UNIVERSIDADE FEDERAL DO PARANÁ

ROSELI PESSIN LEAL

SEGURANÇA E CONFIANÇA NO COMÉRCIO ELETRÔNICO: UM ESTUDO EXPLORATÓRIO

CURITIBA
2009

ROSELI PESSIN LEAL

SEGURANÇA E CONFIANÇA NO COMÉRCIO ELETRÔNICO: UM ESTUDO EXPLORATÓRIO

Trabalho de Conclusão de Curso apresentado à disciplina Pesquisa em Informação II, como requisito parcial à conclusão do Curso de Gestão da Informação, Setor de Ciências Sociais Aplicadas, Universidade Federal do Paraná.

Orientador: Professor Dr. Mauro José Belli.

CURITIBA
2009

TERMO DE APROVAÇÃO

ROSELI PESSIN LEAL

SEGURANÇA E CONFIANÇA NO COMÉRCIO ELETRÔNICO:
UM ESTUDO EXPLORATÓRIO

Trabalho de Conclusão de Curso aprovado como requisito parcial para obtenção do grau de Bacharel no Curso de Bacharelado em Gestão da Informação, Setor de Ciências Sociais Aplicadas da Universidade Federal do Paraná, pela seguinte banca examinadora:

Orientador: Prof. Dr. Mauro José Belli
Departamento de Ciência e Gestão da Informação, UFPR

Prof. Dr. Egon Walter Wildauer
Departamento de Ciência e Gestão da Informação, UFPR

Profª. Drª. Denise Fukumi Tsunoda
Departamento de Ciência e Gestão da Informação, UFPR

Curitiba, 15 de dezembro de 2009

Dedico ao meu esposo Adriano.
À minha filha Yasmin.
Aos meus pais, Antonio e Josefa.

Por todo amor e carinho, por quem sou, e por tudo que alcancei.

AGRADECIMENTOS

A Deus, pela vida, sabedoria e proteção.

Ao meu esposo Adriano, e à minha filha Yasmin, pela paciência e compreensão nos momentos em que me ausentei para dedicar aos estudos.

Ao meu orientador, Professor Dr. Mauro José Belli, pelo incentivo, perseverança e dedicação na orientação deste trabalho.

Aos professores do Departamento que, de alguma forma, contribuíram para a minha formação pessoal e profissional.

Aos amigos e colegas de faculdade. Em especial à Viviane, Idemara e Elias, pela amizade, colaboração e convivência agradável.

Aos colegas da CAIXA que direta ou indiretamente, contribuíram para que eu concluísse esta pesquisa e a graduação no prazo previsto. Em especial ao Francisco Fachini, por sua generosidade, compreensão e incentivo.

Às pessoas que responderam ao questionário, pela disposição e prontidão em colaborar. Sem a participação dos mesmos, não seria possível o prosseguimento e êxito deste trabalho.

“É da natureza do conhecimento que ele sofra mutações rapidamente e que, portanto, as certezas de hoje se tornarão os absurdos de amanhã”

Peter Drucker

RESUMO

A presente pesquisa, de cunho exploratório, tem como objetivo principal verificar as condições de segurança do comércio eletrônico *Business-to-Consumers (B2C),* sob o ponto de vista tecnológico e legal, no âmbito nacional. Apresenta conceitos sobre comércio eletrônico e segurança da informação. Descreve os principais recursos tecnológicos que visam garantir a segurança e a privacidade das informações na internet. Levanta normas que norteiam as transações eletrônicas na internet e qual a principal lei que assegura o direito do consumidor no comércio eletrônico B2C. Verifica, através de levantamento de dados, realizado com aplicação de um questionário junto a alguns usuários do comércio eletrônico, se os mesmos conhecem tanto os recursos tecnológicos, quanto as leis que visam garantir a segurança e o direito do consumidor no comércio eletrônico. Paralelamente, investiga se os mesmos estão satisfeitos com as informações disponibilizadas nos sites das lojas virtuais e com o serviço, de maneira geral. Verifica que a criptografia e a certificação digital são os recursos tecnológicos mais indicados para garantir a segurança e a privacidade na internet. O Código de Defesa do Consumidor é a principal lei que assegura o direito do consumidor no comércio eletrônico B2C. Os resultados obtidos com a aplicação do questionário indicam que alguns consumidores desconhecem os recursos tecnológicos e a lei que assegura seus direitos no comércio *online*. A maioria alega estar satisfeito com o serviço de comércio eletrônico, porém, gostaria que as lojas virtuais disponibilizassem informações sobre segurança e direito do consumidor, em seus *sites,* na internet. Conclui que o comércio eletrônico não é totalmente seguro, para o consumidor, do ponto de vista tecnológico e legal. Sugere que as empresas que exploram a internet para comercializar seus produtos e serviços façam uso dos recursos tecnológicos e legais disponíveis, de modo a proporcionar mais confiança nos usuários, para que os mesmos se sintam mais seguros e satisfeitos em relação ao serviço e utilizem com maior frequência.

Palavras-chave: Comércio eletrônico. Consumidor. Internet. Segurança.

LISTA DE ILUSTRAÇÕES

LISTA DE SIGLAS

ABNT – Associação Brasileira de Normas Técnicas

B2B – *Business-to-Business*

B2C – *Business-to-Consumers*

BS – *British Standard*

C2C – *Consumer-to-Consumer*

CDC – Código de Defesa do Consumidor

CPF – Cadastro de Pessoas Físicas

CNPJ – Cadastro Nacional de Pessoas Jurídicas

G2C – Governo-para-Cidadãos

HTTP – *HyperText Transfer Protocol*

HTTPS – *Secure HyperText Transport Protocol*

ICP – Infraestrutura de Chaves Públicas

INTERNET – *Intercontinental Networks*

IEC – *International Engineering Consortium*

ISO – *International Organization for Standartization*

ITI – Instituto Nacional de Tecnologia da Informação

MP – Medida Provisória

NBR – Norma Brasileira

SET – *Secure Electronic Transaction*

SSL – *Secure Socket Layer*

SRF – Secretaria da Receita Federal

UFPR – Universidade Federal do Paraná

SUMÁRIO

1 INTRODUÇÃO

No cenário atual, as empresas buscam cada vem mais atrair novos clientes e fidelizar os que já possuem fazendo uso da tecnologia da informação, uma importante aliada nesse processo.

Pode-se afirmar que o desenvolvimento das tecnologias da informação, em particular da internet, criou oportunidades para que as empresas se tornem mais competitivas e explorem novos nichos de mercado, à medida que com a internet as barreiras de tempo, distância e forma são praticamente destruídas e as relações comerciais tornam-se quase ilimitáveis.

Nesse contexto, surge o comércio eletrônico provocando uma revolução nas relações de compra e venda de bens e serviços. “Sem dúvida, a internet revolucionou e vem revolucionando as relações de mercado e as formas de interação entre empresas e consumidores”.(DELOITTE, 2009, p.5)

Deve-se ressaltar, no entanto, que essa novidade propõe mudanças e o novo tende a provocar resistência e insegurança nas pessoas. Por isso, a internet enfrentou por muito tempo o receio das empresas em se lançar no comércio eletrônico e a falta de confiança propiciou um relativo atraso no mercado brasileiro.

Não obstante, a Internet e o comércio eletrônico estão cada vez mais presentes no dia-a-dia das pessoas, possibilitando adquirir bens e serviços de maneira fácil e rápida. “Embora a maioria das transações ainda ocorra pelos canais tradicionais, um número cada vez maior de consumidores e empresas estão usando a internet para fazer comércio eletrônico.” (LAUDON e LAUDON, 2007, p.280).

Essa evolução apresenta diversas consequências a serem entendidas para o aproveitamento efetivo das potencialidades desse ambiente e, principalmente, para o tratamento adequado dos riscos envolvidos em uma situação com tal poder revolucionário.

Diante do exposto, buscou-se identificar as condições de segurança do comércio eletrônico *Business-to-Consumer* (B2C) no Brasil, para o consumidor, considerando tanto os aspectos tecnológicos quanto os legais. Paralelamente, verificou-se, junto a alguns consumidores do comércio eletrônico, se os mesmos conhecem os recursos tecnológicos que visam garantir a segurança e a privacidade,

bem como as normas e legislação, que norteiam as transações eletrônicas, no ambiente virtual.

O trabalho está estruturado da seguinte forma. Na introdução apresenta-se a contextualização do problema, a justificativa e indica os objetivos da pesquisa. O capítulo 2 apresenta a literatura pertinente obtida através da pesquisa bibliográfica. O capítulo 3 descreve os métodos e materiais utilizados na pesquisa. Os resultados obtidos são mostrados e analisados no capítulo 4. No capítulo 5, discutem-se os resultados, à luz da literatura pertinente. Por fim, no capítulo 6 apresentam-se as considerações finais, apoiadas no desenvolvimento da pesquisa, e sugestões para pesquisas futuras.

1.1 PROBLEMA E JUSTIFICATIVA

O crescimento da internet e do comércio eletrônico, nos últimos anos, tem proporcionado comodidade e benefícios para a sociedade. Entretanto, por se tratar de um ambiente relativamente novo, muitas pessoas desconhecem os riscos desse ambiente complexo e dinâmico.

A segurança das transações comerciais via internet é uma preocupação tanto para os clientes quanto para os fornecedores. De acordo com Matte (2001) pode-se afirmar que um dos fatores que impedem a expansão do comércio eletrônico no mundo todo, principalmente no Brasil, são as questões relacionadas à segurança das informações que trafegam pela internet.

Nesse contexto, em que a segurança da informação é uma necessidade evidente, as questões relativas à segurança na internet, especificamente no comércio eletrônico, devem ser levantadas e investigadas.

Diante do exposto, faz-se necessário verificar as condições de segurança e confiança do comércio eletrônico B2C para o consumidor. Averiguar se o usuário tem consciência dos riscos a que está exposto quando opta pela internet como meio de adquirir produtos e serviços. Se conhece e utiliza os recursos tecnológicos que visam minimizar esses riscos e a legislação que assegura seus direitos, no âmbito nacional.

De acordo com a problemática exposta, motivaram esta pesquisa as seguintes questões:

a) quais são os principais recursos tecnológicos que visam garantir a segurança e a privacidade da informação na internet, no contexto do comércio eletrônico varejista?
b) em relação às normas reguladoras, o comércio eletrônico no Brasil, está apoiado em princípios jurídicos sólidos? Qual é a principal lei que assegura a privacidade e o direito do consumidor no comércio eletrônico B2C?
c) os consumidores conhecem e utilizam os recursos tecnológicos e as nomas que norteiam o comércio eletrônico, no âmbito nacional?

Não menos importante, verificar se os consumidores do comércio eletrônico B2C gostariam que mais informações sobre segurança e direito do consumidor fossem viabilizadas nos sites das lojas virtuais e, se estão satisfeitos com essa modalidade de comércio.

1.2 OBJETIVOS

Com o intuito de desenvolver o estudo e visando atender a problemática exposta estabeleceram-se os objetivos a seguir.

1.2.1 Objetivo geral

Realizar um estudo exploratório acerca do comércio eletrônico *Business-to-Consumer* (B2C), visando verificar as condições de segurança para o consumidor, sob o ponto de vista tecnológico e legal, no âmbito nacional.

1.2.2 Objetivos específicos

Visando alcançar o objetivo principal da pesquisa, os objetivos específicos propostos são:

a) identificar os principais recursos relacionados à segurança e privacidade da informação na internet, considerando o aspecto tecnológico, aplicáveis ao comércio eletrônico;
b) levantar normas reguladoras que norteiam as transações eletrônicas na internet, bem como a principal lei que assegura o direito do consumidor no comércio eletrônico B2C, no Brasil;
c) verificar, através de levantamento de dados, junto a alguns usuários do comércio eletrônico B2C, se conhecem os recursos tecnológicos que asseguram a segurança das informações e leis aplicáveis a essa modalidade de comércio;
d) averiguar se os mesmos estão satisfeitos em relação às informações sobre segurança e direito do consumidor disponibilizadas nos sites das lojas virtuais e com o serviço de comércio eletrônico, de maneira geral.

2 LITERATURA PERTINENTE

Para possibilitar a compreensão do tema e das questões abordadas, foram explorados os temas conforme segue.

2.1 INTERNET

De acordo com Matte (2001), a internet nasceu de um audacioso projeto militar americano e acabou se espalhando pelo mundo por meio das universidades (das comunidades científicas), tornando-se um dos maiores e provavelmente o melhor meio de comunicação já criado pelo homem.

Segundo Volpi Neto (2003), a internet consiste na interligação de redes de computadores de alcance mundial, tendo em comuns padrões de transmissão de dados, os chamados protocolos. A padronização na transmissão é o que permite a milhares de redes a comunicação entre si, formando o que conhecemos por Internet.

A internet está cada vez mais presente na vida das pessoas. “Dentro de alguns anos, com a facilidade que iremos obter com sua utilização como meio de comunicação e troca de informações, poderá quem ignorá-la, sofrer dentre as diversas formas de exclusão da sociedade, a denominada tecnológica” (MATTE, 2001, p. 29).

O crescimento explosivo da internet é um fenômeno revolucionário em computação e telecomunicações. “A internet está constantemente se expandindo, à medida que mais e mais empresas e outras organizações e usuários, aderem a essa rede mundial” (O`BRIEN, 2006, p. 169).

