

**LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO DO RN
BACHARELADO EM SISTEMA DE INFORMAÇÃO**

**UM ESTUDO TEÓRICO SOBRE SEGURANÇA E PRIVACIDADE NO COMÉRCIO
ELETRÔNICO**

**UM ESTUDO TEÓRICO SOBRE SEGURANÇA E PRIVACIDADE NO COMÉRCIO
ELETRÔNICO**

Monografia apresentada ao Curso de
Graduação em Sistema de Informação da
Faculdade Natalense para o Desenvolvimento do Rio
Grande do Norte como requisito parcial para obtenção do
grau de Bacharel em Sistema de
Informação

Orientadora:

Leite Augusto da Silva **Maria de Fátima Araújo**

**NATAL
2002**

Maria de Fátima Araújo

**UM ESTUDO TEÓRICO SOBRE SEGURANÇA E PRIVACIDADE NO COMÉRCIO
ELETRÔNICO**

**Monografia apresentada ao Curso de
Graduação em Sistema de Informação da
Faculdade Natalense para o
Desenvolvimento do Rio Grande do Norte
como requisito parcial para obtenção do
grau de Bacharel em Sistema de
Informação**

Orientador:

Luiz Augusto Machado Mendes Filho

**NATAL
2002**

RB-13741 M

FARN
BIBLIOTECA
Nº Reg. M000224
04 / 05 / 05

004.738-5:658.8

A 692

Maria de Fátima Araújo

2002

UM ESTUDO TEÓRICO SOBRE SEGURANÇA E PRIVACIDADE NO COMÉRCIO ELETRÔNICO

Monografia apresentada ao Curso de
Graduação em Sistema de Informação da
Faculdade Natalense para o
Desenvolvimento do Rio Grande do Norte
como requisito parcial para obtenção do
grau de Bacharel em Sistema de
Informação

Orientador:

Luiz Augusto Machado Mendes Filho

NATAL
2002

UNIVERSIDADE DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO DO RN
BACHARELADO EM SISTEMA DE INFORMAÇÃO

UM ESTUDO TEÓRICO SOBRE SEGURANÇA E PRIVACIDADE NO COMÉRCIO
ELETRÔNICO

Maria de Fátima Araújo

Monografia apresentada e aprovada em 18 de Dezembro de 2002, pelo banca examinadora
composta pelos seguintes membros:

Araújo, Maria de Fátima

Um estudo teórico sobre segurança e privacidade no comércio eletrônico / Maria de Fátima Araújo, ____ Natal, 2002.

32p.

Monografia (Bacharelado em Sistema de Informação)-
Faculdade Natalense para o Desenvolvimento do Rio Grande do
Norte.

1.Comércio Eletrônico – monografia. 2. Segurança de dados
na Internet – monografia. 3. Privacidade na Internet – monografia. I.
Título

RN/FARN/BC

CDU – 004.736.5658.8

LIGA DE ENSINO DO RIO GRANDE DO NORTE
FACULDADE NATALENSE PARA O DESENVOLVIMENTO DO RN
BACHARELADO EM SISTEMA DE INFORMAÇÃO

UM ESTUDO TEÓRICO SOBRE SEGURANÇA E PRIVACIDADE NO COMÉRCIO
ELETRÔNICO

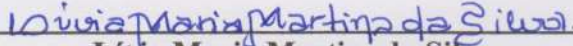
Maria de Fátima Araújo

Monografia apresentada e aprovada em 18 de Dezembro de 2002 pela banca examinadora
composta pelos seguintes membros:



Luiz Augusto Machado Mendes Filho
Orientador

Selma Monteiro da Silva Veldman
Membro examinador



Livia Maria Martins da Silva
Membro examinador

Natal, 18 de Dezembro de 2002

AGRADECIMENTOS

Este trabalho foi desenvolvido com o apoio de várias pessoas e instituições. Por isso, quero agradecer a todos, com a mais simples palavra "OBRIGADO", especialmente ao final da graduação, com o encargo e as responsabilidades de todos que contribuíram para a realização deste trabalho.

Assim, agradeço a todos os meus professores, pelos ensinamentos ministrados e pelo estímulo aos desafios profissionais e acadêmicos que me deram.

Aos meus professores revisores e orientador, os quais expõem toda a minha produção, e me inspiram ao professor Luis Augusto M. Mendes Filho, que incondicionalmente me distingue com atenção, seu apoio e sua dedicação e soube perceber os erros e acertos deste trabalho. Também ao amigo o melhor.

A Faculdade Marilense para a Desempenho do Rio Grande do Norte, particularmente aos membros do seu Diretoria, professores e funcionários, pela atenção e suporte que me ofereceram para a realização e conclusão deste trabalho produtivo e valioso que é a produção de conhecimento.

E a todos que de alguma forma, contribuíram tanto direta quanto indiretamente na elaboração deste trabalho, agradeço pelas suas palavras, sugestões, críticas e lições de vida e amizade, também para aqueles que não estão mais conosco, pois todos os momentos são respeitos e confiantes, e com a certeza de que todos os momentos são aproveitados de vida.

Dedico este trabalho a Deus, pela saúde, proteção, e oportunidade que me tem concebido. A meu filho Marcelo Araújo, a meus pais, a minha família, e em especial ao meu irmão Carlos Paz Araújo e a Wallkin Spencer que sempre me incentiva e apóia.

AGRADECIMENTO

Este trabalho foi construído com o apoio de várias pessoas e instituição. Por isso, venho agradecer a todos, com a mais simples palavra "OBRIGADO", espero ter atingido os fins pretendidos neste empenho e ter atendido as expectativas de todos que contribuíram para a realização desta construção.

Assim, agradeço a todos os meus professores, pelos ensinamentos ministrados e pelo estímulo aos desafios profissional e acadêmico que deles recebi.

Aos meus professores revisores e orientador, os quais expresso toda a minha gratidão, e em especial ao professor Luiz Augusto M. Mendes Filho, que incondicionalmente me distinguiu com atenção, seu apoio e sua dedicação e soube perceber os erros e acertos deste trabalho, Fazendo-o sempre o melhor.

À Faculdade Natalense para o Desenvolvimento do Rio Grande do Norte, particularmente nas pessoas de seus Diretores, professores e Funcionários, prestação e suporte que me ofereceram para a realização e conclusão desta oportunidade produtiva e valorosa que é a produção de conhecimento.

E a todos que, de alguma forma, contribuíram tanto direta quanto indiretamente na elaboração deste trabalho, agradeço pelas suas amizades, profissionalismo, e lições de vida e seriedade, também para aqueles que tem a falta dessas características, pois todos os equilíbrio entre respeitos e confrontos, e entre simpatias e antipatia são sempre necessários para o nosso aprendizado de vida.

SUMÁRIO

1. INTRODUÇÃO.....	8
1.1 PROBLEMA DE PESQUISA.....	10
1.2 OBJETIVOS.....	11
1.3 JUSTIFICATIVA.....	11
1.4 METODOLOGIA.....	12
2. REFERENCIAL TEÓRICO.....	13
2.1 INTERNET.....	13
2.2 COMÉRCIO ELETRÔNICO.....	15
2.3 FIREWALL.....	17
2.4 SEGURANÇA.....	18
2.5 PRIVACIDADE.....	21
3. ANÁLISE DE RESULTADOS.....	25
3.1 CRIPTOGRAFIA.....	25
3.2 CRIPTOGRAFIA DE CHAVE PÚBLICA E PRIVADA.....	28
3.3 CRIPTOGRAFIA DE CHAVE PÚBLICA.....	29
4. CONCLUSÃO.....	31
5. REFERÊNCIAS BIBLIOGRÁFICAS.....	32

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, discute os aspectos tecnológicos, 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: Segurança, Privacidade, Comércio Eletrônico

ABSTRACT

Abstract:

Internet technology has been accomplishing a revolution in managements 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 thouse new technologies has been questionel, inhibitting its growth.

