FACULDADE DE TECNOLOGIA DE SÃO PAULO

André Massami Nakamura

COMÉRCIO ELETRÔNICO RISCOS NAS COMPRAS PELA INTERNET

SÃO PAULO
2011

FACULDADE DE TECNOLOGIA DE SÃO PAULO

André Massami Nakamura

COMÉRCIO ELETRÔNICO RISCOS NAS COMPRAS PELA INTERNET

Monografia submetida como exigência
parcial para a obtenção do Grau de
Tecnólogo em Processamento de Dados
Orientador: Prof. Irineu Francisco de Aguiar

SÃO PAULO
2011

Dedico este trabalho a minha família e aos meus amigos.

Agradeço ao Orientador Professor Irineu Francisco de Aguiar, pela atenção e dedicação na elaboração e correções do trabalho.

Resumo

Atualmente o mercado de negócios mundial tem sofrido mudanças significativas, por influência do grande desenvolvimento da Tecnologia e dos meios de transmissão das informações. Diante desse novo cenário comercial, o Comércio Eletrônico surgiu com a inovação nos processos de negócio em vários setores econômicos.

Grandes possibilidades de atingir milhões de empresas e consumidores de forma consideravelmente barata tem interessado pessoas físicas e jurídicas a investir no Comércio Eletrônico, buscando um retorno nos investimentos aplicados.

Comércio Eletrônico já é uma realidade, uma nova forma de realizar negócios, de usar a tecnologia e de construir empresas.

Neste trabalho tem por objetivo tratar dos principais assuntos referentes ao Comércio Eletrônico como: o conceito, segurança e as tendências para o futuro do Comércio Eletrônico.

Palavras-chave: comércio eletrônico. internet. segurança. tecnologia.

Abstract

Currently, the global business market has undergone significant changes, influenced by the great development of technology and the means of transmission.

Great possibilities to reach millions of businesses and consumers have so considerably cheaper interested individuals and companies to invest in E-Commerce, seeking a return on the investments made.

E-commerce is already a reality, a new way of doing business, to use technology and building companies.

This work aims to address key issues relating to electronic commerce such as the concept, security and trends for the future of Electronic Commerce.

Keywords: e-commerce. the internet. security. technology.

Lista de Ilustrações

Lista de Abreviaturas e Siglas

B2B - Business to Business

B2C – Business to consumer

DES - Data Encryption Standard

DLL – Dynamic link library

DNS - Domain Name System

E-commerce – Comércio Eletrônico

G2B - Government to Business

G2C - Government to Citizen

HTML - HyperText Markup Language

IDEA - International Data Encryption Algorithm

ISO - International Organization for Standardization

NCP - Network Control Protocol

NCSA - Centro Nacional para Aplicações de Supercomputação

PGP - Pretty Good Privacy

PSN - Playstation Network

RC - Ron´s Code ou Rivest Cipher

RSA - Rivest, Shamir and Adleman

SET - Transação Eletrônica Segura

S-http - Secure Hyper Text Transfer Protocol

SSL - Secure Socket Layer

SSL - Secure Sockets Layer

TCP/IP - Transfer Control Protocol/ Internet Protocol

URL - Uniform Resource Locator

SUMÁRIO

1.Introdução

Nos últimos anos, o ambiente empresarial tem sofrido grandes mudanças, tanto na visão nacional como mundial. Essas mudanças estão diretamente ligadas ao grande desenvolvimento da tecnologia da informação. Envolvendo o surgimento de novas tecnologias e da criação de aplicações utilizadas para atender as necessidades das empresas.

Atualmente as características predominantes no novo mundo empresarial são a globalização, integração interna e externa das empresas, a grande concorrência, necessidades de operações em tempo real, orientação a clientes, excesso de informação, responsabilidade social, regulamentação governamental e entre outras. Com essa nova tendência de mercado, o Comercio Eletrônico surgiu como novo modelo de negócio.

Esse novo modelo proporciona mecanismos para automatizar as vendas eletrônicas, gerenciar suprimentos e estoques, a logística e cobrança que são acompanhadas através da Internet.

O Comércio Eletrônico já é uma realidade para muitas empresas nacionais e internacionais. Grandes possibilidades de realizar compras, pesquisar preços, conhecer as características dos produtos oferecidos, realizarem serviços bancários entre outros benefícios proporcionados, realizar tudo isso sem sair de casa ou da empresa e a qualquer hora do dia, é o grande responsável pelo crescimento desse segmento.

No entanto o grande desafio que o Comercio Eletrônico tem enfrentado é a preocupação dos usuários em relação à segurança.

As transações através da internet quando são realizadas, provocam inúmeras conseqüências principalmente na questão da segurança dos negócios.

A grande preocupação é com a validade dos documentos digitais e o iminente risco da sua manipulação, como conseqüência a utilização da tecnologia de segurança torna-se cada vez mais importante, visando aumentar a confiabilidade.

Os meios de comunicação ultimamente têm noticiado, freqüentes invasões de hackers a sites de empresas de grande renome mundial.

Sites importantes como do governo federal e da Playstation Network (PSN) ficaram indisponíveis por um longo período devido às terríveis invasões dos hackers, onde vários dados pessoais dos usuários cadastrados foram obtidos .

Revelando o quanto é vulnerável a Internet, mesmo se tratando de sites conhecidos e de empresas tradicionais.

Isso causa uma imagem negativa do Comércio Eletrônico, pois muitos internautas deixaram de efetuar a compra eletrônica, devido à desconfiança e o receio de sofrer prejuízos.

Apesar da ampla divulgação das freqüentes invasões do ambiente virtual, aqui no Brasil , o Comércio Eletrônico ainda não possui uma regulamentação legal, o único amparo ao consumidor se restringe a norma do Código de Defesa e Proteção do Consumidor.

2. Histórico do Comércio Eletrônico

Tudo começou com desenvolvimento da Internet, épocas passadas durante a Guerra Fria a comunicação entre bases militares americanas era feita atrás de uma rede chamada ArpaNet.

Desenvolvida pela empresa ARPA em 1969, com intuito de interligar os departamentos de pesquisa, tinha como principalmente objetivo diminuir a vulnerabilidade da comunicação.

Disponibilizava um Back Bone que utilizava o espaço subterrâneo, dificultando a interrupção da comunicação, conectava os militares e pesquisadores, sem ter um centro pré determinado, tornando confiável.

Por volta da década de 70, as universidades e outras comunidades que faziam atividades referentes à defesa tiveram permissão para acessar à ARPANET. Em 1975, constatou-se a existência de 100 sites. A grande preocupação dos pesquisadores era como manter a comunicação entre computadores sem que houvesse interrupção.

No final da década de 70, a ARPANET tinha se expandido com tamanha proporção, que seu protocolo de comutação de pacotes originais chamados Network Control Protocol (NCP), tornou-se insuficiente. O Sistema de comutação de pacotes funciona dividindo os dados em pequenas partes, onde elas são identificadas da forma a mostrar de onde vem e para onde vai. Então são enviados esses pacotes de um computador para outro.

Após algumas pesquisas realizadas, a ARPANET modificou NCP para novo protocolo com nome de Transfer Control Protocol/ Internet Protocol (TCP/IP) criada pela Unix.

A característica do TCP/IP era de permitir crescimento ilimitado da rede, com fácil implementação em diferentes plataformas do computador.

Em 1979, inventor inglês chamado Michael Aldrich inventou as compras online. A invenção foi feita utilizando uma televisão personalizada de 26 polegadas para um computador doméstico, onde possuía um real sistema de processamento de tempo de transação através da linha telefônica.

Por volta dos anos de 1980, as diversas formas de Comercio Eletrônico como cartão de crédito, caixas automáticos e bancários via telefone foram bem aceitos e desenvolvidos.

Outros sistemas considerados como e-commerce foram reservas da Airline tipificado por Savre nos Estados Unidos e a Travicom no Reino Unido.

Durante essa década de 1980, a CompuServe disponibilizava os primeiros serviços a usuários domésticos de PC, oferecia ferramentas como e-mail, painéis de mensagens e sala de bate-papo, adicionando serviço chamado Eletronic Mall.

Esse novo serviço funcionava como shopping virtual, onde usuários podiam comprar produtos diretamente do formulário de 110 comerciantes online. Tratava-se de um dos primeiros exemplos de Comércio Eletrônico.

Em 1990, o pesquisador Tim Berners-Lee da Organização Européia para Pesquisa Nuclear (CERN), propôs um hipertexto onde informações da internet poderiam ser usufruídas pelos usuários de modo dinâmico e rápido, com uma interface simples chamada navegador. O pesquisador nomeou como World Wide Web.

Em 1993, Marc Andresen desenvolveu o primeiro web browser grande expandido chamado Mosaico no Centro Nacional para Aplicações de Supercomputação (NCSA).

Por volta de 1994, surgiu o Netscape 1.0 com Secure Socket Layer (SSL), trata-se de um protocolo de segurança que criptografa mensagens em uma transação via internet, essa ferramenta é utilizada tanto no envio como no recebimento.

O SSL tem como principal função de garantir a segurança das informações pessoais como nome, endereço e numero de cartão de credito através da criptografia.

Durante ano de 1995, empresas como eBay e Amazon.com iniciaram o caminho de sucesso do Comércio Eletrônico. Oferecem aos consumidores a opção de realizar a compra de qualquer produto. Onde o consumidor poderia realizar a busca do produto, em questão de segundos apareceria uma lista dos produtos relacionados.

Hoje em dia com Internet desenvolvida, os sites de compras online expandiram significativamente, os produtos agora são solicitados via web, pagos no ambiente virtual mesmo, entrega é feita através do serviço postal ou serviço de entrega comercial.

Conforme dados da Fecomercio-SP, o Brasil hoje contabiliza 80 milhões de usuários da Internet, sendo que desses 27 milhões são consumidores da compra online. O valor médio do ticket de compra no país subiu para R$ 350, está entre os maiores do mundo. Estimativa que em 2011 o numero de usuários compradores online cresce para 32 milhões, fazendo uma comparação com ano de 2009 o número de consumidores dobrou.

