Faculdade de Tecnologia de Americana
Curso de Segurança da Informação

Segurança da Informação do Sistema Bancário

Matheus de Mira Aoqui

Americana, SP
2011

Faculdade de Tecnologia de Americana
Curso de Segurança da Informação

Segurança da Informação do Sistema Bancário

Matheus de Mira Aoqui

aoqui.mts@gmail.com

Trabalho de conclusão de curso para obtenção de grau de Tecnólogo em segurança da Informação da Faculdade de Tecnologia de Americana, sob orientação do Prof. Irineu Ambrozano Filho.

Americana, SP
2011

BANCA EXAMINADORA

Prof. Irineu Ambrozano Filho (Orientador)

Prof. Rogério Nunes de Freitas (Convidado)

Prof. Antonio Alfredo Lacerda (Presidente da Banca)

AGRADECIMENTOS

A Deus pela vida, a minha familia pelos ensinamentos. A Talma sempre presente, me dando força e atenção. Aos meus colegas de trabalho do Banco. Ao meu orientador Irineu Ambrozano Filho, pela disposição em ajudar. Meus agradecimentos a todos que contribuíram direta ou indiretamente, para o resultado deste trabalho que tem um pouco de cada um de vocês!

DEDICATÓRIA

Aos professores da Faculdade de Tecnologia de Americana que me orientaram a cada etapa para o desenvolvimento desse trabalho.

À minha família, pela educação, motivação e confiança que se sempre me deram.

À minha companheira, pela compreensão, força e auxilio que me deu durante o tempo de desenvolvimento atribuído a este trabalho.

Aos colegas e professores do curso, já que juntos caminhamos uma etapa fundamental de nossas vidas.

RESUMO

A segurança dos espaços eletrônicos como a internet tem sido largamente debatida por diversas áreas acadêmicas de forma variadas por abranger tecnologia e recursos humanos.

Sob essa assertiva os bancos foram os pioneiros a adotar a internet como meio de se relacionar com seus clientes. Dessa forma, os bancos permitiram o acesso aos seus clientes em rede pública, no entanto, juntamente a isso sobreveio a vulnerabilidade para fraudes e crimes cibernéticos, já que as aplicações financeiras circulam e se materializam no meio digital.

O presente texto desenvolverá um assunto que ultimamente vem instigando a curiosidade das pessoas, por se mostrar um ponto vulnerável dos bancos diante de um ambiente como a web, qual seja a segurança em internet banking.

Os riscos, com os quais os bancos suportam, no mundo físico, se refletem, de forma particular, na internet, onde as fraudes e delitos financeiros, bem como problemas com a imagem do banco, ocorrem em uma velocidade não experimentada em tempos remotos.

É perceptível, que a internet gerou a redução de custos das instituições financeiras, no entanto, concomitantemente possibilitou um novo espaço para as ameaças e tentativas de invasão aos seus sistemas e aplicativos. Para isso, caso os riscos e investimentos em segurança não adequados, o banco, bem como seus clientes, pode sofrer perdas financeiras, em vez de benefícios com redução de custos.

Palavras Chave: internet banking - fraude - segurança.

ABSTRACT

The security of electronic spaces such as the Internet has been widely discussed by various academic areas in order to cover various technology and human resources.

Under this statement the banks were the pioneers to adopt the Internet as a means to relate to their customers. Thus, banks are allowed access to their clients in public, however, came along with it the vulnerability to fraud and cyber crimes, since the investments circulate and materialize in the digital environment.

This paper will develop a topic that lately has been stirring up the curiosity of people turning out to be a vulnerable spot on the banks of an environment like the web, what is the security in Internet banking.

The risks with which banks support in the physical world, reflected in a particular way, the Internet, where fraud and financial crimes, as well as problems with the image of the bank, occurring at a rate not experienced in ancient times.

It is noticeable that the Internet has created the reduction of costs of financial institutions, however, simultaneously allowed a space for new threats and attempts to hack into their systems and applications. To do so, if the risks and investment in safety is not adequate, the bank and its clients may suffer financial losses rather than benefits with cost reduction.

Keywords: internet banking - fraud - security.

ABREVIATURAS E SIGLAS

AC – Autoridade de Certificação

AR – Autoridade de Registro

ARPA – Advanced Research Projects Agency

ARPANET - Advanced Research Projects Agency Network

CPD's - Centro de Processamento de Dados

HTML - HiperText Markut Language

HTTPS - HyperText Transfer Protocol Secure

IP - Internet Protocol

MAC - Message Authentication Code

MILNET - Military Network

PC - personal computer

RNP – Rede Nacional de Ensino e Pesquisa

SGBD's - Sistema de gerenciamento de banco de dados

SSL - Secure Sockets Layer

TI – Tecnologia da Informação

UCE - Unsolicited Commercial E-mail

WWW – *World Wide Web*

LISTA DE FIGURAS

LISTA DE TABELAS

Sumário

INTRODUÇÃO

É perceptível que os computadores estão presentes de forma constante em nossos dias, são nos nossos relógios até nos fogões que aquecem a nossa comida, passando pelos freios dos carros, telefones, celulares, dentre outros. No entanto, a informática não se limita exclusivamente à produção de máquinas e equipamentos, mas também na transferência de notícias, troca de dados e informações, além da consignação de novos condutos de comunicação entre as pessoas, permitindo a concepção de um novo modo de realizar negócios.