Nesse sentido, Laudon e Laudon (2007, p. 178) afirmam que na última década, a Internet se tornou o sistema de comunicação público mais abrangente. É também o maior exemplo de redes interconectadas e computação cliente-servidor no mundo, conectando centenas de redes individuais em todo planeta.

O número de usuários da Internet cresce no mundo todo; e no Brasil a situação não é diferente. Uma pesquisa realizada em 2008 mostrou que o Brasil está entre os 20 países com maior número de internautas, ocupando a sexta posição, como mostra a tabela abaixo:

TABELA 1 - OS 20 PAÍSES COM MAIOR NÚMERO DE USUÁRIOS DA INTERNET

#	País ou Região	Usuários	Adoção da Internet	% de usuários	População (2008)	Crescimento dos Usuários (2000 – 2008)
1	China	253.000.000	19.0 %	17.3 %	1.330.044.605	1.024.4 %
2	Estados Unidos	220.141.969	72.5 %	15.0 %	303.824.646	130.9 %
3	Japão	94.000.000	73.8 %	6.4 %	127.288.419	99.7 %
4	Índia	60.000.000	5.2 %	4.1 %	1.147.995.898	1.100.0 %
5	Alemanha	52.533.914	63.8 %	3.6 %	82.369.548	118.9 %
6	Brasil	50.000.000	26.1 %	3.4 %	191.908.598	900.0 %
7	Reino Unido	41.817.847	68.6 %	2.9 %	60.943.912	171.5 %
8	França	36.153.327	58.1 %	2.5 %	62.177.676	325.3 %
9	Korea do Sul	34.820.000	70.7 %	2.4 %	49.232.844	82.9 %
10	Itália	34.708.144	59.7 %	2.4 %	58.145.321	162.9 %
11	Rússia	32.700.000	23.2 %	2.2 %	140.702.094	954.8 %
12	Canadá	28.000.000	84.3 %	1.9 %	33.212.696	120.5 %
13	Turkia	26.500.000	36.9 %	1.8 %	71.892.807	1.225.0 %
14	Espanha	25.623.329	63.3 %	1.8 %	40.491.051	375.6 %
15	Indonésia	25.000.000	10.5 %	1.7 %	237.512.355	1.150.0 %
16	México	23.700.000	21.6 %	1.6 %	109.955.400	773.8 %
17	Irã	23.000.000	34.9 %	1.6 %	65.875.223	9.100.0 %
18	Vietnã	20.159.615	23.4 %	1.4 %	86.116.559	9.979.8 %
19	Paquistão	17.500.000	10.4 %	1.2 %	167.762.040	12.969.5 %
20	Austrália	16.355.388	79.4 %	1.1 %	20.600.856	147.8 %
Os 20 Mais		1.115.713.572	25.4 %	76.2 %	4.388.052.548	284.5 %
Resto do Mundo		347.918.789	15.2 %	23.8 %	2.288.067.740	391.2 %
Total - Usuários Mundo		1.463.632.361	21.9 %	100.0 %	6.676.120.288	305.5 %

Fonte: http://www.internetworldstats.com e institutos diversos (2008).
* Compilado por www.e-commerce.org.br. Adaptado.

2.2 COMÉRCIO ELETRÔNICO

O conceito de comércio eletrônico evoluiu à medida que as tecnologias de informação, utilizadas para automatizar a compra e venda de bens e serviços, também evoluíram.

De acordo com Laudon e Laudon (2007) comércio eletrônico ou (*e-commerce*) refere-se ao uso da Internet e da *Web* para comercializar mercadoria e serviços. Diz respeito às transações comerciais realizadas digitalmente entre organizações e indivíduos ou entre duas ou mais organizações.

2.2.1 Modelos

Existem vários modelos de comércio eletrônico. De acordo com Turban, McLean e Wetherbe (2004, p. 162-163), os principais são:

a) B2B – *business-to-business* (empresa-a-empresa): são transações em que tanto os compradores quanto os vendedores são empresas;

b) B2C – *business-to-consumers* (empresa-a-consumidores): neste caso, os vendedores são empresas e os consumidores são indivíduos (consumidores);

c) C2B – *consumer-to-business* (consumidor-a-empresa): onde os clientes anunciam a necessidade específica de um produto ou serviço, e as empresas concorrem para fornecê-los;

d) C2C - *consumer-to-consumer* (consumidor-a-consumidor): ocorre quando alguém vende produtos ou serviços a outras pessoas;

e) *Intrabusiness* (comércio intraorganizacional): uma empresa utiliza o comércio eletrônico internamente para melhorar as operações;

f) G2C – governo-para-cidadãos: neste caso, o governo fornece serviços aos seus cidadãos via tecnologias de comércio eletrônico. Os governos também podem fazer negócios com outros governos e com empresas;

g) *c-commerce* – comércio cooperativo: é a modalidade em que os parceiros de negócios colaboram pela via eletrônica. Essa cooperação ocorre, em geral, entre parceiros de negócios na cadeia de suprimentos;

h) *m-commerce* – comércio móvel: quando o comércio eletrônico ocorre em um ambiente sem-fio – via telefone celular para acesso à Internet, por exemplo.

Dentre os diversos tipos de comércio eletrônico, Matte (2001) afirma que, dois tipos de comércio eletrônico movimentam a grande rede: o *Business-to-Business* (B2B) e o *Business-to-consumer* (B2C). O primeiro diz respeito à compra e venda entre parceiros de negócios (entre empresas – pessoas jurídicas), ou seja, quando a situação é de meio. O segundo ocorre entre fornecedor (pessoa jurídica) e consumidor (pessoas física), ou seja, quando a situação é de fim.

2.2.2 Comércio eletrônico na Internet

Comercializar produtos e serviços pela internet é uma realidade cada vez mais presente na vida das pessoas. Volpi Neto (2003) acredita que o homem viverá no tempo da praticidade, onde buscará tornar a sua vida o mais simples possível. Nesse contexto, o tempo e a informação serão bens cada vez mais preciosos. O autor ainda afirma que o comércio eletrônico não é um novo conceito. Há tempos, muitas empresas e consumidores têm usado a mídia eletrônica para conduzir transações comerciais e financeiras. “O que há de novo é a facilidade de acesso e a popularização desse tipo de comércio, além de, obviamente, a forma de comunicação.” (VOLPI NETO, 2003, p.17).

Volpi Neto (2003) acredita que essa revolução é considerada tão importante como a industrial de 200 anos atrás. A lógica indica que o consumidor, tendo acesso direto aos fornecedores dos produtos e serviços, não necessitará de intermediários atuais. O autor afirma que essa realidade já é vivida no comércio de automóveis, livros etc. “Surgirão, porém, outros tipos de intermediação, como os provedores de conectividade e certificadores, por exemplo.” (VOLPI NETO, 2003, p.17).

Não obstante, o autor ressalta que, apesar das previsões animadoras em relação ao comércio eletrônico, ainda há muito a ser trilhado, para que esse novo mercado se consolide no plano jurídico e comercial.

> Sua complexidade afasta uma boa parte das pessoas, que já possuem uma noção clara do comércio convencional e carecem de conhecimentos mínimos sobre o eletrônico. Sem esse conhecimento não se poderá gerar confiança e, portanto, desenvolvimento. (VOLPI NETO, 2003, p. 18)

Conforme Laudon e Laudon (2007), o comércio eletrônico começou em 1995, quando um dos primeiros portais da internet, o Netscape.com, aceitou os primeiros anúncios de grandes corporações e popularizou a idéia de que a Web poderia ser usada como uma nova mídia que poderia ser utilizada para publicidade e vendas. “Na época, ninguém vislumbrava a curva de crescimento exponencial que as vendas no varejo eletrônico experimentariam, vindo a triplicar e dobrar nos anos seguintes.” (LAUDON e LAUDON, 2007, p. 271).

De acordo com uma pesquisa publicada pelo site E-commerce.org, o montante faturado com o e-commerce no Brasil em 2008 foi de mais 8 bilhões. Em dois anos (2006-2008) o faturamento praticamente dobrou, apresentando uma forte tendência de crescimento, conforme tabela abaixo:

TABELA 2 - FATURAMENTO ANUAL DO VAREJO EM BILHÕES

ANO	FATURAMENTO	VARIAÇÃO
2009 (previsão)	R$ 10 bilhões	22%
2008	R$ 8,20 bilhões	30%
2007	R$ 6,30 bilhões	43%
2006	R$ 4,40 bilhões	76%
2005	R$ 2,50 bilhões	43%
2004	R$ 1,75 bilhão	48%
2003	R$ 1,18 bilhão	39%
2002	R$ 0,85 bilhão	55%
2001	R$ 0,54 bilhão	...

Fonte: Ebit (2009) - Compilação www.e-commerce.org.br. Adaptado.
* Nota: Não considera as vendas de automóveis, passagens aéreas e leilões on-line.

2.2.2.1 Questões levantadas

O crescimento explosivo do comércio eletrônico revelou ou acentuou algumas questões relacionadas à segurança na internet.

Segundo Beal (2005) o comércio eletrônico, está sujeito a uma série de ameaças de ataques que podem resultar em fraude, descumprimento de contratos e divulgação indevida de dados confidenciais e outras conseqüências negativas.

A autora ainda ressalta que todos os aspectos relacionados à segurança das comunicações eletrônicas devem ser considerados quando se trata de garantir a credibilidade e a proteção das trocas eletrônicas envolvidas em processos comerciais.

Segundo O`brien (2006), o uso da tecnologia da informação nas transações eletrônicas apresenta importantes desafios à segurança e afeta a sociedade de maneira significativa.

Nesse sentido, Laudon e Laudon (2007), afirmam que controle e segurança inadequados podem criar sérios riscos legais. As empresas precisam proteger não apenas seus próprios ativos de informação, mas também o de clientes e parceiros de negócio.

> Uma organização pode ser responsabilizada pelo risco e pelo dano desnecessários gerados caso não tenha tomado as medidas preventivas apropriadas para evitar a perda de informações confidenciais, corrupção de dados ou violação de privacidade. (LAUDON e LAUDON, 2007, p. 220)

2.3 SEGURANÇA DA INFORMAÇÃO

A segurança da informação deixou de ser tratada como um assunto técnico da área de informática, tornando-se uma preocupação constante na sociedade da Informação. É um requisito estratégico, que interfere diretamente na capacidade das empresas em realizar negócios e no valor agregado de seus serviços e produtos.

De acordo com a NBR ISO/IEC 17799 (2001), a segurança da informação é caracterizada pela preservação de:

a) confidencialidade: garantia de que as a informação é acessível somente por pessoas autorizadas;
b) integridade: salvaguarda da exatidão da informação e dos métodos de processamento;
c) disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Devido ao valor estratégico da informação, no cenário atual, os requisitos citados acima, são essenciais para preservar não somente a competitividade e a lucratividade da organização, mas também o atendimento aos requisitos legais e a imagem perante mercados e clientes.

Beal (2005) afirma que alguns autores acrescentam a esses três requisitos, o da legalidade (garantia de que a informação foi produzida em conformidade com a lei), ou ainda o de “uso legitimo” (garantia de que os recursos de informação não são usados por pessoas não autorizadas ou de maneira não autorizada).

Em relação às normas de segurança da informação, vale lembrar que, a ISO/IEC 17799 - Código de prática para a gestão da segurança da informação – foi criada tendo como base o padrão BS 7799 e, em 2005 evoluiu para a ISO/IEC 27002 – a qual compõe a série de normas 27000 – reservadas para tratar de padrões de segurança da informação.

2.3.1 Princípios básicos de segurança da informação

Segundo Ferreira (2003) os princípios básicos da segurança são:

a) autenticidade: o controle de autenticidade está associado à identificação correta de um usuário ou computador. O serviço de autenticação deve assegurar ao receptor que a mensagem é realmente procedente da

origem informada. Normalmente, isso é implementado a partir de mecanismo de senhas ou de assinatura digital. É uma medida de proteção de um serviço/informação contra personificação por intrusos;

b) confidencialidade: significa proteger informações contra sua revelação para alguém não autorizado. Consiste em proteger a informação contra alguém que não tenha sido explicitamente autorizado. No caso de rede, isto significa que os dados, enquanto em trânsito, não serão decifrados, alterados, ou extraídos da rede pó pessoas não autorizadas ou capturadas por dispositivos ilícitos, ou seja, o objetivo é proteger a informação privada, evitando a inteligibilidade dos dados;

c) integridade: consiste em proteger a informação contra modificação sem a permissão explicita do proprietário daquela informação. A modificação inclui ações como: escrita, alteração, alteração de conteúdo, alteração de status, remoção e criação de informações.

Ferreira (2003) ressalta que os princípios acima, proporcionam benefícios como: reduzir os riscos com vazamentos de informações, fraudes, erros, uso indevido, sabotagens, e diversos outros problemas ocasionados pela falta de segurança.

2.4 SEGURANÇA E PRIVACIDADE NO COMÉRCIO ELETRÔNICO

Ao longo dos últimos anos tem crescido o número de negócios conduzidos via internet.

Nesse contexto, Albertin (2001) afirma que por causa de suas origens e sua estrutura aberta, a internet é notória pelas brechas de segurança. Entretanto, o autor considera que os mecanismos de segurança que estão sendo disponibilizados, podem ser utilizados para a transmissão de informações sensíveis e a transferência de valores, de maneira eficiente.

