Análise de Satisfação com a Segurança no Uso de Internet Banking em Relação aos Atuais Recursos Disponíveis no Canal Eletrônico

Autoria: Marcos Leandro Donner, Leonardo Rocha de Oliveira

RESUMO

Os últimos anos mostraram mudanças significativas na forma como as pessoas e as organizações se comunicam. Em grande parte, estas mudanças têm sido proporcionadas pela Tecnologia de Informação (TI), com destaque aos novos modelos de negócios suportados pela Internet e sistemas na Web. O setor financeiro é um dos que mais tem investido na adoção destes sistemas, tendo como um importante mecanismo os bancos eletrônicos na Internet e seu papel como catalisador de novas estratégias de mercado e redução de custos operacionais. Entretanto, tratando-se de tráfego de informações sigilosas na Web, preocupações com segurança devem estar entre as prioridades de investimentos. Estes investimentos também têm gerado mudanças que são discutidas no corpo deste trabalho, cujo objetivo é avaliar o nível de satisfação de usuários de Internet Banking com as funcionalidades e a segurança disponíveis neste canal eletrônico no Brasil. Para isso foi elaborada uma pesquisa exploratória com análises quantitativas e qualitativas, elaboradas a partir da aplicação de questionário a usuários ativos de Internet Banking. Os resultados mostram que a maioria dos usuários se sente seguro ao utilizar este canal, embora isto não esteja diretamente ligado a nenhum dos recursos de segurança em especial. Como conclusão cabe destacar que usuários em geral, apesar de sentirem segurança com este tipo de operação bancária, deixam que os esforços de proteção fiquem sob a responsabilidade das instituições financeiras.

1. Introdução

O rápido desenvolvimento dos canais de relacionamento e necessidades em atender aos mais diferentes tipos de clientes e potenciais de negócios tem encorajado as instituições financeiras a estimular o uso de Internet Banking. Os próprios clientes estão cada vez mais reconhecendo o potencial do canal Internet para suas atividades financeiras pessoais ou profissionais, buscando agilidade, comodidade e segurança.

As mudanças organizacionais e o suporte das novas tecnologias estão provocando mudanças significativas no uso comercial da comunicação eletrônica em geral, onde se inclui o protocolo TCP/IP de Internet com seu papel em atividades de comércio eletrônico, e-business e demais transações financeiras e de comunicação. As aplicações abertas e com conectividade irrestrita, utilizando a grande rede como plataforma tecnológica são os principais direcionadores das atuais tecnologias e soluções de comunicação. Navegadores, editores eletrônicos, servidores de Internet e Intranets, sistemas de gestão de redes e demais produtos que trafegam sob o protocolo TCP/IP, assim como os dispositivos de segurança que devem estabelecer critérios de segurança para esta infinidade de acessos, são apenas alguns exemplos desta realidade (O'BRIEN, 2004).

A utilização efetiva dos canais eletrônicos para produtos e serviços é uma necessidade no atual mundo dos negócios. Entretanto, a transposição das práticas utilizadas de distribuição destes produtos não é automática para os serviços (DONNELLY, 1976). Na indústria bancária, a intensa competição, poucas oportunidades para diferenciação de produtos, novas tecnologias e demandas constantes, tem levado as instituições a reavaliar suas estruturas de distribuição (DINIZ, 1998). A característica que pode diferenciar esta estrutura de canais é a intangibilidade, pois devido a impossibilidade de transpor ou de armazenar serviços, estas empresas são obrigadas a oferecê-los em diversos locais, utilizando estruturas múltiplas (STERN, 1996).

Os serviços financeiros têm um componente de intangibilidade que faz com que a apreciação do serviço dependa muito da relação que se estabelece com o cliente (GALLEGO, 1998). Pode-se dizer que a grande vantagem que os bancos devem explorar em relação aos seus concorrentes será a confiança, através de recursos de segurança e relacionamento. Conforme Diniz (1999), as características básicas da Web podem contribuir para incrementar o relacionamento dos bancos com seus clientes, com destaque a interatividade, resposta imediata, conectividade, interoperabilidade, multimídia e facilidade de uso. No entanto, todas devem estar associadas a processos seguros para promover maiores níveis de atratividade. O estudo destes fatores em relação a realidade atual dos sistemas oferecidos pelos bancos no Brasil representam o foco deste trabalho, cujo objetivo é de avaliar o nível de satisfação de usuários com a segurança no uso de Internet Banking em relação aos atuais recursos disponíveis no canal eletrônico.

2. Segurança da Informação

Em todas as fases do processo evolutivo das empresas as informações estiveram presentes. Neste constante e necessário processo, a dependência do compartilhamento de informações passou a se tornar uma prática moderna e vital para transações e agilidade nas ações. O que muitas vezes não se percebe é a necessidade da proteção adequada a este importante ativo das organizações. As informações são consideradas recursos estratégicos para o sucesso da empresa, e por isso, deve ser tratada como um ativo tão importante como qualquer outro e protegida de acordo com o seu valor (ABNT NBR ISO/IEC 17799:2005).

A segurança da informação se caracteriza como o processo de proteção das informações de ameaças para assegurar sua integridade, disponibilidade e confidencialidade. Ou seja, o objetivo deve ser de preservar os ativos de informação, levando em conta estes três objetivos, conforme descrito a seguir.

- Confidencialidade - garantia de que somente pessoas autorizadas terão acesso à informação. De acordo com Sêmola (2003), toda informação deve ser protegida conforme o sigilo exigido ao seu conteúdo. Fator este, particular às informações privadas de clientes bancários e usuários de meios eletrônicos.
- Integridade - garantia de precisão das informações, de que elas estão corretas e que não foram modificadas sem a devida autorização. Para Beal (2005), integridade é a garantia da criação legítima e da consistência da informação ao longo do seu ciclo de vida.
- Disponibilidade - garantia de acesso às informações e aos ativos associados quando necessário.

Além destes três objetivos, alguns aspectos adicionais emergem quando a informação está inserida num processo de comunicação, sobretudo com a abrangência da Internet. Problemas como a alteração fraudulenta ou roubo de informações, levam à necessidade de estabelecer objetivos adicionais relativos à segurança da comunicação como um todo.

