UNIVERSIDADE DE SÃO PAULO
ESCOLA DE ENGENHARIA DE SÃO CARLOS

ANDRÉ LUIS DAMIANO

**AS FRAUDES NO INTERNET BANKING
E SUA EVOLUÇÃO PARA O SOCIAL BANKING**

São Carlos
2013

ANDRÉ LUIS DAMIANO

**AS FRAUDES NO INTERNET BANKING
E SUA EVOLUÇÃO PARA O SOCIAL BANKING**

Dissertação apresentada à Escola de Engenharia de São Carlos da Universidade de São Paulo para obtenção do título de Mestre em Engenharia de Produção.

Área de Concentração: Economia, Organizações e Gestão do Conhecimento

Orientador: Prof. Dr. Edson Walmir Cazarini

São Carlos
2013

AUTORIZO A REPRODUÇÃO TOTAL OU PARCIAL DESTE TRABALHO,
POR QUALQUER MEIO CONVENCIONAL OU ELETRÔNICO, PARA FINS
DE ESTUDO E PESQUISA, DESDE QUE CITADA A FONTE.

D158a Damiano, André Luis
AS FRAUDES NO INTERNET BANKING E SUA EVOLUÇÃO PARA
O SOCIAL BANKING / André Luis Damiano; orientador Edson
Walmir Cazarini. São Carlos, 2013.

Dissertação (Mestrado) - Programa de Pós-Graduação
em Engenharia de Produção e Área de Concentração em
Economia, Organizações e Gestão Conhecimento -- Escola
de Engenharia de São Carlos da Universidade de São
Paulo, 2013.

1. Fraudes Eletrônicas. 2. Social Business. 3.
Redes Sociais. 4. Marketing Digital. 5. Bancos. 6.
Internet Banking. 7. Social Banking. I. Título.

Aos meus Pais, os quais foram os grandes incentivadores dos meus estudos, para a busca do conhecimento como forma de progresso moral, pessoal e profissional.

À minha querida esposa Renata que me estimulou e me incentivou a realizar essa pesquisa e nunca desistir dos meus sonhos.

Aos meus irmãos pelo amor e carinho que sempre tiveram por mim.

FOLHA DE JULGAMENTO

Candidato: Tecnólogo **ANDRÉ LUÍS DAMIANO**.

Título da dissertação: "As fraudes no *internet banking* e sua evolução para o *social banking*".

Data da defesa: 28/06/2013

Comissão Julgadora:

Prof. Dr. **Edson Walmir Cazarini** (Orientador)
(Escola de Engenharia de São Carlos/EESC)

Prof. Dr. **Milton Vieira Junior**
(Universidade Nove de Julho/UNINOVE)

Dr. **Nelson Marinelli Filho**
(KWB5 Social Learning)

Resultado:

Aprovado

APROVADO.

APROVADO

Coordenador do Programa de Pós-Graduação em Engenharia de Produção:
Prof. Titular **Henrique Rozenfeld**

Presidente da Comissão de Pós-Graduação:
Prof. Titular **Denis Vinicius Coury**

AGRADECIMENTOS

Ao Professor Dr. Edson Walmir Cazarini que me aceitou como orientando, sendo sempre muito paciente e acolhedor, contribuindo para o meu crescimento e aperfeiçoamento acadêmico.

Ao amigo Marcos Pelliciari pelo companheirismo, otimismo e trabalho em equipe principalmente no início dos trabalhos.

Ao amigo Márcio Campos pelo aprendizado e pelas valiosas e relevantes contribuições para o aprimoramento pessoal e acadêmico.

À amiga Virgínia Perez pela dedicação, eficiência e contribuição durante a etapa de pesquisa e formatação do trabalho.

*“A mente que se abre a uma nova idéia
jamais voltará ao seu tamanho original.”*

Albert Einstein

RESUMO

DAMIANO, A. L. **As fraudes no Internet Banking e sua evolução para o Social Banking**. 2013. 119p. Dissertação (Mestrado em Engenharia de Produção) - Escola de Engenharia de São Carlos, Universidade de São Paulo, São Carlos, 2013.

A tecnologia da informação e comunicação é um fator importante no desenvolvimento futuro da indústria de serviços financeiros, com especial atenção ao setor bancário. A maioria dos bancos utiliza a Internet como um canal estratégico de distribuição onde seus serviços e produtos possuem uma relação muito próxima com o conceito mais amplo possível de marketing, aquele que descreve plenamente um ambiente e um nicho de negócio e onde o desenvolvimento e evolução deste canal associa-se diretamente a própria evolução do marketing em si. O tema central deste trabalho é apresentar uma revisão bibliográfica sobre o canal Internet Banking analisando as principais questões e desafios referentes às fraudes eletrônicas e suas ameaças, além de descrever o impacto das mídias sociais que estão ocasionando dentro das corporações. Realiza-se também um paralelo de como os serviços e produtos bancários acompanharam de perto a evolução do marketing e como, hoje, neste momento de transição de um paradigma econômico para outro, estes dois modelos se relacionam em um ponto específico: a tendência das fraudes no ambiente de Internet Banking e sua evolução para o *Social Banking*. Analisam-se também quais caminhos serão abertos dentro do novo paradigma de economia e marketing sociais para este tipo de ocorrência. Para atenuar de forma eficaz o risco de fraude, é importante implementar um amplo programa decisório para prevenção, que se estenda além de um conjunto de controles internos sofisticados em todos os níveis e divisões de uma organização. Finalmente, a conclusão e perspectivas futuras da evolução do Internet Banking para o *Social Banking* com uma análise da evolução das ameaças e fraudes eletrônicas neste novo canal.

Palavras-chave: Fraudes Eletrônicas. Internet Banking. Bancos. Marketing Digital. Redes Sociais. Social Business. Social Banking.

ABSTRACT

DAMIANO, A. L. **Internet Banking fraud and its trends to Social Banking** 2013. 119p. Dissertação (Mestrado em Engenharia de Produção) - Escola de Engenharia de São Carlos, Universidade de São Paulo, São Carlos, 2013.

Information technology and communication is an important factor in the future development of the financial services industry, with particular attention to the banking sector. Most banks use the Internet as a strategic distribution channel where its services and products have a very close relationship with the broader concept of marketing, one that fully describes an environment and a niche business and where the development and evolution of this channel is directly associated with the evolution of the marketing itself. The central theme of this work is to present a literature review on the Internet Banking channel analyzing key issues and challenges related to electronic fraud and threats, and describes the impact of social media is causing in corporations. Additionally to the threats on the Internet Banking, this work brings an analyze of how the banking products and services are closely followed by the marketing evolution and how at this moment of transition from a economic perspective to another, these two business models are co-related to a specific aspect: The future and trends of the electronic fraud on the Internet Banking towards the evolution to the Social Banking. It also analyzes which paths will also open within the new paradigm of economics and social marketing for this type of occurrence. To effectively mitigate the risk of fraud, it is important to implement a comprehensive decision-making prevention program that extends beyond a sophisticated set of internal controls at all levels and divisions of an organization. Finally, the conclusion and future prospects of the development of Internet Banking for Social Banking with an analysis of the evolution of electronic fraud and threats in this new channel.

Keywords: Internet Banking Fraud. Electronic Fraud. Internet Banking Evolution. Social Marketing. Banking. Social Network. Social Business. Social Media.

LISTA DE SIGLAS E ABREVIATURAS

B2C	<i>Business to Consumer</i>
CAPTCHA	<i>Completely Automated Public Turing test to tell Computers and Humans Apart</i>
CERT.BR	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil
CMS	<i>Content Management Systems</i>
CRM	<i>Customer Relationship Management</i>
DoS	<i>Denial of Service</i>
FEBRABAN	Federação Brasileira de Bancos
IP	<i>Internet Protocol</i>
IRC	<i>Internet Relay Chat</i>
MITM	<i>Man in the Middle</i>
OTP	<i>One Time Password</i>
SMS	<i>Short Message Service</i>
TIC	Tecnologia da Informação e Comunicação
URL	<i>Uniform Resource Locator</i>
WoM	<i>Word of Mouth</i>

LISTA DE GRÁFICOS

Gráfico 1 – Pirâmide de Classificação Econômica, 2006-2010	18
--	----

LISTA DE TABELAS

Tabela 1 - Totais mensais classificados por quantidade de fraudes	23
Tabela 2 - Modelos atuais de segurança adotados pelos bancos brasileiros	41
Tabela 3 - Tipos de crimes mais comuns na Internet	43

LISTA DE FIGURAS

Figura 1 - Total de incidentes anuais reportados de 1999 a 2012	22
Figura 2 - Distribuição dos tipos de tentativas de fraudes reportadas nos anos de 2010 e 2011	23
Figura 3 - Linha do tempo da automação bancária no Brasil	31
Figura 4 - O Marketing, segundo o Marketing Capabilities Wheel	63
Figura 5 - A sobreposição do Social Marketing e do Social Business	65
Figura 6 - O Ágora Virtual e a configuração do Mundo Social.	70
Figura 7 - A configuração do Mundo Social.	71
Figura 8 - Representação da visão de Anderson (2001) sobre a presença social	75
Figura 9 - Social LUMAscape.....	78
Figura 10 - Social LUMAscape (KAWAJA, 2012) modificado para melhor entendimento do tema	79
Figura 11 - Conversation Prism de Solis e Thomas (2012).....	80
Figura 12 - Sobreposição do prisma de conversação de Solis e Thomas (2012)	81
Figura 13 - Grau de avaliação social de um negócio.....	83
Figura 14 - Análise dos dados do Banco 1	86
Figura 15 - Análise dos dados do Banco 2	87
Figura 16 - Análise dos dados do Banco 3	88
Figura 17 - Análise dos dados do Banco 4	89

SUMÁRIO

1 INTRODUÇÃO	13
1.1 Contextualização e Justificativa	14
1.2 Formulação do Problema da Pesquisa	16
1.3 Objetivo da Pesquisa	16
1.4 Relevância da Pesquisa.....	17
1.5 Motivação	24
1.6 Estrutura do Trabalho	25
2 MÉTODO DE PESQUISA	27
2.1 Caracterização Geral da Pesquisa.....	27
2.2 Etapas da Pesquisa.....	27
2.3 Procedimentos Metodológicos	28
3 FUNDAMENTAÇÃO TEÓRICA.....	29
3.1 O Papel da Tecnologia da Informação no Setor Bancário.....	29
3.2 Fases da Automação Bancária no Brasil	31
3.3 Integração e Segurança do Internet Banking.....	33
3.4 A Evolução das Fraudes no Ambiente do Internet Banking	34
3.5 Modelos Atuais de Segurança Adotados pelos Bancos Brasileiros	40
3.6 Estratégias de Ataques.....	42
3.7 Identificando as Ameaças, Meios, Métodos e Ferramentas	44
3.7.1 Ameaças sob o Ponto de Vista de Segurança da Informação	46
3.7.2 Meios de Propagação.....	46
3.7.3 Métodos e Ferramentas.....	48
3.7.4 Ferramentas Utilizadas para os Ataques.....	52
3.8 Riscos Associados aos Bancos	55
3.8.1 Gerenciamento de Riscos	55
3.8.2 Gerenciamento de Risco no Internet Banking.....	57
3.9 Redes Sociais.....	58
3.9.1 Sociedade em Redes	58
3.9.2 WEB 2.0 e o Universo dos Espaços Virtuais	60
3.9.3 O Impacto das Tecnologias da Informação e Comunicação Sobre o Marketing	62
3.9.4 O Impacto das Redes Sociais nas Organizações	66
3.9.5 A Estrutura do Social World e o Social Business	69

3.9.6 Presença Social	73
4 RESULTADOS.....	77
4.1 Modelo de Presença Social Proposto pela Pesquisa	77
4.2 Interpretação do Modelo de Presença Social	83
4.3 Levantamento e Análise dos Dados	84
5 CONSIDERAÇÕES FINAIS	91
REFERÊNCIAS	95

1 INTRODUÇÃO

Vive-se hoje em um mundo globalizado, tecnológico e em constante evolução. Uma parte do que está em evolução constante são os serviços financeiros disponibilizados pelos bancos em formato de Internet Banking. Este tipo de serviço é muito conveniente e de fácil acesso atualmente.

A constante migração e evolução das agências tradicionais para as puramente digitais, juntamente com as necessidades de redução de custos, estão levando os bancos a adotarem cada vez mais serviços online. De acordo com Ramos e Costa (2000, p. 139) “as organizações buscam a hegemonia da tecnologia, oferecendo cada vez mais serviços acessíveis, de qualidade superior e de custo baixo”. Desta maneira, presencia-se uma evolução na maneira de realizar transações bancárias, saindo de uma estrutura de agência de relacionamento físico com o cliente para uma voltada ao autoatendimento eletrônico.

Para Ramos e Costa (2000, p. 139) esse processo evolutivo “enriquece a produtividade das tarefas dos escriturários em serviços e contribui para alcançar ganhos de escala pela padronização e técnicas de produção em massa”. Essa transição no modelo de negócio entre o tradicional para o digital é viabilizado e compreendido como canais alternativos ou eletrônicos.

Diante deste novo cenário evolutivo, presencia-se um aumento nos riscos principalmente os associados às fraudes nestes canais, abrindo espaço para as ameaças e tentativas de invasão pelo lado do banco ou do cliente. Adachi (2004) reforça que os riscos enfrentados pelos bancos no mundo físico, se reproduzem no ambiente virtual, cenário das fraudes e crimes financeiros. Já Nakamura e Geus (2002) mencionam que a proteção dos ativos (informações) é de relevância e importância para o sucesso e sobrevivência das organizações onde falhas podem ocasionar perdas e impactos negativos ao negócio e imagem da instituição, gerando prejuízos financeiros.

Observado esse cenário e a evolução das transações financeiras no canal eletrônico, surge a necessidade de se estruturar meios e mecanismos de segurança para combater tais ameaças sob o ponto de vista do cliente e do próprio banco. A economia de escala e modelo ágil de distribuição e realizações de serviços financeiros envolvendo principalmente pagamentos e transferências que a Internet e seus usuários conectados constituem serve também para a prática de atos ilícitos.

Tais atitudes na gestão efetiva das fraudes financeiras tornaram-se mundialmente conhecidas por meio de escândalos no mundo dos negócios, quando executivos de grandes

empresas de classe global afirmaram o desconhecimento de atitudes duvidosas realizadas por suas empresas. Essa situação ocasionou uma série de incertezas nos resultados dos balanços apresentados pelas empresas, colocando em xeque sua capacidade de governança corporativa e transparência ao mercado.

Esse abalo econômico aconteceu na década de noventa quando foram descobertas fraudes nos resultados financeiros de algumas grandes corporações americanas que operavam suas ações na NYSE¹ e NASDAQ² (BORGERTH, 2007). Esse fato desencadeou a criação da lei Sarbanes-Oxley (SOX), assinada em 2002, que por sua vez iniciou o desenvolvimento de uma cultura de regulamentação e monitoramento mais apurados da integridade das informações das empresas, obrigando-as a constituírem controles e processos mais transparentes no fornecimento de informações ao mercado, sujeito a severas punições dos controladores das empresas.

O objetivo atribuído à sua criação foi de restabelecer a confiança do mercado nas empresas e adotar padrões éticos no tratamento das informações financeiras e seu respectivo direcionamento aos investidores (BORGERTH, 2007). O impacto na implementação dos controles afetou também a área de tecnologia da informação, exigindo-se que todos os registros, controles e autorizações fossem sistêmicos e auditáveis segundo Kaarst-Brown e Kelly (2005).

Segundo Defond e Francis (2005), além dos rígidos parâmetros legais impostos às empresas com ações negociadas nas bolsas americanas, seu conjunto de regras busca garantir:

- A criação de mecanismos confiáveis de auditoria;
- A criação de comitês para supervisionar suas atividades e assegurar maior independência na atuação da auditoria externa, de modo a mitigar riscos aos negócios e evitar fraudes;
- Garantir a transparência dos resultados contábeis das companhias.

Inclui também políticas de retenção de informações por tempo determinado e sua destruição após essa validade (BEQUAI, 2003; ANISINGARAJU, 2003).

1.1 Contextualização e Justificativa

A evolução da Internet é uma das maiores inovações do século XX e tem mudado a

¹ NYSE: New York Stock Exchange (Bolsa de Valores de Nova Iorque)

² NASDAQ: National Association of Securities Dealers Automated Quotations (Associação Nacional Corretora de Valores e Cotações Automatizadas)

vida de indivíduos e organizações empresariais. Compartilhamento de informações, colaboração, e-commerce e comunicações unificadas são alguns dos principais benefícios deste uso. Tendências como a globalização, maior produtividade, distribuição e redução de custos tornam as organizações cada vez mais dependentes dos seus sistemas de informação e dos serviços da Internet. Possíveis ataques em sistemas de informação e eventuais acidentes podem causar grandes perdas de informações, serviços e operações de negócios (BOJANC; JERMAN-BLAZIC, 2008).

Na visão de Langheinrich e Karjoth (2011) adicionalmente ao fenômeno de utilização dos serviços bancários por meio da Internet surge a utilização das mídias sociais como meio de crescimento e interação online, de comportamento exponencial, entre grupos de usuários e empresas.

A Web 2.0 tem transformado o modo de vida e trabalho das pessoas e organizações. As corporações têm percebido de maneira positiva sua utilização no relacionamento com seus colaboradores, aumento e retenção da base de clientes, geração de novos nichos de negócios e facilidade de transferência de conhecimento dentro da própria empresa. No entanto, se planejado e gerenciado de forma errada, podem também destruir rapidamente sua imagem, ocasionando perdas financeiras, de fatia de mercado, produtividade, vazamento de informações e impactando o relacionamento com clientes e parceiros. Usuários ansiosos e/ou sem a devida orientação quanto à confidencialidade das informações também podem divulgar dados e informações internas confidenciais para concorrentes ou para o público em geral (LI, 2010).

Em julho de 2010, o Facebook possuía ao menos meio bilhão de usuários (OSTROW, 2010), alguns milhões a mais do que a soma da população de todos os vinte e sete estados membros da União Europeia. Só nos Estados Unidos, a base de usuários do Facebook, em um período de vinte e quatro meses, cresceu mais de 350% passando de 27 milhões de usuários em julho de 2008 para mais de 125 milhões em julho de 2010 (BURCHER, 2010), representando 40% da população do país.

Todas essas mudanças fez surgir o Social Banking que pode ser entendido como a união do Internet Banking com as mídias sociais.

Embora tenha já sido escrito muito sobre os benefícios e os riscos das redes sociais para os indivíduos (BILGE et al., 2009; BOYD, 2006; ELLISON; STEINFELD; LAMPE, 2006; FOGEL; NEHMAD, 2009), sua generalizada utilização afeta cada vez mais as empresas e instituições públicas. Alinhado aos objetivos deste trabalho, o crescente aumento na utilização desses canais sociais podem viabilizar novos vetores de ataques para

fraudadores, aumentando significativamente a exposição da empresa para o risco de fraudes.

1.2 Formulação do Problema da Pesquisa

Fundamentado em uma análise e reflexão sobre as fraudes no ambiente do Internet Banking, o problema de pesquisa pode ser descrito por meio da seguinte pergunta: Com base na crescente participação dos recursos da Internet na vida diária das pessoas, empresas e organizações, quais serão as principais tendências, ou adjacentes possíveis, para a evolução dos métodos de prevenção das fraudes eletrônicas no processo de transição do Internet Banking para o Social Banking?

1.3 Objetivo da Pesquisa

O objetivo principal desta pesquisa é propor um modelo de avaliação de presença social para servir como auxílio nas estratégias de prevenção às fraudes eletrônicas em bancos. O modelo é desenvolvido com o propósito de que os bancos possam iniciar um processo maior de aderência e presença nas redes e mídias sociais dentro de um contexto de estudo específico.

Este objetivo é desdobrado nos seguintes objetivos secundários:

- Identificar e ordenar os elementos que formam os problemas existentes no Internet Banking, suas ameaças, riscos e medidas preventivas adotadas pelos bancos;
- Identificar os aspectos fundamentais da evolução das mídias sociais e o seu impacto na relação entre os consumidores e as organizações;
- Identificar a estrutura do *social world* e o *Social Business* e o enquadramento dos serviços bancários online através deste novo modelo de negócios;
- Desenvolver um modelo com o propósito de orientar os bancos a aumentarem o índice de aderência e presença nas principais mídias sociais para colaborar com soluções de prevenção às fraudes eletrônicas.

1.4 Relevância da Pesquisa

As fraudes eletrônicas já custam aos usuários da Internet e aos bancos brasileiros milhões de reais. Segundo dados da FEBRABAN (Federação dos Bancos), os prejuízos com fraudes eletrônicas em 2011 atingiram R\$ 1,5 bilhão, sendo R\$ 900 milhões provenientes de fraudes com cartões de crédito e débito através da clonagem dos números, R\$ 300 milhões através do Internet Banking e Mobile Banking e R\$ 300 milhões provenientes das fraudes com cartões de crédito utilizados de forma não presencial, denominado de cartão não presente – golpe muito utilizado em sites de comércio eletrônico. Nessa pesquisa, o termo fraudes eletrônicas faz referência às fraudes realizadas por meio do Internet Banking.

Ataques sustentados aos clientes pelos criminosos cibernéticos também pode afetar gravemente a confiança do público nos serviços bancários pela Internet. Além disso, eles apontam que, para manter a confiança nesses serviços, os bancos e clientes precisam assumir uma responsabilidade conjunta, ou seja, devem investir em medidas excelentes de segurança e os clientes devem usar as ferramentas fornecidas (LAU, 2006).

Os bancos estão continuamente prestando serviços online para seus clientes há anos. Transferência eletrônica de fundos, pagamento de contas, aplicações financeiras, serviços de autoatendimento e gerenciamento dos recursos financeiros são alguns dos dispositivos amplamente utilizados pelos clientes. No entanto, a utilização desses serviços através da Internet trouxe uma mudança fundamental nesta indústria (FATIMA, 2011).

Pesquisas do relatório IPSOS/CETEM (2011) também apontam a transformação que a economia brasileira vem sofrendo ao longo do tempo, refletindo diretamente no fenômeno de bancarização no setor. Os reflexos e as mudanças pelas quais passaram a sociedade nos últimos seis anos, fruto da grande transformação econômica do Brasil, foram acompanhadas pelo relatório desde 2006. De acordo com o estudo, a pirâmide da classificação econômica brasileira mudou, representando aumento de 48% da classe C, e a redução de 54% das classes D/E no período de 2006 a 2010.

Em termos relativos, os dados em 2006, relativos às classes AB e C juntas correspondiam a 49% da população; em 2010, elas somavam 72%, conforme o Gráfico 1. Essa análise demonstra que a pirâmide de classificação econômica brasileira está sendo modificada, com expressivo aumento da classe C, passando a utilizar de meios e recursos financeiros para suprir suas necessidades, com aumento de gastos em itens relativos ao acesso a crédito e alguns itens relativos à seguridade social, seguros e previdência privada de acordo com o relatório.

Gráfico 1 – Pirâmide de Classificação Econômica, 2006-2010

Fonte: Pesquisa IPSOS/Cetelem (2011)

Essa mudança é também evidenciada através de pesquisas realizadas pela FEBRABAN (2012) elencando o aumento do número de pessoas utilizando o Internet Banking e volume de transações efetuadas neste canal, sociedade mais conectada, impacto da crescente bancarização das classes C e D, inclusão social, entre outros.

De acordo com Heikki et al. (2002), a transformação do sistema bancário tradicional para o banco eletrônico tem sido um salto em direção à essa mudança. O aumento na disponibilização dos terminais de acesso às informações, juntamente com o uso crescente de aplicações oferecidas através de comércio eletrônico e *e-Banking* têm gerado uma exigência real no modelo de confidencialidade, usabilidade e controles.

Por outro lado, a necessidade de privacidade deve ser equilibrada com requisitos de segurança oferecidos aos clientes. Os sistemas eletrônicos de pagamento estão ao longo dos anos passando por mudanças radicais provenientes, em grande parte, pelo avanço tecnológico como: processamento em tempo real, computação distribuída, além da inclinação dos clientes aderirem facilmente à utilização do Internet Banking (SHARMA; SINGH, 2010).

