UNIVERSIDADE FEDERAL DO PARANÁ

# O PROCESSO DE INOVAÇÃO TECNOLÓGICA DOS BANCOS BRASILEIROS A PARTIR DAS FRAUDES ELETRÔNICAS

CURITIBA

2016

**ILUY MANOEL DE CASTRO LIMA**

# O PROCESSO DE INOVAÇÃO TECNOLÓGICA DOS BANCOS BRASILEIROS A PARTIR DAS FRAUDES ELETRÔNICAS

Monografia apresentado como requisito parcial a obtenção do grau de Bacharel em Ciências Econômicas da Universidade Federal do Paraná - UFPR.

Profº Orientador: José Wladimir Freitas Fonseca

**CURITIBA**

**2016**

Dedico este trabalho primeiramente a Deus, minha família e minha esposa que me apoiaram.

## AGRADECIMENTOS

Agradeço primeiramente ao meu orientador, professor José Wladimir Freitas Fonseca pela orientação, generosidade e paciência.

Agradeço aos professores do curso pelo conhecimento compartilhado ao longo do curso.

Agradeço aos meus familiares e minha esposa, Tamara, que souberam compreender a minha ausência em diversas ocasiões.

## RESUMO

O objetivo geral deste estudo é analisar o sistema bancário no que tange as relações dos clientes com o atendimento remoto (autoatendimento) e o processo de inovação que os bancos estão sendo obrigados a realizar para inibir as fraudes eletrônicas, de forma a diminuir as perdas financeiras. A metodologia adotada para este estudo é a revisão bibliográfica, exploratória/qualitativa, desenvolvida a partir de artigos buscados em sites como Scielo, google acadêmico, livros, teses e dissertações pesquisadas em banco de teses, entre outros materiais. Ao finalizar este estudo pode-se observar que, com a inclusão das novas tecnologias da comunicação, especialmente nos serviços consolidados no campo da Internet, as relações comerciais passaram a adotar novas configurações visando atender as demandas especificas, como no caso do contexto mercadológico que abrange as instituições bancárias e seu relacionamento com seus clientes. Diante da diversidade de transações oferecidas por meio do canal virtual e os consequentes investimentos realizados em segurança, as fraudes bancárias tem feito com que as instituições bancárias repensem seus procedimentos em termos de inovação, buscando ferramentas tecnológicas que devolvam ao usuário a segurança de utilizar estes serviços pela internet. Pode-se concluir, atendendo o objetivo proposto para este estudo, que as inovações tecnológicas que surgiram no âmbito da segurança da informação vieram como resposta ao desenvolvimento das fraudes eletrônicas e, devido a necessidade de apresentar uma solução dos problemas de segurança no setor bancário, os bancos se viram diante da necessidade de dispor de novos produtos para atender seus clientes com segurança e passaram a avaliar as condições de segurança de seus produtos e serviços. Destaca-se que as evidências observadas ao longo deste estudo mostraram que a economia demanda soluções tecnológicas visando minimizar prejuízos com fraudes e aumentar sua eficiência.



Palavras-chave: Sistema bancário. Inovações tecnológicas. Segurança. Fraudes bancárias.

## ABSTRACT

The aim of this study was to analyze the banking system, with respect to customer relations with the remote service (self-service) and the process of innovation that banks are being forced to perform to inhibit electronic fraud, in order to reduce losses financial. The methodology for this study was a literature review, exploratory / qualitative, developed from fetched articles on sites such as Scielo, academic google, books, theses and dissertations surveyed in bank theses, among other materials. Upon completing this study can be seen that the inclusion of new communication technologies, especially in services consolidated in the Internet field, trade relations have adopted new configurations to meet the specific demands, as in the marketing context covering institutions bank and its relationship with its customers. Before the transaction diversity offered through the virtual channel and the resulting security investments, bank fraud has caused the banks to rethink their procedures in terms of innovation seeking technological tools that give back to the user the safety of using these services by Internet. It can be concluded, given the objective proposed for this study that technological innovations that have emerged in the context of information security came in response to the development of electronic fraud and because of the need to present a solution of the banking industry security problems, from the banks found themselves facing the need for new products to serve its customers with security, began to evaluate the safety conditions of its products and services. It is noteworthy that the evidence observed throughout this study showed that the economy demand technology solutions to minimize losses from fraud and increase efficiency.



Keywords: Banking system. Technological innovations. Safety. Bank fraud.

**SUMÁRIO**

# 1 INTRODUÇÃO

O tema proposto para este estudo é o processo de inovação tecnológica dos bancos brasileiros na última década a partir das fraudes eletrônicas.

O cenário brasileiro no inicio da era digital se encontrava muito defasado, o que afetou o desenvolvimento de metodologias e políticas de segurança e resultou em empresas que não possuíam uma política de segurança bem estruturada. Contudo, este cenário foi mudando aos poucos, até que em 2008 o governo brasileiro lançou uma Instrução Normativa GSI - Disciplina a Gestão de Segurança da Informação e Comunicações que tinha por objetivo regulamentar a adoção de políticas de segurança da informação nas organizações públicas (RAMON, 2008).

Com a internet e os avanços tecnológicos, as inovações chegaram ao setor bancário e, com elas, as fraudes têm atribulado as relações entre clientes e organizações. No entanto, apesar da fragilidade que algumas instituições mostram diante dessas fraudes, outras estão muito bem adaptadas e utilizam sistemas em que os acessos aos servidores estão bem configurados e, por isso, protegidos. Um bom exemplo dessa adequação são os servidores de instituições bancárias.

De acordo com a Febraban (2012), as fraudes eletrônicas já ultrapassam a marca de um bilhão de reais e o desenvolvimento de meios de coibi-la é cada vez mais dispendioso para as instituições financeiras. Em face do crescimento das possibilidades de fraude, os bancos têm investido em soluções cada vez mais complexas e caras de maneira a procurar dar proteção à conta de seus clientes. A evolução constante dos meios digitais de acesso às informações bancárias e às inovações no que se refere à digitalização dos processos trazem as instituições financeiras atuais uma grande diversidade de riscos, especialmente nas plataformas digitais, sendo que muitos riscos estão atrelados aos próprios usuários, enquanto outros se referem aos meios de utilização dos serviços disponibilizados.

Para Bocchini, (2012) as fraudes eletrônicas causaram prejuízos de aproximadamente R$ 1,4 bilhão aos bancos brasileiros em 2012. Em 2011 representaram 0,006% do total de transações, ocorrendo de maneira geral pela internet ou por meio da falsificação do cartão bancário, causando prejuízo de R$ 1,5 bilhão.

Conforme informações da Febraban, estima-se que cerca de 24% de todas as transações bancárias são realizadas atualmente pela internet, o que exige que as

instituições bancárias invistam anualmente aproximadamente US$ 9,2 bilhões para combater os crimes virtuais. Contudo, este alto investimento em tecnologia e inovação não são suficientes para bloquear todas as possíveis entradas dos criminosos cibernéticos e ainda destaca que o comportamento dos clientes, dessas instituições representam a maior fragilidade do sistema. (FEBRABAN, 2014).

Segundo Bocchini (2012), entre os comportamentos dos clientes que podem ser classificados como de risco para a segurança de uma transação bancária estão: a falta de manutenção do sistema operacional do computador; navegador e antivírus desatualizados; além do costume de abrir e executar arquivos de remetentes duvidosos.

Desta forma, a Febraban (2014) faz recomendações aos usuários de se manterem atentos quando estiverem navegando em *sites* bancários, observando sua disposição visual, a sequência de solicitação das senhas exigidas e, ao detectar qualquer alteração visual ou aumento da quantidade de perguntas sobre dados pessoais, contatar o banco. Outra instrução se refere à alteração com certa frequência das senhas cadastradas.

O mecanismo de invasão se processa normalmente a partir de golpes típicos feitos por meio de *e-mails* de remetentes duvidosos trazendo algum assunto curioso e demandando que o usuário clique em uma figura ou *link* e, ao clicar, se instala um programa espião no computador, que identificará a senha do usuário no próximo acesso ao *site* do banco (BOCCHINI, 2012).

Outro mecanismo da fraude é o redirecionamento feito pelos programas maliciosos que fazem o navegador da vítima levá-la a um *site* falso no momento de entrar na página do banco. Nestes casos, geralmente, a página falsa solicita informações que o *site* do banco exigiria.

Segundo Carloto (2013), os investimentos das instituições financeiras trouxeram projetos como a tecnologia da biometria do Banco Bradesco desenvolvida em seus terminais eletrônicos no ano de 2006 e também a interligação do seu Internet Banking ao Facebook. O Banco Itaú, visando garantir mais seguranças a seus clientes, adotou a utilização do *QR Code*, que se trata de um tipo especifico de código de barras que, com o auxilio de uma câmera no celular possibilita ao cliente efetuar uma compra ou uma transação bancária. O banco dispõe também do projeto *Itaú Mobile Card* que possibilitaria ao cliente transformar o celular móvel em um cartão de crédito.

Destaca-se ainda outras novas tecnologias como o token, que é uma chave com senha extra que muda a cada minuto podendo ser usada nos computadores por meio da entrada USB ou nos caixas eletrônicos; os smart cards, cartões chipados e cartões de senhas que contem senhas extras que necessitam ser digitadas de acordo com o pedido do banco (FEBRABAN, 2014).

Assim sendo, diante de tantas inovações tecnológicas e o número cada vez mais crescente de fraudes bancárias disponibilizadas pelas mesmas surge o seguinte questionamento: Quais são e como funcionam as inovações tecnológicas apresentadas pelos bancos brasileiros na última década que se desenvolveram a partir das fraudes eletrônicas?

Partindo dessa questão o objetivo geral deste estudo é analisar o sistema bancário, no que tange às relações dos clientes com o atendimento remoto (autoatendimento) e o processo de inovação que os bancos estão sendo obrigados a realizar para inibir as fraudes eletrônicas, de forma a diminuir as perdas financeiras.

Para o desenvolvimento do trabalho e do objetivo proposto foram necessários os seguintes objetivos específicos:

- Pesquisar os conceitos relacionados com as fraudes e sua tipologia;
- Analisar como os bancos estão lidando com as fraudes e os mecanismos que vêm desenvolvendo para inibi-las;
- Estudar a teoria Evolucionista como referencial teórico do estudo;
- Estudo de caso do Banco do Brasil.

No que se refere aos aspectos metodológicos, este trabalho configura-se um estudo teórico. Conforme destaca Demo (1987, p.23) “pesquisa teórica é aquela que monta e desvenda quadros de referência [...] que são contextos essenciais para o pesquisador movimentar-se”. A partir desse ponto de vista, pretende-se aqui analisar as ideias dos teóricos relacionados de maneira que, ao finalizar o estudo, se possa analisar o sistema bancário e o processo de inovação pelos quais os bancos estão passando para inibir as fraudes eletrônicas visando a diminuição das perdas financeiras. Para tanto, foram pesquisados artigos buscados em sites como Scielo, google acadêmico, livros, entre outros materiais que versam sobre a questão trazida no problema de pesquisa.

Assim, buscou-se algumas pesquisas desenvolvidas sobre o tema abordado neste estudo, tanto no que diz respeito a inovações tecnológicas quanto a questão

das fraudes bancárias propiciadas por estas inovações. Além deste estudo ser teórico, pode-se classifica-lo como bibliográfico, qualitativo e exploratório. Inicialmente, trata-se de uma pesquisa bibliográfica por terem sido buscados em materiais já escritos os fundamentos para o desenvolvimento da temática a que se propõe este trabalho monográfico.

Segundo Gil (2002), a presente pesquisa, tendo em vista seus objetivos, pode ser classificada como exploratória/qualitativa porque a pesquisa exploratória tem como objetivo proporcionar maior familiaridade com o problema, com vistas a torná-lo mais explícito que é o que se pretende com este estudo.

