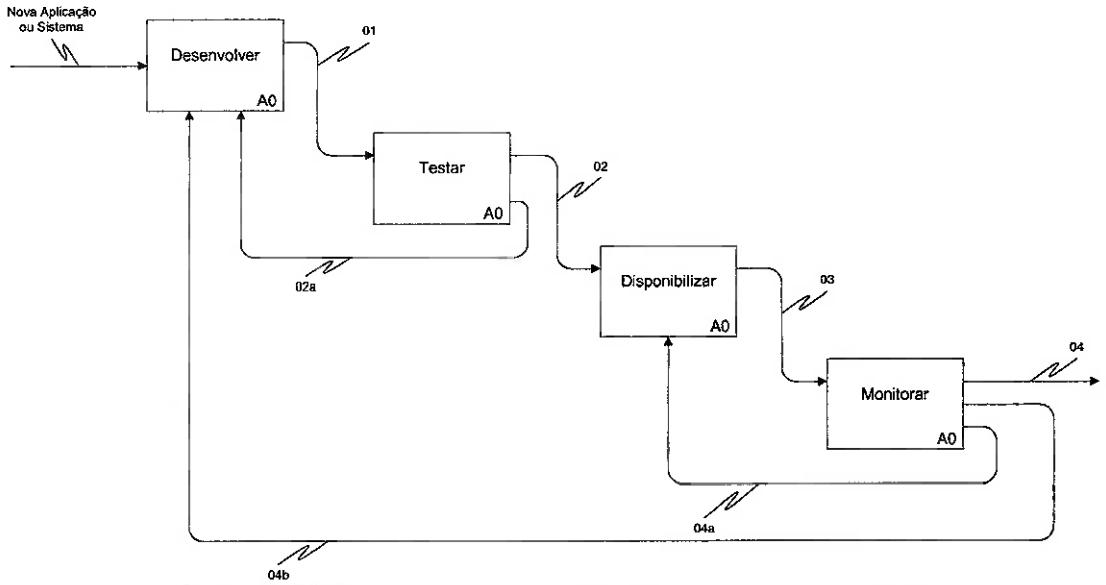

Figura 11 – Ciclo de Vida para manutenção da Segurança da Informação.

De tudo que foi apresentado, podemos agora dizer que o administrador possui em suas mãos um conjunto de boas práticas de segurança para minimizar os problemas gerados pela falta de segurança, e estas regras proporcionam ao administrador de rede um conhecimento a mais na área de segurança da informação. Mas a idéia deste assunto não é solucionar ou ter a pretensão de resolver todos os problemas de segurança, tendo em vista que isto é uma utopia, porém representar o mínimo de recomendações dentro do universo de boas práticas que o administrador de rede deve implementar, sem com tudo, mais uma vez, garantir a resolução de todas as situações.

CAPÍTULO 5 – CONCLUSÃO

Os temas relacionados com infra-estrutura, procedimentos e recursos de segurança devem ser vistos com prioridade e estar em constante reavaliação dentro das corporações. Como conseqüência do cenário ao mesmo tempo amigável e hostil que a *Internet* oferece, algumas análises precisam ser focadas na pauta do profissional que atua com a segurança da informação, tais como:

- A estratégia de segurança adotada está alinhada às necessidades de negócio da instituição?
- A alta administração recebe atenção devida no que diz respeito à segurança das informações que armazenam em seus computadores? A cultura de segurança está disseminada entre eles?
- Estrutura, funcionalidade e orçamento dedicados à segurança estão compatíveis com a estratégia de negócios da organização? Existe medição sobre o retorno dos investimentos com segurança?
- Qual é a abrangência e profundidade com que se trata segurança nos ativos eletrônicos da corporação? Toma-se medidas que vão além da implantação de ferramentas e produtos para proteção?
- Qual o impacto que as falhas de segurança podem provocar na relação de confiança e fidelização com os clientes, parceiros e colaboradores?

O objetivo de reavaliar segurança nas organizações, imposta pela nova realidade global, não deve tirar o foco de negócios. Por outro lado, não é desejável que se tome decisões a partir de análises superficiais ou de direcionamentos extremistas e pouco flexíveis, fundamentados simplesmente por medo e insegurança.

Elaborar a política de segurança é sem dúvida um trabalho longo e maçante, exatamente o oposto do tipo de trabalho que a maioria dos

técnicos apreciam. Porém, desenvolve-la e mante-la é vital para a segurança da instituição. É importante que ela não apresente textos técnicos e/ou políticos demais, para que o usuário a compreenda e que sumarize de forma simplificada todas as ações que ele precisa tomar, para cumprir sua parcela de comprometimento com a segurança da organização como um todo.