O mercado virtual está com grande expectativa de crescimento, considerado como promissor, mas uma das barreiras constatada foi à elevada tributação. (Editora Abril, 2011)

3. Conceito do Comercio Eletrônico

Comércio eletrônico trata-se de todos os processos envolvidos da cadeia de valor realizada num ambiente eletrônico, utilizando de ferramentas com grande tecnologia de informação e de comunicação, tendo como principal objetivo atender as necessidades exigidas pelos negócios. Pode-se realizar de forma completa ou parcialmente, caracterizando por transações negócio a negócio, negócio a consumidor, intra-organizacional, com fácil e livre acesso.

Para Rogério de Andrade o conceito de comércio eletrônico define-se como:

> O Comércio Eletrônico é a aplicação de tecnologias de comunicação e informação compartilhadas entre as empresas, procurando atingir seus objetivos. No mundo dos negócios, quatro tipos diferentes de comércio eletrônico se combinam e interagem.(Andrade, 2001, p.13)

Já para Rob Smith o Comércio Eletrônico trata-se de:

> Negócios conduzidos exclusivamente através de um formato eletrônico. Sistemas que se comunicam eletronicamente uns com os outros são sistemas de e-commerce, e têm de ser capazes de funcionar normalmente com quaisquer aplicações da Internet que estiver planejando utilizar. Também se refere a quaisquer funções eletrônicas que auxiliam uma empresa na condução de seus negócios.”(Smith, 2000, p.74)

Ou ainda pode-se definir Comércio Eletrônico como a compra e venda de produtos, informações e serviços através da rede mundial de computadores.

A figura a seguir apresenta um modelo básico do Comércio Eletrônico. Retrata todas as fases de uma compra eletrônica, numa visão de comprador-vendedor .

Fonte: Albertin, Alberto Luiz

Figura 1 - Modelo de Comércio Eletrônico

O Comércio Eletrônico trouxe as empresa ferramentas com novas tecnologias, para realizar negócios eletronicamente com maior eficiência, rapidez e menor custo.

Para um negócio tornar-se bem sucedido, é de extrema importância saber utilizar da maneira adequada à tecnologia disponível no mercado e também que seja apropriada aos consumidores do mercado extenso.

4. Tipos de Comércio Eletrônico

4.1 Negócio-Negócio - Business to Business (B2B)

Comércio praticado pelos fornecedores e empresas, ou seja de empresa para empresa. Onde é feito operações de compra e venda de produtos, informações e serviços por meio da web ou utilizando redes privadas partilhadas entre as empresa. Substituindo o tradicional comercio físico nas lojas e estabelecimentos comerciais.

Podemos considerar também B2B como troca de informações estruturadas com parceiros de negócios através de redes privadas ou pela web afim de manter um relacionamento efetivo entre os parceiros de negócios.

Esse tipo de comércio necessita atingir patamares de eficiência diferenciados. Com a globalização, diversos desafios são impostos ao Comércio Eletrônico, então as empresas necessitam de um processo eficaz e eficiente que atendam as expectativas dos negócios, comprar e vender de forma econômica e eficaz.

Podem-se citar três grupos principais de portais do B2B são:

Portal para colaborador (Intranet), trata-se do portal utilizado para comunicação interna da empresa. Esse tipo de portal é exclusivo aos colaboradores da instituição e ao grupo das empresas, disponibilizando o acesso a uma variedade de recursos da rede interna. Através dessa ferramenta, podemos manter a comunicação entre os colaboradores, sem importa com local físico onde se encontram, distância não será empecilho para manter a comunicação entre os colaboradores.

Portal para parceiro (Extranet), foi criado para manter relacionamento entre as empresas B2B, trata-se de uma rede que liga a empresa aos seus parceiros de negócios, com objetivo de incentivar a colaboração e compartilhamento de informação.

Portal de terceiros, define-se como uma intermediação entre varias instituições de compradores e vendedores. Negociação de mercadorias e serviços através da Internet, facilitando e incentivando a compra online.

Em 2005, segundo revista InfoExame, foi movimentado 67 bilhões de dólares no mercado eletrônico brasileiro. Apenas a Petrobrás foi responsável por 45 bilhões de dólares com B2B. (Mendes, 2011)

4.2 Negócio-Consumidor - Business to Consumer (B2C)

Comercio realizado por empresas produtora, vendedora e prestadora de serviços com consumidor por meio da Internet.

As vantagens na utilização do B2C destacam-se na criação de lojas virtuais, onde poderá promover promoções de determinadas marcas, obtendo lucro por meio dos consumidores que usam freqüentemente a Internet.

A cada dia surgem novas tecnologias e ferramentas, favorecendo a criação de novas formas de comercializar os produtos.

Outra vantagem seria que a loja virtual comporta tanto a pequena empresa como também os grandes negócios.

Existem três tipos importantes de B2C são: leilões, lojas virtuais e serviços online.

Leilões oferecem uma licitação eletrônica, possibilidade de acompanhamento de uma apresentação da mercadoria.

As vantagens sugeridas para esse tipo de modelo é a conveniência, flexibilidade, acesso global e economia para realizar tal evento.

As grandes desvantagens apresentadas por essa atividade seria a falta de inspeção da mercadoria e grande chances de ocorre fraude durante o pagamento do produto leiloado.
Lojas online é o comércio de produtos utilizando a web. Podendo ser usada com a finalidade de promover os produtos e serviços da empresa ou realmente comercializar as mercadorias usando como ambiente a loja virtual.

As vantagens apresentadas aos clientes são de preços mais baixos, maior variedade de escolha dos produtos, melhor informação e descrição do produto, conveniência em comprar sem ter que se locomover a uma loja física.

Serviços online é disponibilização de serviços a clientes via web. Um dos bons exemplos seria no setor bancário e de ações comerciais. Objetivo dos serviços online é de praticidade, facilitar a realização das tarefas pelos clientes.

Os serviços online têm vários produtos disponíveis tais como transferência bancária, jornais, revistas e etc.

A grande preocupação do B2C está voltada para o sistema logístico, pois a entrega dos produtos adquiridos via Internet em ótimas condições e no prazo determinado são um dos

requisitos fundamentais no comércio eletrônico. Essa estruturação do sistema de logística é um fator determinante para o sucesso do empreendimento.

Segundo estudo realizado pela revista InfoExame, ano de 2005 foi movimentado pelas 50 maiores empresas de comércio eletrônico o equivalente de 3 bilhões. Só a empresa Gol linhas aéreas contribuiu com 1 bilhão. Bons exemplos de B2C é o site das lojas americanas e do submarino. (Mendes, 2011)

4.3 Consumidor –Consumidor

Comércio realizado entre usuários restritos a Internet, transação de bens e serviços apenas entre consumidores.

Trata-se da comercialização entre consumidores diretamente ou através de uma empresa intermediária. Bom exemplo desse tipo de comércio é o leilão online, como Ebay e Mercado Livre.

Os leiloes funcionam da seguinte maneira, o consumidor deixa disponível seu produto para venda com um valor mínimo estipulado, outros consumidores irão dar lances com valores maiores, depois que o tempo pré-determinado terminar , o maior lance até aquele momento ficará o produto.

4.4 Governo Consumidor - Government to Citizen (G2C)

Representa o comércio do governo ou outro órgão público com consumidor via web. Exemplo dessa atividade seria o pagamento de taxas de imposto, multas e tarifas através da Internet.

Sendo um portal do governo oferecendo orientação e serviços aos cidadãos, voltado para área desde serviços, educação e empregos.

Esse tipo de ferramenta proporciona ao cidadão o conhecimento, a informação e os serviços diversos disponíveis pelo governo.

4.5 Governo Negócio - Government to Business (G2B)

Trata-se de negócios realizados entre governo e as empresas utilização a Internet como meio de comunicação. Por exemplo compras realizadas pelo governo usando a web como pregões e licitações, tomada de preços, compra de fornecedores, etc.

5. Ambiente Virtual

Pode-se ser definido como teia mundial de redes de computadores e serviços de informação no ambiente digital. Tendo as pessoas à possibilidade de comunicação interativa, solicitar pedidos de compras e serviços, realizar transações de negócios com fornecedores, sem a necessidade de estar na mesma localização. (Albertin, 2000, p.36)

Existem dois tipos de produtos e serviços disponíveis na rede mundial para sempre utilizados são eles:

Produtos de forma padrão e homogênea, como exemplo temos discos de computadores e papel de impressora.

Outro tipo seria produtos customizados, um bom exemplo seria o sistema de software especializado.

O Ambiente virtual apresenta vários elementos envolvidos referentes ao custo são:

Custo da comunicação entre fornecedor e comprador;

Custo da elaboração da proposta de compra aos vendedores;

Avaliação do custo pelos compradores;

Custo interno de produção; e

Custo da organização interna.

A tecnologia da informação tem beneficiado os negócios, com a redução do tempo e o custo da comunicação. Entretanto a influência em outras partes do negócio ainda não foi possível detectar tais mudanças.

5.1 Infovia

Trata-se de conjuntos de linhas digitais por onde são transmitidos os dados na rede eletrônica. Foi desenvolvida a partir da idéia de criar uma rede descentralizada, mudando o conceito tradicional da rede com um computador centralizado.

Baseada no formato da Internet, a infovia a cada dia está –se tornando um sistema de redes de computadores com utilização da banda larga, realizando a transmissão de um grande

volume de textos, som, imagens e vídeos, internamente e externamente são feito o tráfego de dados das residências, empresas, escolas, hospitais e etc.(Albertin, 2000, p.37)

Constata-se que a infovia será utilizada para diversos setores da comunicação, informação, negócios, educação, entretenimento e aplicações para desenvolvimento social.

