UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL

ESCOLA DE ADMINISTRAÇÃO

PROGRAMA DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO

Gilson Fabeny

FATORES GERADORES DE RESISTÊNCIA AO USO DO *INTERNET BANKING* NO BANCO DO BRASIL S.A.: Um Estudo de Caso na Agência de Itapema SC

Porto Alegre
2007

Gilson Fabeny

FATORES GERADORES DE RESISTÊNCIA AO USO DO *INTERNET BANKING* NO BANCO DO BRASIL S.A.: Um Estudo de Caso na Agência de Itapema SC

Trabalho de conclusão de curso de Especialização apresentado ao Programa de Pós-Graduação em Administração da Universidade Federal do Rio Grande do Sul, como requisito parcial para a obtenção do título de Especialista em Administração – Gestão em Negócios Financeiros.

Orientadora: Prof. Raquel Janissek Muniz

Porto Alegre
2007

Gilson Fabeny

FATORES GERADORES DE RESISTÊNCIA AO USO DO *INTERNET BANKING* NO BANCO DO BRASIL S.A.: Um Estudo de Caso na Agência de Itapema SC

Trabalho de conclusão de curso de Especialização apresentado ao Programa de Pós-Graduação em Administração da Universidade Federal do Rio Grande do Sul, como requisito parcial para a obtenção do título de Especialista em Administração – Gestão em Negócios Financeiros.

Conceito final:
Aprovado em ..... de .....de.....

BANCA EXAMINADORA

_____
Prof. Dr. ..... – Instituição

_____
Prof. Dr. ..... – Instituição

_____
Orientador – Prof. Dra. Raquel Janissek Muniz
Universidade Federal do Rio Grande do Sul

“A felicidade é um bem que se multiplica ao ser dividido”.

(Marxwell Maltz)

Agradeço à Prof. Dra. Raquel Janissek Muniz, pelas orientações e direcionamentos recebidos durante a elaboração deste trabalho.

À minha esposa e filho, pelo apoio e colaboração recebidos.

Aos colegas da agência de Itapema, pela colaboração durante o desenvolvimento dos trabalhos.

À Deus, que sempre está conosco.

RESUMO

As inovações tecnológicas revolucionaram o sistema financeiro e têm demonstrado que os investimentos em tecnologias de informação geram uma crescente lucratividade, redução de custos e vantagem competitiva. Elevados investimentos foram realizados com o objetivo de atrair o maior número possível de clientes a este ambiente, eliminando em muitos momentos a presença do cliente na agência. A importância desta questão reside no fato de que a adoção e fortalecimento de políticas corretas, voltadas para as necessidades dos usuários e a identificação de possíveis falhas deve ser uma constante para se evitar a perda de mercado. Além disso, o grande número de transações realizadas em uma agência bancária tem como conseqüência custos operacionais elevados que podem ser reduzidos com a utilização do sistema de *Internet Banking*. Assim, este estudo teve por objetivo principal identificar os principais fatores geradores de resistência ao uso do *Internet Banking*, e como objetivos específicos os serviços mais demandados através deste canal e a satisfação dos clientes usuários. Para o levantamento dos dados, foi utilizada a pesquisa qualitativa do tipo "*survey*", com a aplicação de questionário junto aos clientes do Banco do Brasil da agência de Itapema (SC). Entre os diversos atributos levantados na pesquisa feita com os usuários do *Internet Banking* como sendo as possíveis razões para a restrição do uso do sistema alguns índices se destacaram, principalmente o fator segurança. Em segundo lugar, estão aqueles que preferem outras formas de atendimento, dado este reforçado pelos tipos de transações realizadas já que as transações como aplicações e resgates, aquisição de produtos, empréstimos e transferências não são citadas pelos entrevistados.

PALAVRAS-CHAVE

Internet Banking, fatores geradores de resistência, segurança na *internet*.

LISTA DE ILUSTRAÇÕES

SUMÁRIO

1 INTRODUÇÃO

O início da participação do Brasil na *Internet* ocorreu com a iniciativa das comunidades acadêmicas de São Paulo e Rio de Janeiro em 1988 com o estabelecimento de contatos com instituições de outros países para o compartilhamento de dados por meio de uma rede de computadores. Nos anos de 1992 e 1993 foi desenvolvida a estrutura física para sua utilização, ocorrendo sua liberação para fins comerciais em 1995.

A *internet* transformou rapidamente as relações entre empresas e clientes e consolidou-se como um importante canal de vendas e uma poderosa ferramenta com as mais variadas utilizações, contribuindo para a realização de mais e melhores negócios.

A primeira aplicação de *Internet Banking* foi desenvolvida pelo banco Bradesco, posteriormente seguido pela maioria dos bancos brasileiros. O setor financeiro, pioneiro na ampla utilização do comércio eletrônico no Brasil, acredita e demonstra que investimentos em TI provocam uma crescente lucratividade ou uma redução de custos e, fundamentalmente, uma vantagem competitiva.

Assim como no mundo, a popularização da *Internet* no Brasil ocorre em grande escala. A ampliação das linhas telefônicas, a sofisticação e barateamento dos artigos tecnológicos, o surgimento de provedores gratuitos e de novas tecnologias de acesso contribuem para a aceitação crescente pelos consumidores.

Esses facilitadores proporcionaram um aumento de 49,7% no número de usuários de *Internet Banking* em 2005, chegando a 26,3 milhões, segundo dados da Federação Brasileira de Bancos (FEBRABAN). No entanto, em 2006 o número de clientes permaneceu praticamente estável, com uma variação de apenas 3,8%, com 27,3 milhões de usuários.

A soma destes e de outros fatores fez com que a *web* ocupasse seu espaço no mercado financeiro. Os bancos realizaram grandes investimentos em automação e informatização para racionalizar e reduzir os custos de seus processos de

negócios, produtos e serviços, apresentando diversas vantagens aos clientes que foram direcionados aos novos canais de atendimento.

As mudanças ocorridas posicionaram os clientes diretamente no processo de produção dos serviços, consolidando o auto-atendimento. Transações de pagamentos, transferências, emissão de extratos, saldos , empréstimos e aplicações financeiras, anteriormente somente efetuadas nas agências, agora são efetuadas na *internet*, no melhor momento que convier ao cliente.

O *Internet Banking* consolida-se como uma opção para fidelizar o cliente a determinado banco, reduzir custos, reduzir a escala de serviços e aumentar a velocidade de atendimento. Porém muitos clientes ainda são resistentes ao seu uso, quer pela necessária quebra de paradigmas, principalmente em relação às mudanças associadas ao uso de novas tecnologias, quer pela falta de hábito na sua utilização. Estão envolvidos também outros fatores como confiabilidade, segurança, privacidade, acessibilidade, preferência pelo atendimento pessoal e falta de conhecimento do sistema *Internet Banking.*

Na relação clientes e *Internet Banking* existem ainda muitos aspectos a serem estudados, principalmente no que se refere aos aspectos que definem a aceitação ou rejeição deste canal eletrônico. Buscando as causas que levam o cliente a não utilizar este tipo de serviço ou a restringir seu uso, percebe-se que muitos fatores estão envolvidos e que, o maior ou menor grau de influência de cada um depende muito do aspecto cultural. Assim, a questão de pesquisa centra-se na seguinte pergunta: Quais os principais fatores geradores de resistência ao uso *do Internet Banking* oferecido pelo Banco do Brasil na Agência de Itapema (SC)?

A importância desta questão reside no fato de que a adoção e fortalecimento de políticas corretas, voltadas para as necessidades dos usuários e a identificação de possíveis falhas deve ser uma constante para se evitar a perda de mercado. Além disso, o grande número de transações realizadas em uma agência bancária tem como conseqüência custos operacionais elevados que podem ser reduzidos com a utilização do sistema de *Internet Banking*. Pode-se considerar que uma transação realizada via internet custa cerca de dez por cento daquela realizada diretamente no caixa.

Outro aspecto que torna relevante a questão de pesquisa é o número reduzido de publicações científicas sobre o assunto e, dentre as encontradas, a especificidade, fundamentada no aspecto cultural, dificulta a generalização dos dados.

Como forma de contribuição nesta área de conhecimento, este estudo busca identificar os principais fatores geradores de resistência ao uso do *Internet Banking* na agência do Banco do Brasil S.A. de Itapema (SC), bem como a faixa etária e a escolaridade dos usuários, a freqüência de acesso ao *Internet Banking*, o grau de conhecimento do cliente acerca do sistema, os tipos de transação mais utilizados e o grau de satisfação dos mesmos com o sistema *Internet Banking*.

Visando atingir tais objetivos, escolheu-se a pesquisa quantitativa, realizada através do método de estudo de caso. Formulou-se um questionário estruturado a ser aplicado em uma amostra da população-alvo (clientes usuários da *Internet Banking*) cujos resultados deverão ser sistematizados e analisados para que se chegue a conclusões plausíveis e recomendações realistas com relação aos objetivos propostos.

Para tanto, estruturou-se o presente trabalho em quatro capítulos. No primeiro, determinam-se as bases teóricas do sistema de *Internet Banking*, sua caracterização, evolução, formas de segurança e fatores restritivos ao seu uso. O segundo capítulo descreve a metodologia utilizada no desenvolvimento da pesquisa quantitativa, bem como os instrumentos e procedimentos de coleta de dados. No terceiro capítulo, apresenta-se a sistematização e a análise dos dados e, no quarto e último, as conclusões obtidas e as recomendações de utilização das informações, bem como as recomendações para futuras pesquisas.

2 FUNDAMENTAÇÃO TEÓRICA

Este capítulo pretende fornecer a base teórica necessária ao bom entendimento do tema proposto, incluindo os aspectos gerais da economia digital, da *Internet* no Brasil, da tecnologia da informação e da tecnologia dos bancos brasileiros. Apresenta-se também alguns conceitos básicos e a caracterização, evolução, formas de segurança e fatores restritivos ao uso do sistema de *Internet Banking*.

2.1 CARACTERÍSTICAS DA ECONOMIA DIGITAL

A economia mundial iniciou-se verdadeiramente com as grandes navegações e continuou crescendo com a revolução industrial e depois com os blocos econômicos. Na velha economia os fluxos de informações eram físicos (dinheiro, cheques, faturas, relatórios, reuniões presenciais, plantas, mapas, fotografias, etc.) e os recursos humanos utilizados e o tempo gasto em transações eram enormes.

Com a emergência da economia da informação, a função de produção que era composta por três fatores (capital, terra e mão-de-obra) passa a contar com mais um: o conhecimento. Para Tapscott (1995 *apud* CORREIA e DIAS,1999, p.105):

> "Na economia digital a informação em todas suas formas ficou reduzida a bits armazenados em computadores e correndo na velocidade da luz por redes. É também uma economia do conhecimento, baseada na aplicação do *know-how* humano a tudo o que produzimos e como produzimos. Mais e mais valor agregado será criado pelo cérebro e não pela força. Quer as pessoas ajam como consumidoras ou produtoras, a incorporação de idéias será crucial para a criação da riqueza. Esta é uma era de interligação em rede não apenas da tecnologia, mas também de seres humanos, organizações e sociedade."

Para identificar suas principais características e salientar a sua interligação Castells (1996 *apud* CORREIA e DIAS, 1999) qualifica esta "nova economia" como informacional e global. Por um lado, é informacional porque a produtividade e competitividade dos agentes econômicos dependem fundamentalmente da sua capacidade de gerar, processar e utilizar de forma eficiente informação baseada no

conhecimento. Por outro lado, é global, porque o núcleo principal das atividades de produção, consumo e circulação, bem como os seus componentes (capital, trabalho, matérias primas, gestão, informação, tecnologia, mercados) encontram-se organizados à escala global, diretamente ou através de redes de ligação entre agentes econômicos.

Apresenta-se a seguir aquilo que Tapscott (1995 *apud* CORREIA e DIAS, 1999) considera os traços distintivos do que designa por "Nova Economia". Estes traços correspondem a doze temas que, na sua opinião, diferenciam a "Nova Economia" da "Velha Economia", são eles: o conhecimento, a digitalização, a virtualização, a molecularização, a integração/interconexão em rede, a desintermediação, a convergência, a inovação, a "produconsumo", a proximidade ou imediatismo, a globalização e as clivagens ou discordâncias.

O referido autor entende que as novas tecnologias de informação possibilitam uma economia baseada no conhecimento onde os novos valores agregados estarão diretamente ligados a ele. A informação e a tecnologia tornam-se partes dos produtos. Estas informações configuram-se em formato digital e são transferidas por redes com extrema velocidade. Com a digitalização, a informação é transformada de analógica para digital e suas características físicas tornam-se virtuais. Neste ambiente, as organizações, equipes de trabalho, agências governamentais, entro outros, não precisam de sua forma física para existir.

Desta forma, a empresa deixa de ter a sua estrutura organizacional tradicional, hierárquica e dividida em áreas funcionais, passando a ter suas funções realizadas por grupos de trabalhos, entidades externas ou comunidade de profissionais que assumem o papel de moléculas e interagem para o cumprimento do objetivo organizacional (molecularização). Ocorrem grandes mudanças nos processos gerenciais, pois os tradicionais não mais atendem as necessidades. Esse novo ambiente permite e exige a mudança do processamento centralizado para redes interligadas e integradas, tanto na economia quanto nas organizações. As novas tecnologias permitem a integração de componentes organizacionais modulares e independentes formando uma rede integrada de serviços que pode se interconectar a outras redes.