O documento de política de segurança pode se dividir em inúmeras políticas, que tem a função de proteger a organização como um todo; sua abrangência vai do Departamento de Recursos Humano, Jurídico, passando pelo Departamento de Tecnologia, Comercial e etc. Uma boa política deve ser adequadamente divulgada, e seus usuários devem ser educados e conscientizados. Para isso pode-se desenvolver inúmeros programas de treinamento que podem ser alinhados aos interesses da Companhia.

A política de segurança pode, proporcionar para a Companhia os seguintes benefícios:

- Aderência aos padrões internacionais de gestão de segurança;
- Alinhamento dos objetivos da empresa com as leis e obrigações contratuais;
- Aumento da conscientização da empresa;
- Definição das penalidades pela não aderência à Política de Segurança;
- Definição dos responsáveis pelos ativos da empresa;
- Equalização dos conceitos e práticas de segurança entre colaboradores e prestadores de serviços;
- Formalização e documentação dos procedimentos de segurança adotados pela organização;
- Maior padronização das informações e processos;
- Transferência de conhecimento para a equipe da Companhia;
- Valorização da companhia.

Manter *firewalls* de forma eficaz e em concordância com a política de segurança é também um trabalho de excelência. O conjunto de sistemas computacionais que filtra conteúdo deve ser um espelho daquilo que a diretoria da corporação espera do cumprimento da política de uso da *Internet*, bem como deve minimizar as possibilidades de ataques, invasões e vazamento de informação, mantendo a integridade e reputação da instituição.

Acredita-se, que a proposta apresentada neste trabalho, é de grande utilidade para os participantes da pesquisa. A elaboração de um documento de política de segurança é de grande importância para a continuidade do negócio da companhia, adicionando uma nova e importante camada de segurança para as redes que auxiliarão a companhia para melhorar seu desempenho e garantir o fornecimento de Energia Elétrica mais barata e com qualidade aos consumidores.

Devemos lembrar também que, segurança requer um trabalho contínuo de acompanhamento e análise crítica periódica dos riscos, dos controles implementados, dos eventos, das mudanças nos requisitos de negócio e suas prioridades, de que os controles aplicados continuam eficientes e adequados além do constante estudo de novas tecnologias, de novas táticas de defesa e de novos ataques que poderiam comprometer a segurança da Companhia.

BIBLIOGRAFIA

ANÔNIMO. ***Segurança Máxima***. Rio de Janeiro: Ed. Campus, 2001.

BASTOS, Alberto. ***Gerenciando a Segurança das Informações nas Empresas***. Disponível em: <http://modulo.com.br>. Acesso em: 04/2002.

BUGTRAQ (2001) BUGTRAQ ***Discussion list. List mantained by Security Focus***. Disponível em: <bugtraq@securityfocus.com> Acesso em: 10/2002.

CERT/CC (COMPUTER EMERGENCY RESPONSE TEAM). ***Estatísticas sobre incidentes de seguranças.*** Disponível em: <http://www.cert.org> Acesso em: 06/2002.

COMITÊ GESTOR (2001) COMITÊ GESTOR. ***Sobre o comitê gestor.*** Disponível em: <http://www.cg.org.br/grupo/grupos.htm>. Acesso em: 10/2002.

CTEEP – Transmissão Paulista. ***Origens***. Disponível em: <http://www.cteep.com.br/apresentacao/origens.htm>, Acesso em: 01/2002.

CT-STI (CÂMARA TÉCNICA DE SEGURANÇA DA TECNOLOGIA DA INFORMAÇÃO). ***A Segurança das Informações e a Internet.*** Brasília, Ministério do Planejamento, Segunda Edição, 2000.

FERREIRA, Aurélio Buarque de Holanda. ***Mini Aurélio Século XXI: O Minidicionário da língua portuguesa***. Rio de Janeiro: Ed. Nova Fronteira, 2002.

FONTES, Edison. ***Segurança da informação não é uma atitude, são muitas.*** Artigo, Jornal da Segurança, Ano 6, Número 64, 1999.

FONTES, Edison. ***Vivendo segurança da informação.*** São Paulo: Ed. Sicurezza, 2000.

GAMMA. ***BS-7799***. Disponível em: <http://www.gammassl.co.uk/bs7799>. Acesso em: 11/2002.