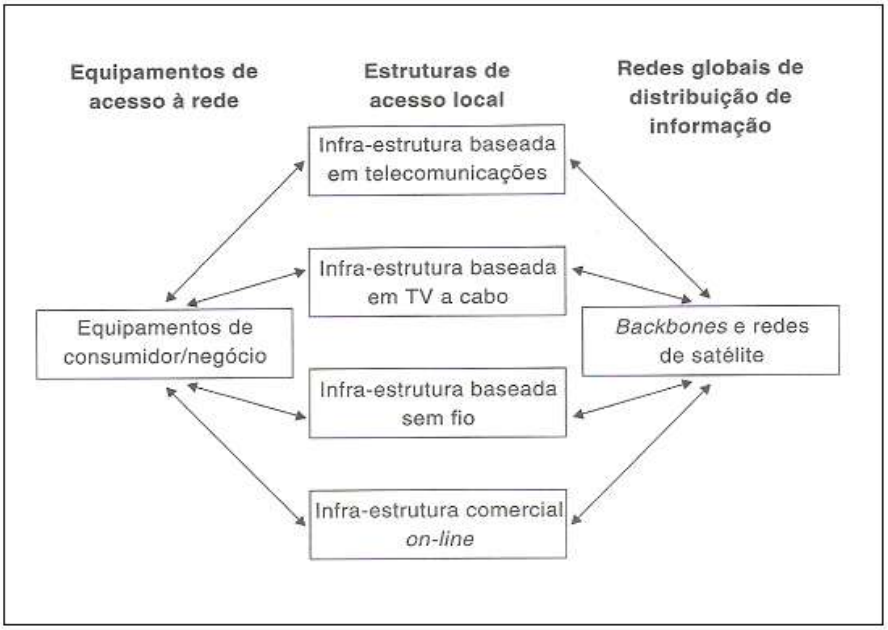
A infovia possui três elementos fundamentais para seu estabelecimento com relação à infra-estrutura, são eles:

Equipamentos de acesso à rede: nesse segmento podem-se destacar os vendedores de hardware e software, que disponibilizam de meios físicos como roteadores e switches e também de meios de acessos como computadores e televisão a cabo, além disso oferecem plataformas de software como software de navegação na Internet e sistemas operacionais.

Estrutura de acesso local: identifica-se como provedores de acesso a plataforma principal de comunicação ligando usuários e provedores de TI.

Redes globais de distribuição de informação: são representados pela infra-estrutura entre países e continentes. Onde a maior parte dessa estrutura está localizada na extensa rede de fibra óptica, cabos coaxiais, ondas de rádio e satélites.

Segue abaixo a estrutura da infovia:



Fonte: Albertin, Alberto Luiz

Figura 2 - Componente da Infra-estrutura da Infovia

5.2 Internet

Podemos definir como um conglomerado de redes com abrangência mundial entre milhões de computadores interligados pelo TCP/IP que possibilita o acesso a diversos tipos de informações através da transferência de dados. Disponibilizando uma variedade de recursos dentre elas estão o correio eletrônico, comunicação instantânea e o compartilhamento de arquivos.

Segundo (Albertin, 2000, p.40), a Internet é um dos principais componente da infra-estrutura da rede da infovia. Nos dias de hoje, a Internet é considerada como um sistema de distribuição de informações espalhadas por diversos países.

O ambiente da web é a junção do serviço postal, sistema de telecomunicação, pesquisa bibliográfica, Comércio Eletrônico, facilitando a interação entre as pessoas. A Internet é considerada como um protótipo da infovia emergente, tornando-se um componente.

5.3 Intranet e Extranet

O nome Intranet refere-se ao uso de tecnologias da Internet dentro da corporação, afim de melhorar a conectividade e a comunicação entre os funcionários. Usando sistemas de emails da rede local ou base de dados de acordo com as necessidades da organização. Isso significa que será disponibilizado um site Intranet com informações em tempo real facilitando as tarefas dos usuários. (Andrade, 2001, p.36)

Empresas implementam Intranets pelas seguintes razões:

Facilitar o trabalho em grupo na realização de projetos;

Reduzir Custos;

Melhorar o fluxo de informação;

Baixa manutenção;

Escalabilidade e fácil distribuição de software.

Podem-se destacar também algumas desvantagens por utilizar essa ferramenta seria:

Aplicações para intranets não são tão eficientes como as oferecidas por groupware tradicional;

Risco a curto prazo; e

Menor integração com o back-end.

Pode-se considerar Extranet a infra-estrutura que permite o acesso seletivo de consumidores e fornecedores ao site da Intranet da empresa. Onde o acesso é permitido apenas em algumas informações, requerendo medidas de segurança da informação para restringir acessos não autorizados e aplicativos e informações confidenciais. (Andrade, 2001, p.36)

Algumas ferramentas utilizadas para restringir acessos indevidos são:

Senha de acesso;

Roteador filtragem;

Autenticação;

Firewall, onde é feito o isolamento da rede local da Internet, bloqueado acessos indevidos.

5.4 World Wide Web

Trata-se de uma coleção de documentos partilhados, considerando como páginas, localizadas em computadores chamados de servidores. Onde ficam guardados arquivos em HyperText Markup Language (HTML) e respondem solicitações.

Para usar o World Wide Web é necessária uma conexão a Internet, além disso o usuário precisa de um software navegador para acessar essa página eletrônica.

Software navegador realiza a interface gráfica do usuário com a Internet, enviando comandos importantes para solicitar os dados do servidor e então formatar a tela que o usuário irá visualizar.

A partir do navegador, os usuários terão a chance de localizar e visualizar os documentos armazenados nos servidores. Esses softwares permitem o acesso fácil aos arquivos guardados nos servidores e à exibição de dados de multimídia. (Albertin, 2000, p.46)

5.5 Serviços Online

A Internet e o serviço online possuem grandes diferenças, dentre elas podemos destacar que a Internet está relacionada à área educacional e nos últimos tempos com o comércio eletrônico.

Já a indústria de serviços online está ligada ao consumo, operando com pouca percepção nos últimos anos.

6. Sistema Eletrônico de Pagamento

Pagamento eletrônico é qualquer pagamento que não utiliza dinheiro vivo ou cheque em formato de papel. Nada mais conveniente do que realizar um pagamento eletronicamente, onde tudo o que precisa é inserir alguns dados e confirmar via web.

Sistemas eletrônicos de pagamentos estão se tornando um fator importante para a evolução do processo do Comércio Eletrônico, quando as empresas procuram por soluções mais rápidas e com custo menor para oferecer aos consumidores.

Os sistemas de pagamentos eletrônicos de pagamentos estão divididos em : dinheiro eletrônico, cheque eletrônico, cartão inteligente, cartão de crédito e cartão de débito.

Essas formas de pagamentos estão diretamente ligadas ao comércio eletrônico, visto que os clientes online necessitam pagar pelos produtos e serviços adquiridos.

Os sistemas de pagamentos eletrônicos estão se expandindo em vários setores do mercado como rede bancária, varejo, área da saúde, mercado online e também no governo. O que motiva as empresas a procurarem por essa ferramenta, está na necessidade de entregar produtos e serviços a custo efetivo e com boa qualidade ao cliente, pois a satisfação do cliente é um detalhe relevante para alcançar o sucesso do negócio. (Albertin, 2000, p.154)

Um dos benefícios proporcionados pelo pagamento eletrônico é a conveniência oferecida ao consumidor. Onde é preciso entrar com os dados pessoais apenas uma única vez no sistema. Além disso, diminuem os custos as empresas deixando de gastar com papel e postagem. Tudo isso favorece a melhoria do negócio e também a manutenção dos clientes. Com grandes chances de o consumidor retornar ao site de negócios, por causa da comodidade de já estar cadastrado nesse ambiente.

6.1 Dinheiro Digital

Refere-se a transações realizadas eletronicamente com a finalidade de transferir fundos de uma parte para outra. Nada mais é do que outro valor corrente e as transações realizadas podem ser visualizados como uma troca de moeda no mercado estrangeiro. Antes de realizar qualquer transação é necessário disponibilizá-la de alguma forma.

Isso representa uma forma de alterar o sistema de pagamentos, surgindo novas moedas negociadas pelas empresas, sem esquecer das atribuições necessárias para realização do comércio como a segurança, confiabilidade e sigilo.

Dinheiro digital terá que refletir as principais características vistas pelos consumidores que são:

Anonimato - ao realizar uma compra a identidade do comprador e os detalhes da transação seriam confidencias, sendo apenas o vendedor ter o direito do conhecimento.

Liquidez - o dinheiro eletrônico teria que ser aceito por todos agentes econômicos como uma forma de pagamento.

O Dinheiro eletrônico pode ter vários tipo dentre eles estão cartões pré pagos e sistemas genuinamente eletrônicos:

Cartões pré pagos - Consumidores podem adquirir cartões pré pagos que são aceitos por vendedores especiais. Nos dias de hoje, um bom exemplo de cartão pré pago é o cartão telefônico, entretanto não possui a liquidez , ou seja, não são aceitos para compra de mercadorias. Outros cartões inteligentes com múltipla funcionalidades estão em fase de teste, onde também irá compor sua funcionalidade de dinheiro digital.

Sistemas genuinamente eletrônicos – trata-se do pagamento eletrônico sem a forma física explicita, são utilizadas em transações via Internet, onde o comprador e o vendedor estão em localidades remotas.

O pagamento funcionaria da seguinte maneira, seria feita a dedução eletrônica do dinheiro digital do comprador e transferido ao vendedor. Essa transferência costuma ser realizada acompanhada de um sistema de criptografia com chave pública ou privada, onde somente o receptor vendedor poderá utilizar do dinheiro digital.

O dinheiro eletrônico é uma novidade aos sistemas de pagamento online, pois forma uma união entre a conveniência computadorizada com segurança e privacidade.

Por ter versátil, novos mercados e ferramentas estão sendo desenvolvidos . O dinheiro eletrônico possui certas propriedades interessantes como:

Valor monetário;

Interoperabilidade;

Recuperabilidade;

Segurança.

A utilização do dinheiro eletrônico através do comércio eletrônico promove riscos que podem ser diminuídos utilizando limites durante a compra tais como:

Atribuir tempo de validade ao dinheiro eletrônico;

Monte de dinheiro digital pode ser armazenado ou transferido;

Limite do numero de trocas antes do dinheiro precise ser novamente depositado;

Número de transações permitidas durante um período.

Ao longo dos tempos, está pretendendo substituir o dinheiro tradicional , o de papel, pelo dinheiro eletrônico como uma forma de pagamento online.

Apesar do grande empenho para ser concretizada essa mudança no sistema de pagamento online, ainda predominam incertezas e desconfianças por parte dos consumidores, dentre outras razões como falta de confiança no sistema bancário, compensação e faturamento sem eficiência nas transações feitas e as taxa de juros nos depósitos bancários.

Para poder haver essa substituição para o dinheiro eletrônico, é fundamental que a nova moeda eletrônica tenha as mesmas características da moeda tradicional como: negociável, moeda legal, um instrumento do portador, possibilidade de ser usado por qualquer pessoa e não apresentar riscos ao consumidor. (Albertin, 2000, p.157)

6.2 Cartões Inteligentes

Conhecido como smart card, é um cartão parecido com cartão de credito. Utilizado como cartão bancário e de identificação pessoal, além disso têm a capacidade de processamento, devido a um microprocessador e uma memória embutida no cartão, proporcionando o recurso de armazenar várias informações na forma eletrônica.