De acordo com Tapscott (1995 *apud* CORREIA e DIAS, 1999), esta integração/interconexão em rede acaba provocando a desintermediação, ou seja, a eliminação de intermediários dos vários processos de negócios. No inicio da *Internet* esta era uma das crenças bastante difundida, atribuindo à *Web* a responsabilidade desta eliminação dos intermediários, porém esta crença não se confirmou como realidade. Este processo que já ocorreu ou ainda irá ocorrer está relacionado com os elos da cadeia que não agregam valor ou simplesmente unem as duas pontas.

Nesta nova economia, setor econômico dominante está sendo criado por três setores convergentes (computação, comunicação e conteúdo) que, por sua vez, garantem a infra-estrutura para a criação de riqueza em todos os setores. É o que Don Tapscott chama de convergência. O autor ressalta também a valoração da inovação que é, atualmente, a principal vantagem competitiva entre as organizações e que leva o conhecimento e a imaginação a se constituírem na principal fonte de valor.

Na economia digital, a proximidade ou imediatismo torna-se uma direção e variável-chave na atividade econômica e no sucesso dos negócios. A nova empresa é uma empresa em tempo real, que se ajusta contínua e imediatamente para alterar as condições de negócio por meio da proximidade das informações. A tecnologia passa a viabilizar o gerenciamento de todos e quaisquer processos a qualquer instante, permitindo a interferência no próprio processo.

Outra característica relevante é o que Tapscott chama de “produconsumo”, ou seja, a pouca diferenciação entre consumidores e produtores, já que os produtores, em algum momento, são consumidores de outros produtos e os consumidores passam a ser produtores de idéias, informações, etc.

Esta nova economia é uma economia globalizada. O conhecimento transcende as fronteiras e se torna o principal recurso econômico muito embora cada organização ou instituição individualmente opere em um cenário nacional, regional ou local. A rede estabelecida permite as comunicações em tempo real , a retenção e encaminhamento das comunicações quando as pessoas não se estão em contato e também o acesso aos recursos de informação coletiva a partir de

qualquer lugar. Estas possibilidades são hoje essenciais ao bom desenvolvimento dos processos econômicos e empresariais.

Como último tema exposto por Tapscott (1995 *apud* CORREIA e DIAS, 1999), tem-se as clivagens ou discordâncias, que referem-se basicamente às questões sociais que surgem com o desenvolvimento e crescimento da economia digital, principalmente no que diz respeito à natureza do trabalho e às exigências sobre a força de trabalho.

2.2 TECNOLOGIA DA INFORMAÇÃO (TI)

Desde a passagem da Economia Industrial para a chamada Era Digital, um considerável número de organizações tem buscado se modificar. Tal reestruturação tem sido, em grande parte, impulsionada pelos constantes avanços em Tecnologia de Informação (TI) (TAPSCOTT e CASTON, 1995). A partir da década de 90, inúmeras novidades surgiram, principalmente nas áreas de automação, informática e comunicação, influenciando de forma bastante intensa a sociedade moderna.

A sigla TI, tecnologia da informação, abrange todas as atividades desenvolvidas na sociedade pelos recursos da informática. É a difusão social da informação em larga escala de transmissão, a partir destes sistemas tecnológicos inteligentes. Segundo a WIKIPEDIA (2007), TI é o conjunto de recursos não humanos dedicados ao armazenamento, processamento e comunicação da informação, e à maneira como esses recursos estão organizados em um sistema capaz de executar um conjunto de tarefas. Castells (1996 *apud* CORREIA e DIAS, 1999, p. 98) entende como tecnologias de informação:

> "[...] o grupo convergente de tecnologias formado pela microelectrônica, informática (hardware e software), telecomunicações e optoelectrônica; diz-se convergente porque os efeitos sinergéticos entre as várias tecnologias-chave foram fundamentais para o surgimento do novo sistema tecnológico na década de setenta."

Conforme mencionado por Bettis e Hitt (1991 *apud* ALBERTIN, 1995), a Tecnologia da Informação apresentou mudanças substanciais nos últimos anos.

Computadores, softwares e telecomunicações evoluiram de forma muito rápida e complexa. Essas mudanças, juntamente com o declínio dos custos e aumento do acesso a esses recursos, intensificaram o uso da Tecnologia da Informação e levaram ao surgimento de novas estratégias competitivas.

Atualmente, o setor bancário é considerado como um dos que mais investem em tecnologia de informação, tendo seus produtos e serviços fundamentalmente apoiados nesta tecnologia (ALBERTIN, 1999). Para Lau (2006), cada banco por meio de recursos tecnológicos busca aumentar o conjunto de serviços oferecidos aos clientes com o objetivo claro de atrair o maior número a este ambiente, eliminando em muitos momentos sua presença na agência bancária, reduzindo em números expressivos o custo destes clientes.

A atividade bancária também sofreu o impacto da globalização dos mercados, obrigando os bancos a saírem das fronteiras do Brasil e interagirem no mercado financeiro global, onde a Tecnologia da Informação desempenha um papel preponderante. Estruturas ágeis, informação em tempo real e satisfação dos clientes, são premissas cada vez mais consideradas. Ainda, conforme o mesmo autor, os obstáculos ao progresso neste campo concentram-se na adaptação, tecnologia, segurança e confiabilidade.

2.3 TECNOLOGIA NOS BANCOS BRASILEIROS

Os bancos brasileiros investem muitos recursos em tecnologia, seja para ampliar a área geográfica de atendimento, para diminuir os seus custos ou ainda para proporcionar conveniência a seus clientes, entre outras razões.

Para Costa Filho (1996 *apud* PIRES E COSTA FILHO,2001) uma das utilizações mais antigas, no Brasil, do processamento de dados se deu com a adoção de sistemas automáticos de controle, em 1956, pelo Bradesco, através de máquinas IBM eletromecânicas que utilizavam sistemas de cartões perfurados. Accorsi (1990) relata que o processamento de dados ocorreu efetivamente a partir

de 1964 com a obsolescência das máquinas de contabilidade que não permitiam o rápido atendimento e com a necessidade de redução dos custos nas agências.

Bulhões (1993 *apud* OLIVEIRA 2000) divide a evolução do processo de adoção da automação tecnológica por parte dos bancos no Brasil em três fases. A primeira fase, denominada por ela de automação de controle ou administrativa, ocorreu na segunda metade da década de 1960 e no início da década de 1970. Era baseada em um sistema centralizado e visava o desenvolvimento do processamento eletrônico de retaguarda e o atendimento da necessidade de padronização e agilização das transações bancárias. Os grandes volumes de lançamentos nas contas de depósito exigiram a criação dos centros de processamento de dados (CPD). Os dados referentes ao movimento do dia de cada agência eram enviados e processados nos CPDs durante a noite e remetidos às agências, no dia seguinte, sob a forma de listagens, que eram, então, modificadas a cada lançamento durante o expediente. O sistema, porém, se mostrou ineficiente nos primeiros anos da década de 70, em função de um aumento ainda mais significativo no volume das transações bancárias e da expansão geográfica da rede de agências.

Segundo Costa Filho (1996), o governo interveio de modos distintos na automação bancária. Em 1970, o Banco Central incentivou os investimentos em processamento de dados e, pouco tempo depois, o governo decretou a criação da reserva de mercado na área de informática promovendo o desenvolvimento de sistemas mais adequados às necessidades bancárias.

A estrutura existente implicava custos operacionais bastante elevados o que forçou a adoção de novas tecnologias. Segundo Oliveira (2000), no início da década de 80, desenvolveu-se o processamento de dados *on-line* e também os primeiros testes voltados para o atendimento ao público, aproveitando as vantagens geradas pelo uso de máquinas automáticas.

Na segunda fase da automação bancária, denominada por Bulhões (1993 *apud* OLIVEIRA, 2000) de automação de gerenciamento, houve necessidade de administrar o grande volume de serviços e operações que crescia juntamente com a expansão das agências bancárias.

> "A automação possibilitou o acesso a informações diárias, semanais e mensais sobre todos os serviços e operações realizados nas agências e nos níveis global e regional. Como resultado da maior agilidade obtida, houve uma sensível melhora na qualidade dos serviços e aumento na rentabilidade" (BULHÕES, 1993 *apud* OLIVEIRA, 2000, p. 30).

Essa fase terminou com a implantação dos Planos Cruzado e Collor que levaram os bancos a reduzirem custos. Além disso, segundo Costa Filho (1996), a Lei de Informática (1984) estimulou a iniciativa privada nacional através de incentivos tributários e financeiros e controle da importação de bens e serviços de informática promovendo o processo de adoção de tecnologia por parte dos bancos.

Para Bulhões (1993 *apud* OLIVEIRA 2000), a terceira fase, chamada de fase de automação de atendimento, visava reduzir o custo elevado do atendimento personalizado da época, afastar dos clientes das agências, enxugar o fluxo de papéis, dar agilidade ao processo de obtenção de informações para tomada de decisões e propiciar maior controle por parte dos bancos. Esta fase foi dividida em quatro etapas: a colocação do computador junto aos funcionários; a colocação de caixas automáticos e do auto-atendimento permitindo saques, depósitos, pagamentos, consultas de saldos, etc.; a colocação de caixas 24 horas, fora das agências; e, a evolução dos caixas automáticos para agências automáticas (nas ante-salas dos bancos) juntamente com os serviços de atendimento ao cliente por telefone. Segundo Oliveira (2000), existe uma quinta etapa que seriam os canais que possibilitaram o atendimento à distância como o *Home Banking* e o *Internet Banking*.

De acordo com Costa Filho (1996), o fim da Lei de Informática (1992) possibilitou aos bancos buscarem soluções tecnológicas mais adequadas às suas necessidades, no Brasil ou no exterior. A partir de então, vários produtos e serviços foram lançados e o número de transações realizadas através de caixas automáticos começou a superar as transações nas agências.

Para Diniz (2000) o contexto estrutural e conjuntural empurrou os bancos no sentido da adoção de sistemas eletrônicos de atendimento. Tal esforço, possibilitou aos bancos brasileiros o oferecimento, hoje, de uma vastíssima gama de canais de

atendimento eletrônico, que vai além da bem distribuída malha tradicional, alcançando quase toda a sua clientela.

Tais canais de acesso são o *home* e *office banking*, o *Internet Banking*, o *smart card*, o banco por telefone e as centrais de atendimento, que os bancos vêm tornando disponíveis, de forma eletrônica, para distribuir quase todos os seus produtos e serviços, os quais eram anteriormente oferecidos de modo exclusivo através de atendimento pessoal ou no ambiente de agência.

2.4 *INTERNET BANKING*

Os bancos têm investido muitos recursos em tecnologia, seja para ampliar a área geográfica de atendimento, para diminuir os seus custos ou ainda para proporcionar conveniência a seus clientes (DINIZ, 2000).

Como colocam Pires e Marchetti (1997 *apud* OLIVEIRA, 2000), são novos canais de acesso, tais como o *home* e *office banking*, a Internet, o *smart card*, o banco por telefone e as centrais de atendimento, que os bancos vêm tornando disponíveis, de forma eletrônica, para distribuir quase todos os seus produtos e serviços, os quais eram anteriormente oferecidos de modo exclusivo através de atendimento pessoal ou no ambiente de agência.

Dos canais eletrônicos passíveis de serem acessados por clientes de bancos destaca-se a *Internet Banking* que funciona a partir de um computador pessoal com um adaptador de comunicação de dados (*modem*) conectado ao computador do banco (ZINGLER, 1993). Diferentemente do *Home Banking*, não há necessidade de utilização de softwares específicos para o acesso aos dados.

De acordo com Lau (2006), é uma opção adicional aos clientes de bancos que buscam realizar transações bancárias em qualquer localidade, onde se dispõe de um computador e conectividade com a *internet*.

O banco californiano *Wells Fargo* foi um dos primeiros a oferecer o serviço de *Internet Banking* em 1995, com estrondoso sucesso. No Brasil, o caminho aberto

pelo Bradesco, primeira instituição a usar a *Internet* para serviços bancários, logo foi trilhado pelos demais bancos Os investimentos do Banco do Brasil, Caixa Econômica Federal, Itaú e Bradesco somaram, em 1998, perto de um bilhão e trezentos milhões de dólares (MÜLLER, 2001).

Ao longo dos últimos anos, a utilização do *Internet Banking* teve um crescimento espantoso. Segundo a FEBRABAN (2003 *apud* ABDALA, 2004), o número de usuários de *Internet Banking*, cresceu de 8,3 milhões em 2000 para 13 milhões em 2001, um aumento equivalente a 56,63%. Em 2004, passou-se de 18,1 milhões de usuários para 26,3 milhões. Estas cifras geraram grandes expectativas nas instituições bancárias que continuaram investindo alto em TI. Porém, a partir de 2004, este crescimento teve seus números reduzidos.

De acordo com dados da FEBRABAN (2007), as transações em *Internet Banking* (transferências, pagamentos, investimentos, financiamentos, empréstimos, agendamentos de transações, etc.) cresceram moderadamente nos últimos três anos. As transações bancárias realizadas por pessoas jurídicas tiveram um crescimento de 7,6% entre 2005 e 2006 e as realizadas por pessoas físicas cresceram 3,5% no mesmo período.