Em função do potencial poder econômico, os bancos possuem acesso ao que há de mais sofisticado em recursos de Tecnologia da Informação e Comunicação. No entanto possui desafios significativos em termos de segurança: sistemas de monitoramento multicanal, biometria, equilíbrio entre conveniência e proteção ao cliente, redução das etapas de autenticação, entre outros.

O número de aplicações maliciosas que visam transações bancárias online tem

aumentado dramaticamente nos últimos anos. Segundo estatísticas do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.BR), o total de incidentes reportados em 2012 foi de 466 mil, um acréscimo de 17% comparado à 2011 e 325% comparado à 2010.

A divulgação de informações importantes que devem permanecer confidenciais, por pessoas não autorizadas ou que excedam a sua autoridade pode causar perdas significativas para os bancos. Alterar informações, introduzindo, modificando ou sobrescrevendo dados no sistema sem autorização é um tipo de ataque que poderia prejudicar o relacionamento neste ambiente e comprometer informações confidenciais.

Uma das formas mais comuns de realizar ataques é através da instalação de programas maliciosos, como por exemplo, o cavalo de tróia, no computador dos clientes. Isso acontece quando os usuários visitam sites não seguros e programas maliciosos, não autorizados são instalados em seu computador sem o seu consentimento. Quando os usuários fazem a autenticação no site do seu banco, as informações digitadas durante a sessão poderão ser capturadas e enviadas para o atacante (ZIN; YUNOS 2005). Maiores detalhes sobre esse tipo de ataque serão abordados em sessão específica neste trabalho.

Isso torna necessário a implementação constante de sistemas e processos capazes de realizar monitoramento online das transações devendo fazer parte do contexto geral de prevenção às fraudes com o objetivo de assegurar que os controles e ferramentas de autenticação sejam apropriados para os bancos e clientes. Processos de autenticação devem ser projetados para maximizar a comunicação de forma transparente e devem ser coerentes com a estratégia do banco para o canal Internet Banking. O nível de autenticação em uma determinada aplicação deve ser adequado ao nível de risco de sua exposição (FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL, 2010).

As ameaças de segurança podem afetar um banco através de inúmeras vulnerabilidades. Muitos problemas relacionados com a segurança das transações são provenientes de dados desprotegidos. Plataformas de Internet Banking oferecem vários métodos para assegurar um elevado e sofisticado nível de segurança contemplando:

- Identificação e autenticação;
- Criptografia;
- Mecanismo de firewalls.

Segundo Fonseca, Meirelles e Diniz (2010), acompanhando o crescimento da economia brasileira, as transações bancárias chegaram a quase 56 bilhões de operações em

2010 e Internet Banking já representa 23% do total, representando um aumento de 27,4% na comparação com 2009. O total de máquinas de autoatendimento em pontos públicos aumentou em 43%, o que enfatiza a busca dos bancos para ampliar a conveniência para seus clientes.

As operações com cheques caíram 9% em 2010, mostrando que os clientes utilizam cada vez menos esse meio de pagamento. Sob o ponto de vista de tecnologia da informação e comunicação, os gastos totais foram de R\$22 bilhões em 2010, com um crescimento de 15% em relação a 2009, o que mostra que a tecnologia cresce em ritmo acelerado. Houve um aumento de 5,7% no número de contas correntes existentes, que chegou a 141 milhões em 2010, evidenciando uma crescente bancarização das classes C e D, segundo pesquisa Anuário Febraban 2012.

Segundo a empresa de pesquisas Ibope NetRatings, em 2011, o Brasil possuía aproximadamente 80 milhões de usuários de Internet. Tal utilização, inevitavelmente, provocou o aumento no número de crimes eletrônicos. Isso mostra que, se a inclusão digital no Brasil ocorreu com velocidade avassaladora, o nível de educação digital não evoluiu com a mesma rapidez (CASTRO, 2010).

Castro (2010) confrontou a velocidade da expansão da internet com a velocidade de inclusão digital no Brasil e constatou que os dois não evoluíram com a mesma rapidez, trazendo um novo nicho de oportunidades para as fraudes no internet banking.

Uma prova disso, ainda hoje golpes primários são aplicados com taxas de sucesso elevadas, o que mostra a falta de conhecimento e educação digital dos usuários para lidar com estes recursos. As empresas também sofrem por serem alvos dos fraudadores que adquirem produtos e serviços com os dados financeiros de seus clientes. Ainda no universo corporativo, os criminosos burlam controles ou exploraram vulnerabilidades de sistemas empresariais em benefício próprio. As vulnerabilidades nesse caso podem ter sido implementadas no sistema voluntariamente ou mesmo sem intenção (CASTRO, 2010). Maturidade e supervisão no desenvolvimento dessas aplicações e de suas manutenções podem prevenir falhas, fraudes e ataques. Há modelos internacionalmente reconhecidos que orientam o desenvolvimento de softwares de forma segura, assim como modelos para gestão de mudanças (CASTRO, 2010).

Ainda sob a visão expressa de Castro (2010), o que em geral acontece, até mesmo pelo dinamismo que determinadas linhas de negócio demandam, é que há pouco tempo para análise do problema, e tempo ainda menor para colocar em prática uma solução adequada. Nesse contexto, dificilmente é possível realizar testes adequados para garantir que falhas, intencionais ou não, venham a ser implementadas. Diante do alto índice de aderência e

utilização dos meios eletrônicos, torna-se praticamente inviável manter-se livre dos ataques - o que é possível nesse caso é evitar que uma parcela desses ataques tenha sucesso.

Neste contexto crescente na utilização desses serviços, em 2011, de acordo com Fonseca, Meirelles e Diniz (2010), as perdas com fraudes bancárias realizadas por meio eletrônico somaram R\$ 685 milhões no primeiro semestre de 2011, o que representa um aumento de 36% em relação ao mesmo período do ano anterior (2010), que foi de R\$ 504 milhões.

Os bancos por sua vez investem em infraestrutura, recursos tecnológicos e humanos para evitar possíveis tentativas de fraudes, garantir confidencialidade dos dados dos clientes e a segurança no uso dos canais eletrônicos. Em 2009, o montante investimento no setor bancário totalizou R\$ 1,4 bilhão em segurança e R\$ 19,4 bilhões em tecnologia da informação, além de desenvolver diversas soluções de proteção com diferentes níveis de senha de acordo com Fonseca, Meirelles e Diniz (2010), significando que para cada tipo de transação a ser realizada, exigem-se diferentes e mais robustos sistemas de autenticação.

Para tanto, estão constantemente prospectando e implementando novas ferramentas capazes de aumentar e garantir cada vez mais a segurança dos processos, oferecendo um ambiente confiável para seus clientes (FONSECA; MEIRELLES; DINIZ, 2010).

Nesse sentido, há poucos registros de invasão e/ou fraude eletrônica a partir dos sistemas internos dos bancos, pois esse tipo de fraude acontece principalmente a partir do usuário. No caso de tentativa de fraude interna, o processo de rastreabilidade das informações fica mais fácil, permitindo identificar a natureza do ataque como captura de trilhas de cartões nas operações de compras, ou obtenção indevida de senhas de acesso e dados pessoais dos clientes (FONSECA; MEIRELLES; DINIZ, 2010).

No caso da Internet, é comum que a fraude ocorra pelo fato do cliente ser iludido por programas maliciosos solicitando informações pessoais e/ou de seu relacionamento bancário, além de não adotar as medidas recomendáveis de segurança nos seus equipamentos, como software antivírus atualizado, sistemas operacionais legítimos, *firewall*, entre outros.

Por meio da exploração da curiosidade ou da ingenuidade dos usuários, os criminosos conseguem instalar programas clandestinos nos seus computadores. Por isso os bancos procuram conscientizar seus cliente e publicar dicas de segurança em seus sites (FONSECA; MEIRELLES; DINIZ, 2010).

Dados publicados pela FEBRABAN afirmam que, em junho de 2012 os principais bancos brasileiros aderiram ao convênio firmado em 2011 entre a FEBRABAN e o Departamento de Polícia Federal para acelerar o mapeamento e a identificação de fraudes em

pagamentos eletrônicos. No Brasil, o Grupo de Resposta a Incidentes de Segurança para a Internet Brasileira (CERT.BR) tem como objetivo tratar e reportar os incidentes de segurança e fraudes em âmbito nacional, classificando através de uma série de relatórios e estatísticas referentes a evolução e tendências das fraudes eletrônicas no contexto nacional.

Baseada em informações do CERT.BR (2012) o gráfico apresentado na Figura 1 mostra o crescente número de incidentes reportados entre os anos de 1999 a 2012. É importante ressaltar que esse gráfico representa os incidentes relacionados à *worms*, *DoS*, invasão, web, *scan*, fraudes e outras notificações que não se enquadram nas categorias anteriores.

Figura 1 - Total de incidentes anuais reportados de 1999 a 2012

Fonte: CERT.BR (2012)

Na tabela 1, demonstra-se a evolução dos incidentes de fraudes reportados ao CERT.br entre os períodos de janeiro a dezembro de 2011, 2010 e 2009, com a quantidade de fraudes reportadas mensalmente, o total de incidentes no período e a respectiva porcentagem entre o total e a quantidade de fraudes.

Tabela 1 - Totais mensais classificados por quantidade de fraudes

	2011				2010				2009		
Mês	fraude (%)		Total	Mês	fraude (%)		Total	Mês	fraude (%)		Total
jan	3098	18	16840	jan	2545	30	8223	jan	74909	70	105945
fev	3457	13	26289	fev	2313	27	8266	fev	66214	89	73883
mar	3814	8	47630	mar	3529	29	11836	mar	32440	84	38246
abr	3891	8	44908	abr	2829	24	11462	abr	19228	75	25496
mai	3307	7	42715	mai	2359	24	9680	mai	38790	88	43819
jun	2544	6	39458	jun	2872	24	11680	jun	2023	18	10792
jul	3307	7	42262	jul	2440	19	12661	jul	2421	24	9831
ago	3451	10	33209	ago	2596	18	14171	ago	2997	30	9783
set	3300	12	25409	set	2413	18	13177	set	2392	24	9810
out	3238	11	27966	out	1968	15	13078	out	2988	26	11342
nov	3819	14	27248	nov	2257	15	14551	nov	3143	30	10183
dez	3155	12	25581	dez	2887	20	14059	dez	2817	30	9213
Total	40381	10	399515	Total	31008	21	142844	Total	250362	69	358343

Fonte: CERT.BR (2012)

O total de notificações recebidas em 2011 foi de 399.515, este número foi quase três vezes maior que o total de 2010. O quarto trimestre de 2011 totalizou 80.795 notificações o que representa uma queda de 20% em relação ao trimestre anterior e a um aumento de 94% em relação ao quarto trimestre de 2010. Em tentativas de fraudes o qual está inserido o escopo deste trabalho, em 2011 totalizaram 40.381 casos, correspondendo a um aumento de 30% em relação a 2010 conforme mostra os gráficos da figura 2.

Tentativas de fraudes reportadas em 2011

Tentativas de fraudes reportadas em 2010

Figura 2 - Distribuição dos tipos de tentativas de fraudes reportadas nos anos de 2010 e 2011

Observa-se também crescimento e 62% das notificações de casos de páginas falsas de bancos e sites de comércio eletrônico em 2011 em relação a 2010.

Abaixo descrição da legenda referente ao gráfico apresentado:

- **Cavalos de tróia:** Tentativas de fraude com objetivos financeiros envolvendo a captura de informações pessoais e bancárias;
- **Páginas falsas:** Tentativas de fraude com objetivos financeiros envolvendo o uso de páginas falsas;

- **Direitos autorais:** Notificações de eventuais violações de direitos autorais;
- **Outras:** Outras tentativas de fraude.

Estes dados mostram o crescente montante envolvido no volume transacional bancário no Brasil e o impacto das fraudes. Novas modalidades e canais das fraudes, que apenas se adicionam aos riscos já existentes poderão ter um impacto significativo sobre os processos financeiros atuais. Como dito anteriormente, mecanismos de prevenção e monitoração são fundamentais para a gestão eficaz dos incidentes, além do profundo alinhamento do posicionamento estratégico do banco com relação ao seu marketing, modelos de divulgação dos seus produtos e serviços proporcionando uma comunicação clara e transparente através de um ambiente seguro e colaborativo, o que torna o presente trabalho desta pesquisa relevante.

1.5 Motivação

A partir de meados de 2008 a economia mundial vem sofrendo alguns impactos financeiros oriundos por falhas e deficiências na gestão de recursos, ocasionado dentre outros fatores pela falta de confiança nas operações financeiras deste segmento. Diante deste cenário de crise e competição financeira, somado às necessidades de constantes mudanças operacionais, os bancos estão sendo estimulados a modificarem suas políticas e controles na gestão de crédito com o objetivo de identificar e minimizar os riscos inerentes às operações e tomadas de decisão deste setor (KRUGMAN, 2009).

Os prejuízos deste mercado vão além das perdas financeiras oriundas de créditos fornecidos a pessoas e empresas que passaram a encontrar dificuldades de honrar os compromissos assumidos. Existem outros tipos de riscos associados, como os riscos de fraudes, operacionais e de imagem, os quais necessitam de uma atuação e posicionamento claro por parte dos gestores para reduzir a exposição das organizações às ameaças deste segmento (EL-ERIAN, 2008).

Greenspan (2008) reforça que os bancos precisam se fortalecer neste momento de crise para darem respostas firmes ao mercado mundial, reduzindo não só a exposição aos riscos operacionais e de imagem, mas aos de fraudes em todos os seus aspectos.

Através do crescimento das transações eletrônicas realizadas pelo Internet Banking e as consequências financeiras provenientes das fraudes eletrônicas que conforme mencionado anteriormente representa um desafio para a indústria financeira, os bancos estão, neste momento, com um dilema para ser resolvido. Se por um lado os bancos já sabem como lidar com as fraudes eletrônicas provenientes do Internet Banking, por outro, com a popularidade e

ampla utilização das mídias sociais e sua utilização como novo canal de relacionamento com os clientes, exige-se novas políticas e estratégias de prevenção. Assim, cresce a importância sobre sua utilização e definições estratégicas de âmbito corporativo que definirão e nortearão a transição entre o atual banco digital para o banco social (acesso ao banco por meio das mídias sociais, como por exemplo o Facebook), na maneira que os mesmos irão se posicionar no mercado dentro do processo de prevenção, mitigação e redução das fraudes eletrônicas.

Diante deste cenário, ordenam-se neste trabalho os elementos que formam o conceito de fraudes eletrônicas e mídias sociais, demonstrando o enquadramento dos produtos e serviços bancários na transição do Internet Banking tradicional para o novo conceito de *Social Banking*, elencando quais os passos que devem ser tomados para que as fraudes bancárias não inviabilizem este novo modelo de negócio.

1.6 Estrutura do Trabalho

Este trabalho está estruturado em cinco capítulos. O primeiro apresenta uma visão geral de todo o trabalho descrevendo a contextualização e justificativa, formulação do problema, declaração do objetivo e a relevância. O segundo capítulo detalha a metodologia, etapas e procedimentos metodológicos utilizados. O terceiro capítulo traz a fundamentação teórica o qual apresenta os principais conceitos que sustentam a pesquisa: evolução da tecnologia da informação no setor bancário, fraudes eletrônicas e redes sociais. O quarto capítulo faz a análise da matriz dos dados e apresenta os resultados da pesquisa na forma de modelos de negócios de acordo com o grau de presença social dos bancos. O quinto capítulo traz a conclusão do trabalho.

2 MÉTODO DE PESQUISA

Neste capítulo são apresentadas as escolhas metodológicas da pesquisa, etapas necessárias para o seu desenvolvimento e os procedimentos metodológicos.

2.1 Caracterização Geral da Pesquisa

Para atingir o objetivo desta pesquisa em função da problemática, optou-se pela pesquisa com abordagem qualitativa com caráter descritivo e exploratório (YIN, 2001).

A abordagem qualitativa justifica-se, pois este estudo contemplou características inerentes a este tipo de abordagem de pesquisa, sendo (BOGDAN; BIKLEN, 1994):

- A pesquisa qualitativa tem como fonte direta de dados o ambiente natural, sendo o pesquisador o seu principal instrumento.
- Os dados coletados são predominantemente descritivos. O material obtido durante a pesquisa possibilitou descrever a situação atual dos bancos com relação aos assuntos investigados.

A pesquisa é descritiva no que se refere à descrição dos principais elementos que compõe a evolução da tecnologia da informação no setor bancário brasileiro, os impactos que as fraudes eletrônicas influenciam no processo decisório e a evolução que as mídias sociais está proporcionando em um novo modelo de negócios. A pesquisa descritiva tem como objetivo a descrição das características de determinada população ou fenômeno ou o estabelecimento de relações entre variáveis (GIL, 2007). Também é caracterizada como exploratória, pois se buscou maior conhecimento sobre os assuntos tratados para viabilizar o desenvolvimento do modelo. A pesquisa exploratória, segundo Gil (2007), é desenvolvida com o objetivo de proporcionar uma visão geral, de tipo aproximativo mais amplo, ou seja, quando o tema é genérico torna-se necessário seu esclarecimento e delimitação.

2.2 Etapas da Pesquisa

Esta pesquisa foi desenvolvida em duas etapas. A primeira foi o levantamento bibliográfico, no qual se buscou compreender os principais conceitos referentes aos processos, ameaças e mecanismos de prevenção no combate às fraudes eletrônicas em bancos. Ainda na primeira etapa, realizou-se o entendimento dos aspectos fundamentais que compõem a evolução das mídias sociais, o impacto das tecnologias da informação e comunicação sobre

o marketing e o surgimento de um novo modelo de negócios (*Social Business*).

A segunda etapa foi a construção do modelo de presença social o qual foi desenvolvido mediante coleta/sistematização de dados através de estudos de casos com bancos selecionados.

2.3 Procedimentos Metodológicos

Os procedimentos metodológicos adotados para essa pesquisa são os seguintes:

- Efetuar um levantamento bibliográfico procurando o estado atual dos produtos e serviços bancários relacionados ao Internet Banking no Brasil, os principais tipos de fraudes e seus impactos no sistema, bem como a configuração do *Social Business* a partir das mídias sociais e como a presença social dos bancos pode ser medida e utilizada para evitar fraudes no Internet Banking.
- Organizar os conceitos de mídias sociais, *Social Business* e *Social Banking* para construir um mapa de avaliação de presença social para os produtos e serviços bancários.
- Aplicar este mapa em pelo menos quatro bancos com operações no Brasil e comparar suas diferenças e seu desempenho em relação à presença social.
- Analisar e sistematizar os dados obtidos e responder aos questionamentos iniciais.
- Apresentar os resultados finais e discutir a possível estrutura teórica para relacionar presença social e fraudes no Internet Banking.

3 FUNDAMENTAÇÃO TEÓRICA

Este capítulo apresenta a evolução da tecnologia da informação no setor bancário no Brasil e uma visão geral da literatura acadêmica sobre fraudes eletrônicas, seus métodos, ameaças, riscos e modelos de prevenção através da perspectiva dos bancos e dos clientes. Adicionalmente, apresenta-se revisão da literatura sobre os conceitos, termos e definições das redes sociais e o seu impacto na relação entre os consumidores e organizações.

3.1 O Papel da Tecnologia da Informação no Setor Bancário

O crescimento econômico mundial nas últimas décadas abriu espaço para o aparecimento de novas empresas, de todos os portes, em diferentes e muitas vezes até novos segmentos da economia. Junto com estas empresas, vieram grandes mudanças tecnológicas.

Não há dúvidas quanto ao papel determinante da tecnologia de informação no processo de desenvolvimento de inovações no setor bancário. A tecnologia participa tanto do processo de criação de produtos, quanto de sua distribuição aos clientes. Mesmo inovações tecnológicas que surgem no mercado sem relação direta com o setor podem influenciar o processo de criação de novos produtos bancários. Um produto originado de uma inovação tecnológica externa ao universo bancário, como por exemplo, a telefonia celular, pode determinar a criação de um produto bancário específico – acesso remoto via dispositivos móveis aos dados bancários do cliente (FONSECA; MEIRELLES; DINIZ, 2010).

Diniz (2004, p. 64) destacou que a automação bancária tem associação estratégica com a ideia de que “o dinheiro caminha para se transformar exclusivamente em informação, o que leva os bancos a estarem na vanguarda da Tecnologia de Informação”.

A tecnologia de minicomputadores, desenvolvidas no final dos anos 1960 foi incorporada pelos bancos brasileiros no desenvolvimento de uma estrutura de sub-centros para teleprocessamento de informações de regiões distantes para o mainframe central dos bancos, responsáveis pelo processamento de *back-office*. No final dos anos 1970, com o desenvolvimento da indústria nacional de informática apoiada pelos bancos, o barateamento das tecnologias de automação teve importância decisiva na incorporação de sistemas online (FONSECA; MEIRELLES; DINIZ, 2010). Nesta época os bancos tiveram um papel importante no desenvolvimento tecnológico do país, por investirem em desenvolvimento da sua área de informática, “amplamente facilitada pelo ritmo acelerado do crescimento da inflação naquela época” (DINIZ, 2004, p. 57).

Já nos anos 1980, os microcomputadores entraram em larga escala nos bancos através de automação de escritório, de novos modelos de caixas eletrônicos e nos primeiros projetos de home-banking. Nos anos 90, depois de chegar aos bancos como um espaço institucional, a Internet e a Web foram incorporadas como alternativa segura para transações dos clientes. Para os bancos, por causa da maior confiança na segurança oferecida pela Internet, a estratégia de usar a Web como um canal para transações, poderia trazer também economia no processamento de serviços bancários usualmente realizados em outros canais.

Mais adiante, com a incorporação da Web nos processos bancários através de portais corporativos, intranet, utilização de voz sobre IP e na crescente infraestrutura de caixas eletrônicos, fez com que todas essas tecnologias, embora nascidas fora do ambiente bancário, fossem incorporadas, adaptadas e evoluídas, tornando-se importantes elementos nos processos decisórios dos bancos, seja como suporte a novos canais, seja como geradores de novos produtos e serviços (FONSECA; MEIRELLES; DINIZ, 2010).

Com a migração dos serviços tradicionais executados nas tradicionais agências bancárias para a Internet, proporcionou aos clientes uma forma extremamente eficiente e rápida de comunicação com seu banco sem a necessidade de intervenção direta dos funcionários dos bancos. Com a evolução da tecnologia da informação, processamento de transações de crédito, empréstimos, câmbio, dentre muitas outras, podem ser feitas rapidamente em tempo real ou de acordo com a característica da operação. Além dessas facilidades e comodidades, a inexistência de restrição geográfica possibilita às empresas trabalhar além da sua fronteira física (GHOSH, 1998). Diante disso, os aplicativos de home banking, que eram disponibilizados em rede de comunicação privada, começaram a migrar para a Internet, ocorrendo no Brasil, em meados de 1996 (GATES, 1999).

Os clientes dos bancos, a partir da década de 70 até metade da década de 90, fim da bolha inflacionária, demandavam rapidez e eficiência do sistema financeiro para compensar a inflação galopante afirma Adachi (2004). Do outro lado, os bancos lucravam com a inflação e, conseqüentemente, investiam pesadamente na automação bancária, para dar sustentação ao sistema financeiro. Este benefício transcendeu o ambiente tecnológico beneficiando também a sociedade. Nos eventos mais recentes desta transformação surgiu a denominação de Economia Digital (TAPSCOTT, 1997), descrevendo este novo modelo, no qual a Internet tem um papel fundamental na construção de novas formas de relacionamento, assim como de estrutura institucional:

Estamos no limiar de uma nova economia digital, onde os microprocessadores e as redes públicas que seguem o modelo da Internet possibilitam tipos fundamentalmente novos de estruturas institucionais e de relacionamentos. O que está acontecendo é isto: indivíduos eficientes, trabalhando em estruturas de equipe de alto desempenho; transformando-se em redes organizacionais e integradas, com clientes e servidores: que saem ao encontro de clientes, fornecedores, grupos de afinidade e até mesmo concorrentes; que se conectam à Net pública, alterando a maneira como produtos e serviços são criados, comercializados e distribuídos (TAPSCOTT, 1997, p. 100).

3.2 Fases da Automação Bancária no Brasil

Além da tecnologia, algumas inovações acabam por ser desenvolvidas para atender demandas que surgem no mercado. Estas demandas podem estar associadas a diversas mudanças que impactam o ambiente do mercado, como por exemplo, fatores macroeconômicos, ambiente concorrencial, variáveis demográficas, etc. A pressão por mudanças no mercado podem inspirar a criação de novos produtos e serviços financeiros e estes acabam por ajudar na consolidação de inovações no setor bancário.