This work present a discussion on that subject and discusses technological 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.

1. INTRODUÇÃO

Este trabalho irá abordar um estudo teórico sobre Segurança e Privacidade no Comércio Eletrônico. A pesquisa foi planejada para mostrar algumas das estratégias do projeto ao longo desta monografia e muitas das idéias fundamentais empregadas na análise de segurança e privacidade.

O movimento da 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 propondo um intercâmbio entre países como se todos estivessem fisicamente próximos. Essa sensação de proximidade ocorre devido aos 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 insegurança 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.

Segundo Bernstein (1997), as oportunidades de negócio vêm aumentando cada vez mais e as empresas de acordo com suas necessidades, estão utilizando a Internet para os serviços como: propaganda, marketing, suporte ao cliente e comércio eletrônico. Nesses últimos anos, há um aumento exponencial de possibilidades de negócio, 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 de tecnologias como por exemplo a compra eletrônica ou com a quebra de paradigmas através de novas aplicações como leilão eletrônico ou os metamediários que são intermediários virtuais de transações comerciais.

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 utilizando essa tecnologia.

Estima-se que em 1998, prejuízos causados por falha de segurança da informação chegaram a cifras da ordem de US\$140 milhões. Nessa pesquisa feita por Zanini (1999) e Roças (2000), constatou-se que as fraudes eram relacionadas ao roubo de informações privadas, sabotagem, 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 linha bem gerais, controlam o acesso a dados e sistemas ou codificam a informação para evitar sua leitura (criptografia), conforme o Tanenbaum (1997). 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 antivírus com versões semanais, em virtude da grande propaganda de vírus, provocando grandes prejuízos, é uma verdadeira ameaça segundo Penteado (1999).

Esse é o 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, treinam as pessoas para que elas fiquem atentas e tenham atitudes, tais como não deixarem documentos á vista, senhas frágeis e anotadas em agendas pessoais. Todos esses procedimentos evitarão grandes problemas, que hoje comprometem a segurança de empresas, organismo governamentais e pessoas físicas.

A política de segurança, conforme Caruso (1998), é um conjunto de diretrizes gerais destinadas a governar a proteção a ser dada a ativos da organização. Desenvolver política de segurança, padrões, diretrizes e procedimentos devem ser feitos 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 pode consultar os representantes dos departamentos. Envolvendo estas várias unidades no processo, pode-se estabelecer as normas e procedimentos de segurança, segundo Hutt (1995). Isto mostra que, com o envolvimento da classe 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 atividade qualquer dentro da empresa, pois implica em uso de capital, mão de obra, e recursos, representado assim, investimento para a organização.

1.1 PROBLEMA DE PESQUISA

Com o crescimento exponencial do comercio eletrônico fica cada vez mais importante a melhoria deste sistema. Pois, hoje um simples PC pode passar de mais de um Gigahertz, e assim pode tentar fatorizar em tempo recorde o produto dos dois números primos e descobrir a chave secreta durante uma transação bancária.

Com a chegada da Internet sem fios "WIRELESS INTERNET" a capitação de uma senha, código de cartão de crédito, etc. via rádio aumenta ainda mais a necessidade de códigos robustos.

Além da óbvia necessidade de manter em segredo a identidade, número de conta, históricos médicos etc.; nos cartões de crédito, um sistema deste tipo já vem sendo usado a alguns anos. Por exemplo, uma quantidade de cartões tipo "Visa , American Express " e outros, a sua chave secreta é passar para os bancos no mundo inteiro uma (ou várias) chaves publicas. Uma vez que um banco, membro do grupo de usuários da Visa obtém a chave pública, neste pode emitir cartões com números em códigos, isto é cifrados e enviá-los dentro do sistema Visa sem colocar em jogo a segurança do sistema caso alguém descubra a chave do código do seu cartão. O tipo de cifragem é irrelevante, mas este protocolo, ou seja a infraestrutura Pki é o que é importante.

1.2. OBJETIVOS

O objetivo geral desta monografia foi estudar as características de segurança e privacidade no Comércio Eletrônico.

Os objetivos específicos que o trabalho se propõe a encontrar são os seguintes:

- Descrever o uso do sistema de segurança e privacidade para as empresas;
- Explicar como funciona a criptografia por chave pública e privada
- Explicar como funciona a criptografia RSA.

1.3. JUSTIFICATIVA

A justificativa deste tema, apenas apresenta-se ainda mais da própria monografia dentro da área de sistemas de informações que o abrange o nosso curso; e, a justificativa do valor do tema dentro desta área.

No primeiro caso, o fator segurança e proteção de bancos de dados já foram discutidos e é óbvio. No segundo, o valor deste tema é de tal importância que a própria evolução do uso de cartões de credito via compras na Internet é limitada pela falta de confiança do publico na privacidade do sistema. Daí, o uso dos cartões com "CRIPS" ou "SMART CARDS" já estão sendo testados para dar maior segurança.

O estudo desta pesquisa está também na coordenação de uma bibliografia especializada que é muito carente na literatura nacional na área de sistemas de Informação.

1.4 METODOLOGIA

A metodologia utilizada consiste em uma pesquisa exploratória porque visa entender uma situação, a partir de estudos feitos por diferentes autores ou vivenciados por várias pessoas.

O método de pesquisa se deu através da navegação, coleta de dados, livros de explanação simplória para o publico em geral e também textos com mais rigor. Revistas e catálogos de publicações de congressos nesta área também serão fonte de informações. Enfim, é um campo emergente no Brasil e continuamente preocupante nos Estados Unidos, a seleção de fontes será de necessidade fundamental ao conteúdo deste trabalho dado o espaço resumido de uma monografia.

O objetivo maior para a realização deste estudo exploratório foi mostrar a necessidade da qualidade e desempenho dos Sistema de Informação em sua unidade de negócio. Como quaisquer outros recursos vitais para as empresas, os recursos de hardware, redes e dados dos sistemas de informação precisam ser protegidos por controles embutidos para garantir sua qualidade e segurança.

A pesquisa foi dividida em duas etapas: A explicação básica do RSA (RSA sua evolução, história do RSA e o RSA hoje, criptografia no Brasil e o estudo-da-arte), e a pesquisa do estudo abrangente do que existe nesta área de encriptografia (códigos e cifragem, a criptografia na era digital), desde caso de software que vendem "packages", até as associações, usuários, peculiaridade única no Brasil, uso em governo, etc.

2. REFERENCIAL TEÓRICO

Para focalizar melhor e discutir questões da análise de Segurança e Privacidade é preciso citarmos alguns conceitos de comércio eletrônico (CE), Internet, Sistema de Criptografia de chave pública RSA, Além da óbvia necessidade de manter em segredo a identidade, número de conta, históricos médicos etc. ; a análise deste estudo está também na coordenação de uma bibliografia especializada que é muito carente na literatura nacional na área de sistemas de informação.

2.1 INTERNET

Segundo Bernstein et. al (1997), A Internet é um aglomerado de redes TCP/IP espalhadas pelo mundo inteiro que na verdade ninguém controla, apesar de tradicionalmente a IBA (Internet Activities Board) tê-la administrado. A IAB, através de uma organização subsidiária, a IETF (Internet Engineering Task Force), prevê o desenvolvimento e a utilização do conjunto de protocolos TCP/IP. Isso envolve, dentre outras coisas, a definição de uma direção a ser seguida em termos de pesquisa, a definição de padrões na Internet e a determinação dos protocolos necessários em implementações do conjunto de protocolos TCP/IP. A IAB foi extremamente bem-sucedida em prever a criação da Internet global atual, mas a Internet pode ter ultrapassado as expectativas.