Para Carlos Eduardo Fonseca, diretor de Tecnologia da FEBRABAN, chegou-se ao limite de uso entre os internautas existentes e há uma necessidade premente de fomento à inclusão digital para que se possa ampliar a base de usuários. O diretor descarta a hipótese de o *Internet Banking* não estar sendo utilizado por questões ligadas à segurança, ele admite que há um paradigma cultural com a aplicação, porém a utilização do *Internet Banking* pelos clientes continua movimentando um grande volume de dinheiro, apesar do reduzido crescimento apresentado (LOBO, 2007).

2.5 SEGURANÇA NO USO DO *INTERNET BANKING*

As oportunidades de negócio que surgiram com o advento da *Internet* foram inúmeras. Desde simples propaganda, que anteriormente circulava por outros meios

e passou a ser veiculada pela rede, até mesmo anúncios de compra e venda. Talvez tenham sido esses anúncios as primeiras iniciativas de se implementar o comércio via *Internet*. As transações comerciais continuavam sendo feitas pessoalmente, mas as pessoas se encontravam através dos anúncios publicados.

Segundo Ferro (2003), a evolução dessa ferramenta foi muito rápida e logo surgiram os *sites* de compra e venda, de leilões e até mesmo os bancos virtuais que, a princípio, suscitaram dúvidas na comunidade virtual. Atualmente, no entanto, é possível realizar qualquer operação financeira que não requeira a presença na agência como transferências, pagamentos, contratação de serviços e operações financeiras (câmbio, importação e exportação, etc.).

Os bancos enxergam a *Internet* como uma ferramenta muito promissora para o futuro de seus negócios. Uma grande vantagem da *Internet* para os bancos é o barateamento do custo das transações, que são em grande parte realizadas apenas pelos sistemas sob comando direto dos clientes/usuários, sem nenhuma intervenção de qualquer funcionário. No entanto, muitos clientes ainda preferem ir até a agência bancária quando o assunto envolve suas finanças, principalmente por questões relacionadas à segurança das transações.

Esta insegurança tem uma fundamentação. Segundo Weber (1999), a *Internet* foi projetada visando fornecer conectividade entre computadores para uma comunidade restrita de usuários que confiavam mutuamente entre si. Ela não foi projetada para um ambiente comercial, para tráfego de informações valiosas ou sensíveis, ou para resistir a ataques mal-intencionados. Durante a década de 80, antes da popularização da *Internet*, os computadores foram alvos de ataques individuais e isolados. A solução adotada foi relativamente simples: incentivar os usuários a escolherem boas senhas, prevenir o compartilhamento indiscriminado de contas e arquivos e eliminar os *bugs* de segurança de programas como *sendmail, finger* e *login* à medida que eles iam sendo descobertos.

Na década de 90, entretanto, os ataques se tornaram mais sofisticados e organizados. Estes ataques são diretamente relacionados ao protocolo IP que não foi projetado para o ambiente atual da *Internet*, já que não possui muita resistência contra ataques intencionais, e nem para fornecer segurança. Apesar disso, o IP está

em permanente evolução e futuras versões provavelmente fornecerão a segurança e a confiabilidade requeridas.

No ambiente *on-line*, contudo, a falta de segurança atinge também as informações colecionadas pelas empresas a respeito dos seus clientes, uma vez que elas geralmente ficam armazenadas em bancos de dados que precisam ser acessados durante uma transação *on-line*.

Guizzo (2001 *apud* ABDALA, 2004) ressalta que, percebendo vulnerabilidades[1] nos sistemas, os *hackers* realizam invasões nos servidores das empresas, podendo se apropriar de informações sigilosas. A partir daí, conseguem ganhar acesso privilegiado ao sistema e às informações nele armazenadas. As vulnerabilidades são progressivas e, a cada dia, são encontradas novas falhas que podem comprometer a segurança de um sistema previamente implantado. Por este motivo é importante realizar uma manutenção constante do ambiente, através de política de segurança, estabelecimento de um plano de contingências, treinamento para os funcionários e, principalmente, monitoração da infra-estrutura.

As políticas de segurança estabelecem as bases para um bom programa de segurança. Essas políticas, freqüentemente chamadas de controles básicos, funcionam juntas no estabelecimento de um determinado nível de segurança na empresa como um todo, abordando aspectos físicos e lógicos (ARANTES, 2000). Para Estrada (2005), a política de segurança física consiste na implementação das instalações físicas dos sistemas e equipamentos de informática empregados para a *Internet Banking*, como a escolha de um local adequado, afastado de áreas públicas, com sistemas de prevenção e combate à falta de energia elétrica, incêndio, processamentos alternativos e cópias dos processamentos. Já a política de segurança lógica, compreende a proteção dos bancos de dados contra vírus, o cuidado no armazenamento e na manutenção dos arquivos, o gerenciamento de risco, etc.

---

[1] Vulnerabilidade é definida como uma falha no projeto, implementação ou configuração de um *software* ou sistema operacional que, quando explorada por um atacante, resulta na violação da segurança de um computador.

Além disso, para se evitar que intrusos acessem as bases de dados relativas às transações bancárias pode-se utilizar de meios como o emprego da certificação digital[2] e criptografia[3] e a utilização de senhas ou de biometria, que é o método de identificação por aspectos físicos, como a íris, impressão digital ou voz.

A Medida Provisória 2200-2 de 24 de agosto de 2001 estabelece o uso de sistema de segurança baseado em criptografia assimétrica, instituído pela Infra-estrutura de Chaves Públicas do Brasil (ICP-Brasil), que é uma organização composta por uma autoridade gestora de políticas (Comitê Gestor, vinculado à Casa Civil da Presidência da República) e por uma cadeia de Autoridades Certificadoras (AC) que são as responsáveis pela emissão dos certificados eletrônicos, tomando providências para estabelecer a identidade das pessoas ou organizações solicitantes do certificado (ESTRADA, 2005).

Segundo Howard (1997 *apud* ABDLA, 2004), baseados no sistema de criptografia, existem alguns protocolos[4] que garantem a troca de informação em redes abertas. Os Bancos comerciais em sua totalidade, conjugaram esforços a fim de desenvolver este protocolo, que garante proteção para as transações com cartões de crédito, contas operadas por senhas eletrônicas e através de redes abertas. No caso da *Internet Banking* o cliente acessa o *site* do banco onde possui a conta e a partir daí tem acesso à sua conta para fazer as transações bancárias para as quais estiver autorizado pelo banco. As informações sobre a conta ficam armazenadas no disco rígido ou em um cartão especial. Em seguida, o *software* cria uma chave pública e outra privada para criptografar a informação, que é transmitida através da rede para o banco. O *software* do banco realiza as transferências bancárias, assina o pagamento e envia ao cliente, que então decriptografa a informação, emitindo um recibo para o cliente.

---

[2] O certificado digital ou eletrônico é um arquivo de computador que identifica o seu usuário para outra pessoa ou para outro computador, com a finalidade de garantir a autenticidade, privacidade e inviolabilidade da comunicação. Este sistema executa a criptografia e é o suporte tecnológico da assinatura digital.

[3] É o processo de codificar informações, de modo que apenas o destinatário pretendido da informação possa decodificá-las.

[4] Um protocolo é um conjunto de regras bem definidas que descrevem o funcionamento de um determinado sistema.

De acordo com Abdala (2004), no Brasil as empresas estão procurando meios de fazer com que seus *sites* estimulem a geração de uma sensação de segurança nos consumidores. Várias empresas da *Web*, até mesmo rivais, uniram-se para desenvolver uma carta de intenções para estimular o crescimento das transações *on-line*. O objetivo é mostrar ao consumidor virtual que a *Web* é um meio moderno, conveniente e seguro e que também se pode fazer valer os direitos do consumidor no mundo virtual.

Levando-se em conta todas estas questões relativas à segurança nas transações, estão sendo desenvolvidas ferramentas para a identificação dos internautas e de suas ações na rede. A assinatura digital[5] e os certificados digitais são algumas ferramentas que buscam garantir que uma determinada operação esteja realmente sendo realizada por quem o afirma.

Os bancos mantêm fortes sistemas de segurança em seus computadores e nos programas de acesso via *internet*, mas não têm como garantir a segurança do computador de clientes, de provedores ou de terceiros, eventualmente usados por seus clientes. Assim, uma outra forma de prevenção de danos aos usuários de *Internet Banking*, segundo Diniz (2000), é a política de divulgação de dicas. Algumas destas dicas serão apresentadas mais adiante.

2.6 AMEAÇAS NO *INTERNET BANKING*

A *Internet* apresenta uma grande variedade de ameaças, cada vez mais sofisticadas, com objetivos diversificados. De acordo com Lau (2006), os fraudadores roubam as identidades das vítimas que acessam os serviços bancários na *Internet* e passam a efetuar a subtração de fundos, que são direcionados para o pagamento de contas de concessionárias públicas, boletos bancários e

[5] A assinatura digital consiste na criação de um código, através da utilização de uma chave privada, de modo que a pessoa ou entidade que receber uma mensagem contendo este código possa verificar se o remetente é mesmo quem diz ser e identificar qualquer mensagem que possa ter sido modificada.

transferências para outras contas bancárias que possibilitem o saque dos valores nos terminais de auto-atendimento.

Conforme a Cartilha de Segurança para a *Internet*, os motivos de invasão dos computadores podem ter como objetivos: utilizar o computador em alguma atividade ilícita, para esconder a real identidade e localização do invasor; utilizar o computador para lançar ataques contra outros computadores; utilizar o disco rígido como repositório de dados; destruir informações (vandalismo); disseminar mensagens alarmantes e falsas; ler e enviar e-mails em nome do usuário do computador invadido; propagar vírus de computador; furtar números de cartões de crédito e senhas bancárias; furtar a senha da conta do provedor, para acessar a Internet fazendo se passar pelo usuário do computador invadido; e furtar dados do computador, como por exemplo, informações do Imposto de Renda.

As perdas causadas pelas fraudes podem atingir grandes cifras e podem colocar em risco os dados que estão em trânsito, bem como os que estão na rede local da organização que presta serviços pela *Internet*.

2.6.1 Fraudes no ambiente *Internet Banking*

Na década de 1990 a utilização de canais eletrônicos se restringia a um grupo de pessoas, com alto nível educacional e de renda. A disseminação do seu uso dependia do desenvolvimento de um processo de aprendizagem com equipamentos automatizados em geral, o que parecia poder ocorrer a médio e longo prazos. Para Dayal (1999 *apud* OLIVEIRA, 2000), esses canais não vêm sendo mais amplamente utilizados por conta do medo de fraudes.

A fraude na *internet* consiste na distorção intencional da verdade de um fato visando à obtenção de lucro ilícito utilizando os serviços disponíveis na *Web* tais como salas de bate-papo, mensagens eletrônicas e sites disponíveis na *Internet* (LAU, 2006). Existem três maneiras de se realizar uma fraude na *Internet*. Atacando o servidor, interceptando dados durante a transmissão e usando técnicas e táticas para roubar informações do usuário.

Com o desenvolvimento do ambiente da *Internet* surgiram pessoas especializadas no ataque às informações em trânsito e naquelas armazenadas por usuários e organizações. Dentre estas encontram-se os *hackers* e os *crackers* que se utilizam de vários métodos e tipos de ataques empregando várias pragas virtuais ou códigos maliciosos como os vírus, cavalos de tróia, *adwares* e *spywares*, entre outros.

Esta seção tem como objetivo conceituar os elementos destes ataques e proporcionar uma visão geral sobre as ameaças ao ambiente da *Internet Banking*.

2.6.1.1 Fraudadores ou atacantes

Existem hoje dois tipos de fraudadores do sistema de *Internet Banking*: os *hackers* e os *crackers*.

Para Thompson (2002), *hacker* é aquele que descobre falhas em sistemas e se aproveita dessas falhas em benefício próprio ou de uma causa. Segundo a WIKIPÉDIA (2007), são indivíduos que elaboram e modificam *softwares*, *hardwares* e computadores, seja desenvolvendo funcionalidades novas, seja adaptando as antigas. Podem agir tanto de forma positiva quanto negativa ou, muitas vezes, simplesmente por brincadeira.

Conforme definição da Wikipédia (2007), *cracker* é o termo usado para designar quem pratica a quebra (ou *cracking*) de um sistema de segurança, de forma ilegal ou sem ética. Este termo foi criado em 1985 por *hackers* em defesa contra o uso jornalístico do termo "*hacker*". O uso deste termo reflete a forte revolta destes contra o roubo e vandalismo praticado pelo *cracking*.

2.6.1.2 Métodos de Ataque

Os métodos de ataque mais comuns atualmente são a engenharia social e a utilização de *spans*.

Segundo o CERT (2006 *apud* BONFIETTI, 2007), o termo “engenharia social” é utilizado para descrever um método de ataque, onde alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações.

O atacante se faz passar por outra pessoa e utiliza meios, como uma ligação telefônica ou e-mail, para persuadir o usuário a fornecer informações ou realizar determinadas ações.

Já o termo *spam*, de acordo com Bonfietti (2007) é usado para se referir aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas. Na sua forma mais popular, um *spam* consiste numa mensagem de e-mail com fins publicitários. Quando o conteúdo é exclusivamente comercial, este tipo de mensagem também é referenciada como UCE (do inglês *Unsolicited Commercial E-mail*).

Geralmente os *spams* têm caráter apelativo e na grande maioria das vezes são incômodos e inconvenientes e se tornaram uma das principais perturbações para os internautas, administradores de redes e provedores, de tal forma que o abuso desta prática já se tornou um problema de segurança de sistemas.