A figura abaixo exemplifica as fases da automação bancária no Brasil sob o ponto de vista de tecnologia e investimentos no setor.

Figura 3 - Linha do tempo da automação bancária no Brasil

Nos anos 60, o processo de concentração bancária influenciou decisivamente a adoção e utilização de computadores no processamento de *back-office*, quando provocou um aumento significativo dos volumes processados nos grandes bancos nacionais que surgiram deste processo. Na segunda metade dos anos 70 e início dos 80, o processo inflacionário em curso

no Brasil provocou nos clientes de serviços bancários uma preocupação específica com o tempo transcorrido entre transações feitas no setor financeiro, colocando aos bancos a necessidade de investir em sistemas online.

Após os planos de estabilização nos anos 80 e 90, a redução dos lucros obtidos pelos bancos com a inflação obrigou-os a redirecionar os investimentos em tecnologia, direcionando-os para a obtenção de eficiência e redução de custos nas transações efetuadas. Da mesma forma, o crescimento de renda da população nos níveis sociais menos privilegiados faz com que bancos procurem desenvolver estratégias para esses mercados, apoiados no uso de canais eletrônicos de baixo custo.

Algumas mudanças demográficas são expressas na alteração de comportamento dos usuários dos serviços financeiros. Um exemplo particularmente interessante deste tipo de determinante associado às demandas de mercado diz respeito ao lançamento dos primeiros serviços de Internet Banking no Brasil. Em 1995, após lançar seu primeiro website institucional, o Bradesco começou a receber e-mails que elogiavam a iniciativa da instituição. Esta fase de elogios, entretanto, durou pouco e logo depois os e-mails recebidos passaram a questionar quando seria possível consultar o saldo e extratos das contas correntes através da Internet.

A partir de um determinado momento, 80% destes e-mails questionavam a utilidade do website desse banco, praticamente exigindo se disponibilizasse serviços mais interessantes para os clientes. O banco não resistiu à crescente pressão dos clientes por tais serviços, e decidiu desenvolver uma solução que agregaria ao website institucional a possibilidade dos clientes realizarem transações bancárias pela Internet (FONSECA; MEIRELLES; DINIZ, 2010).

O Home Banking, antecessor do Internet Banking, versão de acesso ao banco por meio de linha dedicada (comunicação ponta a ponta entre o banco e o cliente), e software próprio, distribuído pela instituição, segundo Seybold e Marshak (1998), não teve muita adesão por parte dos clientes, como por exemplo, no caso do Banco Californiano Wells Fargo. Todavia, quando o banco colocou à disposição os serviços bancários na web, no primeiro dia houve a adesão de 1.500 clientes, contra 20 mil em sete anos, de 1989 a 1995, do home banking. Com a crescente adoção do Internet Banking pelo mercado, novas preocupações com a segurança começaram a surgir, conforme o aumento da popularização e utilização.

A utilização de informações em rede implica, por si só, aumento de exposição e vulnerabilidade. A integração dos bancos no ambiente web é passível de exposição de suas fragilidades de segurança das informações e do patrimônio, vivendo, portanto, em um

ambiente de risco (GARFINKEL; SPAFFORD, 1997).

O Tribunal de Contas da União (2003), em seu guia de Boas Práticas em Segurança da Informação, bem como Nakamura e Geus (2002) descrevem a influência da rede pública no quesito de segurança e seu peso nas organizações.

Com a chegada dos computadores pessoais e das redes de computadores que conectam o mundo inteiro, os aspectos de segurança atingiram tamanha complexidade que há a necessidade de desenvolvimento de equipes e métodos de segurança cada vez mais sofisticados. Paralelamente, os sistemas de informação também adquiriram importância vital para a sobrevivência da maioria das organizações modernas, já que, sem computadores e redes de comunicação, a prestação de serviços de informação pode se tornar inviável (TRIBUNAL DE CONTAS DA UNIÃO, 2003, p. 10).

Cameron (1997), a seguir, aumenta a amplitude da segurança, antes restrita à organização. Surge neste momento o elemento meio, associado à organização para endereçar o processo de segurança.

Security is no longer simply matter of ensuring that users within an organization use computing resources appropriately. It now extends to guarding against those skilled and savvy global users who consider it their hobby, obsession, and perhaps even mission to gain illegal access to systems and data (CAMERON, 1997, p. 7).

3.3 Integração e Segurança do Internet Banking

O primeiro Internet Banking surgiu em Atlanta, Estados Unidos, no dia 18 de outubro de 1995. O Banco, que só existia na Internet, chamava-se *Security First Network Bank* (SFNB) (ADACHI, 2004; HUMPHREYS, 1998). O Brasil é um dos pioneiros no uso da Internet para realizar transações e distribuir serviços bancários. Segundo Gates (1999), o Bradesco, um dos maiores bancos privados do Brasil, foi o quinto banco, no mundo, a lançar o Internet Banking para seus clientes, em 1995. Gates (1999) também indica que, em 1962, o Bradesco foi o primeiro a usar computadores e, em 1982, o primeiro a oferecer caixas automáticos e home banking.

Com base na adoção tecnológica no Bradesco é possível inferir o quanto a Tecnologia de Informação é importante para o crescimento e sucesso dos bancos, principalmente os de varejo no mercado brasileiro.

A utilização da Internet, como um novo e inovador meio para se relacionar e transacionar, foi impulsionada principalmente pela redução de custos que ela teoricamente gera, em contraste com o custo da rede física de agências e terminais de autoatendimento

(ADACHI, 2004).

A partir do momento em que os bancos iniciam o relacionamento com seus clientes por meio deste canal, pode torna-se exposto às situações envolvendo riscos de segurança, bem como potenciais ataques em seus sistemas transacionais, dentre outros. Com isso, a demanda por uma gestão de segurança integrada, proativa e com respostas rápidas e eficientes às ameaças e vulnerabilidades e que reflita rapidamente às mudanças organizacionais, tecnológicas, operacionais e mercadológicas, tornou-se necessária, para usufruir os benefícios deste canal (D'ANDRÉA et al., 2000).

Este novo canal proporciona aos clientes acesso aos serviços bancários 24 horas por dia, 7 dias da semana, sem a necessidade de intervenção de qualquer funcionário do banco. O processamento das vendas e transações pode ser feito em tempo real ou em lotes noturnos. Além disso, a inexistência de restrição geográfica possibilita às empresas trabalharem além da sua fronteira física (GHOSH, 1998).

Com isso, os aplicativos de home banking, que eram disponibilizados em rede de comunicação privada, começaram a migrar para a Internet. Ghosh (1998) justifica que a ubiquidade e as possibilidades de interação por meio do autoatendimento levaram os bancos a criarem um ambiente ainda mais competitivo. Um levantamento, realizado no mercado britânico, em 2002, aponta que 5% do mercado bancário local era dominado por quatro bancos que existiam apenas de forma virtual (LAUDON, K.; LAUDON, J., 2004).

De acordo com Lunn (1999), os bancos são fundamentais para o crescimento dos mercados emergentes, sendo que a tecnologia é o lubrificante que viabiliza as engrenagens financeiras:

Emerging markets represent the vast majority of the world's population and the growth markets of the next century. Banking is the essential lubricant to these new economies, first helping them make the initial transition from subsistence farming and then helping their companies trade with the world; and technology is the essential lubricant of banking (LUNN, 1999, p. 2-1).

3.4 A Evolução das Fraudes no Ambiente do Internet Banking

Nos últimos anos, fraude financeira, incluindo fraudes eletrônicas, fraude corporativa e lavagem de dinheiro, tem atraído uma grande preocupação e atenção das empresas e sociedade. Há muitas definições de fraudes, dependendo do ponto de vista a ser considerado. De acordo com o *American Heritage Dictionary - Second College Edition*, a fraude é definida como: “um engano deliberadamente praticado para assegurar ganho ilícito ou ilegal”. O

Dicionário de Inglês *Oxford* define fraude como: "atividade ilícita ou criminal com intenção de ganho financeiro ou pessoal".

Para fins deste trabalho, nosso foco será o ambiente e definições das fraudes eletrônicas. De acordo com Lau (2006), a fraude eletrônica é definida como sendo a aplicação de qualquer golpe, utilizando os serviços disponíveis na Internet, tais como salas de bate-papo, mensagens eletrônicas e sites disponíveis na Internet. Adicionalmente menciona que a fraude pode ser compreendida pelo aliciamento de potenciais vítimas através do fraudador com a intenção de realizar transações fraudulentas beneficiando um indivíduo ou grupo de pessoas envolvidas no esquema. Na visão de Phua et al. (2005) a fraude pode ser definida como abuso de um sistema de lucro organizacional, sem que isto resulte necessariamente em consequências legais diretas.

Embora não exista uma definição universalmente aceita de fraude financeira, Wang et al. (2006, p. 1120) a define como: "um ato deliberado que é contrário à lei, à política ou regra cuja intenção é obter benefício financeiro não autorizado."

Diante dessas afirmações expostas acima, Kovach (2011) define a fraude eletrônica como sendo qualquer acesso não autorizado ou uma transação não autorizada efetuada em uma conta corrente através da Internet. Ainda sob a visão de Kovach (2011), a fraude também pode ser compreendida como resultante de um conjunto de violações de controles de segurança que, em última instância, resultam na efetivação de uma operação financeira não autorizada, conforme descrito abaixo:

- **Operação financeira:** evento de negócio que ocasiona movimentações em contratos de produtos bancários, como CC, Poupança, Fundos, etc.;
- **Operação financeira não autorizada:** operação financeira efetuada de forma ilegítima, ou seja, em desacordo com as regras de negócio ou regras de controle.

Bolton e Hand (2001) descrevem o processo de prevenção às fraudes como medidas de segurança para evitar indivíduos não autorizados a iniciarem transações em contas nas quais eles não foram autorizados. Para o contexto e foco deste trabalho, utiliza-se e referencia-se o conceito, evolução e implicações das fraudes eletrônicas efetuadas por meio do Internet Banking e sua evolução e características no cenário de transição para o *Social Banking*.

Crimes Cibernéticos

A democratização dos computadores e acesso às redes de comunicações de qualidade possibilitou a disseminação dos recursos e serviços disponibilizados através da Internet. Este cenário propiciou, ao mesmo tempo, o aumento de fraudes, roubos, desvios de informações e de capital. Diante desta crescente evolução tecnológica, surge o crime cibernético que pode ser denominado como uma ofensa online cometida por fraudadores e outros tipos mal-intencionados que usam a Internet para roubar informações, sequestrar computadores, enviar e-mails não solicitados, entre outros tipos de atividades ilícitas (RUSSEL; GANGEMI, 1991).

Este ambiente cibernético faz com que o assunto prevenção às fraudes seja gerenciado de forma estratégica e com constante atenção pelas organizações. “As empresas devem se conscientizar da existência dos riscos, reconhecê-los, e desenvolver estratégias de segurança em resposta às ameaças” (CAMERON, 1997, p. 8). Com os benefícios da tecnologia também aparecem novos riscos facilitando novas formas e métodos mais eficientes de cometer fraudes e roubos de identidade, conforme análise de Glaessner, Kellermann e McNevin (2002).

Há um debate sobre a definição exata dos crimes cibernéticos e seu significado tem mudado possivelmente como resultado da evolução da própria Internet.

Gordon e Ford (2006) definem crime cibernético como sendo qualquer crime que é facilitado ou realizado através da utilização de computadores, redes ou *hardware*. Adicionalmente propõem uma separação entre dois grandes tipos:

- **Tipo I:** geralmente requer um número limitado de eventos e é muitas vezes facilitado pelo uso de softwares maliciosos como *keyloggers* ou cavalos de tróia. Este tipo de crime tende a possuir ganhos financeiros como objetivo, através da captura de informações confidenciais dos clientes, o qual posteriormente os fraudadores podem utilizar dessas informações para realizar as fraudes.
- **Tipo II:** geralmente requer múltiplos eventos e muitas vezes são realizadas com a utilização de softwares não maliciosos, como por exemplo, programas de mensagens instantâneas. Atores do tipo II tendem a ter um motivo mais pessoal ou político, como perseguição ou terrorismo cibernético. Embora esta tipologia de crime não vise ganhos financeiros para o executor, pode por outro lado causar perdas financeiras às suas vítimas.

Através da visão de Carter (1995), Davis e Hutchison (1997), os crimes cibernéticos podem ser classificados da seguinte forma:

- Casos em que o computador é o objeto do crime, tais como ataques à infraestrutura de tecnologia da informação ou uso não autorizado de sistemas;
- Casos em que os computadores atuam como ferramentas viabilizadoras dos crimes que ocorrem no mundo real, tais como fraudes ou assédio;
- Casos em que crimes do mundo real são apoiados por computadores, utilizando-os apenas para comunicação ou recurso computacional.

Reforçando essas definições, Lau (2006) menciona que mesmo com o crescimento das fraudes eletrônicas, as formas para que estas evoluem são continuamente modificadas à medida que os fraudadores se tornam mais capacitados na exploração das tecnologias existentes e criativos na invenção de esquemas fraudulentos. Ficar à frente do elemento criminoso é uma tarefa difícil e desafiadora para os gestores de prevenção às fraudes.

O desafio a essas ameaças evolui na medida em que o setor financeiro adiciona novos canais de distribuição, aumentando a oferta de produtos e serviços aos clientes através de dispositivos celulares e *tablets*. Essa tendência, combinada com a ocorrência de fusões e aquisições no mercado brasileiro, tende a aumentar a complexidade do cenário de tecnologia da informação no qual o monitoramento das fraudes deve ocorrer independentemente das diferentes linhas de negócio, tipos de canais e plataformas tecnológicas (ADAMS, 2010).

A ausência de uma visão holística e abrangente por parte dos bancos perante às atividades realizadas pelos seus clientes em todos os canais de relacionamento torna o processo de prevenção e detecção de fraude mais complexa e desafiadora (ADAMS, 2010).

Ainda sob a ótica de Adams (2010), embora os fraudadores possuam cada vez mais recursos e estão cada vez mais ativos, há um esforço contínuo da indústria financeira na tentativa de ficar à frente da curva da fraude, ou seja, desenvolvendo sistemas analíticos preditivos e capazes de identificar atitudes suspeitas e/ou fora dos padrões de cada cliente mesmo antes delas ocorrerem.

Por não haver uma solução única ou abordagem definitiva para combater essas ameaças, os bancos devem trabalhar cada vez mais integrados entre si com o intuito de disponibilizar constantemente novas e modernas tecnologias. Desta forma protegem-se os interesses do banco na medida em que possam desenvolver estratégias analíticas e de modelagem de dados capazes de atuarem antecipadamente ao possível risco de violações de

privacidade e acesso indevido às informações dos clientes.

Adams (2010) complementa que é primordial aos bancos a necessidade de aumentar a interação dos clientes nos canais eletrônicos, gerando maior engajamento, objetivando auxiliar no processo de redução de riscos. Assim, torna-se importante a intensificação dos esforços em marketing, comunicação e campanhas sincronizadas com as demandas e tendências dos negócios de forma a disponibilizar informações inerentes ao negócio, de forma clara, objetiva e sincronizada, criando uma cultura de educação corporativa entre o banco e seus clientes. Adicionalmente torna-se necessário uma gestão por serviços e processos mais robustos em todos os canais de relacionamento, coordenando de forma efetiva a evolução e padrões das transações eletrônicas.

Segurança Eletrônica no Internet Banking

Os avanços da tecnologia da informação e comunicação abriram caminho para o surgimento da Internet, mudando, radicalmente, a forma de uso da tecnologia (ADACHI, 2004; RUSSEL; GANGEMI, 1991). A Internet é uma rede de computadores de mão dupla: assim como o usuário tem acesso a milhões de informações, publicadas na rede, os criminosos e indivíduos de má índole também podem ter o mesmo nível de acesso. Somado a isso, a web é um ambiente de fácil navegação, porém, a sua tecnologia é complexa e cheia de falhas de segurança (ADACHI, 2004; GARFINKEL; SPAFFORD, 1997).

O crescimento e proliferação do Internet Banking motivaram os bancos a se preocuparem com a segurança eletrônica. Segurança em Tecnologia de Informação baseia-se na tríade que assegura a preservação da integridade, confidencialidade e disponibilidade (ADACHI, 2004; KRUTZ; VINES, 2001). A Internet agregou a esta tríade os conceitos de privacidade, não repúdio e autenticidade (ADACHI, 2004; CAMP, 2000). Estes conjuntos de componentes são tratados de tal forma a minimizar os riscos estratégicos, financeiros e operacionais, em busca da eficiência operacional com redução de custos, incremento da conquista de novos mercados, democratização da rede, e novas possibilidades no relacionamento com o meio interno ou externo (ADACHI, 2004).

Adachi (2004) e Brands (2000) indicam que a sociedade, baseada em documentação física com fotos e assinaturas manuscritas, está sofrendo a transição para uma comunidade cibernética, e esta nova forma de se comunicar e transacionar só será possível se os mecanismos que suportam esta nova realidade estiverem seguros.

A utilização da Internet como canal de relacionamento pelos bancos deu-se através de

razões relacionadas à redução de custos operacionais e processuais; presença e incremento da marca; vantagem competitiva, maior capilaridade na oferta de produtos, migração dos serviços bancários tradicionais efetuados em agências para os canais eletrônicos. A utilização dos canais eletrônicos alavancam diversas oportunidades, porém, riscos associados a esses canais devem ser vistos e gerenciados, principalmente aqueles relacionados à autenticação dos clientes pelos bancos.

Nami (2009) sugere uma variedade de tecnologias e metodologias disponíveis para a autenticação dos clientes. Estes métodos incluem o uso de senhas, certificados digitais que utilizam infraestrutura de chave pública, dispositivos físicos como cartões inteligentes, *tokens*, *plug-ins* (que utilizam scripts para transação de perfis), identificação biométrica, entre outros. Os métodos de seleção e utilização de tecnologias de autenticação devem depender dos resultados do processo de avaliação de riscos e segurança realizados constantemente pelos bancos.

A seguir, Nami (2009) descreve um exemplo de metodologia de autenticação envolvendo três princípios básicos:

- Algo que o usuário sabe, por exemplo, a senha do banco;
- Algo que o usuário possui, por exemplo, o dispositivo *token*;
- Algo que o usuário é, por exemplo, o mecanismo de biometria.

Os modelos atualmente adotados pelos bancos são estruturados em várias camadas de prevenção, consistindo em diversas soluções paralelas e mecanismos que visam proteger o aplicativo bancário e os dados dos usuários, proporcionando identificação, autenticação e autorização, complementa Nami (2009).

Na visão de Healy e Walsh (1984), a segurança pode ser um processo ou resultado de uma atividade. Harris (2002) complementa que segurança no ambiente Internet não deve ser vista apenas como um aspecto da gestão de riscos, ela deve ser aderente aos objetivos e à estratégia do banco e gerida de forma coesa, pelas áreas de negócios e tecnologia.

Protegendo o Cliente

Alguns métodos de proteção propostos por Albertin e Moura (1998) também chamados de autorização ou controles de acesso têm sido desenvolvidos para resolver os problemas de segurança, como por exemplo:

- **Segurança baseada na confiança:** significa confiar em todo mundo e não fazer nada extra para proteção.
- **Segurança através de obscuridade:** utiliza a noção de que qualquer rede pode ser segura, uma vez que ninguém de fora do grupo de administração poderia ter acesso a informações operacionais e que os usuários são providos apenas de informações necessárias para suas atividades.
- **Esquemas de senha:** provém uma barreira em primeiro nível para a intrusão accidental, sendo que estes esquemas fazem pouco no caso de ataques deliberados, especialmente quando palavras comuns ou nomes próprios são selecionados como senhas.
- **Sistemas biométricos:** são considerados como o nível mais seguro de autorização, envolvendo alguns aspectos únicos da pessoa, incluindo comparação de impressão digital, impressões da palma da mão, padrões de retina, verificação de assinatura e reconhecimento de voz. Estes sistemas são muito caros.

Bancos que oferecem produtos e serviços baseados na Internet devem utilizar métodos e ferramentas de monitoramento eficientes e capacitadas para identificar, tratar e mitigar seus riscos eletrônicos (PEOTTA et al., 2011).

3.5 Modelos Atuais de Segurança Adotados pelos Bancos Brasileiros

Conforme exemplificado no item anterior, os modelos atualmente adotados pelos bancos em operações envolvendo o Internet Banking baseiam-se em várias camadas de segurança, consistindo em soluções paralelas diversas e mecanismos que visam proteger o banco e as informações dos clientes, proporcionando a tríplice camada de segurança (PEOTTA et al., 2011):

1. Identificação;
2. Autenticação;
3. Autorização das Transações.

Abaixo os principais mecanismos de segurança oferecidos pelos bancos aos clientes, exemplificado na tabela:

Tabela 2 - Modelos atuais de segurança adotados pelos Bancos brasileiros

Princípios de Segurança	Descrição
Certificados Digitais	Os certificados digitais são usados para autenticar os usuários e o próprio sistema bancário. Este tipo de autenticação depende da existência de uma infraestrutura de Chave Pública (PKI) e uma Autoridade Certificadora (AC), que representa uma terceira parte confiável, que assina os certificados atestando a sua validade. No Brasil, os sistemas bancários usam certificados A1 e A3 emitidos e assinados pela ICP-Brasil (BERTOL; SOUZA Jr.; MELO, 2009).
Dispositivos <i>One-Time Password (Token)</i>	Dispositivos <i>One-Time Password</i> (HALLER et al., 1998) são comumente usados como segundo fator de autenticação, que pode ser solicitados em situações específicas ou aleatórias. Este tipo de dispositivos de processamento faz uso de senhas que podem ser utilizadas apenas uma vez.
Cartões <i>One-Time Password</i>	Cartões <i>One-Time Password</i> constituem um método mais barato para gerar senhas dinâmicas, fornecendo também um segundo fator de autenticação. Porém, em alguns sistemas bancários, senhas geradas por cartões OTP são reutilizadas várias vezes antes de serem descartadas, tornando este sistema vulnerável a vários outros ataques.
Proteção do Navegador	Neste modelo, o sistema é protegido no nível do navegador de Internet do cliente. Com essa proteção, o usuário e seu navegador estão protegidos contra programas maliciosos conhecidos através do monitoramento da área de memória alocada pelo navegador, a fim de detectá-los e impedir o roubo de credenciais e captura de informações confidenciais.
Teclados Virtuais	Teclados virtuais foram desenvolvidos para impedir o uso eficiente dos <i>keyloggers</i> (dispositivo que capturam informações digitadas no computador). Estes dispositivos são geralmente baseados em Java e softwares baseados em criptografia, permitindo a portabilidade entre diferentes dispositivos. Atualmente estão sendo substituídos por outros métodos mais eficientes, que exigem menos poder de processamento e taxas de transmissão mais rápida.
Dispositivos Registrados	Este método restringe o acesso ao sistema bancário a dispositivos previamente conhecidos e registrados pelo banco. Esse tipo de técnica, chamada de “impressão digital de hardware” é usada em conjunto com a identificação do

usuário por meio de credenciais secretas.

CAPTCHA

CAPTCHA - *Completely Automated Public Turing test to tell Computers and Humans Apart* (YAN; EL; SALAH, 2008), é um método recentemente adotado em alguns sistemas bancários, cujo objetivo é tornar ineficazes os ataques automatizados contra sessões autenticadas pelos bancos. Este método requer que o usuário real introduza informações (solicitadas pelo site) exibidas em imagens difíceis de reconhecimento e processamento por robôs automatizados (*Bots*).

Short Message Service (SMS)

Este método tem sido aplicado em alguns sistemas bancários para notificar os usuários sobre as transações que requerem sua autorização. Ele fornece um canal de segunda autenticação para transações que se enquadram em determinadas características, enviando para o usuário um conjunto de caracteres que devem ser informados, a fim de autorizar e processar a transação através do sistema bancário online.

Identificação Positiva

Identificação positiva é um modelo em que o usuário é obrigado a introduzir algumas informações secretas apenas conhecidas por ele, a fim de identificar-se. É aplicado como um método de autenticação secundário.

Monitoramento de Transação

Mesmo que este método não seja minuciosamente analisado no presente trabalho, é atualmente aplicado em muitos sistemas bancários online, cada um deles usando diferentes técnicas. Inteligência artificial (WEIMING et al., 1995), análise de históricos de transações e outros métodos que identificam padrões de fraudes em transações processadas anteriormente estão entre as várias abordagens para a monitoração de transações.