Alguns dos computadores na Internet oferecem uma variedade de serviços, que pessoas como você e eu usam por meio de nossos computadores. Eles publicam documentos, por exemplo, ou oferecem fóruns para nos comunicarmos com outras pessoas. O crescimento da Internet tem sido explosivos. Em 1985, havia mais de 2.000 computadores host na Internet. Agora há bem mais de 9 milhões de computadores host que suportam muitos milhões de usuário. A cada mês, a Internet incorpora milhões de novos usuários.

Hoje em dia, as empresas utilizam a Internet principalmente para propaganda, marketing e suporte ao cliente. Por ser uma rede global, a base de clientes da Internet é a população do mundo inteiro, o que a torna incrivelmente atraente para transações comerciais. Mas como a Internet pode ajudar as empresas a fazer negócios?

A Internet pode se mostrar como uma ferramenta de imenso valor para o desenvolvimento de novos produtos; ela é ideal para qualquer produto que possa ser armazenado como informação digital em um computador. Muitos setores poderiam se beneficiar de um processo de fabricação baseado na Internet, os mais óbvios seriam os programas de computador, as publicações financeiras e os campos da música e da arte.

A tecnologia da Internet teve um êxito tão grande que as empresas estão começando a utilizá-la internamente. A tecnologia que é usada para anunciar produtos e compartilhar informações mundiais está sendo empregada para disseminar informações internas de uma empresa. As empresas estão começando a reprojeter seus processos comerciais com base na tecnologia da Internet.

A desintermediação deverá ser um objetivo estratégico para as empresas estão reprojutando seus processos comerciais. As áreas da tecnologia da informação poderão explorar as vantagens do desenvolvimento e da pesquisa colaborativa independentes de um local fixo. As empresas estão começando a usar a tecnologia da Web para compartilhar informações internas, particularmente em relação a aplicações comerciais e atividades cooperativas envolvendo o uso de computadores.

Oliveira (2000) a Internet é hoje um dos assuntos mais discutidos na maior parte do mundo e o mais estudado, devido ao impacto que seu uso tem trazido para a humanidade.

Constituir um universo novo onde a cada dia uma nova idéia nasce, um novo problema surge, novos programas revolucionam o mercado, uma nova forma de comércio surge, cresce e desaparece. Podemos observar, nos diversos setores da sociedade, uma crescente preocupação com a Internet, tendo em vista a relevância do assunto, tanto no âmbito familiar, quanto no empresarial.

O problema da segurança na Internet é, atualmente, uma grande barreira para o comércio eletrônico. Em todo o mundo discute-se maneiras e soluções para proteger a Internet de ataques e invasões. O primeiro obstáculo encontrado é a própria alma da Internet. A WWW nasceu livre, liberdade esta, quase que absoluta, e a colocação de barreiras assusta a todos. O problema é que, um dos aspectos mais interessantes e agradáveis da Internet é fato de que se pode entrar e sair de um site de maneira rápida e sem a necessidade de identificar-se.

2.2 COMÉRCIO ELETRÔNICO

Segundo Bernstein et. al. (1997), o comércio eletrônico é a nova fronteira e, como tal, tem sua própria linguagem e terminologia. Primeiro, existem instrumentos financeiros associados ao comércio eletrônico, tais como o dinheiro eletrônico, o dinheiro digital, cartões de valor armazenamento, cartões inteligentes e cheques eletrônicos.

Segundo, há muitos termos de contabilidade usados para descrever os diferentes tipos de sistemas de pagamento eletrônico: pagamento anônimo, pagamento identificado; sistemas on-line, sistemas off-line; e transações rastreáveis, transações incondicionalmente não-rateáveis e transações "as cegas".

Por último, existem as tecnologias que ativam a segurança: criptografia com chave pública, assinatura digital, autenticação, credenciais e certificados. Todos esses termos serão conhecidos de todos os que projetam e implementam sistemas de pagamento seguros.

Um dos principais objetivos de como avaliar soluções de segurança para o CE é afirmar que a Internet é uma rede descentralizada e heterogênea, que não é gerenciada por uma única entidade. Consequentemente, os padrões e as práticas de segurança de seus hosts são muito diversos. Pressupor que qualquer mensagem enviada pela Internet está a salvo de atividades malignas é uma infantilidade. Como a Internet não foi projetada para se proteger desses ataques, cabe a você atender às necessidades de segurança de sua empresa. O nível de segurança a ser exigido dependerá do tipo de atividade que você deseja conduzir e das políticas de segurança de sua empresa. Cabe lembrar que suas necessidades na Internet podem surgir aos poucos, e sua primeira exigência poderá ser apenas um recurso de marketing. Pense no futuro, e crie sua infraestrutura de segurança tendo em mente suas futuras necessidades, e não apenas ao de hoje.

Ao avaliar suas soluções para o comércio eletrônico, você vai ter que determinar o que deseja oferecer em termos de serviço, o mecanismo de entrega para esses serviços e os tipos de transações que deseja desenvolver. A exemplo do que acontece com outras decisões técnicas, suas escolhas técnicas dependerão das suas necessidades para o comércio eletrônico.

As ofertas de serviços podem variar desde fornecer informações on-line e aceitar aplicações on-line dos usuários, até processar transações completas junto a bancos de dados corporativos. À medida que as necessidades comerciais se aproximarem de um processamento

financeiro on-line, as exigências quanto à segurança acabarão se tornando mais rígidas. Seu primeiro passo no processo é identificar as ofertas de serviço da sua empresa. Lembre-se de proteger os tipos de atividades que você conduzirá na Internet para pelo menos os próximos 18 meses.

Quanto mais as suas necessidades comerciais se aproximarem de um processamento de banco de dados totalmente on-line, maior será o controle que você deverá ter sobre seu mecanismo de entrega. Essa escolha também determinará o nível de especialidade em segurança que você precisará oferecer em sua empresa, bem como o número de recursos exigidos para manter as instalações.

Os tipos de transações financeiras necessárias aos seus negócios determinarão sua próxima escolha. As opções de tipos de sistemas de pagamento eletrônico.

- Transações on-line com cartão de crédito (CyberCash, Inc.)
- Sistemas de débito/crédito (First Virtual Holdings, Inc.)
- Moeda eletrônica (DigiCash, Inc.)

Segurança em comércio eletrônico segundo Oliveira (2000), é uma preocupação nas transações, particularmente com cartão de crédito, é o grande ponto de desconfiança dos consumidores. Além disso, existe a dificuldade das empresas de cartão de crédito aceitarem pagamento pela rede, devido ao fato de que elas estão bancando sozinhas, até então, o investimento na segurança. A saída está nas parcerias entre as instituições financeiras para a diluição desse custo.

Uma preocupação muito comum entre a maioria dos participantes da negociação eletrônica é com relação à segurança, reduzindo ou dificultando a comercialização. A atual ausência de segurança no pagamento on-line está impedindo que grandes segmentos da população efetuem suas compras.

Entretanto, a barreira está sendo superada e comerciantes on-line não deixam que as preocupações com a segurança no pagamento sejam obstáculo aos seus negócios na Web.

Segundo Cormen, et. al. (2001), o comércio eletrônico permite que mercadorias e serviços sejam negociados e trocados eletronicamente. A capacidade de manter privativas informações como números de cartões de créditos, senhas e extratos bancários é essencial para ampla utilização do comércio eletrônico. A criptografia de chave pública e as assinaturas digitais

estão entre as tecnologias centrais utilizadas e se baseiam em algoritmos numéricos e na teoria dos números.

Para Nacamura (2001), o Comércio Eletrônico está gerando uma forma de negócios. Esta forma de negócio poderá, em breve, vir a ser o modo padrão de operar, substituindo a forma de trabalho atual.

