Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

LAÍS COSTA JULIÃO

COMÉRCIO ELETRÔNICO: SEGURANÇA E CONFIABILIDADE

Assis
2010

Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

LAÍS COSTA JULIÃO

COMÉRCIO ELETRÔNICO: SEGURANÇA E CONFIABILIDADE

Projeto de pesquisa apresentado ao Curso de Bacharelado em Ciência da Computação do Instituto Municipal de Ensino Superior de Assis – IMESA e a Fundação Educacional do Município de Assis – FEMA, como requisito parcial à obtenção do Certificado de Conclusão.
Orientador(a): Rita de Cássia Cassiano Lopes.

Assis
2010

FICHA CATALOGRÁFICA

JULIÃO, Lais Costa

Comércio Eletrônico: Segurança e Confiabilidade / Lais Costa Julião. Fundação Educacional do Município de Assis – FEMA – Assis, 2010.

56p.

Orientador (a): Rita de Cássia Cassiano Lopes.
Trabalho de Conclusão de Curso – Instituto Municipal de Ensino Superior de Assis – IMESA.

1. Comércio Eletrônico. 2. Segurança. 3. Criptografia.

CDD: 001.6
Biblioteca da FEMA

Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

COMÉRCIO ELETRÔNICO: SEGURANÇA E CONFIABILIDADE

LAIS COSTA JULIÃO

Trabalho de Conclusão de Curso apresentado ao Instituto Municipal de Ensino Superior de Assis, como requisito do Curso de Bacharelado em Ciência da Computação, analisado pela seguinte comissão examinadora:

Orientador (a)**:** _____

Analisador (1): _____

Assis
2010

DEDICATÓRIA

Dedico este trabalho ao meu pai Antonio Julião e minha mãe Silvia, que me deram a oportunidade de cursar uma faculdade até o final. Obrigada.

AGRADECIMENTOS

Agradeço em primeiro lugar a Deus, por estar sempre comigo principalmente nesta longa caminhada da faculdade.

Á professora Rita de Cássia Cassiano Lopes, pela maravilhosa orientação por estar presente em todos os momentos do decorrer deste trabalho.

Á uma pessoa especial, que me apoiou durante todos os anos da faculdade, sempre me parabenizando nas vitórias conquistadas.

Aos amigos, familiares, professores e a todos que colaboraram direta ou indiretamente, na execução deste trabalho.

RESUMO

Com o crescimento da internet, o chamado Comércio Eletrônico passa a ser uma das formas mais fáceis, rápidas e cômodas de se fazer compras. Nos últimos anos o Comércio Eletrônico têm crescido bastante e atraído um grande número de usuários.

Porém, a Internet não é um ambiente que proporciona total segurança e confiança a esses potenciais compradores. Por essa razão, o presente trabalho tem por objetivo apresentar algumas formas, técnicas e métodos de segurança, desenvolvidos e utilizados pelas empresas virtuais, para tentar proporcionar a maior segurança possível a seus clientes. Fazendo parte do Comércio Eletrônico, as formas de pagamento também serão abordadas.

E por fim, faz-se uma análise prática de uma compra através de um site implementado, para a apresentação final deste trabalho.

Palavras - chave: comércio eletrônico; segurança.

ABSTRACT

Caused by the internet growing, the electronic commerce, commonly known as e-commerce, becomes one of the easiest, fastest and simplest ways of shopping. The last few years the e-commerce has been growing and attracting a large number of users.

On the other hand the internet is not an environment that provides complete safety for its customers. For this reason this piece of work has the objective of presenting forms, techniques and safe methods developed and used by virtual companies that try to supply their customers the best safety they can. As long as the payment methods are a part of the electronic commerce they will also be included.

In the end there will be a practical analysis of shopping through an implemented website for the presentation of this piece of work.

Keywords: electronic commerce; e-commerce; safety.

LISTA DE ILUSTRAÇÕES

Figura 1 – Processo de criptografia simétrica.....33

Figura 2 – Processo do algoritmo DES Triplo.....35

Figura 3 – Selo Site Blindado.....40

Figura 4 – Site Blindado Alerta.....41

Figura 5 – Site Blindado Alerta, pesquisa Google.....41

Figura 6 – Certificação SSL EV.....43

Figura 7 – Página Inicial - Site.....52

Figura 8 – Categoria com respectivo livro.....52

Figura 9 – Carrinho de compras – Pag Seguro.....53

SUMÁRIO

1. INTRODUÇÃO..... 12

2. REVISÃO BIBLIOGRÁFICA..... 14

3. COMÉRCIO ELETRÔNICO..... 19

3.1 MODALIDADES DE COMÉRCIO ELETRÔNICO..... 20

3.1.1 Negócio-a-Negócio..... 20

3.1.2 Negócio-a-Cliente..... 21

3.1.3 Negócio-a-Governo..... 21

3.1.4 Governo-a-Consumidor..... 21

3.1.5 Consumidor-a-Consumidor..... 22

3.2 IMPACTOS DO COMÉRCIO ELETRÔNICO NA SOCIEDADE..... 22

4. SEGURANÇA DAS INFORMAÇÕES..... 26

5. CRIPTOGRAFIA..... 29

5.1 CRIPTOGRAFIA SIMÉTRICA..... 31

5.1.1 Algoritmos para chave simétrica..... 32

5.1.1.1 *Data Encryption Standar (DES)*..... 33

5.1.1.2 *International Data Encryotion Algorithm (IDEA)*..... 34

5.2 CRIPTOGRAFIA ASSIMÉTRICA..... 34

5.2.1. Algoritmo para chave Assimétrica..... 36

5.2.1.1 Rivest-Shamir-Adleman Algorithm *(RSA)*..... 36

6. SEGURANÇA NO COMÉRCIO ELETRÔNICO..... 37

6.1 BLINDAGEM DE SITE..... 38

6.1.1 Site Blindado Alerta..... 39

6.1.2 Certificação SSL – EV..... 41

6.2 ASSINATURA DIGITAL..... 43

6.2.1 Algoritmos de resumo..... 45

6.2.1.1 Algoritmo MD2..... 45

6.2.1.2 Algoritmo MD5..... 46

6.2.1.3 Algoritmo SHA -1..... 46

7. FORMAS DE PAGAMENTO..... 47

7.1 DINHEIRO ELETRÔNICO..... 47

7.2 CARTÕES INTELIGENTES..... 48

7.3 CARTÕES DE CRÉDITO..... 48

7.4 BOLETO BANCÁRIO..... 49

8. COMPRA ELETRÔNICA NA PRÁTICA 50

9. CONCLUSÃO..... 53

REFERÊNCIAS..... 54

1. INTRODUÇÃO

A área da tecnologia está sempre em busca de novas técnicas e ferramentas para que a sociedade possa usufruir em seu benefício.

A internet, dentre todas estas ferramentas, é a mais comentada e utilizada na atualidade. Ela evolui a cada dia e, desta maneira, tornou-se um dos principais meios de comunicação, permitindo à sociedade um avanço tecnológico e econômico, trazendo comodidade e rapidez àqueles que possam fazer uso dela.

Por meio da internet o comércio de produtos conquistou um novo espaço, o espaço virtual. O que antes era apenas realizado de forma tradicional, ou seja, em uma loja física, com clientes e vendedores reais, hoje pode ser feito por meio de um computador ou qualquer outro equipamento com acesso a internet. Esta nova modalidade de comércio é conhecida por Comércio Eletrônico.

A sua crescente se dá no momento em que as pessoas vêem no computador não apenas mais um mero editor de texto, mas sim, uma necessidade cotidiana, seja para o trabalho, ou para a vida pessoal. As pessoas estão mais informadas e com menos tempo para sair de casa, o que faz com que peçam seus produtos ou serviços através da internet (SILVA, 2006, p.15).

O comércio eletrônico é uma forma de realizar transações de compra e venda na qual as empresas disponibilizam seus produtos para que possam ser conhecidos, avaliados, comparados e finalmente adquiridos pelos clientes. Todo este processo ocorre virtualmente, ou seja, por meio eletrônico.

Apesar de toda comodidade proporcionada por este meio, ainda há pessoas que não se utilizam do comércio eletrônico para realizarem suas compras. As razões são as mais variadas, desde falta de recursos, dificuldade na adaptação às mudanças, ou ainda por receio das ameaças que a internet pode trazer quando no exercício desta modalidade comercial, como, por exemplo, a violação, roubo e troca de dados dos usuários.

Em virtude dessas ameaças, o consumidor que realiza compras pela internet, primeiramente tem que verificar se o sistema dispõe de métodos de segurança, capazes de evitar que terceiros tenham acesso às informações confidenciais. Diante disso, vale destacar que o comércio eletrônico está voltado para segurança, não apenas para os consumidores, mas também para empresas. Uma das opções disponíveis para aumentar a segurança do comércio por meio eletrônico é uma técnica desenvolvida chamada Criptografia.

Neste sentido, é importante a colocação de Gregores (2006, p.81), que diz: “a criptografia é um dos métodos mais seguros colocados à disposição dos consumidores, para a transferência de informações pela rede, porque tem como base um processo de codificação secreta”.

Este trabalho tem por objetivo analisar a segurança e privacidade dos clientes, ao optar pelo comércio eletrônico para realizar suas compras e descrever as técnicas utilizadas pelo comércio eletrônico para proporcionar maior segurança, como a Criptografia, o Site Blindado e a Assinatura Digital, mostrando também as formas de pagamento e até que ponto as mesmas são seguras.

Pretende-se também, ao término deste trabalho, demonstrar na prática o funcionamento de uma compra eletrônica, através de um site, implementado na linguagem PHP, que é uma linguagem voltada para web.

A metodologia da pesquisa será qualitativa, de caráter exploratório, com levantamento bibliográfico, baseando-se em informações presentes em livros da área, pesquisas na internet, artigos, dentre outros.

2. REVISÃO BIBLIOGRÁFICA

O principal objetivo da Internet é proporcionar às pessoas o acesso remoto à informação. A rede das redes é considerada um sistema aberto que, por consequência, demanda por parte das organizações a preocupação de proteger os dados das pessoas que a utilizam.

