A Internet e as Conseqüências da Globalização da Informação

Francisco Sérgio dos Santos
Marcelo Schneck de Paula Pessôa
universidade paulista – unip
e-mail: cocao@snet.com.br, mpessoa@nutencnet.com.br

Resumo

A tecnologia Internet tem realizado uma revolução nos meios de gerenciamento e disseminação da informação. Essa tecnologia tem agilizado e melhorado a forma dos negócios tradicionais, além do surgimento de formas totalmente novas de realizar se negócios. Ao mesmo tempo, a segurança de transações nessas novas tecnologias tem sido questionada, inibindo seu crescimento.

Esse trabalho apresenta uma discussão sobre essa questão e discute os aspectos tecnológicos e de comportamento das pessoas. É proposto um modelo de estratégia de segurança para redes de computadores, abordando a importância da padronização de normas, procedimentos e diretrizes, ressaltando também a necessidade de acompanhamento da disseminação da cultura de segurança.

Aplicação de recursos para garantir a atualização tecnológica e treinamento necessários e a administração para avaliar continuamente a aplicabilidade do processo bem como sua atualização.

Palavras chaves : privacidade, política, ética, processo, cultura.

Abastract:

Internet technology has been accomplishing a revolution in management means and information dissemination . This technology has been activating and improving traditional business, besides the appearance of totally new ways to make business. At the same time, safety of transactions in those new technologies has been questioned, inhibiting its growth.

This work presents a discussion on that subject and discusses technological aspects and people behavior. A model of safety strategy is proposed for computer networks, approaching the importance of standardization of procedures and guidelines, also standing out the need of accompaniment the dissemination of safety's culture, application of resources to guarantee technological modernization and necessary training and administration to evaluate the applicability of the process continually as well as its modernization.

Key Word : privacy, policy, ethics, process, Culture.

1. Introdução.

O movimento de globalização, que torna o planeta quase uma aldeia, tem sido viabilizado pelas tecnologias de comunicação e de computação. Quebradas as barreiras culturais que fechavam o livre comércio entre os países, a Internet está viabilizando o intercâmbio entre países como se todos estivessem fisicamente próximos. Essa sensação de proximidade é viabilizada pelos sistemas de comunicação por áudio (telefonia), vídeo (TV) e dados (Internet). Ao lado desse movimento saudável, existem oportunistas e criminosos que se aproveitam de brechas deixadas pelas tecnologias para realizar roubos e criar uma imagem de falta de privacidade e de segurança nesse novo ambiente.

Este trabalho mostra que ao lado do vetor técnico que cria uma série de mecanismos de proteção aos sistemas e aos usuários, existe um segundo vetor comportamental que precisa ser trabalhado na sociedade e nas empresas para garantir que o uso da Internet se torne mais seguro.

2. As oportunidades de negócio

Segundo Bernstain [BER97] as empresas estão utilizando a Internet para os seguintes serviços: propaganda, marketing, suporte ao cliente , comércio eletrônico. Nesse último, há um aumento exponencial de possibilidades de negócios, fato que traz benefícios a todos: do pequeno ao grande empreendedor, além de nivelar o campo de ação das empresas de forma independente de seu tamanho.

A Internet está revolucionando a forma como as transações comerciais são conduzidas. Utilizando algumas ferramentas simples, baseadas na Internet, muitas empresas descobriram que poderiam aumentar a produtividade de maneira significativa. Essa produtividade pode ser aumentada

apenas com o uso das novas tecnologias como por exemplo a compra eletrônica ou com a quebra de paradigmas através de novas aplicações como o leilão eletrônico ou os metamediários que são intermediários virtuais de transações comerciais.

Segundo IDC - International Data Corporation, as vendas através da Internet movimentariam cerca de US$ 54 bilhões até o ano 2000, segundo Fajardo [FAJ98] , e até o ano 2002 US$ 327 Bilhões, Estima Forrester Group, segundo Santos [SAN98].

O rápido crescimento do comércio eletrônico utilizando a Internet tem sido tolhido em virtude da sensação de falta de privacidade e de insegurança na realização de transações usando essa tecnologia.