As principais mudanças estão relacionadas ao gerenciamento dos documentos e ao modo como a comunicação está sendo estabelecida, com alto índice de informatização e automatização de processos. A realização de parcerias ou alianças estratégicas é a ordem do dia para a sobrevivência em um mundo cada vez mais competitivo.

Estão em alta a integração, a padronização e a automatização, em um processo de reengenharia de processos que visa maior eficiência e eficácia no atendimento aos clientes.

Este é o reflexo do movimento da globalização, que foi acelerado com o advento da Internet.

Segundo O'Brien (2001), para as empresas interconectadas na era da Internet, intranets, e extranets, o comércio eletrônico é mais do que a mera compra e venda de produtos online. Em lugar disso, ele engloba o processo online inteiro de desenvolvimento, marketing, venda, entrega, atendimento e pagamento por produtos e serviços comprados por comunidades mundiais de clientes virtuais, com o apoio de uma rede mundial de parceiros comerciais. Os sistemas de comércio eletrônico se valem de recursos da Internet, intranets, extranets e outras redes de computadores para apoiar cada etapa desse processo. O comércio eletrônico pode incluir, por exemplo, processos de marketing interativo, pedidos e pagamentos na Rede Mundial de Computadores, acesso por extranet a banco de dados de estoque pelos clientes e fornecedores, acesso por intranet a cadastros de clientes por representantes de vendas e atendimento ao consumidor e no desenvolvimento de produtos via grupos de notícias da Internet e trocas de e-mail.

Para O'Brien (2001), as empresas se dedicam a três categorias básicas de aplicações de comércio eletrônico que são: processos empresa-consumidor, empresa-a-empresa e processos empresariais internos.

Comércio empresa-consumidor : as empresas precisam desenvolver praças de mercado eletrônico atraentes para seduzir e vender produtos e serviços aos consumidores. As empresas podem oferecer, por exemplo, sites em multimídia que apresentam fachadas de lojas virtuais e

centros comerciais virtuais, processamento interativo de pedidos e sistemas seguros de pagamentos eletrônico.

Aplicações Empresas-a-Empresas: Nesta categoria de comércio eletrônico envolve mercados comerciais eletrônicos e ligações diretas de mercado entre as empresas. Muitas empresas, por exemplo, oferecem à comunidade dos negócios uma multiplicidade de informações de marketing e produtos na Rede Mundial de Computadores. Outras também recorrem ao intercâmbio eletrônico de dados (EDI) pela Internet ou extranets para troca direta computador-a-computador de documentos de transações comerciais com seus clientes e fornecedores.

Processos Empresariais Internos: Todas as funções organizacionais e muitos processos empresariais são afetados por atividades de comércio eletrônico. Muitas empresas interconectadas são movidas pelos clientes e pelo mercado. Elas monitoram e avaliam constantemente as informações online sobre seus clientes, fornecedores e concorrentes a partir de seus sites e grupos de discussão na Internet. Essas informações são disponíveis via intranets para todas as funções organizacionais e utilizadas para moldar o desenvolvimento de produtos, programas de marketing, atendimento ao cliente e estratégias competitivas de uma empresa.

2.3 FIREWALL

Outro item importante segundo Oliveira (2000), com relação à segurança necessária ao comércio eletrônico é a utilização do Firewall. É um conjunto de hardware e software utilizado como alternativa para proteger computadores individuais na rede.

Muitas organizações têm optado pela solução de proteger a sua rede interna a sua rede interna sem primeiro contar suas premissas. Para criar esse isolamento é utilizado o Firewall, que do modo, também pode controlar o acesso da rede interna à Internet.

Para Oliveira (2000). Firewall é uma barreira inteligente entre a rede local e a Internet, através da qual só passa tráfego autorizado. Este tráfego é examinado pelo Firewall em tempo real e a seleção é feita de acordo com a regra “o que não foi expressamente permitido, é proibido”, portanto, ele pode ser usado para bloquear o acesso a sites particulares na Internet, ou para prevenir que certos usuários ou máquinas, acessem certos servidores ou serviços, monitorando comunicações entre a rede interna e a externa.

O Firewall também possibilita armazenar toda comunicação entre sua rede interna e externa e criptografar dados que são enviados pela rede.

Firewalls são sistemas que têm como objetivo estabelecer regras e filtros de tráfego entre duas redes. Eles são utilizados como a primeira linha de defesa contra ameaças externas a sua rede.

Por ser a primeira linha de defesa, os sistemas de Firewall devem ser cuidadosamente instalados e gerenciados. No caso de Firewalls instalados em servidores (normalmente Windows NT e Unix), o Sistema Operacional deve também ser cuidadosamente configurado para o nível máximo de proteção.

Segundo Oliveira (2000). Todo sistema, por mais seguro que seja, está sujeita a falhas. As principais são:

- Se um usuário interno conectar na rede externa, ele criará uma porta de acesso à rede sem passar pelo Firewall;
- Efetivo contra ataques externos, mas internamente não. A maioria dos incidentes é causado por pessoal interno;
- Bugs, problemas de má configuração ou falha de equipamento, podem deixar o Firewall suspenso por algum tempo;
- Colisões da rede interna e externa podem evitar o acesso ao Firewall por instante, um intruso poderá invadir a rede interna.

Nem todos os modelos de Firewall são iguais. Existem três tipos básicos de Firewall, sendo que algumas combinam os tipos e chegam a implementar novas funcionalidades.

2.4 PRIVACIDADE

Segundo O'Brien (2001), a tecnologia da informação torna viável em termos técnicos e econômicos a coleta, armazenamento, integração, intercâmbio e recuperação rápida e fácil de dados e informações. Esta característica produz um efeito benéfico importante na eficiência e eficácia dos sistemas de informação computadorizados.

Entretanto, o poder da tecnologia da informação de armazenar e recuperar informações pode ter um efeito negativo no direito à privacidade de cada indivíduo.

Mensagens de e-mail confidenciais dos funcionários, por exemplo, são monitorizadas por muitas empresas. Informações pessoais individuais estão sendo coletadas a cada vez que as pessoas visitam um site da Rede Mundial de Computadores. Informações confidenciais sobre indivíduos, contidas em bancos de dados centralizados de escritórios de créditos, agências governamentais e empresas privadas tem sido roubados ou exploradas, resultando em invasão de privacidade, fraude e outras injustiças.

O uso não autorizado dessas informações tem prejudicado seriamente a privacidade dos indivíduos. Erros em tais bancos de dados podem prejudicar gravemente a situação de crédito ou reputação do indivíduo.

Os padrões de segurança na Internet :

- PGP: Pretty Privacy;
- SHTTP: Secure Hyper Text Transmission Protocol;
- SSL: Secure Sockets Layer;
- PEM: Privacy Enhancel Mail;
- S/MINE: Secure Multi- purpose Internet mail Ext.

A privacidade, segundo O'Brien (2001), 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 éticos), dados médicos (históricos ou condições de saúde, etc.), escolaridade (graus e outros) imagens da pessoa e outras informações identificáveis como hobbies, área 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, senhas de acesso a serviços financeiros on-line, dados sobre renda ou patrimônios 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 mais 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 banco 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 Commission dos Estados Unidos (PIT99) 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 identifica-se para o usuário e informar quais dados esta 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.

2.5 SEGURANÇA

Segurança segundo Simson (1999), é definida como um conjunto de procedimentos, práticos e tecnologias usadas para proteger os servidores, usuários da Web e suas empresas e deve possuir os seguintes aspectos segundo Hutt (1995):

- **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 acesso 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 atitude para uma ação corretiva.
- **Disponibilidade:** O sistema tem que prover resposta eficiente e capacidade adequada para apoiar um desempenho aceitável. Recuperar-se depressa de inter rompimento de longo prazo. Cópias de segurança de dados, inclusive de equipamentos, testes 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 e 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 controle administrativos e técnicos. Medidas administrativas incluem publicação de políticas de segurança, padrões, e diretrizes treinamentos 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 recursos), 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.