Ferreira (2003) ressalta que o comércio eletrônico envolve uma série de atividades dentre elas, as transações financeiras.

> Entretanto a simples apresentação de um cartão de crédito pode levar o seu proprietário a ser fraudado tendo o seu número de cartão usado sem sua permissão. O uso de mecanismos de transação segura na internet, onde o número de cartão de crédito é enviado junto com outras informações de forma encriptada tem permitido que estes pagamentos possam se dar de forma segura. (FERREIRA, 2003, p.69)

2.4.1 Segurança das comunicações eletrônicas

Os processos devem estabelecer confiança mútua e acesso seguro entre as partes numa transação de e-commerce, reconhecendo os usuários, autorizando o acesso e reforçando características de segurança. “A segurança das transações eletrônicas é uma importante questão de controle no comércio eletrônico. É essencial que dados sejam mantidos privados ao serem transmitidos eletronicamente” (LAUDON e LAUDON, 2001, p. 348).

Considerando ainda, que alguns aspectos adicionais de segurança da informação emergem quando esta precisa ser transmitida. Beal (2005), afirma que problemas como a alteração fraudulenta de documentos em trânsito e disputas sobre a origem de uma comunicação precisam ser equacionados, levando-se à necessidade de estabelecer alguns objetivos adicionais relativos à segurança da comunicação, com o objetivo de preservar:

a) integridade de conteúdo: garantia de que a mensagem enviada pelo emissor é recebida de forma completa e exata pelo receptor;
b) irretratabilidade de comunicação: garantia de que o emissor ou o receptor não tenha como alegar que uma comunicação bem sucedida não ocorreu;
c) autenticidade do emissor e do receptor: garantia de que quem se apresenta como remetente ou destinatário da informação é realmente quem diz ser;

d) confidencialidade de conteúdo; garantia de que o conteúdo da mensagem somente é acessível a seu(s) destinatário(s);
e) capacidade de recuperação do conteúdo pelo seu receptor: garantia de que o conteúdo transmitido pode ser recuperado em sua forma original pelo destinatário. Para que esse objetivo seja alcançado, emissor e receptor precisam usar protocolos de comunicação consistentes.

A autora ainda ressalta a adoção de medidas adicionais:

> Situações em que os impactos da corrupção do conteúdo de comunicações eletrônicas, ou de corrupção do conteúdo de mensagens transmitidas, são significativos, como nos casos de transferência eletrônica de fundos e das transações de comércio eletrônico, medidas de proteção adicionais, dentre as quais de destacam as técnicas de criptografia e assinatura digital, são necessárias para minimizar os riscos existentes. (BEAL, 2005, p.100)

Nesse contexto, um dos benefícios da criptografia assimétrica ou criptografia de chave pública é a utilização em instrumentos eletrônicos como a assinatura digital e o certificado digital que permitem proteger os mais diversos tipos de troca eletrônica de informação.

2.4.1.1 Criptografia

Os canais pelos quais os dados são transmitidos na internet não são totalmente seguros; portanto, qualquer informação privada que esteja sendo transmitida tem de estar protegida. Uma maneira de proteger as informações é através da criptografia.

Dias (2000), afirma que a criptografia como mecanismo de segurança, atende a mais de um requisito de segurança da informação. Por exemplo, ao ocultar a informação, por meio do texto cifrado proporciona confidencialidade. Ao mesmo tempo, garante a integridade de dados, pois o conteúdo da mensagem fica inalterado desde a cifragem até a decifragem.

De acordo com Laudon e Laudon (2001) uma mensagem pode ser criptografada aplicando-se um código numérico secreto chamado chave criptográfica de forma que é transmitida como um conjunto de caracteres embaralhados. (a chave consiste em um grande número de letras números e símbolos). Para ser lida, a mensagem precisa ser decriptografada (desembaralhada) com uma chave de combinação. “Existem vários padrões de criptografia, entre eles o SSL (*Secure Sockets Layer*) e o S-HTTP (*Secure Hypertext Transport Protocol*), os quais são usados para o trafego baseado na *Web*.” (LAUDON; LAUDON 2001 P. 349).

Segundo Ferreira (2003), a criptografia nasceu da necessidade de manter a privacidade das informações. Desde a antiguidade já se tinha conhecimento da criptografia onde era utilizada a substituição ou a troca de símbolos com o objetivo de confundir um possível interceptador das mensagens. “Para a computação esse princípio é mantido, porém a escrita é substituída pelo processamento digital da informação e com a capacidade de processamento de dados desta tecnologia” (FERREIRA, 2003, p.58)

O autor afirma que os dois tipos de criptografia mais usados são:

a) criptografia simétrica ou algoritmo simétrico - usa somente uma chave tanto para criptografar como para decriptar. Essa chave deve ser mantida secreta para garantir a confidencialidade da mensagem. Também conhecido como algoritmo de chave secreta;

b) criptografia assimétrica ou algoritmo assimétrico é um algoritmo de criptografia que usa duas chaves: uma pública e uma chave privada, onde a chave pública pode ser distribuída abertamente, enquanto a chave privada é mantida secreta. Os algoritmos assimétricos são capazes de muitas operações, incluindo criptografia e assinaturas digitais.

Beal (2005) considera que os mecanismos de criptografia são amplamente adotados em ambientes computacionais para oferecer garantia de autenticação, privacidade e integridade de dados e comunicações, e sem essa tecnologia não teria sido possível popularizar o comércio eletrônico.

O`brien (2006) acredita que a criptografia de dados tornou-se uma maneira importante de proteger informações, principalmente na internet. Senhas,

mensagens, arquivos e outros dados podem ser transmitidos de forma embaralhada e desembaralhados pelos sistemas de computadores apenas para os usuários autorizados.

De acordo com Laudon e Laudon (2007), criptografia é o processo de transformar textos comuns ou dados, em um texto cifrado, que não possa ser lido por ninguém a não ser o remetente (quem enviou a mensagem) e o destinatário (receptor).

2.4.1.2 Certificado digital

Laudon e Laudon (2001) consideram que a autenticação na comunicação pode ser reforçada anexando-se um certificado digital para uma mensagem eletrônica.

Segundo Ferreira (2003 p. 67) os certificados digitais funcionam como credenciais. Semelhante a um cartório na vida real, os cartórios digitais atestam a autenticidade das informações incluídas no certificado, considerando-se que, existe confiança frente ao cartório digital. Um certificado digital é constituído de três componentes básicos:

a) uma chave pública;

b) informação de certificado (identificação do usuário, dados pessoais e profissionais, contatos etc.);

c) uma ou mais assinaturas digitais do cartório digital.

Numa visão notarial, Volpi (2003) afirma que a melhor forma de se entender o papel de uma entidade certificadora é o trabalho dos tabelionatos. Quando nos dirigimos a um serviço notarial para depositar nossa assinatura, é com a finalidade de que, quando necessária a verificação da veracidade da mesma , qualquer um possa solicitar que o tabelião a reconheça. Dessa forma, por meio de reconhecimento de firma, pode-se provar a autoria de determinado documento. O autor afirma que a certificação eletrônica ocorre da seguinte forma.

> O usuário solicita a emissão de um Certificado Digital que o identifique, preenchendo um formulário com seus dados pessoais ou da empresa. Após a perfeita identificação do usuário, este deverá assinar uma escrita pública, no caso de tabelionato, da qual constarão as condições de certificação. Esse contrato com o tabelião deverá conter todas as condições, prazos e responsabilidades para ambas as partes. (VOLPI NETO, 2003, p.80).

Deve-se ressaltar, entretanto, o que alguns autores chamam de cartórios digitais, normalmente, são entidades, conhecidas como Autoridades de Registro, devidamente credenciadas na Infraestrutura de Chaves Públicas Brasileiras – ICP-Brasil, responsáveis pela interface entre o usuário e a Autoridade Certificadora.

As Autoridades Certificadoras são entidades responsáveis por autorizar e promover a emissão de certificados digitais e também por agendar a data da expiração, revogação e respectiva publicação dos certificados revogados.

Beal (2005) afirma, que a certificação digital desempenha um papel importante na segurança do comércio eletrônico: uma relação de negócios, mesmo entre desconhecidos, pode ser estabelecida de forma ágil e segura pelo uso de certificados digitais emitidos por entidades certificadoras devidamente reconhecidas.

De acordo com informações obtidas no *site* do Instituto Nacional de Tecnologia da Informação (ITI), o certificado, na prática, equivale a uma carteira de identidade virtual ao permitir a identificação de uma pessoa no meio digital/eletrônico quando enviando uma mensagem ou em alguma transação pela internet que necessite validade legal e identificação inequívoca. Um certificado digital contém dados de seu titular, tais como nome, identidade civil, *e-mail*, nome e assinatura da Autoridade Certificadora que o emitiu, entre outras informações. É importante saber que essa tecnologia confere a mesma validade jurídica ao documento assinado digitalmente do equivalente em papel assinado de próprio punho.

2.4.1.3 Assinaturas Digitais

Segundo Laudon e Laudon (2001) uma assinatura digital é um código digital anexado a uma mensagem transmitida eletronicamente que é usada para verificar a origem e o conteúdo de uma mensagem. Ela fornece um modo de associar uma

mensagem com o remetente, desempenhando uma função similar à assinatura escrita. Um destinatário de dados pode usar a assinatura digital para verificar quem enviou os dados e que os dados não foram alterados de depois de ela ter sido assinada.

Numa abordagem mais abrangente a NBR ISO/IEC 17799 (2001) afirma que as assinaturas digitais fornecem os meios para proteção da autenticidade e integridade de documentos eletrônicos. Por exemplo, elas podem ser utilizadas no comércio eletrônico onde existe a necessidade de verificar quem assinou o documento eletrônico e checar se o conteúdo do documento eletrônico assinado foi modificado. Assinaturas digitais podem ser aplicadas a qualquer forma de documento que é processado eletronicamente, por exemplo, elas podem ser usadas para assinar pagamentos eletrônicos, transferências de fundos, contratos e acordos.

Matte (2001) considera que as assinaturas digitais, juntamente com as autoridades certificadoras, é a esperança dos operadores do direito para solucionar alguns problemas e proporcionar maior segurança, não somente no comércio eletrônico, mas em todas as questões que envolvam necessidade de prova e privacidade.

As assinaturas digitais permitem ao destinatário verificar a autenticidade e integridade da informação recebida. “Além disso, uma assinatura digital não permite o repúdio, ou seja, o emitente não pode alegar que não realizou a ação, considerando sua assinatura digital” (FERREIRA, 2003 p. 66).

Volpi Neto (2003) ressalta que:

> Uma das grandes vantagens da assinatura digital é que ela vem associada ao texto, garantindo não somente a origem do subscritor como também a vinculação de sua autoria ao texto, em função conhecida como *hash.* Isso lhe outorga uma outra característica bastante peculiar: nunca uma assinatura digital é igual a outra, pois se encontra completamente vinculada a um determinado conteúdo de um documento. (VOLPI NETO, 2003, p. 53)

Nesse sentido, Deitel, Deitel e Steinbuhler (2004) fazem uma observação importante. Os autores afirmam que as assinaturas digitais equivalem às assinaturas manuscritas e foram desenvolvidas para solucionar problemas de autenticação e integridade. Complementam que uma assinatura digital autentica a identidade do emissor e, como uma assinatura escrita é difícil de ser falsificada, com uma diferença fundamental - uma assinatura manuscrita é independente do documento que está sendo assinado. Desse modo, se alguém conseguir falsificá-la, poderá usá-

la em múltiplos documentos. Já uma assinatura digital é criada utilizando-se os conteúdos do documento. Portanto, ela será diferente para cada documento que se assine.

2.4.2 Sistemas eletrônicos de pagamentos

O modelo de transações eletrônicas seguras - *secure eletronic transactions* - (SET) é um protocolo para transferências de pagamentos com cartão de crédito criptografadas.

Segundo Albertin (2001) o SET estabelece um padrão único para proteger as compras com cartão realizadas pela internet e em outras redes abertas. Os objetivos da segurança de pagamento são: prover autenticação dos portadores de cartão, vendedores e adquirentes; prover confidencialidade dos dados de pagamento; preservar a integridade dos dados de pagamento; e definir os algoritmos e protocolos necessários para esses serviços de segurança.

O autor afirma que os objetivos declarados nas especificações SET são:

a) confidencialidade de informação;
b) integridade de informação;
c) autenticação da conta do consumidor;
d) autenticação do vendedor; e
e) interoperabilidade.

Albertin (2001) acrescente que o protocolo SET oferece pacotes de dados para todas as transações, e cada transação é assinada com uma assinatura digital. Essa situação faz com que esse protocolo seja o maior consumidor de certificados e faz dos bancos um dos maiores distribuidores deles. O setor bancário é considerado um dos que mais se preocupam com a segurança das assinaturas digitais. Os bancos reconhecem que o comércio na internet requer uma maneira pela qual as pessoas possam verificar a autenticidade de documentos, tais como cheques ou autorizações de cartão de crédito.