3. Privacidade

A privacidade pode ser definida como o direito que tem o usuário de um sistema - ou o direito de um cidadão- a ter preservadas suas informações pessoais.

Entende-se por informação pessoal qualquer informação que torne o indivíduo identificável. Portanto trata-se de dados de contato (nome completo, endereço, telefones, email, etc.), dados de cobrança ou financeiros (número de cartão de crédito, nível de renda, patrimônio, etc.), documentos de identidade e profissionais (CPF, RG, etc.), informações sócio-demográficas (sexo, idade, estado civil, dados étcnicos), dados médicos (históricos ou condições de saúde, etc.), escolaridade (graus e outros) imagens da pessoa e outras informações identificáveis como hobbies, áreas de interesse social, entretenimento, etc.

Além das informações pessoais existem as denominadas informações pessoais sensíveis que podem ser definidas como sendo aquelas cuja divulgação possa causar algum tipo de constrangimento moral ou danos ou prejuízos à sua pessoa ou a empresa à qual pertence. Estão incluídos nesse critério os dados históricos médicos do usuário em relação à sua saúde (inclusive registro de compras de medicamentos, de pesquisa ou solicitações de serviços e informações ligados à saúde), os dados que revelem origens raciais ou étnicas, dados que revelem a opinião política, hábitos sexuais, religião ou credos filosóficos e os dados econômico-financeiros como número de cartão de créditos, de contas correntes em bancos, de senhas de acesso a serviços financeiros on-line, dados sobre renda ou patrimônio e outras informações confidenciais que, se divulgadas em o consentimento do usuário, possam dar origem a fraudes ou outros tipos de problemas.

Evidentemente essa questão da privacidade sempre existiu e não há novidade nenhuma com relação ao seu sigilo. A ética médica sempre preservou sigilo sobre a situação de seus pacientes, os bancos suíços são famosos por preservarem sigilo total sobre seus clientes. Os cadastros e bancos de dados sobre clientes e usuários sempre existiram e sempre foram preservados. O que está ocorrendo de diferente, entretanto é que as novas tecnologias estão permitindo a integração desses dados, tornando quase que trivial o cruzamento de informações de dois ou mas bancos de dados permitindo a identificação de novas informações sigilosas sobre o cidadão. Essas informações possuem valor comercial e podem prejudicar o cidadão ou serem usadas de maneira indevida.

Sem a tecnologia de redes, de bancos de dados e da Internet, o cruzamento de informações sobre uma pessoa é um trabalho muito grande que, na maioria dos casos, não vale a pena fazer. Com essas tecnologias essa atividade se torna relativamente fácil e o que vai segurar essa invasão de privacidade são exatamente os aspectos éticos que as organizações devem passar a adotar e respeitar.

Nesse sentido o Parlamento Europeu [DAV98] e o FTC-Federal Trade Commision dos Estados Unidos [PIT99], [PIT98] e [DD00] desenvolveram diversos estudos para estabelecer quais seriam os pontos a serem respeitados para um tratamento ético referente à privacidade dos usuários Internet. Desses estudos, pode-se resumir como requisitos mínimos:

- **aviso e conhecimento**: a Organização deve identificar-se para o usuário e informar quais dados está coletando e para qual finalidade;
- **escolha**: a Organização deve informar ao usuário quais os dados mínimos necessários para a prestação de serviço solicitado e dar a opção de escolha aos demais dados a serem fornecidos,
- **consentimento**: a Organização deve esclarecer ao usuário como utiliza os dados pessoais e solicitar o consentimento para seu uso;
- **acesso**: a Organização deve possibilitar ao usuário o acesso a seus dados pessoais;
- **retificação**: a Organização deve permitir ao usuário a retificação de seus dados pessoais;

Observe-se que a Organização possui acesso aos dados do usuário e deve, com clareza, especificar como eles serão usados. Não há nenhum problema em utilizar esses dados agregados ,ou seja, que não identifiquem o usuário.