Durante todo seu ciclo de processamento, as informações estão sujeitas a ameaças e vulnerabilidades, conceitos que muitas vezes se confundem, mas que precisam ser entendidos claramente para agregar segurança ao processo. A ameaça é a causa potencial de um incidente, que pode comprometer o estado de segurança da informação. Criminosos virtuais são ameaças constantes a informações privadas de usuários de Internet Banking, por exemplo. Vulnerabilidades são fragilidades em um processo, que permitem que uma ameaça se concretize. Um sistema de antivírus desatualizado, a não atualização de um sistema operacional (*patches*) ou a ausência de uma ferramenta de segurança adequada são vulnerabilidades graves em computadores pessoais quando se trata de transações na Internet. A vulnerabilidade humana pode ser considerada um capítulo a parte. As pessoas

são consideradas o elo mais frágil num fluxo de informações de um processo. Atualmente a maioria dos golpes através da Internet são especialmente direcionados a esta fragilidade. Os seres humanos não possuem um comportamento binário e previsível em que se possa eliminar ou tratar determinadas características de forma pontual.

As informações envolvidas em transações *on-line* são as mais críticas e que despertam o interesse de criminosos para concretizar fraudes eletrônicas. Estas informações devem receber níveis superiores de segurança, prevenindo transmissões incompletas, erros de roteamento, alterações não autorizadas de mensagens, divulgações não autorizadas, duplicação ou representação de mensagem não autorizada (ABNT NBR ISO/IEC 17799:2005). As considerações de segurança para transações devem incluir itens como:

- uso de assinaturas eletrônicas para cada uma das partes envolvidas na transação;
- garantia de que existam credenciais de usuário para todas as partes;
- garantia da confidencialidade e privacidade dos envolvidos;
- comunicação criptografada;
- uso de protocolos seguros para comunicações;
- garantia de que o armazenamento das informações de transações seja localizado fora de qualquer ambiente publicamente acessível.

As transações geradas também precisam estar de acordo com as leis, regras e regulamentações da jurisdição em que as mesmas são geradas, processadas e armazenadas. Mais detalhes sobre esta realidade no setor financeiro Brasileiro são apresentadas a seguir.

3. Internet Banking

É claro que se um canal eletrônico de negócios como Internet Banking fosse um sucesso incontestável, substituiria totalmente as agências bancárias e caixas eletrônicos em todo o mundo (BINOTTO, 2001). Este canal deve ser considerado como um serviço complementar aos demais já disponibilizados pelos bancos há muitos anos.

Por outro lado, poucas inovações englobam tantas vantagens quanto o comércio eletrônico e Internet Banking. A natureza globalizada da tecnologia e seus custos acessíveis geram oportunidades de alcance por milhões de pessoas e a uma infinidade de aplicações com inúmeras vantagens para os usuários, empresas e a para a sociedade como um todo (TURBAN, 2002). Estas vantagens estão se expandindo significativamente e os bancos eletrônicos têm desempenhado papel importante neste crescimento, cabendo destacar aspectos como:

- possibilidade de atingir um grande número de clientes em qualquer lugar do mundo e com baixo custo operacional;
- rápida localização e acesso a produtos e serviços com custos de 5 a 20% menores do que nas modalidades de negócios tradicionais;
- redução de até 90% de custos de desenvolvimento, processamento, distribuição, armazenamento e recuperação de informações em relação a documentação impressa;
- redução de tempo no fluxo entre o desembolso de capital e contratação dos produtos e serviços;
- possibilidade de modelos inovadores de negócios com base em uma rede de relacionamento com milhões de usuários, gerando lucratividade e competitividade.

Os benefícios para os clientes também são significativos e isto pode ser comprovado pela amplitude deste modelo que não para de crescer. A seguir estão elencados os principais benefícios para os clientes de canais eletrônicos de produtos e serviços:

- produtos e serviços mais acessíveis - pode-se fazer uma associação com determinados serviços e produtos bancários disponibilizados com tarifas mais atrativas pela Internet;
- comodidade e segurança - é desnecessário sair de casa ou da empresa para concretizar a aquisição de produtos, serviços ou transações;
- possibilidade de compras ou transações 24 horas por dia, durante todo o ano e em qualquer lugar do mundo;
- acesso a informações mais detalhadas e em tempo real, ao invés de esperas para determinados tipos de dados consolidados;
- interatividade com a instituição financeira onde o usuário é cliente

4. Crimes com Internet Banking

A Internet é um universo de informações cada vez mais presente e imprescindível em na vida das organizações. Como este mundo virtual cresce em proporções gigantescas, o grande uso da rede, computadores, sistemas e aplicações que trafegam em seu ambiente, conseqüentemente estão cada vez mais expostos a riscos antes desconhecidos (NAVARRO, 2001). Uma variável clara do acesso generalizado de pessoas de todos os lugares do planeta a este novo cenário virtual é a ação constante de criminosos que se valem de seus conhecimentos e das vulnerabilidades existentes em sistemas e *websites* para obterem vantagens das mais variadas formas. Um dos fatores que vem limitando o crescimento do comércio eletrônico são problemas de segurança (BALARINE, 2002). E este ambiente com variáveis de insegurança é que exige um processo de gestão de segurança da informação, de uma infra-estrutura de tecnologia e arquitetura de soluções muito bem estruturados (WILLIAMS, 2001).

Com esta nova cultura de interatividade, lazer, comércio e transações consolidados no domínio da tecnologia, novas maneiras de praticar atos ilícitos surgiram e, crimes anteriormente realizados com armas e contato pessoal, encontraram meios alternativos, onde as distâncias não representam barreiras, os criminosos ficam sentados diante de computadores e a violência é dispensada (LIRA, 2004). Devido à grande concentração de informações privadas e relativas à transações financeiras, os crimes por computador tornaram-se fonte de elevadas perdas e alto risco para uma empresa que lança mão de meios eletrônicos para estratégias comerciais.

Os roubos ou assaltos a bancos são crimes cada vez menos praticados, e os volumes subtraídos de uma ação criminosa desta natureza são muito menores do que numa fraude eletrônica. As agências bancárias estão cada vez mais seguras e a própria cultura de segurança patrimonial já está presente há várias gerações. Realidade diferente quando se trata de cultura de segurança da informação.

O tipo de crime que mais cresce no setor financeiro é justamente o roubo de informações privadas, como números de contas, cartões e senhas. E estes criminosos não são grandes especialistas em intrusão de redes, sistemas ou servidores, pois os níveis de segurança implementados pelos bancos são extremamente efetivos. Os esforços são concentrados nas vulnerabilidades dos computadores pessoais e na ingenuidade dos próprios usuários.

As fraudes em canal eletrônico, especificamente Internet Banking podem se conectar a muitas outras, mas sempre são caracterizadas pelo roubo de informações sigilosas através de técnicas de Engenharia Social. A Engenharia Social se baseia na construção de métodos e estratégias para enganar através de informações ou confiança exploradas em vulnerabilidades humanas. Engenharia porque se constitui em táticas de

acesso a sistemas e informações sigilosas de forma indevida, Social porque se utiliza de indivíduos que pessoal ou profissionalmente vivem em grupos organizados. Particularmente a transações financeiras eletrônicas, a Engenharia Social é um tipo de ataque utilizado por criminosos virtuais, onde a principal ferramenta é a habilidade de persuasão e de lidar com pessoas, induzindo-as a fornecer informações privilegiadas e executar códigos (programas) maliciosos.