GARFINKEL, Simson; SPAFFORD, Gene. ***Practical UNIX & Internet Security.*** Sebastopol/CA: Ed. O'Reilly & Associates, Second Edition, 1996.

HAICAL, Cristiane. ***BS 7799 – O Novo Paradigma da Segurança***. Modulo Security Solutions. Disponível em: <http://www.modulo.com.br.> Acesso em: 09/2002.

HUNT, Craig. ***TCP/IP Network Administration.*** Sebastopol/CA, Ed: O'Reilly & Associates, Second Edition,1997.

ISO/IEC (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION FOR OPEN SYSTEMS INTERCONNECTION/INTERNATIONAL ELECTROTECHNICAL COMMISSION). ***ISO/IEC 17799 – Information technology – Code of practice for information security management***. First edition. 12/2000.

JORNAL INTERLIG, Jornal da CTEEP. ***Nasce uma nova CTEEP: Nosso Negócio é transmitir energia***. Número 37, pp. 4-5. São Paulo: 11/2001.

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

NIC BR SECURITY OFFICE. ***Práticas de Segurança para Administradores de Redes Internet.*** 2003. Disponível em: <http://www.nbso.nic.br/docs/seg-adm-redes/>. Acesso em: 10/2003.

RAMOS, F. F. ***Qualidade na Segurança da Informação Digital.*** E-Security Solutions. Axur Communications Inc. Disponível em: <http://www.axur.org/bs7799/bs7799.pdf>. Acesso em: 07/2002.

RFC 2196, ***Request for Coments: Site Security Handbook***, 2000. Disponível em: <http://www.rfc.net> .Acesso em: 08/2002.

SELEGUIM, Guilherme Cestarolli. ***Perigos do Mundo Virtual***. Monografia – Pontifícia Universidade Católica, Campinas, 2002.

ZWICKY, Elizabeth D., CHAPMAN, D. Brent. ***Building Internet Firewalls.*** Sebastopol/CA, Ed: O'Reilly & Associates, First Edition,1995.

GLOSSÁRIO

Antivírus – São programas capazes de detectar e eliminar o vírus.

Backup – Uma cópia exata de um programa, disco ou arquivo de dados feitos para fins de arquivamento ou para salvaguardar arquivos importantes na eventualidade de que a cópia ativa (original) seja danificada ou destruída. Por esse motivo, o *backup* também é chamado de cópia de segurança. Alguns programas aplicativos fazem automaticamente cópias de *backup* dos arquivos de dados, mantendo em disco tanto a versão atual quanto a anterior.

Browser – Programa para abrir e exibir as paginas da *web*. Os mais populares são o explore, da Microsoft, e o Navigator, da Netscape.

Crackers – São pessoas que realizam artifícios hackeanos, porém com o objetivo de quebrar códigos para obter senha.

Firewall – "Muro de fogo", programa ou componente dedicado, que protege a rede contra invasões externas e acessos não autorizados.

Host – Computador hospedeiro de um ou mais softwares servidores.

LOG – Registro das transações, eventos ou atividades realizadas em um sistema de computador.

Logbook (diário de bordo) – Serve para registrar os detalhe dos componentes instalados no sistema e *todas as modificações* na sua configuração global.

Password cracker – Todos servidores baseados em sistema Unix possuem um arquivo com as senhas dos usuários criptografadas. É virtualmente impossível decriptar estas senhas, mas é possível usar "dicionários" (lista de palavras), encriptá-las e comparar o resultado com as senhas contidas no arquivo.

Secure Shell – Protocolo usado para gerenciamento remoto em substituição ao Telnet. Toda comunicação ocorre de forma criptografada impedido a ação de sniffers.

Service packs ou *patches* – São pacotes de correção de falhas.

Shell – A camada mais externa de um programa que fornece uma interface para os usuários lançarem comandos. O Unix possui múltiplos *shells* incluindo Bash, C Shell e Korn. Também é conhecido como interpretador de comandos.

Web Site – Conjunto de documentos da *World Wide Web* hospedados em um servidor acessado por intermédio de um navegador.

ANEXO I – NORMA ISO/IEC 17799:2000 PARA GERENCIAMENTO DE SEGURANÇA DA INFORMAÇÃO

A norma internacional ISO/IEC 17799:2000, referenciada como ISO/IEC (2000), está ligada à norma britânica BS 7799, referenciada como BSI (1995), pelo cordão umbilical. De fato, a primeira é um "espelho" da segunda, com uma diferença fundamental: ela é uma norma internacional de direito, posto que foi estabelecida pela *Internacional Organization For Standardization* – ISO.