A falta de segurança é citada como uma das maiores barreiras para a expansão e utilização do comércio eletrônico. Por meio de técnicas de segurança como a Criptografia, a indústria do comércio eletrônico tem acelerado nos últimos anos. O comércio eletrônico é baseado em computadores e redes, e estas mesmas tecnologias podem ser usadas para o "ataque" a sistemas de segurança (FILHO, 2000, p. 57-59).

A citação acima corrobora com a afirmativa de que a segurança é um dos principais itens investigados pelos clientes virtuais, quando têm interesse em fazer compras pela internet.

Ainda para Filho (2000, p.60) as pessoas de má índole têm o intuito de: “lograr algum benefício, lesar alguém ou mesmo conseguir publicidade própria”.

Assim, a falta de segurança acaba prejudicando os usuários da internet, que fazem uso dela seja para se comunicar, trocar informações, trabalhar ou fazer suas compras, dentre tantas outras atividades.

Filho (2000, p.59-60) destaca as principais conseqüências da insegurança no contexto do comércio eletrônico:

- Consumidores e fornecedores podem sofrer prejuízos monetários, e até serem acusados de crimes que não cometeram.
- O clima de insegurança na Internet faz com que muitas empresas existentes (ou prestes a existirem) não adquiram o negócio online.
- De igual modo, os consumidores, desconfiados, preferem não fazer compras online, não se beneficiando dessa facilidade de compra.

E para que essas conseqüências da insegurança não ocorram, o autor destaca que algumas técnicas, como por exemplo, a criptografia, devem ser utilizadas por empresas, para que se garanta a segurança de seus consumidores, impedindo que os dados armazenados em um computador, ou as transferências de mensagens, sejam acessados (lidos) ou comprometidos.

A maioria das medidas de segurança envolvem a encriptação, que é a transformação de dados para uma forma ilegível e não acessível, a menos que se tenha o respectivo mecanismo de decifragem (FILHO, 2000, p.60).

O fenômeno internet possibilitou aos empresários uma série de vantagens como: serviços disponibilizados 24 horas para os clientes, não havendo necessidade de fechar o comércio; a diminuição de mão-de-obra; a dispensa de local próprio e estruturado para atendimento ao público, sem pagamentos de aluguéis, impostos, dentre outros. Mas, junto com essas vantagens, surgiram preocupações como, por exemplo, transmitir confiabilidade aos consumidores, criar mecanismos de segurança, estabelecer métodos para recebimento de pagamentos etc (GREGORES, 2006, p.32-33).

A autora cita também a Criptografia como “um dos meios mais seguros, colocados à disposição dos consumidores, para a transferência de informações pela rede, porque tem como base um processo de codificação secreta” (GREGORES, 2006, p.81).

Na visão de Gregores (2006), as organizações estão preocupadas em como melhor atender aos clientes, priorizando a segurança, demonstrando confiabilidade para que possam fazer uso do comércio eletrônico através da internet, tendo como forma de segurança, a técnica da Criptografia, que é a mais utilizada nos dias de hoje.

Para Albertin (2010, p.205):

> A segurança dos sistemas on-line tem evoluído muito rapidamente, sendo que novas soluções técnicas têm surgido assim que novas estratégicas de comércio eletrônico têm sido implementadas. Dessa forma, a maioria dos

> sistemas de segurança é suficientemente boa para ser utilizada nas transações comerciais.

Algumas das maneiras pelas quais os problemas de segurança na internet se manifestam são:

- Bisbilhotice: os ataques de bisbilhotice na rede podem resultar no roubo de informações de contas, tais como números de cartões de crédito, número de contas de clientes ou informações sobre saldo e extrato de contas.
- Espionagem de senhas: esse pode ser utilizado para se obter acesso a sistemas nos quais informações proprietárias são armazenadas, sendo que o uso crescente de algoritmos fortes de criptografia tem inibido esse tipo de ataque.
- Modificação de dados: esses ataques podem ser utilizados para modificar os conteúdos de certas transações.
- Falsificação: os ataques de falsificação podem ser utilizados para permitir a uma parte mascarar-se como outra. Em tal situação, um criminoso pode estabelecer uma loja de fachada e coletar milhares de números de cartões de crédito, números de contas ou outras informações de clientes sem levantar suspeitas (Bhimani (1996 apud ALBERTIN, 2010, p. 205)).

Conforme os itens acima, podemos perceber o quanto é importante a implementação de sistemas de segurança, para que se possa garantir o sigilo das informações depositadas nos sites e que tais informações estejam protegidas de ataques como a bisbilhotice, roubo de senhas e adulteração de dados.

Infelizmente a internet não é um ambiente onde existem pessoas com intuito de utilizá-la somente para fins benéficos. Há também pessoas cuja intenção é interferir em comunicações e até mesmo roubar dados ou valores de outras pessoas (LARA, 2003, p.29).

O autor acima define a internet como um meio de comunicação, informação, entretenimento, e também, especialmente hoje em dia, um meio fácil e confortável de realizarmos compras no conforto de nossos lares. Porém, também ressalta que por toda esta comodidade, acabamos pagando um alto preço, pois ficamos

suscetíveis a pessoas com más intenções, os chamados *hackers*, indivíduos cuja intenção é cometer crimes através da internet.

Para Lara (2003, p.29): “esses indivíduos sabem que podem encontrar falhas nos sistemas de segurança e tem tempo disponível para viabilizar suas idéias. Deixando assim, muitas vezes, uma imagem de insegurança e total falta de privacidade na internet”.

Devido às ações dos *hackers* o comércio eletrônico está atento à segurança, um argumento importantíssimo para quem planeja investir no segmento ou transmitir confiança ao usuário. O uso da criptografia, já citada, e a manutenção do sigilo dos clientes, amparam não apenas os consumidores, mas também os comerciantes eletrônicos, evitando prejuízos de ambos.

Vale destacar a definição de Lara (2003, p.30) que diz: “implementar ferramentas que tornem o uso de transações na internet seguras, além de proteger o patrimônio próprio e o patrimônio dos clientes, é também uma forma de manter e conquistar novos clientes”.

Lara (2003, p.31) descreve que: “estas ferramentas podem, conjuntamente, desde que bem implementadas, garantir o sucesso das transações eletrônicas, afastando os *hackers* do conteúdo das informações que se deseja proteger”.

Além de utilizarmos a criptografia para maior segurança, temos também em mãos a técnica blindagem de sites, que, por sua vez, é efetuada através de uma empresa líder no Brasil e tem como especialização a segurança na *web,* conhecida por Site Blindado.

Essa empresa é responsável por realizar vários testes a fim de evitar roubos de informações ou clonagens de cartões de crédito. Após esses testes, o site estará liberado para mostrar aos seus clientes que possuí o selo “site blindado”, garantindo ao consumidor maior segurança ao efetuar suas compras.

A empresa Site Blindado, é uma das empresas que possui o maior sistema de segurança do mundo, que protege informações confidenciais em mais de 45 países. Após a empresa contratar os serviços do Site Blindado, são realizados vários testes contra invasão de *hackers* para verificar todas as vulnerabilidades de segurança.

Servidores certificados pelo Site Blindado estão prevenidos em 99,9% de crimes de invasão de *hackers* (HUGO; MICHEL; JANSEN).

Para que os usuários se sintam ainda mais confiantes para com esta área tecnológica que vem crescendo dia-a-dia, este segmento os apresenta a uma nova forma de assinar: a técnica conhecida por assinatura digital, que é baseada em um funcionamento complexo, que envolve uma série de funções matemáticas.

Com a assinatura digital, que tem como finalidade elevar a segurança do documento assinado, o usuário tem certeza de que o documento não será modificado sem deixar vestígios e o destinatário também poderá confiar que a mensagem é realmente proveniente de seu cliente (GANDINI; SALOMÃO; JACOB, 2001, p.16).

Dentre esses contextos de comércio eletrônico temos ainda suas formas de pagamento, que vêm a ser a finalização da compra, onde é escolhida a forma que mais agrada ao consumidor para efetuar a transação. Dentre estas formas temos: dinheiro eletrônico, cartões inteligentes, cartões de créditos e boleto bancário, cada uma trazendo sua comodidade, conforme a necessidade do usuário.

Vale destacar o que diz Gregores (2006, p.99) sobre as formas de pagamento: “da mesma maneira que a evolução tecnológica proporcionou uma corrida ao comércio eletrônico, a forma de pagamento nas relações por meio eletrônico também está se modernizando”.

Por meio de técnicas sofisticadas como a Criptografia, Sites Blindados, Assinaturas Digitais, dentre outras técnicas, esperamos que o comércio eletrônico torne-se uma forma segura de realizar compras *on-line*.

3. COMÉRCIO ELETRÔNICO

Há alguns anos, os meios de comunicação existentes para realizar uma compra ou venda eram o telefone, fax, rádio e televisão, que hoje caíram em desuso diante da possibilidade do comércio eletrônico virtual. No caso do telefone, a venda era feita através de uma exposição ou oferta oral, e, nos demais, o resultado da compra e venda ficava na dependência de uma resposta de um dos destinatários. Por meio do rádio ou televisão, o cliente gostando da oferta respondia por escrito, ou até mesmo por telefone, concretizando assim a sua compra. E também havia a opção por correspondência, onde o vendedor fazia suas ofertas utilizando catálogos e havendo interesse do comprador, fazia a sua encomenda via postal (GREGORES, 2006, p.56).

Com o passar do tempo e com o avanço da tecnologia, houve o aprimoramento dos meios de comunicação para a população em geral. Dentre essas novas formas e meios de comunicação, destacamos o surgimento da Internet, considerada hoje uma das formas mais populares de integração, entretenimento e comunicação da atualidade.

A internet foi criada pela *Advanced Research Projects Agency (ARPA).* Começou a ser desenvolvida nos Estados Unidos, na década de 60, na época da Guerra Fria. Seu nome na época era *Arpanet* e tinha como objetivo manter as bases militares sempre comunicadas. Sua utilização no início era para fins militares e a partir dos anos 70 passou a ser disponibilizada para a comunidade acadêmica mundial, até chegar ao meio social, transformando-se assim na maior rede de comunicações.

Segundo Gregores (2006,p.23):

> Entre a década de 80 e início dos anos 90, a rede foi aperfeiçoada e começaram a aparecer os serviços que dão à internet a feição atual, como a *word wide web (www)*, lançada em 1991, que viabiliza a transmissão de imagens,som e vídeo pela rede.