2.6.1.3 Tipos de ataque

Para Simon (2007), não é uma tarefa nada fácil fraudar os dados de um servidor de uma instituição bancária ou comercial já que eles são muito bem protegidos. Para driblar esse problema, os fraudadores têm concentrado seus esforços na exploração de fragilidades dos usuários para realizar fraudes bancárias através da *Internet*.

Na tentativa de fraudar os clientes dos bancos que utilizam a *Internet Banking*, os fraudadores se basearam principalmente em três tipos de ataques conhecidos como *Scam*, *Phishing* (ou *Phishing Scam*) e *Pharming*.

Scam é uma mensagem enviada em massa, como o *spam*, que contém um arquivo anexado ou um *link* de condução para *download* de arquivo que instala um cavalo de tróia no computador do usuário. Esta mensagem pode ser passada através de diversos canais de informação disponíveis como *e-mail*, *chats*, IRC, ICQ, MSN Messenger, Orkut entre outros. As mensagens que escondem o *scam* têm características próprias de instituições financeiras, *sites* de cartões de mensagem, notificações de órgãos públicos, notícias de destaque, *downloads* de programas, promoções e eventos, temas pornográficos e mensagens pessoais, sempre com o intuito de deixar as vítimas curiosas ou instigadas (SIMON, 2007). Segundo Lau (2006), hoje o *scam* é a modalidade de ataque mais utilizada em relação ao *Internet Banking* por sua versatilidade, praticidade e grande possibilidade de disseminação.

O *phishing*, também conhecido como *phishing scam* , segundo Bonfietti (2007) pode ser considerado um tipo particular de *scam*. O termo foi originalmente criado para descrever o tipo de fraude que se dá através do envio de mensagem não solicitada que se passa por comunicação de uma instituição conhecida, como um banco, empresa ou site, e que procura induzir o acesso a páginas fraudulentas (falsificadas), projetadas para furtar dados pessoais e financeiros de usuários.

A palavra *phishing* (de "*fishing*") vem de uma analogia criada pelos fraudadores, onde "iscas" (*e-mails*) são usadas para "pescar" senhas e dados financeiros de usuários da *Internet*. Atualmente, este termo vem sendo utilizado também para se referir às mensagens que procuram induzir o usuário a instalar códigos maliciosos, projetados para furtar dados pessoais e financeiros, ou a mensagens que, no próprio conteúdo, apresentam formulários para o preenchimento e envio de dados pessoais e financeiros de usuários. De acordo com Simon (2007, p. 3):

> "Este ataque não compensa muito ao fraudador em razão do trabalho que lhe será exigido para falsificar o sítio. Ele termina dispendendo muito tempo para criar as páginas. O custo é alto frente ao benefício. Por isso, essa modalidade nunca teve grandes números e apresentou queda significativa em virtude da evolução tecnológica dos *trojans* direcionados ao *scam"*.

Pharming é o termo usado para definir ataques baseados em uma técnica que modifica o *Domain Name System servers* (Servidores de Nome de Domínio), denominados DNS conhecida também como "envenenamento de cache DNS". Consiste basicamente em corromper o sistema de nomes (DNS) de uma rede de computadores, de tal forma que o endereço de um site passe a apontar para um servidor diferente do original. Segundo Bonfietti (2007, p. 23):

> "O sistema DNS é composto por servidores de nomes que nada mais são do que computadores equipados com um software que traduz os nomes dos sites, inteligíveis para os seres humanos, em números, inteligíveis para as máquinas. Este número é chamado de IP (*Internet Protocol*) e cada computador conectado à Internet possui um IP diferente. É como o número de identidade de uma máquina numa rede. Se este servidor estiver vulnerável a esse tipo de ataque, o usuário poderá ser redirecionado a uma página falsa hospedada, Se a página falsa tiver sido especialmente preparada e copiada fielmente da página do banco, o cliente da instituição poderá inserir seus dados privados sem se dar conta de ter sido levado a um site fraudulento".

De acordo com Lau (2006), hoje este tipo de ataque não preocupa tanto como o *scam*. Depois de grandes prejuízos no setor financeiro em 2002 e 2003, as instituições financeiras, junto dos servidores, investiram em melhor controle dos ataques. Desde 2004 percebeu-se a ausência do *pharming* no cenário brasileiro. Acredita-se que as ações junto dos DNS praticamente extinguiram esta ameaça.

2.6.1.4 Códigos maliciosos (*malware*)

Código malicioso ou *malware* (*malicious software*) é um termo genérico que abrange todos os tipos de programa especificamente desenvolvidos para executar ações maliciosas em um computador. Na literatura de segurança o termo *malware* também é conhecido por "software malicioso".

Existe uma grande diversidade de códigos maliciosos como vírus, cavalos de tróia, *adware*, *spyware*, entre outros, cujas definições se encontram a seguir.

a) Vírus: Vírus é um programa ou parte de um programa de computador, normalmente malicioso, que se propaga infectando, isto é, inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos de um computador. O vírus depende da execução do programa ou arquivo hospedeiro para que possa se tornar ativo e dar continuidade ao processo de infecção (CERT, 2006).

b) Cavalo de tróia: De acordo com o CERT (2006), o cavalo de tróia, ou *trojan horse* é um programa, normalmente recebido como um "presente" (por exemplo, cartão virtual, álbum de fotos, protetor de tela, jogo, etc), que além de executar funções para as quais foi aparentemente projetado, também executa outras funções normalmente maliciosas e sem o conhecimento do usuário, tais como instalar *keyloggers, screenloggers* e *backdoors* ou ainda alterar, corromper ou destruir arquivos.

c) *Adware* e *Spyware:* *Adware (Advertising software)* é um tipo de *software* especificamente projetado para apresentar propagandas através de um programa instalado em um computador. Em muitos casos, os *adwares* têm sido incorporados a *softwares* e serviços, constituindo uma forma legítima de patrocínio ou retorno financeiro para aqueles que desenvolvem *softwares* livres ou prestam serviços gratuitos. *Spyware*, por sua vez, é o termo utilizado para se referir a uma grande categoria de *softwares* que têm o objetivo de monitorar atividades de um sistema e enviar as informações coletadas para terceiros. Os *spywares*, assim como os *adwares*, podem ser utilizados de forma legítima, mas, na maioria das vezes, são utilizados de forma dissimulada, não autorizada e maliciosa (CERT, 2006).

d) *Backdoors:* São programas que abrem "portas" de acesso ao atacante, permitindo acesso remoto ao computador. Os *backdoors* são usados para que os atacantes garantam uma forma de retornar a um computador comprometido, sem precisar recorrer aos métodos utilizados na realização da invasão. Na maioria dos casos, também é intenção do atacante poder retornar ao computador comprometido sem ser notado (CERT, 2006).

e) *Keyloggers e Screenloggers*: De acordo com o CERT (2006), *keylogger* é um programa capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado de um computador. Segundo Bonfietti (2007), após sua ampla utilização para

captura de senhas no *Internet Banking*, a grande maioria dos bancos mudou o modo da autenticação para seu acesso. Antes os dados da agência, conta e senha eram digitados via teclado, agora os dados são fornecidos via mouse clicando sobre os caracteres do teclado virtual.

f) *Worms*: É um programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para computador. Diferente do vírus, o *worm* não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser explicitamente executado para se propagar. Sua propagação se dá através da exploração de vulnerabilidades existentes ou falhas na configuração de softwares instalados em computadores (CERT, 2006). *Worms* são notadamente responsáveis por consumir muitos recursos. Degradam sensivelmente o desempenho de redes e podem lotar o disco rígido de computadores, devido à grande quantidade de cópias de si mesmo que costumam propagar. Além disso, podem gerar grandes transtornos para aqueles que estão recebendo tais cópias (BONFIETTI, 2007).

g) *Bots e botnets*: Segundo o CERT (2006) o *bot* é um programa capaz se propagar automaticamente, explorando vulnerabilidades existentes ou falhas na configuração de softwares instalados em um computador. Adicionalmente, dispõe de mecanismos de comunicação com o invasor, permitindo que o *bot* seja controlado remotamente. Portanto o invasor, ao se comunicar com um *bot*, pode enviar instruções para que ele realize diversas atividades, tais como: desferir ataques na *Internet*, enviar *spam*, e-mails de *phishing*, ataque de negação de serviço[6] e furtar dados de onde foi executado. As *botnets* são redes formadas por computadores infectados com *bots* e são usadas pelos invasores para aumentar a potência de seus ataques.

h) *Rootkits*: Um invasor, ao realizar uma invasão, pode utilizar mecanismos para esconder e assegurar a sua presença no computador comprometido. O conjunto de programas que fornece estes mecanismos é conhecido como *rootkit*. Segundo CERT (2006), *rootkit* não indica que as ferramentas que o compõem são usadas

[6] Negação de serviço ou *Denial of Service* é uma atividade maliciosa que busca derrubar o serviço de um servidor através do excesso de requisições ao servidor alvo.

para obter acesso privilegiado (*root* ou *administrator*) em um computador, mas sim para manter o acesso privilegiado em um computador previamente comprometido.

2.6.2 Medidas de Prevenção

De acordo com Simon (2007), a primeira utilização do sistema *Internet Banking* no Brasil aconteceu há mais de dez anos, com o Banco Bradesco. Desde então, as demais instituições financeiras, frente aos custos reduzidos que o sistema apresenta, resolveram intensificar sua utilização e também motivar os clientes a compartilhar desta comodidade.

O crescimento da utilização do *Internet Banking* acompanhou as tendências de inclusão na rede. Segundo Zanon (2006), cerca de metade dos clientes de bancos se vale desse sistema, movimentando valores vultuosos. Isso demonstra apenas uma parcela do poder desta modalidade e também o risco que correntistas e instituições correm se não superarem a inteligência dos ataques. Torna-se então necessário investir em segurança e capacitação do cliente, fato que não ocorreu em momento apropriado, gerando o desenfreado surgimento de fraudes. Isso não foi exclusividade brasileira, pois ataques com essa característica ocorreram em todo o mundo.

O crime praticado por intermédio do uso da internet não foge à regra da prevenção. Por essa razão, encontrar mecanismos que sejam suficientes para prevenir, controlar e reprimir essa nova produção criminosa se mostra necessário. Saliente-se, contudo, que não se pode depender de medidas jurídicas, mas de medidas que envolvam os clientes e os sistemas bancários. Assim, discorre-se a seguir sobre as formas de prevenção disponíveis, ressaltando-se que a cada dia se aprimoram os ataques e, conseqüentemente, surgem novos tipos de cuidados.

2.6.2.1 Medidas aplicáveis aos usuários

Normalmente as transações, sejam comerciais ou bancárias, envolvem informações sensíveis, como senhas ou números de cartões de crédito.

Portanto, é muito importante, ao realizar transações via *Web*, certificar-se da procedência dos sites e se estes são realmente das instituições que dizem ser. Também é fundamental que eles forneçam mecanismos de segurança para evitar que alguém conectado à *Internet* possa obter informações sensíveis das transações, no momento em que estiverem sendo realizadas.

A FEBRABAN (2007) faz as seguintes recomendações para os clientes possam efetuar transações seguras e adotar medidas que possam prevenir futuras fraudes:

a) Manter programas antivírus[7] atualizados instalados no computador que utilizar para ter acesso aos serviços bancários;
b) Trocar a senha de acesso ao banco na *internet* periodicamente;
c) Só utilizar equipamentos efetivamente confiáveis. Não realizar operações em equipamentos públicos ou que não tenham programas antivírus atualizados nem em equipamento que não se conheça. Existem pragas utilizadas por fraudadores para capturar as informações do cliente quando digitadas no computador;
d) Não executar aplicações nem abrir arquivos de origem desconhecida. Eles podem conter vírus, cavalos de tróia e outras aplicações prejudiciais que ficam ocultas para o usuário e permitem a ação de fraudadores sobre a conta, a partir de informações capturadas após a digitação no teclado;
e) Usar somente provedores confiáveis. A escolha de um provedor deve levar em conta também seus mecanismos, políticas de segurança e a confiabilidade da empresa;
f) Cuidado com e-mails não solicitados ou de procedência desconhecida, especialmente se tiverem arquivos anexados. Correspondências eletrônicas também podem trazer programas desconhecidos que oferecem diversos tipos de riscos à segurança do usuário. É mais seguro apagar os e-mails não solicitados e

[7] Os antivírus são programas que procuram detectar e, então, anular ou remover os vírus de computador. Atualmente, novas funcionalidades têm sido adicionadas aos programas antivírus, de modo que alguns procuram detectar e remover cavalos de tróia e outros tipos de código malicioso; barrar programas hostis; verificar *e-mails*; verificar continuamente os discos rígidos, flexíveis e unidades removíveis; e analisar os arquivos que estão sendo obtidos pela Internet.

que não se tenha absoluta certeza que procedem de fonte confiável. Tomar cuidado especialmente com arquivos e endereços obtidos em salas de bate-papo. Alguns desses *chats* são freqüentados por fraudadores;

g) Evitar sites arriscados e só fazer *downloads* de sites que se conheça e se saiba que são confiáveis;
h) Utilizar sempre as versões de *browsers* mais atualizadas, pois geralmente incorporam melhores mecanismos de segurança;
i) Quando for efetuar pagamentos ou realizar outras operações financeiras, certificar-se que está no *site* desejado, seja do banco ou outro qualquer, clicando sobre o cadeado ou a chave de segurança que aparece quando se entra na área de segurança do *site*. O certificado de habilitação do *site*, concedido por um certificador internacional, aparecerá na tela, confirmando sua autenticidade, juntamente com informações sobre o nível de criptografia utilizada naquela área pelo responsável pelo *site*. Não insirir novos certificadores no *browser*, a menos que conheça todas as implicações decorrentes desse procedimento;
j) Acompanhar os lançamentos em conta corrente. Caso constatar qualquer crédito ou débito irregular, entre imediatamente em contato com o banco;
k) Se estiver em dúvida sobre a segurança de algum procedimento executado, entrar em contato com o banco. Prevenção é a melhor forma de segurança;
l) Em caso de dúvida, procurar pelo banco e perguntar que medidas de proteção estão sendo tomadas quanto à segurança das transações *on-line*;
m) Os meios de comunicação estão permanentemente divulgando dicas de segurança aos usuários da *Internet*.