> Pode-se dizer que há duas especialidades dentro da classificação de artista da trapaça. Alguém que faz falcatruas e engana as pessoas para tirar o seu dinheiro pertence a uma subespecialidade chama *grifter*. Alguém que usa a fraude, a influência e a persuasão contra as empresas, em geral visando suas informações, pertence a outra sub-especialidade: o engenheiro social (MITNICK, 2003)

A instituição financeira pode ter adquirido as melhores tecnologias de segurança, pode ter treinado seus colaboradores tão bem que eles trancam todos os segredos antes de ir embora e contratado vigilantes para o prédio da melhor empresa de segurança disponível, mesmos assim ela ainda estará vulnerável (MITNICK, 2003). As pessoas podem seguir uma série de melhores práticas, instalarem ferramentas de segurança e monitorar criteriosamente as configurações adequadas para sistemas e correções de segurança. Porém, o próprio fator humano é o elo mais fraco de qualquer cadeia de segurança, e é esta fragilidade que é explorada e atacada por criminosos virtuais. O alvo dos fraudadores em Internet Banking foi modificado assim que os bancos começaram a investir cada vez mais em recursos de segurança na sua infra-estrutura de informação, nas suas aplicações e na conscientização dos seus colaboradores e clientes.

A evolução das pragas virtuais compreende desde os primeiros vírus surgidos nos anos 80 até os códigos dos dias atuais, muito mais sofisticados e com objetivos direcionados cada vez mais para desvio de capital de forma ilícita. A Internet atualmente convive com uma enorme variedade de ameaças às organizações de todos os portes, mas principalmente as financeiras, causando impactos que variam de indisponibilidade de sistemas e ativos de infra-estrutura até o desvio de grandes volumes de dinheiro de contas correntes. A facilidade de propagação com a rede mundial e a utilização massiva de correio eletrônico, redes e o compartilhamento de arquivos P2P (*peer-to-peer*) associados a vulnerabilidades nos canais, produtos e sistemas operacionais, auxiliam esta propagação a atingir escalas mundiais em questão de horas. Atualmente os artefatos se potencializam principalmente com os denominados *phishings*. O *phishing* é um tipo de fraude projetada pra roubar informações confidenciais. Através de um *phishing* o criminoso virtual envia uma mensagem eletrônica (e-mail, mensagem instantânea ou recado em portais de relacionamento) utilizando falsos pretextos, principalmente utilizando temas atuais ou explorando fragilidades humanas.

No Brasil esta realidade é bastante particular, com o País há alguns anos entre os primeiros no ranking mundial de volumes de fraudes em meios eletrônicos. Conforme a 9ª Pesquisa Nacional de Segurança da Informação (MÓDULO, 2003), 60% dos respondentes consideram a Internet como principal alvo de ataques por criminosos virtuais. Sendo estes, os responsáveis por 32% dos ataques e invasões em sistemas corporativos. Outro percentual expressivo diz respeito à empresas que sofreram ataques ou invasões, um total de 77% afirma ter sofrido ações desta natureza.

Existe ainda o agravante da falta de uma legislação adequada, o que faz com que muitos incidentes não sejam reportados e judicialmente tratados, pois os bancos, na grande maioria dos casos, vem a ressarcir os clientes fraudados. E a falta desta legislação

específica incentiva cada vez mais a formação de quadrilhas especializadas nesta modalidade de crime.

Os grandes bancos brasileiros já estão com milhões de usuários ativos e usando freqüentemente Internet Banking. É impossível assegurar o mesmo nível de proteção no computador pessoal ou profissional do usuário que as áreas responsáveis pela infra-estrutura de segurança em tecnologia destas organizações disponibilizam em suas redes e demais ativos de informação. A garantia de que o cliente bancário está com o mínimo necessário para efetivação de uma transação segura é impossível.

5. Recursos de Segurança em Internet Banking

5.1 Firewalls

São sistemas que estabelecem regras e filtros de tráfego entre computadores e serviços, como Internet Bankings, por exemplo. São utilizados como defesa contra ameaças externas e são considerados como separadores e analisadores, utilizados para delimitar perímetros e ambientes lógicos, seja numa Intranet, rede local ou até mesmo na Internet (O'REILLY, 1998). Neste recurso de segurança, entre outros, verifica-se se a política de segurança da empresa, relativa a controle de acessos e redes, está aplicada de forma adequada. A principal missão de um *firewall* é oferecer conexão entre redes internas e externas com níveis de segurança satisfatórios, e sua implementação tem como base os seguintes princípios (MÓDULO, 2003):

Autenticação – necessidade de validar o acesso de um ou mais usuários a recursos internos da corporação.

Autorização – necessidade de definir os direitos de acesso em perímetros da infra-estrutura.

Auditoria – rastreabilidade, ou seja, evidências de que os usuários acessaram determinados recursos internos da corporação.

Integridade – necessidade de preservar ativos e dados de possíveis invasões, perdas ou danificações.

5.2 Intrusion Detection System

O IDS é outro componente essencial de segurança e que deve estar presente na infra-estrutura de tecnologia de instituições com dados privados e transações financeiras trafegando em seus ambientes. Sua função é antecipar a detecção de possíveis invasões ou ataques, e responder a ataques, se estes ocorrerem, em tempo real, garantindo também a rastreabilidade de acessos desta natureza. Os sistemas de IDS possuem observação proativa de eventos relevantes à segurança e podem ter maior sensibilidade para eventos em ativos de maior relevância para o ambiente, por exemplo, em servidores com componentes e camadas de aplicações de bancos eletrônicos (SÊMOLA, 2003).

5.3 Intrusion Prevention System (IPS)

O IPS agrega funcionalidades de um IDS e de um *firewall*. Ele é um sistema mais sofisticado, complexo e com níveis de pró-atividade. Além de monitorar todo o tráfego de rede e identificar eventos anômalos, este sistema também tem a capacidade de tomar determinadas ações, como o bloqueio completo do ataque, da origem dos ataques e da possibilidade que a iniciativa maliciosa chegue até serviços ou ativos de tecnologia

(MÓDULO, 2005). Além desta proteção mais efetiva em tempo-real, o IPS também tem a capacidade de análise de pacotes em camadas de aplicação.