> No Brasil a internet começou a ser utilizada nas universidades e centros de pesquisa a partir de 1988.

A partir de então a sociedade ganhou um meio mais simplificado e popular de realizar uma compra ou venda; um meio que permite às pessoas compartilhar e trocar informações entre elas, além de ser uma ferramenta para apoiar o comércio eletrônico.

O comércio eletrônico, como é conhecida esta vertente virtual, trata da compra e venda de produtos ou da prestação de serviços, realizado por meio de um computador ou qualquer outro equipamento com acesso a internet, na qual as empresas disponibilizam seus produtos para que possam ser conhecidos, comprados ou vendidos.

Também inclui todos os tipos de esforços de pré-vendas e pós-vendas, em um conjunto de atividades auxiliares como anúncios, compras e distribuição de produtos, suporte aos clientes e transações financeiras (Applegate, L. M. et al.1996 apud Albertin, Alberto L, 1998, p.57).

3.1 MODALIDADES DE COMÉRCIO ELETRÔNICO

Podemos distinguir várias modalidades no comércio eletrônico, tais como: *Business-to-Business (B2B), Business-to-Consumer (B2C), Business to Government (B2G), Government to Consumer (G2C) e Consumer to Consumer (C2C)*, as quais podem ser definidas da seguinte forma:

3.1.1 Negócio-a-Negócio

A modalidade *Business-to-business*, mais conhecida como B2B é definido como o comércio eletrônico entre empresas.

As empresas se comunicam através de um meio eletrônico, como a internet, e entre elas são realizadas vendas e/ou compras de produtos.

3.1.2 Negócio- a-Cliente

Outra modalidade do comércio eletrônico é *Business-to-consumer* mais conhecido como B2C.

O conceito do B2C é a comunicação da empresa e o consumidor final, é realizado através da internet no site de uma determina empresa, que começa na escolha de produtos ou serviços e a entrega do mesmo.

Nesta modalidade a empresa tem o dever de manter seguras as informações dos clientes através de técnicas, dentre elas a criptografia, que será explicada mais a frente. Quanto ao cliente, nesta modalidade, ele tem a expectativa de receber o produto em ótimas condições.

3.1.3 Negócio-a-Governo

O conceito de *Business to Government* conhecido como B2G é o comércio feito entre um meio público e empresas onde é disponibilizado via internet editais de licitações e pregões para compra de produtos e serviços.

3.1.4 Governo-a-Consumidor

Temos ainda a modalidade *Government to Consumer* conhecida como G2C, é o comércio feito entre governo e consumidor. Sendo feitos pagamentos como impostos e multas através da internet.

3.1.5 Consumidor-a-Consumidor

E por fim, a modalidade *Consumer to consumer* mais conhecida como C2C que é o comércio eletrônico entre consumidores. Denominado como a “terceira onda” do comércio eletrônico, sendo a primeira entre empresas, a segunda entre empresa e consumidor e agora a interação entre pessoas físicas. A maior representação do C2C são os leilões virtuais, nos quais a empresa não tem o contato diretamente com o consumidor, ela apenas dispõe sua infra-estrutura tecnológica e administrativa.

3.2 IMPACTOS DO COMÉRCIO ELETRÔNICO NA SOCIEDADE

O comércio eletrônico surgiu com a evolução da internet e acabou modificando o modo de agir das pessoas em relação às compras, proporcionando uma forma ágil e prática de realizá-las. Sua tendência é crescer a cada dia, pois a Internet nunca deixará de evoluir.

Hoje, o comércio em geral está migrando para a rede e acredita-se que é uma das melhores fases de mudança estrutural na sociedade. Na verdade, é a formação de uma nova sociedade: a Sociedade da Informação. Estamos na Era da Digitalização, cujos processos fazem parte de quase todas as atividades do dia-a-dia de pessoas e profissionais em geral. Pode-se perceber facilmente essa evolução, pois deixamos de escrever cartas, utilizar agendas, assim como se tornou obsoleto o uso papel e caneta para anotações, o dinheiro para transacionar mercadorias foi substituído por informações de débito e crédito em contas e cartões (LUPPI, 2009).

De acordo com os dados publicados na 22ª edição do Relatório *WebShoppers*[1] elaborado pela *E-bit*,[2] com o apoio da Câmara Brasileira de Comércio Eletrônico[3], o faturamento para os primeiros seis meses deste ano foi de R$ 6,7 bilhões. Esse valor representa um aumento nominal de 40% em relação ao primeiro semestre de 2009, quando registrou R$ 4,8 bilhões. As categorias de produtos mais vendidos podem ser observadas na Tabela 1.

Categorias de produtos mais vendidas – 1°Semestre 2010	
Livros e Assinaturas de Revistas e Jornais	1°
Eletrodomésticos	2°
Saúde, beleza e medicamentos	3°
Informática	4°
Eletrônicos	5°

Tabela 1- Categorias de produtos mais vendidas – 1°Semestre 2010 (Fonte: Relatório WebShoppers apud e-bit Informação (www.ebitempresa.com.br))

A 22ª edição do Relatório *WebShoppers* declara que: “até o primeiro semestre de 2010, foram 20 milhões de pessoas que compraram pela internet ao menos uma vez, na metade do ano passado, eram 17,6 milhões de usuários. Até o final do ano, esse número deverá alcançar 23 milhões”.

---

[1] *WebShoppers* - Analisa a evolução do comércio eletrônico, as mudanças de comportamento e preferências dos consumidores.

[2] *E-Bit* - Empresa que gera diariamente informações detalhadas sobre o comércio eletrônico.

[3] Câmara Brasileira de Comércio Eletrônico - missão de capacitar indivíduos e organizações para a prática segura dos negócios eletrônicos.

Ainda segundo o relatório *WebShoppers:*

> Com a forte movimentação nos primeiros seis meses, o setor caminha para mais um recorde de faturamento. No 2º semestre de 2010, espera-se que as lojas virtuais alcancem R$ 7,6 bilhões em vendas de bens de consumo, exceto vendas de automóveis e sites de leilão virtual. Dessa forma, espera-se um faturamento de R$ 14,3 bilhões ao final de 2010, que representaria um crescimento nominal de 35% se comparado ao resultado de 2009, quando o setor faturou cerca de R$ 10,6 bilhões.

O comércio eletrônico veio para ficar e, como qualquer outra atividade, trouxe evidentes vantagens se compararmos esta com as formas de transação tradicionais. (RUIZ; LOURENÇO; FREITAS; GENEOLE; TABUTI; 2000).

A facilidade de uso do comércio eletrônico é uma vantagem, pois é disponível a todos, a qualquer hora do dia ou da noite, bastando ter acesso à internet. Tendo a possibilidade de efetuar pesquisas de preços de todas as lojas de sua preferência e assim escolher o produto de melhor qualidade e preço que desejar.

Seu processo para concretizar compras é simples, basta escolher o produto de sua preferência e em seguida seguir os passos que a empresa determinar no site, como: confirmação de dados pessoais, informação de endereço de entrega do produto comprado, escolha das possibilidades de forma de pagamento, etc.

O ponto forte é que não é necessária a locomoção do interessado até a loja específica no momento da compra e lá ficar esperando por alguns minutos até que um vendedor esteja disponível para atendê-lo. Na loja real, muitas vezes não temos o desfrute de observar todos os detalhes que realmente desejamos, ou por falta de interesse do vendedor, ou mesmo pela pressa do dia-a-dia.

Com todas essas evidências, podemos perceber o quanto é importante a atualização na questão da compra e venda eletrônica. A facilidade e a aceitação desta tecnologia a tornou bem sucedida.

Entretanto, para algumas pessoas, este avanço tecnológico passa despercebido, seja por falta de recursos, seja por não se adaptarem às novas mudanças e assim não saberem utilizar os meios eletrônicos. Estas pessoas ficarão de fora das

facilidades proporcionadas pela compra eletrônica. A aquisição do equipamento necessário para realizar as compras também pode ser o empecilho para algumas delas, além do fator segurança, pois o interessado deverá disponibilizar no site seus dados pessoais, suas informações mais importantes, o que, muitas vezes, inviabiliza o desfrute dessa tecnologia devido ao medo das ações dos hackers.

Com relação à segurança de informações, deve-se procurar sites seguros, para que assim seja possível realizar cadastros via internet. Para que tal ato seja confiável, existem técnicas como a criptografia e sites blindados, que explanaremos mais detalhadamente adiante no trabalho.

4. SEGURANÇA DAS INFORMAÇÕES

A segurança em transações eletrônicas é um dos aspectos de maior preocupação de todos os envolvidos com o comércio eletrônico. Preocupados com a privacidade dos dados pessoais e o sigilo das informações como nome, telefone, e-mail, endereço, etc., alguns clientes tentam resistir ao fornecê-los para determinado site, pensando na possibilidade de que as informações possam ser alteradas por alguns “piratas eletrônicos”.

A falta de confiança dos consumidores é outro ponto do comércio eletrônico que se manifesta em questões relativas à segurança dos sistemas deste comércio. Existe a percepção entre os consumidores de que as redes de computadores estão sujeitas a ataques constantes de pessoas ou grupos interessados em roubar ou adulterar informações. Apesar de essa percepção poder ser considerada exagerada, ela existe e deve ser levada em conta. Além disso, a facilidade de se criarem empresas em qualquer lugar e vender produtos para o mundo todo implica no risco de um consumidor transacionar com uma empresa virtual que desapareça assim que recolhe o seu dinheiro (Kline(1995 apud Diniz, Eduardo H,1998)).

Tais preocupações e falta de confiança são transmitidas pelas ações dos *hackers*, infratores virtuais que driblam até mesmo programas eficientes de proteção, circulando pela rede, até conseguirem ter acesso aos dados pessoais dos clientes tais como: e-mails, senhas, número de cartões de crédito, número de conta corrente ou até mesmo para testar a segurança de sistemas. Com essas informações podem ser feitas várias operações, como sacar dinheiro, fazer transferências de valores, espionar informações, dentre outras.