As Organizações são levadas a elaborarem um Sistema da Privacidade como um meio para cumprir a sua política da privacidade que obedece os princípios acima definidos. Dessa forma fica garantido o respeito à privacidade do usuário.

Hoje, particularmente nos Estados Unidos, existem muitas Organizações que possuem e declaram sua política de privacidade em seus sites. No Brasil também está começando a ocorrer o mesmo fenômeno.

4. Segurança

Segurança segundo Simson [SIM99], é definida como um conjunto de procedimentos, práticas e tecnologias usadas para proteger os servidores, usuários da Web e suas empresas e deve possuir os seguintes aspectos segundo Hutt [HUT95]:

- **Integridade:** É a habilidade do sistema em garantir com precisão e confiabilidade os dados que estão depositado na sua base, sendo que (hardware, software e comunicação) devem possibilitar o tráfego entre os pontos (origem e destino) sem alterações, processando-os corretamente , e não permitir acessos não autorizado. Sendo o desempenho essencial, e que qualquer fracasso deveria ser previsível, reportando todos os problemas existentes, a fim de poder em tempo hábil tomar atitudes para uma imediata ação corretiva.
- **Disponibilidade :** O sistema tem que prover resposta eficiente e capacidade adequada para apoiar um desempenho aceitável. Recuperar-se depressa de interrompimentos de longo prazo. Cópias de segurança de dados, inclusive de equipamentos, Teste constantes do plano de contingência deveriam estar em lugar de destaque na administração do ambiente computacional. Prevenção é de alta prioridade , evitar sobrecarga do sistema em determinados períodos de atividade, evitar a dependência de equipamentos simples e ou dispositivos simples de comunicação, Providenciar equipamentos de backup (dispositivos de energia, ar condicionado, e outros sistemas de suporte, limitando acesso indevido) reduzindo a exposição a agentes indesejados e não autorizados.
- **Controle** : Administração deve ter a capacidade para limitar quem pode ter acesso ao sistema, quanto de recurso pode ser usada para cada propósito ou funcionalidade, que propósitos são permitidos, que tipo dados é acessível e transmitido para cada usuário, e que conexões podem ser feitas. Deveriam ser utilizados controles administrativos e técnicos. Medidas administrativas incluem publicação de políticas de segurança, padrões, e diretrizes , treinamento sobre conscientização sobre questões de segurança procedimentos de controle de mudança de sistemas, inclusive critérios de segurança no desígnio de sistema, e monitoração de atividade de sistema , medidas técnicas incluem controle de acesso (acesso de sistema, restrições de recurso), logon e controle de senha, métodos de identificação alternativos (fichas pessoais, assinaturas digitais), isolamento da rede (da rede pública), firewalls, e segurança física de componentes de sistemas.
- **Auditoria**: Administração deve usar a função de auditoria como um árbitro independente, medir complacência com políticas de segurança, padrões, e diretrizes como também avaliar a suficiência de proteção técnica. O sistema deve preservar seus dados, bem como a sua utilização. Devem ser registrados todos os acessos e eventos solicitados ao sistema.

5. Proposta de uma política de segurança

A Política deve conter os seguintes tópicos relacionados a seguir, lembrando que não é uma regra, mas cada empresa pode definir seus requisitos de acordo com seus objetivos e necessidades, conforme relata Caruso [CAR99].

5.1. Propósito da política

Apoiar os objetivos da organização e nunca apoiar-se em ferramentas e plataformas; descrever o programa geral de segurança da rede; demonstrar os resultados de sua determinação de risco, com as ameaças que está combatendo e as proteções propostas; definir responsabilidades para implementação e manutenção de cada proteção; definir normas e padrões comportamentais para os usuários.

5.2. Conteúdo da política

Descrever os recursos a proteger, programas permitidos; relacionar os participantes do desenvolvimento das normas, procedimentos e padrões, a quem pertence os privilégios e a quem se

destina; deve determinar gerência específica e responsabilidades dos envolvidos no controle e manuseio do ambiente operacional e das informações armazenadas; descrever como as informações serão colhidas e armazenadas, e a quem se destina as informações.