Palavra de Passe

É um modelo de segurança baseado em informações detidas pelo usuário. É normalmente utilizado como um método de autenticação secundário em transações que envolvem movimento de recurso financeiro.

3.6 Estratégias de Ataques

De acordo com Johnson (2008), existem quatro tipos principais de ataque ao Internet Banking. Todos os ataques vistos no transcorrer desta pesquisa estão dentro das primeiras duas categorias:

- Obter credenciais de autenticação da vítima ou;
- Modificar transações legítimas desta.

Os outros dois ataques serão menos abordados neste trabalho, que são a negação do

acesso ao banco ou simplesmente observando as transações da vítima.

3.6.1 Tipos de Ataques e Operação do Submundo das Fraudes

A segurança da Internet se torna fragilizada com o crescente aumento de crimes eletrônicos principalmente aqueles com foco em bancos, sites de comércio eletrônico e mais recentemente pelas mídias sociais. O impacto destes crimes e dos prejuízos financeiros gerados, muitas vezes, não é sequer mensurado, seja por desconhecimento, ineficácia na detecção ou pelo grande prejuízo financeiro associado.

Segundo Wadlow (2000, p. 40), “Saber que está sendo atacado representa mais da metade da batalha”. A seguir, lista com os tipos de crimes eletrônicos mais utilizados na Internet, envolvendo funções tecnológicas e sociais, descritos por Adachi (2004), Krutz e Vines (2001) e Harris (2002):

Tabela 3 - Tipos de crimes mais comuns na Internet

Tipos de ataques	Descrição
<i>Denial of Service (DoS)</i>	Sobrecarregar o servidor de um banco para indisponibilizar serviços e informações, caracterizando um ataque de negação de serviço.
Engenharia social	Usar a habilidade social para conseguir informações privilegiadas.
Códigos maliciosos	Vírus, cavalos de tróia e pragas virtuais que causam negação de serviço, destruição ou modificação de informações.
<i>Spoofing</i> de endereço IP ou de e-mail	Forjar o endereço internet de um website para dar aparência do site oficial do banco. Por exemplo, forjar o endereço do remetente de e-mail para dar credibilidade à mensagem.
<i>Sniffing</i> de senhas	Captura de informações que trafegam na rede. O mais comum é a busca de senha não protegidas.
HOAX (Boato)	Mensagem falsa sobre vírus ou, mais usualmente, de promoções, geralmente na forma de e-mail, com um link para um endereço que na realidade é uma armadilha para coletar senhas. Este é o golpe mais comum, aplicado pelos fraudadores, para colher informações de usuário e senha no Internet Banking.
<i>Phishing</i> / Scam	E-mail que, aparentemente, foi enviado por uma entidade

legitimada na Internet, porém, com intuito de enganar e coletar dados pessoais ou informações de senha bancária.

O relacionamento com o banco no momento de realizar transações pela Internet se dá através de duas entidades, cliente e Banco. Conforme mencionado anteriormente por (BOJANC; JERMAN-BLAZIC, 2008) a ponta mais frágil neste relacionamento é o cliente, portanto, os criminosos concentram os seus esforços em ameaçar, atacar e fraudar esse elo do processo. O foco dos ataques, portanto, está concentrado no cliente final.

Wadlow (2000) esclarece que a gestão da segurança não envolve somente tecnologia. O fator humano é um dos principais agentes responsáveis por acidentes segundo Leveson (1995). Wadlow (2000) descreveu três qualidades que podem levar uma pessoa a atacar um sistema: habilidade, motivação e oportunidade. Normalmente, não é uma tarefa simples atacar e fraudar dados em um servidor de uma instituição bancária. Então, os ataques tem se projetado na exploração das fragilidades dos usuários/clientes, com o objetivo de realizar fraudes bancárias ou em sites de comércio eletrônico.

3.7 Identificando as Ameaças, Meios, Métodos e Ferramentas

Os bancos estão preocupados e atentos às fraudes cometidas em seus canais de atendimento e medidas de prevenção são amplamente divulgadas aos clientes nas agências e no próprio site do Banco. Por outro lado, o comprometimento das informações e senhas dos clientes para ocorrer transações indevidas requer a existência de algum tipo de falha, seja pelo elo mais fraco (cliente), seja através de um sistema, geralmente software, ou em ambos (VAN GOOL, 2011).

Ainda, sob a visão tradicional expressa por Van Gool (2011), a ação da fraude sobre o Internet Banking poderia ser classificada sob dois pontos de vista:

- **Fraudes através da combinação de hardware e software:** os ataques são realizados sem ação direta do usuário. Esta classificação não exclui os ataques que foram possíveis pela ação humana indireta. Um exemplo das ações humanas que indiretamente causam fraudes eletrônicas é a instalação acidental e/ou por desconhecimento do usuário de softwares maliciosos que, uma vez acionados, executam o ataque.
- **Fraudes através da combinação de hardware, software e usuário:** estes são os métodos que fazem uso de hardware e software para executar seus ataques, mas

também exigem ação direta do usuário. Um exemplo é o *phishing*, o qual o usuário é induzido a inserir manualmente as informações de sua conta em uma página falsa do banco.

Nesses casos, o componente tecnológico é inferior ao social de acordo com Van Gool (2011) conforme demonstrado abaixo.

A partir desta distinção, derivam-se dois novos conceitos:

- **Ameaças Tecnológicas:** é baseada em uma fraqueza tecnológica, com ou sem a ajuda de um componente social. A ameaça tecnológica também é conhecida como uma falha na segurança.
- **Ameaças Sociais:** é baseada em uma fraqueza social, com ou sem ajuda de um componente tecnológico. Isto não significa, no entanto, que haja necessidade do envolvimento de vários usuários como o título pode sugerir. A ameaça social também pode ser conhecida como uma ameaça humana ou organizacional. Para efeitos desta pesquisa, estas definições são equivalentes.

A ameaça, conforme Kumar (1995) é a possibilidade potencial de uma tentativa, desautorizada e deliberada de alcançar e manipular informações, deixando o sistema não confiável e inutilizável. A segurança existe para proteger os ativos contra as ameaças, segundo Peltier (2001).

Ameaça é composta pelos seguintes elementos (PELTIER, 2001):

- Agente que catalisa e executa a ameaça, podendo ser um indivíduo, uma máquina ou a própria natureza;
- Motivo que incentiva o agente a atuar, acidental ou intencionalmente e;
- Resultado que é o efeito causado pela execução da ameaça.

As ameaças estão intrinsecamente ligadas às vulnerabilidades. Schneier (2001, p. 27) afirma que: “As ameaças do mundo digital espelham as ameaças do mundo físico.” Em termos organizacionais, Bojanc e Jerman-Blazic (2008) mencionam que ativos de informações das empresas estão sempre expostos às ameaças. Complementam afirmando que ameaça é também qualquer evento em potencial com impacto indesejável.

Para reforçar o nível de proteção e estratégias de segurança, os bancos devem identificar claramente as ameaças que seus ativos de informações estão sujeitos e distribuídas entre diferentes meios como redes, softwares, dados ou infraestrutura física.

3.7.1 Ameaças sob o Ponto de Vista de Segurança da Informação

Do ponto de vista de segurança da informação, ameaça é definida como uma circunstância, condição ou evento com potencial de causar danos em dados ou recursos de rede, na forma de destruição, exposição, modificação de dados, negação de serviço, fraude, perda ou abuso (ALBERTIN; MOURA, 1998).

As ameaças de segurança de mensagem podem ser divididas em três categorias:

- **Confidencialidade de mensagem:** a confidencialidade é importante para a utilização que envolve dados sensíveis, tais como números de cartões de crédito. Este requisito será ampliado quando outros tipos de dados, tais como registro de empregados, arquivos governamentais e senhas dos clientes começarem a ser tratados no ambiente internet. A confidencialidade impede o acesso a tais informações ou a sua liberação para usuários não autorizados.
- **Integridade de mensagem e sistema:** as transações de negócio requerem que seus conteúdos permaneçam inalterados durante seu transporte. Em outras palavras, a informação recebida precisa ter o mesmo conteúdo e organização que a informação enviada. Enquanto a confidencialidade protege contra a monitoria passiva de dados, os mecanismos para integridade têm que prevenir os ataques ativos envolvendo a modificação desses dados.
- **Autenticação/identificação do emissor da mensagem:** A autenticação é um mecanismo pelo qual o recebedor de uma transação ou mensagem pode ter certeza da identidade do emissor e/ou da integridade da mensagem. Em outras palavras, a autenticação verifica a identidade de uma entidade, um usuário ou um serviço, utilizando certas informações criptografadas transferidas do emissor para o destinatário.

3.7.2 Meios de Propagação

Como já evidenciado anteriormente neste trabalho, as fraudes eletrônicas são um sistema complexo multibilionário, uma indústria global conduzida por gangues criminosas profissionais, altamente organizadas e sofisticadas. Seus meios utilizados para comprometimento das informações bancárias para darem início às fraudes são variados (BOJANC; JERMAN-BLAZIC, 2008).

Alguns esquemas de fraudes envolvem o roubo de identidade e credenciais. Este esquema busca a obtenção de dados pessoais da vítima como número de documentos pessoais, dados do cartão de crédito e senhas para acesso, objetivando a apropriação ilícita de recursos financeiros das vítimas (LAU, 2006). Os meios de propagação geralmente envolvem aspectos sociais e tecnológicos combinados.

Segundo Van Gool (2011), o meio de propagação descreve a maneira pela qual uma entidade é atacada. Esta pesquisa bibliográfica identificou três meios de propagação utilizados na realização de fraudes eletrônicas, conforme abaixo:

- **Engenharia social:** Seu principal objetivo é o de convencer o usuário e/ou cliente do banco de que o atacante é realmente uma entidade na qual o usuário confie, como seu banco por exemplo. Em um ataque de engenharia social, o usuário voluntariamente fornece informações vitais para o fraudador como senhas, dados do cartões de crédito e informações confidenciais, induzido por uma falsa sensação de segurança (THORNBURGH, 2004).
- **Falhas de segurança:** Como sistemas computacionais não são totalmente perfeitos podendo conter falhas de segurança passíveis de serem exploradas através de, por exemplo, softwares maliciosos, buscando capturar informações vitais sem o auxílio ou consentimento do usuário.
- **Invasão de canal via MITM:** este tipo de ataque é baseado na mesma premissa das falhas de segurança, porém é tratado de forma distinta pela natureza do ataque. Um ataque envolvendo a técnica “homem no meio” (*MITM, man-in-the-middle*), ocorre na conexão entre o cliente e o seu banco.

Todos os três meios de propagação mencionados acima realizam uma atividade que, a partir da perspectiva dos bancos, podem ser classificadas como roubo de identidade. Elenca-se no decorrer desta pesquisa uma série de afirmações referentes ao roubo de identidade. Hayward (2004) define roubo de identidade como posse ilegal de informações confidenciais e pessoais para fins ilícitos e/ou fraudulentos. Às vezes, o roubo de identidade é limitado às informações de clientes não bancarizados, ou seja, que não possui nível de acesso aos serviços financeiros, enquanto outros usam uma abordagem mais ampla que inclui qualquer tipo de informação de identificação pessoal.

Adicionalmente complementa-se à definição de roubo de identidade como um meio de fraude eletrônica, com ênfase principalmente em operações financeiras que envolvem bancos de varejo por possuírem grande capilaridade de agências e canais de relacionamento com os

clientes cada vez mais automatizados (FEDERAL TRADE COMMISSION, 2007; FINANCIAL FRAUD ACTION UK, 2010; INNOPAY, 2010).

Segundo relatório do NIC.BR (2011), engenharia social também pode ser compreendido como o termo utilizado para descrever um método de ataque, onde alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter dados sigilosos que podem ser utilizados para ter acesso não autorizado a computadores e/ou informações.

Em termos operacionais, quando o processo de roubo de identidade é realizado, os dados geralmente capturados podem variar de acordo com os canais, como o próprio Internet Banking, terminais de autoatendimento, call center, telefones celulares (smartphones), lojas de comércio eletrônico e mais recentemente através das mídias sociais. Como meio de captura, este tipo de roubo de dados pode ocorrer através de invasão, *phishing* ou uso de *malware*, ambos mencionados e definidos neste trabalho.

Na visão de Laudon e Laudon (2004), existe ainda o risco de ameaças de funcionários inescrupulosos comprometerem sistemas corporativos com o objetivo de vender informações a terceiros.

3.7.3 Métodos e Ferramentas

Para entender os controles de segurança que atenuam os riscos das fraudes eletrônicas é necessário, primeiramente, entender os diferentes métodos e ferramentas mais utilizados atualmente para captura de informações confidenciais dos clientes. Estes estão em constante evolução e são utilizados pelos fraudadores através dos métodos de ataques apresentados a seguir.

Phishing

Um dos métodos mais difundidos e de fácil aplicação é o *phishing* - a melhor tradução para este termo é pescaria, onde o fraudador envia e-mails não solicitados a vários clientes a fim de capturarem informações bancárias. Uma das maneiras na qual a parte que comete a fraude capitaliza e fomenta a insegurança na Internet é o roubo de identidade (MOORE, 2010), conforme já abordado neste trabalho. De acordo com NIC.BR (2012) *phishing* foi um termo originalmente criado para descrever o tipo de fraude que se dá através do envio de

mensagens não solicitadas, que se passa por comunicação de uma instituição conhecida, como um banco, empresa ou site popular, e que procura induzir o acesso à páginas fraudulentas, ou seja, falsificadas, projetadas para furtar dados pessoais e financeiros de usuários.

Atualmente, este termo (*phishing*) é utilizado também para se referir aos seguintes casos:

- Mensagem que procura induzir o usuário à instalação de códigos maliciosos, projetados para furtar dados pessoais e financeiros;
- Mensagem que, no próprio conteúdo, apresenta formulários para o preenchimento e envio de dados pessoais e financeiros de usuários.

Com a popularização e ampla utilização do Internet Banking, os bancos através de suas estratégias e campanhas de marketing têm impulsionado seus clientes a adotarem cada vez mais os serviços oferecidos no formato online devido à enorme redução de custos em comparação com a realização de transações nas agências físicas. Por outro lado, os meios de autenticação não mantiveram o mesmo ritmo.

Existe uma lacuna a ser analisado na transição dos padrões de utilização do modelo do banco tradicional com estrutura de agências para o digital com relação a segurança da informação e prevenção às fraudes (MOORE, 2010).

Ao utilizar um ataque de *phishing* o fraudador utilizando-se de telas falsas, se passa pelo banco e solicita informações confidenciais aos clientes infectados. Sites que utilizam desta técnica são normalmente anunciados via e-mails através de *spams*, que, supostamente dizem ser oriundas dos bancos (MCGLASSON, 2009).

Sob o ponto de vista de Jakobsson e Myers (2006) e no contexto bancário do termo, *phishing* pode ser descrito como: uma forma de engenharia social no qual o atacante tenta atrair o usuário, trazendo uma falsa sensação de segurança, a fim de obter suas principais credenciais, que podem ser usadas para envolvimento em uma transação financeira não desejada pelo usuário.

Como essa técnica requer ações dos usuários, é classificado como uma ameaça social no campo das fraudes eletrônicas. Desta maneira, como ocorre fora dos limites do sistema bancário, é classificado como uma ameaça externa.

Softwares Maliciosos

Software malicioso é um software projetado para explorar vulnerabilidades em outros programas. Podem também ser descritos como softwares que realizam ações ilegais imprevistos por um usuário que o executa, visando benefícios financeiros para seu distribuidor (EMIGH, 2006).

Este software pode se manifestar de muitas maneiras, como em um jogo online, cópia pirata dos softwares legítimos, ou talvez um cartão de felicitações eletrônico. Uma vez instalado, ele pode permanecer no computador da vítima por um longo tempo, passando por mutações e escapando de detecção por sistemas antivírus ao tentar roubar alguma informação com características bancárias (VAN GOOL, 2011).

Como alguns programas maliciosos tem a necessidade de explorar o psicológico das pessoas a fim de executar suas tarefas, os controles necessários para evitar o uso de softwares maliciosos precisam ser sociais também.

Existem inúmeros tipos de programas maliciosos, como cavalos de tróia, pragas virtuais, mecanismos de roubos de seção, entre outros. Além disso, uma distinção pode ser feita entre esses programas que executam o ataque e os que permitem outras formas de ataque pelo envio de *spam* ou disseminação de outros artefatos (VAN GOOL, 2011).

Nestes casos, o programa malicioso muitas vezes transforma o computador da vítima em um *botnet* (EMIGH, 2006), como será discutido posteriormente no parágrafo *Botnets*. Como softwares maliciosos existem fora dos limites do sistema bancário, estes são classificados como ameaças externas.

Man-in-the-middle

O termo homem no meio - *man-in-the-middle* - é o tipo de ataque onde os fraudadores invadem uma conexão existente para interceptar os dados trocados e injetar informações falsas no site do banco. Trata-se de mecanismos de escutas em uma conexão, interceptando mensagens, modificando dados e realizando transações não autorizadas pelo usuário.

Em um ataque desta natureza, a comunicação entre o usuário (cliente) e o servidor (banco) parece ser confidencial e correta, enquanto na realidade há um terceiro agente no processo (VAN GOOL, 2011). Uma visão geral dos diferentes tipos de opções de proteção contra esse tipo de ataque é dada em (OPPLIGER; RYTZ; HOLDEREGGER, 2009).

Em suma, o ataque acontece da seguinte forma:

- Ataque envolvendo usuário, geralmente cliente bancarizado, interagindo com o site do seu banco, o qual apresenta as mesmas características e informações do site da instituição, no entanto, é um website falso, projetado para coletar as informações pessoais e financeiras dos clientes.
- Ao mesmo tempo e de maneira imperceptível em segundo plano, um fraudador, que serve como um intermediário nesta conexão está recebendo os dados informados pelo usuário em tempo real no site original do banco, validando as credenciais e realizando uma transação mal-intencionada. Se o usuário for obrigado a oferecer uma autenticação adicional, o serviço do banco passará a solicitação ao usuário e será validado. Esses tipos de ataque podem parecer legítimos, mesmo ao usuário final mais experiente.

O aumento dos ataques *MITM* e de cavalos de tróia é ainda mais evidenciado pela maior demanda por programas maliciosos no mercado negro. A mercadoria é tão completa que os desenvolvedores até oferecem pacotes de atualização que incluem contratos de nível de serviço e suporte técnico para os compradores do submundo da fraude, e garantia de que, caso o tipo de programa se torne detectável pelos fornecedores de antivírus, será fornecida uma nova variante indetectável a um custo mínimo.

Oppliger, Rytz e Holderegger (2009) identificam três diferentes classes de ataques MITM:

- **Roubo de credencial:** nesse ataque, os usuários são atraídos por uma falsa sensação de segurança e, no processo, as informações da conta são obtidas pelo fraudador. Este é um subconjunto nas possibilidades de ataques de *phishing* discutido anteriormente.
- **Invasão de Canal:** neste tipo de ataque, o fraudador interrompe a conexão criptografada segura que existe entre o cliente e o banco. A partir desta posição, é capaz de apresentar ou capturar todas as informações que são transmitidas.
- **Manipulação de conteúdo:** o código malicioso na máquina do cliente manipula a informação transmitida entre o cliente e o banco em tempo real. Desta forma, um cliente pode visualizar as informações que foram alteradas e, que consequentemente perderam sua integridade.

3.7.4 Ferramentas Utilizadas para os Ataques

Uma série de ferramentas utilizadas para a efetuação das fraudes eletrônicas pode ser identificada a seguir. Estas servem como base para a realização das fraudes, mas não executam diretamente os ataques. A ampla divulgação, ações preventivas, sistemas de autenticação e monitoração de eventos no Internet Banking, dificultou sobremaneira o sucesso no roubo das informações e sua utilização para fins fraudulentos. Além disso, o aumento do conhecimento dos clientes sobre como se proteger das principais técnicas e ameaças como a correta identificação de um e-mail contendo *phishing* ou até mesmo a identificação do que poderia ser um roubo de identidade tornou mais difícil enganar clientes utilizando vetores tradicionais de ataques. Isso fez com que os fraudadores evoluíssem aumentando seu nível de sofisticação em diversas áreas, principalmente com a utilização da tecnologia da informação, desenvolvendo novas técnicas e atuando em novos canais de relacionamento com os clientes (mídias sociais).

Botnets

Uma *botnet* é uma rede de robôs, computadores que estão infectados com programas maliciosos controlados por indivíduos (VAN GOOL, 2011). *Botnet* é "o exército que responde à vontade do comandante" (ABU RAJAB et al., 2006). Essas ameaças estão intimamente relacionadas aos softwares maliciosos para envio de mensagens não solicitadas e sites falsos para computadores comprometidos. Os usuários muitas vezes não sabem que seu computador foi infectado.

Usuários online podem se infectar de diversas maneiras, conforme descrito a seguir:

- Seu computador não estiver devidamente protegido com antivírus e soluções de segurança, os fraudadores podem instalar programas maliciosos por meio de brechas de segurança.
- O software contendo o programa malicioso também pode ser enviado por anexos contendo links ou imagens incorporados em e-mails e no momento que o usuário acessa esse conteúdo, a *botnet* é instalada de forma despercebida pelo usuário.
- Finalmente, um usuário que não utiliza de sistemas antivírus atualizados, pode ser infectado apenas visitando um site ou fazendo download de arquivos infectados.

As redes de computadores robôs podem apresentar características sociais, pois

requerem ação humana e tecnológica para serem disseminadas. Como existem fora dos limites do sistema bancário, é considerada como ameaça externa.

Sua utilização é frequentemente usada para roubo de senhas bancárias online e comprometimento da atividade bancária e serviços corporativos. Este tipo de ferramenta é também utilizada para organizar os computadores infectados em uma rede organizada de ataques: uma rede de milhares ou mesmo milhões de computadores sob o controle de um atacante utilizada para realizar uma ampla gama de serviços (VAN GOOL, 2011).

Os serviços incluem o envio de mensagens indesejadas, publicidade online, hospedagem de programas maliciosos para realizar ataques de *phishing* com anonimato do tráfego durante sua realização. As redes de computadores robôs são diferentes das três categorias anteriores, porque representam um método de ataque, em vez de um alvo, podendo ser empregados em ataques direcionados a todas as três categorias.

Segundo Clark e Landau (2011), essas redes são tipicamente criadas para uma finalidade específica, que varia de acordo com as preferências do fraudador que está controlando o artefato.

Websites Falsos

Sites falsos facilitam certos métodos de ataques. Esses sites falsos tem o objetivo de atrair os usuários para coleta de e-mails para posterior envio de mensagens indesejadas, ou tentar induzir o usuário a realizar *download* de programas maliciosos sem sua real pretensão (VAN GOOL, 2011).

No entanto, sites falsos nem sempre são ameaças de natureza social. Uma vez que eles também são usados para comandar redes de computadores infectadas e controlada por indivíduos, eles também possuem um componente tecnológico. Além disso, existe a possibilidade de que estes sites falsos estejam hospedados, criados ou geridos sem ação humana. Portanto, esta ferramenta é ao mesmo tempo social e tecnológica. Como sites falsos existem fora dos limites do sistema bancário, estes são classificados como uma ameaça externa.

Spam

Segundo Van Gool (2011), spam é o nome dado a uma mensagem não solicitada enviada de forma massiva. Na maioria das vezes são e-mails, mas também podem incluir mensagens instantâneas, fóruns e redes sociais. Como já abordado anteriormente, *phishing* é um desses métodos e pode usar mensagens indesejadas para atingir este objetivo. Portanto, o spam é uma ferramenta para cometer fraudes eletrônicas.

Apesar de várias tentativas técnicas para filtrar mensagens indesejadas, este processo ainda não é muito confiável (DAMIANI et al., 2004; LUCA BECCHETTI, 2008). Redes de computadores infectados e programas maliciosos desempenham um papel importante na distribuição das mensagens. Como *spam* é enviado e lido fora dos limites do sistema bancário, é considerado uma ameaça externa.

Resumo do Panorama Geral das Fraudes Eletrônicas

O esquema abaixo resume os principais aspectos discutidos neste capítulo que envolve o desenho esquemático dos principais modelos, tipos de ataques, ameaças e ferramentas prevenção às fraudes utilizadas pelos bancos.