De qualquer forma, é impossível discutir a norma ISO/IEC 17799:2000 sem mencionar sua irmã gêmea (e primogênita), a norma BS 7799.

Assim, na seção 1 é apresentado um histórico da norma ISO/IEC 17799:2000, enfocando a origem da mesma. Na seção 2 apresenta-se, respectivamente, o escopo do padrão e modos de se identificarem requisitos de segurança.

Cabe ressaltar que neste trabalho não se pretende aprofundar na análise da norma. Para tanto, refira-se ao documento original ISO/IEC (2000). Pretendesse apresentar os tópicos, de forma sumária, e num nível de detalhe apenas suficiente para embasar a apresentação da Norma.

1 – ORIGENS DA NORMA ISO/IEC 17799:2000

De acordo com a GAMMA (2000), em 1987 o Departamento de Indústria e Comércio do Reino Unido (*UK Department of Trade and* Industry – DTI) criou o Centro de Segurança de Computação Comercial (*Commercial Computer Security* Centre – CCSC). Este centro, dentre as suas atribuições, tinha a tarefa de produzir um código com as melhores práticas de segurança em tecnologia da informação, com a finalidade de auxiliar usuários na implantação de sistemas de segurança em seus ACC – Ambiente Computacional Complexo. Desse esforço, que foi realizado conjuntamente com o Centro de Computação Nacional dos EUA (*National Computing Centre* – NCC), resultou um "Código de práticas para usuários" (*Users Code*

of Practice), que foi publicado em 1989. Para fazer uma avaliação desse código, do ponto de vista do usuário, foi formado um grupo de trabalho ligado à indústria britânica. O resultado dessa avaliação foi a publicação de um guia de segurança denominado documento PD 0003 e intitulado "Um código de práticas para gerenciamento de segurança da informação" (*A code of practice for information security management*). Após um período de consulta pública, foi publicada, em 1995, a versão final desse documento, intitulado Padrão Britânico (*British Standard*) BS7799:1995. Conforme HAICAL (2000), já nesta sua primeira versão, o padrão despertava interesse de organizações ao redor do mundo, apesar de apresentar algumas limitações para sua expansão mundial, como, por exemplo, a legislação voltada para os padrões britânicos. Para superar essas limitações, uma extensiva revisão e uma consulta pública foram iniciadas em novembro de 1997, culminando com a publicação da primeira revisão do padrão, o BS7799:1999, em abril de 1999. Para a revisão, foram solicitadas opiniões de vários países como forma de melhorar a norma. Ainda de acordo com HAICAL (2000), com essas contribuições, a BS 7799 atingiu dois objetivos: tornou-se mais flexível diante da necessidade de cada país e foi amplamente divulgada. Como conseqüência, a norma foi adotada não apenas pela Inglaterra – cujo governo a recomendou como parte de seu Ato de Proteção aos dados de 1999, e que foi efetivado em março de 2000 – como também por outros países da comunidade britânica, tais como Austrália, Nova Zelândia e África do Sul, além da Holanda e Noruega. A segunda parte desse documento – criada em resposta à necessidade de certificação da segurança implantada em um ACC, seguindo os códigos da primeira parte – foi apresentada em novembro de 1997 para consulta publica e avaliação. E, em fevereiro de 1998, o documento final foi publicado como BS7799-2:1998. A norma BS7799 procura tratar da segurança da informação em todos os seus aspectos, tanto lógicos quanto físicos. Cabe ressaltar que a norma BS 7799 é a única que define segurança física; as outras normas só tratam da segurança lógica da informação. A norma BS7799:1999 – Primeira Parte descreve o código de melhores práticas para o gerenciamento de segurança

da informação. Ela está dividida em dez títulos principais, com 127 controles de segurança e mais de 500 subcontroles, sendo o foco geral o gerenciamento de riscos, cujo objetivo é ajudar a organização a planejar a sua política de segurança. Como, normalmente, nem todos os controles precisam ser aplicados, a própria norma ajuda a organização a identificar os controles relevantes para seus negócios. No processo de certificação, a organização deverá especificar os controles que não estão incluídos na sua política de segurança e justificar sua exclusão. Os dez títulos principais cobrem todas as formas pelas quais se pode obter uma informação, sejam mensagens de voz ou escritas, transmitidas por telefones móveis, fixos, fax ou circuitos de comunicação de dados. Identificam também as novas formas de se fazer negócios, tais como *e-commerce*, *internet*, terceirização, computação móvel etc. HAICAL (2000) afirma que a grande flexibilidade da norma está justamente em tratar a segurança de informações independentemente dos meios nos quais a mesma se apresente. Estes dez títulos estão assim divididos:

- política de segurança;
- segurança organizacional;
- controle e classificação de ativos de informação;
- segurança pessoal;
- segurança física e ambiental;
- gerenciamento das operações e comunicações;
- controle de acesso ao sistema;
- desenvolvimento e manutenção de sistemas;
- gerenciamento da continuidade de negócios;
- conformidade.