O tema Internet Banking é essencial por tratar-se de um prestigioso instrumento financeiro. A Internet, advinda pelo desenvolvimento da tecnologia da comunicação, já é indispensável na vida do homem contemporâneo e vem alterando completamente os padrões de negócio e a história da comunicação no mundo.

Compreendendo que serviço é um ato ou desempenho oferecido por uma parte à outra[1], é a Internet Banking um serviço da economia moderna.

Aprender Internet Banking é um desafio que conduz a delinear os tipos de negócio que este influente utensílio pode alcançar. A Internet por si só já acende variações na vida de cada pessoa, que já aproveita este elemento de comunicação e, sobretudo, na vida daqueles que experimentam profunda rejeição ao uso deste produto da tecnologia.

O desígnio do presente trabalho tem como **objetivo geral** apresentar o âmbito da internet bem como do sistema de informação, com o fim de se chegar as diferentes feições da internet banking e as ameaças que por ventura sofre. Já como **objetivo especificou** buscou-se oferecer os meios de segurança que permitem assegurar o fiel uso desse utensílio importante. Para isso o **método científico utilizado** foi com base em pesquisas realizadas via internet, como também em referencias literárias e orientações com profissionais da área de TI, com intuito de complementar o tema em litígio, tendo em vista que a internet banking se apresenta como um dos engenhos do desenvolvimento do comércio eletrônico, considerando o mundo globalizado no qual nós vivemos.

Dessa forma, o trabalho foi estruturado em sete capítulos, sendo que o primeiro apresenta um breve histórico do surgimento da internet com o fim de se dar

[1] Conforme dicionário Universal da Língua Portuguesa, acto ou efeito de servir; utilidade ou préstimo de alguma coisa.

um ponto de partida para o desenvolvimento do trabalho, sendo seguido do segundo capitulo que aborda sobre a tecnologia da informação, tratando a respeito de seu conceito e como se desenvolveu para chegar até o que nos dias atuais. Assim, dentro desse capitulo são apresentados outros capítulos que se interligam ao apresentar os aspectos de segurança na TI, seguido dos sistemas bancários com o fim de se chegar ao intuito desse trabalho: internet banking.

O terceiro capítulo traz consigo as ameaças que por ventura surgem e podem trazer danos aos usuários da tecnologia, como por exemplo, vírus, fraude, dentre outros. Já o quarto capítulo, que é o fim específico desse trabalho, traz os meios de proteção para garantir o uso leal da ferramenta internet banking, diga-se apresenta quais os meios de segurança utilizados para garantir o amparo do instrumento tecnológico.

E por fim, o quinto capítulo foi reservado exclusivamente para abordar sobre o selo digital, o qual é um tema bem discutido nos dias atuais.

Com base nas informações conseguidas a partir dos estudos realizados no capítulo anterior, o sétimo capítulo se reserva às considerações finais.

Figura 1 – internet banking

Fonte: The Advantages of Online or Internet Banking

(http://allaboutindiancelebrities.blogspot.com/2011/04/advantages-of-online-or-internet.html)

2. HISTÓRIA DA INTERNET

O meio de comunicação mais popular dos ultimos tempos – a Internet – surgiu nos tempos remotos da Guerra Fria, por intermédio de pesquisas militares. Na década de 1960 duas grandes potencias mundiais politicamente antagônicas – EUA e Rússia – exerciam um vasto poder e influencia sobre o resto do mundo. A disputa entre essas potencias era tão acirrada que qualquer inovação poderia contribuir na liderança. Foi a partir desse ponto que observou-se a necessidade dos meio de comunicação.

Diante desse cenário o governo dos EUA suspeitava constantemente que a União Soviética viesse a atacar suas bases militares, uma vez que o ataque proporcionaria a divulgação a público de dados sigilosos, tornando, dessa forma, os EUA derrotável.

Nessa perspectiva, foi planejado um modelo de troca e compartilhamento de informações que permitisse a sua descentralização[2] , de certa forma que se o Departamento de Defesa dos EUA fosse atingido, os dados nele contidos não estariam extraviados. Para isso, tornou-se necessário a criação de uma rede para o armazenamento e compartilhamento de informações, a qual a ARPA – *Advanced Research Projects Agency* – criou e denominou de *ARPANET.*

A rede galáxia – como muitos a chamavam - desenvolvia-se por meio de um sistema de *chaveamento de pacotes*, ou seja, ocorria a condução de dados em rede de computadores no qual estes eram divididos em pequenos pacotes, os quais armazenam trecho das informações, endereço do destinatário e informações que possibilitam a busca da mensagem original[3].