Segundo Gregores(2006, p.74):

> O sucesso do comércio eletrônico depende, necessariamente, da confiança depositada na rede e, para que ela exista, se faz necessário que os consumidores se sintam seguros para realizar transações eletrônicas,

> devendo, portanto, as empresas que visam obter lucro pela internet, cuidar para que as suas transações não sejam interceptadas ou mesmo alteradas e buscar um nível de segurança cada vez mais confiável e menos falível.

Entretanto, a segurança tem se aprimorado, pois o interesse da melhoria é de ambas as partes, tanto para consumidor, quanto para vendedor e para que os clientes se sintam à vontade e se beneficiem da facilidade de compra, que é o comércio eletrônico, devemos então garantir a segurança na internet através de alguns conceitos como: confidencialidade, autenticação, integridade e não repúdio.

O conceito da confidencialidade deve garantir que os conteúdos das informações fornecidas nas transações eletrônicas estejam protegidos de pessoas que não estão autorizadas a recebê-las. Deve-se manter o sigilo de informações como: valores, números de contas ou cartões.

Já a autenticação é responsável por identificar os usuários, que neste caso devem garantir autenticidade de ambas as partes envolvidas. Assim, garante que a informação que se está passando, seja para o destinatário correto e não para um impostor e que a mensagem que o destinatário receberá seja a mensagem original.

No quesito integridade, é garantido que as informações cadastrais não sejam modificadas durante a transmissão e que sejam entregues no destino correto.

Para o entendimento do conceito de não-repúdio, é necessário primeiramente que este seja definido, para que o termo seja entendido completamente.

Para Lara (2006, p.27), “repúdio é o fato de se negar a participação numa determinada operação. O problema realmente surge se a negativa, ou seja, o repúdio, acontecer sobre uma operação que de fato ocorreu”.

No comércio virtual, assim que realizada a transação, tanto o comprador quanto o vendedor, não podem negar sua participação na mesma.

Podemos concluir neste capítulo que a segurança das informações no comércio eletrônico é mesmo essencial. E para que seja aumentada e os clientes se sintam mais à vontade para utilizar o comércio eletrônico, várias técnicas estão sendo empregadas por fornecedores, entre elas, a já citada Criptografia, que estudaremos com mais detalhes no próximo capítulo. Porém, além da Criptografia, podemos

destacar ainda como outras formas alternativas de segurança o chamado Site Blindado, também bastante usado por empresas na internet.

5. CRIPTOGRAFIA

A técnica da Criptografia existe há muito tempo. A palavra Criptografia tem sua origem nas palavras gregas *kryptós* e *gráphein*, que significam escondido e oculto respectivamente, sendo a técnica de segurança mais conhecida mundialmente.

Com o surgimento da internet, se fez necessário implementar alguma ferramenta para garantir as transferências de dados na rede. Assim começou a ser utilizada a Criptografia, para que os dados sigilosos fossem enviados e recebidos devidamente. A Criptografia torna as informações ilegíveis, permitindo que consumidores e vendedores troquem informações de forma mais segura, dificultando assim o acesso aos dados por pessoas de má índole.

Segundo Albertin (2010, p.217):

> A criptografia é definida como a arte ou a ciência de escrever em cifra ou em códigos, ou ainda, como o conjunto de técnicas que permitem tornar incompreensível uma mensagem originalmente escrita com clareza, de forma a permitir que somente o destinatário a decifre e a compreenda.

A tarefa da criptografia é transformar arquivos legíveis em algo incompreensível para pessoas não detentoras de uma chave de decodificação pré-determinada deste arquivo. Por exemplo, suponha que o seu material sigiloso se pareça com isso:

“O comércio eletrônico é uma forma de realizar compras pela internet, onde você pode pesquisar preços de todas as lojas que desejar e assim poderá concretizar a compra com sucesso.”

-Eis como o texto acima ficaria, na forma criptografada:

G?SdJt:1/41Y18’1Y gmdcA#[< b:vR- o UGO>e’Q V , < loj’UtLO_”G

Ris6&igy £u&_a7AFT1=0_. . A’’ –R81~ykh . . . o2ii?itr0(trn) trv6R1 ‘ i ,,

(04; _U6R’ Q3 /4V6 – A#Au&-9f > FemB06_c&&B1 /28#uh& [G [gh_l

>%=Gmdtn* b81/.

Mesmo que o invasor obtenha o conteúdo do arquivo, ele é ilegível. O segredo ainda é secreto. (BURNETT,PAINE, 2002, p. 8).

Para passar segurança aos clientes ao fornecer dados que serão transmitidos pela rede, existem três serviços da criptografia:

- Confidencialidade: tem como objetivo proteger informações, como números de cartões de crédito, senhas, uma vez que ambos são extremamente sigilosos, e que essas informações não sejam entregues a pessoas não autorizadas, que possam fazer cópias ou leitura destas.
- Integridade: garante que o conteúdo da informação não seja alterado durante seu percurso. É necessária a prevenção das modificações de dados que incluem gravação, alteração ou remoção dos mesmos.
- Autenticidade: é necessário que o usuário se autentique para o sistema, o sistema para o usuário e que ambos se autentiquem entre si. No processo da autenticação, esta identifica a entidade (usuário ou sistema) através de informações criptografadas transmitidas entre destinatário e receptor.

Os primeiros métodos existentes na criptografia são conhecidos como: cifra de substituição e cifra de transposição. O primeiro deles substitui cada letra ou grupo de letras por outra letra ou conjunto de letras, as letras são modificadas, mas a ordem é a mesma. Já a cifra de transposição troca caracteres do mesmo texto, de posição. Ambos os métodos são fáceis de serem decifrados.

A criptografia é uma técnica muito antiga, como já dito, e hoje muito mais eficiente do que nos tempos passados. Com seu crescimento e uso diário surgiram dois tipos de criptografia: simétrica e a assimétrica, que serão explicadas mais adiante. Ambas trabalham com o conceito de chaves.

Na Criptografia, para proteger o conteúdo dos seus arquivos, é instalada uma fechadura (um algoritmo de criptografia) na sua porta (o computador). Para operar a fechadura (encriptar os dados), você insere a chave (o número secreto) e a executa

(em vez de girar essa chave, você opera o programa dando um clique duplo, clicando em OK ou pressionando Enter). O algoritmo realiza seus passos utilizando a chave para alterar o texto simples e convertê-lo em texto cifrado. Para desbloquear o arquivo encriptado, você insere a mesma chave e executa. O algoritmo inverte os passos e converte o texto cifrado de volta no texto simples original. Assim como apenas a chave correta da casa pode abrir a sua porta de entrada, apenas a chave de criptografia correta pode decriptar os dados (BURNETT, PAINE, 2002, p. 16).

A utilização de chaves é um método mais seguro do que somente algoritmos, pois no uso apenas do algoritmo, pessoas com má intenção poderão decifrá-lo e assim ter acesso a todas as informações. Com as chaves, pode-se utilizar várias delas para proteger diferentes informações, assim, se um impostor conseguir ter acesso a uma das chaves, as outras informações estarão seguras.

As chaves são calculadas através de número de bits, tais como: 8bits, 64 bits, 128 bits, etc. Por exemplo: se o valor de uma chave corresponde a 8 bits, este valor deverá ser elevado ao quadrado, ou seja 8^2, no qual o resultado será 256. Este valor representará o total de chaves possíveis para a decodificação, que por sinal, é um número pequeno e que poderá ser facilmente decifrado por alguém que tenha tempo para fazer combinações. Conclui-se então que, quanto maior for o número de bits, maior será a segurança da Criptografia.

Este é o conceito de chaves e para que fique mais claro e se entenda melhor, veremos a seguir duas subdivisões importantes, a Criptografia Simétrica e a Assimétrica.

5.1 CRIPTOGRAFIA SIMÉTRICA

É a mais comum das Criptografias e também conhecida como Criptografia de Chave Privada ou Chave Secreta. Esta técnica trabalha apenas com uma única chave, sendo que o emissor a usa para cifrar a mensagem e o receptor para decifrá-la. E para concretizar a transmissão das mensagens, o emissor e o receptor devem possuir o algoritmo da mensagem. Mesmo que o intruso venha a conhecer o

algoritmo, ele não conseguirá decifrar a mensagem, pois não possuirá a chave. Uma desvantagem desta técnica é que ela faz a distribuição de chaves e ambas as partes recebem a mesma chave e assim aumentam as chances de quebra das informações enviadas. O processo da chave simétrica pode ser visualizado na

Figura 1, onde o algoritmo de encriptação usa uma única chave para converter o texto simples em texto cifrado e vice-versa.

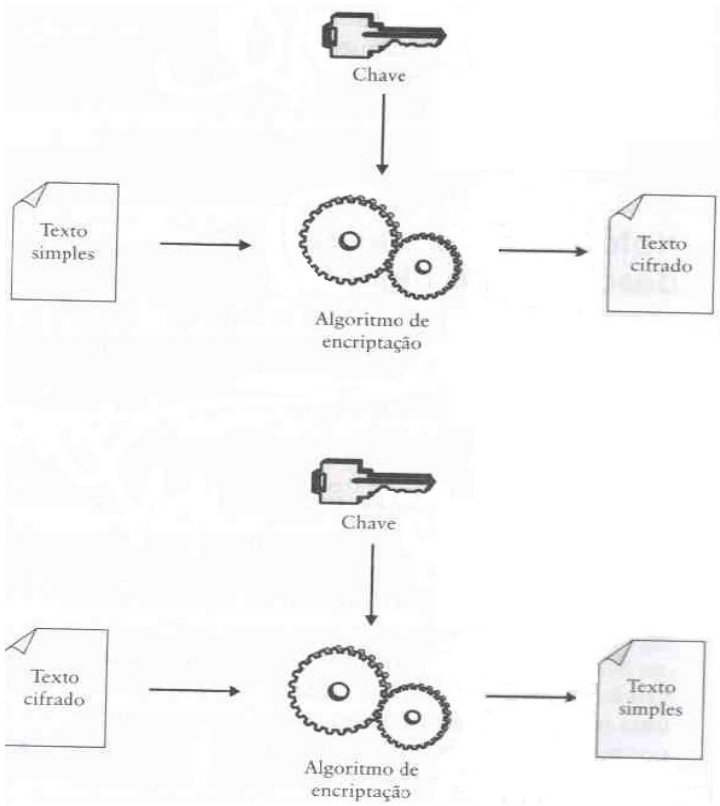

Figura 1- Processo de criptografia simétrica (Fonte: BURNETT,PAINE, 2002, p. 17)

5.1.1. Algoritmos para chave simétrica

Nesta seção serão apresentados os algoritmos: *Data Encryption Standar* (DES) e suas novas aplicações que foram surgindo como: DES Duplo, DES Triplo. Também

será apresentado o algoritmo: International Data Encryotion Algorithm (IDEA). Logo são algoritmos para chave simétrica que serão esclarecidos a seguir.