5.4 Criptografia e certificados digitais

A criptografia é considerada a mais avançada técnica de segurança para informações eletrônicas. Esta tecnologia é considerada padrão mundial para segurança na transmissão de dados através da Internet. Criptografia é a ciência de escrever mensagens em forma cifrada ou em código. É parte de um campo de estudos que trata das comunicações privadas e confidenciais, usadas para autenticação e identidade de um usuário, sigilo das comunicações pessoais, de transações comerciais e bancárias, assim como a proteção da integridade de transferências eletrônicas de fundos (CERT.br, 2007). Uma informação criptografada deve ser privada, ou seja, somente aquele que enviou e aquele que recebeu a informação devem ter acesso ao seu conteúdo. Uma mensagem também pode ser assinada digitalmente, ou seja, a pessoa que a recebeu pode verificar se o remetente é mesmo a pessoa que diz ter a capacidade de identificar se uma mensagem pode ter sido modificada.

Para garantir a autenticidade de informações, e no caso de um Internet Banking, do próprio *web site*, são utilizados certificados digitais. Através deste recurso se atesta que a página da Internet realmente pertence a uma determinada instituição e não se trata de um *site* falso. Certificado digital é um documento eletrônico que comprova a identidade de um usuário, sistema ou servidor de uma rede. Nele estão contidas informações importantes sobre a autoridade certificadora e seu titular, que garantem sua origem e confiabilidade (FEBRABAN, 2007).

5.5 Fatores de autenticação

Destinados a suprir processos de identificação de usuários, equipamentos, sistemas e agentes em geral, os mecanismos de autenticação mostram-se fundamentais para os atuais padrões de informatização, automação e compartilhamento de informações (SÊMOLA, 2003).

> Os sistemas de autenticação são uma combinação de hardware, software e procedimentos que permitem o acesso de usuários aos recursos computacionais. Na autenticação o usuário apresenta algo que ele sabe ou possui, podendo até envolver a verificação de características físicas pessoais. (DIAS, 2003)

Sem a identificação da origem de um acesso e seu agente, praticamente se inviabilizam autorizações em conformidade com os direitos de acesso. Os métodos de autenticação são divididos em três grupos de acordo com o nível de segurança agregado.

5.5.1 O que Você Sabe

Método baseado na definição de senhas, que devem ser pessoais, inequívocas, intransferíveis e entregues diretamente ao usuário autorizado a utilizá-las. Habitualmente é o primeiro fator de autenticação em um acesso a Internet Banking. Este método, por natureza, já revela fragilidades, pois a segurança do processo depende de fatores internos como a estrutura de formatação e manutenção das senhas (SÊMOLA, 2003). Também depende de fatores externos, como o comportamento e comprometimento do usuário com a proteção da sua própria credencial.

5.5.2 O que Você Tem

Método baseado na utilização de dispositivos físicos que são apresentados em processos de autenticação de acessos. Existem muitas possibilidades e tipos de dispositivos

que se enquadram neste perfil. A escolha do melhor mecanismo está diretamente ligada ao nível de segurança necessário para as informações e, inevitavelmente, ao orçamento disponível (SÊMOLA, 2003). Os principais recursos de autenticação física são cartões, *smartcards*, tabelas de senha (*tan lists*) e *tokens*. Estes dois últimos são os mais utilizados pelos bancos. O *token* é um dispositivo físico que gera novas senhas em períodos pré-determinados, e é utilizado em Internet Bankings como fator adicional de segurança para autenticação de transações.

5.5.3 O que Você É

Ainda não utilizados por Internet Banking, mas já com algumas iniciativas em caixas eletrônicos, este método, que é baseado em identificações biométricas, é uma evolução natural dos sistemas manuais de reconhecimento, amplamente difundidos há alguns anos, como a análise grafológica de assinaturas, análise de impressões digitais e o reconhecimento de voz (DIAS, 2003). O nível de segurança agregado por recursos de autenticação desta natureza é muito superior.

5.6 Cultura de Segurança

O processo de aculturamento e conscientização dos clientes de instituições financeiras em relação às ameaças na Internet é cada vez mais importante. Os usuários de Internet Banking também devem ter ciência de suas responsabilidades e dos cuidados que devem tomar ao acessarem a seu banco pela *web*. É impossível pensar em um sistema de segurança para proteção de um processo, por exemplo, que não passe pela confiança das pessoas (MÓDULO, 2005). Por isso a grande parcela da eficácia de um sistema que envolva segurança, reside também na contribuição que os usuários estão dispostos a fornecer, além da definição de controles para minimizar os riscos associados. De acordo com a ABNT NBR ISO/IEC 17799:2005, a conscientização, educação e treinamento nas atividades de segurança da informação e as orientações e conhecimentos referentes a ameaças são fatores críticos de sucesso para um processo de segurança.

5.7 Dispositivos de Segurança

O dispositivo de segurança é um componente, disponibilizado por alguns bancos, que instalado pelo usuário, agrega novos padrões de segurança ao Internet Banking, provendo segregação do navegador de Internet (*browser*) enquanto a transação eletrônica é efetuada. Seu principal objetivo é estruturar um ambiente virtual blindado, controlado e com requisitos necessários para realização de transações financeiras mais seguras.

5.8 Cadastros de Favorecidos

Para proporcionar mais segurança em transações, alguns bancos solicitam o cadastro de dados dos favorecidos para transferências entre contas. Esta prática limita as transações em função de volumes financeiros. Se a pessoa que irá receber um crédito em conta corrente não estiver previamente cadastrada, a instituição financeira limita os valores a serem creditados, ou até mesmo não autoriza a transferência eletrônica. Algumas modalidades de golpes são efetuadas por quadrilhas que precisam contar com clientes do próprio banco ou de outros bancos como cúmplices para recebimento dos valores fraudados. Por possibilitar maior rastreabilidade e controle nas transferências, este recurso tem agregado níveis satisfatórios de segurança e possibilitando maiores movimentações e limites diferenciados de transações.

5.9 Políticas de Privacidade

Uma política de segurança da informação tem por objetivo prover orientação e apoio para segurança das informações de acordo com os requisitos de negócio, leis e regulamentações relevantes (ABNT NBR ISO/IEC 17799:2005). Uma política de segurança é um documento que descreve os objetivos de todas as atividades ligadas à segurança da informação em uma organização ou em determinado processo. Também são consideradas regras que em vários níveis estabelecem o comportamento e as ferramentas para manter o nível de segurança adequado.

Uma política de privacidade deve orientar em como proceder com informações de clientes e tratar questões referentes à manipulação e divulgação de informações. Através desta política, a instituição se compromete a tratar as informações fornecidas e trafegadas em seus *web sites* de forma segura e com o sigilo necessário.