Conforme mostra Gonsalves (2003, p. 65):

> [...] a pesquisa exploratória é aquela que se caracteriza pelo desenvolvimento e esclarecimento de ideias, com objetivo de oferecer uma visão panorâmica, uma primeira aproximação a um determinado fenômeno que é pouco explorado.

Para Costa (2001, p. 40) entre os objetivos elencados de uma pesquisa qualitativa encontra-se o de "[...] contribuir para geração de teorias a respeito da questão sob exame."

Já com relação ao método a pesquisa seguiu o que coloca Garcia (1998, p. 44),

> representa um procedimento racional e ordenado (forma de pensar), constituído por instrumentos básicos, que implica utilizar a reflexão e a experimentação, para proceder ao longo do caminho (significado etimológico de método) e alcançar os objetivos preestabelecidos no planejamento da pesquisa (projeto).

Segundo Lakatos e Marconi (2007), os métodos podem ser subdivididos em métodos de abordagem e métodos de procedimentos. Desta forma, neste trabalho foi utilizado o método de abordagem hipotético-dedutivo: que se inicia pela percepção de uma lacuna nos conhecimentos acerca da qual formula hipóteses e, pelo processo dedutivo, testa a ocorrência de fenômenos abrangidos pela hipótese.

E como método de procedimento, o monográfico, que para Lakatos e Marconi (2002, p. 151) é:

> [...] um estudo sobre um tema específico ou particular de suficiente valor representativo e que obedece a rigorosa metodologia. Investiga

> determinado assunto não só em profundidade, mas em todos os seus ângulos e aspectos, dependendo dos fins a que se destina.

No que se refere às técnicas para coleta de dados, a principal forma de coleta de dados foi a leitura de material escrito utilizado para todos os tipos de pesquisa, por isso optou-se pela pesquisa bibliográfica que dará suporte teórico.

A partir da coleta de dados secundários foi feita a análise e interpretação dos dados, que de acordo com Rauen (1999, p. 141),

> (...) é a parte que apresenta os resultados obtidos na pesquisa e analisa-os sob o crivo dos objetivos e/ou das hipóteses. Assim, a apresentação dos dados é a evidência das conclusões e a interpretação consiste no contrabalanço dos dados com a teoria.

Para Triviños (2001, p. 161), "o processo de análise de conteúdo pode ser feito da seguinte forma: pré-análise (organização do material), descrição analítica dos dados (codificação, classificação, categorização), interpretação referencial (tratamento e reflexão)".

De acordo com Selltiz et al. (apud RAUEN, 1999, p. 143) tem-se como objetivo da análise dos dados obtidos nesta pesquisa enumerar e destacar as observações, de forma que estas possibilitem respostas ao problema de pesquisa. O objetivo da interpretação é, desta forma, procurar sentido mais amplo para tais respostas, por sua ligação com outros conhecimentos já obtidos.

Para a análise do material levantado foram utilizadas as normas da pesquisa qualitativa que se referem a análise mais subjetiva do tema estudado a partir de uma argumentação lógica das informações obtidas como pressupõe Michel (2009).

## 2 AS INOVAÇÕES TECNOLÓGICAS NOS BANCOS E AS FRAUDES

De acordo com o que discutia Castells (1999) a concorrência globalizada se desenvolve a partir de fatores característicos que se articulam no âmbito de uma rede baseada em Tecnologia da Informação - TI. Desta forma, a capacidade tecnológica se constitui num dos principais processos que definem a forma e o resultado da concorrência. O autor no desenvolvimento de seus estudos sugere que a tecnologia é uma das principais ferramentas utilizadas para estabelecer o contexto de competição no cenário da nova economia.

Segundo Silva (2014) este cenário proposto por Castell determina que cada vez mais as organizações atuem em um contexto onde a rapidez e complexidade se referem sobretudo, às mudanças no campo das tecnologias da comunicação. Presentemente aproximadamente três bilhões de pessoas estão conectadas à Internet utilizando distintos dispositivos. São indivíduos que destinam uma parcela significativa de seu tempo online, desenvolvendo atividades de compras, comunicação, de trabalho e entretenimento por meio do acesso à internet.

Assim, as novas tecnologias de informação e comunicação quando se analisa os conceitos, técnicas, políticas e estratégias relacionados determinam alterações importantes na estrutura competitiva local e mundial, além de transformar as formas como se financiam as atividades da economia, o funcionamento dos mercados financeiros e criar novas configurações para as organizações (SILVA, 2014).

Para Damiano (2013) em face deste novo cenário de evolução, no setor bancário, pode-se observar uma elevação dos riscos, especialmente aqueles relacionados com as fraudes nos canais tecnológicos, surgindo um contexto de ameaças e tentativas de invasão tanto da organização bancaria quanto do próprio cliente. Complementa Adachi (2004) destacando que os riscos aos quais estão expostos os bancos no mundo físico se repetem no ambiente virtual, estabelecendo um cenário de fraudes e crimes financeiros. Diante disso, a necessidade de proteger os ativos (informações) é de extremamente relevante e importante para o sucesso financeiro e sobrevivência das organizações onde qualquer falha na proteção de seus sistemas de informática podem acarretar perdas e impactos negativos para a gestão dos negócios e para a imagem da mesma perante a sociedade, causando prejuízos financeiros.

De acordo com o estudo desenvolvido por Damiano (2013) a partir da observação desse cenário e do processo evolutivo no que tange as transações financeiras efetuadas por meio do canal eletrônico, aparece a necessidade de estruturação de meios e mecanismos de segurança com o objetivo de combater estas ameaças que podem atingir o cliente e o próprio banco. Na concepção do autor:

> 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 (DAMIANO, 2013, p. 13).

Considera Silva (2014) que o aumento significativo dos ataques e ameaças que se espalham pela internet pode ser atrelado às susceptibilidades e falhas dos sistemas de informática ou dos próprios usuários no momento em que concretizam transações financeiras utilizando a internet. Desta forma, pode-se estabelecer a relação direta destes problemas com o gerenciamento de investimentos, contas bancárias, pagamentos de cartões de crédito ou transações realizadas por meio de comercio eletrônico, além de estar associado também ao processo contínuo de desenvolvimento de inovações tecnológicas e com a obrigação peremptória de se manter em concordância com regulamentações de múltiplos mercados. O autor destaca aqui a importância de se compreender que estes fatores emergem como elementos fundamentais para a adoção de mecanismos de segurança da informação que promovam a correta identificação do usuário, o gerenciamento do acesso, entre outros, como indispensáveis para a efetivação de atividades em ambiente virtual.

Conforme discutem Mello; Queiroz (2006), o contexto do setor bancário, em especial, tem sido berço de amplas transformações ao redor do mundo, determinadas pelas necessidades estabelecidas pelo processo de globalização e pela redução das barreiras de regulamentação entre os mercados financeiros. Segundo os autores, pode-se associar a esses fatores as alterações provenientes dos padrões de comportamento do consumidor, o estabelecimento de um padrão de concorrência acirrado e o movimento de fusões e aquisições, que conferem novas características à competição entre os bancos.

Os autores acima citados destacam a utilização de uma linha de estratégia pelos bancos que se refere a incorporação de novas tecnologias da informação aos seus procedimentos operacionais. Segundo eles a automação bancária que teve inicio no interior das agências, de maneira muito rápida transpassou esse limite físico para disponibilizar serviços aos clientes utilizando uma grande rede de caixas eletrônicos, ao colocar à disposição dos mesmos equipamentos implantados em lugares de grande afluência de público, como por exemplo, centros de lazer, shoppings centers, entre outros. Desta forma, não levou muito tempo para que os serviços bancários alcançassem os níveis industriais, organizacionais e as residências de seus clientes, por meio de redes públicas de comunicação, como a *Internet*.

Assim, diante disso passa-se a discorrer sobre a utilização da internet nas transações eletrônicas e as possiblidades de fraudes no ambiente bancário.

## 2.1 A INTERNET E AS FRAUDES BANCÁRIAS

O desenvolvimento e utilização cada vez maior da Internet teve influências expressivas na mudança de uma velha economia porá o estabelecimento de uma nova ordem econômica, pautada no poder do consumidor que no seu papel de comprador passam a apresentar um poder nunca sentido anteriormente pelo mercado no que se refere a evitar produtos e serviços que não desejam, admirá-los a partir de seu gosto e comprar apenas o que lhe oferecer melhor custo-benefício conforme preconizam em seu estudo Rezabakhsh et al. (2006). Estes autores asseveram que, ainda que o consumidor atual goze de poder suplementar no desenvolvimento das relações de consumo com a utilização da Internet, devem ser ativados mecanismos governamentais, legais e corporativos visando a coibição de práticas prejudiciais nas transações concretizadas.

De acordo com o que expõe Machado (2011, p. 23) complementado o processo exposto.

> O mercado emergente da comunicação via Internet tem sido associado a crescentes números em função de alguns fatores: riqueza acentuada de informações nas transações e relações; menor custo na procura por informações dos consumidores; troca de informação assimétrica entre vendedores e compradores; proximidade espacial eletrônica entre

> vendedores e consumidores; tempo de compra e posse do bem adquirido nas compras digitais.

Ainda em complementação ao tema discutido, Naím (2006) acredita que as práticas fraudulentas efetivadas no contexto do comércio realizado pela Internet estão inseridos na pirataria global que assola o mercado, onde marcas são clonadas, produtos são falsificados e o processo de lavagem de dinheiro se desenvolve em escala mundial.

Segundo Fletcher (2007) somente no ano de 2004 os recursos financeiros que foram perdidos em fraudes financeiras pela Internet no país foram similares às perdas devidas a roubos de bancos. Por exemplo, na Inglaterra foram roubados aproximadamente 400 milhões de libras em 2005 do banco japonês Sumitomo utilizando a Internet e, também em 2005, um hacker extraiu informações de 40 milhões de cartões de crédito igualmente por meio da Internet.

As crescentes fraudes na Internet além de trazer muitos problemas aos usuários, têm originado uma crise de confiança nos sistemas comerciais que tem suas operações apoiadas no comércio eletrônico, o que alcança igualmente o sistema bancário. Por isso, diante da expressividade das fraudes bancárias, o referido setor se viu impelido a investir e desenvolver sistemas de segurança para seus procedimentos eletrônicos.

Para Sarma; Singh (2010), no caso específico dos serviços bancários, o Internet banking refere-se a sistemas que permitem aos clientes acessarem suas contas e obter informações gerais sobre produtos e serviços bancários através de um computador pessoal (PC) ou outros dispositivos inteligentes. Entre estes produtos bancários via Internet pode-se incluir serviços que incluem produtos por atacado para clientes corporativos, bem como produtos de varejo e fiduciários para consumidores. Em última análise, os produtos e serviços obtidos através de Internet banking podem espelhar produtos e serviços oferecidos através de outros canais de distribuição bancária. Alguns exemplos de produtos por atacado e serviços incluem a gestão de dinheiro, transferência bancária, transações, contas de apresentação e de pagamento, entre outros. O exemplo de varejo são os produtos e serviços fiduciários que incluem consulta de saldo, transferência de fundos, informações sobre a transação, pagamento de contas, pedidos de empréstimo, atividade de investimento e outros serviços de valor acrescentado.

As fraudes estão presentes também neste tipo de utilização como demonstra o levantamento desenvolvido pelo Banco Central do Brasil em agosto de 2010 com os bancos que possuem mais de um milhão de clientes averiguou que problemas de segurança nos meios eletrônicos destacam-se em terceiro e sétimo lugar no ranking dos dez primeiros motivos que ocasionam a insatisfação dos clientes com os serviços bancários (MACHADO, 2011).

## 2.2 A INTERNET E AS POSSIBLIDADES DE INVASÃO DO AMBIENTE BANCÁRIO

De acordo com o que expõe Sydow (2015) a informática é o emprego do tratamento automático das informações. Isto posto, é de se entender que é necessária uma linguagem uniforme para que o uso, a transformação e a transmissão de informações sejam amplos e difundidos de maneira global e universal. Essa ferramenta foi intensamente utilizada para o desenvolvimento dos computadores e da internet e todas as suas características e possíveis riscos.