5.1.1.1 - *Data Encryption Standar (DES)*

Existem vários algoritmos que usam chaves simétricas, como o *Digital Encryption Standard – DES*. Este algoritmo nasceu de um esquema chamado Lucifer, inventado pelo criptógrafo *Horst Feistel* com a ajuda da *National Security Agency (NSA)* agência responsável por manter em sigilo as informações secretas do governo dos Estados Unidos e com pesquisadores da IBM na década de 70. Utiliza chaves de 56 bits que correspondem a 72 quatrilhões de combinações, um valor extremamente alto na época e que nenhum computador conseguia decifrar uma mensagem.

Com o passar do tempo este algoritmo foi ficando fraco e não podia ser utilizado para transitar informações muito importantes, até que em 1999 ele foi quebrado por técnicas de força bruta. Porém, para o aperfeiçoamento do DES, foram surgindo novas aplicações como:

- DES Duplo: um algoritmo que realiza duas vezes o algoritmo DES, utilizando duas chaves distintas, que por sua vez se mostrou inseguro.
- DES Triplo: esse realiza três vezes o algoritmo DES, com três chaves de 56 bits cada. Desta forma, para o invasor conseguir decifrá-las terá que descobrir os valores corretos das mesmas, para que assim tenha acesso aos dados (BURNETT, PAINE, 2002, p. 40,41).

Na Figura 2 podemos ver um exemplo onde o impostor conseguiu detectar apenas o valor da primeira chave, não logrando êxito, pois o texto simples correto somente aparecerá quando todas as três chaves forem corretas.

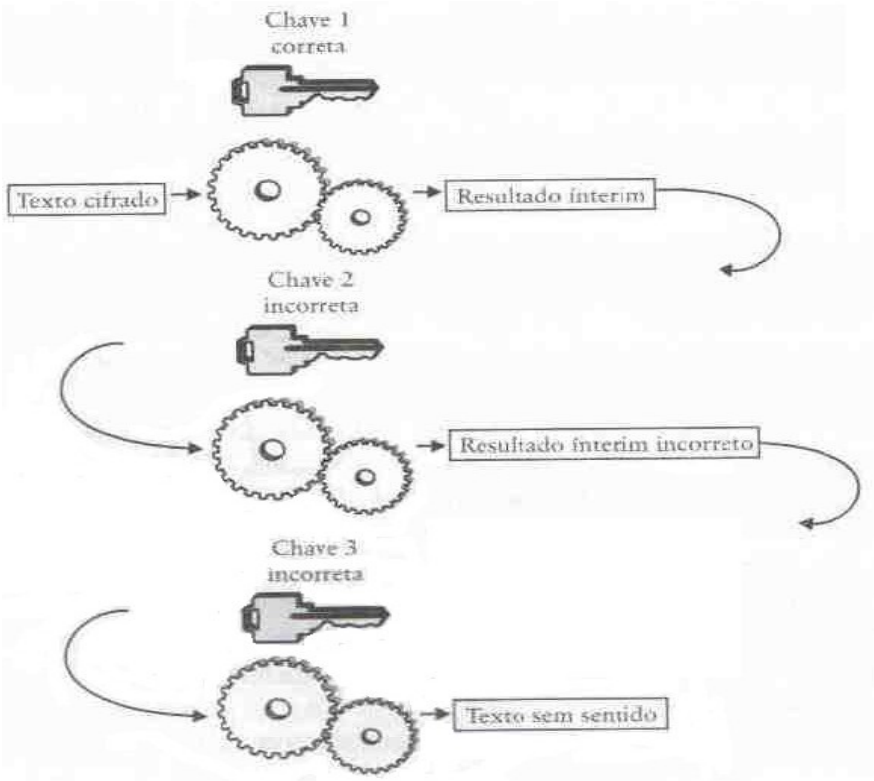

Figura 2- Processo do algoritmo DES Triplo (Fonte: BURNETT, PAINE, 2002, p. 42)

5.1.1.2 - *International Data Encryotion Algorithm (IDEA)*

O algoritmo IDEA foi criado em 1990 por *Lai* e *Massey*, usado também no processo de Criptografia Simétrica.

Segundo Filho (2000, p. 74), “este algoritmo utiliza chaves de encriptação com um tamanho de 128 bits, o que o torna substancialmente mais resistente a ataques do que o DES”.

5.2 CRIPTOGRAFIA ASSIMÉTRICA

Outro método conhecido é a criptografia assimétrica ou também chamada de chave pública, tal método trabalha com um par de chaves, sendo elas, pública e privada.

A Criptografia Assimétrica foi criada em 1976 por *Whitfield Diffiee Martin Hellman*, para contornar o problema da criptografia simétrica, que utilizava uma mesma chave para codificar e decodificar dados.

Vejamos um exemplo de seu funcionamento: imaginemos duas pessoas querendo se comunicar, Alice e Tiago. Bem, Tiago deseja se comunicar com Alice de forma segura e gera uma chave de ciframento (conta de e-mail), que é a sua chave pública e que qualquer pessoa pode obter uma cópia dela. Gera também a sua correspondente, a chave de deciframento (senha), mantendo-a segura, que recebe o nome de chave privada. Quando Alice deseja enviar uma mensagem a Tiago, precisa primeiro encontrar a chave pública dele. Feito isto, ela cifra sua mensagem utilizando a chave pública de Tiago, despachando-a em seguida. Quando Tiago recebe a mensagem, ele a decifra com sua chave privada. O intruso não tem conhecimento sobre a chave privada de Tiago, embora conheça sua chave pública, mas apenas com ela não consegue decifrar a mensagem. Mesmo Alice, que foi quem cifrou a mensagem com a chave pública de Tiago, não pode decifrá-la agora (LARA, 2003, p.66,67).

O sistema de Criptografia Assimétrica pode fazer uso da assinatura digital que autentica o emissor. Pois apenas o emissor, o proprietário, faz uso exclusivo de sua chave privada, constando nela o documento e sua assinatura digital. Assim, o destinatário verifica de quem veio a mensagem através da chave pública disponibilizada pelo proprietário.

A vantagem da Criptografia Assimétrica é a utilização de duas chaves que servem para encriptar e decriptar as informações, sendo que uma delas pode ser a privada, que o proprietário utilizou para encriptar as informações. Diante disso, só a chave pública poderá decriptá-las, ou vice-versa, sendo este o método mais seguro, onde o proprietário mantém as informações em sigilo e de uso exclusivo dele.

5.2.1. Algoritmo para chave Assimétrica

Nesta seção será apresentada apenas um único algoritmo de chave assimétrica, que é conhecido por *Rivest-Shamir-Adleman Algorithm(RSA)* e que será esclarecido a seguir.

5.2.1.1 - *Rivest-Shamir-Adleman Algorithm(RSA)*

Segundo Albertin (2010, p.218), “este algoritmo foi desenvolvido em 1977 por *Ron Rivest, Adi Shamir e Leonard Adleman*”. Tais sobrenomes representam a sigla do algoritmo RSA.

“O sistema de RSA utiliza um par casado de chaves de criptografia e decriptografia, cada uma desempenhando uma transformação de uma direção dos dados” (ALBERTIN, 2010, p.218).

Complementando seu conceito, o RSA permite assinaturas digitais, as quais fazem a autenticação de documentos eletrônicos e verificação do emissor, garantindo assim, a não-repudiação.

6. SEGURANÇA NO COMÉRCIO ELETRÔNICO

As lojas virtuais precisam deixar claro para seus clientes sua política de trocas e devoluções e também que se tiverem problemas com o produto, que o mesmo será resolvido. Essas medidas devem ser tomadas, para que consigam conquistar clientes no tão vantajoso e rentável meio eletrônico. Além das medidas apresentadas, outra de importância superior e a mais procurada pelos potenciais clientes virtuais é a Segurança. As lojas investem em segurança nos sites e mostram seus selos de proteção contra *hackers*, para que os clientes se sintam seguros no momento de efetuar suas compras.

Além dos itens citados, outros ainda são recomendados, como por exemplo, quais os passos a seguir para realizar sua compra, investigar se a loja possui alguma certificação de segurança, verificar quais os comentários sobre a loja virtual, opiniões de outros consumidores, classificação do seu atendimento, entre outras coisas. Verificamos assim que com o crescimento do comércio eletrônico e o aumento de seus usuários, a segurança é o item mais importante e de maior investimento.

Segundo Carneiro “foi realizada uma pesquisa pela empresa Site Blindado[4], onde diz que as vendas aumentam entre 12% e 15% por conter o selo de segurança”. Assim percebemos que a segurança chega a um ponto em que muitas vezes demonstra ser mais importante do que o preço do produto.

Ainda para Carneiro (2010):

> Foi realizado um estudo através da empresa Site Blindado com quatro mil internautas, onde aponta que para 30% o fator segurança inibe as compras online. O medo de não receber o produto é o principal motivo

[4] Empresa Site Blindado - Especialização em segurança da *web.*

> para 18%. Possíveis problemas com troca dos produtos (16%) e consumidores que não querem pagar frete (15%) completam a lista.

O que mais persegue os consumidores na hora de finalizar uma compra é o receio de digitar os dados de cartão de crédito, pois *hackers* poderão cloná-lo e causar-lhes prejuízos.

Segundo Carneiro (2010) “foi realizada uma pesquisa pela 15ª Edição do Relatório Global de Ameaças à Segurança na Internet da *Symantec*[5], onde o Brasil foi citado como sendo o terceiro país no mundo com o maior número de fraudes online”.

Em um ambiente que proporcione maior segurança, os consumidores têm mais confiança em realizar suas compras pela internet. Outras opções de segurança ainda podem ser citadas como é o caso da empresa chamada Site Blindado, que utiliza ferramentas que alertam aos consumidores se determinado site é seguro ou não. E para que fique mais claro o entendimento das ferramentas proporcionadas pela empresa Site Blindado serão apresentadas a seguir algumas informações complementares.