5.3. Implementação da política

Nenhuma política deve ser implementada até que os usuários sejam treinados nas habilidades necessárias para segui-la. As boas políticas de segurança e privacidade dependem do conhecimento e cooperação dos usuários. Todos devem saber como agir quando se virem diante de uma incidência. Todos usuários devem saber a quem recorrer se tiverem perguntas ou suspeitas, e devem saber qual atitude tomar para minimizar riscos de segurança. Todos devem ter consciência que as medidas de segurança e privacidade são criadas para seu próprio benefício, conforme Caruso [CAR99] e Oliveira [OLI00].

5.4. Política geral de segurança

É interessante apresentarmos itens de uma política que determinam o início de parâmetros necessários à criação de um ambiente com segurança e confiabilidade, conforme Caruso [CAR99] e Hutt [HUT95], tais como:

- Todos os funcionários são responsáveis pela integridade dos ativos da organização;
- O cumprimento das políticas é obrigatório e o seu não-cumprimento implica em sanções disciplinares ou trabalhista cabíveis;
- Todos os ativos devem receber classificação quanto à preservação e proteção;
- Todos os ativos pertencem a organização, e portanto devem receber proteção adequada conforme a importância do negócio;
- Os programas de usuário devem ser executados somente das estações de trabalho;
- Não devem existir múltiplas identificações/senhas de entrada no sistema, devendo haver indicação quando o mesmo usuário tentar utilizar sua identificação simultaneamente;
- Deve existir um planejamento formal, completo e testado de recuperação de desastres, de qualquer recurso;
- Controle de acessos físicos ;
- Administração de segurança ;
- Controle de acessos lógicos ;
- Monitoração e auditoria de segurança .

6. Falta de padrões técnicos

Um dos problemas do tema segurança é sua forte dependência da tecnologia. Assim, as técnicas existentes se tornam obsoletas com a chegada de novas tecnologias situação agravada pela dificuldade de padronização.

Segundo Bernstein [BER97], a IETF (Internet Engineering Task Force), trabalhando sob os auspícios da IAB (Internet Activities Board), define diretrizes para a Internet. A associação à IETF é aberta a qualquer interessado em como tratar questões técnicas para o estabelecimento de padrões. A IETF desenvolve padrões para a Internet, além de inúmeros documentos informativos que abrangem questões como as origens da Internet, diretrizes para os participantes de reuniões da IETF, e até mesmo como desenvolver uma política de segurança na Internet.

À medida que a Internet passou a ser mais comercial, no entanto, o papel da IETF se tornou mais indefinido. Cada vez mais, fornecedores estão propondo sua própria versão de padrões, sem passar pelo processo tradicional da IETF. Os fornecedores que criam padrões nem sempre fazem isso por motivos altruístas. - Colocar no mercado um produto baseado em um padrão patenteado se traduz em muito dinheiro. Dentre os exemplos desse tipo de comportamento estão as empresas que desenvolveram os protocolos de comunicação segura, tais como - S-HTTP (Secure Hypertext Transfer Protocol), SSL (Secure Sockets Layer), PCT (Private Communications Technology), STT (Secure Transaction Tecnology), e o SEPP (Secure Electronic Payment Protocol).

Muitos destes problemas, segundo Bernstein [BER97], podem ser resultantes de deficiência nos protocolos de comunicação. Dentre vários problemas podemos destacar a sua inabilidade para confirmar a identidade dos participantes em um processo de comunicação.

Outra deficiência importante é a sua inabilidade de proteger a privacidade dos dados de uma rede. Devido a uma característica de um dos protocolos básicos do TCP/IP, uma determinada máquina pode monitorar todo o tráfego de uma rede a que está conectada, independente de seu destino.

Outro tipo de deficiência decorre do fato de que muitos sistemas são grandes, complicados e difíceis de configurar.