Desenho esquemático de Prevenção às Fraudes Eletrônicas

3.8 Riscos Associados aos Bancos

Segundo Pennathur (2001), com o crescimento de sites bancários transacionais, as agências reguladoras estão cada vez mais preocupadas com os riscos associados ao Internet Banking. O relatório de Supervisão Bancária do Comitê de Basiléia (1998, p. 1) afirma que a agência "reconhece que, juntamente com os benefícios, serviços bancários eletrônicos e atividades financeiras eletrônicas apresentam riscos para organizações bancárias, e esses riscos devem ser ponderados frente aos benefícios". Abaixo, uma revisão de alguns dos riscos inerentes aos serviços bancários online.

3.8.1 Gerenciamento de Riscos

A norma ISO (2009) define a gestão de riscos como um conjunto coordenado de atividades e métodos que são usados para direcionar uma organização a controlar os diversos riscos que podem afetar sua capacidade de alcançar seus objetivos.

De acordo com Adachi (2004), Greenstein e Feinman (2000), o objetivo do gerenciamento de risco é mensurar as incertezas e o potencial, positivo ou negativo, dos eventos futuros, para desenvolver uma estratégia de custo e eficiência que possam maximizar os ganhos. Na visão de Bessis (1998), o objetivo primário da gestão de risco é mensurar os riscos para monitorá-los e controlá-los. O gerenciamento de risco é um processo em que as organizações calculam, avaliam e decidem quais e em que nível de risco elas pretendem operar.

Culp (2002) e Bessis (1998) definem gestão de riscos: "Risk management is the process by which organizations try to ensure that the risks to which they are exposed are the risks to which they think are and need to be exposed to operate their primary business." (CULP, 2002, p. 199).

Risk management is both a set of tools and techniques and a process that is required to implement the strategy of a bank. It also includes all the management processes, and the organization design, required to implement efficiently the set of techniques and models, which deal with risk measurement and control. (BESSIS, 1998, p. 23)

Na literatura de gestão de riscos, uma série de termos novos é introduzida, os quais possuem relacionamento, porém ainda são muito distintos uns dos outros. Antes de discutir a prática da gestão de riscos no Internet Banking, estes termos e suas interações precisam ser

definidos.

De acordo com as normas ISO / IEC (2008), RFC 2828: *Internet Security Glossary* (SHIREY, 2000) e ISO / IEC (2004), os riscos são classificados conforme abaixo:

- **Ativo:** Qualquer coisa que tenha valor para a organização, suas operações de negócios e sua continuidade, incluindo recursos de informação que suportam a missão da organização (ISO / IEC, 2004).
- **Vulnerabilidade:** A fraqueza de um ativo ou grupo de ativos que podem ser exploradas por um ou mais ameaças que um ativo é qualquer coisa que tenha valor para a organização, as operações de seus negócios e sua continuidade, incluindo recursos de informação que suportam a missão da organização (ISO / IEC, 2008).
- **Ameaça:** uma causa potencial de um incidente que pode resultar em danos de sistemas e organização (ISO / IEC, 2008).
- **Segurança de controle (ou contramedida):** Uma ação, dispositivo, processo, técnica que reduz ou uma ameaça, uma vulnerabilidade, ou um ataque, eliminando ou evitando que ele, minimizando os danos que pode causar, ou por descobrir e denunciá-lo para que corretiva ação pode ser tomada (SHIREY, 2000).
- **Risco:** Uma expectativa de perda expressas como a probabilidade de que uma ameaça em particular irá explorar uma vulnerabilidade especial com um determinado resultado danoso (SHIREY, 2000).

A relação entre estes conceitos de acordo com Van Gool (2011) é a seguinte:

- **Vulnerabilidades** são falhas em componentes do sistema (incluindo seus usuários), que poderiam ser exploradas por uma ameaça. Sem uma ameaça, não há danos porque não há a exploração da vulnerabilidade. Se a vulnerabilidade for explorada, conduz a um resultado indesejável, que é o risco que a organização enfrenta quando se emprega o ativo. Note que este tipo de risco é fundamentalmente diferente do risco do negócio, que aponta para os assuntos financeiros de uma organização.
- **Controles (ou contramedidas)** são ações, dispositivos, procedimentos ou técnicas que podem ser implantadas para diminuir ou neutralizar a ameaça (ISO/IEC, 2004; ISO/IEC, 2008; SHIREY, 2000). No contexto dos riscos associados ao Internet Banking, é um conjunto de normas para orientar as organizações e os clientes na criação de controles e estruturas de controle com menores riscos de fraude a níveis aceitáveis. O nível aceitável de segurança é parte de um compromisso entre o nível de

segurança e o custo de sua efetivação. Camp (2000) classifica em três, as fontes básicas de risco: falha de segurança, mal uso de dados e falha na confiabilidade.

Os riscos bancários de acordo com Adachi (2004) e Marshall (2002) são classificados em três grupos:

- **Riscos estratégicos:** são os riscos vinculados ao tipo de estratégia que a empresa adotará para atingir os seus objetivos. A estratégia é montada com base em uma série de opções táticas, direcionadas para se atingir diversas metas, que levarão a empresa a alcançar o objetivo financeiro e mercadológico. Os riscos estratégicos podem ser internos ou externos. Os internos são: o tipo de arquitetura tecnológica a ser adotada; os segmentos de mercado a serem atingidos como público-alvo; ou até ao tempo de chegada ao mercado de seus produtos e serviços. Os riscos estratégicos externos são: pressões do mercado, como a concorrência e a dinâmica dos avanços tecnológicos; falta de agilidade para se adaptar a ambientes instáveis.
- **Riscos financeiros:** são os riscos associados às transações financeiras que uma empresa realiza. A precificação e a volatilidade cambial são exemplos deste tipo de risco. O risco financeiro também envolve a definição de limites financeiros e formas de transações.
- **Riscos operacionais:** são os riscos ligados à integridade dos processos de negócio, bem como à condição de fornecedor de produtos e serviços, de forma consistente e oportuna. Estes riscos são subdivididos em: risco de conformidade; de processos; de tecnologia e processamento de informações; de recursos humanos; de retidão e ética.

3.8.2 Gerenciamento de Risco no Internet Banking

A organização *Bank for International Settlements*, denominada de Comitê da Basiléia, órgão internacional que incentiva a cooperação entre bancos publicou um manual com os princípios de gerenciamento de risco para o Internet Banking (BASEL COMMITTEE, 2003).

Segundo Adachi (2004) os princípios desenvolvidos pelo comitê para gerenciamento de riscos no Internet Banking, estão classificados em três categorias:

- **Princípios de vigilância da comissão de diretoria e gerência sênior:**
 1. Gerenciamento efetivo das atividades de Internet Banking.
 2. Instituição de um processo de controle de segurança compreensível.

3. Planejamento minucioso da terceirização, com análise de consequências.

- **Princípios de controles de segurança:**

4. Autenticação dos usuários de Internet Banking.
5. Não repúdio e contabilização das transações realizadas pelo Internet Banking.
6. Medidas apropriadas para assegurar as obrigações de segregação.
7. Controle de autorização apropriado, dentro do sistema de Internet Banking, de Banco de dados e dos aplicativos.
8. Integridade dos dados de transações, registros e informações do Internet Banking.
9. Estabelecimento de um caminho de auditoria para as transações realizadas no Internet Banking.
10. Confidencialidade das informações importantes.

- **Princípios legais e de reputação do gerenciamento de risco:**

11. Apresentação apropriada dos serviços de Internet Banking.
12. Privacidade das informações do cliente.
13. Capacitação e plano de continuidade e de contingência do negócio para assegurar a disponibilidade do sistema e serviços de Internet Banking.
14. Plano de resposta para incidentes.

3.9 Redes Sociais

Para melhor entendimento sobre a evolução das redes sociais, é necessário realizar previamente um estudo do comportamento e definições de **SOCIEDADE** e **REDES**, ou seja, entender a perspectiva histórica e a representação desse modelo na transformação qualitativa da experiência humana.

3.9.1 Sociedade em Redes

De acordo com Castells e Cardoso (2006), a Sociedade em Rede, como a conhecemos atualmente, é o “conjunto de seres humanos que partilham interesses comuns, ligados por pontos e ferramentas que facilitam a comunicação e a partilha de experiências entre si. Nesta partilha coletiva, cada indivíduo rumo ao descobrimento da sua identidade individual e coletiva”.

A SOCIEDADE é formada por todos os seres humanos que ocupam um determinado espaço num determinado tempo. O espaço pode ser um país ou região, por exemplo, e o

tempo que, historicamente, pode ser bastante longo, mas que, sociologicamente ou estatisticamente, pode ser extremamente curto. Ainda há uma terceira dimensão a considerar, a dos traços de união entre os elementos, que podem ser os mais variados: família, vizinhança, trabalho, povoação de origem, origem étnica, opções políticas, país, etc.

Já a REDE é um conjunto de nós interligados por relações aleatórias que permitem o fluxo de informação. Abstraindo essa definição para a nossa sociedade, pode-se considerar que a primeira rede da qual fazemos parte é a família. Nesta, os nós são os familiares e todos eles se comunicam, trocam experiências e se ajudam para o bem comum. Outra rede que integramos é a escola. Aqui também há a comunicação e a troca de experiências que formam uma rede um pouco mais abrangente.

Deste entendimento de rede apresentado na esfera da vida privada (família, escola, entre outros) denota-se certa limitação, seja por espaço, tempo ou traços de união. Algumas dessas limitações poderão ser, no entanto, ultrapassadas através das tecnologias de informação e comunicação.

As sociedades sempre viveram em rede, ou em redes. No entanto, segundo Castells e Cardoso (2006), o avanço tecnológico proporcionou um aumento exponencial do efeito de rede, modelando a sociedade atual, na qual se insere a sociedade da informação e do conhecimento.

As tecnologias modernas, por exemplo, permitem a formação de redes informais e comunidades de aprendizagem cuja afinidade é o encontro num ambiente virtual. Da mesma maneira, as afinidades existentes ou geradas podem proporcionar a formação de redes porque o encontro de interesses semelhantes induz a procura dos meios de comunicação (ou tecnologias) adequados.

Ao somar SOCIEDADE + REDE encontra-se uma construção moderna, apesar de sociedade e de rede terem antecedentes que reportem ao passado. Percebe-se que o conceito Sociedade em Rede não é uma mera soma das partes e sim o resultado do equilíbrio das afinidades com as tecnologias, que permite e/ou mantém em comunicação, em tempo real, pessoas e grupos de pessoas independentemente da sua localização geográfica, tempo e traços de união.

Castells e Cardoso (2006) afirmam que a comunicação superou barreiras e em que a Internet e a Sociedade em Rede têm permitido a troca rápida de informação, bem como capacidade de processar e gerar conhecimento.

3.9.2 WEB 2.0 e o Universo dos Espaços Virtuais

A WEB 2.0 não é nenhuma revolução surpreendente, trata-se apenas da evolução natural da tecnologia e infraestrutura da Internet que possibilitou que os aplicativos funcionassem sob o modelo de computação em nuvem e que toda a comunicação pudesse ser feita em duas direções. Agora o usuário não precisa mais instalar fisicamente os aplicativos em seu computador pessoal, ou dispositivo equivalente, e espera-se que toda a comunicação se realize na forma de um diálogo. O *broadcast* tornou-se uma forma de comunicação considerada até mesmo como ofensiva. Musser e O'Reilly (2004) detalham cuidadosamente este ambiente.

Para desenvolver qualquer discussão sobre redes sociais é necessário, em primeiro lugar, expor algumas definições que servem como pontos cardeais neste novo universo de espaços virtuais. Estas definições são estabelecidas a seguir:

- **Rede Social:** é todo o conjunto de conexões no espaço real, ou virtual, que um determinado indivíduo estabelece em sua vida. Estas conexões devem se manter em um determinado momento no tempo.
- **Sites de Mídias Sociais:** são todos os aplicativos Web que servem apenas para espalhar uma notícia, uma opinião, ou seja, um conteúdo pequeno, fácil de ser compartilhado. Encaixam-se nesta definição Twitter, Youtube, Google+, Foursquare, LinkedIn, Blogs entre outros.
- **Aplicativos de Mídias Sociais:** são todos os aplicativos Web que suportam o diálogo, o compartilhamento de informações e a discussão de temas. Nesta definição estão o Facebook e o LinkedIn. A grande diferença para a identificação é que os sites podem ser colocados dentro dos aplicativos, mas o inverso é impossível.
- **Plataformas de Mídias Sociais:** são os espaços proprietários de organizações, ou grandes usuários, que possuem os atributos fundamentais da WEB 2.0. Um exemplo é o site da rede de televisão norte-americana CNN (www.cnn.com) que foi construído sobre uma plataforma de gestão de conteúdo. Solis e Thomas (2012) mostram o alinhamento destas definições.

As redes sociais são um conceito pré-estabelecido que se tornou uma realidade presente em uma velocidade surpreendente e colocam o consumidor como sujeito ativo nos processos comerciais. Barabási (2002) explica esta transição através da sua teoria das redes sem escala contrapondo ao modelo de redes aleatórias defendido por Erdos e Rényi (Watts,

1999 e 2003; Buchanan, 2002 e Barabási, 2003) e ao modelo dos mundos pequenos definido por Watts e Strogatz (Watts, 1999 e 2003). O modelo de Barabási (2002) discorda que os modelos de redes entre as conexões de indivíduos sejam aleatórios. Para ele há uma ordem dinâmica na estruturação das redes. De acordo com essa teoria alguns nós seriam altamente conectados enquanto outros teriam poucas conexões. Isso quer dizer que quanto mais conexões um nó possuir maior será a probabilidade de vir a ter mais ligações, denominando essa estrutura de ligação preferencial.

Um exemplo da teoria das redes sem escalas proposto por Barabási é a própria topologia da internet através do modelo de links utilizados pelo Google na indexação de suas páginas. Neste exemplo, os sites mais ricos, ou seja, com maiores números de conexões estão nos primeiros lugares nos mecanismos de pesquisas, aumentando sua probabilidade de ser visto.

Neste ambiente de rápida transição existem alguns parâmetros comprovados e que são fundamentais para entender o ambiente de negócios definido pelas redes sociais. Estes parâmetros são listados a seguir:

- As redes sociais expandiram o número de conexões ativas que cada indivíduo pode manter, superando o valor limite de 150 relacionamentos estáveis definidos para o ambiente real (MCCARTY et al., 2001);
- As redes sociais encurtaram as distâncias entre os indivíduos. Segundo Barabási (2002) duas pessoas quaisquer no planeta estarão separadas por uma média de seis graus de separação, significando pessoa que conhece uma pessoa que conhece uma pessoa;
- Os laços fracos, contatos que os indivíduos em uma rede social raramente veem e mal conhece, são mais valiosos para a resolução de crises do que os laços fortes. Por exemplo, em uma situação de desemprego, as melhores oportunidades surgiram mais rapidamente através dos laços fracos de uma rede social do que através dos laços fortes. Há um significativo número de trabalhos que exploram esta conclusão enunciada primeiramente por Granovetter (1973);
- Em cada conjunto demográfico, para uma determinada ação - campanha de marketing, desenvolvimento de um aplicativo, etc. - haverá tantas oportunidades, no mesmo grupo alvo, quantos forem os nichos estabelecidos no modelo de Cauda Longa. Este modelo estabelece as regras de negócio para comercialização de um grande número de itens únicos em quantidades relativamente pequenas. Aplicativos de comércio

eletrônico, sites, aplicativos e plataformas de redes sociais que a partir do modelo de negócio denominado Cauda Longa - *The Long-Tail*, Amazon.com e Netflix são os exemplos mais conhecidos (ANDERSON, 2006).

Há uma nova geração, *The Millenials*, daqueles nascidos entre 1977 e 1994 começando a atingir posições consolidadas de liderança no mercado de trabalho. Estes novos profissionais não conheceram um mundo onde o espaço virtual não tivesse importância significativa e, por isso, tem uma postura radicalmente diferente das gerações anteriores, com relação às Tecnologias da Informação e Comunicação. Esta atitude tem trazido mudanças significativas no ambiente profissional e nos parâmetros de consumo. Li (2010), Orihuela (2011) e Rossi (2011) alinham, em seus respectivos trabalhos os elementos desta discussão.

Estes elementos modificaram as regras do relacionamento humano e transformaram o mundo dos negócios, excluindo modelos antigos e trazendo novas oportunidades. No item a seguir esta afirmação é discutida detalhadamente, a partir da sequência de transformações pelas quais o marketing passou, em função da evolução das Tecnologias da Informação e Comunicação.

3.9.3 O Impacto das Tecnologias da Informação e Comunicação Sobre o Marketing

O Marketing, em sua função de definir o ambiente geral de negócios e suas regras básicas de relacionamento pode ser entendido como uma disciplina formal desde o final do século XIX, com o conceito de *the main street marketing*, onde prevalecia a personalização total de produtos e serviços. A partir desta idéia inicial, o Marketing entrou em um ciclo de evolução sempre influenciado pelas Tecnologias da Informação e Comunicação. Toda a inovação de ruptura destas tecnologias fez com que o ambiente de negócios e a definição de Marketing se modificassem significativamente. Este ciclo foi ilustrado por Alterian (2011), com a apresentação do *Marketing Capabilities Wheel*.

A Figura 4 mostra de forma linear a sequência de transformações do Marketing, em função de cada grande momento de ruptura das Tecnologias da Informação e Comunicação.

Figura 4 - O Marketing, segundo o Marketing Capabilities Wheel
Fonte: Alterian (2011)

Entender esta sequência é importante, pois o seu conjunto forma um ciclo que está se fechando e construindo o adjacente possível do *Social Marketing* integrado ao *Social Business* (JOHNSON, 2010). A primeira movimentação contemporânea das Tecnologias da Informação e Comunicação (TIC's) ocorreu com os serviços de correios e depois com o telégrafo e o telefone. Um novo conjunto de serviços inaugurou um novo estágio do Marketing denominado de Marketing Tradicional - *Traditional Marketing*, onde está concentrada a maior parte do nosso entendimento sobre o próprio Marketing (EDELMAN, 2010; GAINES-ROSS, 2010).

O marketing tradicional desenvolveu-se sobre a superposição dos conceitos de marketing direto, mídias de massa - jornais, revistas, rádio e televisão - e valorização da imagem. A consolidação de seu ciclo se traduz no paradigma da Gestão de Campanhas, onde o indivíduo, o contato humano e a personalização deixam de existir e passam a valer o conjunto e a massificação. A tecnologia digital levou a aceleração dos processos de

administração da informação, principalmente com os mecanismos de buscas (Bing, Google e Yahoo).

No marketing digital continuaram valendo as regras básicas do marketing tradicional, mas com energia concentrada na categorização dos indivíduos. Neste momento, torna-se fundamental poder classificar de alguma maneira cada indivíduo, podendo atribuir-lhe um grupo de identificação. Assim, a gestão de campanhas passou a dar lugar à gestão de programas, à captura de dados e à sua análise. A integração de todos estes atributos está levando a sociedade, neste momento, ao marketing social.

O *Social Marketing* ainda não se estabeleceu. Isto somente acontecerá no momento em que for possível coordenar a energia do WOM e a capacidade das comunidades de gerar conhecimento, monitorando-as para a realização do *syndication*. (BLACKSHAW, 2010; GAINES-ROSS, 2010; LI, 2010).

Syndication é uma expressão antiga relacionada ao trabalho de geração de conteúdo de um jornal ou revista, e significa poder entregar o conteúdo certo no momento certo. Ou seja, no *Social Marketing* o conteúdo passará a encontrar o usuário no momento em que este necessita. Em última análise é o fechamento do ciclo do Marketing, dentro de nossos adjacentes possíveis, levando novamente à personalização. Esta personalização é automatizada, sem contato humano, e significa identificar as necessidades de cada usuário em cada momento, sem deixá-lo preso a um perfil de consumo.

O *Social Marketing*, enquanto se desenvolve, leva à sociedade a um novo paradigma de modelo de negócio, principalmente em função das possibilidades de integração das informações e de acesso aos canais de comunicação das mídias sociais. Este novo paradigma é o *Social Business*. O *Social Business* pode ser entendido como o ponto de conexão entre os novos negócios que agregam, ao mesmo tempo, valor ao trabalho e à sociedade, a partir da implementação de novas soluções das tecnologias da informação e comunicação. A Figura 5 ilustra esquematicamente a relação entre o *Social Marketing* e o *Social Business*, a partir dos conceitos discutidos anteriormente sobre a configuração do *Marketing Capabilities Wheel*.

Figura 5 - A sobreposição do Social Marketing e do Social Business

(a) **Word of Mouth (WOM):** a tradução literal mais próxima desta expressão para uma língua latina seria viva voz. No universo virtual é todo o conjunto de diálogos orgânicos que ocorrem, a todo o instante, sobre os canais de comunicação disponibilizados pelas mídias sociais. A representação visual do *WOM* seria algo semelhante ao ruído branco que pode ser captado em qualquer antiga televisão analógica sem antena.

(b) **Análise:** o *WOM* irá existir por si só nas mídias sociais. O *Social Marketing* deve ser capaz de promover a análise desta quantidade incrível de informação e transformá-la em conhecimento.

(c) **Networking:** toda a informação e conhecimento gerado pelo *Social Marketing* irá formar uma rede de relacionamento social, destacando-se naturalmente os nós que possuem valor intrínseco. Para que isto ocorra, o *Social Business* deverá fornecer a infraestrutura necessária para que rede de relacionamento se estabeleça e encontre os caminhos necessários para alinhar os diferentes atributos relacionados aos valores de trabalho, sociedade e tecnologia. Será a capacidade de monitorar assertivamente este novo ambiente em busca de padrões, informações e conhecimento que irá revelar as oportunidades de negócio e possibilitar a extração de valor deste ambiente. Este ecossistema será formado pela união da capacidade dos mecanismos de buscas de classificar informação com a velocidade de disseminá-la e gerar conhecimento das mídias sociais. Esta é a real explicação para a união entre o Facebook e o Bing. (FACEBOOK ANNOUNCEMENTS, 2011; BARABÁSI, 2002).

(d) **Comunidades (Hivemind):** o *Social Marketing* deve se encarregar de formar as comunidades dentro do ecossistema proporcionado pelo *Social Business*. São estas comunidades que geram real valor dentro do universo social, pois é a partir delas que surgem insights alinhados aos possíveis adjacentes de nossos estágios de desenvolvimento econômico, tecnológico e social. O papel fundamental da teoria dos possíveis adjacentes proposto pelo cientista Stuart Kauffman nos processos de inovação revela que essa teoria como sendo um futuro espectral nas bordas do atual estado das coisas, um mapa de todas as maneiras segundo as quais o presente pode se reinventar. Ele não é, contudo, um espaço infinito, ou um campo de jogo totalmente aberto. O possível adjacente revela que a qualquer

momento o mundo é capaz de mudanças extraordinárias, mas apenas certas mudanças podem ocorrer (JOHNSON, 2010)

(e) **Syndication e Personalização:** É a partir do momento em que a estrutura de monitoramento fornecido pelo *Social Business* for capaz de identificar a necessidade de conteúdo de um usuário e entregá-la é que voltará a personalização, fechando o ciclo do *Marketing Capabilities Wheel*.

A interação das comunidades – *hivemind* - e o conteúdo entregue pelo *syndication* dá origem a um terceiro elemento: o *new social learning*. A interação entre estes três elementos, *Social Marketing*, *Social Business* e o *New Social Learning*, formam a estrutura do Mundo Social.

No presente trabalho de pesquisa não foi possível ainda identificar instituições da economia tradicional que de forma claramente consciente se alinhem a estas novas condições de mercado. Até mesmo no caso de instituições que atuam puramente na economia do conhecimento, mas longe da economia criativa, é difícil encontrar empresas que tenham estratégias completas de *Social Marketing* e o enxerguem como um caminho para o *Social Business*. No item a seguir serão apresentados os pontos fundamentais do impacto das redes sociais sobre as organizações.