Entretanto o ataque em que temia os EUA nunca ocorreu e o Pentágono jamais imaginou que estava dando a partida a maior manifestação midiático do século XX.

Foi em Outubro de 1969 que aconteceu a primeira transmissão denominada E-mail[4]. No ano seguinte, a disputa entre as grandes potencias amenizou,

---

[2] BOGO, Kellen Cristina. **História da Internet.** Diponível em http://www.kplus.com.br/materia.asp?co=11&rv=Vivencia. Acesso em 21/03/2011 ás 10:03.

[3] A.I.S.A. **História da Internet.** Diponível em http://www.aisa.com.br/historia.html. Acesso em 21/03/2011 ás 10:10

[4] DIÁRIO DIGITAL. **Primeira mensagem de correio electrónico enviada há 40 anos.** Disponível em http://diariodigital.sapo.pt/news.asp?section_id=18&id_news=417591. Acesso em 21/03/2011 ás 10:24.

caracterizando um momento histórico conhecido como Coexistencia Pacífica. Dessa forma, foi possivel nos EUA o desenvolvimento da ferramenta de compartilhamento – ARPANET -, permitindo o seu acesso nas universidades em que o estudo fosse voltado na área de defesa. No entanto, a ARPANET deparou-se com dificuldades para administrar todo este sistema, diante do aumento no numero de acesso nas diversas localidades universitárias.

Isto posto, surgiu a necessidade de dividir o sistema em duas partes – MILNET, a qual contia as localidades militares, e a nova ARPANET, que detinha as não militares. Nessa perspectiva foi possivel a ocorrencia de uma ambiente mais livre, ou seja, pesquisadores, alunos e amigos dos alunos, poderiam ter acesso aos estudos já compreendidos, possibilitanto também o aperfeiçoamento do sistema[5]. Consequentemente, cada vez mais jovens contribuiram decisivamente para a formação da Internet como é hoje conhecida: “a internet é, acima de tudo, uma criação cultural”[6].

Com seu desenvolvimento surgiu o *Internet Protocol* – Protocolo de Internet -, ou seja, uma programação que possibilitava a circulação de dados fosse transmitida de uma rede a outra. Essas redes eram então conectadas pelo endereço IP – que indica o local de um equipamento[7] -, o que permitia a troca de mensagens.

Vale a pena ressaltar que por intermédio da *National Science Foundation* os EUA desenvolveram a espinha dorsal – *backbones* -, isto é, criou computadores incomparável potencial na epoca que eram conectados por linhas que possibilitavam uma capacidade maior para a transmissao de informações, como por exemplo elos de satélite e transmissao por rádio.

Contudo, foi com a empresa *Netscape* (empresa norte americana) que foi possivel a criação e desenvolvimento do protocolo *https,* o qual permitia a circulação de informações por meio de uma conexão criptografada para transações comerciais em que seja possível a verificação da autenticidade do servidor e do cliente através de certificados digitais.

---

[5] BOGO, Kellen Cristina. **História da Internet.** Diponível em http://www.kplus.com.br/materia.asp?co=11&rv=Vivencia. Acesso em 21/03/2011 ás 10:03.

[6] CASTELLS, Manuel. **A Galáxia da Internet.** Diponível em http://www.edrev.info/reviews/revp49.pdf. Acesso em 21/03/2011 ás 10:35.

[7] ALECRIM, Emerson. **Endereço IP**. Disponível em http://www.infowester.com/internetprotocol.php. Acesso em 21/03/2011 ás 10:45.

No inicio a Internet disponibilizava poucos serviços. Os principais serviços eram essencialmente o E-mail, um básico serviço de chat, a transferencia de arquivos via FTP, dentre outros.

Em 1990, o cientista *Tim Berners-Lee*, da CERN lançou o WWW – *World Wide Web*, que foi base para diversos desenvolvimentos de sistemas, sendo um deles criado para a versão do Windows. Esse sistema tinha como finalidade a navegação de uma pagina a outra, sem complexidade. Na perspectiva desse sistema era possível criar um conteudo utilizando um simples editor de texto e linguagem, que ficou conhecido como *HTML - HiperText Markut Language*[8].