Conforme estas ferramentas evoluem mais a tecnologia informática acaba ocupando espaço na vida da sociedade. Esta inserção se faz a partir da possiblidade de criação e armazenamento de documentos, como por exemplo, as informações bancárias são transformadas em bits e ficam disponível para consulta e utilização.

A partir disso, o desenvolvimento levou o ser humano a elaborar tecnologias e, simultaneamente, a ser capaz de detectar os riscos provenientes de tais avanços, tornando-se capaz de assumir posturas visando evitar os riscos desnecessários e de contenção de atitudes que possam interferir na elevação da quantidade mínima de riscos aceitáveis para esta evolução.

Com os avanços tecnológicos se desenvolvendo a taxas vertiginosas, como apontado por Avelino (2011), torna-se cada vez mais difícil obter-se compreensão que abranja as diversas possibilidades que o mercado apresenta aos consumidores, e por isso, acompanhar de maneira criteriosa as ameaças e vulnerabilidades que cercam o ambiente cibernético se constitui numa tarefa indispensável no contexto de evolução das inovações tecnológicas no ambiente bancário.

Estas inovações tecnológicas vêm se desenvolvendo no ambiente bancário ao longo dos anos. Segundo abordam Silva; Oliveira (2001) a inserção de tecnologia no ambiente bancário a partir do uso de computadores ocorreu na década de 1950.

Os computadores, então, eram empregados no processamento da movimentação diária das contas correntes especificamente, e no período noturno de maneira centralizada. As listagens eram disponibilizadas para as agências no período da manhã para serem usadas pelos caixas ao longo do expediente bancário, sendo que o processamento *online* em tempo real, ainda nem era cogitado.

Para Chorafas (1987) apenas na metade dos anos 1960 surge a primeira geração de computadores *online*, que significava estar conectado diretamente a um sistema. Esta fase se estendeu por aproximadamente dez anos, de 1965 a 1975, sendo que ao logo deste período, o processamento ainda era centralizado e com foco principal na movimentação de investimentos e contas correntes.

Silva; Oliveira (2001) destacam que a segunda geração conectada *online* também se desenvolveu por uma década, de 1975 a 1985, apresentando, contudo, diferenças básicas em relação a antecedente. Enquanto a primeira compreendia serviços de comércio exterior e transações realizadas no mercado de ações e processamento distribuído que se constituía numa maneira descentralizada de processamento de dados desenvolvida em computadores menores distribuídos por uma determinada região; na segunda destaca-se a importância deste período por causa da sua relação com a invenção do cartão de débito e igualmente pelo início de autorizações *online* em transações efetuadas no comércio.

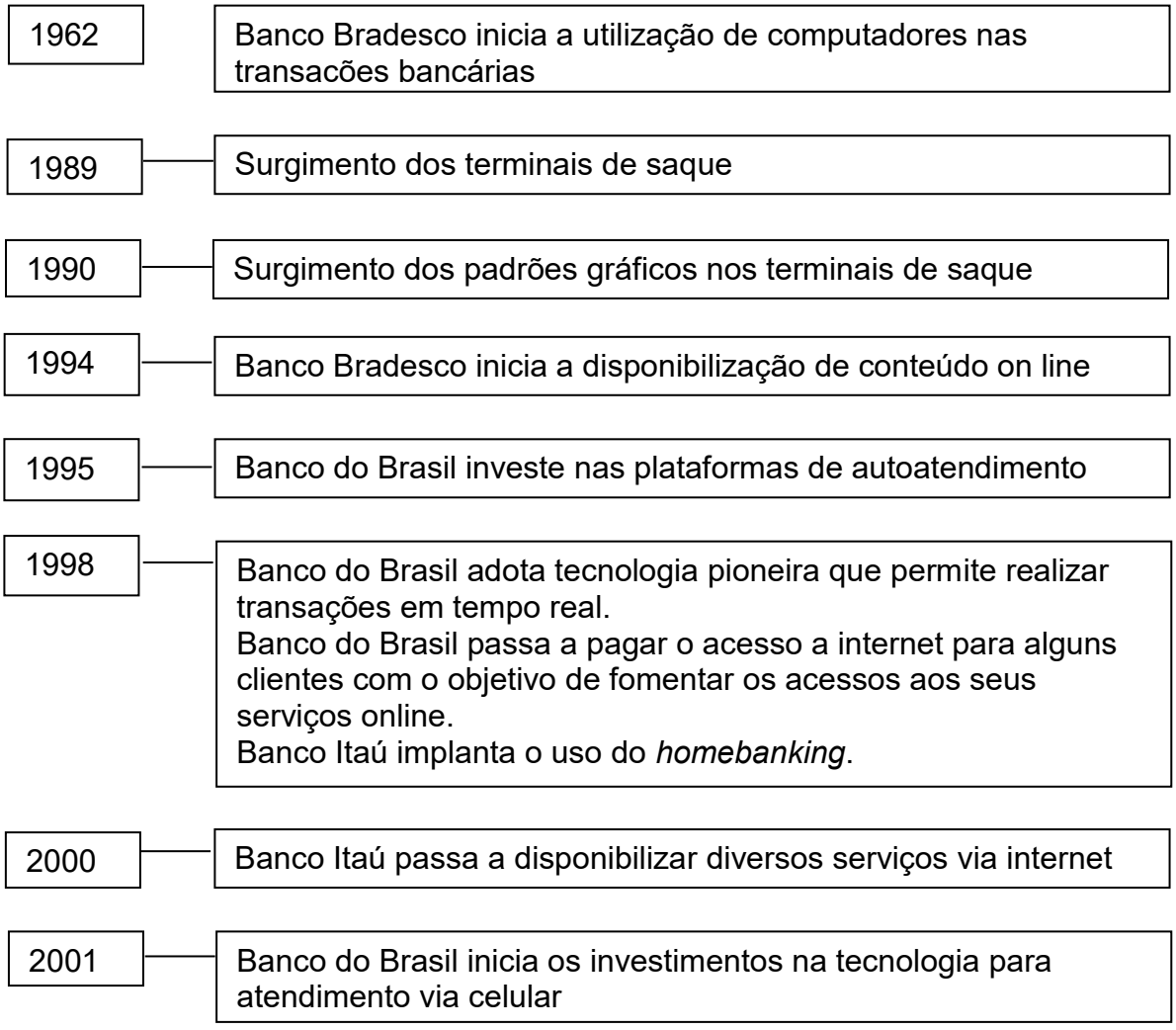
Os autores acima citados destacam que a terceira geração online se desenvolveu no período de 1985 a 1995, apresentando algumas mudanças de relevância significativa:

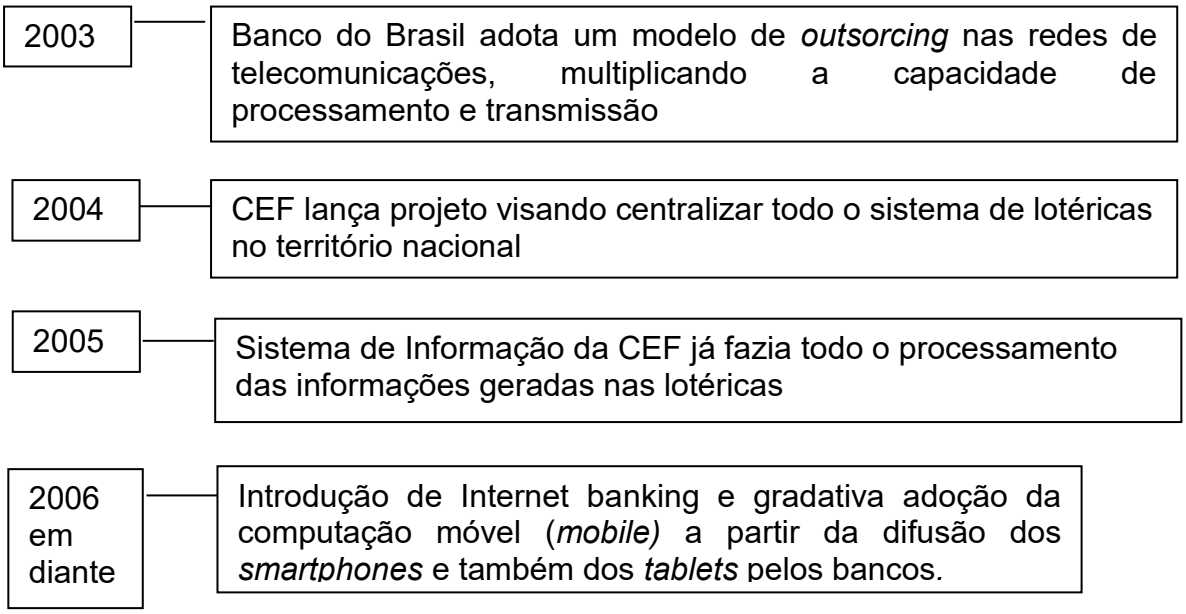
- Inteligência local: a partir do que os bancários passam a poder processar informações a partir de suas próprias mesas de trabalho, deixando para traz a necessidade de acessar um *mainframe* remotamente, que era bastante problemático;
- Desenvolvimento e implementação de terminais online: a partir dos quais o cliente pode se conectar efetivamente em tempo real com o banco e suprir suas necessidades bancárias;
- arquiteturas de rede fazendo a integração da utilização dos sistemas: que foi desenvolvido a partir de investimentos maciços em computadores e telecomunicações.

Muitas inovações foram desenvolvidas ao longo dos anos com aplicabilidade ao contexto bancário. Em linhas gerais, esse processo evolutivo resumido pode ser visualizado na figura 1.

Segundo demonstra Nunes (2014) a Internet assumiu além das prerrogativas de ser um novo meio de comunicação, o papel de ferramenta que pode ser utilizada como instrumento de entretenimento e prestação de serviços, que trouxe consigo características capazes de atuar na redução de custos e no aumento da velocidade das operações. Diante disso, aquelas empresas que se mantiveram inseridas no mercado competitivo ao longo do processo de desenvolvimento da internet, precisaram fazer adaptações para se adequar a inserção na nova concepção de espaço, o espaço virtual, e disponibilizaram suas atividades também através da internet.

Figura 1 – Linha do tempo da automação bancária






Fonte: adaptado de Damião (2013, p. 31).

Neste contexto, as instituições bancárias também se viram obrigadas a se inserir no ambiente virtual, investindo em *sites* na Internet, adotando ferramentas como o Internet Banking para estabelecer relações com seus clientes utilizando rede mundial de computadores e, desta forma, puderam reduzir custos, diminuir a superlotação de suas agencias e possibilitando mais conforto e praticidade aos seus clientes. Contudo, este cenário acabou se tornando vulnerável atraindo um grande número de indivíduos mal intencionados, que se aproveitando da ausência de informação de alguns clientes para perpetrar fraudes eletrônicas (NUNES, 2014).

De acordo com o que expõe Sydow (2015), estes usuários, os chamados hackers, se valem do conhecimento de informática, normalmente acima da média, para programas, modificar softwares, invadir sistemas, encontrar brechas na segurança, para adquirir informações pessoais e senhas dos correntistas, com o objetivo de se apossar de suas identidades virtuais e fazer movimentações indevidas em suas contas-correntes. Diante disso, os estabelecimentos bancários se viram obrigados a melhorar seus sistemas de segurança no Internet Banking, para que os clientes pudessem sentir maior confiança em utilizar este serviço.

Conforme explicita Nunes (2014, p. 09) o Internet Banking, também denominado como banco *on-line* ou banco virtual pode ser descrito como um serviço opcional que os bancos disponibilizam aos clientes que optem por efetuar suas

transações bancárias utilizando o ambiente Internet, sem qualquer dependência relacionada ao horário de funcionamento das agências.