Já a norma BS7799-2:1998 – Segunda Parte especifica os passos necessários que as organizações devem seguir para obter a certificação de

acordo com a norma. Para isso, define os requisitos necessários para estabelecer, implementar, documentar e avaliar um Sistema de Gerenciamento de Segurança da Informação (*Information Security Management System* – ISMS). DVN (2000) define um ISMS como o resultado de uma ação de gerenciamento explícito, expresso como uma coleção de políticas, princípios, objetivos, medidas, processos, formas, modelos, lista de verificações (*checklist*) etc, que, juntos, definem como os riscos de segurança de um ACC podem ser reduzidos. Para GAMMA (2000), ISMS é o meio através do qual os responsáveis pelo gerenciamento da segurança monitoram e controlam os sistemas de segurança, minimizando os riscos e garantindo que a segurança implantada satisfaz à organização, aos clientes e aos aspectos legais. RAMOS (2000) aponta que o importante é que o conceito de ISMS pode ser aplicado em qualquer organização, independentemente do seu tamanho. E esse conceito pode ser utilizado ainda que a organização não deseje submeter-se à certificação, mas apenas implementar um bom sistema de segurança para suas informações. A certificação serve para complementar o processo de implementação da segurança, atestando a prática da melhor política de segurança da informação, uma vez que é baseada no relato de auditores externos, portanto, supostamente imparciais. Após a certificação, as auditorias contínuas irão manter sempre os sistemas de segurança atualizados com as últimas vulnerabilidades e melhores práticas. Após a BS7799: 1999 – Primeira parte (1999) ter sido publicada, ela foi submetida à ISO para se tornar um padrão internacional. A proposta para sua homologação foi apresentada pelo mecanismo de "*Fast Track*", para um trâmite rápido, uma vez que qualquer norma leva em torno de cinco anos para ser avaliada e homologada pela ISO. Em outubro de 2000, na reunião do comitê da ISO em Tóquio, a norma foi votada e aprovada pela maioria dos representantes, muito embora os países ricos, exceto a Inglaterra, fossem contra sua homologação. Assim, em 1° de dezembro de 2000, ela foi publicada como ISO/IEC 17799: 2000.

A BS7799-2:1998 – Segunda parte (1998) também já está sendo preparada para ser submetida a ISO para homologação. Atualmente diversos países estão estudando com o fim de criarem suas normas baseadas na ISO/IEC 17799: 2000. No Brasil, o projeto 21:204.01-010, que é baseado na norma da ISO, já está em consulta pública, e brevemente deverá se tornar uma norma brasileira.

2 – ESTABELECENDO REQUISITOS DE SEGURANÇA

No contexto da norma ISO/IEC 17799: 2000, é essencial que uma organização identifique as suas necessidades de segurança antes de implantar qualquer controle. Existem três fontes principais a serem analisadas:

- a primeira fonte é obtida a partir da análise de risco dos ativos de informação. Pela análise de risco é que são identificadas as vulnerabilidades e ameaças a que a informação está sujeita, bem como a probabilidade de ocorrência. Com isso, pode-se dimensionar o impacto quando da ocorrência dessas falhas;
- a segunda fonte são a legislação vigente, os estatutos, as regulamentações e as claúsulas contratuais que a organização tem que cumprir;
- a terceira fonte é o conjunto particular de princípios, objetivos e exigências para processamento da informação que uma organização tem que desenvolver para apoiar suas operações.

As necessidades de segurança são, assim, identificadas principalmente pela análise sistemática dos riscos. As técnicas de análise de risco podem ser aplicadas em toda a organização; apenas numa parte específica dela; em um sistema de informação individual; em componentes de um sistema específico, ou serviço. Dessa forma, pode-se fazer uma implementação de segurança bastante seletiva, o que possibilitará um

gerenciamento mais efetivo nos gastos com controles de segurança. A análise de risco é uma consideração sistemática do seguinte:

- o impacto nos negócios é o resultado de uma falha de segurança, levando-se em consideração as potenciais conseqüências da perda de confidencialidade, integridade ou disponibilidade da informação;
- a probabilidade da falha ocorrer deve estar baseada nas ameaças e vulnerabilidades mais freqüentes e nos controles atualmente implementados.