No Brasil, contudo, esse procedimento iniciou mais tardiamente. Apenas em 1988 é que os primeiros rumores da rede surgiram, e com Ibase é que foi possível testar o primeiro sistema brasileiro de Internet não academica e não governamental: a *AlterNex*. No ano seguinte, o Ministério da Ciencia e Tecnologia implantou um projeto denominado RNP – Rede Nacional de Ensino e Pesquisa -, que tinha o objetivo de desenvolver uma rede academica de alcance nacional, em que permitisse a capacitação de recursos de alta tecnologia e a difusão com a Internet por meio da implementação da primeira infra-estrutura nacional que ligasse todos os pontos de uma rede – *backbone*[9]*.*

Entretanto, somente em 1995 é que foi possível o fornecimento dessa infra-estrutura aos acessos comerciais. Com o crescimento da Internet ao acessos comerciais, uma nova fase na Internet brasileira teve inicio em 1997, onde com consequencia do aumento nos acessos ocorreu a necessidade de uma infra-estrutura mais eficaz e segura, o que levou, dessa forma, aos investimentos em tecnologias novas.

Diante dessa da carencia de uma sistematização de fibra óptica que se extendesse em todo o territorio nacional, os investimentos voltaram-se para o desenvolvimento de redes locais que trabalhassem com mais eficácia. Um desses investimentos ocorreu em 2000, quando foi implantado o *backbone RNP2*, com o fim de conectar todo o territorio nacional em um rede de tecnologia avançada.

---

[8] ZEVALLOS, Ruben. **A História da Internet.** *Artigonal Diretório de Artigos Gratuitos.* Disponível em http://www.artigonal.com/ti-artigos/a-historia-da-internet-737117.html. Acesso em 21/03/2011 ás 11:27.

[9] ROSE, Lílian. **A Ética da Internet Anonimato e Impunidade, Liberdade e Censura**. Diponível em http://www.adtevento.com.br/INTERCOM/2007/resumos/R0211-1.pdf. Acesso em 21/03/2011.

Em 2002 a RNP foi transformada em uma organização social, devido ao avanço que alcançara. Consequentemente conquistou administrativamente uma maior autonomia na perspectiva das realizações de tarefas, possibilitando ao poder publico meios mais rápidos para avaliar e cobrar resultados.

Cabe ressaltar que o Brasil já movimentou em 2008, no comércio eletronico, 114 bilhões de doláres, um aumento de 82% sobre o volume de 2005[10]. E tendo em vista essas análises pode-se perceber que cada vez mais o numero de internautas no Brasil veio crescendo considerávelmente nos ultimos tempos. O seu desenvolvimento já foi verificado durante a década de 1990 em que estimou-se um crescimento de mais de 100%, tendo em vista o período de desenvolvimento explosivo entre 1996 e 1997[11].

Diante das análises apontadas, pode-se verificar que a tendência será pela busca da aprimoração do sistema, tendo em vista sempre o alcance da perfeição. Como consequencia verifica-se cada vez mais predominante o interesse dos usuários que buscam por esse meio obter conhecimento e atender os seus anseios, uma vez que estão diantes de uma ferramenta prática, rapida e eficaz, que traz consigo a facilidade e comodidade. Portanto, é possível observar o seu futuro sendo necessário compreender que ela – a internet – apresenta um avanço tão grandioso na perspectiva da troca de conhecimento que o “futuro” pode, muitas vezes, já estar disponível hoje, ou seja, ele pode estar presente e ninguem se quer sabe.

[10] A.I.S.A. **História da Internet.** Diponível em http://www.aisa.com.br/historia.html. Acesso em 21/03/2011 ás 10:10.

[11] ÉDIPO, Luciano. **Internet**. Disponível em http://www.marketing.com.br/index.php?option=com_content&view=article&id=374:no-primeiro-trimestre-de-2008-a-internet-acompanhou-a-taxa-de-crescimento-trimestral-de-2007&catid=43:midias-digitais&Itemid=106. Acesso em 21/03/2011, ás 12:03.

3. TECNOLOGIA DA INFORMAÇÃO

Em tempos remotos tinha-se a presença dos computadores como máquinas grandes que possibilitavam a automatização de algumas atividades em instituições de ensino, bem como nas grandes empresas e nos meios governamentais. Contudo, diante do avanço da tecnologia estas gigantes máquinas foram perdendo o seu espaço para ferramentas cada vez menores e mais eficazes. O avanço foi tão marcante que os novos equipamentos permitiram uma comunicação sem estar no mesmo estabelecimento físico.

Entretanto, as definições de Tecnologia de Informação (TI) são tantas que nenhuma consegue atribuí-la por completo. O termo TI pode significar como uma união de todo o desenvolvimento e soluções providas por recursos de computação.

Frisa-se que é tamanha sua seiva em diversas áreas como finanças, planejamento de transportes, design, produção de bens, imprensa, produção musical, radio, televisão, dentre outros[12]. Sua presença é tão constante que se verifica um célere aperfeiçoamento e desenvolvimento de novas tecnologias de informação que insere novos meios de coordenação e acesso aos dados e produtos armazenados.