Na gestão empresarial integrada na Empresa Virtual, segundo Oliveira (2000), os gestores deverão ter uma política de segurança bastante eficaz, pois toda a tomada de decisão depende da informação. A área de tecnologia deve garantir o controle de acesso às informações.

A informação tem um imenso valor. Além disso, na Empresa Virtual, a informação passa a ser “conduzida” pelo mundo todo, dependendo de como ela está estruturada.

2.5.1 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 (1999).

Propósito de 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 riscos, 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.

Conteúdo da política

Descrever os recursos e 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.

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 um 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 (1999) e Oliveira (2000).

Política geral de segurança

É interessante apresentar itens de uma política que determinam o início de parâmetros necessários à criação de um ambiente como segurança e confiabilidade, conforme Caruso (1999) e Hutt (1995), 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 trabalhistas cabíveis;
- Todos os ativos devem receber classificação quanto à preservação e proteção;
- Todos os ativos devem pertencer 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 acesso físico;

- Administração de segurança;
- Controle de acesso lógicos;
- Monitoração e auditoria de segurança.

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.

Muitos problemas, segundo Bernstein (1997), podem ser resultante 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. A 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 nos produtos.

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 comportamento.

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.

Todas as organizações, segundo Caruso (1998), 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.

Sistema de Segurança nas Empresas

Segundo O'Brien (2001), A responsabilidade pelo controle da qualidade e desempenho dos sistemas de informação em uma unidade de negócio. Como quaisquer outros recursos vitais para as empresas, os recursos de hardware, software, redes e dados dos sistemas de informação precisam ser protegidos por controles embutidos para garantir sua qualidade e segurança por isso que os controles são necessários.

Os controles eficazes propiciam a segurança dos sistemas de informação, ou seja, a precisão, integridade e segurança das atividades de recursos dos sistemas de informação. Os controles podem minimizar erros, fraude e destruição nos sistemas de informação interconectados que hoje ligam entre si usuários finais das organizações. Controles eficazes também fornecem garantia de qualidade para os sistemas de informação, eles podem deixar um sistema de informação computadorizado mais livre de erros e fraude é capaz de fornecer produtos de informação de qualidade mais alta do que os tipos manuais de processamento da informação. Isso pode ajudar a reduzir o impacto negativo potencial e aumentar o impacto positivo que a tecnologia da informação pode produzir na sobrevivência e sucesso das empresas na qualidade de vida na sociedade.

Os controles de instalação hoje já existe métodos que protegem as instalações de computação e redes de uma organização e seu conteúdo contra a perda ou destruição. As redes e os centros de computação estão sujeitos a casualidade como acidentes, desastres naturais, sabotagem, vandalismo, uso não autorizado, espionagem industrial, destruição e roubo de recursos. Consequentemente, várias salvaguardas e procedimentos de controle são necessários para proteger os recursos vitais de hardware, software, rede e dados de uma empresa. Isto é particularmente decisivo quando mais e mais empresas se envolve no comércio eletrônico pela Internet.

3. ANÁLISE DE RESULTADO

3.1 CRIPTOGRAFIA

Segundo o autor Singh (2001), durante milhares de anos, reis, rainhas e generais dependeram de comunicações eficientes de modo a governar seus países e comandar seus exércitos. Ao mesmo tempo, todos estavam cientes das conseqüências de suas mensagens caírem em mãos erradas, revelando segredos preciosos a nações rivais ou divulgando informações vitais para forças inimigas. Foi a ameaça da interceptação pelo inimigo que motivou o desenvolvimento de códigos e cifras, técnicas para mascarar uma mensagem de modo que só o destinatário possa ler seu conteúdo.

À medida que a informação se torna uma mercadoria cada vez mais valiosa e a revolução nas comunicações muda a sociedade, o processo de codificação de mensagens vai desempenhar um processo cada vez maior na vida diária. Hoje em dia nossas chamadas telefônicas saltam entre satélites e nossos e-mails passam por vários computadores. Ambas as formas de comunicação podem ser interceptadas facilmente, ameaçando nossa privacidade.

De modo semelhante, à medida que mais negócios são realizados através da Internet, devem ser instalados mecanismos de proteção para a segurança das empresas e seus clientes. A codificação é o único meio de proteger nossa privacidade e garantir o sucesso do mercado digital. A arte da comunicação secreta, também conhecida como criptografia, fornecerá os fechos e as chaves da Era da Informação.

ANÁLISE DE RESULTADO

Entretanto, a crescente busca do público pela a criptografia entra em conflito com as necessidades da manutenção da lei e da segurança nacional. Durante décadas os serviços policiais e de espionagem têm usado a escuta telefônica para reunir provas contra terroristas e grupos do crime organizado, mas o desenvolvimento recente de códigos ultra-resistentes ameaça enfraquecer o valor dos grampos. À medida que entramos no século XXI, os defensores das liberdades civis começam a pressionar pelo uso generalizado da criptografia de modo a proteger a privacidade dos indivíduos. Ao lado deles fica a comunidade dos negócios, que precisa de uma criptografia forte para proteger suas transações no mundo em rápido crescimento do comércio via Internet. Ao mesmo tempo, as forças da lei pedem um uso mais restrito da criptografia. A questão se resume em, o que é mais valioso para nós, nossa privacidade ou uma força policial mais eficiente? Ou será que existe um meio termo?

De acordo com Oliveira (2000), a criptografia é uma das melhores formas de segurança de dados, é uma possibilidade que não deve ser esquecida, principalmente se quisermos trabalhar com dados confidenciais e envio de mensagens via Internet/Internet.

“A criptografia é uma arte: a arte de escrever ocultamente. Talvez tão antiga quanto à própria escrita, hoje é um método mais eficiente de se transferir informações, sem que haja a possibilidade de comprometimento do sigilo”.

Os Hackers têm grandes conhecimentos de criptografia, pois necessitam conhecer para invadir sistemas e conseguir senhas. Vamos dar nossos primeiros passos em criptografia de dados.

As redes hoje transportam cada vez mais informações vitais para organizações, empresas e até mesmo para o governo. A criptografia está hoje, mais do que nunca, ligada à segurança de dados, já que a segurança está se tornando um problema crítico.

A criptografia, segundo Oliveira (2000), vem do grego, Kriptos=escondido oculto + grafia, é a arte ou ciência de escrever em cifra ou em códigos, é então um conjunto de técnicas que tornam uma mensagem incompreensível permitindo apenas que o destinatário que conhece a chave de encriptação consiga decifrar e ler a mensagem com clareza. Agora existem pessoas que por meios ilícitos podem ter acesso à mensagem cifrada e determinar a chave de encriptação, estes se chamam criptoanalistas que não fazem nada mais que a decomposição da mensagem sem conhecer a chave quebrando o sistema.

A segurança de uma criptografia de um criposistema não pode estar baseada nos algoritmos de codificação e decodificação, mas sim em um valor da chave. Este mecanismo deve ser tão seguro que mesmo o autor de um algoritmo não seja capaz de decodificar a mensagem se não possuir a chave. Podemos dizer então que um bom criptoanalista conhece todo o sistema com exceção das chaves que foram utilizadas. Esta, conhecida como a premissa de “Kerckoffs”. Para um algoritmo ser analisado do ponto de vista de robustez a ataques, são assumidas as seguintes premissas.