No comércio eletrônico essa preocupação é mantida, no entanto muitas pessoas temem o uso de cartões no ambiente virtual. Deitel, Deitel e Steinbuhler (2004) afirmam que, embora o cartão de crédito seja um meio de pagamento

amplamente utilizado para compras on-line, muitas pessoas resistem ao apelo e simplicidade das operações em virtude das preocupações com a segurança. Os clientes temem fraudes praticadas por comerciantes e outros.

Deitel, Deitel e Steinbuhler (2004) ressaltam que, para aceitar pagamentos com cartão de crédito, o comerciante deve ter uma conta bancária. Com o crescimento do e-commerce, foram instituídas contas bancárias específicas para a internet, próprias para as transações com cartão de crédito on-line. Por exemplo, quando se faz uma compra na web, o número do cartão e a data de validade podem ser fornecidos, mas o comerciante não vê o cartão sendo utilizado na compra. As informações são enviadas ao banco no qual o cliente possui conta, que por sua vez verifica as informações sobre a conta do comprador. Isso envolve o banco no qual foi emitido o cartão e a administradora do cartão de crédito. Quando o titular de um cartão de crédito alega que não fez a compra, ou ela foi feita por alguém não autorizado, dá-se o estorno. Quando isso ocorre, a despesa em questão não é responsabilidade do titular. Neste caso, o ônus geralmente é do comerciante.

2.4.3 Site certificado/ seguro

De acordo com Pontes (2008) o *Secure HyperText Transport Protocol* (HTTPS) é o protocolo ou conjunto de regras e códigos com uma camada de segurança que torna a navegação na internet mais segura. Essa camada adicional permite que os dados sejam transmitidos com segurança (através de criptografias) e que se verifique a autenticidade do servidor e do cliente através de certificados digitais.

O autor acrescenta que o HTTP não oferece a mesma segurança do HTTPS porque as informações navegam na rede de uma forma muito parecida com a apresentada na tela ou digitada pelo usuário. O HTTPS é usado para permitir que os navegadores na internet dialoguem com os servidores, mas fornece mais segurança em dois aspectos: encripta os dados trafegados, embaralha-os de forma que somente o destinatário pode entendê-los. Esses dados podem ser interceptados,

mas não são legíveis para as pessoas ou computadores. O HTTPS também garante que o site que o usuário está visualizando é quem diz ser.

Segundo a Cartilha de segurança para a internet, elaborada pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.BR), existem pelo menos dois itens que significam que as informações transmitidas entre o *browser* e o *site* visitado estão sendo criptografadas e que, consequentemente, o site pode ser considerado seguro.

O primeiro item pode ser visualizado no local onde o endereço do *site* é digitado. O endereço deve começar com https:// (diferente do http:// nas conexões normais), onde o **s** indica que o endereço em questão é de um *site* com conexão segura e, portanto, os dados serão criptografados antes de serem enviados, conforme figura abaixo.

FIGURA 1: HTTPS - identificando site com conexão segura.
FONTE: CERT.BR (2009)

O segundo item a ser visualizado corresponde a algum desenho ou sinal, indicando que a conexão é segura. Normalmente, o desenho mais adotado nos *browsers* recentes é de um "cadeado fechado", apresentado na barra de *status*, na parte inferior da janela do *browser* (se o cadeado estiver aberto, a conexão não é segura).

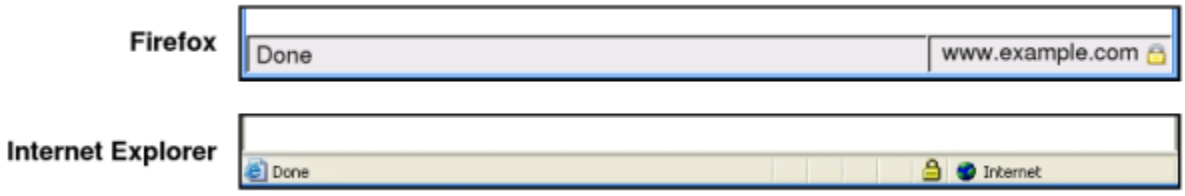

FIGURA 2: CADEADO - identificando site com conexão segura.
FONTE: CERT.BR (2009)

Ao clicar sobre o cadeado, será exibida uma tela que permite verificar as informações referentes ao certificado emitido para a instituição que mantém o site, bem como informações sobre o tamanho da chave utilizada para criptografar os dados.

O usuário deve averiguar as informações do certificado, clicando sobre o cadeado, atentando para a autenticidade e validade do mesmo.

Pontes (2008) considera que muitas vezes os usuários desconhecem a diferença entre navegar em um site HTTP e HTTPS. O autor afirma que o HTTP não oferece certeza absoluta de que o site acessado é realmente quem diz ser. Nesse caso, pode acontecer de um *cracker* interceptar os dados que trafegam e criar um falso sítio de destino, respondendo às requisições do navegador na web. Por exemplo, o usuário pode pensar que está navegando numa loja virtual, mas está, na verdade, interagindo com uma quadrilha que roubará seus dados pessoais, como senhas e números de cartão de crédito.

Pontes (2008) ainda ressalta que, em conjunto com o uso do HTTPS, o usuário precisa estar atento à segurança de seu computador principal, com a utilização de antivírus, *firewalls, antispywares* e outros softwares de proteção.

2.5 DIREITO DO CONSUMIDOR NO COMÉRCIO ELETRÔNICO

De acordo com Volpi Neto (2003), o comércio eletrônico teve sua fase inicial praticada entre grandes corporações financeiras e, posteriormente, por grandes lojas e seus clientes. Dessa forma, inexistia a preocupação com a identidade das partes, com sua evolução a realidade mudou.

> Com o indiscriminado crescimento do comércio eletrônico, na sua chamada "terceira onda", na qual as partes tornaram-se anônimas e seu caráter extraterritorial acentuou-se, começaram a surgir preocupações com a segurança e com a identidade das partes. (VOLPI NETO, 2003 p. 66)

De acordo com O`brien (2006) no Brasil ainda não há uma legislação específica sobre segurança e privacidade na internet, mas continua valendo o Código de Defesa do Consumidor (CDC).

Segundo Relvas (2008) as preocupações com as questões do comércio eletrônico têm avançado através de projetos de lei em discussão no Congresso Nacional, de algumas medidas do Executivo, nos três níveis (federal, estadual e

municipal) e do judiciário nos tribunais superiores e alguns tribunais estaduais, que não se trata do comércio eletrônico propriamente dito, criam antecedentes e experiências para a validade do documento eletrônico.

> No âmbito federal, o governo Brasileiro tem se vangloriado do seu alto grau de automação dos serviços públicos, reconhecendo, portanto, várias transações eletrônicas e através do Decreto 3.587 de 05.09.2000, dá um passo importante nesta seara ao estabelecer normas para a Infra-Estrutura de Chaves Públicas do poder executivo Federal – ICP-Gov, com o fim de se criarem regras de identificação e segurança para os usuários. (RELVAS, 2008, p.105-106)

Ainda de acordo com Relvas (2008), com a evolução desse processo, a Instrução Normativa da Secretaria da Receita Federal - SFR 156 DE 22.12.1999 instituiu os Certificados Eletrônicos para o CPF (Cadastro de Pessoas Físicas) e o CNPJ (Cadastro Nacional de Pessoas Jurídicas), que poderão ser utilizados no relacionamento, por meios eletrônicos, com a Secretaria da Receita Federal. Em 28.06.2001, o governo federal editou a Medida provisória 2.200 que institui a Infraestrutura de Chaves Públicas Brasileiras – ICP-Brasil, o que vem sendo chamado de “cartórios virtuais”.

O objetivo desse instrumento – MP 2.200-2 de 24.08.2001, art. 1º “é garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais bem como a realização de transações eletrônicas seguras” (MP 2.200-2, 2001).

Existem também Projetos de Lei em tramitação no Congresso Nacional sobre o tema. Relvas (2008, p.107-108) cita vários, dentre eles:

- Projeto de lei nº 4.906/01– Dispõe sobre fatura, assinatura e comércio eletrônico.

- Projeto de lei 1589/99 24/9/1999 - dispõe sobre o comércio eletrônico, a validade jurídica do documento eletrônico e a assinatura digital.

2.5.1 Código de Defesa do Consumidor

Manucci (2000) considera que o consumidor que opta em fazer suas transações pela internet, goza indiscutivelmente, de todos os direitos e prerrogativas previstos no Código de Defesa do Consumidor (CDC), haja vista que se trata indiscutivelmente de relação de consumo. Havendo ainda uma relação jurídica entre as partes.

Matte (2001, p. 91-124) ao analisar a aplicação do Código Brasileiro de Defesa do Consumidor nos contratos do comércio eletrônico, através de um estudo de caso em uma loja virtual de comércio eletrônico varejista, concluiu que o CDC, exterioriza a preocupação não somente brasileira sobre as questões de defesa do consumidor, mas reflete uma realidade internacional, em que as compras online são, além de contratos de consumo, relações de consumo.

Nesse sentido Relvas (2008, p. 113) acrescenta que, nos casos de relações de consumo, entende-se que internamente deva prevalecer A LEI 8.078/90.

Não obstante, o autor ressalta a importância de recursos complementares.

> Nos casos de B to C (Business to Consumer), ou seja, relações de consumo, entendemos que internamente deva prevalecer o Código de Defesa do Consumidor, ressaltando-se a necessidade do reconhecimento do documento eletrônico, da assinatura eletrônica ou, pelo menos a equiparação dos negócios jurídicos pela via eletrônica a contratos verbais" (RELVAS, 2008, p.113).

Relvas (2008) ainda faz outras observações em relação à aplicação do CDC.

> Desta feita, entendemos que as aquisições realizadas utilizando-se da internet como meio, instrumento para a viabilização do negócio jurídico, com entrega do produto ou serviço no endereço do consumidor, pode ser comparado ao contrato realizado fora do estabelecimento, assegurando o direito do arrependimento do art.49 do Código de Defesa do Consumidor. (RELVAS, 2008, p.109)

Aplica o Código de Defesa do Consumidor nas relações de consumo, entre fornecedor e consumidor final, para aquisições de produtos quer seja no meio físico ou comprados diretamente online, somente se consumidor e fornecedor estiverem estabelecidos no âmbito nacional.

3 MATERIAL E MÉTODOS

Buscou-se nesta seção descrever os procedimentos metodológicos adotados, bem como os recursos utilizados, na condução desta pesquisa.

3.1 CARACTERIZAÇÃO DA PESQUISA

A presente pesquisa pode ser caracterizada, do ponto de vista de sua natureza, como pesquisa básica que, segundo Silva (2001), é o tipo de pesquisa que objetiva gerar conhecimentos úteis para o avanço da ciência sem aplicação prática prevista. Envolve verdades e interesses universais.

Do ponto de vista de seus objetivos, de acordo com Gil (1996), possui caráter exploratório**,** visando proporcionar maior familiaridade com o problema para torná-lo explícito. Também pode ser considerada, de acordo com os procedimentos técnicos, como bibliográfica, seguida de levantamento de dados.

3.2 PROCEDIMENTOS METODOLÓGICOS

A primeira etapa da pesquisa, após a identificação do problema e definição dos objetivos, foi a pesquisa bibliográfica a respeito do assunto, o que se constituiu na Literatura Pertinente. Foi realizado utilizando-se de materiais já elaborados e publicados sobre o tema da pesquisa, como livros, artigos, normas e alguns sítios na internet.

Após a identificação das principais teorias sobre o assunto, procedeu-se a fase de levantamento de dados.

A técnica de pesquisa adotada, para a coleta de dados, foi à observação direta extensiva, realizada através de aplicação de um questionário, junto a alguns usuários da internet que utilizam o serviço de comércio eletrônico varejista – B2C.

Segundo Lakatos e Marconi (1990 p. 88), “questionário é um instrumento de coleta de dados, constituído por uma série de perguntas, que devem ser respondidas por escrito sem a presença do entrevistador”.

A Elaboração do instrumento de coleta exigiu dedicação e, algumas orientações buscadas junto à literatura foram fundamentais. De acordo com Lakatos e Marconi (1990), o processo de elaboração de um questionário é longo e complexo, exigindo cuidado na seleção das questões, considerando a sua importância para a obtenção de informações válidas. Deve ser limitado em extensão e em finalidade. “Se for muito longo, causa fadiga e desinteresse; se curto demais, corre o risco de não oferecer suficientes informações. Deve conter de 20 a 30 perguntas e demorar cerca de 30 minutos para ser respondido” (LAKATOS e MARCONI 1990, P.90).

Com base nessas informações, elaborou-se um questionário composto por 20 questões fechadas, buscando obter respostas mais objetivas. As perguntas foram ordenadas iniciando com perguntas gerais e explorando questões específicas no final (APÊNDICE A).

Após a elaboração do instrumento de coleta, foi realizado um pré-teste do questionário, aplicando-o a uma amostra de 8 pessoas. Verificadas as falhas, reformulou-se o questionário, alterando alguns itens.

Validado o instrumento de coleta, o questionário foi editado no aplicativo Google docs. Optou-se por essa ferramenta por viabilizar a coleta dos dados de maneira *online* e, principalmente, porque os elementos da amostra são todos usuários da internet.

A amostragem foi não-probabilística, por conveniência, que segundo Laville e Dionne (1999) é o tipo de amostra onde o pesquisador escolhe as pessoas para responder a pesquisa até o momento em que se estima que ter interrogado suficientemente. Segundo Lakatos e Marconi (1990), na amostragem não-probabilística o pesquisador está interessado na opinião de determinados elementos da população, mas não representativos da mesma.