Ademais, este célere desenvolvimento promoveu e ativou a comunicação pessoal e institucional por intermédio de programas que processam textos, formatam banco de dados, transmitem documentos, enviam mensagens e arquivos, dentre outras funcionalidades. Ocorre, no entanto, que essa facilidade e intensificação do desenvolvimento de novas tecnologias permitiu, consequentemente, impasses quanto a privacidade e direito a informação dos usuários, pois uma grande quantidade de informações sobres estes podem ser coletadas por instituições particulares, como também públicas.

Sob esta perspectiva pode-se verificar que essa ferramenta sempre foi necessária, e ainda é nos dias atuais. Tendo isso em vista é cabível acercar

---

[12] KENN, Peter G. W. **Guia Gerencial para a tecnologia da informação: Conceitos essenciais e terminologia para empresas e gerentes**. Rio de Janeiro: Campus, 1996,p.XLIX.

previamente o contexto histórico da TI, iniciando a abordagem com a argumentação de que o desenvolvimento de TI se divide em quatro momentos históricos[13].

O primeiro momento, denominado como a Era do Processamento de dados, ficou marcado nas décadas de 60 e 70 pela sua importância nas grandes e médias empresas. Contudo em 1960 as aplicações eram limitadas e incompatíveis entre si, tendo em vista que não existiam empresas voltadas para o desenvolvimento de programas que permitissem um melhor condicionamento atrelado à velocidade dos equipamentos e suas respectivas atribuições. Diante disso, em 1970, foi desenvolvido o acesso a terminais remotos de computadores por linhas telefônicas que possibilitaram as empresas à automatização das funções burocráticas. Tem-se como base tecnológica, nessa época, as telecomunicações, as quais permitiram que o procedimento ocorresse em um Centro de Processamento de Dados (CPD's), ou seja, eram responsáveis pelo acolhimento das informações, que possibilitavam o acesso por meio de relatórios desenvolvidos pelos terminais ligados a máquina central[14].

O segundo momento, por sua vez, ficou conhecido como a Era dos Sistemas de Informações. Na década de 70 o desenvolvimento tecnológico permitiu acesso a novas oportunidades para a transformação de dados em informações, como também o aperfeiçoamento dos programas conforme a necessidade apresentada pela empresa. Nessa época o terminal se tornou flexível, o que possibilitou a realização de inúmeras atividades concomitantemente com vários usuários. Ademais, surgiram também pacotes de software, que eram combinados com a flexibilidade dos terminais, os quais estimulam uma série de inovações que ficaram conhecidas como: sistemas de apoio à decisão. Dessa forma, foi possível o aparecimento de programas de gerenciamento de dados – SGBD's – que coordenam as informações de uma forma dinâmica, a certo modo que evita a duplicidade e facilita a análise[15].

---

[13] RFTecnologia. **História da tecnologia**. Disponível em: http://www.rftecnologia.hd1.com.br/historiadatecn.htm. Acesso em 04/5/2011, ás 13:45.

[14] PACHECO, Roberto C.S; TAIT, Tania Fatima Calvi. **Tecnologia de Informação: Evolução e Aplicações.** Disponível em: http://www.upf.br/cepeac/download/rev_n14_2000_art6.pdf. Acessado em 06/5/2011, ás 12:01.

[15] RASKIN, Sara. **Uma arquitetura de tecnologia de informação**. XXV SEMINÁRIO NACIONAL DE INFORMÁTICA PÚBLICA, Anais, Salvador, Bahia, 1997.

Em 1980, diante de muitas mudanças tecnológicas, ficou-se diante da Era da Inovação e Vantagem Competitiva, momento este em que o termo TI passou a ser relevante. A tecnologia dos gerenciadores de banco de dados passaram ser acessados nos PCs e software de baixo custo tornou-se mais evidente no mercado, fazendo com que fosse maior a busca por novas habilidades com base das tecnologias de TI. Consequentemente desenvolveu-se programas de conscientização gerencial, como também Centro de suporto ao usuário – Help Desk – no qual o usuário consulta o Centro para tirar suas dúvidas, alem de receber consultoria na área, ambos com o fim de permitir a ciência das ferramentas de TI existentes. No entanto, mesmo diante desses avanços tecnológicos os computadores ainda eram incompatíveis entre si, o que dificultava a integração dos sistemas e uma maior flexibilidade. Foi sob essa perspectiva que se buscou a descentralização[16].

Por fim, o ultimo e quarto momento histórico da Tecnologia de Informação, foi a Era da Integração e Restauração do Negócio. Este momento ocorreu em meados de 1990, onde a integração, modelos e sistemas tornaram-se essenciais, acabando, dessa forma, com a incompatibilidade. Essa integração permitiu a flexibilização, acesso e troca das informações. De fato, nessa época, TI ficou reconhecida como fator critico de capacitação, principalmente através das telecomunicações, que permite eliminar barreiras impostas por local e tempo às atividades de coordenação, serviço e colaboração[17].