Esse tipo de cartão tem a curiosa característica de representar uma forma de comercio eletrônico sem usar a Internet. A diferença do cartão inteligente para o cartão tradicional, é que contem o dinheiro armazenado neles. Possui o saldo armazenado no cartão, onde as compras são descontadas desse cartão.

Outro nome atribuído a esse tipo de cartão é o de cartão de valor armazenado, onde usa a tecnologia de chip integrado para guarda informações do cliente e também dinheiro digital.

O cartão inteligente possui diversas funcionalidades e podem ser usados para realizar compras de produtos e serviços, guarda informações, controlar permissão de acesso a conta e outras diversas funções disponíveis.

Podem-se notar benefícios proporcionados pelo cartão inteligentes tanto para vendedores como para os consumidores. Dentre as vantagens que verificamos está na redução das despesas com manipulação de dinheiro e prejuízos com fraude, melhor conveniência e segurança do consumidor.

O setor público também está adotando esse tipo de recurso, onde cartões de valor de armazenamento estão sendo uma opção boa para substituir habilitações do governo.

Essa tecnologia também está sendo usufruída por outros países da Europa e o Japão, com a finalidade de pagar ligações telefônicas públicas, transporte e programa de fidelidade nas compras.

Os cartões inteligentes são divididos em dois tipos: cartões de inteligentes baseados em relacionamento ou bolsas eletrônicas.

Os cartões de bolsas eletrônicas substituem o dinheiro, conhecemos também como cartão de debito e dinheiro eletrônico.

Já cartão inteligente do tipo relacionamento, possui uma qualidade de serviços em relação aos cartões já existentes no mercado, onde disponibiliza de novos serviços e produtos incluindo acesso a múltiplas contas bancárias ou qualquer informação que o cliente gostaria de armazenar.

As funções que o cartão de relacionamento deve oferecer são:

Acesso a múltiplas contas como crédito e debito.

Variedades de opções de serviços como disponibilidade de dinheiro, verificar saldo, realizar transferências de fundos monetários.

Ter a opção de acessar através de diferentes tipos de meio de comunicação, como telefone, computador e etc.

Já os cartões de bolsas eletrônicas operam da seguinte forma: bolsa é feita a recarga com dinheiro, podendo ser usada para realizar pagamento de produtos e serviços.

Os benefícios atribuídos a esse tipo de cartão é de evitar possíveis roubos, fraudes e uso indevido. (Albertin, 2000, p.164)

6.3 Cheque Eletrônico

Consiste em quase todos os pagamentos eletrônicos realizados, tendo três elementos relacionados: comprador, o vendedor e o intermediário.

Funcionando da seguinte maneira: o comprador começa uma transação com vendedor, resultando em um pagamento. O consumidor retira uma única certificação do pagamento que seria o cheque virtual, vindo do intermediário. Esse cheque eletrônico debita da conta do comprador com o intermediário. Então o comprador envia esse certificado ao vendedor, logo ele também transmitiu o documento ao intermediário.

As vantagens em utilizar o cheque eletrônico são:

Tempo ganho – ocorre atualização dos saldos em tempo real, permitindo maior flexibilidade financeira.

Diminuição do custo do manuseio do papel - menos trabalhos para impressões dos cheques e menos árvores derrubadas.

Não haver devoluções de cheques – visto que antes de realizar a transação é feita a verificação do saldo da conta financeira.

Flexibilidade – podendo realizar a transação em qualquer lugar do mundo e também se pode efetuar grandes ou pequenas operações bancárias. (Albertin, 2000, p.161)

6.4 Cartão de crédito

Uma forma de pagamento eletrônico muito utilizado ultimamente pela Internet, pode ser usada para realizar compras e contratar serviços. O consumidor recebe todo mês em sua residência uma fatura com os pagamentos a serem realizados. Cada cartão de credito possui certo limite de credito de compras disponibilizado pelas instituições financeiras.

O pagamento realizado através do cartão de credito funciona da seguinte maneira: O vendedor informa o preço dos produtos e serviços, as formas de pagamentos possíveis e a notificação de entrega. Então o consumidor informa o tipo de pagamento a ser realizado de uma forma segura.

Parar realizar uma transação segura utilizando o cartão de crédito, é necessário seguir as seguintes recomendações:

Cliente informa os dados do seu cartão de crédito de forma segura ao vendedor.

Validação do consumidor como proprietário do cartão.

Comerciante enviar as informações do débito e a assinatura do cliente ao banco.

Enviar as informações ao banco do cliente para que seja autorizado e aprovação do credito do consumidor.

Retornando os dados do cartão com autenticação do débito e autorização.

6.5 Cartão de Débito

Podemos chamar também de cartão pré pago, uma maneira de realizar pagamento eletrônico, onde o desconto é feito direto na conta corrente ou poupança do consumidor. Considerado como uma forma de pagamento mais seguro e cômodo.

Apresenta várias vantagens em relação ao cartão de crédito sendo:

Maior controle nos gastos mensais, a compra é efetuada de acordo com valor dos fundos disponíveis na conta bancária do cliente.

Ao realizar comprar usando cartão de débito certos encargos não são cobrados.

O funcionamento da compra feita com cartão de débito possui grandes semelhanças ao cartão de crédito, mas a característica principal dessa forma de pagamento seria o pagamento descontar no momento da compra, sendo que o cartão de crédito disponibiliza fundos para compensar a transação.

6.6 Carteira Eletrônica

É um pagamento realizado com maior segurança e integridade das informações no momento da compra eletrônica. Esse tipo de método é formado por um software que armazena dados relacionados com os cartões, e o certificado digital a ser usado, utilizando um protocolo Transação Eletrônica Segura (SET). Não há nenhuma vulnerabilidade ao inserir

dados do cartão de credito nesse sistema, pois a troca de informações é feita a partir do computador, onde foi feito o cadastro e usando a ferramenta da criptografia. (Luppi, 2011)

7. Segurança no Comercio Eletrônico

Nos últimos anos, a segurança vem-se tornando um tema importante no cotidiano das pessoas. Grandes investimentos são destinados a manutenção e melhorias dos sistemas de segurança, afim de garantir o funcionamento perfeito dos sistemas online, como sites de comércio eletrônico, Internet Banking e outros serviços online disponíveis.

Apesar de tanto investimento na proteção dos sistemas eletrônicos, um detalhe muito importante vem sendo esquecido, outro lado do intermediário da compra, o cliente em si. Não basta ter um grande sistema de segurança de um lado, mas o ambiente do cliente continua vulnerável e propicio a possíveis invasões e fraudes.(Wongtschowski, 2011)

A Internet ainda tem sido vista como um ambiente virtual inseguro, conseqüentemente muitas compras eletrônicas deixaram de ser feitas.

O grande problema da segurança apareceu pois originalmente a World Wide Web não foi criada para realizar pagamentos, o que torna sua arquitetura não tão segura.

Diante disso a segurança de um sistema de Comércio Eletrônico deve ser feita em quatro etapas: a segurança do consumidor da web, a segurança na transmissão das informações, a segurança do servidor da web e a segurança do sistema operacional.

Os riscos de segurança envolvendo o cliente são tão importantes que devem ter uma atenção especial, para ser possível entender a visão ampla do problema na segurança do Comércio Eletrônico. (Andrade, 2001, p.55)

Grande parte dos usuários da Internet, que já realizaram compras ou nunca efetuaram comprar, possuem as mesmas preocupações com relação à privacidade das informações, incluindo a aquisição e sua transmissão pelas empresas. (Kovacs, 2011)

Constata-se a grande influência dos meios de comunicação em massa na opinião dos consumidores, diante das constantes noticiais sobre fraudes cometidas por hackers, interferindo na hora de realizar uma compra virtual

Outra questão que vem chamado atenção no momento da realização da transação eletrônico, é o fato da falta de confiabilidade vem sendo um grande inibidor para os consumidores no momento de efetuar a transação online.

As principais razões pela essa falta de confiança foram: chance do número do cartão de crédito ser usado por outros, pagamento adiantado sem garantia de recebimento do produto e falta de informação no geral.

Essa variável pode se transformar em uma forma positiva para realizar compra eletrônico, se as empresas conseguirem transmitir aos clientes uma imagem de segurança nas suas paginas na web.

Quando um cliente verifica que o comercio virtual é apenas uma extensão da loja física de uma empresa consolidada, passando a sentir mais confiante, visto que se trata de produtos legítimos da loja.

Um possível risco no momento da compra online, torna-se um dos fatores fundamentais para a desmotivação do consumidor em realizar a operação comercial.

Quando o cliente percebe o risco eminente, por menor que seja o prejuízo, não irá fornecer os dados pessoais confidenciais, deixando de efetuar a compra eletrônica.

Então é necessário que as empresas disponham de ferramentas e tecnologia de segurança, que venham inibir as ações infratoras dos hackers. (Garran, 2011)

Diante tanta insegurança no meio virtual, segundo (Sêmola, 2011) , podemos citar alguns procedimentos importantes para garantir a segurança corporativa são elas:

Conscientização - é o detalhe fundamental, com comprometimento dos altos executivos em mudar a cultura da empresa, conscientizando os funcionários da importância da segurança e a colaboração de todos afim de alcançar os objetivos esperados.

Análise do Negócio – a solução da segurança deve ser planejada a partir de todos os setores da empresa e principalmente em relação ao negócio. Para avaliar o negócio na qual se deve implementar uma política de segurança, deve-se utilizar de algumas ferramentas como entrevistas, onde serão levantados competências, a cultura da empresa, o tráfego das informações e os processos do negócio.

Análise das Vulnerabilidades – identificar as principais vulnerabilidades e ordenar de forma a priorizar as mais critica. Analisar também o ambiente físico e detalhar a segurança no ambiente de trabalho. Realizar uma analise dos documentos de acordo com a política da empresa e verificar especificações técnicas, regras de configuração e até mesmo as normas de qualidade. Observar o ambiente informatizado a procura de possíveis pontos de vulnerabilidade e ameaças.