3.9.4 O Impacto das Redes Sociais nas Organizações

A WEB 2.0 e suas redes sociais irão modificar as funções de negócio das organizações (LI, 2010; GAINNE-ROOS, 2010). De forma geral, estas modificações serão sentidas principalmente nos pontos enumerados a seguir:

- **Corporações mudarão a forma como se comunicam:** As redes sociais estão ampliando o acesso dos usuários a uma ampla gama de novas tecnologias e inovações na área das comunicações: multimídia, presença, interatividade, etc. Agora, os clientes não procuram somente o valor dos produtos, mas valores corporativos que façam sentido. Ser visível e ter comunicação personalizada são grandes prioridades, mesmo para empresas que fazem negócios entre si, denominadas de *business to business* (B2B) bem como a necessidade de abrir mão de alguns controles imagem;
- **Corporações vão mudar a sua visão:** As organizações serão mais transparentes, graças ao aumento do volume de informações disponíveis online, e os funcionários passarão a confiar mais na cultura empresarial e procura-la quando esta não estiver suficientemente explícita. Paralelamente, os interessados irão procurar prova de

responsabilidade social corporativa, inevitável pela transparência crescente. Eventualmente, empresas irão definir a sua estratégia de colaboração e comunicação unificada ao mais alto nível - a visão;

- **Corporações vão mudar a sua organização:** As organizações passarão, neste processo, a ter a opção de achatar a pirâmide organizacional para ganhar os benefícios de startups com sua adaptabilidade associada a rápidos modelos de crescimento. As consequências disto serão variadas, papéis e mutações de responsabilidade como resultado das redes sociais: gerentes terão de se adaptar e se tornar evangelistas de redes sociais; profissionais de gestão do conhecimento serão os arquitetos desta evolução e o grupo de tecnologia da informação precisará trabalhar de forma mais estreita e sinérgica com os Gestores de Conhecimento e usuários para permitir as novas aplicações;
- **Inteligência coletiva e experiência do cliente vão liderar a inovação:** Os diferentes modelos de inovação estão sendo testados, com destaque aos que dão ênfase ao pensamento coletivo. São famosos produtos e modelos de negócios desenvolvidos rapidamente através de ações colaborativas específicas. Com ciclos de vida de produto cada vez mais curtos, a empresa precisa capitalizar seus relacionamentos, em suas cadeias de valor, e antecipar as necessidades dos clientes. No entanto, este processo precisa de um grau maior de formalização.
- **Networking será a chave para a excelência do empregado:** Cada indivíduo ampliará seus horizontes globais, conforme os seus contatos tornam-se cada vez mais internacionais. Os recursos das redes sociais poderão ser utilizados para ganhar maior profundidade de conhecimento em suas áreas de interesse. Desta forma, será possível ter acesso a múltiplos conselheiros e mentores, além da informação bruta. As redes sociais, em última análise, são ferramentas de autodesenvolvimento que podem ser usadas a qualquer hora, a partir de um terminal móvel.
- **A Mobilidade dos funcionários vai aumentar:** Como funcionários aumentam a sua visibilidade e tornam sua experiência disponível para as comunidades, dentro ou fora de suas organizações, eles serão mais frequentemente solicitados. Isso também irá acontecer à medida que cresce o número de contatos online que mantêm desde que estas ligações sejam significativas.
- **As organizações terão que modificar seus sistemas de motivação e planos de carreira:** Para fazer com que os funcionários participem do trabalho colaborativo, as

corporações terão de adaptar os seus sistemas de motivação. Eles também terão que encontrar dentro da empresa ou externamente os melhores animadores, que valorizam a essência das novas ferramentas. Por último, eles precisam desenvolver as motivações da comunidade e recompensas, além de apenas localizar indivíduos alvo. Quanto à carreira, tornar-se um *blogueiro* de negócios, por exemplo - será reconhecido como uma experiência específica complementar e caminhos de especialistas vão se tornar mais abertos por conta das novas ferramentas que ajudam os indivíduos a se tornarem visíveis e conhecidos dentro da comunidade com o mínimo de barreiras possíveis. E a excelência continuará a ser o ingrediente para o sucesso.

- **Aplicações de tecnologia da informação e comunicações terão mutação:** Alguns resultados já serão visíveis: diretórios corporativos irão se tornar aplicações ricas, não necessariamente comparáveis às redes sociais como o LinkedIn ou Facebook, mas provavelmente com semelhante nível de capacidades; intranets serão personalizáveis e características de presença vão invadir quase todas as aplicações.
- **Adoção corporativa acontecerá em velocidades diferentes:** Algumas empresas vão adotar ferramentas de redes sociais e seus benefícios mais rápido do que outras. Vários gatilhos e aceleradores vão ajudar a prever como cada empresa irá agir e diferentes modelos de redes sociais corporativas vão surgir: gestão do conhecimento, desenvolvimento de negócios, integração e consolidação da marca.
- **Redes sociais podem permitir maior receita:** Como resultado das alterações na comunicação e inovação, a empresa será mais visível e acessível a seu mercado.

Adotar uma estratégia de redes sociais pode, ainda, permitir:

- I. Conversão de marketing direto e anúncios de estáticos para dinâmicos, para melhores perspectivas;
- II. Lançamento mais rápido de novos e melhores produtos;
- III. Transformação do sistema de relacionamento com o cliente (CRM) em personalização do contato e reconexão dos serviços online e centrais de relacionamento para uma melhor experiência e retenção.

E por último, mas não menos importante, redes sociais podem permitir que as empresas identifiquem novos mercados e desenvolvam novas práticas de marketing. O

Internet Banking enquadra-se perfeitamente nesta categoria e tem se transformado rapidamente em um *Social Business* (ROZWELL, 2011; 2012; SKINNER, 2012).

A seguir são apresentados os elementos que caracterizam o Internet Banking como um *Social Business*.

3.9.5 A Estrutura do Social World e o Social Business

A evolução da infraestrutura da Internet em praticamente todas as nações do globo, a consolidação do conceito WEB 2.0 na vida diária de todos e a configuração dos mais diversos tipos de canais sociais, as chamadas mídias sociais, se alinharam para formar um novo espaço de discussão dos problemas sociais. Um novo Ágora (1) surgiu e evoluiu a partir dos atentados aos trens de Madrid em 2004; ganhou destaque a partir da Primavera Árabe e consolidou-se em movimentos como o M-152 e Occupy Wall Street (ROSSI, 2011; ORIHUELA, 2011).

De toda esta movimentação surgiu um novo paradigma de relacionamento entre as instituições e os indivíduos com os quais estas se relacionam: a idéia de fazer tudo pelo povo, mas sem o povo, não existe mais, o que vale é fazer com o povo (ROSSI, 2011). Em outras palavras, toda a vez que uma instituição assumir unilateralmente a responsabilidade de se expressar em nome de um grupo de indivíduos, ou até mesmo de uma população, irá correr o risco de ser desautorizada e perder a sua credibilidade. Um exemplo completo deste novo paradigma é a matéria jornalística, Nocauteados Pela Lógica, publicada pela Revista Veja (ELER; DINIZ, 2011).

O estabelecimento deste novo Ágora talvez seja o evento de ruptura essencial para disparar a transição entre os Séculos XX e XXI, como sempre ocorreu na história moderna (HOBBSAWN, 1998). Alinha-se desta maneira os três conceitos em constante evidência neste momento de transição social: o *Social Marketing*, o *Social Business* e o *New Social Learning*.

O conceito de *Social Marketing* já foi discutido nos itens anteriores do presente trabalho, onde o *Marketing Capabilities Wheel* de Alterian (2011) se destaca. Uma proposta de definição do *Social Business* é dada por Dachis et al. (2009, p.), que diz:

Tecnologia, trabalho e sociedade estão se modificando em velocidades nunca vistas antes. Negócios que procuram criar e capturar valor a partir destas mudanças devem aproveitar as oportunidades na interseção destes três elementos, que é o ponto focal do *Social Business*.

O *New Social Learning* abre os adjacentes possíveis para que as organizações encontrem o caminho da comunicação, que não pode mais ser apenas de cima para baixo, mas sim em fluxo contínuo como em um organismo vivo (BINGHAM; CONNER, 2011). A Figura 6 a seguir foi adaptada de Dachis et al. (2009) e mostra esquematicamente o alinhamento de todos estes elementos discutidos até o momento e que formam o Mundo Social composto pelo: Ágora Virtual, o Trabalho, a Sociedade, as Tecnologias da Informação e Comunicação, o *Social Business*, o *Social Marketing* e o *New Social Learning*.

No entanto, esta visão leva a uma simplificação exagerada da interação entre os movimentos envolvidos. Este é um fato que acontece com certa frequência nas discussões sobre as dinâmicas do universo virtual. Por exemplo, a planificação do funil de compra apresentada por Edelman (2010) contrasta com o *Conversation Prism* de Solis e Thomas (2012). O prisma de conversação busca apresentar as atividades de ouvir, aprender e compartilhar nos canais de mídias sociais como um fluxo de conhecimento contínuo. Em suas publicações posteriores, Brian Solis trata deste aspecto inerente às mídias sociais (SOLIS, 2010).

Figura 6 - O Ágora Virtual e a configuração do Mundo Social.

Assim, para buscar a explicação correta sobre a interação dos elementos que formam o “Mundo Social”, no presente trabalho modificou-se esta visão cartesiana em um modelo tridimensional (Figura 7), onde o “Mundo Social” se estabeleceu a partir da constituição do novo Ágora sobre a Internet e sua infraestrutura cada vez mais robusta, bem como seus aplicativos e WEB 2.0. Este novo ambiente atraiu o marketing e os profissionais que gravitam ao seu redor, que tentaram iniciar um novo paradigma: o *Social Marketing*.

Figura 7 - A configuração do Mundo Social.

As iniciativas neste momento do *Social Marketing* ocorreram apenas sobre o *Word of Mouth* (WOM), o que gerou uma coleção de casos de *antimarketing*, sem enxergar os outros elementos que configuram o *Social Marketing* como a base do *Social Business*: monitoramento, comunidades e *syndication*.

O *Social Business* é a utilização destes quatro elementos sobre os espaços da vida cotidiana atual na busca e captura de valor. No modelo, estes elementos são direcionados pelo estado de maturidade das Tecnologias da Informação e Comunicação, das necessidades do Mercado de Trabalho e o grau de interação das Redes e Comunidades da Sociedade Moderna.

A visão cartesiana do Mundo Social, como discutida ao redor da Figura 7 pode ser observada na tendência de transformação dos produtos e serviços bancários na direção do *Social Banking*, discutida por Skinner (2012). Já o histórico de trabalhos de Rozwell (2011; 2012) mostra a modificação em torno do modelo de Mundo Social apresentado na Figura 7.

O elemento restante no modelo proposto de Mundo Social é o *New Social Learning*, que é o momento onde as comunidades formadas nestes espaços passam a atuar em conjunto para a resolução de seus dilemas sociais.

A fraude bancária entra exatamente neste ponto, ao observarmos o *Social Banking* como um modelo de *Social Business*. A seguir serão discutidos os termos específicos da caracterização da fraude bancária como um dilema social e a sua influência no *Social Banking*.

As Fraudes Bancárias como Social Business

Essencialmente, a fraude bancária pode ser entendida como um *Social Business*, pois, como descrito anteriormente utiliza os quatro elementos fundamentais do *Social Marketing* alinhados pelos três fatores direcionadores da vida cotidiana atual, como apresentado no modelo de Mundo Social da Figura 7.

Antes de demonstrarmos as fraudes como *Social Business*, é importante elencarmos alguns pontos essenciais que demonstram fases pelos bancos em direção ao *Social Banking*.

Sob o ponto de vista tradicional, a fraude bancária na Internet pode ser vista como um jogo de números. Grupos exageradamente grandes de vítimas em potencial são atacados, mas a taxa de sucesso resultante sempre foi marginal (FEDERAL TRADE COMMISSION, 2008). Neste contexto, segundo Van Gool (2011), a realização de todos os tipos de controles de segurança e verificação é de responsabilidade, principalmente, dos usuários. É nesta lacuna que pode ocorrer o comprometimento das credenciais dos usuários e os fraudadores encontram espaço para agir sobre o sistema de Internet Banking.

Ainda, sob a visão tradicional expressa por Van Gool (2011), a ação de fraude sobre o Internet Banking poderia ser classificada sob dois pontos de vista:

- **Fraudes através da combinação de hardware e software:** os ataques são realizados sem ação direta do usuário. Esta classificação não exclui os ataques que foram possíveis pela ação humana indireta. Um exemplo das ações humanas que indiretamente causam fraudes eletrônicas é a instalação acidental e/ou por desconhecimento dos usuários de softwares maliciosos que, uma vez acionados, executam o ataque.
- **Fraudes através da combinação de hardware, software e usuário:** estes são os métodos que fazem uso de hardware e software para executar seus ataques, mas também exigem ação direta do usuário. Um exemplo é o *phishing*, onde o usuário é induzido a inserir manualmente as informações de sua conta em um aplicativo web falso.

Neste caso há duas combinações que devem ser levadas em conta e que são importantes em relação à discussão geral do presente trabalho:

- **O componente social é o menos importante:** Por se tratar de uma ameaça tecnológica, há uma falha clara de segurança no sistema onde a fraude ocorrerá com ou sem a participação do usuário.

- **O componente social é o mais importante:** ocorre fundamentalmente sobre uma fraqueza/abertura do usuário, com ou sem a ajuda de um componente tecnológico.

O *phishing* é um exemplo claro desta combinação, pois o atacante tenta atrair o usuário, trazendo uma falsa sensação de segurança, a fim de obter suas principais credenciais, que podem ser usadas para envolvimento em uma transação financeira não autorizada (JAKOBSSON; MYERS, 2006). Isto pode ser feito de diversas formas, desde a forma tradicional explicitada pelo *Federal Trade Commission* (2008), ou em ações individuais que, sob a visão de Moore (2010) tem recebido pouco interesse das organizações bancárias. As diversas estratégias de *phishing* relatadas por Mcglasson (2009) confirmam esta afirmação.

Ou seja, as organizações bancárias preocupam-se apenas com as ocorrências em larga escala que podem lhe causar prejuízos significativos em um curto espaço de tempo. A fraude no Internet Banking que ocorre sob um componente social dominante e não somente no tecnológico não é devidamente observada (FINANCIAL FRAUD ACTION UK, 2010; GOVCERT.NL, 2010). Trabalho como o de Rozwell (2011; 2012) mostra que esta tendência está se modificando, pois o modelo de Social Business tem ganhado cada vez mais importância para os serviços e produtos bancários.

3.9.6 Presença Social

Com o objetivo de adicionar argumentos para a construção do modelo teórico-referencial para prevenção às fraudes eletrônicas em bancos é necessário expor e contextualizar o conceito e significado de presença social.

As redes de comunicação são ambientes sociais. A sua evolução depende de duas dimensões: tecnológica e social. A capacidade física de transportar dados e convertê-los rapidamente em informação são os aspectos fundamentais da tecnologia. A dimensão social, no entanto, é mais complexa de ser entendida. Sucessivamente, acompanhando a evolução tecnológica, tem-se apresentado gerações de interfaces para mediar a comunicação social, sendo que pode-se visualizar claramente neste processo evolutivo a busca progressiva para melhorar a comunicação humana, principalmente, para o trabalho colaborativo, a educação, serviços sociais e, com grande significado econômico o comércio eletrônico.

Respectivamente, Weiming (2001), McNaught (2002), Kehrwald (2007) e Li, Daugherty, Biocca (2001) demonstram esta progressão, em cada uma destas áreas, de forma precisa e com exemplos de desenvolvimento de sistemas nas seguintes áreas:

- Ambientes de trabalho colaborativo;
- Comunicação móvel;
- Interfaces de banda larga para teleconferência;
- Agentes especialistas em e-commerce e interfaces de ajuda;
- Interfaces de reconhecimento do discurso e fala; e
- Ambientes virtuais sociais em 3 dimensões (3D).

O trabalho de Short, Williams e Christie³ (1976 apud KEIL; JONHSON, 2002, p. 20-26) é citado frequentemente como sendo o precursor do termo “presença social”, que é definida como uma qualidade subjetiva de um meio de comunicação e deriva do conceito psicológico de intimidade (determinada pela distância física, contato com os olhos, sorriso e tópicos pessoais de conversação) e imediatismo (determinado pela capacidade do meio de informação de transmitir informação). Assim, entendendo-se estes dois componentes da presença social (verbal e não-verbal), os meios de comunicação que conseguem entregar informações não-verbais terão maior presença social.

Este conceito foi amplamente aplicado nas discussões sobre a satisfação do aluno nos processos de educação à distância e desdobrado no desenvolvimento de sistemas em todas as áreas citadas logo acima. Anderson (2001) constrói um significado interessante para esta questão, mostrada na Figura 8.

³ SHORT, J., WILLIAMS, E., CHRISTIE, B. (1976). **The social psychology of telecommunications**. Toronto: Wiley.

Figura 8 - Representação da visão de Anderson (2001) sobre a presença social

A evolução do patamar tecnológico das Tecnologias da Informação e Comunicação (TIC's) e a transição para uma nova dinâmica social, onde a colaboração toma o lugar da livre iniciativa na construção da reputação tornou, hoje, um meio virtual (WEB) mais efetivo e pessoal do que as formas tradicionais para a percepção da presença social. Principalmente, em função da maximização do efeito do imediatismo das mídias sociais que está transformando o conceito de presença social em rede de relacionamento social segundo Downes (2006).

4 RESULTADOS

Este capítulo apresenta os resultados a partir da pesquisa qualitativa e da literatura acadêmica que resultaram no modelo proposto para essa pesquisa. Inicialmente, na Seção 4.1 é apresentado a etapa da construção do modelo de presença social. A Seção 4.2 refere-se à interpretação do modelo e na Seção 4.3 refere-se à análise dos resultados através da aplicação deste modelo em quatro bancos brasileiros.

4.1 Modelo de Presença Social Proposto pela Pesquisa

A construção do modelo teórico (mapa) de presença social proposto pela pesquisa para os serviços e produtos relacionados ao Internet Banking foram baseados em informações do banco de investimentos americano denominado **LUMA PARTNERS** e do **Prisma de Conversação – *The Conversation Prism*** - demonstrados e definidos a seguir.

O LUMA PARTNERS é um banco de investimentos norte-americano especializado em consultoria estratégica para as empresas que desenvolvem sites, aplicativos ou plataformas de mídia social que se destaca por traduzir o desenvolvimento empresarial de seus clientes para os parâmetros usuais do mercado financeiro.

Como resultado, este trabalho passou a compilar mapas que buscam trazer alguma ordem ao complexo ecossistema das mídias sociais. Tornaram-se claros referenciais desta indústria quando se deseja entender o ambiente de negócios das mídias sociais em seus nove setores chaves demonstrados pelos modelos de negócios do LUMA Partners, distribuídos em: *Display, Search, Video, Mobile, Social, Commerce, Gaming, Digital e Strategic Buyer*.

No contexto desta pesquisa, o mapa que trata do ecossistema do Social Business (Social LUMAScape) (KAWAJA, 2012) é de especial importância. No mapa **Social LUMAScape**, é possível visualizar em pequenos grupos, ferramentas e soluções que envolvem o ecossistema das mídias sociais, apresentado na Figura 9.

Social LUMAScape – Representação do ecossistema envolvendo as ferramentas de mídias sociais.

Figura 9 - Social LUMAScape

Este mapa é o ponto de partida para a elaboração da metodologia de avaliação do grau de presença dos bancos no universo das mídias sociais. No entanto, da forma com que é apresentado inicialmente é difícil visualizar seus eixos de orientação. Para facilitar esta visualização, primeiro, destacam-se os elementos genéricos principais deste mapa. Isto é apresentado na Figura 10.

Figura 10 - Social LUMAscape (KAWAJA, 2012) modificado para melhor entendimento do tema

Na sequência, utiliza-se o Prisma de Conversação de Solis e Thomas (2012), apresentado na Figura 11 abaixo, evidenciando o alinhamento dos sites, dos aplicativos e das plataformas de mídia social para o trabalho de marca (*branding*), demonstrado ao centro do infográfico. O Prisma de Conversação oferece uma visão geral do universo das redes sociais, categorizadas e organizadas também pela forma como as pessoas utilizam cada rede. Uma síntese gráfica de todos os sistemas de interconectividade existentes e que vem surgindo na Web.

Figura 11 - Conversation Prism de Solis e Thomas (2012)

resultado gerado através de um modelo de avaliação do grau de presença no universo das mídias sociais. Este modelo é estruturado em quatro eixos de atuação conforme descrito anteriormente (**vendas, marketing, suporte e comunidades**). Para fins dessa pesquisa, utilizou-se o modelo Social LUMAScape para coletar dados e avaliar a estratégia social dos bancos para transformar o Internet Banking em um *Social Business*, com diferentes graus de imunidade contra fraudes eletrônicas. Por apresentar uma estrutura abrangente em sua característica de avaliação e identificação de canais, esse modelo pode ser adaptado e evoluído para analisar graus de presença social em diferentes negócios. Dessa maneira, estratégias podem ser desenvolvidas de acordo com o tipo de negócio analisado, utilizando-se critérios específicos no preenchimento e ponderação dos resultados.

Neste trabalho utilizou-se o modelo Social LUMAScape para delinear a estratégia e objetivo, ou seja, procurou-se identificar o universo das mídias sociais através desse panorama referencial para construção do mapa de avaliação aplicado à Bancos, objetivando entender os transformação do Internet Banking em um Social Business.

A definição esquemática das cores do modelo de avaliação de presença social foi desenvolvida por meio da análise da figura 7. Utilizou-se como premissa os elementos que compõem o Mundo Social, composto pelo Ágora, o Trabalho, a Sociedade, as Tecnologias da Informação e Comunicação, o *Social Business*, o *Social Marketing* e o *New Social Learning*. Dessa forma, foi realizado uma correlação entre o ambiente da figura 7 com o prisma de conversação de SOLIS (2011), figura 11 e com o LUMAScape de KAWAJA (2012), figura 9, identificando em cores as estratégias de curto, médio e longo prazos, apresentado no modelo deste trabalho.

Quadro avaliativo de presença social

Figura 13 - Grau de avaliação social de um negócio

A fim de exemplificar o modelo acima proposto, se uma empresa deseja implantar a função de **Vendas** no mundo social com objetivo apenas de curto prazo esta deve estruturar sua estratégia no Twitter e no máximo desenvolver aplicativos para este *microblog*. Desta forma a empresa que preencher todo o quadro terá a sua presença social completa, em todas as funções e com objetivos (resultados) que são obtidos em curto, médio e longo prazo, evidenciados nos diferentes tons das cores, ou seja, quanto mais claro, maior a eficiência da ação no curto prazo.

4.2 Interpretação do Modelo de Presença Social

O quadro avaliativo de presença social foi concebido inicialmente com quatro eixos: Venda, Marketing, Suporte e Comunidade. Sendo que cada um tem uma escala de intensidade/profundidade. Por exemplo, no eixo **VENDAS**, o nível mais simples ou mais

próximo do cliente é o Twitter. A explicação do motivo pelo qual o Twitter ocupa essa posição foi desenvolvida e estruturada nos itens anteriores do presente trabalho, assim como todos os pontos restantes.

A presença total ou preenchimento total do quadro representa uma estratégia coesa e planejada com antecedência, já um preenchimento aleatório significa falta de planejamento e/ou conhecimento sobre a estruturação de uma relação social B2C (*business to consumer* ou entre a instituição e seu usuário).

A estratégia aparente de cada banco pode ser avaliada a partir do seu URL principal, que, usualmente, concentra os principais links para os seus canais de mídias sociais. Estes níveis de interação mais próximos do usuário levam à avaliação total da presença social de cada banco. No entanto, nos níveis mais distantes, a avaliação estrutural pode ser prejudicada pela política de acesso de cada banco.

Seleção dos Bancos

Nesta pesquisa, utiliza-se a matriz proposta como modelo teórico de presença social como referencial para apresentar por meio de pesquisas online os resultados de dados coletados de quatro bancos múltiplos aleatórios (que possuem operações de segmento varejo e de investimentos). Os critérios sugeridos para a escolha da seleção foram analisar três bancos privados (não controlado pelo Governo) e um controlado pelo Governo. Todos os bancos analisados oferecem uma ampla gama de produtos e serviços bancários e financeiros no Brasil e no exterior. Possuem amplas redes de agências, presença no Internet Banking, postos de autoatendimento (caixas eletrônicos) e serviços abrangendo grandes bases de clientes em diversos segmentos.

Todos apresentam rede de conveniência e atuação em larga escala em todo território nacional, sendo denominados para essa pesquisa como sendo: **Banco 1**, **Banco 2**, **Banco 3** e **Banco 4**, respectivamente.