Sob esta perspectiva verificou-se uma forte aceleração nas áreas da tecnologia, de certo modo que o usufruto dos instrumentos da TI passaram a ser globais, extinguindo qualquer distinção antes existente entre o computador e a comunicação, e conseqüentemente alterando radicalmente o mundo dos negócios.

Isto posto, pode-se observar que nesses últimos tempos, tem avançado a perspectiva e o questionamento acerca do desempenho da TI, tanto nas publicações acadêmicas como aquelas voltadas aos executivos e empresários como também, naquelas voltadas ao público em geral. Ao mesmo tempo em que nascem equívocos acerca dos efeitos provenientes dos investimentos em TI, há uma condição de

---

[16] WALTON, Richard E. T**ecnologia de informação - o uso de TI pelas empresas que obtêm vantagem competitiva**. Trad. Edson Luiz Riccio. São Paulo: Atlas, 1994.

[17] KENN, Peter G. W. **Guia Gerencial para a tecnologia da informação:** Conceitos essenciais e terminologia para empresas e gerentes. Rio de Janeiro: Campus, 1996,p.XLIX.

"sedução" com as aplicações de TI que proporcionam mecanismos da chamada "economia globalizada"[18].

Diante desse aspecto se constata que a evolução da TI ocorreu de uma direção tradicional de suporte administrativo para uma função ardilosa dentro da organização. Essa visão astuciosa da TI como instrumento estratégico competitivo ampara as intervenções de negócio existentes, bem como possibilita que se viabilizem novas táticas empresariais[19].

A TI, juntamente com seus avanços, estão cada dia mais presentes na vida dos cidadãos. Tornou-se ferramenta tão necessária que os bancos brasileiros, por exemplo, gastaram mais de R$ 22 bilhões em tecnologia da informação (TI) no ano passado, cifra que representa um crescimento 15% em relação a 2009. A Federação Brasileira dos Bancos (Febraban) divulgou também que as transações bancárias atingiram quase 56 bilhões de operações em 2010, das quais as transações de internet banking já representam 23% do total, segundo noticiários atuais[20].

Essa necessidade é tamanha que há um déficit de profissionais de TI, chegando em 2020, segundo pesquisas realizadas pela Brasscom de Convergência Digital (IBCD), com um déficit de 750 mil profissionais de tecnologia da informação (TI). O estudo realizado observa, ainda, que a falta de profissionais é crescente, ou seja, verificou-se em 2010 um déficit foi de 75 mil profissionais, sendo possível até o final deste ano um déficit de 92 mil profissionais[21].

Como já mencionado, com o evidente desenvolvimento da TI, observou-se o crescimento da procura e, consequentemente, a vasta necessidade de seus usuários. No entanto, diante de tantas aplicações disponíveis e possibilidades quase ilimitadas, as empresas ficam vulneráveis a exposição de suas valiosas informações a respeito de sua organização, motivo pelo qual devem se preocupar com investimentos na gestão de segurança[22].

---

[18] **PORTER**, 2001; **DRUCKER**, 2000; **EVANS & WURSTER**, 1999; **FRONTINI**, 1999

[19] LAURINDO, Fernando José Barbin; DE CARVALHO, Marly Monteiro; JR, Roque Rabechini, SHIMIZU, Tamio. **O PAPEL DA TECNOLOGIA DA INFORMAÇÃO (TI) NA ESTRATÉGIA DAS ORGANIZAÇÕES**. Disponível em http://www.scielo.br/pdf/gp/v8n2/v8n2a04.pdf, acesso em 09/5/2011, ás 09:45.

[20] TADEU, Erivelto. **Gastos dos bancos com TI crescem 15% e somam R$ 22 bi.** Disponível em http://www.tiinside.com.br/04/05/2011/gastos-dos-bancos-com-ti-crescem-15-e-somam-r-22-bi/ti/223001/news.aspx. Acesso em 10/5/2011, ás 12:10.

[21] OLIVEIRA, Bruno de. **Déficit de profissionais de TI chegará a cerca de 750 mil vagas em 2020**. Disponível em http://www.dci.com.br/noticia.asp?id_editoria=9&id_noticia=372580. Acesso em 11/5/2011, ás 14:09.

[22] Rdc Tech. **Segurança nas Tecnologias de TI**

3.1. Segurança na TI

Desde a inclusão do computador em meados de 1940, como instrumento de múltiplas atividades, tem-se observado até os dias atuais um desenvolvimento constante da tecnologia no que tange a manipulação, armazenamento e apresentação de informações. Tem-se averiguado uma freqüente migração de centros de processamentos de dados para recintos de computação distribuída[23].