6. Negócios com Internet Banking

6.1 O Internet Banking como Canal de Divulgação

A extensão da marca destas instituições para Internet traz vantagens naturais para todos os envolvidos. A facilidade de encontrar os *sites* e a lealdade à marca se transferem para o mundo virtual. O portfólio de produtos também costuma ser o mesmo do mundo físico, com algumas adaptações necessárias para o ambiente virtual (BREI, 2001). As ações para promoção dos bancos eletrônicos geralmente são incorporadas à comunicação institucional, desta forma não há ações específicas para nichos de clientes que sejam mais propensos a utilizarem este canal.

6.2 Parcerias na *web*

Investimentos em segurança, proporcionando maior credibilidade e visibilidade do Internet Banking também possibilitam parcerias *on-line* efetivas. Estas alianças acontecem quando um banco estabelece um relacionamento com outra empresa de telecomunicações, um provedor de serviços ou um portal *web*, por exemplo, permitindo o acesso de um grande número de clientes atuais ou potenciais. Trata-se de uma forma efetiva e rápida de assegurar credibilidade através da imagem bastante associada ao mundo virtual do parceiro estratégico. O que estimula esta estratégia é a possibilidade da base de clientes, para ambas as empresas, procurando ressaltar os atributos do parceiro.

6.3 Novos Clientes e Relacionamento

A Internet atinge uma parcela de usuários cada vez mais influentes e com graus elevados de exigência de qualidade e confiabilidade. E a segurança do banco eletrônico tem papel crucial neste processo. Um banco ou qualquer outra empresa com maior número de produtos e serviços torna-se mais atrativo, mas com o acentuado volume de crimes e fraudes nos meios eletrônicos, a segurança da informação se constitui atualmente como fator de sucesso na busca de novos clientes e na gestão do relacionamento. A percepção de que a *web* pode ser utilizada como instrumento de melhoria do relacionamento já é bastante presente, mas para isso os componentes básicos de segurança devem estar em evidência.

Os serviços financeiros têm um componente de intangibilidade que faz com que a apreciação do serviço dependa muito da relação que se estabelece com o cliente (GALLEGO, 1998). Pode-se dizer que a grande vantagem que os bancos devem explorar

em relação aos seus concorrentes será a confiança, através de recursos de segurança e relacionamento.

6.4 Fidelização

Grande parte dos serviços oferecidos pelas agências bancárias já estão disponíveis nos bancos eletrônicos. Existem exceções, por questões estratégicas e principalmente de segurança. A promoção e estímulo ao uso dos bancos eletrônicos é constante, buscando a fidelização dos clientes com um serviço de qualidade e seguro além de benefícios em taxas de serviços.

Uma transferência interbancária de até cinco mil reais, por exemplo, pode ter taxas até 60% menores pela Internet, e consultas, como saldos e extratos, tem custo zero (FACCHINATO, 2005). Entre os principais objetivos da indústria financeira estão a fidelização e a oferta de serviços diferenciados, como pagamentos, transferências, compras, pagamento de tributos, cartões, empréstimos, financiamentos e investimentos pela *web*. De acordo com Facchinato (2005), a Internet já compete com as agências principalmente em horários de expediente bancário, deixando ainda mais visível a mudança de hábitos e de fidelização. Grande parte dos acessos ocorre entre 8h e 12h e próximo às 18h, evidenciando o uso dos bancos eletrônicos no horário de trabalho dos usuários.

Uma das maiores exigências em relação à fidelidade diz respeito à transação eletrônica segura e à disponibilidade do canal. São pontos básicos priorizados pelos bancos, que buscam a migração para transações através da Internet e a manutenção dos usuários do canal (ABNT NBR ISO/IEC 27001)

6.5 Limites de Transações

As ferramentas de segurança mais sofisticadas, com níveis de segurança superiores, são cada vez mais utilizadas para disponibilizar limites de transações maiores em Internet Bankings. Infelizmente os valores de aquisição e, principalmente, a complexidade de implementação e logística, limitam a utilização de recursos de segurança como *tokens* e certificados digitais de forma massificada. Mesmo não sendo fatores de autenticação utilizados em larga escala, estas ferramentas vem potencializando o uso do canal para transações com valores vultuosos, o que é vital para clientes pessoas jurídicas. A estratégia mais utilizada pelos bancos brasileiros é disponibilizar estas soluções de autenticação forte para clientes potenciais, que necessitam transacionar valores diferenciados.

Já os dispositivos de segurança (blindagem, *browser defense*, etc.) e as tabelas de senhas (*tan list,* token de papel, etc.), com custo e implementação mais acessíveis para grandes números de usuários, estão sendo disponibilizados para todos clientes de algumas instituições financeiras do País, e também limitando os limites de transações para aqueles que os utilizam. Em alguns bancos, a instalação do *plugin* dos dispositivos de segurança é item obrigatório para transacionar em Internet Banking.

6.6 Comodidade e Segurança Pessoal

Não há dúvidas que o principal apelo do Internet Banking é a comodidade (DINIZ, 1998). Não depender de filas e de horários é o principal objetivo dos clientes que migram para meios eletrônicos. A grande maioria só necessita se deslocar para movimentações

físicas de dinheiro ou cheques. Estatísticas apontam em mais de 50% o total de consumidores que escolhem o banco para trabalhar de acordo com os serviços *on-line* disponíveis. A localização física e a quantidade de ATM's já não é fator determinante para a escolha de grande parte do público alvo destas instituições.

Para os clientes habituados com pagamentos em meios físicos, a sensação de insegurança no mundo virtual é o primeiro obstáculo. Será que alguém não terá como obter minhas informações privadas, como CPF, dados bancários e senhas? A resposta é positiva, como já mencionado na abordagem sobre crimes na Internet. E alguns dos fatores de segurança fundamentais dependem dos próprios usuários. Porém, aqueles que já estão com percepção apurada em relação à segurança na *web*, e tomam as medidas necessárias para sua proteção no mundo virtual, tem escolhido o Internet Banking também devido à segurança pessoal, além da comodidade. Com os altos índices de violência nos grandes centros urbanos e até mesmo em algumas cidades do interior, muitas pessoas sentem-se mais seguras ao acessar seu banco de dentro de suas casas ou empresas, em detrimento ao deslocamento até uma agência bancária.