Nas palavras de Santos (2007, p. 61), o Internet Banking pode ser compreendido como a “realização de transações bancárias como consulta de saldo, pagamento de contas, transferências de recursos, investimentos, etc., por meio de um *Web site*, proporcionando conveniência e satisfação para o cliente”.

Conforme destaca Pereira Filho (2008) uma vantagem para as instituições bancárias da efetivação de operações utilizando a Internet é a redução de custos operacionais. *Outra* questão de destaque é que a grande utilização do Internet Banking se reflete diretamente na redução do número de clientes nas agências físicas, contribuindo para que haja economia por parte do banco em termos de possiblidade de diminuição do número de empregados contratados e de diminuição das possibilidades de algum erro operacional devido a falha humana.

Para o cliente, as vantagens se referem a praticidade e comodidade que são disponibilizadas por este tipo de serviço e pela velocidade com que as operações bancárias podem ser efetivadas no ambiente virtual (PEREIRA FILHO, 2008). No entanto, as instituições financeiras tem que lidar com questões relacionadas a credibilidade e segurança do Internet Banking em face do aumento do número de fraudes, acessos indevidos e operações não regulares efetivadas no site do banco (NUNES, 2014).

Segundo o explanado por Sydow (2015, p. 65) neste cenário surgem os crimes informáticos que podem ser perpetrados em meio tecnológico como alvo da conduta ou em meio eletrônico como ferramenta para conseguir obter a finalidade delituosa, com alvo diverso do tecnológico. Assim, pode-se destacar três formas de se perpetrar aquilo que se denomina delito informático:

> 1) Violando-se o meio informático em si, em seus elementos, fazendo uso de ferramentas comuns.
> 2) Utilizando-se do meio informático como instrumento para atacar bem jurídico diverso do informático; e
> 3) Violando-se o meio informático em si, em seus elementos, mas utilizando-se para isso exclusivamente do meio informático (portanto, não ferramentas comuns).

Neste contexto, existe a necessidade de elementos que possam garantir a segurança informática nos ambientes onde as informações se propagam a

velocidade admirável. Assim aponta-se três elementos nos quais se baseia o conceito de ambiente informático.

O primeiro é a confidencialidade que se constitui na garantia de sigilo em relação às informações tratadas pelos aparatos informáticos que não são públicas e por isso, não podem ser lidas, usadas ou acessadas por qualquer indivíduo que não seja legítima ou legitimada. O segundo é a integridade que conceitualmente se constitui bastante equívoco, que grosso modo poderia ser definido como manter a inteireza das informações, que por isso são desenvolvidas a partir de linguagem própria para o computador e que dificulte sua usurpação por outros. O terceiro é a disponibilidade que se refere a questão da estabilidade, segurança e funcionalidade da rede, visto que os aparatos informáticos apresentam como característica a sua disponibilidade, possibilitando que seus proprietários possam fazer uso dos mesmos para a tradução dos dados e para desempenharem suas funções a partir da execução de comandos.

Sobre este contexto, Avelino (2011, p. 02) alude que:

> Ao permitir o exercício de imaginar algum sistema computacional cujo objetivo seja outro que não o apoio às atividades genuinamente humanas, pode-se estabelecer uma situação de difícil solução caso o objetivo seja encontrar exemplos que contrariem esta argumentação. Isto talvez por que os usuários sejam os destinatários de qualquer sistema computacional, algo como '*la raison d´etre'* [1] dos mesmos. Neste sentido, sistemas computacionais devem ser projetados para atender as necessidades de seus usuários, embora em se tratando de segurança, esta necessidade não possa ser encarada como regra.

Assim, Lar et al. (2010) diante do exposto discutem que muito da produção relacionada com dispositivos computacionais que tem como objetivo garantir a segurança acabam focando a proteção de ativos empresariais, como por exemplo, os arquivos, sistemas, informações em geral, entre outros. Desta forma, foram criados dispositivos como *firewalls* [2] e *Intrusion Prevention System*/*Intrusion Detection System - IPS/IDS*[3] que são os mais conhecidos no que tange a segurança de transações via internet, mas que dificilmente podem ser relacionados com a proteção direta de usuários neste ou qualquer outro ambiente.

---

[1] Razão de ser em francês.
[2] Solução de segurança baseada em hardware ou software (mais comum) que, a partir de um conjunto de regras ou instruções, analisa o tráfego de rede para determinar quais operações de transmissão ou recepção de dados podem ser executadas.
[3] Sistemas que tem por função detectar e prevenir os acessos não autorizados às redes ou hosts de uma ou mais redes

Complementa Avelino (2011) dispondo que uma das dificuldades atreladas a uma implementação destes dispositivos de forma eficiente se refere a necessidade de conhecimentos específicos imprescindíveis para afiançar que estes não operem gerando somente impressão de segurança que não é totalmente verdadeira. Destaca ainda o autor que estes dispositivos apresentam como função fundamental auxiliar no processo de implementação de regras e políticas de segurança em um determinado ambiente, que necessariamente precisam ser desenvolvidas antecipadamente para que a segurança possa ser aplicada de fato. Diante disso foca clara a ideia de que somente a implementação do dispositivo não pode garantir que sua operação seja eficiente, passando estes dispositivos a servir penas como redutor do espaço de possibilidades para a possível ocorrência de um evento de fraude. Esse processo se estabelece porque quando se insere em um firewall uma regra que proíbe o acesso a uma determinada porta, somente se previne que uma ameaça se concretize utilizando a referida porta.

De acordo com o exposto por Machado (2011) as instituições bancárias congregaram de maneira muito rápida a Internet em suas estratégias de comunicação com o consumidor, contudo, desde o principio houve a necessidade de lidar com fraudes que se consolidavam contra seus clientes ou públicos de interesse. Esse processo pode ser visualizar via manifestações de consumidores na mídia social, que tornam as relações entre instituições bancarias e consumidores tensas devido a problemas nos sistemas virtuais.

Sobre a possibilidade que se estabeleça esta relação conflituosa entre clientes e bancos, discorre Machado (2011, p. 30) afirmando que:

> a tecnologia vem alterando significativamente o modo de se atender o cliente bancário. Se antes os clientes obrigatoriamente percebiam os bancos como sinônimo de filas com sua tradicional perda de tempo, hoje, esses mesmos bancos podem ser alcançados a partir da casa do consumidor. Cabe saber se esse cliente conhece os serviços oferecidos pelos novos canais, se enxerga atributos da comunicação da segurança e se detecta algum ponto de restrição ao seu uso.

Por isso, aliado a esta possível instabilidade nas relações, Silva (2014) destaca que acelerado desenvolvimento das tecnologias de informação e comunicação constituiu um desafio relacionado ao aumento da complexidade dos ambientes de realização das transações e o desenvolvimento de questões referentes à segurança das informações que circulam por estes ambientes.

Questões como a propagação do uso de aparelhos móveis e das próprias redes móveis nos últimos dez anos tornou o limite delicado entre a utilização profissional e pessoal dos dispositivos adicionados ao grande desenvolvimento dos mecanismos de ataques às redes passível de uma indispensável revisão das estratégias de segurança de informação e das políticas de riscos das empresas em geral, aqui incluídos os bancos. Consequentemente, a grande elevação do volume de transação de informações e de transações financeiras chama a atenção dos indivíduos que vislumbram oportunidades de consolidar empreendimentos no mundo virtual, mas igualmente de pessoas e organizações que não tem boas intenções.

Para atender esta necessidade de segurança cada vez maior, Gartner (2014) mostra que o mercado global de segurança da informação movimentou 65 bilhões de dólares apenas no ano de 2013 pautado pela imprescindibilidade de desenvolvimento de novos produtos e serviços de apoio na detecção de ataques e invasores diante da demanda estimulada pelo surgimento de inovações no meio virtual.

Complementa Chang (2008) que as fraudes perpetradas pela Internet se constituem em uma epidemia crescente que ocasiona gastos de milhões de dólares por ano, porque desde os anos 1990, a Internet tem se constituído em um meio de comunicação atrativo para a prática de fraudes.

Diante disso, para Sarma; Singh (2010) o Internet banking cria novos desafios de controle de risco para os bancos nacionais, visto que a partir de uma perspectiva de supervisão, o risco é o potencial de que os eventos, esperados ou inesperados, possam ter um impacto adverso nos resultados ou no capital do Banco. A direção efetiva de uma atividade regular no ambiente bancário exige que a autoridade bancária entenda e controle os possíveis riscos do banco. A internet banking permite ao cliente conduzir suas transações, em qualquer momento e, portanto, reduz o número de visitas físicas ao banco e reduz o custo por transação, contudo, sua implementação e utilização pelo cliente é uma fomente de possíveis riscos e fraudes.

## 2.3 FRAUDES BANCÁRIAS

De acordo com Nunes (2014) qualquer fraude implica na utilização de algum engodo visando burlar a atenção da vítima, sendo que aquele que pratica a fraude

esconde informações ou as disponibiliza de maneira errada visando conduzir a possível vitima a equívoco para tirar proveito da situação que se estabelece. As origens das fraudes podem ser:

- Interna – quando são perpetradas por indivíduos que apresentem algum vínculo ou estejam inseridos no interior do local que foi fraudado;
- Externa – quando não existe relação entre o agente fraudador e o local que onde aconteceu a fraude. Contudo, existe a possibilidade do autor ter tido relação com a vítima anteriormente.

Para o autor supra citado, não se discute que a Internet propicia um ambiente que predispõe o cometimento de fraudes, acima de tudo porque é muito difícil a identificação do autor do delito e, em alguns casos pela falta de preparo da polícia investigativa. Além disso, os usuários que não apresentem um bom nível de conhecimento em informática ou que não tenham sido apropriadamente cientificados sobre algum procedimento na Internet, acabam sendo vítimas fáceis para os agentes fraudadores.

De acordo com Lau (2006) pode-se definir a fraude eletrônica como sendo a aplicação de qualquer golpe com a utilização dos serviços disponibilizados pela Internet, em seus mais diversos ambientes, como por exemplo, salas de bate papo, mensagens eletrônicas e sites disponíveis. De maneira adicional, o autor alude que a fraude decorre também do aliciamento de potenciais vítimas pelo fraudador com o intuito de consolidar transações fraudulentas em beneficio de um indivíduo ou grupo de indivíduos envolvidas no esquema. Pode-se concluir que a fraude se define pela relação de abuso de um sistema de lucro organizacional que não resulta necessariamente em consequências legais diretas para o fraudador.

Diante dessas afirmações expostas acima, Kovach (2011) faz uma definição de fraude eletrônica como qualquer acesso feito sem a devida autorização ou efetivação de uma transação não autorizada em uma conta corrente através da Internet. Para o autor, a fraude igualmente pode ser vista como uma ação que resulta de um conjunto de violações de controles de segurança que, em último caso, acabou resultando na realização de uma operação financeira sem autorização.

Desta forma, complementa Machado (2011, p. 22) descrevendo que:

> Fruto desse cenário, as empresas têm inserido mecanismos de segurança em seus sites e sistemas virtuais, caso do uso de diversas senhas, fases distintas de acesso a informações de caráter restrito, mensagens de

> advertência, acompanhamento do histórico de transações e outros procedimentos para inibir a prática de fraudes.

De acordo com Soares (2014) as fraudes bancárias que movimentam milhões de reais todo ano no país são resultado da ação de cibercriminosos e da falta de ação dos próprios usuários que não adotam orientações de segurança como atualização de antivírus, utilizar software oficial, atualização constantes no sistema operacional, entre outros.