Os resultados dessa análise é que determinaram as ações a serem tomadas na implementação dos controles para a proteção contra estes riscos. Como a implementação é seletiva, pode ser que seja necessário repetir o processo de análise de risco e seleção de controle várias vezes.

3 – POLÍTICA DE SEGURANÇA

Seus objetivos são descrever a importância de uma política de segurança bem como relacionar os principais assuntos que devem ser abordados nesta política.

A administração deve estabelecer uma política clara e demonstrar apoio e comprometimento com a segurança da informação através da definição e manutenção de uma política que deverá ser seguida por toda a organização.

3.1 – Documento da política de segurança da informação

Este documento deve expressar as preocupações da administração com a segurança de suas informações. Deve também ter o poder de estabelecer as diretivas para o gerenciamento da segurança.

É importante que a política seja aprovada e apoiada pela administração, publicada e comunicada a todos os funcionários, com o aceite de cada um, de preferência por escrito.

3.2 – Revisão e avaliação

Deve haver um responsável pela revisão e manutenção da política, garantindo atualizações em caso de mudanças que afetem a análise de risco original.

ANEXO II – RFC 2196 *SITE SECURITY HANDBOOK*

1. Políticas de Segurança

Neste documento há uma série de referências para políticas de segurança. Seguidamente, estas referências incluirão recomendações para políticas específicas.

O que é uma política de segurança? Por que ter uma?

O que faz uma boa política de segurança?

Mantendo a política flexível

Introdução:

1.1 – O que é uma política de segurança? Por que ter uma?

As decisões que você como administrador toma ou deixa de tomar, relacionadas à segurança, irão determinar quão segura ou insegura é a sua rede, quantas funcionalidades ela irá oferecer, e qual será a facilidade de utilizá-la. No entanto, você não consegue tomar boas decisões sobre segurança, sem antes determinar quais são as suas metas de segurança. Até que você determine quais sejam elas, você não poderá fazer uso efetivo de qualquer coleção de ferramentas de segurança, pois você simplesmente não saberá o que checar e quais restrições impor.

Por exemplo, seus objetivos provavelmente serão muito diferentes dos que são definidos por um vendedor de produto. Os vendedores procuram deixar a configuração e a operação de seus produtos o mais simplificado possível, o que implica que as configurações *default* normalmente serão tão abertas (e por conseguinte inseguras) quanto possível. Se por um lado isto torna o processo de instalação de novos produtos mais simples, também deixa acessos abertos, para qualquer usuário.

Seus objetivos devem ser determinados a partir dos seguintes determinantes:

Serviços oferecidos ***versus*** *Segurança fornecida* – Cada serviço oferecido para os usuários carrega seu próprios riscos de segurança. Para alguns serviços, o risco é superior que o benefício do mesmo, e o administrador deve optar por eliminar o serviço ao invés de tentar torná-lo menos inseguro.

Facilidade de uso ***versus*** *Segurança* – O sistema mais fácil de usar deveria permitir acesso a qualquer usuário e não exigir senha, isto é, não haveria segurança. Solicitar senhas torna o sistema um pouco menos conveniente, mas mais seguro. Requerer senhas "*one-time*" geradas por dispositivos, torna o sistema ainda mais difícil de utilizar, mas bastante mais seguro.

Custo da segurança ***versus*** *o Risco da perda* – Há muitos custos diferentes para segurança: monetário (o custo da aquisição de *hardware* e *software* como *firewalls*, e geradores de senha "*one-time*"), performance (tempo cifragem e decifragem), e facilidade de uso. Há também muitos níveis de risco: perda de privacidade (a leitura de uma informação por indivíduos não autorizados), perda de dados (corrupção ou deleção de informações), e a perda de serviços (ocupar todo o espaço disponível em disco, impossibilidade de acesso à rede). Cada tipo de custo deve ser contra-balançado ao tipo de perda.

Seus objetivos devem ser comunicados a todos os usuários, pessoal operacional, e gerentes através de um conjunto de regras de segurança, chamado de "política de segurança". Nós utilizamos este termo ao invés de "política de segurança computacional", uma vez que o escopo inclui todos os tipos de tecnologias de informação e informações armazenadas e manipuladas pela tecnologia.

1.1.1 – Definição de uma política de segurança

Uma política de segurança é a expressão formal das regras pelas quais é fornecido acesso aos recursos tecnológicos da empresa.