7. Método de Trabalho

A pesquisa elaborada neste trabalho é de caráter exploratório e descritivo, pois objetiva ampliar o conhecimento sobre o problema a ser elucidado pelo pesquisador (MALHOTRA, 2006). Neste trabalho está sendo buscado conhecimento sobre o nível de satisfação de usuários de Internet Banking em relação às funcionalidades e segurança disponibilizadas no banco eletrônico da instituição a qual são clientes. Este método é especialmente útil quando o pesquisador não detém uma idéia clara dos problemas que vai enfrentar durante o trabalho, oferecendo técnicas para desenvolver conceitos, estabelecer prioridades e obter definições operacionais que contribuam para a elaboração do resultado final do trabalho (COOPER; SCHINDLER, 2003).

A coleta de dados foi realizada por meio de questionário aplicado inicialmente com a presença do pesquisador e, após alguns ajustes, enviado por e-mail para uma série de profissionais da universidade onde o trabalho foi desenvolvido e de empresas conhecidas pelos pesquisadores. De acordo com Gil (1999), o questionário é definido como uma técnica de investigação composta por um número de questões considerável, apresentadas por escrito aos respondentes e com objetivos de obter o conhecimento de opiniões, crenças, sentimentos, interesses, expectativas e situações vivenciadas. Portanto, a construção do questionário consiste basicamente em traduzir os objetivos da pesquisa em questões especificas (GIL, 1999).

A estrutura do questionário foi desenvolvida com base em proposta apresentada por Cooper e Schindler (2003), a qual sugere a presença de três tipos de questões de mensuração: (i) Gerenciais, de (ii) Classificação e de (iii) Direcionamento. As questões (i) Gerenciais compõem a primeira parte do instrumento de pesquisa e identificam dados cadastrais do entrevistado, tais como idade, profissão, grau de escolaridade e banco com que trabalha. As questões de (ii) Classificação identificam características da satisfação em relação ao canal de Internet Banking com que operam e a segurança oferecida. As questões de (III) Direcionamento compõem o aprofundamento da análise anterior, buscando explicações para os resultados obtidos nas questões de Classificação. As análises dos resultados apresentados no item a seguir permitem identificar as questões que compõem o instrumento de pesquisa desenvolvido neste trabalho.

Para esta pesquisa foi utilizada uma amostra por acessibilidade de oitenta pessoas, todas usuárias freqüentes de Internet Banking, representando uma população com diferentes características profissionais e níveis de escolaridade. Para Gil (1999), a amostragem por acessibilidade é o método mais flexível e pode ser aplicado em estudos exploratórios, quantitativos ou qualitativos, onde não é requerido elevado nível de precisão na análise dos resultados.

8. Análise de Resultados

Conforme a estrutura do questionário, a análise dos resultados apresenta (i) aspectos referentes ao perfil dos respondentes, (ii) diagnóstico da satisfação dos clientes com as funcionalidades dos recursos de segurança do Internet Banking do qual o respondente é usuário e, (iii) aprofundamento dos motivos apresentados para as respostas do item anterior.

8.1 Perfil Sócio Demográfico dos Entrevistados

As análises apresentadas a seguir indicam resultados da pesquisa em relação a faixa etária dos entrevistados (Fig. 1), nível de escolaridade (Fig. 2), área de atuação (Fig. 3) e tempo de experiência profissional (Fig. 4).

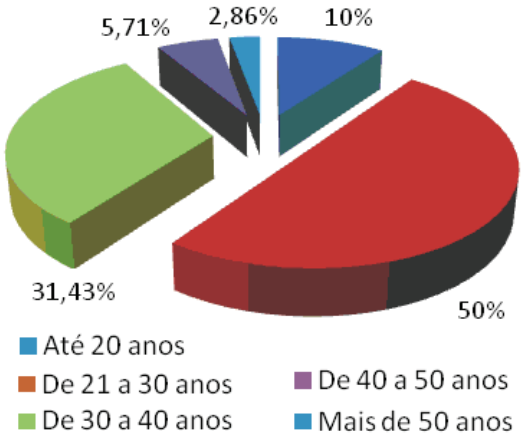

Fig. 1 - Idade dos Respondentes

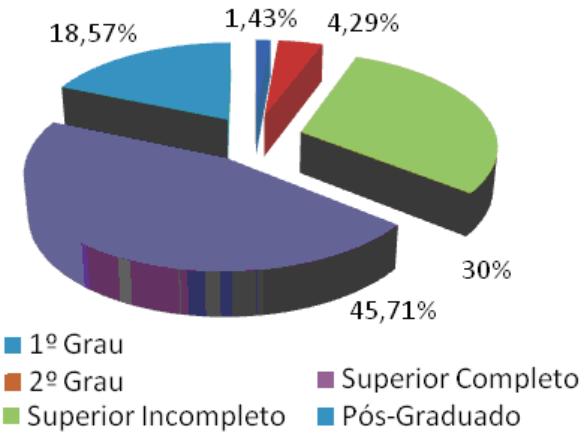

Fig. 2 - Nível de Escolaridade

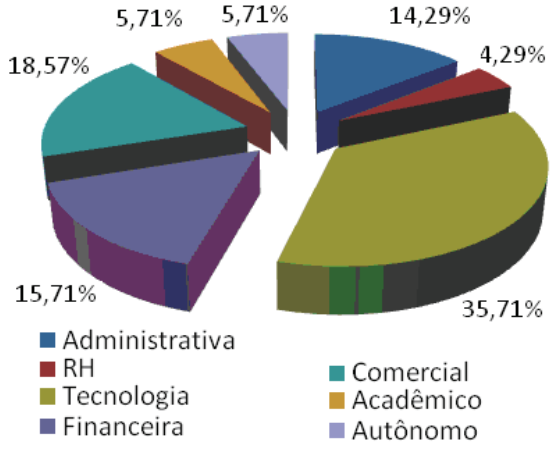

Fig. 3 - Área de Atuação Profissional

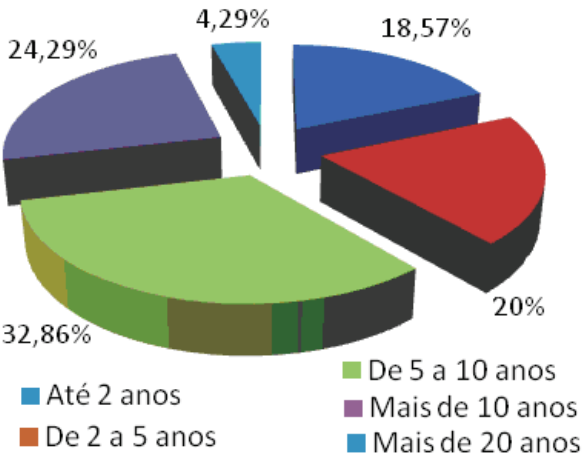

Fig. 4 - Tempo de Experiência Profissional

8.2 Percepção com o Uso de Internet Banking

O grau de satisfação com as funcionalidades disponíveis em um banco eletrônico está intimamente ligado com os recursos de segurança disponibilizados pela instituição. Um Internet Banking contempla determinados tipos de operações e transações bancárias, de acordo com os níveis de proteção agregados ao canal. Na Figura 5, observa-se o índice de satisfação dos respondentes, quanto às funcionalidades disponíveis no canal da instituição que são clientes. Percebe-se que uma parcela considerável dos usuários está satisfeita ou muito satisfeita com as operações que podem realizar através de seu banco eletrônico. Dos 70 respondentes usuários do seu banco pela Internet, 33 (47,14%) apresentam-se satisfeitos e 21 (30%) muito satisfeitos neste critério de avaliação.