6.1 BLINDAGEM DE SITE

A empresa Site Blindado S/A, fundada em 2005, é líder no Brasil e tem como especialização a segurança na *web*. A empresa emite uma certificação (Selo “Site Blindado”), responsável pela blindagem das informações da loja virtual, o que passa mais confiança aos consumidores, para que possam digitar informações pessoais, números de cartão de crédito e assim finalizar uma compra via internet. Esta certificação pode ser observada na Figura 3.

---

[5] *Symantec* - *E*mpresa que oferece segurança, armazenamento e soluções de sistemas de gestão para ajudar os clientes a proteger e gerenciar seu mundo de informação dirigida contra riscos.

Figura 3- Selo Site Blindado

Segundo Carneiro (2010):

> A empresa realiza milhares de testes todos os dias, analisa vulnerabilidades em aplicações *web*, simula ataques de *hackers* para garantir que todas as possibilidades de ataques reais, roubos de informações ou clonagens de cartões de crédito sejam eliminadas. O Selo Site Blindado fica visível somente se o site do cliente passar em todos esses testes.

A empresa Site Blindado S/A faz uso de duas técnicas desenvolvidas por ela para alertar sobre a segurança, a chamada Site Blindado Alerta e a Certificação SSL/EV, que são apresentadas a seguir.

6.1.1 Site Blindado Alerta

A empresa Site Blindado desenvolveu uma ferramenta chamada Site Blindado Alerta, que foi lançada em julho de 2010. Trata-se de uma ferramenta gratuita que ao ser instalada no computador, permite aos consumidores, por meio do seu navegador de internet (*Internet Explorer* ou *Firefox*), visualizar se o site que pretende-se realizar uma compra é um site blindado contra *hackers* ou não. Se, ao acessar um site o selo Site Blindado ficar visível na barra do seu navegador, então é porque o site é garantido por segurança, conforme apresentado na Figura 4.

Figura 4 – Site Blindado Alerta

E essa visualização não é disponível pelo site e sim pela ferramenta instalada no computador do consumidor. Quando algum site aparecer com o selo Site Blindado transparente é porque o mesmo não é blindado pela empresa Site Blindado.

Essa nova ferramenta verifica nos portais de busca se determinado site de uma loja pertence ao selo Site Blindado sem ao menos clicar no link, pois ao lado do nome do site pesquisado já aparece se a loja traz segurança.

Podemos perceber esse recurso da ferramenta na Figura 5, onde foi realizada uma pesquisa pelo *Google* e os sites que fazem parte do Selo Site Blindado foram mostrados na pesquisa.

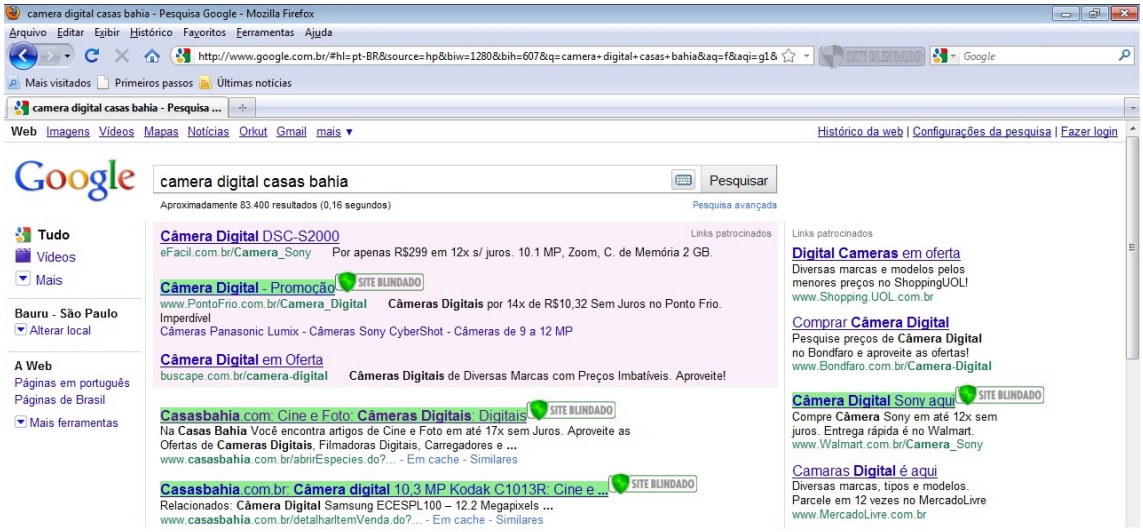

Figura 5 – Site Blindado Alerta, pesquisa *Google*

6.1.2 Certificação SSL – EV

Uma outra ferramenta de segurança desenvolvida pela empresa Site Blindado é a chamada SSL Blindado, que trata de um certificado digital. A sigla SSL significa "*Secure Socket Layer"*, em português, "Camada de Conexão Segura".

Carneiro (2010) esclarece que:

> O certificado SSL é um protocolo que provê a privacidade e a integridade de dados de aplicações que estejam se comunicando pela Internet, ou seja, todos os dados transmitidos passam por um processo de criptografia, que é uma codificação que somente pode ser decifrada pelo site acessado. Desta forma, se tal informação for interceptada na Internet, ela estará codificada e será impossível decifrá-la.

Esta é responsável também pelo aparecimento da figura de um cadeado, na qual, ao seu lado, pode ser visto o nome da empresa no seu navegador de internet e também trás a mudança do endereço de "http" para "https", onde a letra "s" significa segurança.

Este serviço é aplicado na *web* e permite que as informações digitadas que não estão protegidas, como senhas, cadastros, entre outras, não sejam roubadas pelos *hackers* no momento do tráfego pela rede. A prática de ficar constantemente verificando dados pela rede, com o propósito de bisbilhotá-los ou roubá-los, recebe o nome de *Sniffing*. Atualmente, o *sniffing* tem acontecido com grande freqüência, e o serviço de SSL tem se mostrado eficiente em seu combate.

Entretanto, o SSL não tem conseguido combater uma outra prática, até mais perigosa, chamada *Phishing*, que segundo Barreto "corresponde ao roubo de informações por meio de páginas falsas sobrepostas em um site real". Sendo assim, outro serviço de proteção foi criado para combater o *phishing* que é o SSL EV, onde EV significa "*Extended Validation"*, em português, "Validação Estendida". Essa nova certificação SSL EV faz uso de um processo mais rígido no qual a barra de endereços do navegador muda para verde.

Para Barreto (2010): “Empresas interessadas nesta certificação terão que passar por um processo de análise criterioso e ser aprovada em todos os quesitos”. A Figura 3 mostra o serviço do SSL EV, onde ao ser acessada uma página blindada, será solicitada ao usuário uma senha para prosseguir. Outra verificação é que o navegador da internet é destacado em cor verde e o endereço HTTPS e a figura do cadeado são mostrados. Com essas medidas, portanto, é possível combater as práticas *Phishing* e *Sniffing*.

Figura 6 – Certificação SSL EV

Segundo Carneiro (2010) “esta tecnologia já está amplamente difundida nos Estados Unidos e, no Brasil, esse movimento já se iniciou. Grandes empresas como iCarros (grupo Itaú), Corretora Ágora (Bradesco) entre outros já são usuárias do certificado SSL, com a tecnologia EV”.

Com a certificação SSL EV podem ser combatidas duas práticas, pois as informações depositadas no site ficam criptografadas no momento do tráfego pela rede. Porém, tais medidas não garantem a total segurança de um site, sendo necessário ainda proceder à blindagem do site, a qual garantirá que os dados armazenados estejam totalmente seguros, através do selo Site Blindado.

6.2 ASSINATURA DIGITAL

A assinatura digital é aplicada em documentos digitais, também conhecidos por documentos eletrônicos, da mesma forma que as assinaturas comuns, contendo nome completo ou abreviado são utilizadas para documentos impressos. Ambas as assinaturas só existiram através de um documento onde haja alguma declaração de sua concordância para que assim possam conter suas assinaturas de forma tradicional ou digital, logo será garantida à autenticação da assinatura.

Podemos conceituar o documento digital ou eletrônico como sendo o que se encontra memorizado em forma digital, não perceptível para os seres humanos senão mediante a intermediação de um computador. Nada mais é do que uma seqüência de bits, que por meio de um programa computacional, nos mostrará alguma informação (GANDINI; SALOMÃO; JACOB).

“A assinatura digital tem a função de lacrar o conteúdo do documento, fazendo com que este permaneça íntegro, ou se for minimamente alterado, que isso possa ser constatado” (GANDINI; SALOMÃO; JACOB, 2001, p.11).

A assinatura digital é reconhecida por passar um alto grau de segurança aos documentos assinados, utilizando da tecnologia denominada criptografia assimétrica ou também conhecida por chave pública, que trabalha com um par de chaves, sendo elas públicas e privadas.

Segundo Nogueira (2008, p.175-176):

> A assinatura digital é baseada em sistemas criptográficos composto de um algoritmo ou série de algoritmos, mediante o qual é gerado um par de chaves assimétricas exclusivas e interdependentes, uma privada e outra pública, e que permite ao proprietário usar a chave privada para declarar a autoria do documento eletrônico e permite ao destinatário usar a chave pública correspondente para verificar se a assinatura foi criada mediante o uso da chave privada.

Para assinaturas digitais é inviável o uso apenas de algoritmos de chave pública, pois eles apresentam lentidões, principalmente quando se pretende assinar mensagens que contem um texto maior, que pode demorar muito para ser cifrado pela chave privada, trazendo assim um desempenho não satisfatório. Para que isso não ocorra é utilizado a função Hash, que realiza um resumo de mensagens. A seguir um exemplo para exemplificar tal função:

Mensagem 1: Antonio vai comprar 2 livros no site LAsRI Lojas amanhã.

Resumo da mensagem :

66 37 5a 58 98 ab 68 85 44 ca b5 8e 84 a7 dc 21

36 8f lc a5

Mensagem 2: Antonio vai comprar 3 livros no site LAsRI Lojas amanhã.