Conforme coloca Avelino (2011) a fraude se caracteriza pela interação direta entre pessoas, contudo, algumas modalidades com maior grau de sofisticação atacam sistemas bancários, contábeis, judiciários, etc., onde seu alvo é o usuário. Por isso o autor destaca a importância de utilizar algumas tecnologias e metodologias para utilização de alguns tipos de tecnologias e serviços como os bancários, de forma a evitar que ocorram inúmeros tipos de fraudes, porque os serviços disponibilizados pela internet devido a sua característica de rapidez deste ambiente pode-se gerar consequências muito negativas tanto para o usuário quanto para as instituições.

Dentre estas ferramentas destaca-se, segundo CERT.br (2006):

- Criptografia;
- Assinatura digital;
- Certificado digital;
- Ferramentas antimalware;
- Firewall pessoal;
- Filtro antispam.

Outras ferramentas atuais que tem por objetivo aumentar a garantia de segurança têm sido desenvolvidas e são disponibilizadas pelos bancos em ambiente cibernético. O Quadro 1 a seguir faz uma descrição sucinta de algumas dessas ferramentas cuja utilização tem sido implementada:

Quadro 1 – Ferramentas de segurança atuais utilizadas pelos bancos no Brasil.

| Ferramenta | 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. |
| Dispositivos One Time Password (Token) | São dispositivos 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 One Time Password | Constitui 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 | 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 rápidas. |
| 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 | *Completely Automated Public Turing test to tell Computers and Humans Apart* 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 | 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, 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 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. |

Fonte: Damiano (2013, p. 41-42).

Conforme descrito por Silva (2014) a complexidade da segurança da informação tem sido elevada a partir da pesquisa por um algoritmo que afiance a inviolabilidade do sistema criptográfico associada às constantes mudanças tecnológicas. O desenvolvimento das inovações no campo da criptografia foi disseminada para quase a totalidade das tecnologias de informação e comunicação e, como consequência, a maioria dos setores da economia faz utilização da aplicação da criptografia e de outros mecanismos de segurança em seus sistemas inseridos no contexto virtual, em suas redes organizacionais complexas, na computação móvel, na computação em nuvem, no big data, entre outras tecnologias, corroborando a importância da segurança da informação no contexto econômico pela possiblidade de redução do risco de perda financeira e de reputação aos quais as organizações estão sujeitas por operarem no ambiente da internet e digital.

Conforme analisa Barros Filho (2010, p. 1):

> há situações mais sofisticadas em que *hackers* conseguem invadir o sistema de bancos e realizar transferências bancárias. Em tais casos, embora haja a vantagem ilícita em prejuízo alheio, não se configura o estelionato. De fato, não há qualquer pessoa induzida em erro, já que a vantagem foi obtida, sem que houvesse qualquer contribuição do correntista ou de quem o representas- se. Por mais lesiva e socialmente danosa que seja a conduta, não existe estelionato em tais situações.

Os tipos de fraudes que mais assolam os internet bankings são, segundo CERT.br (2006) e Nunes (2014) a utilização de páginas falsas e o cavalo de troia, contudo existem outros códigos maliciosos que abrem caminho para as fraudes:

- *Phishing* ou *phishing/scam*

Este tipo se constitui como uma fraude através da qual um criminoso tenta obter dados pessoais e financeiros de um usuário utilizando uma combinação de meios técnicos e engenharia social.

O phishing sucede por meio do envio de mensagens eletrônicas que procuram efetivar a fraude por meio de comunicação oficial de uma instituição conhecida; buscam atrair a atenção do usuário por curiosidade, caridade ou pela possibilidade de auferir alguma vantagem financeira, entre outras formas.

- Pharming

Pharming é um tipo específico de phishing que cujo mecanismo de ação é o redirecionamento da navegação do usuário para sites falsos utilizando alterações no serviço de DNS (Domain Name System). Este redirecionamento forçado do navegador Web para uma página falsa pode ocorrer através de comprometimento do servidor de DNS do provedor utilizado; devido a ação de códigos maliciosos que alteram o comportamento do serviço de DNS do computador e pela ação direta de invasores que possuam acesso às configurações do serviço de DNS do computador ou do modem de banda larga.

- Códigos maliciosos (Malware)

São programas desenvolvidos especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador.

- Spyware

É um tipo de programa desenvolvido para fazer o monitoramento das atividades de um sistema e remeter as informações recolhidas para terceiros. A conotação de fraude se estabelece quando é utilizado de forma maliciosa, das ações realizadas, do tipo de informação monitorada e da utilização que é feita pelo receptor dos dados coletados.

- Vírus

O vírus se constitui em um tipo de ameaça programada que surge recorrentemente na Internet que se define por ser um código de computador que adere a um programa ou arquivo com o intuito de se disseminar a partir dai para outros computadores. Os *worms*, da mesma maneira que os vírus, igualmente se copiam de um computador para outro com a diferença de se propagar sem depender de outro programa, fazendo-o em uma velocidade tão rápida que obstrui as redes e interfere no funcionamento do computador (GUEDES, 2009).

Estes programas invasores agem de maneira independente, consumindo os recursos do computador e acessando todos os arquivos do mesmo, tornando viável o acesso ilegítimo às informações pessoais da vítima.

- Cavalo de troia (Trojan)

O cavalo de troia, também conhecido como trojan ou *trojan-horse* é um programa que executa as funções para as quais foi aparentemente projetado, mas também executa outras funções, geralmente maliciosas e sem a anuência do usuário.

- Spam

O *spam* trata-se do envio de mensagem eletrônica sem a solicitação do usuário, cuja procedência é de remetente desconhecido. Estas mensagens eletrônicas podem apresentar conteúdo malicioso, como por exemplo, o *site* falso de uma instituição financeira, fazendo com que o usuário possa acreditar que se trata de um *site* real e por isso dispor seus dados pessoais e sua senha bancária nos locais solicitados, sem idealizar que estas informações estão sendo gravadas e remetidas prontamente a um fraudador (GUEDES, 2009).

Avelino (2011) destaca que as instituições bancárias têm sido alvos de ataques cibernéticos que apresentam grau de sofisticação cada vez maiores, que interfere negativamente na sensação de segurança que este tipo de serviço precisa entregar aos usuários. Sobre estas ações de ataque, Barros Filho (2010, p. 1) descreve que:

> Uma das que merece destaque é o envio de *e-mail* em que se simula ser uma mensagem enviada pelo banco, no qual se solicita que os dados da conta (inclusive senha), sejam digitados. Com tais informações, o agente acessa a conta da vítima e realiza transferência em prejuízo do correntista. Em tais situações, está configurado o estelionato, pois o autor usou a fraude (e-mail fictício do banco) que levou a vítima ao erro (fazendo com ela digitasse seus dados), o que permitiu ao agente que ele obtivesse a vantagem (transferência do dinheiro) em prejuízo alheio. Não só estão presentes os elementos, como há o nexo causal entre cada um deles. (BARROS FILHO, 2010, p. 1)

Descreve Avelino (2011) que mesmo diante do fato de alguns tipos de fraude serem de fácil identificação, de algumas condutas bancárias e do aparato tecnológico disponível, a falta de informação em relação aos aspectos de segurança imprescindíveis para que o cliente utilize este tipo de serviço, inúmeras vítimas são atingidas anualmente no país.

Diante da vasta gama de possiblidades de ataques cibernéticos, de acordo com Damiano (2013), torna-se indispensável que sejam implementados constantemente sistemas e processos com a capacidade de proceder ao monitoramento online das transações, devendo este processo estar inserido no contexto geral de prevenção às fraudes com o escopo de garantir que os controles e ferramentas de autenticação estejam adequados aos procedimentos das instituições bancárias e às necessidades dos clientes. Conforme analisa o autor, os processos de autenticação devem ser desenvolvidos de forma a elevar ao máximo a

comunicação de maneira transparente e com coerência em relação a estratégia adotada pelo banco para seu canal de Internet Banking. Desta forma, o grau de autenticação desenvolvida para uma determinada aplicação deve ser apropriada ao nível de risco propiciado pela exposição a este tipo de fraude. A palavra certamente é prevenção acima de tudo, e assim, analisa-se a seguir os procedimentos de prevenção de fraudes.

### 2.3.1 Prevenção de Fraudes

Azevedo (2012) coloca que o cliente bancário é o alvo principal das fraudes eletrônicas que infectam o computador utilizando uma ferramenta maliciosa ou a indução da própria vítima a partir de uma mensagem fraudulenta que tem como objetivo de repassar as informações para o agente fraudador. Diante disso, percebe-se que o próprio sistema de informática da instituição bancária sofre invasão ou ataque direto, nem mesmo aqueles provenientes dos provedores Internet. As principais tentativas de fraude concretizadas sobre clientes do sistema financeiro e usuários do ambiente Internet no país se baseiam principalmente em ataques *pishing scam* e *pharming* já conceituados anteriormente neste estudo.

O desenvolvimento do processo de prevenção de fraudes se refere diretamente ao risco de perdas aos quais o sistema está exposto, conforme analisam Bastos; Pereira (2007, p. 05), destacando que uma “análise de custo-benefício mensurando a probabilidade de danos e perdas prováveis que poderiam ser combatidas com a implantação de um sistema de prevenção de fraudes deve ser considerada”.

Para os autores acima citados, a estratégia para detectar a fraude se desenvolve posteriormente a ocorrência do evento, por isso, a premissa básica das empresas que utilizam esse tipo de estratégia é estreitar a lacuna que se forma entre a ocorrência e a detecção da fraude, de forma a diminuir o tempo de verificação da fraude, visando combater e corrigir as falhas de controle para expurgar a possibilidade de novos prejuízos. Por isso, geralmente o sistema de detecção de fraudes parte do processo acompanhamento dos perfis de utilização de determinado produto ou serviço, observando aqueles que se distanciam dos padrões normais.

Com o objetivo de analisar uma variedade bastante ampla de informações tem se desenvolvido sistemas informatizados inteligentes, com a adoção de ferramentas e técnicas estatísticas que possibilitam a ampliação e a utilização da técnica de inteligência competitiva denominada *Datamining* - Mineração de Dados, que se constitui em um diferencial na detecção de fraudes. Esta ferramenta tem como mecanismo de ação desenvolver a associação dos fatos históricos cujos resultados comprovaram-se em fraudes, de maneira que o sistema consiga identificá-los de maneira imediata à ocorrência dos mesmos eventos, demandando confirmação da fraude posteriormente em alguns casos específicos. A utilização da técnica de *datamining* para detectar as fraudes em cartões de crédito, por exemplo, é indispensável hoje em dia.

Azevedo (2012) destaca que comumente as instituições financeiras informam aos seus clientes que seus sites e serviço de Internet Banking são seguros, contudo, de maneira geral, isso significa que o banco fundamentalmente conta com dois tipos de proteções: os *firewalls* e a criptografia de dados. Os *firewalls* se encontram instalados nos locais onde estão as máquinas servidoras do site da instituição, sendo que sua função básica é regular o fluxo de informações entre redes diferentes e não permitir que haja transmissão e/ou recepção de acessos maliciosos ou não autorizados na comunicação entre estas redes.

Outra proteção que os bancos utilizam é a criptografia de dados entre o computador do usuário e o site da instituição, através do protocolo *Secure Socket Layer* – SSL, que consiste em tecnologia padrão de segurança na transmissão de dados pela Internet, fazendo a codificação de todas as informações que navegam na rede ao longo do período em que a transação eletrônica está sendo realizada. Esse processo garante que não haja a possibilidade de intercepção da comunicação por um terceiro visando capturar e compreender as informações circulantes, como por exemplo, o número da conta e a senha bancária (AZEVEDO, 2012).

Contudo, descreve Azevedo (2012) que as instituições bancárias omitem que essas proteções, mesmo sendo imprescindíveis, são insuficientes para promover uma proteção completa do serviço de Internet Banking, porque normalmente o computador do usuário não está protegido e por isso, a partir de um ataque via *phising*, pode haver a instalação de um programa malicioso localmente que faz o monitoramento do teclado (*keylogger*), obtendo, assim, capturar

informações como número da conta e a senha bancária, antes que estas sejam remetidas e codificadas ao site do banco.