Política de Segurança – Conjunto de composto de diretrizes, normas, procedimentos e instruções que irá guiar o usuário quanto ao uso devido dos recursos disponibilizados. Onde são definidas regras, comportamentos, restrições e até punições por uso indevido. Este documento deve estar conforme a cultura da instituição e seus recursos tecnológicos, para ser obedecidos de acordo com que foi formulado. Além disso, devem-se adotar regras para elaboração senhas e realização de backups.

Classificação das informações – é a tarefa de descrever as regras para seleção, manipulação, transmissão, armazenamento e exclusão de informações, analisando conforme a importância de cada informação. O tráfego das informações deve ser transmitido conforme o tipo do negócio e suas características. Como exemplos de classificação têm: confidencial, restrito, interno e de divulgação. Assim a comunicação no ambiente de trabalho será feita de forma objetiva e correta.

Campanhas de Divulgação – uma forma compacta de segmentar a grande quantidade de informações contida nas normas da política de segurança, visando apenas procedimentos e dicas usadas no cotidiano do departamento. Os funcionários irão recebem informativos mais filtrados, ocasionando melhor entendimento. Além disso, cartazes no ambiente de trabalho e informativos enviados por email complementaram a ação de esclarecimento dos funcionários.

Implementação de Segurança – após analisar e encontrar possíveis pontos de vulnerabilidade, agora é o momento de aplicar as soluções de hardware e software.

Aplicação da Política de Segurança – implementação da política de segurança, onde software pré configurado com determinados critérios, irão usufruir dos recursos tecnológicos.

Termo de Sigilo – compromisso entre funcionário e a instituição, com a correta utilização dos meios tecnológicos disponíveis. Para que isso ocorra é necessária a conscientização de todos os funcionários com as normas e política da empresa.

Teste de Invasão – tendo segurança assegurada por um especialista, nessa etapa é feito o teste da segurança com as ferramentas mais usadas para invasão do sistema como: software de sniffer (grampo digital), Denial of Service (negação de serviço), Trojan Horses (cavalo de tróia), Trashing (análise de lixo) e engenharia social.

Plano de Contingência – garantir a manutenção dos processos ou informações essenciais da empresa, no espaço curto de tempo, com intuição de reduzir os prejuízos. Esse plano de contingência contém janela de tempo, tolerância à paralisação, gatilhos de acionamentos e rotas alternativas de comunicação.

Administração de Segurança – busca continua da segurança, com a revisão das etapas: analise, política e implementação. O processo de segurança é um ciclo continuo, onde deve ser sempre atualizado. (Sêmola, 2011)

8. Tipos de Ameaças a Segurança Virtual

Hoje em dia com avançada tecnologia e a Internet cada dia mais desenvolvida, onde milhares de computadores estão conectados e compartilhando milhões de informações, nesse momento a segurança na Internet Comercial se torna um requisito muito importante.

Algumas das formas mas comuns que afetam a segurança no ambiente virtual e também na hora de realizar a compra virtual, podemos citar:

Bisbilhotice – esses ataques na Internet, resultam no roubo dos dados da conta, como número do cartão de crédito, número de contas do cliente ou dados do saldo e extrato do consumidor.

Espionagem de senhas - esse tipo de invasão tem como principal objetivo ter a permissão de acesso as informações do proprietário armazenadas, entretanto nos tempo atuais, estão disponíveis ferramentas poderosas como algoritmo de criptografia, que anula esse tipo de ataque.

Modificação de dados – realiza a modificação das informações de certas transações econômicas.

Falsificação – ataques virtuais que caracteriza por adulteração das informações ou criação de loja de fachada, afim de coletar os dados dos clientes sem permitir suspeita alguma.

Repúdio – trata-se de repúdio de negociações pode ocasionar grandes problemas com sistemas de faturamento e aceitação do processamento da transação.

Outras ameaças virtuais que afetam a segurança dos clientes, são aquelas de executar software cliente como:

Vírus – determinado código é replicado anexando cópias nos executáveis existentes. Onde o vírus será executado quando o usuário utilizar o programa infectado.

Cavalo de Tróia – um programa ao ser executado realiza a tarefa esperada, mas junto adiciona funções indesejáveis.

Worm – programa auto-replicante, criando uma copia própria ocasionando sua execução, não tendo a intervenção do usuário. (Albertin, 2000, p.175)

Existem muitos ataques focados no consumidor, dentre eles são:

Roubo de dados - Maior intenção é roubar dados críticos de autenticação do cliente. A partir dessas informações, poderá utilizar afim de realizar a autenticação, se passando pelo

consumidor. Esse tipo de ameaça pode ser chamado também de ataque personificação. Esse tipo de roubo pode ser concretizado através de captura de teclado, tela falsa, e-mails falsos.

Roubo de sessão – neste tipo de caso, o ataque realizado é esperar o cliente autenticar e logo utilizar o número de sessão do cliente para efetuar transação online.

Modificação de transações – esse tipo de ameaça ocorre online, utilizando computador do cliente. Este tipo de ataque, um programa adulterador é localmente instalado, ficando no aguardo até o consumidor realizar alguma operação via web. Após o consumidor entrar com os dados da autenticação, o aplicativo vai mudar os dados da transação e transmitir esse pacote adulterado.

Main-in-the-middle – baseia na interceptação das informações no momento da transmissão entre cliente e servidor. O ataque tem acesso de alterar, ler e inserir os dados trocados. Muito utilizando em fraudes pela Internet, onde ao interceptar e modificar as informações importantes trocadas pelo cliente e servidor.

A maioria dos ataques virtuais tem como objetivo final cometer fraudes virtuais. Em especifico roubo de dados, onde é feito a captura dos dados críticos do cliente como senhas, para que no futuro possa replicar num processo de autenticação.

Os ataques virtuais bem sucedidos seguem seguinte modelo:

Instalação – o ataque instala um software malicioso ou alterar de alguma maneira o computador do cliente.

Captura – com esse acesso os dados críticos do cliente são capturados.

Envio dos dados roubados – nesse momento que os dados capturados são enviados para que posso ser acessados por terceiros.

Fraude – nesse instante é utilizado dos dados para realizar a fraude.

Podemos descrever tipos diferentes de ataque sozinhos como:

Ataque completo – ataque sozinho já tem a capacidade de atingir seu objetivo. Não necessita de ajudar de outros ataques.

Ataque parcial – sozinho não consegue realizar a fraude, precisa de outros ataques em conjunto para que conseguir seu objetivo.

Existem diferentes tipos de locais onde são realizados os ataques virtuais dentre eles:

Aplicativos gerais – aplicativos de terceiros, não tão importante no sistema usados pelo usuário.

Aplicativos de sistema – aplicativos do sistema, onde são importantes no cotidiano como email e navegador web.

Sistema operacional – código do sistema operacional como serviços do sistema, DLLs do sistema.

Núcleo do sistema – centro do sistema operacional como drivers de periféricos.

Para que ocorra o ataque, é necessário identificar as vulnerabilidades do sistema, podem-se destacar seguintes vulnerabilidades:

Falha de implementação – sistema operacional possui um bug, uma falha onde pode ser utilizada para o ataque. Normalmente são exploradas por worms Sasser e Blaster.

Defeito de especificação – sistema possui uma brecha na segurança, sistema com arquitetura mal desenvolvida, que pode ser usada para um possível ataque.

Inexperiência do usuário – usuários inexperientes têm mais possibilidades de serem atacados por usuários experientes. Exemplo: emails falsos e links com programas maliciosos.

Podemos destacar também a respeito dos ataques, uma classificação de acordo com a dificuldade de implementação. Segue a seguinte uma escala de dificuldade técnica como:

Ataque simples – não precisa ter muito conhecimento e nem grandes tarefas de programação. O ataque normalmente procura na web, um programa já pronto para ser modificado.

Ataque mediano – necessita de um razoável conhecimento da técnica, com mecanismos internos do sistema operacional. Não necessita de grandes trabalhos de programação.

Ataque complexo – precisa de um conhecimento técnico avançado e extenso do trabalho de programação. Conhecimento em detalhes do sistema operacional, onde funções raramente usadas e não documentados.

Determinados ataques usam programas ocultos para obter informações digitadas e outros mostram janelas para o usuário pedindo todos os dados confidenciais. Nestes tipos de casos pode-se classificar o tipo de transparência dos ataques, que são os seguintes:

Baixa Transparência – o ataque altera muito a forma normal da aplicação original.

Média Transparência – o ataque modifica pouco formal original da aplicação.

Alta Transparência – o ataque modifica muito pouco ou quase nada o programa original.

A seguir podem-se destacar alguns dos ataques mais relevantes são eles:

Trojans – são programas malignos camuflados de programas benignos. Usualmente aproveita da ignorância, curiosidade e falta de informação do usuário.

No momento em que o trojan instala-se no computador do usuário, passa a ter controle total do sistema, podendo monitorar todas as atividades realizadas.

Normalmente a instalação do trojan é feita utilizando emails, na qual o ataque formula um email incentivando a curiosidade do usuário. Induzindo o cliente a instalar o trojan em seu computador.

Exploração das vulnerabilidades – trata-se de um modo comum de instalação de software de maneira ilícita no computador do usuário. Como os worms Sasser e Blaster, usando a vulnerabilidades para instalar trojan na máquina do cliente.

Links falsos – outra possibilidade que é muito usada, é enviar via email em nome de instituições transacionais conhecidas, com link para um site falso semelhante ao site verdadeiro. Assim poderão adquirir informações sigilosas dos clientes como senhas.

Keyloggers – são programas que exercem a captura de informações vinda do teclado, mouse e tela. Na grande parte das vezes, é feita a captura de todos os dados que o cliente digita, quando acessa site de Internet Banking. Alguns métodos mais utilizados para captura de dados são:

Hooks (ganchos) – do sistema operacional pode ser usados para extrair dados do teclado ou mouse. Funciona como pontos dentro do sistema de tratamento de mensagens do Windows, onde um aplicativo é instalado na sub-rotina para observar o tráfego das mensagens no sistema ou processar certas mensagens antes chegar ao destino.

Telas falsas – funcionam basicamente apresentando uma tela semelhante à do site oficial, enganando o usuário. Normalmente ficam sobrepostas ao navegador, dando a impressão que faz parte do site original.

Esses tipos de ataques são muito utilizados, visto que sua implementação não requer muito trabalho, sendo simples de ser realizado.