- O criptoanalista tem acesso à descrição completa do algoritmo;
- O criptoanalista tem acesso a grandes volumes de mensagens originais e suas mensagens cifradas correspondentes;
- criptoanalista é capaz de escolher quais mensagens serão cifradas e receber as mensagens cifradas correspondentes;

Por sigilo da informação, entende-se que somente os usuários autorizados tenham acesso à informação.

Os algoritmos criptográficos segundo Oliveira (2000), são funções matemáticas usadas para codificar os dados, garantindo segredo e autenticação. Os algoritmos devem ser conhecidos e testados, e a segurança reside totalmente na chave secreta, esta chave numérica deve ter tamanho suficiente para evitar sua descoberta por teste exaustivo, os esquemas criptográficos são classificados em Simétricos e Assimétricos. Cada esquema tem vantagens e desvantagens.

Os criptográficos Simétricos , como o DES, usam a mesma chave para encriptar e decriptar.

Os criptográficos Assimétricos:

- Usam duas chaves diferentes, porém associadas;
- O par de chaves pertence a uma pessoa ou entidade, e é calculado a partir de um número aleatório;
- Uma das chaves, a Chave Secreta, deve ficar de posse e uso apenas de seu dono, dela pode ser calculada a outra, mas o processo não pode ser revertido- a função é unidirecional, portanto a segunda chave pode ser revelada, sendo então denominada Chave Pública, uma pessoa ou entidade é identificada pela sua Chave Pública, par de sua Chave Secreta;
- O algoritmo mais conhecido e usado é o RSA.
- Algoritmos de encriptografia são chamados de "cifras".
- Existem cifras e conjuntos ou sistemas de cifras que formam uma " infra-estrutura de segurança
- Uma infra-estrutura de segurança é todo um sistema de codificação, regras, gestão de políticas de segurança de informação numa empresa, inter-empresas e ou sistemas (como um sistema bancário).
- Os problemas que um sistema moderno de encriptografia tente resolver (num sistema de informação - Rede, Internet etc.) são:
 - Confidencialidade: A mensagem enviada de A para B não pode ser lida por ninguém mais.
 - Autenticidade: B pode acreditar que somente A poderia ter enviado a mensagem que B recebeu.

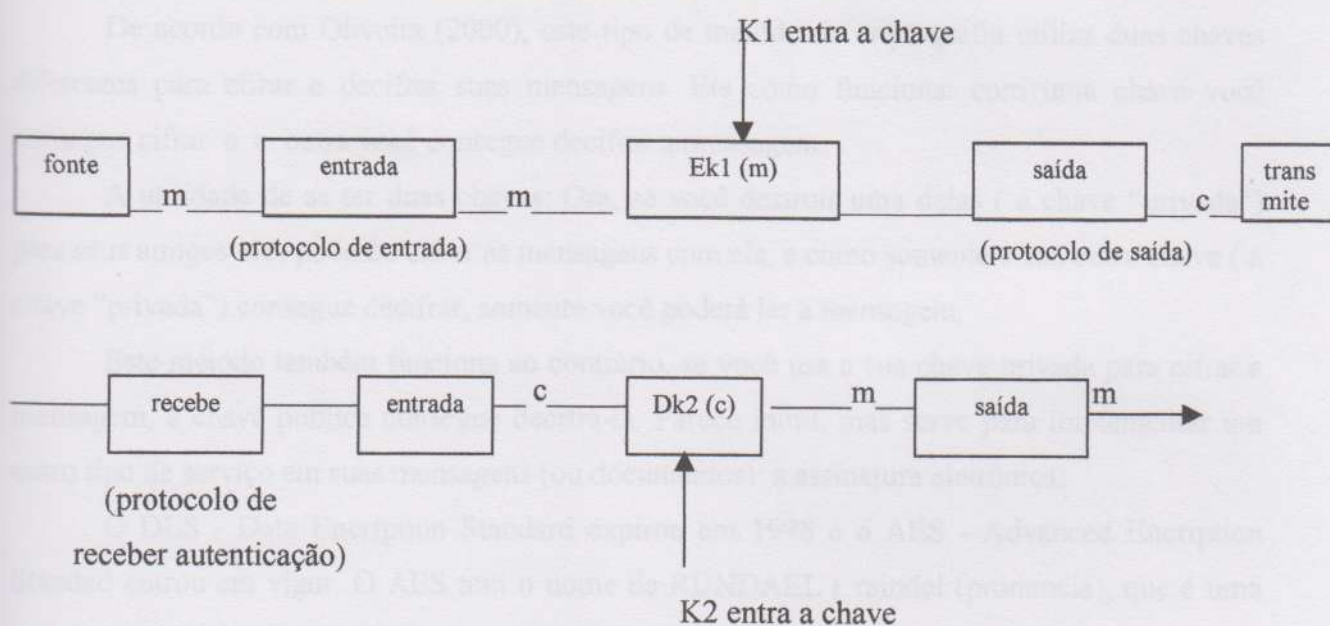
- Integridade : B pode acreditar que a mensagem que ele recebeu de A não foi modificada durante o transito.

- Não - Repudição : É impossível para A mais tarde dizer que ele não enviou a mensagem (repudição) .

Descrição geral de um sistema de encriptografia.

- a) mensagem : m
- b) chave : K
- c) função de encriptação: $E_k(m) = c$ ler-se, e-de-k encripta m e c é o texto cifrado codificado.
- d) Função de -criptação : $D_k(c) = m$ ler-se, d-de-k decripta c (o texto encriptado) e recupera m , a mensagem.

Descrição do sistema geral de encriptação usando um diagrama de blocos.



Chave privada : $K1 = K2$

Chave pública: $K1, \neq K2$

$K1$ é pública e $K2$ é secreta

Segundo Cormen, et al. (2001), o fator segurança e proteção de bancos de dados é de tal importância que a própria evolução do uso de cartões de crédito via compras na Internet é

limitada pela falta de confiança do público na privacidade do sistema. Daí, o uso de cartões com "CHIPS" ou "SMART CARDS" já estão sendo testados para dar maior segurança.

Na indústria e em outras instalações comerciais, muitas vezes é importante alocar recursos escassos da maneira mais benéfica. Uma empresa petrolífera talvez deseje saber onde localizar seus poços para tornar máximo o lucro esperado. Um candidato à presidência da República talvez queira determinar onde gastar dinheiro em publicidade de campanha com a finalidade de ampliar as chances de vencer a eleição. Uma empresa de transporte aéreo pode designar as tripulações para os vôos da forma menos dispendiosa possível, certificando-se de que cada vôo será atendido e que regulamentações do governo relativas à escala das tripulações serão obedecidas. Um provedor de serviços da Internet talvez queira definir onde instalar recursos adicionais para servir de modo mais eficiente a seus clientes.