Outra possibilidade de ataque possível é por meio da indução do usuário a clicar em um *link* presente em uma mensagem falsa recebida, que fará o redirecionamento do mesmo a um site falso que simula o site oficial da instituição bancária. Em regra geral, esse site falso vai solicitar dados pessoais do usuário, inclusive número da conta e senha, que serão disponibilizadas pelo cliente diante de sua crença em se tratar do site verdadeiro do banco, por isso, confiável (AZEVEDO, 2012).

Visando contornar este tipo de fraude, alguns bancos desenvolvem suas ferramentas de segurança do sistema de Internet Banking, adotando recursos como o teclado virtual na tentativa de impedir a ação dos *keyloggers* na interceptação das senhas digitadas ou pela utilização de mecanismos de autenticação com maior nível de segurança do que simples senhas, para tornar mais difícil a simulação do site o verdadeiro e o reencaminhamento a sites falsos (AZEVEDO, 2012).

Segundo o aporte teórico de Silva (2014) pode-se compreender que o processo evolutivo do internet banking estabelecido como canal de relacionamento bancário, se deu a partir de avanços tecnológicos estimulados pelas soluções de problemas de segurança que se apresentam no setor de financeiro, porém, atualmente a computação móvel, denominada no âmbito bancário de *mobile*, que se desenvolveu de maneira especial a partir da ampliação da propagação dos *smartphones* e dos *tablets*, tem se consolidado como um importante canal de relacionamento bancário porque pode garantir ao cliente a possibilidade de acesso às transações bancárias de qualquer lugar. No ano de 2013 os dados mostram que já existiam 1,9 bilhões de smartphones em todo mundo de acordo com os resultados da pesquisa realizada em 2014 pelo Instituto de Pesquisa IDC, que ainda mostrou na referida pesquisa a probabilidade de atingir 2,6 bilhões dispositivos em 2014.

Contudo, este tipo de tecnologia apresenta igualmente desafios a serem suplantados em termos de segurança, porque se caracteriza o aumento dos níveis de ameaças no que se refere a volume e sofisticação dos ataques a estes dispositivos perpetrados utilizando-se *malwares* desenvolvidos especificamente para estes equipamentos que podem trazer potenciais prejuízos financeiros e de reputação. Por isso o movimento no sentido de maior utilização de dispositivos pessoais em utilização corporativa que caracterizam o conceito BYOD também

demanda inovações tecnológicas por parte dos bancos, porque estes dispositivos infectados por vírus ou cavalo de tróia podem atingir a rede corporativa das instituições bancarias.

Outra inovação que tem sido utilizada, conforme mostra Silva (2014), é o *cloud computing* ou computação em nuvem que se refere ao modelo que possibilita acesso onipresente à rede a partir de um conjunto compartilhado de recursos configuráveis de computação como consolidação de novas redes, desenvolvimento de servidores, ferramentas de armazenamento, desenvolvimento de aplicativos e de serviços, entre outros que podem ser provisionados e liberados de maneira rápida empenhando mínimo esforço de gerenciamento ou interação com o provedor de serviços.

Para Silva (2014, p. 60) as principais características da *cloud computing* que a destacam como uma tecnologia que vem sendo muito utilizada pelas organizações em geral são as seguintes:

> I) Provisionamento *on-demand*: trata-se de auto-serviço ou autoatendimento. Os recursos de banda larga, armazenamento ou rede podem ser utilizados sem interação humana com prestadores de serviços.
> II) Ubiquidade de acesso: acesso aos sistemas, independentemente da localização do usuário ou dispositivo (PC, *smartphone, tablet*, etc.)
> III) Pool de recursos: os recursos computacionais da nuvem como armazenamento, processamento, memória, banda e máquinas virtuais, ficam reunidos geograficamente. O cliente não possui controle sobre a real localização dos recursos que está utilizando, tendo somente uma informação mais ampla como o país em que se encontra, o estado ou o *Data Center.*
> IV) Elasticidade Rápida: é a capacidade de alocar mais ou menos recursos no momento em que for necessário e com agilidade. E pode adquirir mais ou menos recursos de acordo com a necessidade de suas aplicações.
> V) Serviços Mensuráveis*:* os serviços são controlados e monitorados pelo provedor de forma transparente. Possibilitando o usuário do serviço otimizar sua utilização da nuvem.

Ainda segundo Silva (2014) o setor financeiro tem se confrontado com obstáculos para adotar este tipo de tecnologia, principalmente, na área de privacidade de informações, disponibilidade e ausência de normatização especifica, entre outras questões. A questão que se consolida é a possiblidade de utilização por terceiros com outras finalidades das informações das instituições bancarias e dos clientes vulneráveis alocadas em nuvem pública. Mesmo em face dessa possiblidade e de outras preocupações suscitadas por este mecanismo, o mercado

de TI tem se desenvolvido no sentido de adotar modelos de implantação de nuvem que possam servir como alternativa para adoção dessa tecnologia.

No âmbito da segurança da informação relacionada às tecnologias de computação em nuvem, se desenvolvem mecanismos que podem colaborar com o pressuposto de que o setor é norteado pelas demandas do mercado que aparecem a partir da adoção de novas tecnologias. Diante disso, ao se observar que o processo de desenvolvimento das tecnologias de informação e comunicação, pode-se perceber que estas tecnologias foram implementadas no contexto bancário após passarem por adaptações que podem ser vistas como inovações tecnológicas empreendidas no campo da segurança da informação visando atender este setor especifico.

## 3 REVISÃO TÉORICA – TEORIA EVOLUCIONISTA

A partir dos anos setenta e oitenta, estudos acerca da dinâmica da inovação tecnológica de alguns autores neo-schumpeterianos desenvolveram uma teoria acerca da inovação tecnológica, como sendo processo evolutivo, dinâmico, acumulativo e sistêmico, com base nas rotinas, aprendizado e acumulação de conhecimento. Esses preceitos contrariam conceitos neoclássicos afirmam que a tecnologia não é um dado que aparece definitivamente realizado no momento que nasce. (DEZA, 1995).

> En ellos se rompe la concepción neoclásica de tecnología y la dicotomia convencional entre la producción de innovaciones y su difusión. La tecnología no es un dato que aparece definitivamente realizado en el momento que nasce, sino que se va desarrollando gradualmente al mismo tiempo que se difunde y, ademas, esa difusión no tiene lugar en un entorno banal y abstracto sino que tiene lugar en un contexto industrial, económico y social específico con el que mantiene un feed-back permanente. (Deza, 1995, p.216).

Nelson e Winter tentando fundamentar teoricamente o evolucionismo, utilizaram preceitos Schumpeterianos, como, competência é um processo e não um estado e, assim como Schumpeter, rechaçam os conceitos neoclássicos de racionalidade maximizadora e de equilíbrio. Propõem dois conceitos alternativos: busca de soluções satisfatórias e seleção, para aplicar sua ideia de racionalidade baseada em rotinas. Acreditam que as variações são pequenas e não aleatória, já que são resultados de processos de pesquisa, diferentemente de Schumpeter que trata das grandes inovações descontínuas na teoria da destruição criativa.

De acordo com Deza (1995), a teoria proposta por Nelson e Winter são caracterizados por três definições: I) As empresas são caracterizadas por certos números de variáveis e de estado (capital, técnicas, P&D), rotinas e condições de mercado; II) As condições atuais permitem definir uma distribuição de probabilidades sobre o conjunto de variáveis que podem obter no futuro; e III) Os modelos são probabilísticos e não deterministas.

Segundo Deza (1995), os determinantes e as direções das mudanças tecnológicas foram trabalhadas por G. Dosi, que construiu um modelo onde, o comportamento das empresas é determinado por suas condições estruturais. A análise de Dosi procura construir uma ponte entre a abordagem microeconômica da firma inovadora e a dinâmica do sistema e seu conjunto. Dosi critica a teoria da

“demand-pull” e a teoria da “technology-push”, essas teorias não conseguem responder aos resultados obtidos nas análises empíricas realizados sobre tecnologias e setores concretos.

Três aspectos são criticados na teoria da “demand-pull”: I) Mudança tecnológica e passiva no sistema; II) Não explicam o porquê e quando de certas mudanças tecnológicas em detrimento de outras; III) Desconsideram a capacidade criativa com o passar do tempo.

Sobre a teoria da “technology-push”, Deza (1995).

> Por lo que se refiere a las teorías de la technology-push su limitación es justamente la inversa: incorporan mal lá importancia de los factores económicos en la dirección del precesso de innovación. Su esquema básico parte de una visión unidireccional de las relaciones ciencia-tecnología-producción, donde la primeira componente es una fuerza exógena que actúa deus-ex-machina. (DEZA, 1995, p. 220).

Através de observações empíricas sobre resultados obtidos dos processos de inovação, Dosi construiu um modelo levado em consideração sete características: I) Os inputs científicos tem um papel crescente no processo de inovação; II) P&D são complexas, por isso são objetos de planejamento de longo prazo por parte das empresas; III) Existe uma significativa correlação entre P&D e inovação em muitos setores; IV) Inovação se origina no processo de “leaning-by-doing”, sendo incorporado pelas pessoas e organizações; V) O planejamento institucional de pesquisa está levando as empresas a terem algum conhecimento prévio da melhores tecnologias; VI) A mudança tecnológica ocorre com base nas rotinas existentes no presente e a possibilidade de que as empresas consigam avanços técnicos e função do nível tecnológico conseguido por elas previamente; e VII) As evoluções tecnológicas apresentam regularidades no longo prazo, de acordo com características econômicas e tecnológica dos produtos e processos. (DEZA, 1995).

Sobre paradigmas tecnológicos e trajetórias tecnológicas, Dosi primeiramente distingue três grandes sistemas, o científico, o tecnológico e o econômico, e estabelece os seus estudos acerca do sistema tecnológico e suas relações com variáveis econômicas. Diferentemente da teoria neoclássica, Dosi define tecnologia de uma forma mais ampla, considerando tanto aspectos materiais quanto conhecimentos e experiência acerca das rotinas de trabalho e não somente como uma informação aplicável e apropriada imediatamente. Dossi então, define progresso técnico como sendo um processo sequencial de resoluções de problemas

de um paradigma tecnológico. Com isso estabelece que paradigma tecnológico é um modelo de solução de problemas tecnológicos e trajetória é um padrão de solução normal dentro de um paradigma que é análoga à trajetória natural de Nelson e Winter. A medida que essas resoluções vão sendo realizadas temos uma direção do progresso tecnológico da firma. (DEZA, 1995).

O processo de seleção se dá através de um mecanismo fundamental, onde o que determina quais as melhores técnicas e rotinas a seguir são fatores econômicos, institucionais e sociais. Mas tanto para Dosi quanto para Nelson e Winter, fatores do entorno econômico e social influenciam na escolha da trajetória a ser seguida.

> Destacan la importancia cresciente de los elementos extramercado, tales como los elementos políticos-institucionales, financeiros, comportamiento de los consumidores, etc., particularmente con respecto a alguns sectores, e insisten en la necesidad de matizar las relaciones entre innovación-beneficios teniendo en cuenta la especificidad de cada sector y la importancia de la relación imitación benefícios. (DEZA, 1995, p. 226).

Estudando especificamente os setores da economia sobre inovação temos o trabalho de K. Pavitt, que a partir de informações descritivas coletas sobre firmas inovadoras, conseguiu agrupar as empresas em setores em função das fontes, natureza e impacto da mudança tecnológica. (DEZA, 1995).