O *link* do questionário, juntamente com a apresentação, foi enviado para 113 pessoas, solicitando-as que respondessem ao questionário e também encaminhassem para que mais usuários da internet, que utilizam o comércio eletrônico, respondessem. O questionário ficou disponível para respostas de 15 de outubro a 20 de novembro de 2009.

No total, 72 pessoas responderam à pesquisa. Por se tratar de um estudo exploratório, considerou-se satisfatório esse número de respondentes.

4 ANÁLISE DOS RESULTADOS

Buscou-se nesta seção, apresentar e analisar os resultados obtidos com a aplicação do questionário. Das 20 questões propostas, apenas as que proporcionaram resultados mais representativos e pertinentes aos objetivos da pesquisa, foram ilustradas nos gráficos. Entretanto, todos os resultados foram considerados na análise.

O questionário proposto foi respondido por 72 usuários da internet, que costumam adquirir produtos através do comércio eletrônico. Das 72 pessoas que participaram da pesquisa, 6,94% possuem o ensino fundamental, 61,11% curso Superior (graduação), 26,39% possuem Pós-graduação – especialização e 5,56% possuem Mestrado, Doutorado ou Pós-Doutorado.

Todos os elementos da amostra utilizaram o *Internet Explorer*, ou outro navegador equivalente, para responder ao questionário de pesquisa - disponibilizado *online*, na internet.

Como resultados da pesquisa obtiveram-se os dados que se seguem.

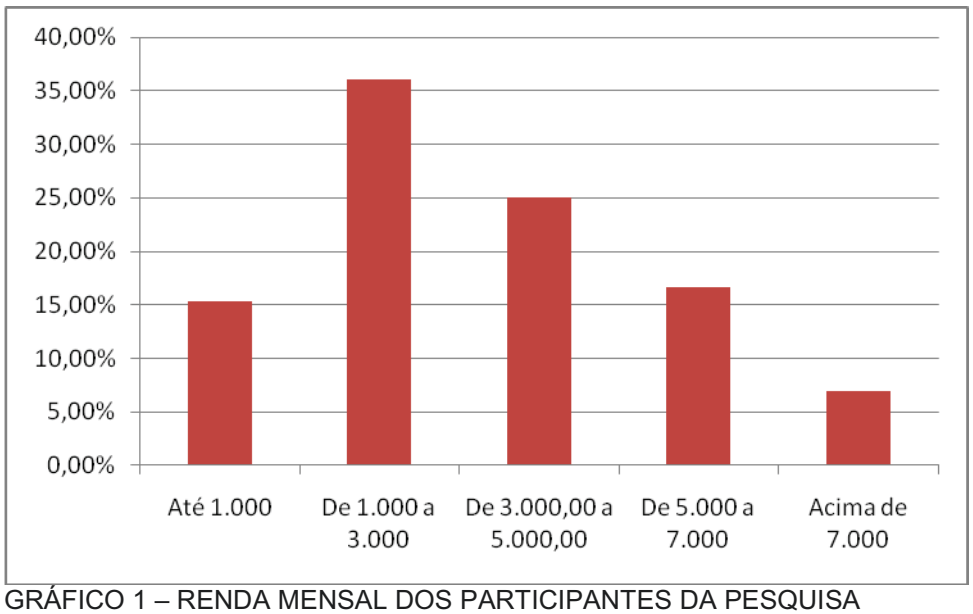

GRÁFICO 1 – RENDA MENSAL DOS PARTICIPANTES DA PESQUISA
FONTE: A autora (2009)

Conforme o gráfico 1, que representa a questão 3 do questionário, a renda mensal com maior número de registros foi a de R$ 1.000,00 a R$ 3.000,00 (36,11%), em seguida a de R$ 3.000,00 a R$ 5.000,00 (25%), posteriormente, a de R$ 5.000, 00 a 7.000,00 (16,67%), na sequência a de até R$ 1.000,00 (15,28%) e por final a de acima de R$ 7.000,00 (6,94%).

Comparando os dados obtidos nesta questão com a frequência com que os participantes utilizam o comércio eletrônico para adquirir bens (questão 4). Verificou-se que, os consumidores que compram com maior freqüência pela internet, na amostra pesquisada, possuem renda mensal de R$3.000,00 a R$ 5.000,00. Das 15 pessoas que possuem renda mensal de R$ 3.000,00 a R$ 5.000,00, 11 delas (73,33%) afirmam comprar pela internet acima de 1 vez/mês - 60% compram de 1 a 3 vezes/mês, 6,66% compram de 3 a 5 vezes/mês e 6,66% compram de 5 a 7 vezes/mês.

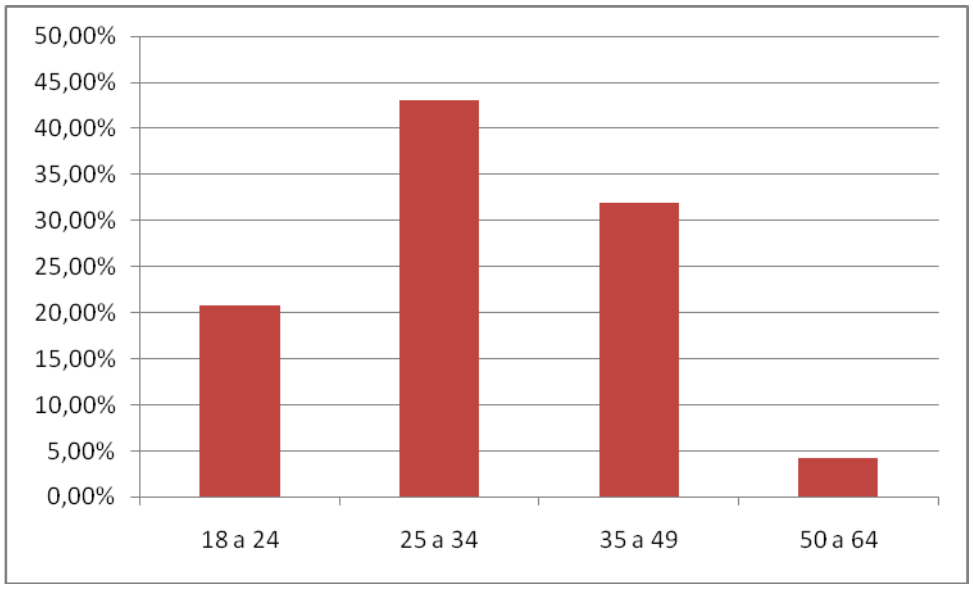

GRÁFICO 2 – FAIXA ETÁRIA.
FONTE: A autora (2009).

No gráfico 2, que corresponde à idade, pode-se observar que houve predominância da faixa etária de 25 a 34 - 43,06%. Em seguida, de 35 a 49 – 31,94%. De 18 a 24 – 20,83%. De 50 a 64 - 4,17%. Não houve registro de pessoa com mais de 64 anos.

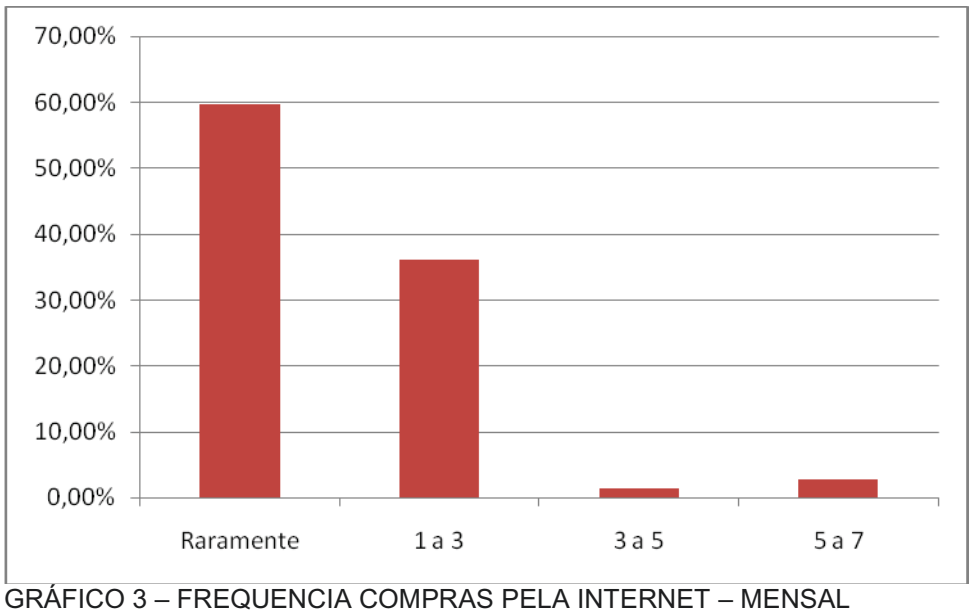

GRÁFICO 3 – FREQUENCIA COMPRAS PELA INTERNET – MENSAL
FONTE: A autora (2009).

Conforme o gráfico 3 - 59,72% realizam compras pela internet raramente (menos de 1 vez/mês). 36,11% - de 1 a 3 vezes/mês, 1,39% – de 3 a 5 vezes/mês e 2,78% - de 5 a 7vezes/mês.

Cabe destacar que, analisando a frequência com que os consumidores compram pela internet com a questão que se, de maneira geral eles estão satisfeitos com o serviço de comércio eletrônico no Brasil, das 29 pessoas que compram pela internet mais de 1 vez/mês, 28 (96,55%), estão satisfeitas. Dessa forma, pode-se afirmar que a frequência com que o consumidor utiliza o comércio eletrônico está, de alguma forma, relacionada com a satisfação em relação ao serviço.

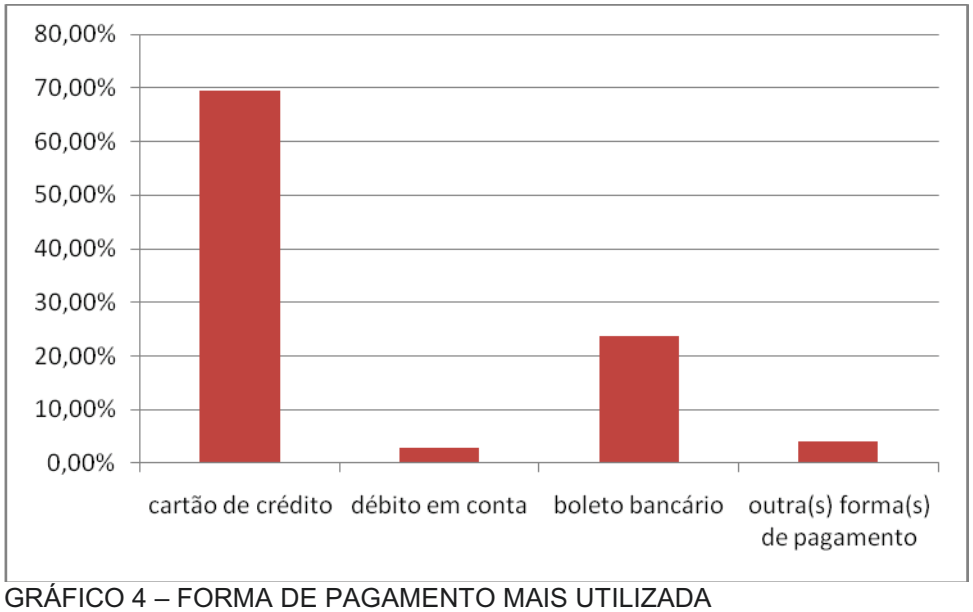

GRÁFICO 4 – FORMA DE PAGAMENTO MAIS UTILIZADA
FONTE: A autora (2009).

Em relação à forma de pagamento mais utilizada nas compras *online*. Pode-se observar que o cartão de crédito é a forma de pagamento mais utilizada pelos respondentes (69,44%). Em seguida o boleto bancário (23,62%), outras formas de pagamento (4,17%). A opção débito em conta ficou com um percentual menor - 2,77%.

Deve-se ressaltar que, apesar de o cartão de crédito ser a forma de pagamento mais utilizado nas compras online, 61,11% das pessoas que responderam à pesquisa, confirmaram que quando efetuam o pagamento com cartão de crédito, sentem receio que o número de seu cartão seja utilizado indevidamente.