Em relação à disponibilidade, conforme a figura 6, 44,29% dos respondentes se consideram satisfeitos com os índices de assertividade dos bancos neste critério de avaliação. O percentual de usuários muito satisfeitos é de 32,86% do total. Aspectos como comodidade, segurança pessoal e agilidade para concretizar negócios financeiros também foram comentados pelos respondentes, pois padrões de disponibilidade e acessibilidade são fundamentais para credibilidade e uso efetivo do Internet Banking. Conseqüentemente os índices de insatisfação podem ser considerados baixos, com 4,29% de clientes insatisfeitos e apenas 1,43% muito insatisfeitos. Entre as pessoas neutras, encontram-se 9 respondentes, representando 12,86% da amostra da população analisada e 4,29% (3 pessoas) não tem opinião formada sobre o assunto.

Controles são geradores de dificuldades em processos de autenticação e autorização, que são vitais para a segurança de uma transação. Desta forma, recursos para autenticação em canais impactam diretamente na agilidade de uma operação. Na Figura 7 são apresentados os níveis de satisfação com a facilidade para efetuar transações. Em relação à facilidade para efetuar transações, 38,57% dos clientes entrevistados que utilizam o Internet Banking estão satisfeitos com os processos para que se concretizem suas transações financeiras. Em seguida um percentual de 28,57% de usuários muito satisfeitos. Os totais de 5,71% de usuários indiferentes e sem opinião formada, respectivamente, demonstra uma falta de percepção em relação à necessidade de um processo de autenticação seguro de uma amostra considerável. Somam-se a estes, àqueles insatisfeitos e muito insatisfeitos com estes procedimentos (12,86% e 8,57%). A probabilidade de que desconheçam a necessidade de processos seguros de autenticação é grande, ou seja, ameaças no ambiente *web* é assunto que provavelmente não está entre suas preocupações.

A ocorrência de fraudes no período, verificação de vulnerabilidades no ambiente e ausência de algum dispositivo de segurança são exemplos de limitadores comuns em operações *on-line* e transações eletrônicas. E também são fatores que impactam diretamente na satisfação dos usuários, conforme avaliação demonstrada na Figura 8.

A figura 9 apresenta resultados de um item avalia o sentimento em relação ao nível de proteção percebido ao utilizar o banco eletrônico e, de acordo com as respostas recebidas, os respondentes usuários em sua maioria estão com percepção positiva, com 65,71% dos entrevistados satisfeitos e 20% muito satisfeitos neste critério de avaliação. Outra avaliação positiva diz respeito ao número de pessoas sem opinião formada, com 1,43% e indiferentes com 4,29% do total. Estes números demonstram que grande parcela de usuários considera os aspectos de segurança, seja de forma positiva ou negativa. No mesmo sentido, apenas 5,71% dos usuários não estão satisfeitos e 2,86% estão muito insatisfeitos com a percepção de segurança em transações de seu banco eletrônico.

Mesmo que se sintam seguros em acessar e realizar operações pela *web*, alguns usuários ainda desconhecem, ou não percebem os recursos disponíveis para segurança no *site*. Esta percepção é detalhada na Figura 10. Verifica-se este comportamento nesta análise

de percepção com os dispositivos de segurança disponíveis. Um percentual de 50% dos respondentes que utilizam Internet Banking, percebe e está satisfeito com as ferramentas de segurança implantadas no seu Internet Banking, enquanto 17,14% sentem-se muito satisfeitos com os recursos de segurança que utilizam. Em proporções menores, mais que devem ser consideradas, 11,43% dos respondentes encontram-se insatisfeitos e 7,14% muito insatisfeitos com a percepção de proteção com os estes dispositivos. Um total de 14,28% dos usuários ativos desconhece com maior propriedade a segurança destes *sites*. É o que se conclui com os percentuais de 5,71% de usuários indiferentes e 8,57% sem opinião formada sobre este critério de avaliação.