Sob essa perspectiva, compreende-se que informação é todo e qualquer teor que possa ser retido ou transferido com um fim determinado e útil ao ser humano, isto é, aquilo que permite a obtenção de conhecimento. Frisa-se isso por que a informação digital é um dos principais produtos atualmente, uma vez que pode ser manuseada e observada por diversas formas, podendo, ainda, ser retida para distintos fins.

Tendo em vista o transcorrer da historia da TI, já mencionada resumidamente, averigua-se a ocorrência da necessidade de proporcionar suporte á cooperação de várias organizações que na maioria das vezes tem interesses acrescentados. Para isso, é essencial ter-se o controle de acesso às informações, já que muitas vezes as informações disponíveis nas empresas estão armazenadas e são transferidas entre um e outro sistema automatizado.

Assim sendo, toda informação deve ser certa, precisa e estar disponível, com a intenção de ser retida, restaurada, manipulada, alem de poder ser trocada de maneira segura e confiável[24].

Diante disso, importante ressaltar que toda e qualquer informação, tendo ela fundo ou dado que tenha valor para a empresa ou pessoa física, pode ser arquivada para manuseio restrito ou disponível para o uso público, como forma de consulta ou investimento. Sob essa perspectiva, têm-se a segurança da informação. Esta, por sua vez, tem como fim proteger as informações existentes de uma determinada empresa ou pessoa, ou seja, a Segurança da informação está ligada com proteção

---

[23] ARAUJO, Nonata Silva. **Segurança da Informação (TI)**. Disponível em http://www.administradores.com.br/informe-se/artigos/seguranca-da-informacao-ti/23933/. Acesso em 07/5/2011, ás 13:45.

[24] ARAUJO, Nonata Silva. **Segurança da Informação (TI)**. Disponível em http://www.administradores.com.br/informe-se/artigos/seguranca-da-informacao-ti/23933/. Acesso em 09/5/2011, ás 11:08

de um conjunto de dados, no sentido de preservar o valor que possuem para um indivíduo ou uma organização[25].

Entretanto, a segurança está vulnerável a ser afetada por diversos fatores, como por exemplo, os fatores comportamentais e de usufruto de quem se utiliza, seja pelo recinto que a cerca ou por pessoas mal intencionadas, digam-se aquelas que têm o objetivo de sonegar, devastar ou alterar determinada informação.

Para isso, importante torna-se o nível de segurança ambicionado, o qual pode ser verificado em uma política de segurança. Esta, portanto, é seguida pela empresa ou pessoa, com o fim de assegurar que uma vez estabelecido determinado nível, será ele encalçado e conservado. E para que seja realizado dessa forma, torna-se necessário à consciência dos riscos associados à falta de segurança, benefícios, custos de implementação dos mecanismos, desenvolvimento, dentre outros fatores[26].

Isto posto, frisa-se que representam características básicas, mas essenciais, da segurança, o que chamam de tríade CIA, isto é, “Confidentiality, Integrity e Availability”[27]. Estes são os fundamentais atributos que guia e avalia a idealização e a implementação da segurança para um determinado grupo de informações que se anseia proteger.

Por confidencialidade compreende-se como a propriedade que limita o acesso à informação, diga-se que são aquelas em que o proprietário da informação autoriza. Já por integridade, é aquela que assegura que a informação manejada conserve todas as características originais constituídas pelo proprietário, o que inclui também o controle de alterações e garantia de seu ciclo. Por fim, disponibilidade é aquela que garante que a informação esteja sempre disponível para o uso autentico, isto é, para os usuários autorizados pelo proprietário da informação.

Além dessas há mais duas que auxiliam na atribuição de segurança, são elas: Autenticidade, que garante que a informação é de determinada fonte que se afirma

---

[25] MOREIRA, Ademilson. **A importância da segurança da informação**. Disponível em http://www.oficinadanet.com.br/artigo/1124/a_importancia_da_seguranca_da_informacao. Acesso em 10/5/2011, ás 15:12.

[26] ARAUJO, Nonata Silva. **Segurança da Informação (TI)**. Disponível em http://www.administradores.com.br/informe-se/artigos/seguranca-da-informacao-ti/23933/. Acesso em 09/5/2011, ás 12:26.

[27] CLESIO, Fabio. **Segurança da Informação**. Disponível em http://info.abril.com.br/forum/viewtopic.php?f=122&t=371. Acesso em 10:5/2011, ás 15:40.

ser; e Não repúdio, que menciona que nem o emissor bem como o receptor de determinada informação podem negar o fato.

Isto posto, compreende-se que política de segurança refere-se a um conjunto de preceitos que carecem ser adotados pelos usuários das portarias de uma organização. Deve, portanto, ser inserida de forma clara e realista, determinando as áreas de responsabilidade dos usuários, do pessoal de gestão de sistemas e redes, bem como da direção.