Ataque redirecionado – quando o ataque afeta endereço IP dos computadores ou o servidor de resoluções de nomes Domain Name System (DNS). Esses ataques podem ser enumerados da seguinte maneira :

Ataque direto ao servidor de DNS - quando o ataque consegue acessar um servidor DNS, possivelmente explorando as vulnerabilidades do servidor. Esse tipo de ataque modifica as tabelas dos nomes próprios do servidor para um endereço IP desejável.

Ataque ao sistema de resolução de nomes da própria máquina do usuário: com ataque conseguindo instalar um trojan localmente no computador do usuário, isso poderá adicionar uma linha no arquivo, impedindo que o sistema verifique o servidor DNS para conseguir IP correto. Assim o sistema redirecionará para o IP desejável e não consultará o servidor DNS.

Troca de Uniform Resource Locator (URL) no navegador do cliente: trojan fica oculto no computador, monitorando todas URLs acessadas. Ao acessar URL a ser atacado, o

trojan redireciona para um endereço local instalo na máquina do usuário. Essa pagina, foi trazida juntamente com o trojan. Logo o cliente irá digitar os dados confidenciais na pagina falsa, então novamente redirecionado para pagina original.

Ataque a maquina virtual Java - o ataque acontece abrindo a biblioteca run-time do Java, que contém a classe Security Manager. Realiza a descompilação e modificação da classe Security Manager, retirando algumas validações. É feito a recompilação da classe e novamente compactada com biblioteca run-time do Java. Alterando a biblioteca original pela fraudada.

Esse tipo de ataque é muito realizado afim de capturar os dados críticos do cliente, onde muitos sites de Internet banking e de comércio eletrônico usam para autenticação. (Wongtschowski, 2011)

9. Modos de Segurança

Nos tempos atuais, o envio e recebimento de informações sigilosas tornaram-se importantes, a Internet se desenvolvendo a cada dia mais, como resultado tem uma facilidade de transmissão dos dados de maneira precisa e extremamente rápida.

Diante dos ataques virtuais freqüentes as informações confidenciais tornam-se fundamental aumentar a segurança tanto no site Internet Banking e também no comércio eletrônico, para isso muitos utilizam de ferramentas apropriadas.

9.1 Criptografia

Trata-se de um conjunto de normas e técnicas que tem como objetivo codificar uma informação de forma apenas o emissor e o receptor possam acessá-las, não permitindo assim que terceiros possam interpretá-las. Com isso, diversas técnicas são utilizadas e muitas outras são desenvolvidas ao longo do tempo.

Na ciência da computação, as técnicas mais conhecidas estão relacionadas ao conceito de chaves, sendo nomeadas de chaves criptográficas. Trata-se de um conjunto de bits de acordo com um algoritmo específico capaz de codificar e de decodificar informações. Caso o receptor da informação usar uma chave diferente da chave do emissor, não conseguirá obter a informação.

As primeiras formas criptográficas existentes utilizavam somente um algoritmo de codificação. Assim, só o receptor dos dados tiver o conhecimento do algoritmo para poder extraí-las. Entretanto, se o invasor tiver domínio desse algoritmo, também terá poder de realizar o processo de decifragem, se conseguir capturar as informações criptografadas.

As chaves possuem determinados valores, que expressam o seu tamanho. Quanto mais bits forem usados, mais segura será a criptografia.

Há dois tipos diferentes de chaves criptográficas são elas:

Chave simétrica – é o tipo mais simples de chave, onde o emissor e receptor usam a mesma chave, ou seja, uma única chave é utilizada para realizar a codificação e decodificação dos dados. Existem diversos tipos de algoritmos que usam chave simétrica como:

Data Encryption Standard (DES): desenvolvida pela IBM no ano de 1977, formada com 56 bits. Traduzindo em 72 quatrilhões de combinações possíveis. É um valor relativamente alto, mas não quando se fala em um computador potente.

International Data Encryption Algorithm (IDEA): criada no ano de 1991 por James Massey e Xuejia Lai, trata-se de um algoritmo que utiliza de 128 bits e tem sua composição semelhante ao DES. Sua implementação no software é mais simples que o deste último.

Ron´s Code ou Rivest Cipher (RC): desenvolvida por Ron Rivest da empresa RSA Data Security, esse algoritmo é normalmente utilizado para emails e sendo composto por 8 a 1024 bits. Possui muitas versões: RC2, RC4, RC5 e RC6. A diferença entre essas chaves, consiste com quantidade de bits trabalhada.

A utilização da chave simétrica possui algumas desvantagens, onde sua utilização não sendo recomendada em situações com informação muito valiosa. Para iniciar, é preciso usar uma grande quantidade de chaves caso muitas pessoas e entidades estejam relacionadas ao trafego das informações. Então tanto o emissor como receptor deve ter o conhecimento da mesma chave.

Chave assimétrica – conhecida como chave pública, onde trabalha com duas chaves uma chamada privada e outra pública. Esse tipo de método, um emissor deve desenvolver uma chave de codificação e transmitir ao receptor. Essa é a chave pública. Outra chave é criada para decodificação, sendo essa a chave privada, que é secreta.

Nos algoritmos de chaves assimétricos podemos destacar:

Rivest, Shamir and Adleman (RSA): criado no ano de 1977 pelo Ron Rivest, Adi Shamir e Len Adleman, é um algoritmo de chave assimétrico usualmente utilizados. Nesse tipo são utilizados números primos, onde dois números são multiplicados para se ter um terceiro valor. Basicamente, a chave privada no RSA são números multiplicados e a chave pública é o resultado obtido;

ElGamal: desenvolvido por Taher ElGamal, esse tipo de algoritmo utiliza um logaritmo discreto para tornar-se mais seguro. Normalmente é utilizado para assinaturas digitais;

Pretty Good Privacy (PGP): trata-se de um software de criptografia desenvolvida por Philip Zimmermman no ano de 1991. Disponibilizado de maneira gratuita, logo se tornou um dos meios de criptografias mais comum, principalmente na troca de emails.

Para composição da PGP é utilizada chaves assimétricas. Afim de aumentar mais segurança, o software também faz uso de um segundo método de criptografia chamado de chave de sessão, sendo chave do tipo simétrica.

Criptografia consiste em 4 princípios básicos: confidencialidade, autenticação, integridade da informação e não repudiabilidade. Por isso que a criptografia é fundamental na transmissão de informações pela Internet, mesmo com toda essa tecnologia ainda não é garantido 100% de segurança. Visto que sempre existe um terceiro capaz de decifrar uma codificação. Por causa desses motivos, que a criptografia está sempre em desenvolvimento, criando novas ferramentas e buscando uma melhoria continua.

9.2 Protocolos de Autenticação

Autenticar é o método de verificar, se usuário que está tentando acessar, é o permitido. Caso o usuário que esteja acessando for outra pessoa, o sistema deve pelo menos ignorar esse usuário.

Existem protocolos de autenticação que tem como finalidade efetuar transações seguras de dados no ambiente virtual, podemos citar:

Secure Eletronic Transaction (SET) – protocolo que oferece transação segura de pagamentos eletrônicos usando cartão de crédito. Assegurando a confidencialidade e integridade dos dados com utilização de certificados digitais.

Secure Hyper Text Transfer Protocol (S-http) – proporciona envio dos dados via web de maneira segura. Usando uma camada de aplicação é feito um processo de negociação entre o cliente e o servidor. Oferece autenticação, integridade, confidencialidade e certificação, mas nem todos os browsers são compatíveis com S-http.

Secure Sockets Layer (SSL) – usa criptografia de chave pública afim de realizar troca de dados via web. É feita diversas transmissões de dados para negociar os parâmetros de segurança da conexão entre cliente e servidor. (Krause, 2011)

9.3 Certificado Digital

Atualmente a Internet tem permitido as empresa, pessoas, governo e outras instituições a realizarem uma variedade de tarefas e transações de forma rápida e eficiente. Por esse motivo, foi possível realizar negócios, enviar e receber informações, acessar e disponibilizar dados confidenciais, diminuir a burocracia. Entretanto, da mesma maneira que os computadores oferecem esses benefícios, também podem ser usados para realizar fraudes, então quando realizamos tais operações sigilosas, deve-se atentar na questão da confiabilidade e segurança. O certificado digital é capaz de atender essa necessidade.

Certificado digital consiste em um tipo de tecnologia de identificação que favorece as transações eletrônicas dos mais variados tipos a serem realizadas com integridade, autenticidade e confidencialidade, evitando assim as possíveis fraudes, obtenção de dados sigilosos e outros tipos de adulteração.

Certificado digital baseia-se em um documento eletrônico com assinatura digital que é composta de dados como nome do usuário, prazo de validade e chave pública. Através do certificado digital fica garantida a autenticidade da empresa ou cliente, que esteja interessada em realizar a transação eletrônica.

Para se obter um certificado digital, deve-se procurar uma entidade emissora apropriada como Autoridade Certificadora (AC) ou Autoridade de Registro (AR). Então essa autoridade vai associar uma identificação a uma chave e inserir os dados no certificado digital. No Brasil essa autoridade que emiti os certificados digitais é a ICP-Brasil.

A ICP-Brasil dispõe de dois tipos de certificados digitais, sendo A e S. O tipo A é reservado para identificação e autenticação, já o tipo S é separado para atividades sigilosas.

Sendo assim dividas esses tipos de certificados digitais:

A1 e S1 : geração de chaves feita para software, tamanho mínimo de 1024 bits. Guardados em dispositivos de armazenamentos como HDs, validade de um ano.

A2 e S2 : geração de chaves criadas para software, com dimensão de 1024 bits. Armazenamento em cartões inteligentes e token, validade de dois anos.

A3 e S3: geração de chaves desenvolvidas para hardware, tamanho de 1024 bits. São guardados em cartão inteligente ou token, prazo de três anos.

A4 e S4: geração de chaves criadas para hardware, dimensão de 2048 bits. Armazenamento em cartão inteligente e token, validade de três anos.

Os certificados A1 e A3 costumam ser os mais usados, onde A1 geralmente fica no computador do cliente e o A3 armazenado em cartão inteligente ou token restringindo por senhas.

9.4 Assinatura Digital

Trata-se de um mecanismo que utiliza da criptografia, ou seja, faz uso das chaves criptográficas. Este método considera duas importantes características como: confidencialidade e autenticidade. Confidencialidade consiste em deixar as informações acessíveis apenas às pessoas e organizações autorizadas. Já autenticidade oferece a certeza da informação enviada da origem correta e a receptora reconhecer a origem.