4.3 Levantamento e Análise dos Dados de Presença Social

O levantamento dos dados foi efetuado seguindo os procedimentos metodológicos sugeridos para esse trabalho, de forma qualitativa e descritiva, utilizando como fonte de dados os próprios sites institucionais dos bancos e por meio de diversas plataformas de mídias sociais objetivando identificar e contextualizar os dados coletados em função da presença

social apresentado pelo modelo proposto neste trabalho, conforme figura 14.

Além dos próprios websites dos bancos, mencionados acima, as plataformas de mídias sociais utilizadas para análise nesta pesquisa foram:

- Facebook (www.facebook.com)
- LinkedIn (www.linkedin.com)
- Youtube (www.youtube.com)
- Twitter (www.twitter.com)
- Google+ (plus.google.com)

Os dados foram coletados de fontes externas e por meio de pesquisas online de modo que a visão e análise finais estão baseadas em resultados onde foi possíveis identificar alguma presença social nas plataformas pesquisadas nos quatro eixos: **VENDAS, MARKETING, SUPORTE e COMUNIDADE**. Isso não quer dizer necessariamente que os bancos não possam ter mais aderência e estratégia social internamente por outras funções como monitoramento, *blog* corporativo, entre outras, que não estão explícitas aos métodos de coleta de dados propostos dessa pesquisa. Estratégias e plataformas de mídias sociais corporativas que não estejam diretamente envolvidas e divulgadas ao usuário final (clientes) não estão consideradas neste trabalho.

Por meio dos levantamentos das variáveis que compõem o mapa de avaliação e presença social, identificou-se uma similaridade nos padrões de resultados entre os bancos selecionados. Os bancos analisados estão presentes e atuantes em pelo menos quatro plataformas de mídias sociais, entre elas o Facebook, YouTube, Twitter e o Google+.

Nesses canais foram possíveis identificar ações de marketing, relacionamento e conscientização sobre prevenção às fraudes e divulgação de medidas preventivas para golpes utilizando Internet Banking, cartões de crédito e em caixas eletrônicos, o que demonstra que os bancos perceberam o potencial que esses canais podem trazer na gestão do relacionamento e conscientização dos clientes.

Abaixo análise dos dados pesquisados nos bancos propostos:

1. Levantamento dos dados de presença social do Banco 1

Venda		Marketing		Suporte		Comunidade	
#	ação	#	ação	#	ação	#	ação
✓	twitter	✓	facebook		social ad networks	✗	social intelligence
✓	twitter APPS	✓	facebook gaming			✗	social business software
✗	content curation	✓	facebook APPS	✗	social scoring	✗	external (costumer) facing internal (employee) facing
✗	stream platforms	✗	social commerce platforms		social data	✗	social scoring
✓	analytics	✓	social brand engagement	✗		✗	blogging platforms
✓	URL shortners				social tv	✓	social/mobile APPS & games
✗	social promotion platforms		social advertising platforms	✓		✓	community platforms
✗	social publishing platforms	✗		✓	social search & browsing	✓	social shopping/referral plug-ins/widgets
✓	social marketing management			✓	plug-ins/widgets	✗	content & photo sharing traditional publishers

Figura 14 - Análise dos dados do Banco 1

O **Banco 1** apresenta, principalmente no eixo **VENDA**, estratégia de média atuação, ou seja, fundamentada basicamente no aplicativo Twitter e na utilização de redutores de URL. No eixo **MARKETING**, a atuação é mais presente, porém centralizada em plataformas como o Facebook para fins de engajamento com seus clientes e com sua marca. Com relação aos eixos **SUPORTE** e **COMUNIDADE**, apresenta elementos de destaque em *Social TV* fundamentada no YouTube, divulgando vídeos sobre produtos, investimentos e também em aplicativos utilizados em smartphones e *tablets*.

Este banco foi o que apresentou o primeiro canal de acesso a contas correntes pelo Facebook, ou seja, o processo de acesso a conta corrente é internalizado dentro do aplicativo, sendo possível realizar operações financeiras permitindo consulta a saldo, investimentos e limites de crédito; transferências entre contas do banco; pagamentos de boletos de cobrança e recarga de celular. Segundo levantamentos da empresa ComScore, já são cerca de 37 milhões de brasileiros no Facebook em 2012.

Foi possível também constatar a interação de caráter de relacionamento, tirando dúvidas sobre questionamentos dos usuários, além de colaborar com dicas de planejamento financeiro além de publicar informes com relação aos elementos que compõem os riscos associados à má utilização das mídias sociais, inclusive dicas de como utilizar os caixas eletrônicos e cartões de crédito com segurança, ou seja, reforçando mensagens inicialmente disponibilizadas em seu site institucional.

2. Levantamento dos dados de presença social do Banco 2

Venda		Marketing		Suporte		Comunidade	
#	ação	#	ação	#	ação	#	ação
✓	twitter	✓	facebook		social ad networks	✗	social intelligence
✓	twitter APPS	✗	facebook gaming	✗		✗	social business software
✗	content curation	✓	facebook APPS	✗	social scoring	✗	external (costumer) facing internal (employee) facing
✗	stream platforms	✗	social commerce platforms	✗	social data	✗	social scoring
✓	analytics	✓	social brand engagement	✗		✗	blogging platforms
✓	URL shortners			✓	social tv	✓	social/mobile APPS & games
✗	social promotion platforms	✗	social advertising platforms	✓		✓	community platforms
✓	social publishing platforms			✓	social search & browsing	✓	social shopping/referral plug-ins/widgets
✓	social marketing management			✓	plug-ins/widgets	✗	content & photo sharing traditional publishers

Figura 15 - Análise dos dados do Banco 2

A estratégia de presença social do **Banco 2** foi semelhante a adotada pelo **Banco 1**, ou seja, também apresentou um posicionamento mais relevante no eixo **VENDAS** fundamentada basicamente no aplicativo Twitter e na utilização de redutores de URL. No eixo **MARKETING**, a atuação é presente, centralizada em plataformas como o Facebook com grande interação entre os clientes e público em geral através de linguagem comum às redes sociais. Por outro lado, não foi possível identificar informações de conscientização e dicas de segurança na utilização dos canais de atendimento e produtos. Com relação aos eixos **SUPORTE** e **COMUNIDADE**, apresenta também elementos de destaque em *Social TV*

fundamentada no YouTube e em aplicativos utilizados em smartphones e *tablets*.

Embora esse banco também exerça um canal de comunicação atuante com seus clientes principalmente com apelo social e sustentável, não foi identificadas evidências na utilização e divulgação de dicas de segurança com caráter informativo para seus clientes e público em geral. Nesse caso, a mídia social mais utilizada foi o Facebook.

3. Levantamento dos dados de presença social do Banco 3

Venda		Marketing		Suporte		Comunidade	
#	ação	#	ação	#	ação	#	ação
✓	twitter	✓	facebook		social ad networks	✗	social intelligence
✓	twitter APPS	✓	facebook gaming			✗	social business software
✗	content curation	✓	facebook APPS	✗	social scoring	✗	external (costumer) facing internal (employee) facing
✗	stream platforms	✗	social commerce platforms		social data	✗	social scoring
✓	analytics		social brand engagement			✗	blogging platforms
✓	URL shortners	✓			social tv	✓	social/mobile APPS & games
✗	social promotion platforms		social advertising platforms	✓		✓	community platforms
✗	social publishing platforms	✗		✓	social search & browsing	✓	social shopping/referral plug-ins/widgets
✓	social marketing management			✓	plug-ins/widgets	✗	content & photo sharing traditional publishers

Figura 16 - Análise dos dados do Banco 3

A estratégia de presença social do **Banco 3** foi semelhante às adotadas pelos **Banco 1** e **2**, ou seja, também apresentou um posicionamento mais relevante no eixo **VENDAS** fundamentada basicamente no aplicativo Twitter e na utilização de redutores de URL. No eixo **MARKETING**, a atuação é presente, centralizada em plataformas como o Facebook com grande interação entre os clientes e público em geral através de linguagem comum às redes sociais. Constatou-se interação sobre divulgação de produtos, depoimentos de clientes e ações de conscientização e dicas de segurança na utilização dos canais de atendimento e produtos. Com relação aos eixos **SUPORTE** e **COMUNIDADE**, apresenta também elementos de destaque em *Social TV* fundamentada no YouTube com grande geração de

conteúdo e interatividade com o usuário.

4. Levantamento dos dados de presença social do Banco 4

Venda		Marketing		Suporte		Comunidade	
#	ação	#	ação	#	ação	#	ação
✓	twitter	✓	facebook		social ad networks	✗	social intelligence
✗	twitter APPS	✗	facebook gaming	✗		✗	social business software
✗	content curation	✓	facebook APPS	✗	social scoring	✗	external (costumer) facing internal (employee) facing
✗	stream platforms	✗	social commerce platforms	✗	social data	✗	social scoring
✓	analytics	✗	social brand engagement	✗		✗	blogging platforms
✓	URL shortners			✓	social tv	✓	social/mobile APPS & games
✗	social promotion platforms	✗	social advertising platforms	✓		✓	community platforms
✓	social publishing platforms			✓	social search & browsing	✓	social shopping/referral plug-ins/widgets
✓	social marketing management			✓	plug-ins/widgets	✗	content & photo sharing traditional publishers

Figura 17 - Análise dos dados do Banco 4

A estratégia de presença social do **Banco 4** foi semelhante às adotadas pelos **Banco 1**, **2 e 3**, ou seja, também apresentou um posicionamento mais relevante no eixo **VENDAS** fundamentada basicamente no aplicativo Twitter e na utilização de redutores de URL. No eixo **MARKETING**, a atuação é presente, centralizada em plataformas como o Facebook com modesta interação entre os clientes e público em geral através de linguagem comum às redes sociais. Presenciaram-se pequenos *posts*, ou seja, publicações de conteúdo relativo aos produtos e serviços financeiros. Com relação à conscientização sobre métodos e dicas de prevenção às fraudes nos canais de atendimento, não foi possível identificar evidências que comprovassem a preocupação do banco em um espaço de tempo de 60 dias. Com relação aos eixos **SUPORTE** e **COMUNIDADE**, apresenta também elementos de destaque em *Social TV* fundamentada no YouTube, porém com baixa geração de conteúdo e interatividade com o usuário.

5 CONSIDERAÇÕES FINAIS

Como resultado desse trabalho, elencou-se um programa estruturado descrevendo as principais modalidades de fraudes eletrônicas, ameaças e métodos de prevenção que compõem o ambiente de combate e mitigação de riscos adotados pelos bancos no Internet Banking, a fim de minimizar o impacto financeiro provenientes dessas perdas e, por consequência, manter a confiança dos clientes. Estar atento às novas tecnologias e como elas passam a interagir com os clientes deve fazer parte da estratégia dos bancos. Isto inclui identificar, testar e estabelecer padrões de segurança que permeiam o ciclo de interação entre os clientes e o banco.

Neste sentido, foi proposta a seguinte questão de pesquisa: “Com base na crescente participação dos recursos da Internet na vida diária das pessoas, empresas e organizações, quais serão as principais tendências, ou adjacentes possíveis, para a evolução dos métodos de prevenção das fraudes eletrônicas no processo de transição do Internet Banking para o Social Banking?”. Essa questão foi respondida por meio da matriz de avaliação de presença social em conjunto com o método de pesquisa empregado, ou seja, o levantamento bibliográfico e o estudo de caso. Os resultados mostraram que essa combinação também possibilitou atingir o principal objetivo da pesquisa que foi desenvolver o modelo de referência para avaliação de presença social para prevenção às fraudes.

Os objetivos específicos também foram alcançados. O primeiro que era o de identificar e ordenar os elementos que formam os problemas existentes no Internet Banking, suas ameaças, riscos e medidas preventivas adotadas pelos bancos foi alcançado por meio de levantamento bibliográfico apresentado no capítulo 3. Esse capítulo teve como objetivo compreender individualmente cada assunto, suas características e os tipos de prevenção às fraudes utilizadas no Internet Banking. Esse capítulo foi importante para elencar os conceitos existentes no cenário de gestão de fraudes dos bancos e identificar a necessidade de novas formas de prevenção com a evolução das redes sociais.

O segundo e terceiro objetivos específicos, que estavam relacionados a identificação dos aspectos fundamentais da evolução das mídias sociais e o seu impacto na relação entre os consumidores e as organizações, bem como o de identificar a estrutura do *Social World* e o *Social Business* e o enquadramento dos serviços bancários online através deste novo modelo de negócios, foram alcançados por meio da literatura apresentada no capítulo 3. Esse capítulo foi igualmente importante, pois além de contextualizar a sociedade em redes, analisou-se a estruturação das redes sociais, seus impactos nas organizações e pode contribuir para a

estruturação do modelo de presença social e conexão do trabalho entre os meios e métodos atuais de prevenção às fraudes e o que poderia ser uma ferramenta auxiliar para os bancos para identificar e explorar novos canais de comunicação para estreitar o papel de relacionamento e informação aos clientes.

O último objetivo específico que era desenvolver um modelo com o propósito de orientar os bancos a aumentarem o índice de aderência e presença nas principais mídias e redes sociais para colaborarem com soluções de prevenção às fraudes eletrônicas é alcançado por meio do modelo referencial proposto, apresentado na seção 4.1.

A pesquisa também contribuiu na identificação que a utilização dos serviços de Internet Banking oferecidos pelos bancos encontra-se em constante evolução a fim de atender a grande demanda dos clientes. O processo de disponibilização deste serviço recebe interferência do meio social e tecnológico, portanto espera-se que continue a aumentar tanto em termos de números como de impacto, principalmente com a utilização cada vez mais crescente das redes sociais.

Também foi possível identificar que através do surgimento do *Social Business* e os novos desafios que a Web 2.0 traz principalmente no processo de comunicação, a transformação e as mudanças deste novo paradigma passa a ser elemento primordial no entendimento do comportamento dos clientes e, como esse novo processo passa a ser realizado sinergicamente, ou seja, a maneira que o banco percebe e se comunica com seus clientes e como esses clientes entendem e interagem com seus bancos por meio de maior presença social. Entende-se neste trabalho que uma alternativa para se combater às fraudes eletrônicas neste novo contexto social, é adotar uma estratégia mais diversificada e abrangendo diferentes mídias sociais, ou seja, estruturar canais de comunicação em aplicativos, plataformas de relacionamento, canais de vídeos, entre outros a fim de aumentar a presença social dos respectivos bancos.

Para que isso ocorra, é necessário diferenciar o pensamento na gestão dos clientes, ou seja, os bancos deverão seguir uma série de passos importantes para aproveitar ao máximo as oportunidades da Web 2.0. Com as redes sociais, observa-se uma ampla gama de novas tecnologias e inovações na área das comunicações: multimídia, presença, interatividade, entre outros, fazendo com que os bancos se re-invetem na forma de se comunicarem com seus clientes. Agora, os clientes não estão procurando somente o valor dos produtos, mas valores corporativos que façam sentido.

Como parte conclusiva dessa pesquisa, os bancos tornam-se mais transparentes por meio de padrões internacionais como Sarbanes-Oxley e também graças ao aumento do

volume de informações disponíveis online, os funcionários irão confiar mais na cultura empresarial e procurá-la quando esta não estiver suficientemente explícita. Paralelamente, os interessados poderão procurar provas de responsabilidade social corporativa, inevitável para a transparência crescente.

Aumentando a interação e evoluindo a presença social, os bancos deverão perceber novos ciclos de vida cada vez mais curtos tanto no processo de inovação no relacionamento com seus clientes, antecipando necessidades, como no início de uma nova experiência com a geração de inteligência coletiva, conceito esse surgido a partir dos debates promovidos por Lévy (1998) sobre as tecnologias da inteligência, caracterizado por um novo tipo pensamento sustentado por conexões sociais que são viáveis através da utilização das redes abertas de computação.

Espera-se que esse novo processo de relacionamento demandando uma forma mais clara de identidade digital através de maior presença social, gerando e propagando conteúdo coletivamente, os clientes poderão ficar mais informados e atentos com relação aos riscos de exposição às fraudes eletrônicas no Internet Banking.

As mudanças no ambiente de negócios dos bancos serão destinados a acomodar o advento de um espaço aberto corporativo, colaborativo, de apoio, aprendizagem, comportamental e coletivo, que os levarão à uma abordagem holística dos negócio mais transparentes. À medida que a cultura corporativa e social evoluírem, estando presente e atuando em diversas mídias sociais, os clientes passam a receber informações e gerar conhecimento sobre como se comportar e se prevenir quanto às tentativas de fraudes nos canais de distribuição. Nesse trabalho de pesquisa já foi possível constatar os primeiros passos no processo de conscientização e aproximação com os clientes através das redes sociais.

Com relação às limitações, o escopo deste trabalho ficou restrito às fraudes que ocorrem no ambiente do Internet Banking e não levou em consideração os riscos associados aos produtos de cartões de crédito e débito. Outra limitação é que o modelo desenvolvido nesta pesquisa não foi avaliado e nem implementado efetivamente em um banco, já que esse não era o foco da pesquisa. Desse modo, sugere-se para prosseguimento deste trabalho a validação e comprovação de que matriz de presença social, preenchida em sua totalidade seja um aliado importante para o combate e prevenção às fraudes eletrônicas face aos grandes desafios que os novos canais de comunicação e redes sociais podem promover. O objetivo final é, através da matriz projetada, aumentar a comunicação e presença social, criando novos mecanismos preventivos, eficientes e capazes de apoiar os gestores das áreas de prevenção às fraudes a gerenciarem de forma mais holística as tentativas de ataques no canal eletrônico de

distribuição, seja ele o Internet Banking, *Mobile Banking* ou *Social Banking*. Assim, espera-se que através do processo evolutivo na gestão de conhecimento gerado com comunicação eficiente e por meio da inteligência coletiva, os clientes passam a adotar uma postura mais preventiva e colaborativa.

REFERÊNCIAS

- ABU RAJAB, M. et al. (2006). A Multifaceted approach to understanding the botnet. In: ACM SIGCOMM CONFERENCE ON INTERNET MEASUREMENT, 6., New York, 2006. **Proceedings...** New York: ACM. p. 41-52.
- ADACHI, T. (2004). **Gestão de segurança em Internet Banking**: estudo de casos brasileiros. Dissertação (Mestrado) – Fundação Getúlio Vargas, São Paulo, 2004.
- ADAMS, R. (2010). Prevent, protect, pursue - a paradigm for preventing fraud. **Computer Fraud & Security**, v. 2010, n. 7, p. 55-11, jun. Disponível em: <<http://www.sciencedirect.com/science/article/pii/S1361372310700804>>. Acesso em: 17 out. 2012.
- ALBERTIN, A.L.; MOURA, R.M. (1998). Comércio eletrônico: seus aspectos de segurança e privacidade. **Revista de Administração de Empresas**, São Paulo, v. 38, n. 2, p. 49-61, abr./jun.
- ALLEN, M. (2010). The Experience of connectivity. **Information, Communication and Society**, v. 13, n. 3, p. 350-374
- ALTERIAN. (2011). **10 Reasons Why You Need a Chief Marketing Technology Officer (CMTO)**. Disponível em: <<http://www.alterian.com/resources/presentations/campaign-management-PRE/10-reasons-you-need-a-CMTO/>>. Acesso em 3 fev. 2011.
- ANDERSON, C. (2006). **The Long tail**: why the future of business is selling less of more. New York: Hyperion.
- ANDERSON, T. (2001). Assessing teaching presence in a computer conferencing context. **Journal of Asynchronous Learning Networks**, v. 5, n. 2, p. 1-17.
- ANISINGARAJU, S. (2003). Legislation refocuses corporate reporting systems. **Network World**, v. 23, n. 10, p. 36.
- BARABASI, A. L. (2002). **LINKED**: the science of networks. Cambridge: Persius.
- BASEL COMMITTEE REPORT ON BANKING SUPERVISION. (1998). **Risk management for electronic banking and electronic money activities**. Basel: Bank of International Settlements.
- _____. (2000). **Electronic banking group initiatives and white papers, #76**. Basel: Bank of International Settlements.
- _____. (2001). **Risk management principles for electronic banking, #82**. Basel: Bank of International Settlements.
- BEQUAI, A. (2003). Safeguards for IT managers and staff under the Sarbanes-Oxley act. **Computers & Security**, v. 22, n. 2, p. 124.

BERTOL, V.; SOUSA JUNIOR, R. T.; MELO, L. P. (2009). Um Modelo para as normas sobre certificação digital no Brasil. In: INTERNATIONAL CONFERENCE ON FORENSIC COMPUTER SCIENCE, 4., Natal, 2009. **Proceedings...** Rio Grande do Norte: s.n. p. 45-52.

BESSIS, J. (1998). **Risk management in banking**. Chichester: John Wiley.

BIGHAM, T.; CONNER, M. (2011). **O Novo social learning**: como transformar as empresas com aprendizagem em rede. São Paulo: Évora.

BILGE, L. et al. (2009?). **All your contacts are belong to us**: automated identity theft attacks on social networks. [S.l.: s.n.].

BINGHAM, T.; CONNER, M. (2011). **The New social learning**: how to transform learning using social media. São Paulo: Évora.

BLACKSHAW, P. (2010). **O Cliente é quem manda**. Rio de Janeiro: Sextante.

BOJANC, R.; JERMAN-BLAZIC, B. (2008). An Economic modeling approach to information security risk management. **International Journal of Information Management**, v. 28, n. 5. Disponível em: <<http://www.sciencedirect.com/science/article/pii/S026840120800039X>>. Acesso em: 18 out. 2012.

BOLTON, R. J.; HAND, D. J. (2001). Unsupervised profiling methods for fraud detection. In: CONFERENCE ON CREDIT SCORING AND CREDIT CONTROL, 7., Edinburgh, 2001. **Proceedings...** Edinburgh: [s.n.].

_____. (2002). Statistical fraud detection: a review. **Statistical Science**, v. 17, n. 3, p. 235-255.

BORGERTH, V. M. C. (2007). **SOX entendendo a lei Sarbanes-Oxley**. New York: Thomson.

BOGDAN, R.; BIKLEN, S. (1994). **Investigação Qualitativa em Educação**. Porto: Porto Editora.

BOURDIEU, P.; WACQUANT, L. (1992). **An Invitation to reflexive sociology**. Chicago: University of Chicago Press.

BOYAS, J. (2007). **Social capital and well-being**: modeling a multigroup analysis of race and ethnicity. Boston: Boston College.

BOYD, D. (2006). Friends, friendsters, and top 8: writing community into being on social network sites. **First Monday**, v.11, n.12. Disponível em: <http://firstmonday.org/issues/issue11_12/boyd/index.html>. Acesso em: 15 dez. 2012.

BRANDS, S. A. (2000). **Rethinking public key infrastructures and digital certificates building in privacy**. New York: MIT.

BURCHER, N. (2010). **Facebook usage statistics by country - july 2010 compared to july 2009 and july 2008**. Nick Burcher Personal Blog. Disponível em: <<http://www.nickburcher.com/2010/07/facebook-usage-statistics-by-country.html>>. Acesso em: 26 out. 2012.

CAMERON, D. (1997). **Security issues for the internet and the world wide web**. [S.l.]: Computer Technology Research.

CAMP, J.; LEWIS, R. (Ed.). (2004). **Economics of information security**. New York: Kluwer.

CAMP, J. L. (2000). **Trust and risk in internet commerce**. New York: MIT.

CARTER, D. (1995). Computer crime categories: how techno-criminals operate. **FBI Law Enforcement Bulletin**, v. 64, n. 7, p. 7.

CASTELLS, M.; CARDOSO, G. (Org.). (2006). **A sociedade em rede – do conhecimento à ação política**. Lisboa: Imprensa Nacional- Casa da Moeda, 2006.

CASTRO, R. (2010). **Sobre crimes eletrônicos e como evitá-los**. Disponível em: <<http://consumidormoderno.uol.com.br/tendencias/sobre-crimes-eletronicos-e-como-evita-los>>. Acesso em: 12 mar. 2012.

CHAN, S. (2004). Sarbanes-Oxley: the IT dimension. **The Internal Auditor**, v. 61, n.1, p. 31.

CHO, A. (2009). Ourselves and our interactions: the ultimate physics problem?. **Science**, v. 325, n. 5939, p. 406-408, jul.