3.2 CRIPTOGRAFIA DE CHAVE PÚBLICA E PRIVADA

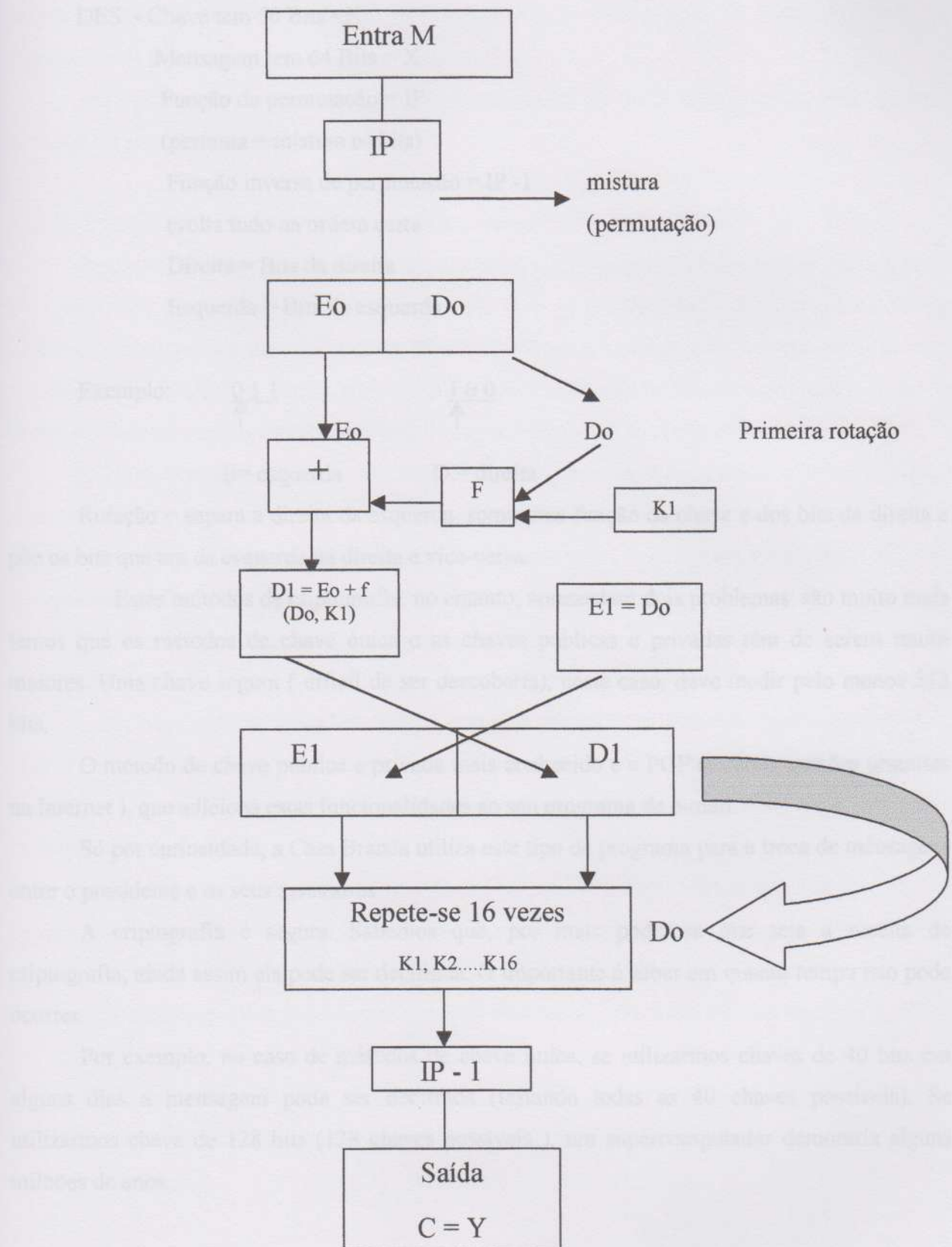
De acordo com Oliveira (2000), este tipo de método de criptografia utiliza duas chaves diferentes para cifrar e decifrar suas mensagens. Eis como funciona: com uma chave você consegue cifrar e a outra você consegue decifrar a mensagem.

A utilidade de se ter duas chaves: Ora, se você destruir uma delas (a chave "privada") para seus amigos eles poderão cifrar as mensagens com ela, e como somente a sua outra chave (a chave "privada") consegue decifrar, somente você poderá ler a mensagem.

Este método também funciona ao contrário, se você usa a sua chave privada para cifrar a mensagem, a chave pública consegue decifrá-la. Parece inútil, mas serve para implementar um outro tipo de serviço em suas mensagens (ou documentos): a assinatura eletrônica.

O DES - Data Encryption Standard expirou em 1998 e o AES - Advanced Encryption Standard entrou em vigor. O AES tem o nome de RIJNDAEL (raindel (pronuncia), que é uma concatenação dos nomes dos inventores dinamarquês.

Explicação com o diagrama do DES.



DES - Chave tem 56 Bits = K

Mensagem tem 64 Bits = X

Função de permutação = IP

(permuta = mistura os bits)

Função inversa de permutação = IP⁻¹

(volta tudo na ordem certa)

Direita = Bits da direita

Esquerda = Bits da esquerda

Exemplo: $\begin{array}{ccc} 0 & 1 & 1 \\ \uparrow & & \uparrow \end{array}$ $\begin{array}{ccc} 1 & 0 & 0 \\ \uparrow & & \uparrow \end{array}$

E = esquerda

D = direita

Rotação = separa a direita da esquerda, soma uma função da chave e dos bits da direita e põe os bits que era da esquerda na direita e vice-versa.

Estes métodos de criptografia, no entanto, apresentam dois problemas: são muito mais lentos que os métodos de chave única e as chaves públicas e privadas têm de serem muito maiores. Uma chave segura (difícil de ser descoberta), neste caso, deve medir pelo menos 512 bits.

O método de chave pública e privada mais conhecido é o PGP (existem versões gratuitas na Internet), que adiciona estas funcionalidades ao seu programa de e-mail.

Só por curiosidade, a Casa Branca utiliza este tipo de programa para a troca de mensagens entre o presidente e os seus assessores.

A criptografia é segura. Sabemos que, por mais poderosa que seja a receita de criptografia, ainda assim ela pode ser decifrada. O importante é saber em quanto tempo isto pode ocorrer.

Por exemplo, no caso de métodos de chave única, se utilizarmos chaves de 40 bits em alguns dias a mensagem pode ser decifrada (testando todas as 40 chaves possíveis). Se utilizarmos chave de 128 bits (128 chaves possíveis), um supercomputador demoraria alguns milhões de anos.

Este é o caso de se testar todas as chaves possíveis e, é claro que podem existir falhas na receita da criptografia. As que estão no mercado foram bem testadas e a complexidade de algumas delas garantem a segurança do método.

Normalmente, as quebras das chaves são realizadas por força bruta mesmo, testando uma por uma até descobrir a chave utilizada.

3.3 CRIPTOGRAFIA DE CHAVE PÚBLICA (RSA)

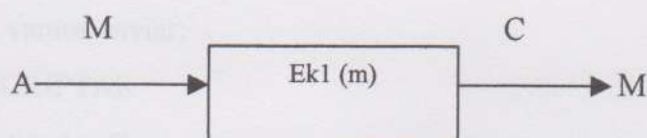
Segundo Cormen, et.ed. (2001), o sistema de Criptografia de chave pública (RSA), pode ser usado: um número inteiro maior do que um ($i > 1$) é chamado de número primo se for divisível apenas por ele mesmo ou pelo número 1. Desta simples propriedade nasceu toda uma infra-estrutura de codificar mensagens na era digital. E, a área da informática que estuda o uso de códigos e defesas contra ataques á códigos de segurança chama-se criptografia.

Cada código tem uma chave secreta (CS) mas, se esta chave fosse distribuída a todos que usam um sistema (por exemplo em banco) uma vez que a chave fosse descoberta, todas as contas estariam em perigo todas as senhas, todos procedimentos enfim, o banco estaria aberto ao usuário que quisesse utilizar do banco para fins desonestos.

Da mesma forma, é qualquer banco de dados ou arquivo espalhados pela Internet. A melhor maneira seria o uso de um código que constitui-se de duas chaves: uma secreta, e uma pública. A chave pública podia ser dada a qualquer pessoa, mas a secreta ficaria nas mãos de apenas uma. Este sistema existe e é usado em toda comunicação digital entre bancos , companhias, governo etc. Este é o sistema de infra-estrutura de Chaves Públicas (Public Key Infra-Structure)

Da maneira mais simples, a criação de chaves para o sistema RSA é utilizado a propriedade de que os números primos não são fatoráveis (apenas por ele mesmo ou o número 1). Daí, se dois números primos, p e q foram multiplicados, o produto seria um número primo enorme que mesmo um computador muito rápido não conseguiria fatorizar. Um número, p , pode ser a "chave pública" e o número q , a "chave secreta".