Além disso é notado o uso da função hash, afim de garantir a integridade. Essa função é um processo criptográfico na qual a informação dever passada, antes de ser transmitida. O resultado é único nomeado de resumo e possui mesmo volume, independente do volume tratado.

Assinatura digital então faz parte da função hash junto ao documento a ser enviado e na utilização das chaves criptográficas. No procedimento de conferência, deve-se calcular o hash e decifrar as chaves criptográficas, onde qualquer alteração nos dados, resultará em um resumo diferente, constatando ocorrência de adulteração das informações. (Alecrim, 2011)

9.5 Firewall

Trata-se de um requisito importante quando se trata de segurança no ambiente virtual. Cada vez maior o volume de troca de informações e sistemas muito complexos, necessitando de uma proteção maior, aderindo ao uso de aplicações e ferramentas mais eficientes na segurança.

O Firewall pode ser determinado como uma barreira de proteção, onde é controlado o trafego de dados entre o computador do usuário e a Internet. Objetivo principal é permitir

apenas a transmissão e recepção de dados autorizados. Existem variedades de tipos de firewall combinando hardware e software ou somente software.

O Firewall é um mecanismo que trabalha como defesa de um sistema computacional ou de uma rede, monitorando os acessos ao sistema e através de normas e regras realizar a filtragem das informações. A grande vantagem de se usar o firewall em redes, é apenas um computador pode atuar como firewall, não necessitando instalar em outros computadores.

Basicamente o funcionamento do firewall consiste em dois tipos: filtragem de pacotes e outro com controle de aplicações. Ambos funcionam de acordo com sistema, aplicação ou critério do desenvolvedor.

Filtragem de pacotes - esse tipo de firewall é muito usado em redes pequenas ou de porte médio. Através de conjuntos de normas definidas, esse tipo de firewall é quem define que endereços IPs e dados podem realizar comunicação ou receber/transmitir dados. Determinados serviços podem ser liberados como email da rede, mas outros serviços por apresentarem alto grau de insegurança e vulnerabilidade como software de mensagens instantâneas deve manter bloqueado.

Um dos problemas apresentados pelo firewall, seria em relação às regras aplicadas podendo ser muito complexas, interferindo no desempenho da rede ou não serem tão eficazes como previsto.

Este tipo de firewall, se limita a operar nas camadas TCP/IP, verificando os pacotes de dados que poderão ser transmitidos ou não. Essa decisão de autorizar ou não, provém das informações obtidas do endereço IP remoto, endereço IP do destinatário, alem da porta TCP.

Quando configurado corretamente, esse firewall autoriza apenas computadores conhecidos transmitirem determinados dados entre si e tenham acesso a recursos pré determinados. Além disso, tem a capacidade de analisar informações a respeito da conexão e verificar alguma alteração suspeita, e também é possível analisar os pacotes, tendo assim maior controle sobre o que autorizar.

Firewall de aplicação – são instalados em computadores servidores e conhecidos como proxy. Esse tipo de firewall não autoriza a comunicação direta entre a rede e a Internet. Todas as informações transmitidas devem passar pelo firewall, fazendo o papel de intermediador. O Proxy realiza a comunicação em todos os lados, através do número da sessão TCP dos pacotes.

Esse firewall é muito complexo, então é considerado mais seguro, pois todas as aplicações devem estar com um proxy, senão não funciona corretamente.

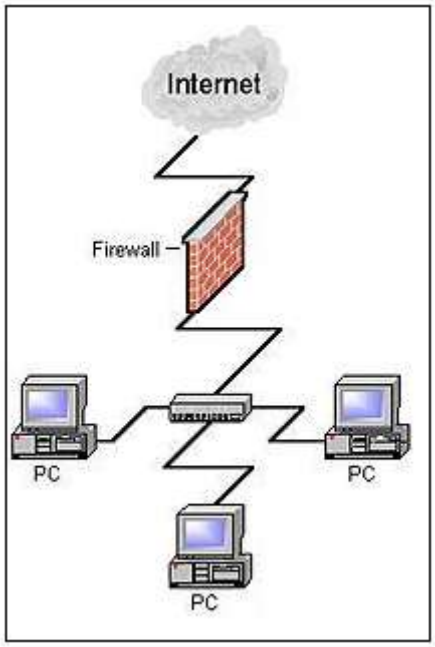
Existem três importantes motivos para se utilizar um firewall são eles:

Firewall contribui para impedir que a rede ou os computadores sejam acessados indevidamente. Assim dificultará as ações de hackers, com possíveis capturas de informações confidenciais.

Firewall é auxiliador para bloquear vírus e cavalos de troia, bloqueando as portas, que possivelmente iriam ser invadidos por vírus e outras pragas virtuais.

Nas redes corporativas, sendo possível restringir acessos em serviços ou sistemas não permitidos, além disso ter o controle da rende, sendo possível identificar quais usuários acessaram determinadas informações. (Alecrim, 2011)

A seguir uma figura ilustrativa da visão mais comum do firewall.



Fonte: Alecrim, Emerson

Figura 3 - Esquema do funcionamento do firewall

9.6 Selos Digitais

Defini-se como assinatura digital de um terceiro de confiança confirmando que o documento digital é valido, no instante (data e hora) que foi assinado. Com isso podemos assinar documentos digitais anexando uma validade neles. Muito utilizado pelos programas de correio eletrônico, afim de assinar e criptografar mensagens eletrônicas.

Tal assinatura é garantida e auditada pelo Observatório Nacional e certificada por ICP-Brasil, garantindo a validade do documento naquele momento.

Pode-se obter o selo digital através do aplicativo GatewaySC, que realiza a solicitação, gerenciamento e verificação de selos digitais do ICP-Brasil.

Podemos citar algumas aplicações para o selo digital sendo: assinatura de contratos eletrônicos, atos normativos governamentais e livros fiscais eletrônicos.

10. Normas de Segurança da Informação

Segurança da Informação está relacionado à proteção de um conjunto de dados, no que se refere à preservação do valor que possuem para uma pessoa ou uma instituição. As características principais da segurança da informação são: confidencialidade, integridade, disponibilidade e autenticidade. Essa segurança não está limitada apenas em sistemas computacionais, também está presente nas informações eletrônicas ou sistemas de armazenamentos.

Dentre as normas de segurança pode-se destacar a ISO/IEC 27001 é um padrão para gestão de segurança da informação. Sua finalidade é ser utilizado juntamente com ISO/IEC 17799, código de procedimentos para gerenciar a segurança da informação. Além delas existem outros padrões dessa família de normas que são:

ISO 27000 – vocabulário de gestão da segurança da informação;

ISO 27001 – certificação de sistema de gestão de segurança da informação;

ISO 27002 – código de boas práticas;

ISO 27003 – regras para implementação do sistema de gestão de segurança da informação;

ISO 27004 – relata medidas e relatórios de um sistema de gestão de segurança da informação.

ISO 27005 – indicação para implementação monitoramento e melhoria continua do sistema de gestão de segurança da informação;

ISO 27006 – norma define requisitos e oferece recomendações para os organismos que realizam serviços de auditoria e certificação de um sistema de gestão da segurança da informação.

11. Futuro do Comércio Eletrônico

O Comércio Eletrônico tem sofrido grandes mudanças, mas nos últimos anos com o desenvolvimento de novas tecnologias, isso tem intensificado a influência no crescimento de outras modalidades de comércio eletrônico.

Como novas modalidades de comércio eletrônico podem citar:

11.1 M-Commerce – Mobile Commerce

Trata-se de toda e qualquer transação que esteja relacionado à transferência de propriedade ou direitos de uso de bens e serviços, que é começada e terminada até o acesso ao computador utilizando o celular intermediado por redes com o auxilio de um aparelho eletrônico.

O Comércio Eletrônico atual será adaptado para a modalidade móbile commerce, ainda em fase de desenvolvimento. Assim como próprio Comércio Eletrônico foi crescendo e nos dias atuais já faz parte do nosso cotidiano, da mesma maneira o mobile commerce vai se desenvolver.

Diante das novas tecnologias, ferramentas e serviços de trafego de dados para celulares cada vez melhores, aparelhos celulares com diversas funções, isso tudo propicia a expansão dos negócios nessa área.

Algumas aplicações mobile já estão disponíveis como:

Mobile ticketing – são tickets transmitidos para celulares, onde o cliente pode apresentar na bilheteria. Pode ser usado como ticket para agencia de viagens, diminuindo o tráfego de pessoas em ambientes como aeroportos e estacionamentos.

Mobile Vouchers – usuário recebe no celular cupom de descontos para ser utilizados.

Compra de conteúdo – serviço de compra de arquivos mp3, ringtones e papéis de parede.

Serviços de location-based – baseia-se na localização do usuário, a partir disso é feito incentivo a vendas de produtos da região.

Serviços de Informação – grande quantidade de informações pode ser comercializada, desde horóscopo até informações financeiras.

Mobile banking – grandes esforços estão para que seja possível acessar conta, consultar saldos e extratos e também realização compra de ações e transferência de dinheiro, mas na questão da segurança das informações e transações tem impedido o crescimento.

Mobile corretora de ações – usuário tenha tempo real nas movimentações da sua carteira. Com informações atualizadas, podendo interferir de acordo com o mercado de ações.

Mobile marketing e publicidade – está em grande crescimento, onde propõem eficácia nas propagandas enviadas para os dispositivos moveis. (Tardin, 2011)

11.2 F-Commerce – Facebook Commerce

Define-se como um comércio eletrônico dentro do Facebook. Na prática a transação realizada via web acontece da mesma forma que o Comércio Eletrônico tradicional, diferencia é na plataforma onde serão comercializados os produtos, será na plataforma do Facebook.

Diante do crescimento significativo do número de usuários do Facebook, motivou o interesse das empresas a estarem presente nessa rede social. Sendo possível desenvolver uma loja virtual dentro do Facebook usando as ferramentas do Comércio Eletrônico. Esses aplicativos funcionam como vitrine dos produtos e serviços dentro da rede social. Quando alguém tentar realizar a compra virtual, irá direcioná-lo para o site do produto. (Peres, 2011)

11.3 Compra coletiva

Destaca-se como uma modalidade de comércio eletrônico que tem como principal objetivo negociar produtos e serviços para um número mínimo pré-definido de compradores por oferta.