Resumo da mensagem:

c2 bd 87 83 78 e7 3d el 92 81 94 0a 16 7b 14 18

c3 6b 09 a7

No exemplo acima foi utilizado em cada mensagem 53 bytes de comprimento sendo que cada letra, espaço e pontuação valem um byte e os resumos das respectivas mensagens valem 20 bytes sempre apresentados aleatoriamente. Para cada mensagem que for digitada, não importa quantos bytes terá, o seu resumo será de 20 bytes oferecendo assim agilidade nas assinaturas digitais e uma integridade confiável. Percebe-se que a mensagem 1 e a mensagem 2 têm uma pequena diferença e mesmo tendo essa diferença que é apenas um byte, o resultado do resumo foi aleatório e diferente.

Para complementar esse estudo Burnett &Paine (2002, p.121) descrevem que a função Hash é:

> Um algoritmo que recebe qualquer comprimento de entrada e mescla a entrada para produzir uma saída pseudo-aleatório de largura fixa. Onde a palavra Hash pode significar desordem ou confusão, que descreve eficientemente o resultado de um resumo de mensagens.

Como já citado, a assinatura digital não é muito viável apenas com algoritmos de chaves assimétricas, mas que a chave privada utilizada nos algoritmos servirão também para encriptar o resumo da mensagem do documento assinado, que também pode se chamar de função hash, onde o resultado dessa mensagem será o conteúdo do documento eletrônico. (Brasil (2000 apud GANDINI; SALOMÃO; JACOB, 2001, p.12)).

Tais resumos de mensagens são executados através de algoritmos que serão conhecidos na próxima seção.

Fazendo uso da assinatura digital o usuário pode ficar tranqüilo sobre a autenticação da assinatura, verificando assim, o remetente corretamente e o conteúdo da mensagem, lembrando que, para cada mensagem, será gerada uma assinatura correspondente e a cada mudança de assunto no documento haverá uma assinatura diferente.

6.2.1. Algoritmos de resumo

Há vários algoritmos de resumo mas, nesta seção, serão apresentados os mais utilizados e os que dominam o mercado, como o Algoritmo MD2, MD5, SHA -1 que serão esclarecidos a seguir.

6.2.1.1 - Algoritmo MD2

O primeiro algoritmo de resumo de Ron Rivest foi o MD, que em seguida criou o seu substituto o MD2, uma melhoria do MD.

Segundo Ishikawa (2003, p.49): “o algoritmo MD2 criado por Ron Rivest produz um bloco de 128 bits (16-bytes) e, assim, existem 2.128 possíveis valores de resumo”.

Este, por sua vez, não tem sido muito utilizado pelo fato de que analistas teriam descoberto alguns defeitos sobre seu funcionamento.

6.2.1.2 - Algoritmo MD5

Ron Rivest queria criar um algoritmo de resumo de mensagens rápido e forte, foi então que criou o MD3, que ao ser apresentado, mostrou algumas fraquezas, logo em seguida criou o MD4 que se apresentou como fraco também. Depois veio a criação de MD5 que trás um resumo de 16 bytes.

Embora largamente usado, foram descobertas algumas falhas nele em meados de 1996. O MD5 ainda não foi quebrado, em vez disso, algumas partes internas do algoritmo são vulneráveis. Se faltasse um ou dois componentes no algoritmo, ele seria quebrado. (Oaks (1999 apud ISHIKAWA, 2003, p.49)).

6.2.1.3 - Algoritmo SHA -1

O SHA-1 surgiu através de uma melhoria do algoritmo SHA (*Secure Hash Algorithm*).

O algoritmo SHA-1 se parece muito com o MD5, no entanto suas partes internas são mais fortes por produzirem um resumo mais longo (160 bits comparados com 128 bits) e, por isso, é altamente recomendado pela comunidade criptográfica. Variantes do SHA-1 que produzem resumos de 192 bits a 256 bits ainda estão em desenvolvimento (BURNETT;PAINE, 2002, p.125).

7. FORMAS DE PAGAMENTO

O comércio eletrônico se mostrou valioso através da internet,o que, por sua vez, fez surgir a necessidade de buscar uma forma pela qual se realizem os pagamentos pelo mesmo meio, ou seja, on-line.

Dessa necessidade surgiram os chamados sistemas de pagamento digitais que “representa uma maneira de dar dinheiro a alguém sem que ele seja representado por ouro, moedas ou qualquer outra coisa tangível, ou seja, é o repasse de valor sem a transferência simultânea de objetos físicos” (Garfinkel; Spaffor (1999 apud GREGORES, 2006, p.100)).

Para as compras serem realizadas com sucesso, é necessário escolher uma forma de pagamento, optando pela que lhe melhor convir, a loja tem a obrigação de entregar a mercadoria em ótimas condições e no prazo correto.

Existem algumas formas de pagamento, umas mais utilizadas e outras não. A seguir serão apresentadas algumas delas.

7.1 DINHEIRO ELETRÔNICO

Essa forma de pagamento é conhecida também por e-cash e se parece muito com a forma tradicional de pagamento.

Segundo Filho (2000, p.96) o sistema de pagamento e-cash funciona da seguinte maneira:

> Um banco emissor fornece o *ecash* aos usuários em troca de dinheiro real; o usuário gasta quanto *ecash* quiser; mais tarde, o fornecedor de serviços pode trocar o *ecash* por dinheiro real. Em cada transação são usadas assinaturas digitais para manter segurança.

Sua transferência é usualmente codificada por sistemas de criptografia por chave pública ou chave privada, de forma que somente o destinatário possa realmente utilizar o dinheiro (ALBERTIN, 2010, p.189).

Diante disso, essa forma de pagamento garante a privacidade do usuário através da técnica criptografia, já abordada. E com a assinatura digital é respeitada a autenticação do usuário.

7.2 CARTÕES INTELIGENTES

Este método é conhecido também por Smarts cards. É semelhante ao tamanho dos cartões de crédito convencionais.

Para Gregores (2006, p.102, 103), “esses cartões contêm verdadeiros chips, que podem guardar desde o nome do portador, o limite de crédito e até a sua ficha médica; podendo ser usados inclusive para pagamento de ônibus”.

Devido esta forma de pagamento possuir o nome do usuário, as empresas não correm o risco de o consumidor alegar que não foi o próprio que o utilizou.

7.3 CARTÕES DE CRÉDITO

Os cartões de crédito são os mais utilizados nas transações eletrônicas e permitem realizar compras em qualquer parte do mundo. Para alguns usuários o receio de digitar o numero do cartão pela rede é grande, por acreditar que possa acontecer roubo de informações.

Considera-se que a prática de criptografar as informações de cartões de crédito e enviá-las de um comprador a um vendedor, como mensagem codificada, não atende a importantes requerimentos, tais como proteção contra danos, privacidade e segurança (ALBERTIN, 2010, p.198).

Embora prático e fácil, o pagamento de compras através do cartão de crédito deve ser feito prevenindo e atentando à ação de pessoas más intencionadas pela internet.

7.4 BOLETO BANCÁRIO

Vários usuários utilizam dessa forma de pagamento. Segundo Albertin (2010, p.190): “o dinheiro em papel ainda é o principal instrumento de pagamento dos consumidores”.

Apesar de ser bastante utilizada, para aquelas pessoas que não utilizam do cartão de crédito ou não possuem, essa forma trás alguns riscos, pois ao realizar uma compra, a mesma, pode ocorrer de não ser entregue, após ser efetuado o pagamento via boleto.

8. COMPRA ELETRÔNICA NA PRÁTICA

Neste capítulo será apresentada a parte prática deste trabalho, um site de livros, contendo algumas categorias. Como exemplo, simularemos uma compra através desse site que foi implementado na linguagem PHP, tal linguagem é voltada para web. No momento da finalização da compra foi utilizado o PagSeguro[6], para guardar a quantidade de livros escolhidos, fazendo assim um somatório, no caso de mais de um, fornecendo os dados para devida entrega e por fim a finalização da compra.

Após acessar a página inicial do site implementado, teremos algumas opções de categorias com os seus respectivos livros. Tal página pode ser observada na figura 7.

Figura 7 – Página Inicial - Site.

[6] PagSeguro – Um site que fornece a finalização do “carrinho de compras”, onde realizará o pagamento on-line.

Em nosso exemplo, o livro que vamos simular a compra será: Criptografia e Segurança – O Guia Oficial RSA da categoria Informática. A figura 7 mostra a categoria com seu respectivo livro.

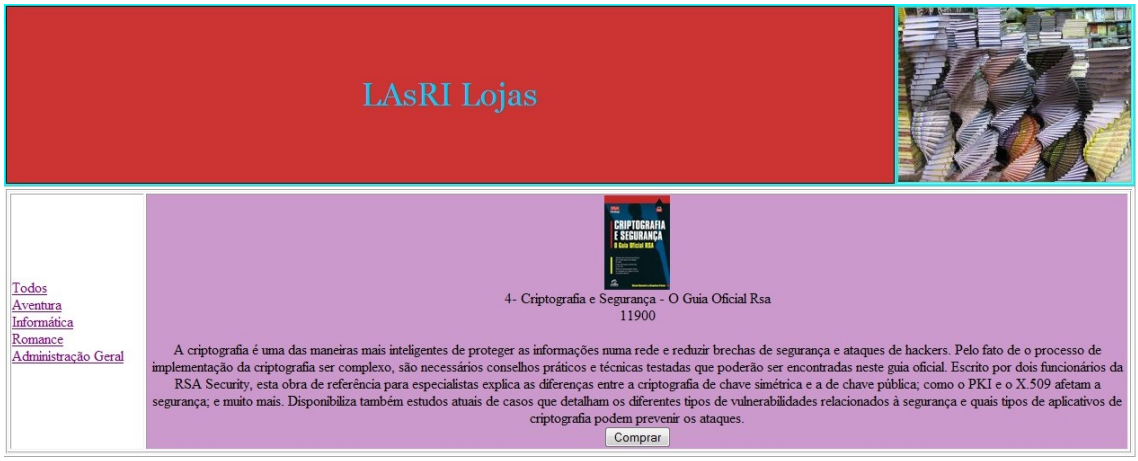

Figura 8 – Categoria com respectivo livro.

Como podemos perceber, o site implementado traz alguns dados sobre o livro escolhido, entre eles o título, o preço e a sinopse. Em seguida, iremos clicar no botão comprar, que levará a página, denominada pelo site PagSeguro de “carrinho de compras”, na qual poderá efetuar a compra.