Alguns pontos fracos na configuração de sistemas são:

- Contas de usuários inseguras ;
- Contas de sistema com senhas originais muito conhecidas que não são alteradas ;
- Serviços de Internet incorretamente configurados ;
- Parâmetros básicos inseguros nos produtos.

7. Comportamento versus privacidade e segurança

Do ponto de vista do usuário de sistemas computacionais, ele passa pelas seguintes fases; de rejeição, adesão involuntária, comportamento e multiplicação. Deve ter como enfoque de trabalho a responsabilidade com a informação, o comprometimento da informação com a atividade-fim da organização, a mudança do relacionamento da visão pessoal da informática em relação a visão profissional e o equilíbrio do problema técnico em relação ao comportamental.

O processo de segurança de informação na organização não traz, por si só, maiores problemas, mas aflora os problemas existentes. Muitas vezes, esses problemas existentes estão camuflados; em virtude do ambiente existente ser bastante flexível.

Segundo Gomes [GOM00], os usuários consideram que o assunto segurança é um tema de responsabilidade dos profissionais de informática e não um tema que deva ser de preocupação de todos dentro da organização.

Os empregados trabalham com informações, produto diretamente relacionado com a cultura específica de cada organização e a rotatividade de pessoas implica em um processo de aculturação que dura algum tempo, durante o qual o custo dos erros freqüentemente ultrapassa os benefícios da redução de custos.

A mudança dos padrões culturais não deve se iniciar por setor específico, mas por todos os departamentos. Deve transparecer que a preocupação com a privacidade e a segurança sempre fez parte da cultura da organização. É necessário vender a idéia para todos os membros da organização, não somente para o alto escalão, mas todos devem participar efetivamente.

Todas as organizações, segundo Caruso [CAR99], desenvolvem sua própria cultura interna, que guia o relacionamento interno e externo. Qualquer elemento cultural novo que venha fazer parte da cultura organizacional , é inicialmente tratado como elemento estranho. Dentre todas as que mais sofrem resistência, é a implantação de controles em uma estrutura que normalmente funciona de forma mais flexível.

8. O anonimato

Privacidade, segundo a ONU [ONU00], é a limitação do acesso às informações de uma dada pessoa, ao acesso à própria pessoa, à sua intimidade, anonimato, segredos, afastamento ou solidão. Ninguém estará sujeito a interferências na sua vida privada, na sua família, no seu lar, ou na sua correspondência, nem a ataques à sua honra e reputação.

Deste modo, o anonimato, segundo Gomes [GOM00], contribui para a insegurança, pois a rede é democrática e transcende as divisas políticas geográficas. O direito a informação, a liberdade de expressão e o anonimato, são garantidos por qualquer nação democrática existente. Muitas operações são realizadas a todo momento pela Internet como por exemplo, troca de mensagens, e todos que utilizam este serviço quer usufruir do direito de entregar a mensagem somente para o destino enviado.

Claro que existe o lado obscuro, onde pessoas inescrupulosas usam o anonimato para usufruir em seu benefício próprio. Mas do mesmo modo que podemos correr o risco de ter alguma informação violada, existem também diversas ferramentas que ajudam a preservar a integridade das informações transmitidas pela rede.

Uma intervenção completa na rede para inibir este tipo de problema fica complicado em virtude da presença marcante da Internet em todas as partes, como aplicar sanções legais. São diversas culturas diferentes. Até que ponto o governo pode intervir, é uma situação muito polêmica, exigindo um debate amplo e aberto por todos os setores da sociedade global, não somente de um único país ou continente.

9. A Educação e aspectos legais para prevenção

Felizmente, têm havido muitas iniciativas de organizações e governos que estabelecem as boas práticas a serem seguidas, como descreve o relatório do FTC [FTC00], que busca a auto-regulamentação do processo nos mercados on-line, para garantir a privacidade das pessoas e de suas

informações; os diversos setores da sociedade e governo trabalham na educação dos usuários para que estes também tenham comportamentos que contribuam para a criação de ambientes seguros e privados.