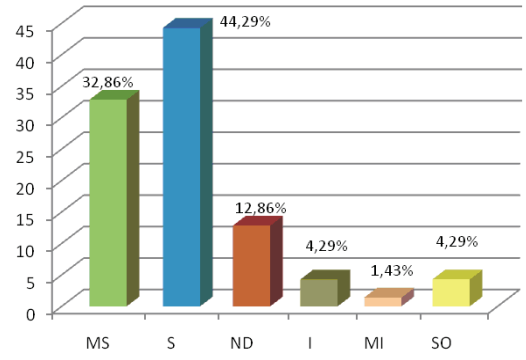

Fig. 5 – Funcionalidades Disponíveis

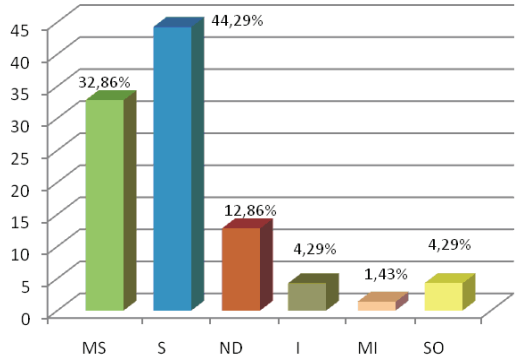

Fig. 6 – Disponibilidade de Acesso

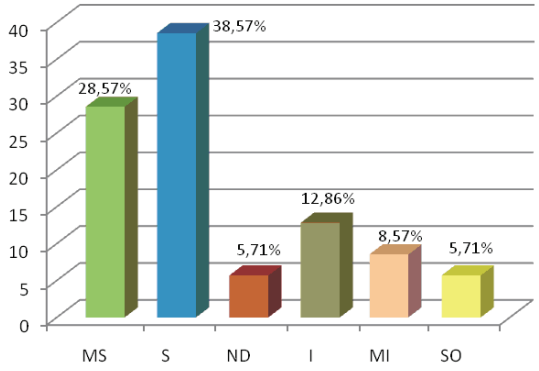

Fig. 7 – Facilidade para Efetuar Transações

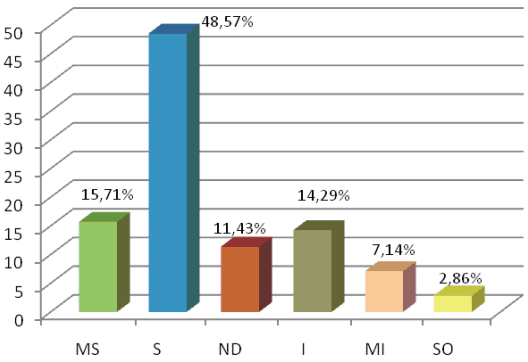

Fig. 8 – Limites de Transações

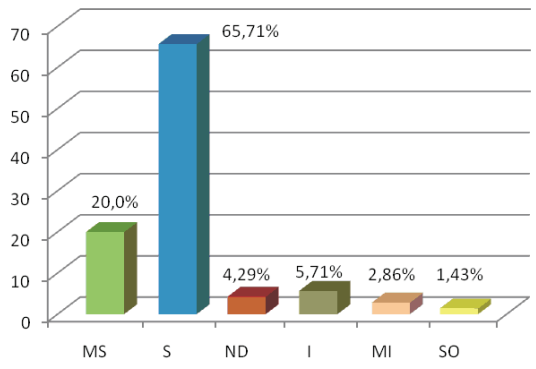

Fig. 9 – Segurança nas Transações

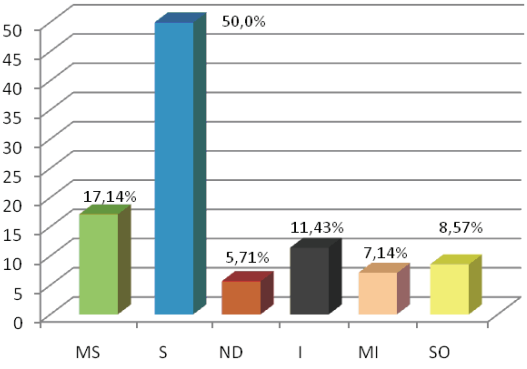

Fig. 10 – Proteção com dispositivos de segurança

9. Conclusões

Não é novidade que o Internet Banking é uma realidade no cenário internacional e oferece benefícios tanto para as instituições financeiras quanto para seus clientes. A fundamentação teórica demonstrou um pouco destes benefícios, a exigência de confiabilidade, e que a segurança das informações deve ser preocupação constante, direcionando esforços e investimentos permanentes.

De acordo com os resultados de pesquisa, o nível de satisfação com relação às facilidades no canal Internet Banking é satisfatório para grande maioria dos clientes. As possíveis variáveis de influência negativa sobre o uso do canal, com destaque para níveis de disponibilidade, limites de transações e a própria segurança, não estão impactando na satisfação dos usuários e os motivando a realizar operações em agências.

Cabe destacar que a definição de processos em canais eletrônicos, investimentos e recursos de segurança possibilitam novos negócios e oportunidades, cuja credibilidade e utilização em larga escala também dependem da segurança e percepção de proteção com o banco eletrônico. As necessidades e exigências dos clientes bancários ao migrarem para transações pela Internet estão associadas com a segurança, mesmo que muitos usuários ainda não tenham essa percepção, associando mais claramente as vantagens com a comodidade.

10. Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 17799:2005. Tecnologia da Informação – Técnicas de Segurança – Código e prática para a gestão da Segurança da Informação**. Rio de Janeiro: ABNT, 2005.

BALARINE, Oscar. **Tecnologia da informação como vantagem competitiva.** RAE Eletrônica. São Paulo: 2002.

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

BREI, Vinícius Andrade. **Antecedentes e conseqüências da confiança do consumidor final em trocas relacionais com empresas de serviço: um estudo com o usuário de Internet Banking no Brasil.** Universidade Federal do Rio Grande do Sul, 2001.

BINOTTO, Renata. **Internet nas organizações financeiras: da propagação no Brasil às novas tendências bancárias**. Universidade de São Paulo: 2001.

CERT.br. **Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil.** Disponível em www.cert.br.

COOPER, D.; SCHINDLER, P. Método de Pesquisa em Administração. 7.ed. Porto Alegre: Bookman, 2003.

DIAS, Cláudia. **Segurança e Auditoria da Tecnologia da Informação**. Rio de Janeiro: Axcel Books, 2003.

DINIZ, Eduardo. **Evolução do uso da web pelos bancos.** Disponível em http://www.anpad.org.br/evento.php?acao=subsecao&cod_edicao_subsecao=136&cod_evento_edicao=3

DONNELLY, Jr. **Marketing intermediaries in channels of distribution for services. Journal of Marketing.** V.40, n.1, 1976.

FACCHINATO, Alexandre.**Trabalho Integrado: Internet Banking Unibanco**. São Paulo, 2005.

FEBRABAN. **Federação Brasileira de Bancos**. Disponível em www.febragan.org.br

GALLEGO, Norberto. **La banca en Internet : a hora empieza el despliegue.** Disponível em www.idg.es/iworld/199810/articulos/banca.asp. 1998.

GIL, A. C.. **Métodos e Técnicas de Pesquisa Social.** São Paulo: Atlas, 1999.

MALHOTRA, N. Pesquisa em Marketing: uma orientação aplicada. 4.ed. Porto Alegre: Bookman, 2006.

MITNICK, Kevin; SIMON, William. **A arte de enganar. Ataques de hackers: controlando o fator humano na segurança da informação.** São Paulo: Makron, 2003.

MÓDULO SECURITY OFFICER. Módulo. Rio de Janeiro, 2005.

NAVARRO, Luis. **Information security risks and managed security services.** Information Security Technical Report. v.6, n.3, 2001.

O'BRIEN, James. **Sistemas de informação e as decisões gerenciais na era da Internet.** São Paulo: Saraiva, 2004.

O'REILLY & ASSOCIATES. **Building Internet Firewalls** Chapman. 1998

SÊMOLA, Marcos. **Gestão da segurança da informação – Uma visão executiva.** São Paulo: Campus, 2003.

STERN, Louis *et al*. **Marketing Channels.** Prentice-Hall: Ed. Englewood Cliffs, 1996.

TURBAN, Efraim; MCLEAN, Ephraim; WETHERBE, James. **Tecnologia da informação para gestão.** Porto Alegre: Bookman, 2002

WILLIAMS, P. **Information security governance. Information security technical report.** v.6, n.3, 2001.