Nesta fase da compra, se desejar comprar mais de uma unidade do produto escolhido, é só mudar o valor Quantidade para dois e atualizar o carrinho para que o mesmo calcule o total dos livros. É possível, ainda, que queira escolher outro produto, assim é necessário voltar à página inicial do site e clicar no livro de sua escolha. Neste caso iremos prosseguir, apenas com um livro, para finalizar a compra será necessário informar alguns dados, como o endereço utilizado para entrega do produto. Podemos observar esse processo da página do site PagSeguro na figura 9.

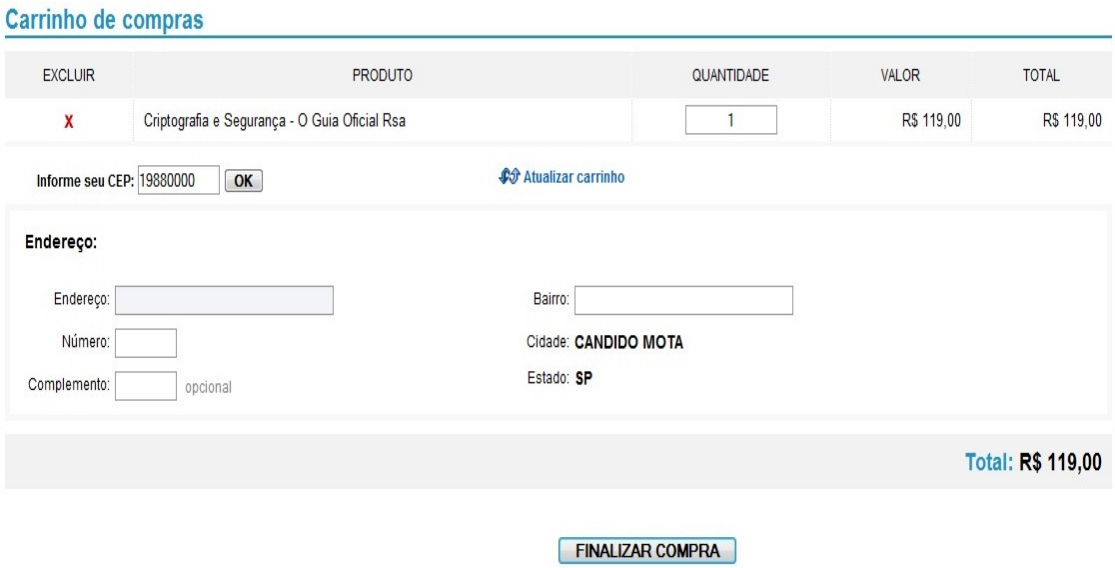

Figura 9 – Carrinho de compras – Pag Seguro

Após informar esses dados, basta clicar em finalizar compra, neste caso, por ser apenas um exemplo de simulação de compra através do site implementado, foi viável finalizar neste ponto a parte prática deste presente trabalho.

9. CONCLUSÃO

Diante do conteúdo exposto nesse trabalho, percebemos que o Comércio Eletrônico tem se desenvolvido bastante nos últimos anos. É um método de compras diferenciado, pela facilidade de aquisição dos produtos, a possibilidade de comprar sem sair de casa, facilidade no pagamento e a disponibilidade das lojas virtuais, 24 horas por dia.

Porém, itens como Segurança tem sido a grande preocupação para uma maior utilização deste tipo de comércio. Estamos à mercê de pessoas mal intencionadas, que sempre estão dispostas a cometer crimes por meio da internet, roubando nossas senhas, números de cartões de crédito, burlando de alguma forma nossa segurança.

Com a pesquisa, pudemos perceber que as empresas que vendem seus produtos por meio da internet, têm investido alto em métodos eficazes de segurança, para garantir a fidelidade de seus clientes e com isso obterem maiores lucros.

Vimos também que existem várias empresas desenvolvendo ferramentas que auxiliam os consumidores a comprar com segurança, informando a eles quais sites são seguros, para que assim, o número de pessoas com interesse neste tipo de comércio aumente a cada dia. Técnicas sofisticadas foram e continuam a ser desenvolvidas como a Criptografia, a Blindagem de Sites, a Assinatura Digital, entre outras, para proporcionar o máximo de confiança e segurança aos clientes virtuais.

E finalmente, notamos que a informação é extremamente importante e aliada do consumidor, para que este possa se cercar dos meios corretos para uma melhor utilização deste novo modelo de comércio, que trás a todos nós enormes benefícios e comodidades.

REFERÊNCIAS

ALBERTIN, Alberto L. Comércio Eletrônico: Benefícios e Aspectos de sua Aplicação. **RAE – Revista de Administração de Empresas,** v.38, n.1, jan/mar, 1998. p. 52-63.

_____. **Comércio Eletrônico: modelo, aspecto e contribuições de sua aplicação.** 6. ed. São Paulo: Editora Atlas, 2010.

BARRETO, Arthur. A importância da certificação SSL EV. Disponível em: < http://www.siteblindado.com.br/blog/2010/08/a-importancia-da-certificacao-ssl-ev/>. Acesso em: 19 set. 2010.

BURNETT, Steve; PAINE, Stephen. **Criptografia e segurança: o guia oficial RSA.** 5. ed. Tradução de Edson Fumankiewicz. Rio de Janeiro: Editora Elsevier, 2002.

CARNEIRO, Bernardo. **Segurança pode aumentar vendas online em até 15%.** Disponível em: <http://www.dihitt.com.br/barra/seguranca-pode-aumentar-vendas-online-em-ate-15>. Acesso em: 19 set. 2010.

_____. **Dicas de como comprar com segurança**. Site Blindado S/A. Disponível em: < http://www.siteblindado.com.br/blog/2010/07/dicas-de-como-comprar-com-seguranca/>. Acesso em: 19 set. 2010.

_____. **Site Blindado S/A cria vídeo com dicas de segurança**. Disponível em: < http://www.siteblindado.com.br/blog/2010/03/site-blindado-sa-cria-video-com-dicas-de-seguranca/ >. Acesso em: 19 set. 2010.

_____. **Aumento da confiança nas transações online**. Disponível em: < http://www.siteblindado.com.br/blog/2010/07/aumento-da-confianca-nas-transacoes-online/>. Acesso em: 19 set. 2010.

_____. SSL Site Blindado eleva confiança dos internautas. Disponível em: < http://www.dihitt.com.br/barra/ssl-site-blindado-eleva-confianca-dos-internautas>. Acesso em: 19 set. 2010.

DINIZ, Eduardo Henrique. **Comércio eletrônico:** Fazendo negócios por meio da internet. **Revista de Administração Contemporânea**, v.3, n.1, jan/apr, 1999.

FILHO, Antonio Alvino da Silva. **Comércio eletrônico: marketing, segurança, aspectos legais e logística.** 2000. 255p. Dissertação (Mestrado) - Departamento de Engenharia da Produção **–** Universidade Federal de Santa Catarina **–** UFSC, Santa Catarina, Mossoró. 2000.

GANDINI, João Agnaldo Donizete; SALOMÃO Diana Paola da Silva; JACOB Cristiane. **A segurança dos Documentos Digitais**. Buscalegis **–** Biblioteca jurídica da Universidade Federal de Santa Caterina, 2001, 18p.

_____. **A Validade jurídica dos documentos digitais**. Buscalegis **–** Biblioteca jurídica da Universidade Federal de Santa Caterina. Disponível em: < http://www.buscalegis.ufsc.br/revistas/files/journals/2/articles/6055/public/6055-6047-1-PB.pdf>. Acesso em: 25 set. 2010.

GREGORES, Valéria E de M. **Compra e Venda eletrônica e suas implicações.** São Paulo: Editora Método, 2006.

HUGO, Vitor; MICHEL, Diego; JANSEN, Dawson. **Segurança no comércio eletrônico.** Centro Federal de educação tecnológica da Paraíba- Sistemas para Internet **–** João Pessoa **–** Paraíba. Disponível em: <http://www.artigonal.com/seguranca-artigos/seguranca-no-comercio-eletronico-489495.html> Acesso em: 16 mar. 2010.

ISHIKAWA, Eliana Cláudia Mayumi. **Um modelo computacional para o funcionamento da assinatura digital no sistema de informatização processual**. 2003. 116p. Dissertação apresentada ao Programa de Pós-Graduação em Engenharia de Produção - Universidade Federal de Santa Catarina, Florianópolis, 2003.

LARA, Daniel Totti de. **Garantias de segurança em sites de comércio eletrônico**. 2003. 101p. Trabalho de Conclusão de Curso. Fundação Educacional do Município de Assis **–** FEMA/Instituto Municipal de Ensino Superior de Assis - IMESA. 2003.

LUPPI, Iria. **História do Comércio Eletrônico.** Oficina da Net. Disponível em: <http://www.oficinadanet.com.br/artigo/1718/historico_do_comercio_eletronico> Acesso em: 16 jun. 2010.

NOGUEIRA, Roberto Henrique Pôrto. **Contrato Eletrônico, Assinatura e Certificação Digitais: da interpretação dos princípios dos contratos na atualidade aos pressupostos, elementos e requisitos de existência e validade**. 2008. 198p. Dissertação apresentada ao Programa de Pós-Graduação em Direito - Pontifícia Universidade Católica de Minas Gerais, Belo Horizonte, 2008.

RUIZ, Nilce; LOURENÇO, Otavio; FREITAS, Robson; GENEOLE, Rogério Augusto; TABUTI, Sandra. **Comércio Eletrônico: Segurança no Serviço Eletrônico**. Faculdades Integradas Campos Salles. Disponível em: <http://www.maurolaruccia.adm.br/trabalhos/comerc.htm>. Acesso em: 15 mar. 2010.

SILVA, Vanusa Cadete da. **O consumidor e o comércio eletrônico.** 2006. 39 p. Trabalho de Conclusão de Curso. Fundação Educacional do Município de Assis **–** FEMA/Instituto Municipal de Ensino Superior de Assis - IMESA. 2006.

WebShoppers 22ª edição. Disponível em: < http://www.webshoppers.com.br/webshoppers/WebShoppers22.pdf>. Acesso em: 06 set. 2010.