Trajetória tecnológica setoriais: determinantes, direções e características

| Categoria da empresa | | Setores típicos centrais | Determinantes da trajetória tecnológica | | | Trajetórias tecnológicas | Características medidas | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | Origem do processo de tecnologia | Tipo de Usuário | Apropriação medida | | Origem do processo de tecnologia | Peso relativo da inovação de produto ou processo | Tamanho relativo das empresas inovadoras | Intensidade e direção da diversificação tecnológica |
| 1 | | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| Dominadas pelos provedores | | Agricultura, Construção, Serviços privados, industria tradicional | Provedores. Serviço de pesquisa e extensão. Grandes usuários. | Sensível ao preço | Não técnicos (marcas, publicidade, desenho, etc) | Redução de custos | Provedores | Processo | Pequena | Baixa-Vertical |
| Intensiva em produção | Intensiva em economias de escala | Materiais industriais (vidro, aço). Montagem (bens de consumo duráveis, veículos) | Provedores. P&D. Departamento de engenharia. | Sensível ao preço | Segredos do processo e Know how. Economias de aprendizagens dinâmicas. Patentes, lags tecnológicos. | Redução de custos (desenhos de produto). | Interna | Processo | Grande | Alta-Vertical |
| | Provedores especializados | Maquinários. Ferramentas. | Desenho e desenvolvimento. Usuários | Sensível ao resultado | Know how em desenhos. Conhecimento dos usuários. Patentes. | Desenho de produto | Interna. Cllientes. | Produto | Pequena | Baixa-Centralizada |
| Baseadas na Ciência | | Eletrônico/Elétrico. Química | Ciência divulgada. P&D. Departamento de engenharia | Mista | Know how em P&D. Patentes. Segredos do processo. Economias de aprendizagens dinâmicas. | Mista | Interna Provedores. | Mista | Grande | Baixa-Vertical.Alta-Centralizada |

Fonte: Pavitt.

Segundo Pavitt, levando em conta a sensibilidade quando a inovação tecnológica, podemos dividir as firmas em quatro grandes setores, conforme segue:

I) Setor com as empresas provedoras, as inovações acontecem no processo produtivo e objetivam a redução de custos;

II) Setores de altas economias de escala, inovações acontecem no processo produtivo e também nos produtos;

III) Setor de provedores especializados, inovações acontecem no produto;

IV) Setores baseados na ciência, trabalham no desenvolvimento de produtos.

Conforme exposta acima, podemos considerar que a teoria evolucionista explica grande parte relações das instituições bancárias no que tange as inovações na área de segurança da informação.

# 4 ESTUDO DE CASO – BANCO DO BRASIL

O estudo de caso busca traçar um paralelo entre as inovações que ocorrem no Banco do Brasil e as fraudes que os clientes estão sujeitos, realizando também uma breve um revisão histórica das inovações e um caso de uma inovação criada pelo banco, o BB CODE. Levando em consideração a teoria evolucionista, destacando Dosi.

> Define el progresso técnico como el proceso secuencial de resolución de problemas en el marco de un paradigma tecnológico, siguiendo una trayectoria tecnológica. Para Dosi ese progresso técnico es irreversible. (DEZA, 1995, p. 221).

O atendimento pela internet do Banco do Brasil S/A, começou a ser desenhado no ano de 1995, com a implantação do sistema de contabilização de transações em tempo real em toda a rede de agência, mas somente a partir de 1998 foi aberto, a alguns clientes, a possibilidade de acesso a dados e movimentações da conta corrente, sem nenhuma movimentação financeira. Em 2001, com a implantação de transações na internet, iniciaram as fraudes.

No início do atendimento bancário *On line* no Banco do Brasil, os clientes conseguiam realizar operações financeiras utilizando somente uma senha de acesso a conta, então, os fraudadores vendo a fragilidade do sistema iniciaram uma ofensiva com o objetivo de realizar fraudes. Utilizando, principalmente, *Spans* para envio de e-mails com *trojan* e link's com endereços fraudulentos do banco para induzir o cliente a digitar os dados bancários e então realizar operações ilícitas. Diante desse movimento o Banco do Brasil incluiu uma senha de acesso e para confirmações de transações passou a utilizar a senha do cartão. As fraudes continuaram, mas agora também utilizavam *Keyloggers* para captura de senhas digitadas no teclado físico, o Banco implantou um teclado virtual, para que o cliente clicasse nos números da senha, não sendo necessário a digitação no teclado físico, os fraudadores passaram a utilizar *Keyloggers* com capacidade de capacidade de captura de tela.

Então em 2006, o Banco do Brasil começou a solicitar o cadastramento prévio de computadores para realização de transações financeiras, onde, o cliente acessava o computador que deseja liberar, colocava um "apelido" para este

computador e posteriormente liberava pela Central de Atendimento, Internet (outro computador já cadastrado), ATM's ou pessoalmente nas agências BB, apesar de ter diminuído as fraudes continuaram mas com uma maior especialização, com uso de engenharia social para obtenção de dados pessoais dos cliente e posterior liberação do computador pela Central de Atendimento ou através de acesso remoto simultâneo ao computados do cliente.

A partir de 2013, o Banco do Brasil realizou a compra de um sistema, que identifica automaticamente o computador de acesso do cliente, reconhece se o computador está liberado ou não e, caso não esteja, solicita a liberação através de uma mensagem SMS, desde que o celular do cliente esteja previamente cadastrado.

Em 2012, a partir de pesquisas de doutorado, de funcionários do Banco do Brasil, foi criado o *BB Code*, uma tecnologia baseada nos leitores de *QR CODE (Quick Responde Code)*, que são códigos de barras bidimensionais que podem ser escaneados digitalmente, através de uma câmera de celular, muito utilizada atualmente. Quando o cliente adere a está solução de segurança em um computador é exibido um *Qr Code*, é necessário que se faça a leitura de um celular que será utilizado para confirmação posteriores, depois o cliente se dirige a um ATM e faz a confirmação utilizando o mesmo celular que foi primeiramente autorizado na internet. Quando o cliente realizar uma operação na sua conta, o sistema irá apresentar um *QR* Code, somente o celular habilitado estará apto a realizar a leitura do *QR Code* e será disponibilizado um código de seis dígitos para confirmação da transação. Não é necessário que o celular esteja ligado a internet, já que toda informação necessária para autorizar uma transação é apresentada através do *QR Code* na tela do computador e como esses dados estão cifrados, apenas o Smartphone do cliente poderá decodificar e gerar o código autorizador específico para aquela transação em particular.

Para o gerente executivo da Diretoria de Gestão da Segurança do Banco do Brasil, Luiz Fernando Ferreira Martins, a solução é totalmente inovadora.

> A solução tecnológica que deu origem ao BB Code já tem pedido de registro de patente depositado junto ao INPI. Não há nada parecido no mercado da tecnologia de segurança. Banco do Brasil S/A. Brasília, 2012 em: <http://w ww.bb.com.br/pbb/pagina-onicial/imprensa/n/33936/BB%20lan %C3%A7a% 20nova%20tecnologia%20de%20 seguran%C3%A7a%20para%20inTernet %20banking#/> Acesso: 29 nov. 2016.

Com mais de quatro anos de utilização e mais de quinhentas mil adesões, a ferramenta se mostrou muito segura, não tendo registros de fraudes dos clientes que utilizam o sistema.

> Desde a criação da ferramenta, em 2012, não há registro de fraudes no seu uso: ela mantém a expressiva marca de 100% de aproveitamento em segurança contra fraudes eletrônicas. Banco do Brasil S/A. Brasília, 2016 em: <http://www.bb.com.br/pbb/pagina-inicial/imprensa/n/52652/BB%20vai%20ampliar%20uso%20do%20BB%20Code%20no%20internet%20banking%20para%20seis%20milh%C3%B5es%20de%20clientes#/> Acesso: 29 nov. 2016.

A intenção do Banco do Brasil é aumentar significativamente o número de usuários do sistema.

> O Banco do Brasil iniciou no último mês de maio uma estratégia para a oferta massificada da tecnologia conhecida como BB Code, para a autenticação de transações via internet. A meta do BB é levar a solução para novos seis milhões de usuários. A adesão à ferramenta, que pode ser baixada em smartphones, é rápida e inteiramente gratuita. Numa etapa inicial, o BB Code será oferecido para 2,4 milhões de clientes do Banco, usuários frequentes do autoatendimento na internet e pelo mobile. Banco do Brasil S/A. Brasília, 2016 em: <http://www.bb.com.br/pbb/pagina-inicial/imprensa/n/52652/BB %20vai%20ampliar%20uso%20do%20B%20Code%20no%20internet%20banking%20para%20seis%20milh%C3%B5es%20de%20clientes#/> Acesso: 29 nov. 2016.

Com base no que foi exposto e o que foi estudado por Pavitt, podemos considerar que o sistema bancário está incluído nos setores na ciência, que trabalham no desenvolvimento de novos produtos.

## CONSIDERAÇÕES FINAIS

Ao finalizar este estudo pode-se observar que a inclusão das novas tecnologias da comunicação, especialmente nos serviços consolidados no campo da Internet, as relações comerciais passaram a adotar novas configurações visando atender as demandas especificas, como no caso do contexto mercadológico que abrange as instituições bancárias e seu relacionamento com seus clientes.

Desta forma, a integração das inovações em tecnologia com os diversos ambientes econômicos trouxe uma realidade que mudou o desenvolvimento destes setores. Assim, as organizações, incluindo-se aqui as instituições bancárias, visualizaram a importância de integrar as novas tecnologias e passaram a fazer uso frequente das mesmas para atender os diversos contextos de seus negócios. Por isso as instituições bancárias passaram a visualizar na Internet uma realidade que tinha potencial de incrementar seus negócios e projetar de maneira positiva sua imagem em um mercado de grande competição. Esta constatação encontrou respaldo no referencial teórico analisado e que trouxe a confirmação de que a relação desenvolvida entre os bancos e seus usuários mostra que o processo de comunicação que os bancos e seus consumidores protagonizaram foi permeado pelas inovações tecnológicas que o setor tem adotado, cujo desenvolvimento foi respaldado e paralelo ao desenvolvimento econômico brasileiro.

É indiscutível que a inovação das tecnologias da informação desenvolveu novos mecanismos que propiciaram uma maior interação entre banco e cliente, como o caso especifico do Internet Banking, que trouxe como benefícios a diminuição dos custos bancários, a redução da superlotação das agências, entre outras coisas. Contudo, a vulnerabilidade desse contexto propiciou o aumento considerável do número de fraudes bancárias, que surgiram devido a falhas do sistema eletrônico ou pela falta de informação de segurança dos clientes no que diz respeito a adoção de medidas de proteção ao utilizar a rede.

Algumas peculiaridades relacionadas aos riscos de ocorrência de fraudes na utilização dos serviços bancários pelo internet banking pode-se perceber que este tipo de ataque tem se sofisticado posicionando as instituições bancárias e seus clientes em uma situação de desconforto, em face das possiblidades de prejuízos financeiros.

Diante disso pode-se concluir, atendendo o objetivo proposto para este estudo, que as inovações tecnológicas que surgiram no âmbito da segurança da informação vieram como resposta ao desenvolvimento das fraudes eletrônicas e devido a necessidade de apresentar uma solução dos problemas de segurança do setor bancário, a partir do que os bancos se viram diante da necessidade de dispor de novos produtos para atender seus clientes com segurança, passaram a avaliar as condições de segurança de seus produtos e serviços. O ciclo se fecha pois quando os bancos identificam os problemas de segurança da informação, recorrem aos seus fornecedores de tecnologia para possibilitar as devidas soluções, resultando no surgimento de inovações tecnológicas ou melhorias nas tecnologias existentes.

Visando superar a insegurança promovida pelas fraudes bancárias as instituições bancárias passaram a utilizar tecnologias como *ATMs*, computadores, *internet*, *mobile, QR Code* e computação em nuvem que tiveram que passar por um processo de adaptações que se caracteriza como inovações tecnológicas desenvolvidas no âmbito da segurança da informação. Diante disso, pode-se destacar que as evidências observadas ao longo deste estudo mostraram que a economia demanda soluções tecnológicas visando minimizar prejuízos com fraudes e aumentar sua eficiência.