Através desse comércio, os consumidores normalmente beneficiam do produto após um número de interessados associarem à oferta, para compensar os descontos disponibilizados que na maioria das vezes chegam até 90% do preço normal. Por regra deste

tipo de negócio os compradores dispõem de um tempo determinado para realizar a oferta, que dura aproximadamente 24horas e 48horas depois do seu lançamento. Se não atingir o número mínimo de pedidos dentro desse período, a oferta será cancelada.

Essa modalidade de compra foi criada nos Estados Unidos pelo Andrew Mason, lançando o primeiro site com esse tipo de comércio em novembro de 2008, o Groupon. Já no Brasil, o primeiro site de compra coletiva foi o Peixe Urbano, iniciado em março de 2010. Esse novo tipo de comércio eletrônico trouxe grandes benefícios tanto para as empresas como também para os consumidores. Empresas estão vendendo produtos em maior volume por causa do preço baixo, além disso os consumidores estão conseguindo descontos significativos motivados pela compra coletiva.

O Buzz Marketing é uma aplicação importante para o setor, visto que auxilia aos próprios consumidores a divulgarem as ofertas das empresas, usando as redes sociais como meio de divulgação, com objetivo de ter mínimo de preciso de pedidos para oferta ser aceita.

O atualmente o dinamismo no comércio eletrônico principalmente na compra coletiva, trouxeram inovações como promoções. Uma das promoções oferecidas seria a disponibilização de créditos aos clientes cadastrados do site, assim mantém o consumo dos produtos e serviços e também a base dos consumidores sempre ativa.

Além disso, são oferecidos bonificações aos usuários já cadastrados que indicarem novos consumidores para realizar compras por esse site.

Nos dias de hoje, a compra coletiva é formada por fornecedores de pequeno e médio porte, comercializando bens de consumo não duráveis, como serviço de estética, fotografia, refeições, academia, hospedagem, Pet Shop e entre outras. (Gavioli, 2011)

11.4 Produtos Virtuais

Hoje já é realidade. Grandes empresas de comércio como Saraiva e Submarino, já disponibilizam produtos virtuais como filmes, jogos, software, livros dentre outros produtos.

12. Conclusão

O desenvolvimento da tecnologia, em especial a fusão entre a computação e a telecomunicação e sua propagação estão evoluindo a área da comunicação no sentido de ampliação do mercado, por ser fundamental na sociedade moderna.

A internet definiu um marco na evolução dos meios de comunicação mundialmente, pois está modificando as possibilidades de realização de transações comerciais ao redor do mundo. A rede mundial está cada vez mais se mantendo como o meio mais eficiente de comunicação entre empresas e clientes, sejam eles pessoas física ou jurídica.

O avanço dessa tecnologia da comunicação trouxe a criação do Comércio Eletrônico, que já existe na prática e está em grande expansão de mercado, mas a aceitação ampla do processo da compra online depende da superação de vários tipos de obstáculos como barreiras tecnológicas, culturais e organizacionais.

A respeito da barreira tecnológica pode-se destacar a necessidade da disponibilidade tecnológica e sua facilidade na sua utilização. A disponibilidade implica na expansão do acesso e no custo da tecnológica, já a facilidade está relacionada com o desenvolvimento de interfaces de comunicação com os consumidores.

Outro detalhe a ser destacado seria a segurança na transação eletrônica. A falta de confiança dos usuários quando se refere à segurança no sistema da compra eletrônica.

Um dos motivos para as compras online terem o crescimento e aprovação dos consumidores limitados seriam a insegurança e desconfiança por parte dos usuários.

A garantia da privacidade é um fator essencial para auxiliar a desenvolver no consumidor um nível de confiança bom em relação ao sistema do Comércio Eletrônico. O sistema oferece aos consumidores diversas formas de informações disponíveis, mas os consumidores ainda apresentam resistência em divulgar as empresas seus dados pessoais e bancários.

A segurança não é totalmente garantida, entretanto as chances de ocorrerem ataques virtuais em uma compra eletrônica na web são pequenas, visto que nos últimos anos várias ferramentas e tecnologia foram desenvolvidas para aumentar a segurança durante uma transação eletrônica.

Culturalmente também é possível notar uma influência sobre a aceitação do comércio eletrônico. Certas regiões possuem o hábito de consumo de produtos via web, mas outros

lugares não são tão comuns, por isso toda essa cultura regional impacta no crescimento do comercio eletrônico. Além disso temos a língua e as diferenças culturais de cada região e país, que são vistas também como uma barreira no desenvolvimento da compra eletrônica.

Outra barreira relacionada ao comércio eletrônico é na organização, onde a utilização apenas da tecnologia não garante sucesso no sistema do Comércio Eletrônico. É necessário mais do que isso, é preciso desenvolver uma qualidade sustentável, afim de manter a fidelidade do consumidor com a empresa.

Boa qualidade nos serviços prestados e um bom relacionamento entre cliente e empresa são fatores fundamentais para garantir fidelidade do cliente. Apenas com o equilíbrio entre solicitação dos consumidores, administração dos pedidos, estoque e administração financeira pode-se garantir qualidade dos produtos e manter os consumidores.

Para obter algum resultado com Comércio Eletrônico é preciso enfrentar e superar as barreiras que existem ainda no campo tecnológico, cultural e organizacional.

A grande tendência da compra eletrônica é de aumentar o número de adeptos compradores virtuais devido às comodidades, conveniência, promoções, economia de tempo e dinheiro, forma mais fácil de encontrar fornecedores e produtos com menores preços em relação ao mercado físico.

A compra online apresenta-se como um grande potencial, visto que o futuro a tendência é tudo tornar-se digital.

As empresas que não aderirem a Internet e ao Comércio Eletrônico e outras formas de novas tecnologias não serão mais competitivas durante muito tempo e entraram em declínio.

Com certeza a Internet e o Comércio Eletrônico são muito importantes para o desenvolvimento e a promoção de negócios, hoje e no futuro.

13. Referências Bibliográficas

ABRIL, Editora. **Comércio Eletrônico Deve Faturar**. Disponível em: <http://info.abril.com.br/noticias/mercado/comercio-eletronico-deve-faturar-36-a-mais-23092011-0.shl>. Acesso: out. 2011.

ALBERTIN, Luiz Albertin. **Comércio Eletrônico**. 2. ed. São Paulo: Atlas, 2000.

ALECRIM, Emerson. **Criptografia**. Disponível em: < http://www.infowester.com/criptografia.php>. Acesso em: out. 2011.

ALECRIM, Emerson. **Entendendo a Certificação Digital**. Disponível em: < http://www.infowester.com/assincertdigital.php>. Acesso em: out. 2011.

ALECRIM, Emerson. **Firewall: Conceitos e Tipos**. Disponível em: < http://www.infowester.com/firewall.php>. Acesso em: nov. 2011.

ANDRADE, Rogério de. **Guia Prático de E-Commerce**. 1. ed. São Paulo: Angra, 2001.

BOGO, Kellen Cristina. **A História da Internet Como Tudo Começou**. Disponível em: <http://www.viaki.com/home/internet/historia.php>. Acesso em: out. 2011.

GARRÁN, Vanessa Gabas**. De Navegadores a Compradores: Os Elementos Motivacionais nas Decisões de Compra pela Internet**. Disponível em: <http://www.contextus.ufc.br/index.php/contextus/article/view/47>. Acesso: nov. 2011.

GAVIOLI, Guilherme. **Compra Coletiva**. Disponível em: < http://ecommercenews.com.br/glossario/o-que-e-compra-coletiva>. Acesso em: set. 2011.

KOVACS, Michelle H. ; FARIAS, Salomão A. de. **Dimensões de Riscos Percebidos nas Compras pela Internet**. Disponível em: <http://www.scielo.br/pdf/raeel/v3n2/v3n2a13.pdf>. Acesso: set. 2011.

KRAUSE, Maico. Protocolos de **Autenticação, Certificado Digital e Assinatura Digital**. Disponível em: < http://my.opera.com/maicokrause/blog/2009/06/16/protocolos-de-autenticacao-certificado-digital-e-assinatura-digital>. Acesso em: set. 2011.

LEMES, Celso. **Comércio Eletrônico Como Tudo Começou**. Disponível em: <http://www.osabetudo.com/comercio-eletronico-como-tudo-comecou/>. Acesso em: nov. 2011.

LUPPI, Iria. **Formas de Pagamento no Comércio Eletrônico**. Disponível em: <http://www.oficinadanet.com.br/artigo/1759/formas_de_pagamento_no_comercio_eletronico >. Acesso em: jul. 2011.

LUPPI, Iria. **Histórico do Comércio Eletrônico**. Disponível em: <http://www.oficinadanet.com.br/artigo/1718/historico_do_comercio_eletronico>. Acesso em: maio 2011.

MENDES, Marcos. **O Comércio Eletrônico no Brasil**. Disponível em: <http://www2.ufpa.br/rcientifica/artigos_cientificos/ed_08/pdf/marcos_mendes3.pdf>. Acesso: nov. 2011.

PERES, Emmanuelle de Moura. **F-Commerce: Facebook Sua Loja Virtual**. Disponível em: < http://pro-manu.blogspot.com/2011/08/f-commerce-facebook-sua-loja-virtual.html>. Acesso em: out. 2011.

SANTOS, Luiz Carlos dos. **Como Funciona a Autenticação?**. Disponível em: < http://www.malima.com.br/article_read.asp?id=64>. Acesso em: set. 2011.

SÊMOLA, Marcos. **Dicas para Proteger o Seu Negócio**. Disponível em: <http://www.semola.com.br/disco/Coluna_IDGNow_25.pdf>. Acesso em: out. 2011.

SMITH, Rob. ; SPEAKER, Mark. ; THOMPSON, Mark. **O Mais Completo Guia Sobre E-Commerce** 1. ed. São Paulo: Futura, 2000.

TARDIN, Vicente. **Mobile Commerce é o Comércio Eletrônico no Celular**. Disponível em: < http://webinsider.uol.com.br/2008/10/31/mobile-commerce-e-o-comercio-eletronico-no-celular/>. Acesso em: set. 2011.

WONGTSCHOWSKI, Arthur. **Segurança em Aplicações Transacionais na Internet: O Elo Mais Fraco**. Disponível em: <http://www.teses.usp.br/teses/disponiveis/3/3141/tde-05092006-175654/en.php>. Acesso em: out. 2011.