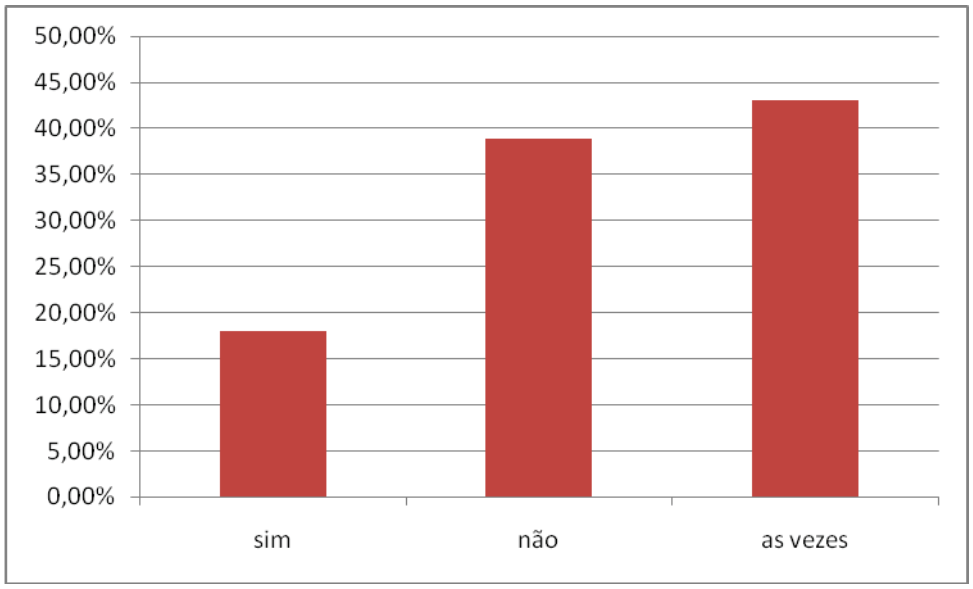

GRÁFICO 5 – COSTUMA LER A POLÍTICA DE PRIVACIDADE E SEGURANÇA
FONTE: A autora (2009).

Ao analisar o gráfico acima, que corresponde aos dados obtidos na questão 7, verificou-se que nem todas as pessoas tem o hábito de ler a política de privacidade e segurança da loja virtual antes de adquirir um bem pela internet. Apenas 18, 05% afirmaram que sim, enquanto 38,89% que não e, 43,06% afirmam que às vezes.

Deve-se ressaltar, entretanto, que de acordo com dados obtidos na questão seguinte (questão 8), apesar das pessoas não ter o hábito de ler, frequentemente, a política de privacidade e segurança da loja virtual, 81,95% costumam buscar informações sobre a qualificação / confiabilidade do fornecedor antes de realizar uma compra pela internet.

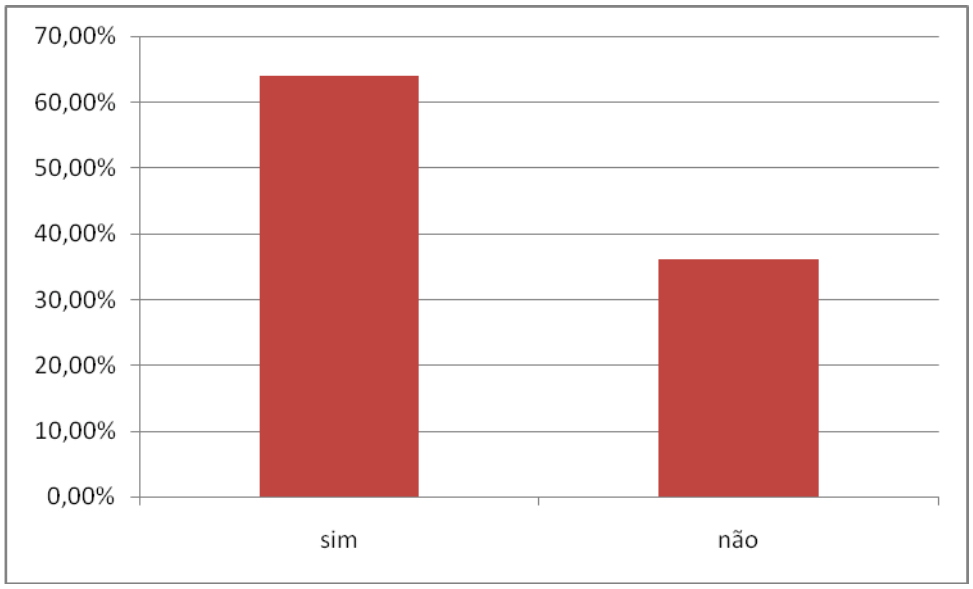

GRÁFICO 6 – CONHECECIMENTO - RECURSOS TECNOLÓGICOS
FONTE: A autora (2009).

Ao serem questionados se conheciam algum recurso tecnológico que visa assegurar a privacidade e a segurança da informação na internet (questão 9), 63,89% assinalaram que sim e, 36,11% que não, conforme gráfico 6.

Em complemento aos dados acima, cabe destacar que, de acordo com dados obtidos na questão 10 - 86,11% realizam compras pela internet, somente em computadores protegidos por *firewalls* e antivírus atualizados e 76,39% afirmaram saber identificar um site certificado/seguro.

No entanto, em relação aos certificados digitais, apenas 56,94%, um pouco mais da metade, alegam saber o que são autoridades certificadoras e para que finalidades são utilizados os certificados digitais.

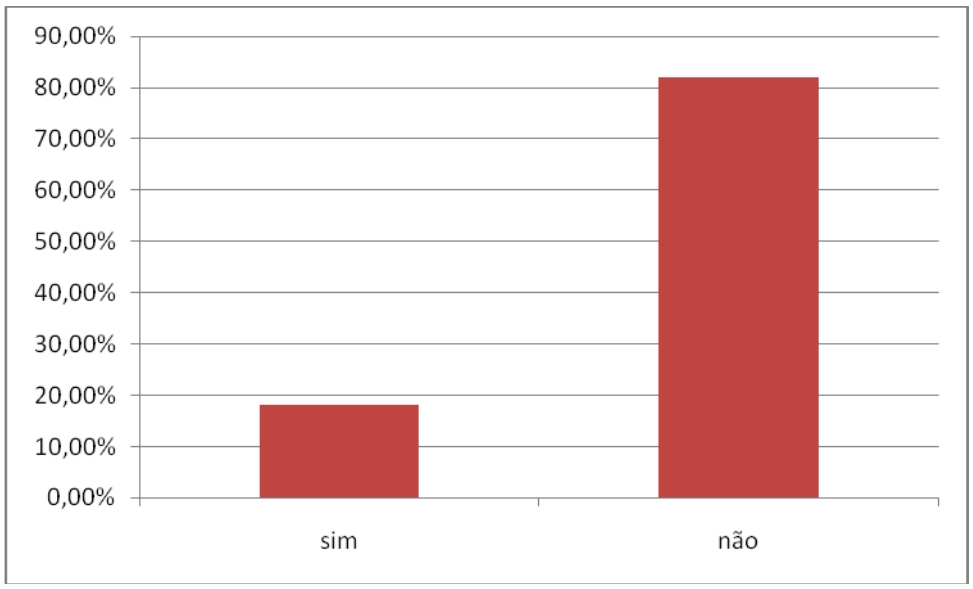

GRÁFICO 7 – CONHECIMENTO SOBRE A LEGISLAÇÃO.
FONTE: A autora (2009).

Em resposta à questão (14) se possuíam algum conhecimento sobre a legislação que visa assegurar o direito do consumidor no âmbito nacional, 81,94% afirmaram não ter conhecimento, conforme gráfico 7.

Por outro lado, de acordo com os dados apresentados na questão 15, percebe-se que apesar de o consumidor não conhecer a legislação, existe certa preocupação em relação a esse aspecto, pois, 95,83% responderam que consideram que deveria existir uma lei específica que regulamentasse as questões de direito na internet, particularmente do direito do consumidor no comércio eletrônico.

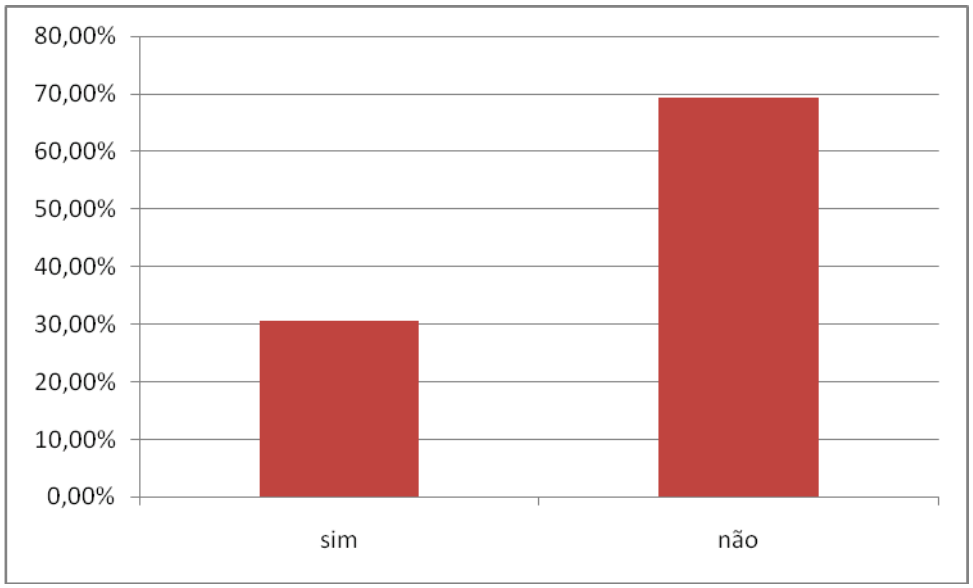

GRÁFICO 8 – JÁ SE ARREPENDEU OU SE SENTIU LESADO NO COMÉRCIO ELETRÔNICO
FONTE: A autora (2009).

Questionado se já havia se arrependido ou se sentido lesado ao adquirir um produto pela internet e o mesmo não atender às expectativas ou as especificações fornecidas pela loja virtual (questão 16), 69,44% respondeu que nunca se arrependeu ou se sentiu lesado, conforme gráfico acima.

No entanto, 30,56% (22 pessoas) responderam que sim. Desse montante, 59,09% (13 pessoas) alegaram não ter conseguido cancelar a compra, na ocasião. (questão 17).

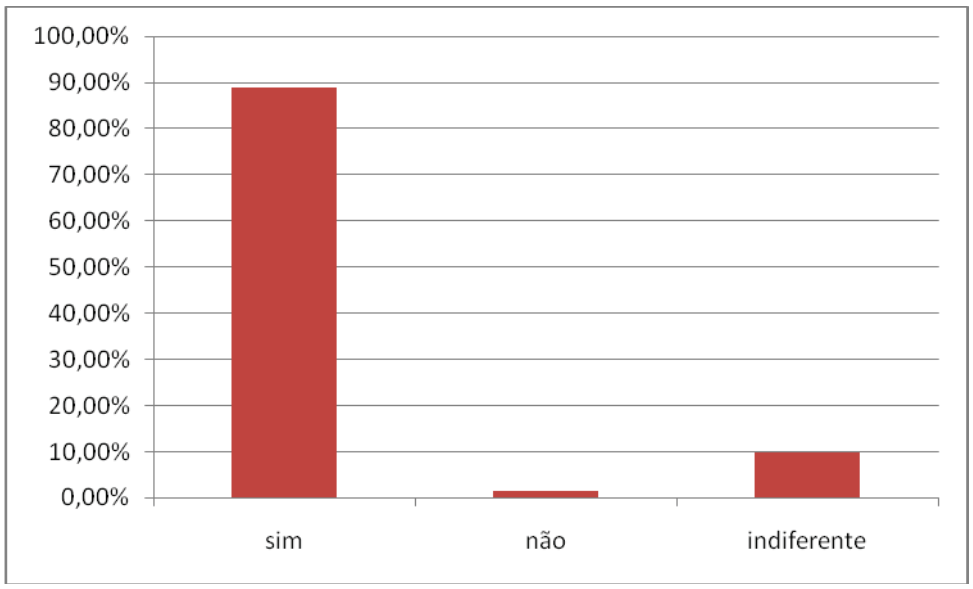

GRÁFICO 9 – GOSTARIA QUE MAIS INFORMAÇÕES FOSSEM DISPONIBILIZADAS
FONTE: A autora (2009)

Em relação à questão 18, representada no gráfico 9, se gostariam que as lojas virtuais viabilizassem mais informações sobre segurança e direito do consumidor em seus sites, 88,89% responderam que sim, 9,72% - indiferente, e apenas 1,39% que não gostariam.

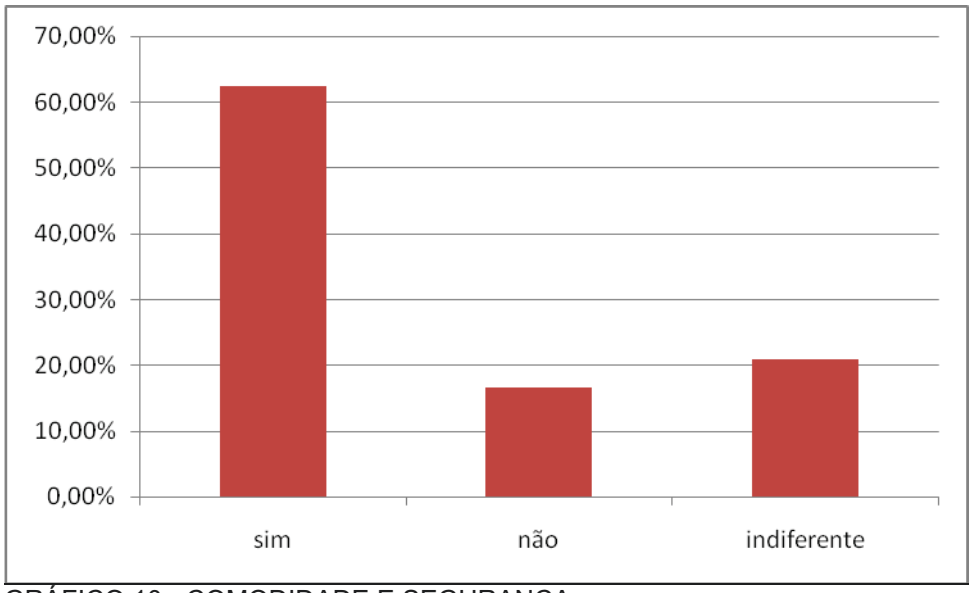

GRÁFICO 10 - COMODIDADE E SEGURANÇA
FONTE: A autora (2009)

Em relação à questão 19, se consideravam que o comércio eletrônico proporciona maior comodidade e segurança que o comércio tradicional, de acordo

com as respostas obtidas, 62,5% considera que sim, 16,67% responderam que não e, 20,83% consideram indiferente.