Além destes cuidados, outros podem ser citados como: somente realizar transações em *sites* de instituições consideradas confiáveis; sempre digitar no *browser* o endereço desejado; não utilizar *links* em páginas de terceiros ou recebidos por *e-mail*; certificar-se de que o endereço apresentado no *browser* corresponde ao *site* que deseja acessar, antes de realizar qualquer ação; estar atento e prevenir-se dos ataques de engenharia social; não acessar *sites* de comércio eletrônico ou *Internet Banking* através de computadores de terceiros; desligar a *Webcam* ao acessar um *site* de comércio eletrônico ou *Internet Banking*; manter o *browser* sempre atualizado e com todas as correções (*patches*) aplicadas; alterar a configurações do *browser* para restringir a execução de *Java script* e de programas *Java* ou *ActiveX*, exceto para casos específicos; configurar o *browser*

para bloquear *pop-up windows* e permiti-las apenas para sites conhecidos e confiáveis, onde forem realmente necessárias; configurar o programa leitor de *e-mails* para não abrir arquivos ou executar programas automaticamente; e não executar programas obtidos pela *Internet*, ou recebidos por *e-mail*.

2.6.2.2 Medidas aplicáveis às instituições

Os principais objetivos das medidas implementadas pelas instituições financeiras são diminuir os riscos de fraudes e evitar prejuízos financeiros. Além de preservar a sua imagem perante o cliente, as instituições buscam formas de garantir um ambiente mais seguro para os usuários, possibilitando a realização das transações com segurança.

Com essa preocupação foi necessária uma evolução dos métodos de autenticação para se garantir maior segurança aos clientes. De acordo com Bonfietti (2007), a evolução dos métodos pode ser dividida em autenticação de senha estática (teclado virtual e teclado codificado) ou dinâmica (tabela de senhas, *One Time Password* – OTP e certificação digital). Segundo Marques (2004), teclado virtual é uma ferramenta de segurança utilizada pelos clientes dos bancos durante a utilização do *Internet Banking*. A inserção da senha é realizada utilizando o mouse e evitando o uso do teclado. Seu principal objetivo é combater a ação de algum *keylogger* instalado no computador do cliente que tem o poder de monitorar tudo o que é digitado no teclado convencional da máquina, incluindo senhas bancárias. Outra utilidade do teclado virtual é evitar que pessoas que tentam obter senhas digitadas olhando por sobre o ombro de quem utiliza o sistema. Pois muitos possuem controle de contraste, o que permite tornar os caracteres mais claros e impossibilitar a leitura à distância.

Os teclados virtuais podem ser numéricos ou alfanuméricos, as teclas podem estar dispostas de forma ordenada ou aleatória e também sua imagem pode ser fixa ou mudar a cada acesso. Essas características dependem de como cada instituição implementa a ferramenta e são utilizadas para evitar ataques de *screenloggers*, que são capazes de capturar as imagens da tela a cada ação do mouse.

Segundo o HSBC (2007), o teclado codificado serve como uma proteção adicional ao teclado virtual. Mas, de modo diferente deste, a digitação dos dados no teclado codificado é feita por meio do teclado convencional e não por cliques do mouse. No teclado codificado cada caractere é relacionado a um grupo de outros caracteres, e esta relação muda a cada novo uso do sistema bancário. Com isso, mesmo que a digitação seja capturada, não é possível descobrir a senha original. Como a cada novo uso do teclado codificado as letras mudam de posição, a correspondência entre estes elementos também muda. Desta forma, na próxima vez em que o sistema for utilizado, a mesma senha pode estar relacionada a outras letras. Esta é a principal vantagem do teclado codificado, pois mesmo que alguém consiga interceptar a imagem após a digitação codificada da senha, não será possível a essa pessoa ter certeza da senha original.

A tabela de senhas, chave de segurança ou tabela de acessos é um método que garante um nível de proteção a mais ao cliente durante as transações financeiras. Essa tabela consiste em uma lista de senhas numéricas exclusivas. Este mecanismo simples e rápido funciona da seguinte maneira: sempre que for efetuar alguma transação que tenha movimentação de dinheiro (pagamentos, DOC, TED, transferências, etc) via *Internet Banking*, o cliente visualizará na página do *Internet Banking* um número que terá uma senha correspondente na sua exclusiva tabela de senhas, basta clicá-lo e dar seqüência à operação.

Diferentemente dos mecanismos de senhas estáticas tradicionais, os dispositivos OTP (*one time password*) ou *tokens* de acesso geram senhas dinâmicas de forma automática e randômica, e somente poderão ser utilizadas apenas em um período curto de tempo. A solução oferecida evita que um atacante possa utilizar a senha capturada durante uma sessão para realizar transações, já que o período de tempo de utilização é limitado. Este método é utilizado como um fator de segurança adicional em transações financeiras realizadas pela Internet.

A certificação digital atesta a identidade de uma pessoa ou instituição pela *internet* por meio de um arquivo eletrônico assinado digitalmente. A certificação digital provê ainda um nível maior de segurança nas transações eletrônicas, permitindo a identificação inequívoca das partes envolvidas, bem como a integridade e a confidencialidade dos documentos e dados da transação (CAIXA, 2007). O

protocolo utilizado pela maioria das instituições financeiras em suas aplicações *on-lines* é o protocolo SSL (*Secure Sockets Layer*). O SSL estabelece um canal seguro onde os dados são cifrados, provendo a autenticação tanto do cliente como do servidor (nesse caso, o servidor é a instituição financeira) e realiza o transporte confiável da mensagem garantindo a integridade. A autenticação ocorre utilizando um certificado digital, considerado um documento eletrônico de identificação digital (MARTINS, 2001).

De acordo com Bonfietti (2007), algumas medidas adicionais de segurança podem ser tomadas para garantir a integridade e a privacidade dos usuários como o cadastramento de computadores onde o computador, depois de cadastrado, é reconhecido pelo sistema do Banco, evitando que terceiros possam movimentar as contas pela *Internet* a partir de outros computadores; também, a utilização de autenticação por frase secreta que é composta por uma pergunta e uma resposta criadas pelo cliente e que serão exigidos como autenticação adicional às outras senhas durante a utilização do *Internet Banking*; por último, o autor salienta a importância da educação do usuário através de manuais e cartilhas *on-line* com dicas de segurança, alertando os usuários dos riscos e quais medidas podem ser tomadas para tornar o ambiente operacional mais seguro. Este método é extremamente eficaz contra a engenharia social, que por falta de treinamento ou até mesmo inocência do usuário, contribui para a efetivação das fraudes.

2.7 FATORES DE RESTRIÇÃO AO USO DA *INTERNET BANKING*

Perder tempo, por menor que seja, pode representar perda de clientes. Devido a esta necessidade de aprimoramento constante para manutenção ou conquista de mercado, surge também a necessidade de se conhecer e acompanhar os passos do consumidor deste serviço, identificando seus anseios, visando manter a linha de satisfação sempre crescente, e por conseqüência, o retorno financeiro da instituição. A adoção e fortalecimento de políticas corretas, voltadas para as necessidades dos usuários e a identificação de possíveis falhas deve ser uma constante para evitar a perda de mercado (MÜLLER, 2001).

Segundo Teixeira (2007) as relações e trocas desenvolvidas através do *Internet Banking* são relativamente recentes. Por conseguinte, existem poucos estudos a respeito do comportamento do consumidor neste tipo de ambiente. Porém, um dos conceitos primordiais para o sucesso dessas transações está relacionado ao desenvolvimento do sentimento de confiança entre as partes relacionadas: consumidores e bancos.

Para Pires e Costa Filho (2001), outro fator a considerar nesta relação é o aspecto cultural. No segmento bancário, a crescente transferência do atendimento tradicional para o auto-serviço, como estratégia de atuação dos bancos, requer um entendimento da aceitação pelo consumidor de serviços bancários e uma análise de forma sistêmica do preparo deste para acompanhar e assimilar novos produtos e serviços a ele oferecidos.

Kotler (1998 *apud* PIRES e COSTA FILHO, 2001) ressalta a conveniência de tempo, lugar e acesso como um dos fatores decisivos de adoção dos canais eletrônicos pelos clientes. Os consumidores, a exemplo do varejo, procuram otimizar as suas relações de compra, organizando o processo de procura de um bem ou serviço pela redução de tempo e esforço para as transações individuais. Os estudos publicados sobre a aceitação dos canais eletrônicos apontam certos tipos de clientes que ainda resistem à adoção dos equipamentos como apoio à realização das operações bancárias. Por outro lado, para um grupo de clientes, os canais eletrônicos tornaram-se elemento essencial na condução dos seus negócios financeiros.

Sob outro foco, a resistência às novas tecnologias por alguns consumidores deve-se aos aspectos de inovação. Neste caso tem-se também dois grupos distintos: um composto por clientes que visam à rapidez, estão acostumados com o uso da tecnologia e sentem-se atraídos por ela; e outro, formado por clientes mais conservadores, que não gostam de inovações, não confiam nelas ou as temem, preferindo um contato pessoal. Como predisponentes do receio ou desconfiança, López-Oliva e Bojórquez (1991 *apud* PIRES e COSTA FILHO, 2001) ressaltam os fatores culturais (hábitos herdados, crenças, costumes e expectativas) que operam como estímulos da sociedade para novas idéias e tudo aquilo que possa alterar o curso normal da vida cotidiana.

As novas tecnologias propiciam benefícios tanto para organizações quanto para usuários, no entanto, afirmam Bitner *et alii* (2000 *apud* OLIVEIRA, 2000, p. 73), "a difusão da tecnologia pode também despertar preocupações junto aos clientes quanto a privacidade, confidencialidade e recebimento de comunicações não solicitadas." Estes e outros aspectos negativos da difusão levam muitos a agir com precaução quando estão diante de novas aplicações tecnológicas. Essa precaução faz com aconteça uma restrição, no mínimo, ao uso da tecnologia.

Por outro lado, segundo Oliveira (2000), a resistência revela indivíduos com estados particulares de ansiedade quando obrigados a lidar com equipamentos e máquinas. A sensação de angústia faz com que o cliente se sinta em perigo quando em contato com a tecnologia o que promove a resistência às mudanças. A constante introdução da tecnologia nas vidas pessoais e profissionais dos indivíduos pode instilar em seus comportamentos sentimentos de medo. A natureza do trabalho que envolve tecnologia diminui as interações humanas e produz confusão e ambigüidade entre as pessoas. Os indivíduos se sentem intimidados pela tecnologia, sem privacidade e envergonhados quando não sabem lidar com ela. A partir daí, a resistência se faz presente.

Rodrigues et alii (1989 *apud* OLIVEIRA, 2000) afirmaram que apesar da postura favorável a canais automatizados, existia certa distância entre aceitação e uso. Assim, parecia que a utilização de canais eletrônicos se restringia a um grupo de pessoas, com alto nível educacional e de renda. A disseminação do uso dependia do desenvolvimento de um processo de aprendizagem com equipamentos automatizados em geral, o que parecia poder ocorrer a médio e longo prazo.

Atualmente, segundo Dayal (1999 *apud* OLIVEIRA, 2000), o medo é a falta de segurança, de privacidade e de confidencialidade. Para alguns autores, existem duas tendências sobre a questão da privacidade:

> "[...] a primeira delas versa sobre a possibilidade de coletar, armazenar, acessar e analisar, com significativa velocidade, grandes quantidades de dados sobre as pessoas e companhias; a segunda tendência aponta o desconforto sentido por muitas pessoas em relação ao uso de seus dados pessoais por instituições financeiras às quais estão vinculados, mesmo que essa utilização renda benefícios para o próprio cliente" (OLIVEIRA, 2000, p. 76).

Para Roboff e Charles (1998 *apud* OLIVEIRA, 2000) os consumidores tendem a pensar em segurança envolvendo a noção de proteção contra crimes, invasões de privacidade e eventuais erros no processamento de suas transações. As mensagens positivas sobre segurança *on-line* ainda não penetraram na consciência do cliente bancário. Segundo Oliveira (2000) a melhor alternativa para reduzir as incertezas é agir na correção imediata de possíveis erros e disponibilizar canais para os clientes colocarem os seus problemas sem limites de horário, procurando solucioná-los o mais imediatamente possível.

Como pode-se observar ao longo da pesquisa bibliográfica, o contexto estrutural e conjuntural empurrou os bancos no sentido da adoção dos sistemas eletrônicos de atendimento o que promoveu um crescimento vultuoso do *Internet Banking* até 2004. A partir de então, este crescimento tornou-se moderado, ou seja, o número de usuários tem aumentado discretamente, fato este fundamentado no limite de uso entre os internautas existentes e na insegurança destes com relação ao sistema, incluindo-se aí aspectos como o medo da falta de privacidade e de confidencialidade. Além disso, a literatura aponta inúmeros fatores restritivos à utilização do *Internet Banking* que dependem em muito do fator cultural. Isto gera variações de uma região para outra que dependem de pesquisas locais para que se tenha dados suficientes para elaboração de uma política de relacionamento adequada a cada realidade específica.