1.1.2 – Propósitos de uma política de segurança

O principal propósito de uma política de segurança é informar aos usuários, equipe e gerentes, as suas obrigações para a proteção da tecnologia e do acesso à informação. A política deve especificar os mecanismos através dos quais estes requisitos podem ser alcançados. Outro propósito é oferecer um ponto de referência a partir do qual se possa adquirir, configurar e auditar sistemas computacionais e redes, para que sejam adequados aos requisitos propostos. Portanto, uma tentativa de utilizar um conjunto de ferramentas de segurança na ausência de pelo menos uma política de segurança implícita não faz sentido.

Uma política de uso apropriado (*Appropriate* – ou *Acceptable* – *Use Policy* – AUP) pode também ser parte de uma política de segurança. Ela deveria expressar o que os usuários devem e não devem fazer em relação aos diversos componentes do sistema, incluindo o tipo de tráfego permitido nas redes. A AUP deve ser tão explícita quanto possível para evitar ambigüidades ou mal entendidos. Por exemplo, uma AUP pode listar *newsgroups* USENET proibidos.

1.1.3 – Quem deve ser envolvido na formulação da política?

Para que uma política de segurança se torne apropriada e efetiva, ela deve ter a aceitação e o suporte de todos os níveis de empregados dentro da organização. É especialmente importante que a gerência corporativa suporte de forma completa o processo da política de segurança, caso contrário haverá pouca chance que ela tenha o impacto desejado. A seguinte lista de indivíduos deveria estar envolvida na criação e revisão dos documentos da política de segurança:

- O administrador de segurança do *site*;
- O pessoal técnico de tecnologia da informação;
- Os Administradores de grandes grupos de usuários dentro da organização;
- A equipe de reação a incidentes de segurança;
- Os Representantes de grupos de usuários afetados pela política de segurança;
- Conselho Legal.

A lista acima é representativa para muitas organizações que tem controle acionário, mas não necessariamente para todas. A idéia é trazer representações dos membros, gerentes com autoridade sobre o orçamento e política, pessoal técnico que saiba o que pode e o que não pode ser suportado, e o conselho legal que conheça as decorrências legais das várias políticas. Em algumas organizações, pode ser apropriado incluir pessoal de auditoria. Envolver este grupo é importante se as política resultante deverá alcançar a maior aceitabilidade possível. Também é importante mencionar que o papel do conselho legal irá variar de país para país.

1.2 O que faz uma boa política de segurança?

As características de uma boa política de segurança são:

- Ela deve ser implementável através de procedimentos de administração, publicação das regras de uso aceitáveis, ou outros métodos apropriados.
- Ela deve ser exigida com ferramentas de segurança, onde apropriado, e com sanções onde a prevenção efetiva não seja tecnicamente possível.
- Ela deve definir claramente as áreas de responsabilidade para os usuários, administradores e gerentes.

Os componentes de uma boa política de segurança incluem:

Guias para a compra de tecnologia computacional que especifiquem os requisitos ou características que os produtos devem possuir.

Uma política de privacidade que defina expectativas razoáveis de privacidade relacionadas a aspectos como a monitoração de correio eletrônico, logs de atividades, e acesso aos arquivos dos usuários.

Uma política de acesso que define os direitos e os privilégios para proteger a organização de danos, através da especificação de linhas de conduta dos usuários, pessoal e gerentes. Ela deve oferecer linhas de condutas para conexões externas, comunicação de dados, conexão de dispositivos a uma rede, adição de novos *softwares*, etc. Também deve especificar quaisquer mensagens de notificação requeridas (por exemplo, mensagens de conexão devem oferecer aviso sobre o uso autorizado, e monitoração de linha, e não simplesmente "*welcome*".

Uma política de contabilidade que defina as responsabilidades dos usuários. Deve especificar a capacidade de auditoria, e oferecer a conduta no caso de incidentes (por exemplo, o que fazer e a quem contactar se for detectada uma possível intromissão.

Uma política de autenticação que estabeleça confiança através de uma política de senhas efetiva, e através da linha de conduta para autenticação de acessos remotos e o uso de dispositivos de autenticação.

Um documento de disponibilidade que define as expectativas dos usuários para a disponibilidade de recursos. Ele deve endereçar aspectos como redundância e recuperação, bem como especificar horários de operação e de manutenção. Ele também deve incluir informações para contato para relatar falhas de sistema e de rede. Este conceito equivale a SLA (*Service Level Agreenment*) que inclui as expectativas do usuário em termos de qualidade de serviço, incluiindo segurança.