CLARK, D. D.; LANDAU, S. (2011). Untangling attribution. Harvard national. **Security Journal**, v. 2, n. 2, p. 531-562.

COLEMAN, J.S. (1988). Social capital in the creation of human capital. **American Journal of Sociology**, v. 94, p. S95-S120, Suppl.

_____. (1990). **Foundations of social theory**. Cumberland: Harvard University Press.

COVERY, S. (2006). **The Speed of trust**. New York: Free.

CRIME virtual: a próxima onda. (2007). Santa Clara. (McAfee Relatório de Criminologia Virtual). Disponível em: <http://www.opiceblum.com.br/download/03_pesquisa_relatoriocriminologiavirtual.pdf>. Acesso em: 27 out. 2012.

CULP, C. L. (2002). **The Art of risk management** - alternative risk transfer. New York: John Wiley.

DACHIS, J. et al. (2009). **Social Business design**. New York: Dachis Group.

DAMIANI, E. et al. (2004). An Open digest-based technique for spam detection. In: INTERNATIONAL WORKSHOP ON SECURITY IN PARALLEL AND DISTRIBUTED SYSTEMS, San Francisco, 2004. **Proceedings...** p. 6.

D'ANDRÉA, E. R. P. et al. (2000). **Segurança em Banco eletrônico**. São Paulo: PriceWaterhouse.

DAVIS, J. (2007). Hackers take down the most wired country in Europe. **Wired Magazine**, v. 15, n. 9. Disponível em: <http://www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all>. Acesso em: 4 nov. 2012.

DAVIS, R.; HUTCHISON, S.C. (1997). **Computer crime in Canada**. Toronto: Thomson Canada.

DEFOND, M. L.; FRANCIS, J. R. (2005). Audit research after Sarbanes-Oxley. **Auditing: a journal of practice & theory**, v. 24, p. 5-30, Suppl.

DINIZ, E. H. (2004). Cinco décadas de automação. **Era Digital**, São Paulo, v. 3, n. 3, p. 55-60, ago./out.

DINIZ, E. H.; PORTO, R. M.; ANGULO, M. J. (2001). **Uso da web nos serviços financeiros**. São Paulo: FGV-EAESP-NPP. (Série Relatórios de Pesquisa).

DINIZ, E. H.; PORTO, R.; ADACHI, T. (2003). Internet Banking sob a ótica da funcionalidade, confiabilidade e usabilidade. In: CONSELHO LATINO AMERICANO DE ESCOLAS DE ADMINISTRAÇÃO, 38., Peru, 2003. **Anais...** p. 1-15.

DOWNES, S. (2006). **Learning Networks and Connective Knowledge**. Instructional Technology Forum. Disponível em: <<http://it.coe.uga.edu/itforum/paper92/paper92.html>>. Acesso em 15 nov. 2012.

EDELMAN, D. C. (2010). Branding na era digital: verba de marketing está indo para o lugar errado. **Harvard Business Review Brasil**, São Paulo, v. 88, n. 12, p. 32-39, dez.

ELER, A.; DINIZ, L. (2011). Nocauteados pela lógica. **Veja**, São Paulo, ed. 2246, ano 44, n. 49, p. 140-146, dez.

EL-ERIAN, M, A. (2008). **Mercados em colisão**. Rio de Janeiro: Ediouro.

ELLISON, N.; STEINFELD, C.; LAMPE, C. (2006). Spatially bounded online social networks and social capital: the role of facebook. In: ANNUAL CONFERENCE OF THE INTERNATIONAL COMMUNICATION ASSOCIATION, Dresden, 2006. **Proceedings...** Disponível em: <http://www.msu.edu/~nellison/Facebook_ICA_2006.pdf>. Acesso em: 7 dez. 2012.

EMIGH, A. (2006). The Crimeware landscape: malware, phishing, identity theft and beyond. **Journal of Digital Forensic Practice**. Disponível em: <www.anti-keylogger.org/articles/APWG_CrimewareReport.pdf>. Acesso em: 10 mai. 2013.

FACEBOOK ANNOUNCEMENTS. (2011). **Bing and facebook**. Disponível em: <http://www.livestream.com/facebookannouncements/video?clipId=pla_8f4164aa-977e-4140-8c76-38403a1fe0c2>. Acesso em: 3 fev. 2011.

FARR, J. (2004). Social capital: a conceptual history. **Political Theory**, v. 32, n. 1, p. 6-33, feb.

FATIMA, A. (2011). E-banking security issues - is there a solution in biometrics?. **Journal of Internet Banking and Commerce**, v. 16, n. 2, aug. Disponível em: <<http://www.arraydev.com/commerce/jibc/2011-08/Fatima.pdf>>. Acesso em: 12 set. 2012.

FEDERAL DEPOSIT INSURANCE CORPORATION. (2000). **FDIC DOS manual of examination policies**: electronic banking. Section 4.6. Disponível em: <<http://www.fdic.gov/regulations/safety/manual/00EBANK.htm>>. Acesso em: 14 nov. 2012.

FEDERAL FINANCIAL INSTITUTIONS EXAMINATION COUNCIL AUTHENTICATION IN AN INTERNET BANKING ENVIRONMENT. (2012). Disponível em: <http://www.ffiec.gov/pdf/authentication_guidance.pdf>. Acesso em: 8 apr. 2012.

FEDERAL OFFICE FOR INFORMATION SECURITY. (2009). **The IT security situation in Germany in 2009**. Essen.

FEDERAL TRADE COMMISSION. (2007). **Consumer fraud and identity theft complaint data**. Washington.

_____. (2008). **Consumer fraud and identity theft complaint data**. Washington.

FINANCIAL FRAUD ACTION UK. (2010). **Fraud, the facts 2010**. London.

FOGEL, J.; NEHMAD, E. (2009). Internet social network communities: risk taking, trust, and privacy concerns. **Computers in Human Behavior**, v. 25, n.1, p.153 -160, jan.

FONSECA, C. E.; MEIRELLES, F. S.; DINIZ, E. H. (2010). **Tecnologia bancária no Brasil**: uma história de conquistas, uma visão de futuro. São Paulo: Fundação Getúlio Vargas.

GAINES-ROSS, L. (2010). A Batalha da reputação. **Harvard Business Review Brasil**, São Paulo, v. 88, n. 12, p. 40-47, dez.

GARFINKEL, S.; SPAFFORD, G. (1997). **Web security & commerce**. Cambridge: O'Reilly.

GATES, B. (1999). **Business at the speed of thought**. New York: Warner Books.

GHOSH, A. K. (1998). **E-commerce security**: weak, links, best defense. New York: John Wiley.

GIL, A. C. (2007). **Métodos e técnicas de pesquisa social**. 5. ed. São Paulo: Atlas.

- GLAESSNER, T.; KELLERMANN, T.; McNEVIN, V. (2002). **Electronic security**: risk mitigation in financial transactions. Washington: World Bank.
- GORDON, S.; FORD, R. (2006). On the definition and classification of cybercrime. **Journal in Computer Virology**, v. 2, n. 1, p. 13-20, aug.
- GOVCERT, N. L. (2010). **National trendrapport cybercrime en digitale veiligheid**. Den Haag: Rijksoverheid.
- GRANOVETTER, M. S. (1973). The Strength of weak ties. **American Journal of Sociology**, v. 78, n. 6, p. 1360-1380, may.
- GREENSPAN, A. (2008). **Epílogo sobre a crise financeira**. Rio de Janeiro: Elsevier.
- GREENSTEIN, M.; FEINMAN, T. M. (2000). **Electronic commerce**: security, risk management and control. New York: McGraw-Hill Higher Education.
- HALLER, N. et al. (1998). **A One-time password system (RFC 2289)**. Fremont: RFC.
- HALPERN, D. (2005). **Social capital**. Malden: Polity.
- HANIFAN, L. J. (1916). The Rural school community center. **Annals of the American Academy of political and Social Science**, v. 67, p. 130-138. Disponível em: <<http://www.jstor.org/stable/10.2307/1013498>>. Acesso em: 15 set. 2012.
- HARRIS, S. (2002). **CISSP Certification**: all-in-one. New York: McGraw-Hill/Osborne.
- HAYWARD, C. L. (2004). **Identity theft**. Hauppauge: Nova Science.
- HEALY, R. J.; WALSH, T. J. (1984). Translating security into business terminology. In: GALLERY, S.M. **Security management**: readings from security management magazine. Houston: Butterworth. Cap. 5, p. 37-45.
- HEIKKI, K. et al. (2002). “**Factors underlying attitude formation towards online banking in Finland**”, International Journal of Bank Marketing; Volume: 20 Issue: 6; 2002 Research paper
- HOBBSAWN, E. (1998). **On History**. São Paulo: Companhia das Letras.
- HUMPHREYS, K. (1998). Banking on the web: security first network bank and the development of virtual financial institutions. In: CRONIN, M.J. **Banking and finance on the internet**. New York: John Wiley. p. 75-104.
- INNOPAY. (2010). **Online payments 2010** - increasingly a global game. (2010). Amsterdam: Innopay.
- INTERNATIONAL ORGANIZATION FOR STANDARTIZATION. (2004). **ISO/IEC 13335-1/2004**: Information technology – security techniques – management of information and communications technology security – part 1 – concepts and models for information and communications technology security management. Geneva.

_____. (2008). **ISO/IEC 27005/2008**: Information technology – security. Geneva.

_____. (2009). **ISO 31000/2009**: Risk management – principles and guidelines. Geneva.

IPSOS/CETEM. (2011) **O Observador 2011**. Disponível em:
<http://www.cetelem.com.br/portal/Sobre_Cetelem/Observador.shtml>. Acesso em: 8 jul. 2013.

JAKOBSSON, M.; MYERS, S. (2006). **Phishing and countermeasures**: understanding the increasing problem of electronic identity theft. New York: Wiley-Interscience.

JOHNSON, M. (2008). **A New approach to Internet Banking**. Thesis (Phd.) - University of Cambridge. Disponível em: <<http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-731.pdf>>. Acesso em: 3, ago. 2012.

JOHNSON, S. (2010). **Where the good ideas come from**. São Paulo: Jorge Zahar.
KAARST-BROWN, M. L.; KELLY, S. (2005). IT Governance and Sarbanes-Oxley: the latest sales pitch or real challenges for the IT function?. In: IEEE HAWAI INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES, 38., Big Island, 2005. **Proceedings...** New York: IEEE. p. 1-10.

KARJALUOLO, H.; MATTILA, M.; PENTO, T. (2002). Factors underlying attitude formation towards online banking in Finland. **International Journal of Bank Marketing**, v. 20, n. 6, p. 261-272.

KEHRWALD, B. Supportive social networks: Community based learner support in online learning. Disponível em:
<<http://www.ascilite.org.au/conferences/singapore07/procs/kehrwald-poster.pdf>>. Acesso em 12 nov. 2012.

KOSIUR, D. (1997). **Understanding electronic commerce**. New York: Microsoft.

KOVACH, S. (2011). **Detecção de fraudes em transações financeiras via internet em tempo real**. São Paulo. Disponível em:
<<http://www.teses.usp.br/teses/disponiveis/3/3141/tde-09082011-155153/pt-br.php>>. Acesso em: 8 jul. 2012.

KRUGMAN, P.R. (2009). **A Crise de 2008 e o retorno da depressão econômica**. Rio de Janeiro: Campus.

KRUTZ, R. L.; VINES, R. D. (2001). **The CISSP prep guide**: mastering the ten domains of computer security. New York: Wiley Computer.

KUMAR, S. (1995). **Classification and detection of computer intrusions**. Thesis (Phd) - Purdue University, West Lafayette.

LANGHEINRICH, M.; KARJOTH, G. (2011). **Social networking and the risk to companies and institutions**. Information Security. (Technical Report, Special Issue: Identity

Reconstruction and Theft). Disponível em: <<http://uc.inf.usi.ch/sites/all/files/2010-ISTR.pdf>>. Acesso em: 8 jul. 2012.

LAU, M. (2006). **Análise das fraudes aplicadas sobre o ambiente Internet Banking**. 129p. Dissertação (Mestrado) – Escola Politécnica, Universidade de São Paulo, São Paulo, 2006.

LAUDON, K. C.; LAUDON, J. P. (2004). **Management information systems** - managing the digital firm. 8. ed. New York: Pearson Prentice Hall.

LEVESON, N.G. (1995). **Safeware**: system safety and computer. Boston: Addison-Wesley.

LÉVY, Pierre. *A inteligência coletiva*". São Paulo: ed. Loyola, 1998. ISBN

LI, C. (2010). **Open leadership**: how social technology can transform the way you lead. New York: Jossey-Bass.

LI, H., DAUGHERTY, T., BIOCCA, F. (2001). Characteristics of virtual experience in electronic commerce: A protocol analysis. **Journal of Interactive Marketing**, v. 15, n. 3, p. 13-30.

LIN, N. (2001). **Social capital**: a theory of social structure and action. Cambridge: Cambridge University Press.

LUCA BECCHETTI, C. C. Y. (2008). Web spam detection: link-based and content-based techniques. **ACM Transactions on the Web**, v. 2, n. 1, p. 1-42, mar.

LUNN, B. (1999). Banking technology in emerging markets. In: KEYES, J. **Banking technology handbook**. New York: CRC. Cap. 2, p. 2.1-2.6.

MARSHALL, C. (2002). **Medindo e gerenciando riscos operacionais em instituições financeiras**. São Paulo: Qualitymark.

MCCARTY, C. et al. (2001). Comparing two methods for estimating network size. **Human Organization**, v. 60, n. 1, p. 28-39, nov.

MCGLASSON, L. (2009). FDIC warns of online fraud against banks, small businesses. **BankInfoSecurity**, ago. Disponível em: <http://www.bankinfosecurity.com/articles.php?art_id=1732>. Acesso em: 8 jul. 2012.

MCNAUGHT, C. (2002). Views on staff development about flexible learning. In: STEEPLES, C.; JONES, C. (Eds.). **Networked learning: Perspectives and issues**. London: Springer. p. 111–124.

MOORE, F.; SWARTZ, N. (2003). Keeping an eye on Sarbanes-Oxley. **Information Management Journal**, v. 37, n. 6, p. 20.

MOORE, T. (2010). The Economics of cybersecurity: principles and policy options. **International Journal of Critical Infrastructure Protection**, v. 3, n.3/4, p.103-117, dez. Disponível em: <<http://www.sciencedirect.com/science/article/pii/S1874548210000429>>. Acesso em: 7 jul. 2012.

MOORE, T.; CLAYTON, R. (2007). Examining the impact of website take-down on phishing. In: ANTI-PHISHING WORKING GROUP eCRIME RESEARCHERS SUMMIT, Pittsburgh, 2007. **Proceedings...** p. 1-13.

MOORE, T.; CLAYTON, R.; ANDERSON, R. (2009). The Economics of online crime. **Journal of Economic Perspectives**, v. 23, n. 3, p. 3-20, nov./dec.

MOYEN, Y. (2010). **Vivendo com não elefantes**. São Paulo: Virgiliae.

MUSSER, J.; O'REILLY, T. (2004). **WEB 2.0: principles and best practices**. Cambridge: O'Reilly Radar.

NAKAMURA, E. T.; GEUS, P. L. (2002). **Segurança de redes em ambiente cooperativos**. São Paulo: Berkeley.

NAMI, M. R. (2009). E-Banking: issues and challenges. In: ACIS INTERNATIONAL CONFERENCE ON SOFTWARE ENGINEERING, ARTIFICIAL INTELLIGENCES, NETWORKING AND PARALLEL/DISTRIBUTED COMPUTING, 10., 2009. **Proceedings...** p. 263-266. Disponível em: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5286659&isnumber=5286585>. Acesso em: 6 nov. 2012.

NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR. (2011). **Perdas com fraudes eletrônicas crescem 36% no 1º semestre**. Disponível em: <http://www.nic.br/imprensa/clipping/2011/midia721.htm>. Acesso em: 18 jul. 2012.

OPPLIGER, R.; RYTZ, R.; HOLDEREGGER, T. (2009). Internet Banking: client-side attacks and protection mechanisms. **IEEE Computer**, v. 42, n. 6, p. 27-33.

ORIHUELA, J. L. (2011). **IREDES 2011: conclusiones de José Luis Orihuela y clausura Juan Carlos Aparicio**. Disponível em: http://www.youtube.com/watch?v=jTNc6PhoT2w&feature=player_embedded. Acesso em: 02 jul. 2012.

OSGOOD, M.; ONG, B. N. (2001). Social capital formation and development in marginal communities, with reference to post-soviet societies. **Progress in Development Studies**, v. 1, n. 3, p. 205-219, jul.

OSTROW, A. (2010). **It's Official: facebook passes 500 million users**. Disponível em: <http://mashable.com/2010/07/21/facebook-500-million-2/>. Acesso em: 20 ago. 2012.

OXFORD concise english dictionary. (1999). 10. ed. Oxford: Oxford: University Press.

PARKINSON, J.; BLOOM, S. (2003). Surviving Sarbanes-Oxley. **Optimize**, n. 22, p. 73.

PELTIER, T.R. (2001). **Information security risk analysis**. New York: Auerbach.

PENNATHUR, A.K. (2001). Clicks and bricks: e-risk management for banks in the age of the Internet. **Journal of Banking & Finance**, v. 25, n. 11, p. 2103-2123, nov. Disponível

em: <<http://www.sciencedirect.com/science/article/pii/S0378426601001972>>. Acesso em: 17 set. 2012.

PEOTTA, L. et al. (2011). A Formal classification of Internet Banking attacks and vulnerabilities. **International Journal of Computer Science and Information Technology**, v. 3, n. 1, p. 186-197, feb.

PHUA, C.; ALAHAKOON, D.; LEE, C. (2004). Minority report in fraud detection: classification of skewed data. **SIGKDD Explorations**, v. 6, n. 1, p. 50-59.

PHUA, C. et al. (2005). A Comprehensive survey of data mining-based fraud detection research. **Artificial Intelligence Review**.

PORTES, A. (1998). Social capital: its origin and application in modern sociology. **Annual Review of Sociology**, v. 24, p. 1-24.

PUTNAM, R.D. (2000). Bowling alone: the collapse and revival of american community. New York: Simon & Schuster.

_____. (2007). E Pluribus unum: diversity and community in the twenty-first century. **Scandinavian Political Studies**, v. 30, n. 2, p. 137-174.

RAMOS, A. M.; COSTA, F. R. (2000). Serviços bancários pela Internet: um estudo de caso integrando a visão de competidores e clientes. **RAC - Revista de Administração Contemporânea**, Curitiba, v. 4, n. 3, p. 133-154, set./dez.

ROSSI, C. (2011). Mídias sociais: rumo à democracia participativa?. **Sociologia**, ano 4, ed. 37, p. 32, out./nov.

ROZWELL, C. (2011). **Business gets social**. Stamford: Gartner.

_____. (2012). **Strategic road map for business gets social**. Stamford: Gartner.

RUSSEL, D.; GANGEMI Sr., G. T. (1991). **Computer security basics**. Cambridge: O'Reilly.

SCHNEIER, B. (2001). **Segurança.com**: segredos e mentiras sobre a proteção na vida digital. Rio de Janeiro: Campus.

SEYBOLD, P.B.; MARSHAK, R.T. (1998). **Customers.com**: how to create a profitable business strategy for the Internet and beyond. New York: Times Books.

SHARMA, K.; SINGH, A. J. (2010). Biometric security in the e world. In: NEMATİ, H.R.; YANG, L. **Applied cryptography for cyber security and defense**: information encryption and cyphering. Hershey: IGI Global. Cap. 13, p. 289-337.

SHIREY, R. (2000). **RFC 2828**: internet security glossary. Disponível em: <<http://tools.ietf.org/html/rfc2828>>. Acesso em: 7 abr. 2012.

SKINNER, C. (2012). **Social Banking 2.0 - der kunde übernimmt die regie interview - mobile banking revolution**: chris skinner über zukunftsentwürfe ohne bank. The Chartered

Institute of Marketing in Association with Accenture. The Future of marketing capability. England. Disponível em: <<http://lochmaier.wordpress.com/>>. Acesso em: 14 mar. 2012.

SOLIS, B. (2011). **ENGAGE**: the complete guide for brands and businesses to build, cultivate, and measure success in the new web. Hoboken: John Wiley.

SOLIS, B.; THOMAS, J. (2012). **The conversation prism**. Disponível em: <<http://www.theconversationprism.com>>. Acesso em: 10 mar. 2012.

TAPSCOTT, D. (1997). **Economia digital**. São Paulo: Makron Books.

TÉCNICA detecta fraude em transação bancária via Internet. (2011). Inovação Tecnológica. Disponível em: <<http://www.inovacaotecnologica.com.br/noticias/noticia.php?artio=fraude-transacao-bancaria-via-internet>>. Acesso em: 21 nov. 2012.

THORNBURGH, T. (2004). Social engineering: the "Dark Art". In: ANNUAL CONFERENCE ON INFORMATION SECURITY CURRICULUM DEVELOPMENT, Kennesaw, 2004. **Proceedings...** Kennesaw: ACM. p. 133-135.

TOWERGROUP. (2011). **The Social Business model**: an emerging path to competitive differentiation in banking. New York.

TRIBUNAL DE CONTAS DA UNIÃO. (2003). **Boas práticas em segurança da informação / Tribunal de Contas da União**. Brasília: TCU; Secretaria Adjunta de Fiscalização.

VAN GOOL, L.M.W. (2011). **Improving external control of online web based banking fraud in the netherlands**. Thesis (MsC.) - Erasmus School of Economics, 2011. Disponível em: <http://oathesis.eur.nl/ir/repub/asset/10421/MA007%20IENE-Gool_283517.pdf>. Acesso em: 20 nov. 2012.

WADLOW, T.A. (2000). **Segurança de rede**: projeto e gerenciamento de redes seguras. São Paulo: CAMPUS.

WANG, J. et al. (2006). Technology-based financial frauds in Taiwan: issue and approaches. In: IEEE CONFERENCE ON SYSTEMS, MAN AND CYBERSPACE, s.l, 2006. **Proceedings...** New York: IEEE. p. 1120-1124.

WATTS, D. J. (2003). **Six Degrees. The Science of a Connected Age**. New York: W. W. Norton&Company.

_____. (1999). **Small Worlds. The dynamics of Networks between Order and Randomness**. New Jersey: Princetown University Press.

WEIMING, G. et al. (1995). Falcon: online monitoring and steering of large-scale parallel programs. In: SYMPOSIUM ON THE FRONTIERS OF MASSIVELY PARALLEL COMPUTATION, 5., 1995, Washington. **Proceedings...** New York: IEEE Computer Society. p. 422.

WEIMING, S.; CONSEIL NATIONAL DE RECHERCHES DU CANADA. (2001). Defining and measuring social presence: Contribution to the Networked Minds Theory and Measure. In: INTERNATIONAL CONFERENCE ON COMPUTER SUPPORTED COOPERATIVE WORK IN DESIGN, 16., 2001, London, Ontario, Canada. **Proceedings...** Ottawa: NRC Research Press, 2001.

WORTHAM, J.; KOPYTOFF, V.G. (2011). Poucos dias para se tornar um sucesso. **O Estado de São Paulo**, São Paulo, 29 ago. Negócios, N3.

ZIN, A. N. M.; YUNOS, Z. (2005). How to make online banking secure. **The Star InTech**, Apr. Disponível em: <http://www.crime-research.org/analytics/online_banking/>. Acesso em: 17 abr. 2012.

YAN, J.; EL, A.; SALAH, A. (2008). Usability of CAPTCHAs or usability issues in CAPTCHA design. In: SYMPOSIUM ON USABLE PRIVACY AND SECURITY, 4., New York, 2008. **Proceedings...** New York: ACM. p. 44-52.

YIN, R. K. (2001). **Estudo de caso: planejamento e métodos**. 2. ed. Porto Alegre: Bookman.

Notas:

1) Ágora: em Atenas era a praça onde se expressavam as opiniões. A Ágora contemporânea inclui as redes sociais.

2) 15-M: primeira manifestação que, seguindo as dinâmicas da primavera árabe, explorou a capacidade de organização dos cidadãos potencializada pelas redes sociais. Aconteceu na Espanha, país com plena legitimidade e garantias democráticas. E faz repensar o atual modelo de democracia ocidental.

3) Social Banking: termo cunhado a partir do ingresso dos bancos nas mídias sociais. Não relacionado com banco como agente de ações sociais de cunho assistencial.