Como forma de contribuição nesta área de conhecimento, este estudo busca identificar os principais fatores geradores de resistência ao uso do *Internet Banking* na agência do Banco do Brasil S.A. de Itapema (SC) por meio de uma pesquisa quantitativa realizada através de um questionário estruturado a ser aplicado em uma amostra da população-alvo cujos resultados serão analisados para que se chegue a conclusões plausíveis e recomendações realistas conforme a metodologia exposta a seguir.

3 METODOLOGIA DA PESQUISA

Este estudo será elaborado na agência do Banco do Brasil S.A. de Itapema (SC). A instituição possui mais de 4 mil agências e mais de 40 mil caixas eletrônicos no Brasil, localizados em quiosques, shoppings, aeroportos, rodoviárias, entre muitos outros. Atualmente conta com 24,6 milhões de clientes correntistas e mais de 85 mil funcionários. Sua presença internacional é caracterizada por mais de quarenta pontos de atendimento, divididos em agências, subagências, unidades de negócios/escritórios e subsidiárias, sendo atualmente o maior banco do país.

Especificamente quanto à agência de Itapema (SC),local de realização do estudo, são mais de 8 mil contas correntes, incluídos poupadores e correntistas. Destes, pouco mais de 700 clientes utilizam o canal de atendimento Internet Banking. A pesquisa será direcionada a estes clientes, através de uma amostra representativa desta população, identificada pelos sistemas internos da agência. Através de um questionário estruturado com sete questões, com respostas únicas e objetivas, serão analisados os itens que compõem o objetivo deste trabalho, notadamente os fatores de restrição ao uso do *Internet Banking*, o grau de satisfação dos usuários e as transações mais efetivadas.

Para atingir o objetivo proposto se faz necessária a adoção de uma metodologia que forneça bases suficientemente confiáveis para a análise e reflexão e permita chegar a conclusões plausíveis e recomendações realistas. Assim sendo, definiu-se como método a pesquisa quantitativa que considera que tudo pode ser quantificável, o que significa traduzir em números opiniões e informações para classificá-las e analisá-las.

Dividiu-se então a pesquisa em duas fases: a pesquisa exploratória e a pesquisa descritiva. A fase exploratória buscou identificar, através da pesquisa teórica, aspectos inerentes ao *Internet Banking*, bem como os instrumentos mais adequados para proceder à avaliação das preferências dos usuários do sistema. O estudo exploratório é caracterizado pela flexibilidade com respeito aos métodos utilizados e visa prover o pesquisador de um maior conhecimento sobre o tema ou problema de pesquisa.

Para Malhotra (2001 *apud* TEIXEIRA, 2007), o objetivo principal da pesquisa exploratória é possibilitar a compreensão do problema enfrentado pelo pesquisador. Ela é usada em casos nos quais é necessário definir o problema com maior precisão e identificar fatores relevantes para o levantamento desse problema. Os estudos exploratórios servem para aumentar o grau de familiaridade com fenômenos relativamente desconhecidos, e obter informações sobre a possibilidade de levar a cabo uma investigação mais completa sobre um contexto particular da vida real, investigar problemas do comportamento humano que os profissionais de determinada área considerem cruciais, identificar conceitos ou variáveis promissoras, estabelecer prioridades para investigações posteriores ou sugerir afirmações verificáveis. Assim, selecionou-se inúmeras fontes de informação (literatura, artigos publicados, sites acadêmicos, etc.) para uma melhor compreensão do problema e que, ao final, serviram como base para o desenvolvimento teórico apresentado anteriormente. Com as informações levantadas nesta fase foi possível desenvolver o instrumento de coleta de dados utilizado na segunda fase da pesquisa.

A pesquisa descritiva, segunda fase, baseia-se na aplicação do instrumento de coleta de dados, ou seja, um questionário direcionado aos usuários do sistema *Internet Banking* da agência do Banco do Brasil de Itapema (SC). Segundo Churchill (1987 *apud* TEIXEIRA, 2007), a pesquisa descritiva objetiva conhecer e interpretar a realidade sem nela interferir para modificá-la. Pode-se dizer que ela está interessada em descobrir e observar fenômenos, procurando descrevê-los, classificá-los e interpretá-los, sendo que este é o objetivo principal deste estudo. A pesquisa descritiva é caracterizada por possuir objetivos bem definidos apresentar procedimentos formais e ser bem estruturada. Estes estudos têm como objetivo prover o pesquisador com as características de grupos, estimar proporções de determinadas características e verificar a existência de relação entre as variáveis.

A pesquisa descritiva tem como delineamento o levantamento tipo *survey* que busca informação diretamente com um grupo de interesse a respeito dos dados que se deseja obter. Neste caso não interessam os indivíduos em si, mas os perfis. Apresenta como vantagem a abordagem simples e direta para levantar atitudes, valores, crenças e motivos. As pesquisas deste tipo se caracterizam pela interrogação direta das pessoas cujo comportamento se deseja conhecer.

Basicamente, procede-se à solicitação de informações a um grupo significativo de pessoas acerca do problema estudado para, em seguida, mediante análise quantitativa, obter as conclusões correspondentes dos dados coletados. Neste caso, o instrumento de pesquisa é o questionário.

3.1 ETAPAS DO TRABALHO

3.1.1 Estruturação do Instrumento de Pesquisa

No *survey*, as questões são colocadas aos respondentes via instrumentos estruturados, formais, com questões arranjadas previamente, em uma ordem rígida, de modo direto onde o objetivo do estudo não é disfarçado. Os métodos de levantamento direto estruturados envolvem a aplicação de um questionário com questões cujas respostas estão dentro de um grupo de alternativas. Esses questionários podem ser aplicados através de diversos canais como a *internet,* o telefone, pessoalmente, etc. (MALLHOTRA, 1996 *apud* OLIVEIRA, 2000).

Após o levantamento dos dados iniciais necessários, seguiu-se a elaboração do questionário supervisionado composto por sete perguntas objetivas, com respostas únicas. O questionário aplicado aos respondentes tem dois blocos. O primeiro contém questões sobre o perfil do usuário de auto-atendimento bancário e o segundo tem as questões envolvendo comportamentos e atitudes em relação à utilização do sistema. As questões levantadas envolvem os seguintes aspectos: faixa etária, escolaridade, freqüência de acesso ao *Internet Banking*, grau de satisfação com o uso do *Internet Banking*, a transação mais utilizada, o grau de conhecimento sobre *Internet Banking* e o fator de restrição ao uso do *Internet Banking* considerado como mais importante.

Uma vez criado o questionário (ANEXO A) fez-se necessária a realização de um pré-teste para verificar a compreensão verbal e o tempo necessário para respondê-lo. O tempo médio gasto na sua execução foi de oito minutos e como não houve problemas de compreensão iniciou-se a aplicação efetiva do questionário.

3.1.2 Coleta e Análise dos Dados

A coleta de dados é a fase da pesquisa onde ocorre a aplicação do instrumento de coleta de dados, para que se possa obter insumos para responder à pergunta de pesquisa. Na prática, a coleta de dados significa colocar em andamento os procedimentos planejados para os objetivos (SANTOS, 1999 *apud* ABDALA, 2004).

Neste estudo, a coleta de dados foi efetuada através de um questionário estruturado, contendo sete perguntas e com o assinalamento de uma única resposta, aplicado a uma amostra da população alvo, pessoalmente ou através do telefone. O período de coleta foi de 01/08/2007 a 31/08/2007.

O universo da pesquisa limita-se aos clientes da agência do Banco do Brasil de Itapema (SC), usuários do *Internet Banking*. São cerca de 800 clientes identificados pelos sistemas do banco. O tipo de amostragem adotada foi a aleatória simples sendo que a amostra corresponde a 5,25% da população em questão, ou seja, 42 clientes entrevistados.

A análise dos dados irá considerar como base a estrutura definida no questionário utilizado na pesquisa, com ênfase nos dados relativos à satisfação dos clientes, transação mais efetuada e o fator de restrição ao uso do *Internet Banking* considerado mais importante pelos usuários pesquisados.

4 ANÁLISE DOS RESULTADOS

A análise dos resultados compreende a sistematização dos dados (tabulação), sua análise e interpretação. Ela tem como base a estrutura definida no questionário utilizado na pesquisa de campo. O instrumento de coleta de dados compôs-se de dois grandes grupos de questões, as de qualificação do respondente, com o objetivo de melhor identificá-lo e as questões envolvendo comportamentos, atitudes e opiniões sobre o sistema *Internet Banking*. O roteiro da análise de dados foi definido com base nestes blocos de questões, ou seja, nos perfis da amostra e nos aspectos ligados diretamente à utilização do *Internet Banking*. A tabulação dos dados foi realizada de forma simples e a análise estatística com freqüência simples.

4.1 SISTEMATIZAÇÃO DOS DADOS

4.1.1 Perfil da Amostra

A seguir são apresentados os dados coletados que caracterizam o perfil da amostra estudada. As características em questão são a faixa etária e a escolaridade.

Tabela 01: Faixa etária

Faixa Etária	Freqüência	%
Menos de 20 anos	00	0,00
Entre 20 e 30 anos	20	47,62
Entre 30 e 40 anos	10	23,80
Entre 40 e 50 anos	08	19,05
Entre 50 e 60 anos	04	9,53
Mais de 60 anos	00	0,00
Total	42	100,00

Fonte: Instrumento de Coleta – Questionário (2007)

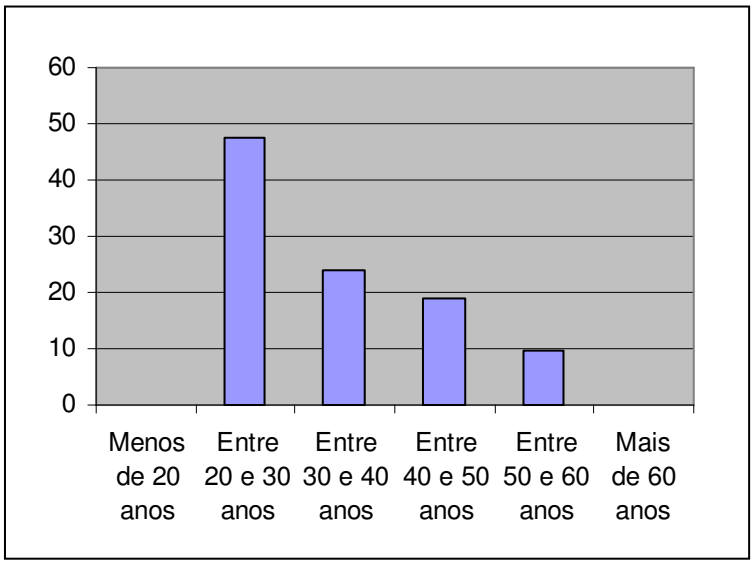

Gráfico 01: Faixa Etária
Fonte: Instrumento de Coleta – Questionário (2007)

Tabela 02: Escolaridade

Escolaridade	Freqüência	%
Até segundo grau	08	19,05
Curso Superior	20	47,62
Pós-graduado	12	28,57
Mestrado	02	4,76
Total	42	100,00

Fonte: Instrumento de Coleta – Questionário (2007)

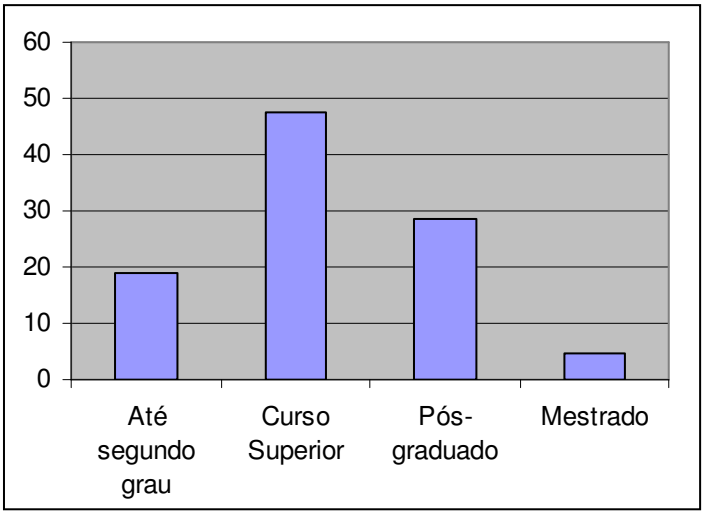

Gráfico 02: Escolaridade
Fonte: Instrumento de Coleta – Questionário (2007)

4.1.2 Aspectos Relativos à Utilização do *Internet Banking*

Nesta seção são apresentados os dados referentes às atitudes e opiniões dos respondentes com relação ao sistema de *Internet Banking*.

Estes dados são a freqüência de acesso ao *Internet Banking*, o grau de satisfação com o uso do *Internet Banking*, a transação mais efetuada, o grau de conhecimento sobre o *Internet Banking* e os fatores de restrição ao uso do *Internet Banking*.