Um sistema de tecnologia de informação e política de manutenção de rede que descreva como tanto o pessoal de manutenção interno como

externo devem manipular e acessar a tecnologia. Um tópico importante a ser tratado aqui é como a manutenção remota é permitida e como tal acesso é controlado. Outra área para considerar aqui é a terceirização e como ele é gerenciada.

Uma política de relatório de violações que indique quais os tipos de violações devem ser relatados e a quem estes relatos devem ser feitos. Uma atmosfera de não ameaça e a possibilidade de denúncias anônimas irá resultar uma grande probabilidade que uma violação seja relatada.

Suporte a informação que ofereça aos usuários informações para contato para cada tipo de violação; linha de conduta sobre como gerenciar consultas externas sobre um incidente de segurança, ou informação que seja considerada confidencial ou proprietária; referências cruzadas para procedimentos de segurança e informações relacionadas, tais como as políticas da companhia e leis e regulamentações governamentais.

Pode haver requisitos regulatórios que afetem alguns aspectos de sua política de segurança (como a monitoração). Os criadores da política de segurança devem considerar a busca de assistência legal na criação da mesma. No mínimo, a política deve ser revisada por um conselho legal.

Uma vez que a política tenha sido estabelecida ela deve ser claramente comunicada aos usuários, pessoal e gerentes. Deve-se criar um documento que os usuários assinem, dizendo que leram, entenderam e concordaram com a política estabelecida. Esta é uma parte importante do processo. Finalmente sua política deve ser revisada regularmente para verificar se ela está suportando com sucesso suas necessidades de segurança.

1.3 – Mantendo a política flexível

No intuito de tornar a política viável a longo prazo, é necessário bastante flexibilidade baseada no conceito de segurança arquitetural. Uma política deve ser largamente independente de *hardware* e *softwares*

específicos. Os mecanismos para a atualização da política devem estar claros. Isto inclui o processo e as pessoas envolvidas.

Também é importante reconhecer que há expectativas para cada regra. Sempre que possível a política deve expressar quais expectativas foram determinadas para a sua existência. Por exemplo, sob que condições um administrador de sistema tem direito a pesquisar nos arquivos do usuário. Também pode haver casos em que múltiplos usuários terão acesso à mesma *userid*. Por exemplo, em sistemas com um usuário *root*, múltiplos administradores de sistema talvez conheçam a senha e utilizem a conta.

Outra consideração é chamada a "Síndrome do Caminhão de Lixo". Isto se refere a o que pode acontecer ao um *site* se uma pessoa chave repentinamente não esteja mais disponível para sua função (ficou doente ou deixou a companhia). Enquanto a grande segurança reside na mínima disseminação de informação, o risco de perder informação crítica cresce quando a informação não é compartilhada. É importante determinar qual o peso ideal desta medida em seu *site*.

ANEXO III – ATRIBUIÇÕES DO COMITÊ GESTOR

Grupo de Segurança de Redes

O embrião do GT-S foi a criação do então subgrupo de trabalho de segurança, apresentado por ocasião da Comdex-SP, em 1996. Um mês depois do seu lançamento, foi publicado o texto "Rumo a Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil".

Em junho de 1997 é criado o NIC.BR Security Office cuja ação, com base em voluntários, permitiu que, no dia 11 de fevereiro de 1998 fosse criado o GT-Segurança com a atual equipe de trabalho.

O GT-S é formado por dois sub-grupos: *backbones*, coordenado por Ricardo Maceira (Embratel), cujo principal objetivo é discutir a questão da segurança nas redes ligadas à Internet sob a ótica das redes provedoras de backbone, e provedores, coordenado por Nelson Murilo (Pangeia) e Rubens Kuhl Jr. (UOL), cujo foco são os aspectos de segurança relacionados com as empresas provedoras de acesso à Internet.

Como forma de reconhecimento pelo seu trabalho, os membros do NIC BR Security Office (NBSO), subordinado ao GT-S, e do Setor de Apuração de Crimes por Computador (SACC), da Polícia Federal, foram convidados a integrar o High Technology Crime Investigation Association (HTCIA), entidade com sede nos Estados Unidos, responsável por investigar crimes cometidos por meios tecnológicos.

O Brasil foi considerado pelo grupo de segurança da marinha norte-americana, Space and Naval Warfare Systems Command, como sendo o país de resposta mais rápida a incidentes nesta área. Confira em http://www.nanog.org/mtg-9905/ppt/broersma/sld017.htm

Coordenador:
Prof. Dr. Pedro Vazquez