Os bancos sempre foram de encontro às necessidades de seus clientes, o que demanda que estas instituições desenvolvam novos serviços e produtos que apresentem diferenciais competitivos aliados a elevado grau de inovações em suas operações. Por isso, acredita-se que o número de transações bancárias que é disponibiliza os clientes do Internet banking tem aumentado. Contudo, mesmo em face da diversidade de transações oferecidas por meio do canal virtual e os consequentes investimentos realizados em segurança, as fraudes bancárias têm feito com que as instituições bancárias repensem seus procedimentos em termos de inovação buscando ferramentas tecnológicas que devolvam ao usuário a segurança de utilizar estes serviços pela internet.

Percebe-se que a Internet ainda é utilizada apenas como um canal adicional de vendas. Para ampliar a sua utilização, aperfeiçoando a qualidade de seus serviços, os bancos deverão trabalhar e divulgar as iniciativas e processos inseridos visando aumentar a segurança do meio transacional.

## REFERÊNCIAS


ADACHI, Tomi. Gestão de segurança em internet banking: estudo de casos brasileiros. Dissertação de Mestrado em Administração de Empresas. São Paulo: Fundação Getulio Vargas, 2004.

AVELINO, Daniel Angelo. **Fraudes eletrônicas em bancos brasileiros e a proteção dos clientes através da conformidade**. Monografia de Especialização. Belo Horizonte: Belo Horizonte, 2011.

AZEVEDO, Carlos Eduardo Mendes de. **Aspectos de responsabilidade civil em fraudes eletrônicas no Internet Banking**. Artigo de Conclusão de Curso. Rio de Janeiro: Escola de Magistratura do Estado do Rio de Janeiro, 2012.

BARROS FILHO, José Nabuco Galvão. Algumas observações sobre o estelionato. A questão da pessoa induzida em erro. **Jus Navigandi**. Teresina, n. 2644, set. 2010.

BASTOS, Paulo Sérgio Siqueira; PEREIRA, Roberto Miguel. Fraudes eletrônicas: o que há de novo? **Revista de Contabilidade do Mestrado em Ciências Contábeis da UERJ**. Rio de Janeiro, v.12, n. 2, p. 1, mai./ago. 2007.

BERNARDES, Roberto; BESSA, Vagner e KALUP, André. A economia da inovação no setor de serviços: desvendando o cenário brasileiro. **São Paulo em Perspectiva**, v. 19, n. 2, p. 115-134, abr./jun./2005.

BOCCHINI, Bruno. **Fraudes eletrônicas ocorrem principalmente pelo comportamento dos clientes**. (2012) Disponível em: http://www.ebc.com.br/2012/11/fraudes-eletronicas-bancarias-ocorrem-principalmente-pelo-comportamento-dos-clientes. Acesso feito em set./2014.

CAMPANARIO, Milton de Abreu. **Tecnologia, Inovação e Sociedade**. VI Módulo de la Cátedra CTS I. Colombia, set./2002.

CASTELLS, Manuel. **A sociedade em rede**. A era da informação: economia, sociedade e cultura. 2. ed. São Paulo: Paz e Terra, 1999.

CERT.br - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Cartilha de Segurança para Internet 3.1**. Disponível em: http://cartilha.cert.br/sobre/old/cartilha_seguranca_3.1.pdf. Acesso feito em set./2014.

CHANG, Joshua J.S. An analysis of advance fee fraud on the Internet. **Journal of Financial Crime**, v. 15, n. 1, p. 71-81, 2008.

CHORAFAS, Dimitris N. Strategic Planning For Electronic Banking. London: Butterworths & Co. Ltd, 1987.

CONDE, Mariza Velloso Fernandez e JORGE, Tania Cremonini de Araujo. Modelos e concepções de inovação: a transição de paradigmas, a reforma da C&T brasileira

e as concepções de gestores de uma instituição pública de pesquisa em saúde. **Ciênc. saúde coletiva**, v. 8, n. 3, p. 727-741, 2003.

CARLOTO, Leandro. **Breve comentário histórico sobre a segurança da Internet Banking no Brasil**. Disponível em: http://leandrocarloto.jusbrasil.com.br/artigos/111941203/breve-comentario-historico-sobre-a-seguranca-da-internet-banking-no-brasil?ref=home. Acesso feito em set./2014.

COSTA, Sergio Francisco. **Método científico**: os caminhos da investigação. São Paulo: Editor Harbra. 2001.

DAMIANO, Andre Luis. **As fraudes no internet banking e sua evolução para o social banking**. Dissertação de Mestrado. São Carlos: Escola de Economia da Universidade de São Paulo, 2013.

DEMO, Pedro. **Introdução à metodologia da ciência**. 2 ed. São Paulo: Atlas, 1987.

DEZA, Xavier Vence. Economía de la Innovación y del cambio tecnológico. México: Silgo Veintiuno Editores S/A, 1995.

FEBRABAN. A sociedade conectada - Setor Bancário em Números, Tendências Tecnológicas e Agenda Atual. CIAB FEBRABAN 2012 Disponível em: http://www.febraban.org.br/7Rof7SWg6qmyvwJcFwF7I0aSDf9jyV/sitefebraban/Pesquisa%20CIAB%20FEBRABAN%202012.pdf. Acesso feito em, set./2014.

_____. **Perdas com fraudes eletrônicas aumentam 36% no primeiro semestre de 2011**. Disponível em: http://www.febraban.org.br/noticias1.asp?id_texto=1321&id_pagina=61&palavra=fraudes%20eletr%f4nicas. Acesso feito em set./2014.

FLETCHER, Nigel. Challenges for regulating financial fraud in cyberspace. **Journal of Financial Crime**. Vol. 14, n. 2, 2007, p. 190-207.

FRONZAGLIA, Thomaz e VEGRO, Celso Luís Rodrigues. **Nanotecnologia e inovação no agronegócio.** (2005) Disponível em: http://www.iea.sp.gov.br/out/LerTexto.php?codTexto=1667. Acesso feito em set./2014.

GARCIA, Eduardo Alfonso Cadavid. **Manual de sistematização e normalização de documentos técnicos.** São Paulo: Atlas, 1998.

GARTNER, Susan Moore. **Gartner Says Worldwide Information Security Spending Will Grow Almost 8 Percent in 2014 as Organizations Become More Threat-Aware**. (2014) Disponível em: http://www.gartner.com/newsroom/id/2828722. Acesso feito em set./2015.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa.** 4. ed. São Paulo: Atlas, 2002.

GONSALVES, Elisa Pereira. **Conversando sobre iniciação a pesquisa científica**. 3 ed. Campinas, SP: Editora Alínea, 2003.

GUEDES, Edmárcio Cerqueira. **Fraudes no *Internet Banking*:** Conceituação e Estado Atual dos Mecanismos de Defesa. Monografia de Graduação em Informática com ênfase em Gestão de Negócios. São Paulo: Faculdade de Tecnologia da Zona Leste, São Paulo, 2009.

KOVACH, Stephan. **Detecção de fraudes em transações financeiras via internet em tempo real**. Tese de Doutorado em Engenharia Elétrica. São Paulo: Escola Politecnica da Universidade de São Paulo, 2011.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. **Técnicas de pesquisa**. 5 ed. São Paulo: Atlas, 2002.

_____. **Metodologia do trabalho científico**. 7 ed. São Paulo: Atlas, 2007.

LAR, Saleem-Ullah; LIAO, Xiaofeng; REHMAN, Aqeel ur; MA, Qinglu. **Proactive Security Mechanism and Desing for Firewall**. International Journal of Information Security. 2011.

LAU, Marcelo. **Análise das fraudes aplicadas sobre o ambiente internet banking**. Dissertação de Mestrado. São Paulo: Escola Politécnica da Universidade de São Paulo, 2006.

MACHADO, Antonio Carlos. **Comunicação para prevenção de danos ao consumidor com o uso da internet**. Dissertação de Mestrado. São Caetano do Sul: Universidade Municipal de São Caetano do Sul, 2011.

MELLO, Roberto Agostinho de; STAL, Eva; QUEIROZ, Ana Carolina S. O Banco na Internet: Inovações em Tecnologia da Informação Moldam Novos Serviços Bancários. **30º Encontro da ANPAD**. Salvador, set. 2006.

MICHEL, Maria H. **Metodologia e pesquisa científica em ciências sociais**: um guia prático para acompanhamento da disciplina e elaboração de trabalhos monográficos. 2ª ed. São Paulo: Atlas, 2009.

NAÍM, Moisés. **Ilícito**: o ataque da pirataria, da lavagem de dinheiro e do tráfico à economia global. Rio de Janeiro: Zahar, 2006.

NUNES, Danilo Arthur de Oliva. **A responsabilidade eletrônica das instituições bancárias.** Revista Unifacs, 2014. Disponível em: http://www.revistas.unifacs.br/index.php/redu/article/download/3129/2252. Acesso feito em set./2015.

PEREIRA FILHO, Valdir Carlos. Responsabilidade civil dos bancos em operações financeiras realizadas pela internet. **Revista de Direito Bancário e do Mercado de Capitais**, v. 11, n. 42, p. 163-181, out./dez. 2008.

RAMON, Miguel. **Fraudes eletrônicas**. (2008) Disponível em: http://slideplayer.com.br/slide/293331/#. Acesso feito em set./2014.

RAUEN, Fábio José. **Elementos de iniciação à pesquisa.** Rio do Sul: Nova Era, 1999.

REZABAKHSH, Behrang; BORNEMANN, Daniel; HANSEN, Ursula; SCHRADER, Ulf. Consumer Power: A Comparison of the Old Economy and the Internet Economy. **Journal of Consumer Policy**, n. 29, p. 3-36, 2006.

SANTOS, Adriana Maria dos. **A influência do Gerente de Conta no uso do *Internet Banking* pelo cliente alta renda no Brasil:** um Estudo de Caso. Dissertação (Mestrado em Administração de Empresas). Fundação Getúlio Vargas: Escola de Administração de Empresas de São Paulo, 2007.

SARMA, Gunajit; SINGH, Pranav Kumar. Internet Banking: Risk Analysis and Applicability of Biometric Technology for Authentication. **Int. J. Pure Appl. Sci. Technol**., v. 1, n. 2, p. 67-78, 2010.

SCHUMPETER, Joseph. **Capitalismo Socialismo e democracia**. Rio de Janeiro: Editora Fundo de Cultura, 1961.

SILVA, Regina Celia Marques Freitas; OLIVEIRA, Paulo de Tarso. O aluno de administração, os avanços tecnológicos no setor bancário e o comportamento do consumidor. **Facef pesquisa**. Franca, v. 4, n. 2, p. 11-123, 2001.

SILVA, Fabio Alves da. **A evolução das tecnologias de segurança da informação a partir das demandas do setor financeiro**. Dissertação de Mestrado em Desenvolvimento Econômico. Curitiba: Universidade Federal do Paraná, 2014.

SOARES, Karla. **Internet banking**: dicas de segurança para se proteger das fraudes. (2014) Disponível em: http://www.techtudo.com.br/noticias/noticia/2014/04/internet-banking-dicas-de-seguranca-para-se-proteger-das-fraudes.html. Acesso feito em set./2014.

STAUB, Eugenio. **Desafios estratégicos em ciência, tecnologia e inovação**. Brasilia: Conferencia Nacional de Ciencias, Tecnologia e Inovação, set./2001.

SYDOW, Spencer Toth. **Crimes informáticos e suas vitimas**. 2 ed. São Paulo: Saraiva, 2015.

TRIVIÑOS, Augusto Nibaldo Silva. **Bases teórico-metodológicas da pesquisa qualitativa em ciências sociais**: ideias gerais para a elaboração de um projeto de pesquisa. 2. ed. Porto Alegre: Faculdades Integradas Ritter dos Reis, 2001.