Tabela 03: Freqüência de Acesso ao *Internet Banking*

Freq. de Acesso	Freqüência	%
Diária	08	19,05
Semanal	28	66,67
Quinzenal	02	4,76
Mensal	04	9,52
Total	42	100,00

Fonte: Instrumento de Coleta – Questionário (2007)

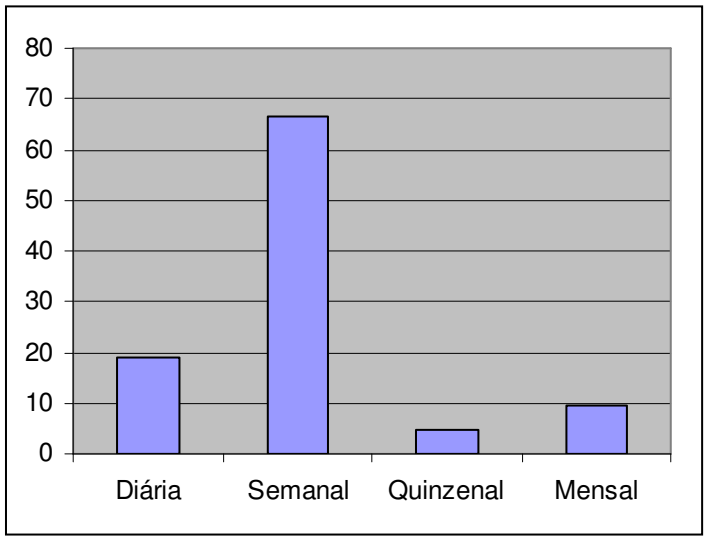

Gráfico 03: Freqüência de Acesso ao *Internet Banking*
Fonte: Instrumento de Coleta – Questionário (2007)

Tabela 04: Grau de satisfação com o uso do *Internet Banking*

Grau de Satisfação	Freqüência	%
Muito satisfeito	08	19,05
Satisfeito	34	80,95
Parcialmente satisfeito	00	0,00
Insatisfeito	00	0,00
Total	42	100,00

Fonte: Instrumento de Coleta – Questionário (2007)

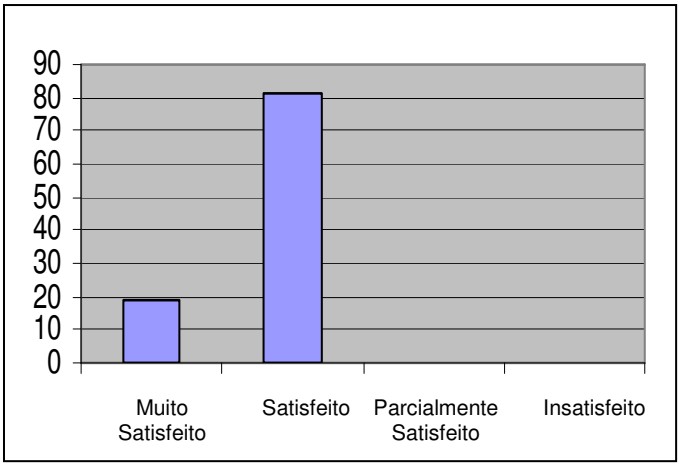

Gráfico 04: Grau de satisfação com o uso do *Internet Banking*
Fonte: Instrumento de Coleta – Questionário (2007)

Tabela 05: Transação mais efetuada

Transação	Freqüência	%
Saldos - Extratos	36	85,72
Aplicação – Resgate investimentos	00	0,00
Pagamentos	02	4,76
Compra de produtos	00	0,00
Empréstimos	00	0,00
Consulta de informações	04	9,52
Transferências	00	0,00
Outros	00	0,00
Total	42	100,00

Fonte: Instrumento de Coleta – Questionário (2007)

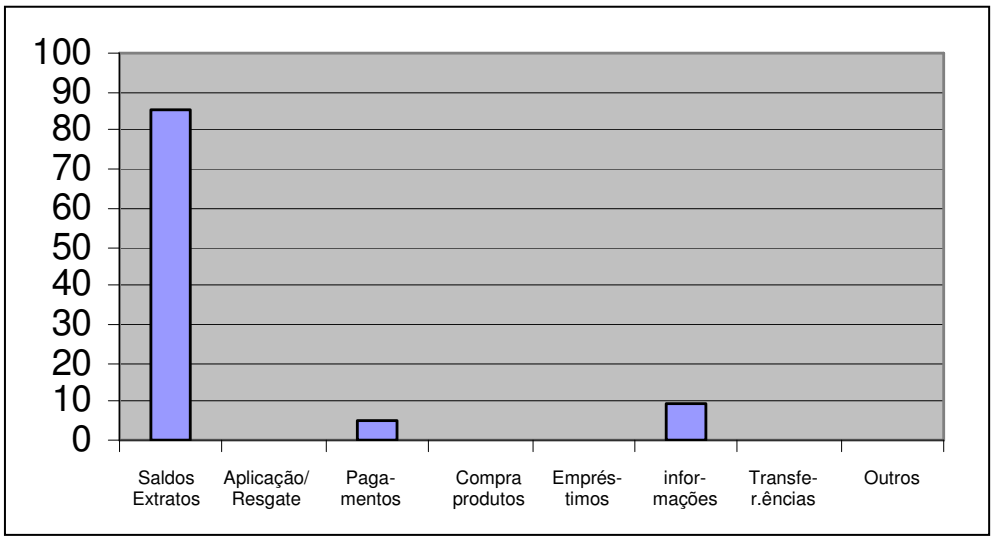

Gráfico 05: Transação mais efetuada
Fonte: Instrumento de Coleta – Questionário (2007)

Tabela 06: Grau de conhecimento sobre o *Internet Banking*

Grau de Conhecimento	Freqüência	%
Não conheço	00	0,00
Conheço pouco	02	4,76
Conheço	30	71,44
Conheço muito	10	23,80
Total	42	100,00

Fonte: Instrumento de Coleta – Questionário (2007)

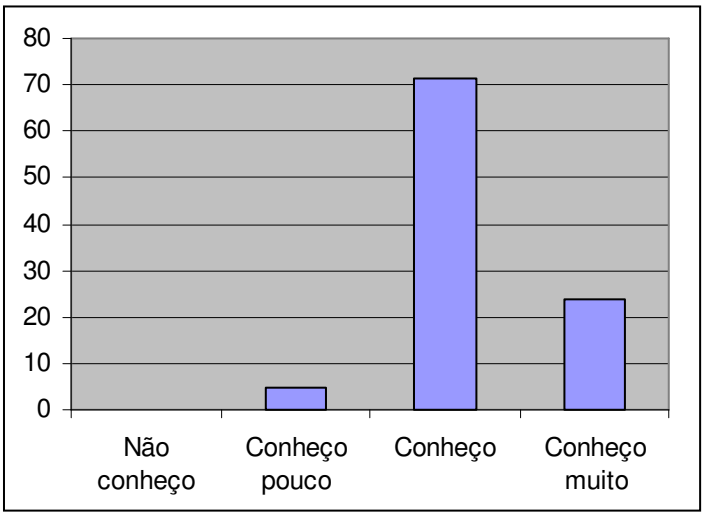

Gráfico 06: Grau de conhecimento sobre o *Internet Banking*
Fonte: Instrumento de Coleta – Questionário (2007)

Tabela 07: Fatores de restrição ao uso do *Internet Banking*

Fator de Restrição	Freqüência	%
Confiabilidade	02	4,76
Segurança	24	57,15
Problemas de uso	00	0,00
Preferência por outra forma de atendimento	12	28,57
Acessibilidade	04	9,52
Outros	00	0,00
Total	42	100,00

Fonte: Instrumento de Coleta – Questionário (2007)

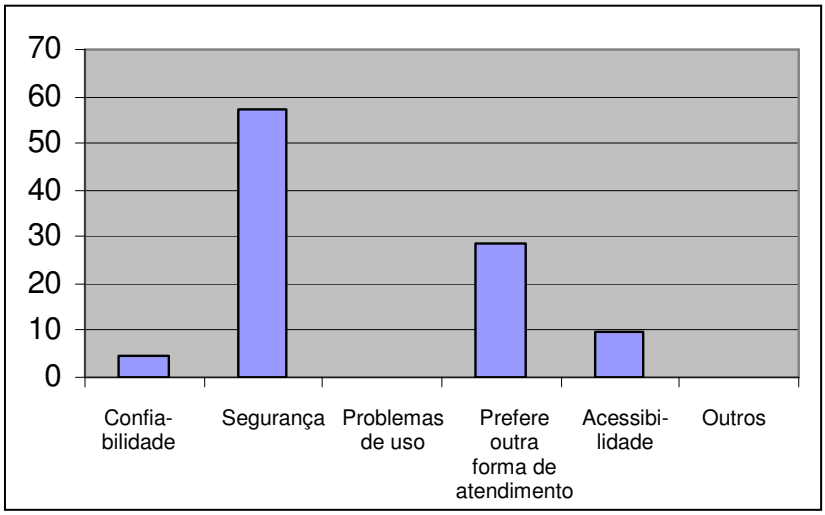

Gráfico 07: Fatores de restrição ao uso do *Internet Banking*
Fonte: Instrumento de Coleta – Questionário (2007)

4.2 ANÁLISE E INTERPRETAÇÃO DOS DADOS COLETADOS

4.2.1 Perfil da Amostra

Na pesquisa realizada percebe-se que a faixa etária predominante dos usuários do sistema *Internet Banking* é aquela entre 20 e 30 anos com um percentual de 47,62%. Observa-se também que as faixas etárias que menos utilizam o sistema são aquelas com idades entre 50 e 60 anos (9,53%) e mais de 60 anos

(0%). Estes dados mostram que, por um lado, as faixas etárias mais elevadas apresentam dificuldades com a introdução de novas tecnologias e, algumas vezes resistência às mudanças. Por outro, os mais jovens percebem as facilidades proporcionadas por ela e adaptam-se facilmente às novidades.

Analisando-se a escolaridade dos entrevistados, nota-se que a grande maioria possui curso superior (47,62%), sendo que a segunda categoria relevante é a dos que possuem pós-graduação com 28,57%. Corroborando com a pesquisa teórica, percebe-se que quanto maior a escolaridade, maior a possibilidade e facilidade do cliente utilizar-se da *Internet* para fazer suas operações bancárias.

4.2.2 Aspectos Relativos à Utilização do *Internet Banking*

Com relação à freqüência de acesso ao *Internet Banking*, o acesso semanal é o predominante com 66,67%. Em segundo lugar está o acesso diário (19,05%). Este dado pode ser explicado pelos tipos de transações mais efetuadas, já que a grande maioria dos acessos é dirigida a algum tipo de consulta como se verá a seguir.

Quanto à satisfação com o uso do *Internet Banking*, 80,95% se dizem satisfeitos e não se percebe nenhum tipo de insatisfação por parte dos respondentes já que nenhum assinalou os itens “parcialmente satisfeito” e “insatisfeito”. O que reforça a idéia de que as instituições se mantêm atentas às inovações tecnológicas e as aplicam como forma de garantir a satisfação dos seus clientes.

A transação mais efetuada é a consulta a saldos e extratos (85,72%) seguida pela consulta de informações (9,52%), isto se explica em função da simplicidade da transação e pela praticidade de realizá-las em qualquer lugar. Transações como aplicações e resgates, aquisição de produtos, empréstimos e transferências não são citadas pelos entrevistados. Neste aspecto, o que se percebe é que o cliente prefere realizar estas transações de forma mais segura e normalmente de forma presencial já que muitas vezes precisa de auxílio para a tomada de decisão.

O grau de conhecimento sobre o *Internet Banking* é bastante alto entre os usuários do *Internet Banking* já que 71,44% afirmam conhecer o sistema e 23,80% dizem conhece-lo muito. Este dado é reforçado pelo fator escolaridade, já que a grande maioria dos usuários rotineiros possui graduação e pós-graduação.

Entre os fatores de restrição ao uso do *Internet Banking* a grande maioria dos respondentes (57,15%) restringem a sua utilização por acreditar que falta segurança para as transações. Este dado reforça a idéia teórica de que a restrição se processa em função do medo dos usuários de que sua conta seja violada ou que outras pessoas possam assistir a uma transação enquanto ela estiver em curso. É um fator ligado à privacidade dos dados mantidos pelos bancos e a um receio quanto ao tratamento oferecido a esses dados. Em segundo lugar, estão aqueles que preferem outras formas de atendimento (28,57%). Fatores como a acessibilidade (9,52%) e a confiabilidade (4,76%) são citados em proporções bem menores, 9,52% e 4,76%, respectivamente. Os problemas na utilização não parecem constituir um fator de restrição já que não foram assinalados (0%).

5 CONTRIBUIÇÕES E CONCLUSÕES

Este estudo visou identificar as razões pelas quais os clientes da agência do Banco do Brasil de Itapema (SC) restringem o uso do sistema *Internet Banking*, disponibilizado para a realização de suas transações bancárias.

Entre os diversos atributos levantados na pesquisa feita com os usuários do *Internet Banking* como sendo as possíveis razões para a restrição do uso do sistema alguns índices se destacaram, principalmente o fator segurança, sobre o qual se discorreu ao longo do trabalho. De acordo com Dayal (1999 *apud* OLIVEIRA, 2000), a segurança e a confidencialidade dos dados do cliente é um receio daqueles que lidam com bancos na Internet. Os dados levantados reforçam a idéia teórica de que a restrição se processa em função do medo dos usuários de que sua conta seja violada ou que outras pessoas possam assistir a uma transação enquanto ela estiver em curso. É um fator ligado à privacidade dos dados mantidos pelos bancos e a um receio quanto ao tratamento oferecido a esses dados. Em segundo lugar, estão aqueles que preferem outras formas de atendimento, dado este reforçado pelos tipos de transações realizadas já que as transações como aplicações e resgates, aquisição de produtos, empréstimos e transferências não são citadas pelos entrevistados. Neste aspecto, o que se percebe é que o cliente prefere realizar estas operações com maior segurança e normalmente de forma presencial, já que muitas vezes precisa de auxílio para a tomada de decisão.