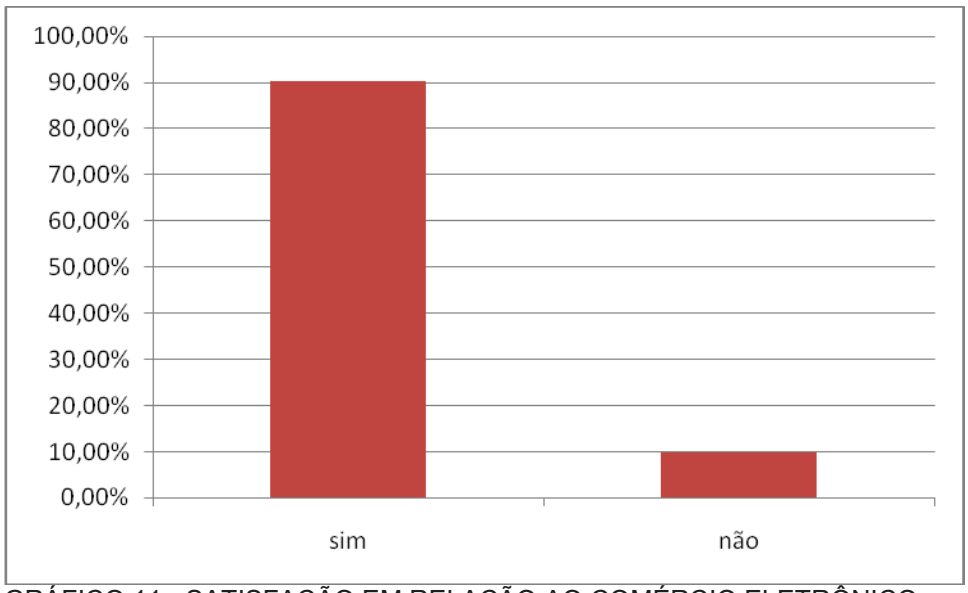

GRÁFICO 11 - SATISFAÇÃO EM RELAÇÃO AO COMÉRCIO ELETRÔNICO
FONTE: A autora (2009).

Na ultima questão, representada pelo gráfico acima, questionou-se de maneira geral, o usuário está satisfeito com os serviços de comércio eletrônico na internet, 90,28% responderam que sim e apenas 9,72% que não.

Desses usuários que não estão satisfeitos com o comércio eletrônico 85,71% responderam na questão 18, que gostariam que as lojas virtuais viabilizassem, em seus sites, mais informações sobre segurança e direito do consumidor no comércio eletrônico. O que leva a concluir que a satisfação em relação ao serviço está relacionada com as necessidades informacionais do usuário/cliente.

5 DISCUSSÃO

De acordo com os resultados obtidos, percebe-se a importância de pesquisas acerca do tema abordado neste trabalho. As tecnologias da informação proporcionaram, de maneira geral, muitos benefícios para a sociedade. Entretanto, muitos problemas surgiram com a evolução, de certa forma, intempestiva dessas tecnologias.

A internet, por ser um ambiente complexo e relativamente novo, apresenta peculiaridades muitas vezes desconhecidas por seus usuários.

Verificou-se, na amostra pesquisada, que nem todos os usuários do comércio eletrônico conhecem as ferramentas tecnológicas que visam assegurar a segurança e a privacidade das informações na internet. Em relação à legislação, que assegura seus direitos, a situação é ainda mais crítica.

Essas questões carecem atenção, pois enquanto o usuário não se sentir seguro em utilizar o serviço, a adoção dessa modalidade de comércio ficará limitada.

Para que se explorem todas as potencialidades do comércio eletrônico B2C, é necessário que os consumidores tenham confiança no serviço e, principalmente, possam utilizá-lo de forma segura. Uma maneira de proporcionar é disponibilizando informações nas lojas virtuais.

Embora a maioria dos usuários responder estar satisfeito com o comércio eletrônico, pode-se verificar que o consumidor do comércio eletrônico gostaria que as lojas virtuais viabilizassem mais informações sobre segurança e direito do consumidor em seus sites.

Apesar de o consumidor, muitas vezes, desconhecer os recursos que visam garantir a segurança e privacidade na internet, verificou-se que, de certa forma, se preocupa com a questão.

Em face do exposto, considera-se importante que as lojas virtuais viabilizem informações sobre segurança das transações *online* e direito do consumidor no comércio eletrônico B2C, em suas lojas virtuais. Para que assim os usuários dessa modalidade de comércio se sintam mais seguros e utilizem o serviço com maior frequência.

6 CONSIDERAÇÕES FINAIS

O propósito principal deste estudo foi levantar as condições atuais de segurança para o consumidor do comércio eletrônico B2C, no âmbito nacional, sob os aspectos tecnológicos e legais.

Do ponto de vista tecnológico verificou-se que, nos últimos anos, muitos recursos foram criados visando garantir a segurança das informações que trafegam pela internet. Entretanto, a adoção desses recursos pelas lojas virtuais não é compulsória. Ficando o consumidor responsável por analisar e decidir se corre o risco comprando em uma loja que não proporciona segurança, ou não.

Pode-se observar que a criptografia e a certificação digital são os recursos mais indicados para garantir a segurança e a privacidade das informações na internet.

Em relação às normas e legislação, constatou-se que existe certa preocupação nas esferas públicas no sentido de criar mecanismos para a resolução de conflitos na internet. Além da MP 2200-2/01, existem vários projetos de Lei, elaborados com a finalidade de regulamentar e solucionar algumas questões relacionadas ao comércio eletrônico. Entretanto, não há muito progresso nesse sentido.

Por entender que as transações realizadas no ambiente virtual também se configuram relações de consumo, no caso do comércio eletrônico B2C, aplica-se o CDC para assegurar os direitos do consumidor.

Através do levantamento de dados, pode-se verificar que alguns respondentes não conhecem os recursos tecnológicos que visam garantir a segurança e privacidade na internet. No tocante à legislação, o desconhecimento é ainda maior. Muitos, inclusive, já se sentiram lesados no comércio eletrônico. A maioria alega estar satisfeito em relação ao serviço, não obstante, gostaria que as lojas virtuais viabilizassem, em seus sites, mais informações sobre segurança e direito do consumidor. Vale lembrar também que a maioria utiliza raramente o comércio eletrônico.

Em face do exposto, não se pode afirmar que o comércio eletrônico B2C pode ser considerado seguro e confiável para o consumidor, do ponto de vista tecnológico e legal. O ambiente virtual, como qualquer outro ambiente, não é

totalmente seguro. O comércio eletrônico apresenta praticamente as mesmas condições de segurança que o comércio tradicional. Contudo, exige mais cautela e atenção do consumidor em sua utilização.

Sugere-se que as empresas que exploram essa modalidade de comércio, façam uso dos recursos disponíveis de modo a garantir a segurança e a privacidade dos consumidores. Também devem viabilizar em seus *sites,* na internet, informações sobre segurança e direito do consumidor. Assim, a confiabilidade deve ser adquirida dia após dia, por meio da qualidade, responsabilidade e comprometimento nos serviços oferecidos.

Em suma, considera-se que os resultados desta pesquisa foram satisfatórios, haja vista que os objetivos do trabalho foram alcançados. Entretanto, por se tratar de um assunto relacionado à internet, que se trata de um ambiente complexo e dinâmico, muito ainda tem a ser explorado.

Cabe lembrar as limitações do levantamento de dados, realizado nesta pesquisa. O questionário foi aplicado a uma amostra não-probabilística, ou seja, os resultados obtidos limitam-se a amostra pesquisada, servindo apenas de referência para o desenvolvimento do estudo.

Como trabalhos futuros, além de se aplicar o questionário proposto nesta pesquisa a uma amostra probabilísta – onde todos os elementos da população tem a mesma probabilidade de serem selecionados para responder à pesquisa - a fim de se obter resultados passíveis de serem generalizados, recomenda-se também repetir a pesquisa em outras modalidades de comércio, haja vista que este estudo limita-se a uma modalidade de comércio eletrônico - B2C, no âmbito nacional.

Considera-se importante também pesquisar porque alguns usuários da internet não utilizam o comércio eletrônico.

REFERÊNCIAS

ALBERTIN, A. L. **Comércio eletrônico:** modelo, aspectos e contribuições de sua aplicação. 3. Ed. São Paulo: Atlas, 2001.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO/IEC 17799 - tecnologia da informação**: código de prática para a gestão da segurança da informação. Rio de Janeiro, 2001.

BEAL, A. **Segurança da informação**: princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo: Atlas, 2005.

BRASIL. **Medida Provisória N.2.200-2, de 24 de agosto de 2001.** Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, e dá outras providências. Disponível em: <http://www.iti.gov.br/twiki/pub/Certificacao/MedidaProvisoria/MEDIDA_PROVIS_RIA_2_200_2_D.PDF >. Acesso em: 03 jun.2009.

BRASIL. **Lei nº 8.078 - de 11 de setembro de 1990 -** Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/LEIS/L8078.htm>. Acesso em: 02 set. 2009.

CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL – CERT.BR. **Cartilha de Segurança para a Internet**. Parte IV: Fraudes na Internet. Disponível em: <http://cartilha.cert.br/fraudes/> Acesso em: 10 nov. 2009.

DEITEL, H. M.; DEITEL, P. J; STEINBUHLER, K. **E-business e e-commerce para administradores.** São Paulo: Pearson Education do Brasil, 2004.

DELOITTE. **Comércio online**: as relações das empresas com seus públicos na internet. 2009. Disponível em: <http://www.deloitte.com/assets/Dcom-Brazil/Local%20Assets/Documents/ComercioOnline1.pdf>. Acesso em: 15 de dez. 2009.

DIAS, C. **Segurança e Auditoria da Tecnologia da Informação.** Rio de Janeiro: Axcel Books, 2000.

E-COMMERCE.ORG: tudo sobre comércio eletrônico. Estatísticas Ecommerce. Disponível: < http://www.e-commerce.org.br/stats.php >. Acesso em: 04 set. 2009.

FERREIRA, F. N. F. **Segurança da informação**. Rio de Janeiro: Ciência Moderna, 2003.

GIL, A. C. **Como elaborar projetos de pesquisa**. São Paulo: Atlas, 1996.

Instituto Nacional de Tecnologia da Informação (ITI). **Certificação Digital**. Disponível em: http://www.iti.gov.br/twiki/bin/view/Main/WebHome. Acesso em: 16 nov. 2009.

LAKATOS, E. M; MARCONI, M. de A. **Técnicas de Pesquisa**. São Paulo: Atlas, 1990.

LAUDON, K. C.; LAUDON, J. P. **Gerenciamento de sistemas de informação**. 3. Ed. Rio de Janeiro: LTC - Livros Técnicos e Científicos Editora S.A, 2001.

_____. **Sistemas de informações gerenciais**. 7. ed. São Paulo: Pearson Prentice Hall, 2007.

LAVILLE, C.; DIONNE, J. **A construção do saber**: manual de metodologia da pesquisa em ciências humanas. Porto alegre: Artemed; Belo Horizonte: Editora UFMG, 1999.

MANUCCI, D. D. **Código de Defesa do Consumidor x Internet.** Disponível em: < http://jus2.uol.com.br/doutrina/texto.asp?id=1801 > Acesso em: 13 set. 2009.

MATTE, M. de S. **Internet:** comércio eletrônico: aplicabilidade do código de defesa do consumidor nos contratos de e-commerce. São Paulo: LTR, 2001.

O´BRIEN, J. **Sistemas de informação e as decisões gerenciais na era da internet**. 2 ed. São Paulo: Saraiva, 2006.

PONTES, F. **INTERNET:** HTTP ou HTTPS, você sabe qual é a diferença? 2008. Disponível em: <http://wnews.uol.com.br/site/noticias/materia_especial.php?id_secao=17&id_conteudo=674> Acesso em: 02 nov. 2009.

RELVAS, M. **Comércio Eletrônico**: aspectos contratuais da relação de consumo. Curitiba: Juruá, 2008.

SILVA, E. L. da; MENEZES, E. M. **Metodologia da pesquisa e elaboração de dissertação**. 2001. Disponível em: <http://projetos.inf.ufsc.br/arquivos/Metodologia%20da%20Pesquisa%203a%20edicao.pdf> Acesso em: 15 jun. 2009.

TURBAN; McLEAN, E.; WETHERBE, J. **Tecnologia da informação para gestão:** transformando os negócios na economia digital. São Paulo: Bookman, 2004.

VOLPI NETO, A. **Comércio eletrônico**: direito e segurança. Curitiba: Juruá, 2003.