A União Européia incentiva, segundo relatório do International Safe Harbor Privacy Principles [ISH00], a adequação de boas práticas e medidas que garantam a privacidade dos dados e informações dos usuários que utilizam serviços na Internet, através do consenso entre as partes envolvidas no processo, onde todos têm parcelas de responsabilidade na garantia da qualidade e integridade da informação. Orienta a sociedade a manter algum relacionamento comercial somente com empresas que declaram explicitamente em seus sites de comercio eletrônico como as informações de seus clientes serão armazenadas e protegidas - (Política de Privacidade) .

Há também como exemplo a IBM que não anuncia mais em sites nos Estados Unidos que não divulgam sua política de privacidade para os internautas. Ela tomou esta iniciativa porque muitos sites onde os internautas forneciam seus dados, passavam a vender ou ceder para outras empresas interessadas no envio de mala direta ou em campanhas de marketing diversas, conforme relata Saraiva [SAR00].

No aspecto legal a maior problemática se estende ao princípio da Territoriedade, Extraterritoriedade e Lugar do Crime elencados nos artigos 5°, 6° e 7° na parte Geral do Código Penal. Por exemplo um jovem tem acesso indevido a uma rede nos Estados Unidos e de lá resolve acessar os computadores na Alemanha, roubando e destruindo as informações. O Artigo 6° trata do Lugar do Crime, “Considere-se praticado o crime no lugar em que ocorreu a ação ou omissão no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado”. Como vemos, a ação foi no Brasil e o resultado no exterior, o local do crime é no Brasil, Estados Unidos ou Alemanha.

O artigo 5°, diz sobre o princípio da Territoriedade – “Aplica-se a lei brasileira, sem prejuízo de convenções, tratados e regras de direito internacional, ao crime cometido no território nacional”, como podemos perceber a ação é no Brasil, mas o resultado na Alemanha, como aplicar esse artigo se existe um conflito de Territoriedade entre a ação e o resultado da conduta.

O artigo 7° trata da Extraterritoriedade – “Ficam sujeitos à lei brasileira, embora cometidos no estrangeiro:

Inciso II, Os crimes – a) que por tratado e convenção, o Brasil se obrigou a reprimir, - b) praticados por brasileiros;

2 ° Nos casos do inciso II, a aplicação da lei Brasileira depende do concurso nas seguintes condições: a) entrar o ageno no território nacional; - b) ser o fato punível no país em que foi praticado”.

Como aplicar o inciso II, letras a e b, se os mesmos dependem do parágrafo 2°, obrigatoriamente, como no exemplo se o agente não saiu ou entrou fisicamente no país. E se no país onde os fatos ocorreram não configura crime?, podemos concluir que uma conduta criminosa aliada à Tecnologia da Informação utilizada na Internet conseguiram afrontar o conceito de espaço físico, substituindo por um espaço denominado de Virtual, que não é definido na legislação brasileira, conforme Gomes [GOM00].

10. Panorama da segurança e controle em informática

Estima-se que em 1998, prejuízos causados por falhas de segurança da informação chegaram a cifras da ordem de 140 milhões de dólares. Nessa pesquisa, feita por Zanini [ZAN9] e Roças[ROC00], constatou-se que as fraudes eram relacionadas a roubo de informações privadas, sabotagem, invasões, vírus e acesso não autorizado. A microinformática tornou essa situação mais crítica pois os sistemas operacionais dos computadores pessoais geralmente são muito frágeis quanto à segurança de acesso. A Internet também abre um flanco para invasão, porque tem a característica de permitir a interligação de praticamente qualquer máquina ao redor do mundo.

Para resolver esses problemas, existem muitas técnicas que, em linhas bem gerais, controlam o acesso a dados e sistemas ou codificam a informação para evitar sua leitura (criptografia), conforme Tanembaum [TAN97]. Essas técnicas são muito dinâmicas e funcionam como uma brincadeira de espionagem e contra-espionagem: na máquina é colocada uma proteção, mas logo alguém descobre uma maneira de quebrá-la e novamente o fornecedor aparece com uma nova versão mais robusta que, após algum tempo, também é violada. Veja o caso dos programas anti-vírus com versões semanais, em

virtude da grande propagação de vírus, provocando grandes prejuízos, é uma verdadeira ameaça, segundo Penteado [PEN99] .