Outro fato confirmado com a pesquisa, é a segregação dos usuários em dois grupos distintos: um composto por clientes que visam à rapidez, estão acostumados com o uso da tecnologia e sentem-se atraídos por ela, representado pela maioria jovem que utiliza o sistema; e outro, formado por clientes mais conservadores, que não gostam de inovações, não confiam nelas ou as temem, preferindo um contato pessoal, corroborado tanto pelo baixo número de pessoas acima de quarenta anos quanto pelos tipos de transações efetuadas. Como predisponentes deste receio ou desconfiança, López-Oliva e Bojórquez (1991 *apud* PIRES e COSTA FILHO, 2001) ressaltam os fatores culturais (hábitos herdados, crenças, costumes e expectativas) que operam como estímulos da sociedade para novas idéias e tudo aquilo que possa alterar o curso normal da vida cotidiana.

Para Roboff e Charles (1998 *apud* OLIVEIRA, 2000) os consumidores tendem a pensar em segurança envolvendo a noção de proteção contra crimes, invasões de privacidade e eventuais erros no processamento de suas transações. As mensagens positivas sobre segurança *on-line* ainda não penetraram na consciência do cliente bancário. Ou seja, as instituições têm cumprido o seu papel nas questões relativas à segurança, falta agora, visando a ampliação do uso do sistema, buscar formas de repasse de informações que realmente atinjam os usuários, principalmente no que se refere às fraudes, aos meios de proteção, aos tipos de ataques possíveis e à disseminação de conceitos de segurança associados à utilização do *Internet Banking*. Em resumo, conscientizar os clientes sobre a necessidade e a eficácia das medidas de prevenção.

Da mesma forma, seria interessante que a instituição incentivasse a utilização de outros serviços e produtos disponibilizados no sistema já que pode-se perceber que a grande maioria dos usuários concentram sua utilização na consulta de saldos, extratos e demais informações. Considerando o percentual de pessoas que preferem ser atendidos de outras formas, a divulgação na própria agência da comodidade e segurança que o acesso ao sistema pode proporcionar poderia ajudar no sentido de uma maior utilização do *Internet Banking*. Sugere-se ainda, a criação de um tutorial de simulação para a realização das transações dentro do *site* do banco que permitiriam uma maior segurança e menor nível de ansiedade do usuário no momento da efetivação das operações.

As principais limitações encontradas no desenvolvimento da pesquisa foram o tempo, a disponibilidade dos respondentes e a escassez de material bibliográfico. O excessivo volume de serviços da agência não permitiu que as entrevistas fossem realizadas no horário de expediente por isso elas foram realizadas via telefone. Assim, muitos dos usuários não foram encontrados ou não dispunham de tempo para responder o questionário. Também, pela impessoalidade do contato muitos ficaram receosos acreditando tratar-se de algum tipo de fraude relacionado ao uso do *Internet Banking*. Outro fato relevante e que sugere-se como tema de futuros estudos é que a pesquisa foi realizada sobre um público que efetivamente utiliza o sistema e esta seleção excluiu as pessoas que possuem computador mas não utilizam o *Internet Banking*.

REFERÊNCIAS BIBLIOGRÁFICAS

ABDALA, Ricardo Almeida. **Avaliação dos Fatores que Influenciam a Decisão de Utilização dos Serviços Bancários através de Internet na cidade de Belo Horizonte.** 129 f. Dissertação (Mestrado em Engenharia de Produção) – Programa de Pós-Graduação em Engenharia de Produção da Universidade Federal de Santa Catarina, Florianópolis, 2004. Disponível em: http://teses.eps.ufsc.br/defesa/pdf/9916.pdf. Acesso em: 18 jun. 2007.

ACCORSI, André. **Automação:** Bancos e Bancários. 127 f. Dissertação (Mestrado em Administração) – Universidade de São Paulo, São Paulo, 1990. Disponível em: http://www.scielo.br/pdf/soc/n12/22260.pdf. Acesso em: 18 mai. 2007.

ALBERTIN, Alberto Luiz. Comércio Eletrônico: um Estudo no Setor Bancário. **RAC**, v. 3, n. 1, Jan./Abr., 1999. Disponível em: http://www.anpad.org.br/rac/vol_03/dwn/rac-v3-n1-ala.pdf. Acesso em: 20 mai. 2007.

ARANTES, Márcia Maria Ribeiro. **Comércio Eletrônico na Internet.** 79 f. Dissertação (Graduação em Ciência da Computação) – Curso de Ciência da Computação do Centro Universitário do Triângulo, Uberlândia (MG), 2000. Disponível em: http://www.computacao.unitri.edu.br/downloads/monografia/19551129386788.pdf. Acesso em: 15 set. 2007.

BONFIETTI, Hugo da Silva. **Fraudes no Internet Banking:** Conceitos, estatísticas e medidas preventivas. 49 f. Dissertação (Graduação em Ciência da Computação) – Curso de Ciência da Computação da Universidade de São Paulo, São Carlos (SP), 2007. Disponível em: http://www.icmc.usp.br/~estagio/computacao/monografias/hugobonfietti.pdf.Acesso em: 11 jul. 2007.

CARATE, Léu Cardoso. **Mudança Comportamental e Tecnologia da Pesquisa Exploratória Sobre o uso da *Internet* em uma Instituição de Ensino Superior.** 113 f. Dissertação (Mestrado em Administração) Programa de Pós-Graduação da Universidade Federal do Rio Grande do Sul, 2001. Disponível em: http://volpi.ea.ufrgs.br/teses_e_dissertacoes/detalheLivro.asp?livro=000409&radioTipo=M. Acesso em: 21 ago. 2007.

CERT. **Cartilha de Segurança na *Internet*.** Disponível em http://cartilha.cert.br/conceitos/sec1.html. Acesso em: 07 mai. 2007.

DIAS, João Salazar e CORREIA, Vítor. **Economia Mundial:** "Sociedades em Rede", "Economia Digital" ou "Nova Economia"?, 1999. Disponível em: http://www.dpp.pt/gestao/ficheiros/infor_inter_1999_II_III.pdf. Acesso em: 18 ago. 2007.

DINIZ, Eduardo. Evolução do Uso da Web pelos Bancos. **RAC**, v. 4, n. 2, mai./ago., 2000. Disponível em: http://www.ufsj.edu.br/Pagina/patricia/Arquivos/rac-v4-n2-edd.pdf. Acesso em: 05 set. 2007.

ESTRADA, Manuel Martin Pino. A Internet Banking no Brasil, na América Latina e na Europa. **Revista do Programa de Mestrado em Direito do UniCEUB**, Brasília, v. 2,

n. 1, p. 138-166, jan./jun., 2005. Disponível em: http://www.mestrado.uniceub.br/revistamestrado/pdf/Artigo%20Manuel%20Martin%20Pino.pdf.Acesso em: 20 ago. 2007.

FERRO, Wanderson Roberto. **Comércio Eletrônico e a Segurança da Rede:** Uma Visão Tecnológica. VI SEMEAD, 2003. Disponível em: http://www.ead.fea.usp.br/Semead/6semead/MQI/011MQI%20-%20Com%E9rcio%20Eletr%F4nico%20e%20a%20Seguran%E7a%20da%20Rede.doc .Acesso em: 25 mar. 2007.

LAU, Marcelo e SANCHEZ, Pedro Luiz Próspero. **Técnicas utilizadas para efetivação e contenção das fraudes sobre internet banking no brasil e no mundo.** Disponível em: http://www.datasecur.com.br/artigo.pdf. Acesso em: 30 set. 2006.

LAU, Marcelo. **Análise das fraudes aplicadas sobre o ambiente *internet banking***. 103 f. Dissertação (Mestrado em Engenharia) – Curso de Engenharia da Escola Politécnica da Universidade de São Paulo, São Paulo, 2006. Disponível em: http://www.teses.usp.br/teses/disponiveis/3/3142/tde-19092006-164238/. Acesso em: 09 set. 2007.

LOBO, Ana Paula. Inclusão digital é meta para ampliar negócios bancários, diz Febraban. **Convergência Digital**, CIAB, 2007. Disponível em: http://www.convergenciadigital.com.br/cgi/cgilua.exe/sys/start.htm?infoid=7641&sid=52. Acesso em: 31 ago. 2007.

MÜLLER, Flávio Roberto. **Identificação das Causas da Não Utilização do Sistema de Internet Banking da Caixa Econômica Federal em Porto Alegre.** 125 f. Dissertação (Mestrado em Administração) - Programa de Pós-Graduaçao em Administração da Universidade Federal do Rio Grande do Sul, 2001. Disponível em: http://volpi.ea.ufrgs.br/teses_e_dissertacoes/td/000511.pdf. Acesso em: 15 set. 2007.

OLIVEIRA, Roberto Almeida Campos de. **O Internet Banking e os Hábitos de Uso entre os Clientes Pessoa Física:** Atributos e Resistências. 182 f. Dissertação (Mestrado em Administração) - Programa de Pós-Graduaçao em Administração da Universidade Federal do Rio Grande do Sul, 2000. Disponível em: http://volpi.ea.ufrgs.br/teses_e_dissertacoes/detalheLivro.asp?livro=000224&radioTipo=M. Acesso em: 09 set. 2007.

PIRES, Péricles José e COSTA FILHO, Bento A. da. O Atendimento Humano como Suporte e Incentivo ao Uso do Auto-Atendimento em Bancos. Rev. **FAE**, Curitiba, v.4, n.1, p.59-67, jan./abr. 2001. Disponível em: http://www.unifae.br/publicacoes/pdf/revista_da_fae/fae_v4_n1/o_atendimento_humano_como_.pdf. Acesso em: 26 jul. 2007.

SIMON, Cláudio Antônio de Paiva. Scam, phishing e pharming: As fraudes praticadas no ambiente Internet Banking e sua recepção no Brasil. **Revista de Derecho Informático**, n. 105, abr., 2007. Disponível em: http://www.alfa-redi.org/rdi-articulo.shtml?x=9077. Acesso em: 23 ago. 2007.

TEIXEIRA, Maria Augusta Carneiro. ***Internet Banking*** **Pessoa Jurídica:** Um Estudo de Caso do Relacionamento de uma Agência Bancária com as Pequenas e Médias Empresas. Dissertação (Graduação em Administração) Curso de Administração e Habilitação em Pequena e Média Empresa da Faculdade 7 de Setembro, Fortaleza (CE), 2007. Disponível em: http://www.fa7.edu.br/iniciacaocientifica/arquivos/41151-AugustaINTERNET_BANKING4.doc. Acesso em: 24 ago. 2007.

WEBER, Raul Fernando. **Segurança na Internet.** Porto Alegre: Instituto de Informática da Universidade Federal do Rio Grande do Sul, 1999. Disponível em: http://www.inf.ufsc.br/~mauro/curso/redes/segur.doc.Acesso em: 02 set. 2007.

ZANON, Érica. Cresce uso de internet banking no Brasil. **Folha de Londrina**, Londrina (PR), ago., 2006. Disponível em: www.bonde.com.br/folha/folhad.php?id=3635LINKCHMdt=20060804. Acesso em: 05 mar. 2007.

ANEXO A – INSTRUMENTO DE PESQUISA (QUESTIONÁRIO)

Questionário sobre utilização do INTERNET BANKING

Data: ___/___/___

1. Faixa etária:
( ) Menos de 20 anos ( ) Entre 20 e 30 anos
( ) Entre 30 e 40 anos ( ) Entre 40 e 50 anos
( ) Entre 50 e 60 anos ( ) Mais de 60 anos

2. Escolaridade
( ) Até segundo grau ( ) Curso Superior
( ) Pós-graduado ( ) Mestrado

3. Qual a freqüência de acesso ao Internet Banking?
( ) Diária ( ) Semanal
( ) Quinzenal ( ) Mensal

4. Qual o grau de satisfação com o uso do Internet Banking?
( ) Muito satisfeito ( ) Satisfeito
( ) Parcialmente satisfeito.Justifique:_____
( ) Insatisfeito Justifique:_____

5. Qual a transação mais utilizada?
( ) Saldos - Extratos ( ) Aplicação – Resgate investimentos
( ) Pagamentos ( ) Compra de produtos
( ) Empréstimos ( ) Consulta de informações
( ) Transferências ( ) Outros

6. Como classifica seu conhecimento sobre Internet Banking?
( ) Não conheço
( ) Conheço pouco
( ) Conheço
( ) Conheço muito

7. Qual o fator de restrição ao uso do Internet Banking que considera mais importante ?

( ) Confiabilidade (Confiança na execução serviços realizados)
( ) Segurança (Receio da ocorrência de fraudes ou violação da privacidade)
( ) Problemas de uso (Dificuldades de interagir com sistemas, conhecimento dos serviços).
( ) Preferência por outra forma de atendimento(Pessoal, auto-atendimento, móbile banking, central atendimento por telefone)
( ) Acessibilidade (rapidez no acesso e efetivação das transações)
( ) Outros. Especificar:_____