O funcionamento do RSA - R. Rivest, A. Shamir, L. Adleman. Três estudantes de pós-graduação do NIT, publicou e patenteou em 1978.



Ler-se, A quer enviar uma mensagem M para B, A usa o sistema RSA com chave pública K1. A chave pública é publicada na Internet, pois assim todo mundo sabe o que é. A mensagem codificada é C. M e C são números inteiros representando letras do alfabeto. A substituição da letra por um número já é uma cifra, mas é ridiculamente fácil de quebrar usando um computador, por isso não é considerada.

Exemplo: $p = 29$
 $Q = 67$
 $N = p \text{ e } q = 1943$
 $(n) = (p-1) \times (q-1) = 28 \times 66 = 1848$

Exemplo: Mandar uma mensagem, codificação do alfabeto (26).

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16
R	S	T	U	V	W	X	Y	Z								
17	18	19	20	21	23	24	25	26								

De 00 a 25 = 26 letras

- Acha-se d usando $1 = exd + \phi(n) \times$
- Coloque um e aleatório $e = 701$ por exemplo

Daí $d = 29$ ($e \times x = -11$)

$M = \text{exames} = \{04, 23, 00, 12, 04, 18\}$

(no computador estes números são representados em ASCII – Binários).

Agora vamos enviar:

⇒ ENCRIPITAR

$$E_{k1}(m) = C$$

$K1 = (n, e) \rightarrow$ chave pública

$$E(n, e)[m] \equiv (m \cdot e \pmod n)$$

$$m \quad m \text{ numerico} \quad c \equiv m \cdot e \pmod n = m \cdot 701 \pmod{1943}$$

$$E \quad 04 \quad 4701 \equiv 613 \pmod{1943}$$

$$X \quad 23 \quad 23 \cdot 701 \equiv 458 \pmod{1943}$$

$$A \quad 00 \quad 0701 \equiv 0 \pmod{1943}$$

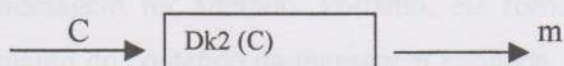
$$M \quad 12 \quad 12701 \equiv 1926 \pmod{1943}$$

$$E \quad 04 \quad 613 \pmod{1943}$$

$$S \quad 18 \quad 18701 \equiv 1439 \pmod{1943}$$

Veja : $C = \{613, 458, 0, 1926, 613, 1439\}$

TRANSMITE-SE C (quando chega do outro lado, em B, B decifra)



$K2 = d$ -----chave privada (secreta)

$$D_d(C) = C \cdot d \pmod n, \quad d = 29$$

C	$M = C \cdot d \pmod n$	Mnum.	M
613	$613 \cdot 29 \pmod{1943} = 04$	04	E
458	$458 \cdot 29 \pmod{1943} = 23$	23	X
0	$0 \cdot 29 \pmod{1943} = 0$	0	A
1926	$1926 \cdot 29 \pmod{1943} = 12$	12	M
613	$613 \cdot 29 \pmod{1943} = 04$	04	E
1439	$1439 \cdot 29 \pmod{1943} = 18$	18	S

Como funciona:

- O racke tem que achar p e q fatorizando (achando os multiplicandos p e q), mas como são primos, p e q s'õ são divisíveis por eles mesmos.
- Como d depende de $\phi(n)$, isto é, de p e q , uma vez que $\phi(n) = (p-1)(q-1)$ não há como se sabe de d .
- Ainda por cima, E é aleatório $\rightarrow$ por exemplo um para cada usuário do sistema.
- $\rightarrow$ daí, chave pública $K_1 = (e, n)$
- $\rightarrow$ chave secreta, d .
- Qualquer computador já tem a função módulo na sua linguagem (Ex. c++).

Um sistema de criptografia de chave pública pode ser usado para codificar mensagens enviadas entre dois participantes de uma comunicação, de forma que um intruso que escute as mensagens codificadas não possa decodificá-las. Um sistema de criptografia de chave pública também permite que um dos participantes acrescente uma "assinatura digital" impossível de forjar ao final de uma mensagem eletrônica. Tal assinatura é a versão eletrônica de uma assinatura manuscrita em um documento de papel, pode ser conferida com facilidade por qualquer pessoa, não pode ser forjada por ninguém, e ainda perde sua validade se qualquer bit da mensagem for alterado. Portanto, ela fornece autenticação, tanto da identidade do signatário quanto do conteúdo da mensagem assinada. É a ferramenta perfeita para assinar eletronicamente contratos de negócios, cheques eletrônicos, pedidos eletrônicos de compras e outras comunicações eletrônicas que devam ser autenticadas.

4. CONCLUSÃO

Este trabalho mostrou que privacidade e segurança no comércio eletrônico são dois temas que caminham juntos, são complementares e necessários para garantir um bom funcionamento das transações na Internet.

No mundo atual, o investimento com segurança é oneroso e tem mudado. Os Softwares de segurança deixaram de ser meros acessórios e passaram a integrar à necessidade básica, principalmente das empresas.

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 possa ser utilizada como meio para realização de transações financeiras e comerciais em um mundo globalizado. O usuário precisa se sentir seguro e ficar tranquilo com relação aos aspectos de privacidade para que as transações possam ocorrer de forma mais maciça.

5. REFERÊNCIA BIBLIOGRÁFICA

ALBERTIN, Alberto Luiz, **Comercio Eletrônico: Modelo, aspectos e contribuições de sua aplicação**. 2.ed. - São Paulo: Atlas, 2000.

BERNSTEIN, Teery. **Segurança na Internet**: Rio de Janeiro: Editora Campos Ltda., 1997.

CARUSO, C.; STEFFEN, F.; D. **Segurança em Informática e de Informações 1998**.

HUTT, ^a, E.; BOWORTH, S.; HOYT, D., B. **Computer security handbook**. 3.Ed. New York John Wiley & Sons Inc, 1995.

H.Cormen Thomas, **Algoritmos Teorias e Praticas** et at; tradução da segunda edição (americana) Vandenberg D. de Souza – Rio de Janeiro: Campus, 2002.

NAKAMURA, Rodolfo, **E-Commerce na Internet**: Fácil de entender. São Paulo: Editora Érica, 2001.

O'BRIEN, James **Sistemas de Informação e as decisões gerenciais na era da Internet**. São Paulo: Editora saraiva, 2001.

PENTEADO, S. De olho na segurança. **Information Week**. Nº 6, julho/1999, pag. 26-34.

RÔÇAS, C. Credibilidade em cheque. **Internet Business**. nº 32, Abril 2000, pag. 48-55.

SINGH, Simon **O Livro dos Códigos**. São Paulo: Editora Campos, 2001.

SARTORI R. ; Tubino D. F. ; PEREIRA, M. F. Utilização da Internet pelas empresas de Maringá sob a ótica de web sites. In: ENCONTRO DA ASSOCIAÇÃO DOS PROGRAMAS DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO, 26. , 2002, Salvador. *Anais...* Rio de Janeiro: ANPAD, 2002.

TANENBAUM, ^a, S. **Rede de Computadores**. Rio de Janeiro, Campus, 1997.

OLIVEIRA, Wilson, José. **Tecnologia e Segurança (WAP) e Segurança da informação: Técnicas e soluções**. Florianopolis –SC: Editora Visual Books, 2000.

ZANINI, A., S. **Proposta e Implementação Controle de Acesso a Informações e ambiente de Microinformatica**. São José dos Campos , 1999. Tese (Doutorado) – Instituto Tecnológico de Aeronáutica.