Esse é um lado da questão. Existe outro lado que é o aspecto do comportamento, da ética. É a Privacidade da Informação definida anteriormente.. As organizações precisam possuir um Sistema da Privacidade que crie mecanismos internos de forma a garantir boas práticas.

A visão de processo para essa atividade é muito apropriada pois leva as organizações a não se preocuparem apenas com hardware e software de segurança, mas com um sistema completo. Esse sistema envolve, além dessa parte técnica, a definição de uma Política da Privacidade, de métodos e procedimentos referentes à privacidade e treinamento de todos os envolvidos.

Desta forma, um controle de acesso perde toda sua eficácia se o usuário divulgar sua senha. Informações sigilosas deixam de ser se não forem tratadas com sigilo pelos responsáveis. Um vazamento de informação pode comprometer uma empresa se não forem tomadas atitudes de correção e feito um esclarecimento para o usuário.

Uma organização que possui um Sistema da Privacidade, aborda de maneira mais global esses aspectos e, no primeiro exemplo acima, gera uma campanha para que o usuário não divulgue sua senha (que realmente os bancos fazem na utilização do cartão magnético, Home-banking) e, no segundo caso, treina as pessoas para que elas fiquem atentas e tenham atitudes, tais como não deixarem documentos à vista, senhas frágeis e anotadas em agenda pessoais. Todos esses procedimentos evitarão grandes problemas, que hoje comprometem a segurança de empresas, organismos governamentais e pessoas físicas.

A Política de Segurança ,conforme Caruso [CAR99], é um conjunto de diretrizes gerais destinadas a governar a proteção a ser dada a ativos da organização. Desenvolver políticas de segurança, padrões, diretrizes, e procedimentos devem ser feitas em consulta com as unidades organizacionais, e também através de funções que compõem o quadro administrativo das empresas como sistemas de informação, recursos humanos, administração de risco, e também departamentos chaves. Se não é possível formar um comitê gestor podemos consultar os representantes dos departamentos. Envolvendo estas várias unidades no processo, pode-se estabelecer as normas e procedimentos da política de segurança, segundo Hutt [HUT95]. Isto mostra que, com o envolvimento da classes de funcionários, os resultados da sua criação serão satisfatórios, levando-os a participar com mais atenção, este envolvimento também reduz as chances de problemas e falhas inesperadas depois que a política é promulgada.

Em qualquer atividade organizacional, a primeira tarefa a ser realizada é a definição do que se deseja e onde quer chegar, fixando objetivos, definindo os meios e recursos necessários, estabelecendo etapas a cumprir e os prazos das mesmas. Após a avaliação do que é necessário fazer é que se começa a executar o necessário. Mesmo assim não conseguimos executar com precisão os cronogramas estabelecidos, tendo a necessidade de acertos no planejamento original.

A política de segurança não é uma exceção, sendo necessário seguir as mesmas etapas como uma outra atividade qualquer dentro da empresa, pois implica em uso de capital, mão de obra, e recursos, representando assim investimento para a organização.

11. Conclusão

Este trabalho mostrou que privacidade e segurança são dois temas que caminham juntos, são complementares e necessários para garantir um bom funcionamento das transações na Internet.

A privacidade trata de aspectos de política e de comportamento e postura das pessoas que lidam com informações pessoais dos usuários e clientes da Organização. A segurança trata de aspectos mais técnicos e tecnológicos e preocupando-se com questões de integridade (invasão) e robustez dos sistemas.

Privacidade e segurança são os pilares necessários para que a Internet possa ser utilizada como meio para realização de transações financeiras e comerciais em um mundo globalizado. O usuário precisa se sentir seguro e ficar tranqüilo com relação aos aspectos de privacidade para que as transações possam ocorrer de forma mais maciça.