APÊNDICE A – QUESTIONÁRIO DE PESQUISA

QUESTIONÁRIO – TRABALHO DE CONCLUSÃO DE CURSO

O objetivo deste questionário é coletar informações junto a usuários da internet que utilizam o serviço de comercio eletrônico, visando explorar alguns elementos dessa modalidade de comércio.

A sua participação nesta pesquisa será voluntária e anônima. Todos os dados recolhidos serão tratados com confidencialidade e utilizados somente para fins acadêmicos.

A sua colaboração é extremamente importante para o prosseguimento e êxito deste trabalho.

Desde já, agradeço a sua participação.

Roseli Pessin Leal
Graduanda em Gestão da Informação
Universidade Federal do Paraná - UFPR

1. Faixa etária

( ) De 18 a 24

( ) De 25 a 34

( ) De 35 a 49

( ) De 50 a 64

( ) Acima de 65

2. Grau de instrução

( ) Ensino fundamental

( ) Ensino médio

( ) Superior (graduação)

( ) Pós-graduação - especialização

( ) Pós-graduação – Mestrado, Doutorado, Pós-Doutorado

3. Renda mensal

( ) Até R$ 1.000,00

( ) De R$ 1.000 a 3.000,00

( ) De R$ 3.000,00 a R$ 5.000,00

( ) De R$ 5.000,00 a R$ 7.000,00

( ) Acima de R$ 7.000,00

4. Realiza compras pela internet com que frequência?

( ) raramente (menos de 1 vez/mês)

( ) 1 a 3 vezes/mês

( ) 3 a 5 vezes/mês

( ) 5 a 7 vezes/mês

( ) Mais de 7 vezes/mês

5. Costuma utilizar qual forma de pagamento nas compras realizadas *online*?

(Assinale a opção utilizada com maior freqüência)

( ) cartão de crédito

( ) débito em conta

( ) boleto bancário

( ) outra(s) forma(s) de pagamento

6. Quando realiza uma compra pela internet e efetua o pagamento com cartão de crédito, normalmente, sente receio que o número de seu cartão seja utilizado indevidamente?

( ) sim

( ) não

7. Costuma ler a política de privacidade e segurança da loja virtual antes de realizar uma compra pela internet?

( ) sim

( ) não

( ) às vezes

8. Costuma buscar informações sobre a qualificação/confiabilidade do fornecedor antes de fechar uma compra na internet?

( ) sim

( ) não

( ) às vezes

9. Conhece algum(s) recurso(s) tecnológico(s) que visa(m) assegurar a privacidade e a segurança da informação na internet?

( ) sim

( ) não

10. Realiza compras pela internet somente em computadores protegidos por firewalls e antivírus atualizados?

( ) sim

( ) não

11. Sabe identificar um site certificado ou "site seguro"?

( ) sim

( ) não

12. Sabe o que são autoridades certificadoras e para que finalidade são utilizados os certificados digitais?

( ) sim

( ) não

13. Já realizou uma compra pela internet de fornecedores estabelecidos fora do Brasil?

( ) sim

( ) não

( ) não se lembra

14. Tem algum conhecimento sobre a legislação que visa assegurar o direito do consumidor no comércio eletrônico, no âmbito nacional?

( ) sim

( ) não

15. Considera que deveria existir uma lei específica, que regulamentasse as questões de direito na internet, particularmente do direito do consumidor no comércio eletrônico?

( ) sim

( ) não

( ) indiferente

16. Já se arrependeu, ou se sentiu lesado, ao adquirir um produto pela internet e o mesmo não atender suas expectativas ou as especificações fornecidas pela loja virtual?

(Se resposta = Não, pule a questão 17)

( ) sim

( ) não

17. Na ocasião, conseguiu cancelar a compra?

( ) sim

( ) não

18.Gostaria que as lojas virtuais viabilizassem mais informações sobre segurança e direito do consumidor em seus sites?

( ) sim

( ) não

( ) indiferente

19. Considera que o comércio eletrônico proporciona maior comodidade e segurança que o comércio tradicional?

( ) sim

( ) não

( ) indiferente

20. De maneira geral, está satisfeito com os serviços de comércio eletrônico na internet?

( ) sim

( ) não

ANEXO A – MEDIDA PROVISÓRIA 2.220-2 DE 24 DE AGOSTO DE 2001

MEDIDA PROVISÓRIA Nº 2.200-2, DE 24 DE AGOSTO DE 2001
Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências.

O **PRESIDENTE DA REPÚBLICA**, no uso da atribuição que lhe confere o art. 62º da Constituição, adota a seguinte Medida Provisória, com força de lei:

Art. 1º Fica instituída a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras.

Art. 2º A ICP-Brasil, cuja organização será definida em regulamento, será composta por uma autoridade gestora de políticas e pela cadeia de autoridades certificadoras composta pela Autoridade Certificadora Raiz - AC Raiz, pelas Autoridades Certificadoras - AC e pelas Autoridades de Registro AR.

Art. 3º A função de autoridade gestora de políticas será exercida pelo Comitê Gestor da ICP-Brasil, vinculado à Casa Civil da Presidência da República e composto por cinco representantes da sociedade civil, integrantes de setores interessados, designados pelo Presidente da República, e um representante de cada um dos seguintes órgãos, indicados por seus titulares:

I - Ministério da Justiça;

II - Ministério da Fazenda;

III - Ministério do Desenvolvimento, Indústria e Comércio Exterior;

IV - Ministério do Planejamento, Orçamento e Gestão;

V - Ministério da Ciência e Tecnologia;

VI - Casa Civil da Presidência da República; e

VII - Gabinete de Segurança Institucional da Presidência da República.

§ 1º A coordenação do Comitê Gestor da ICP-Brasil será exercida pelo representante da Casa Civil da Presidência da República.

§ 2º Os representantes da sociedade civil serão designados para períodos de dois anos, permitida a recondução.

§ 3º A participação no Comitê Gestor da ICP-Brasil é de relevante interesse público e não será remunerada.

§ 4º O Comitê Gestor da ICP-Brasil terá uma Secretaria-Executiva, na forma do regulamento.

Art. 4º Compete ao Comitê Gestor da ICP-Brasil:

I - adotar as medidas necessárias e coordenar a implantação e o funcionamento da ICP-Brasil;

II - estabelecer a política, os critérios e as normas técnicas para o credenciamento das AC, das AR e dos demais prestadores de serviço de suporte à ICP-Brasil, em todos os níveis da cadeia de certificação;

III - estabelecer a política de certificação e as regras operacionais da AC Raiz;

IV - homologar, auditar e fiscalizar a AC Raiz e os seus prestadores de serviço;
V - estabelecer diretrizes e normas técnicas para a formulação de políticas de certificados e regras operacionaisdas AC e das AR e definir níveis da cadeia de certificação;

VI - aprovar políticas de certificados, práticas de certificação e regras operacionais, credenciar e autorizar o funcionamento das AC e das AR, bem como autorizar a AC Raiz a emitir o correspondente certificado;

VII - identificar e avaliar as políticas de ICP externas, negociar e aprovar acordos de certificação bilateral, de certificação cruzada, regras de interoperabilidade e outras formas de cooperação internacional, certificar, quando for o caso, sua compatibilidade com a ICP-Brasil, observado o disposto em tratados, acordos ou atos internacionais; e

VIII - atualizar, ajustar e revisar os procedimentos e as práticas estabelecidas para a ICP-Brasil, garantir sua compatibilidade e promover a atualização tecnológica do sistema e a sua conformidade com as políticas de segurança.

Parágrafo único. O Comitê Gestor poderá delegar atribuições à AC Raiz.

Art. 5º À AC Raiz, primeira autoridade da cadeia de certificação, executora das Políticas de Certificados e normas técnicas e operacionais aprovadas pelo Comitê Gestor da ICP-Brasil, compete emitir, expedir, distribuir, revogar e gerenciar os certificados das AC de nível imediatamente subseqüente ao seu, gerenciar a lista de certificados emitidos, revogados e vencidos, e executar atividades de fiscalização e auditoria das AC e das AR e dos prestadores de serviço habilitados na ICP, em conformidade com as diretrizes e normas técnicas estabelecidas pelo Comitê Gestor da ICP-Brasil, e exercer outras atribuições que lhe forem cometidas pela autoridade gestora de políticas.
Parágrafo único. É vedado à AC Raiz emitir certificados para o usuário final.

Art. 6º Às AC, entidades credenciadas a emitir certificados digitais vinculando pares de chaves criptográficas ao respectivo titular, compete emitir, expedir, distribuir, revogar e gerenciar os certificados, bem como colocar à disposição dos usuários listas de certificados revogados e outras informações pertinentes e manter registro de suas operações.
Parágrafo único. O par de chaves criptográficas será gerado sempre pelo próprio titular e sua chave privada de assinatura será de seu exclusivo controle, uso e conhecimento.

Art. 7º Às AR, entidades operacionalmente vinculadas a determinada AC, compete identificar e cadastrar usuários na presença destes, encaminhar solicitações de certificados às AC e manter registros de suas operações.

Art. 8º Observados os critérios a serem estabelecidos pelo Comitê Gestor da ICP-Brasil, poderão ser credenciados como AC e AR os órgãos e as entidades públicos e as pessoas jurídicas de direito privado.

Art. 9º É vedado a qualquer AC certificar nível diverso do imediatamente subseqüente ao seu, exceto nos casos de acordos de certificação lateral ou cruzada, previamente aprovados pelo Comitê Gestor da ICP-Brasil.

Art. 10º Consideram-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos de que trata esta Medida Provisória.

§ 1º As declarações constantes dos documentos em forma eletrônica produzidos com a utilização de processo de certificação disponibilizado pela ICP-Brasil presumem-se verdadeiros em relação aos signatários, na forma do art.131 da Lei nº 3.071, de 1º de janeiro de 1916 - Código Civil.

§ 2º O disposto nesta Medida Provisória não obsta a utilização de outro meio de comprovação da autoria e integridade de documentos em forma eletrônica, inclusive os que utilizem certificados não emitidos pela ICP-Brasil,
desde que admitido pelas partes como válido ou aceito pela pessoa a quem for oposto o documento.

Art. 11º A utilização de documento eletrônico para fins tributários atenderá, ainda, ao disposto no art. 100 da Lei no 5.172, de 25 de outubro de 1966 - Código Tributário Nacional.

Art. 12º Fica transformado em autarquia federal, vinculada ao Ministério da Ciência e Tecnologia, o Instituto Nacional de Tecnologia da Informação - ITI, com sede e foro no Distrito Federal.

Art. 13º O ITI é a Autoridade Certificadora Raiz da Infra-Estrutura de Chaves Públicas Brasileira.

Art. 14º No exercício de suas atribuições, o ITI desempenhará atividade de fiscalização, podendo ainda aplicar sanções e penalidades, na forma da lei.

Art. 15º Integrarão a estrutura básica do ITI uma Presidência, uma Diretoria de Tecnologia da Informação, uma Diretoria de Infra-Estrutura de Chaves Públicas e uma Procuradoria-Geral.
Parágrafo único. A Diretoria de Tecnologia da Informação poderá ser estabelecida na cidade de Campinas, no Estado de São Paulo.

Art. 16º Para a consecução dos seus objetivos, o ITI poderá, na forma da lei, contratar serviços de terceiros.

§ 1º O Diretor-Presidente do ITI poderá requisitar, para ter exercício exclusivo na Diretoria de Infra-Estrutura de Chaves Públicas, por período não superior a um ano, servidores, civis ou militares, e empregados de órgãos e entidades integrantes da Administração Pública Federal direta ou indireta, quaisquer que sejam as funções a serem exercidas.

§ 2º Aos requisitados nos termos deste artigo serão assegurados todos os direitos e vantagens a que façam jus no órgão ou na entidade de origem, considerando-se o período de requisição para todos os efeitos da vida funcional, como efetivo exercício no cargo, posto, graduação ou emprego que ocupe no órgão ou na entidade de origem.

Art. 17º Fica o Poder Executivo autorizado a transferir para o ITI:

I - os acervos técnico e patrimonial, as obrigações e os direitos do Instituto Nacional de Tecnologia da Informação
do Ministério da Ciência e Tecnologia; e

II - remanejar, transpor, transferir, ou utilizar, as dotações orçamentárias aprovadas na Lei Orçamentária de 2001, consignadas ao Ministério da Ciência e Tecnologia, referentes às atribuições do órgão ora transformado, mantida a mesma classificação orçamentária, expressa por categoria de programação em seu menor nível, observado o disposto no § 2º do art. 3º da Lei no 9.995, de 25 de julho de 2000, assim como o respectivo detalhamento por esfera orçamentária, grupos de despesa, fontes de recursos, modalidades de aplicação e identificadores de uso.

Art. 18º Enquanto não for implantada a sua Procuradoria Geral, o ITI será representado em juízo pela Advocacia Geral da União.

Art. 19º Ficam convalidados os atos praticados com base na Medida Provisória no 2.200-1, de 27 de julho de 2001.

Art. 20º Esta Medida Provisória entra em vigor na data de sua publicação.
Brasília, 24 de agosto de 2001; 180º da Independência e 113º da República.

FERNANDO HENRIQUE CARDOSO

José Gregori

Martus Tavares

Ronaldo Mota Sardenberg

Pedro Parente