12. Bibliografia

[ANG99] ANGEHRN, A. **The Strategic Implications of the Internet**. Harvard Business Review, Nov-Dec 1999.[BER97] BERNSTAIN, T.; BHIMANI, A.; B.; SCHULTZ, E.; SIEGEL, C., A. **Segurança na Internet.** Tr. Insight Serviços de Informática. Rio de Janeiro: Campus. 1997.

[CAR99] CARUSO, C.; A.; A.; STEFFEN, F.; D. **Segurança em Informática e de Informações**.

2.Ed. São Paulo : Senac. 1999.
[DAV98] Davis, Simon; Europe to U.S.: *No privacy, no trade*. Wired Magazine, May 1998 www.wired.com/collections/privacy/6.05_euro_trade1.html 28/03/00
[DD00] - Discussion Draft – *Elements os Effective Self-Regulation for Protection of Privacy* www.ecommerce.gov/staff.html 27/03/00
[FAJ98] FAJARDO, K.; Lojas abrem suas portas com Segurança. **Internet World.** n° 35, 1998, pag. 39 a 43.
[FTC00] FTC, Federal Trade Commission USA, http://www.usis.it/ejournal/other_pdf/ftc9907.pdf, 05/2000.
[GOM00] GOMES, O., J., A. **Segurança Total protegendo-se contra os hackers**, São Paulo: Makron Books,2000.
[HER99] HERNDERSON, S.,C. SNYDER, C.; A. Personal information privacy: implications for MIS managers, **Information & Management,** n ° 36, 1999, pag. 213-220.
[HUT95] Hutt, A, E; Boworth S; Hoyt, D, B; Computer Security Handbook , 3 Edição; John Wiley & Sons, Inc 1995.
[HUT95] HUTT, A., E.; BOWORTH, S.; HOYT, D., B. **Computer security handbook** . 3.Ed. New York John Wiley & Sons Inc, 1995.
[ISH00] DRAFT, International Safe Harbor Privacy Principles Issued by The U.S. Departament of Commerce, http://www.ita.doc.gov/td/ecom/RedlinedPrinciples31600.htm , 05/2000.
[OLI00] OLIVEIRA, E.; Segurança de Informações em Rede, http://www.bhnet.com.br/~comando/pag366.html, 05/2000.
[ONU00] ONU - Organização das Nações Unidas. **Declaração Universal dos Direitos Humanos.** www.unhchr.ch/udhr/lang/port.htm, 05/2000.
[PEN99] PENTEADO, S. De olho na segurança. **InformationWeek.** n ° 6, julho/1999, pag. 26-34.
[PIT98] Pitofsky, R.; Azcuenaga, M.L; .Anthony, S.F.; Thompson, M.W.; Swindle, O.; *Privacy Online: A Report to Co*ngress – Federal Trade Commision, June 1998 www.ftc.gov/reports/privacy3/toc.htm 01/03/00
[PIT99] Pitofsky, R.;Anthony, S.F.; Thompson, M.W.; Swindle, O.; *Self-Regulation and Privacy Online: A Report to Co*ngress – Federal Trade Commision, July 1999 www.usis.it/ejournal/other_pdf/ftc9907.pdf 20/04/2000
[ROC00] RÔÇAS, C. Credibilidade em cheque. **Internet Business.** n ° 32 , Abril 2000, pag. 48-55.
[SAN98] SANTOS, J.; Todo Cuidado é pouco; **Internet Business** n° 14; Outubro 1998, pg 43-45
[SAR00] SARAIVA, J. Privacidade - protegendo o usuário. **meiodigita**l. n.° 1, Maio 2000, pag. 46-7.
[SIM99] Simson G, Spafford G; Comércio & Segurança na Web, São Paulo; Market Press, 1999.
[TAN97] TANENBAUM, A., S. **Rede de computadores**. Rio de Janeiro, Campus, 1997.
[ZAN99] ZANINI, A., S. **Proposta e implementação de controle de acesso a informações em Ambiente de Microinformática**. São José dos Campos, 1999. Tese (Doutorado) - Instituto Tecnológico de Aeronáutica. 1999