Essas políticas, uma vez implantadas, permitem um ajuste para a inserção de ferramentas de segurança, como também deliberam métodos de segurança apropriados, técnicas de auditoria à segurança e fundam uma base para procedimentos legais na seqüência de ataques. Para tanto, o documento que determina a política de segurança terá que abandonar os aspectos técnicos de implementação dos organismos de segurança, bem como deve ser um documento com simples leitura e compreensão, já que pode ser alterado no decorrer do tempo. Como regras que definem os aspectos para elaborar a política de segurança, tem-se como exemplo a ISO[28].

Sob essas perspectivas expostas pode-se averiguar que sendo a segurança da informação um anexo de conceitos que visam a proteção e a conservação de informações e seus respectivos sistemas, fundamental torna-se a presença dos cinco pilares: integridade, disponibilidade, não repudio, autenticidade e confidencialidade, uma vez que garantem a probidade e confiabilidade em sistemas de informação. Dessa forma, estes ao lado das ferramentas de proteção – que a diante serão apresentadas -, têm como finalidade fornecer base à restauração de sistemas de informações, sobrepondo competências, detecção, reação e proteção.

Frisa-se, contudo, que a utilização dos pilares é realizada em consonância com as indigências específicas de cada disposição. Sendo assim, o seu uso poderá ser apurado pela sensibilidade das informações ou sistemas de informações, bem como pelos níveis de ameaça ou por quaisquer outras decisões de gestão de riscos. Isto posto, verifica-se a importância da presença desses pilares diante dos dias

[28] LAUREANO, Marcos Aurelio Pchek. **Gestão de Segurança da Informação**. Disponível em http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf. Acesso em 10/5/2011, ás 16:01.

atuais em que é constante a presença de ambientes de natureza pública e privada conectados a nível global[29].

3.2. Sistemas bancários

Neste contexto, observa-se, como já mencionado, que o crescimento constante da globalização e desenvolvimento tecnológico tem permitido alterações significativas, decretando, assim, que até mesmo as instituições bancárias mudem o pensamento e as atitudes para acompanhar as novas tendências e adequar-se, dessa forma, ao nível de cobrança cada vez mais complicada por parte dos usuários. Sendo assim, torna-se essencial a preocupação dos bancos com a qualidade do atendimento, juntamente com o aspecto tecnológico.

Sob essa perspectiva, averigua-se a presença constante de mudanças significativas no atendimento a clientes de bancos, onde a colocação da tecnologia possibilita o desenvolvimento de bens e serviços que acolham às necessidades dos clientes, como também autoriza ferramentas de controles para potencializar o relacionamento banco e cliente. O orbe de clientes acolhidos pelos bancos continua em crescimento, seja pelo ingresso de novos fortuitos de indivíduos na população economicamente ativa, seja por decorrência de técnicas seguidas pelos bancos, buscando a conquistar clientes de segmentos ainda não bancários[30].

Em conseqüência do avanço da tecnologia os bancos conseguiram desenvolver sistemas cada vez mais elaborados para o atendimento eletrônico de seus clientes, sejam eles internos ou externos. Sendo assim, foi possível modificar serviços mecanizados em automatizados, expandindo, dessa forma, seus ambientes de atuação por meio das informações possíveis para o entrosamento das necessidades e anseios de seus clientes, com o objetivo de manter a lealdade, bem como um relacionamento duradouro.

---

[29] ARAUJO, Nonata Silva. **Segurança da Informação (TI)**. Disponível em http://www.administradores.com.br/informe-se/artigos/seguranca-da-informacao-ti/23933/. Acesso em 10/5/2011, ás 11:45

[30] ALBERTIN, A. L. **Comércio eletrônico. Um estudo no setor bancário.** Resumo da Tese de Doutorado – Faculdade de Economia Administração e Contabilidade (FEA) da Universidade de São Paulo – (USP). São Paulo: FEA/USP, 1997.

Os bancos utilizam ferramentas que ajudam o alto escalão executivo na aceitação de decisões e no desenvolvimento de suas estratégias de negócios, desde meados de 1980. O uso desses sistemas auxilia no lançamento de novos produtos, bem como na ciência e na rentabilidade do cliente, no tratamento de dados disponíveis sobre o mercado, permitindo, dessa forma, uma base mais eficaz as suas metas de negócio[31].

A Tecnologia de Informação permitiu aos bancos a vinculação direta com seus clientes em tempo real, o que possibilitou uma maior interação e melhor diálogo com esses clientes, beneficiando a inovação e a distinção de seus frutos e serviços, sem limite de tempo e espaço. Dessa forma, os sistemas bancários assessoram expressivamente na realização dos atributos diários, seja em nível funcional, seja em nível gerencial, dominando toda a celeridade de uma agencia pelo tratamento de dados, bem como seu processamento e conferencia dos resultados com eficácia satisfatória para atingir o atendimento ao cliente em determinado momento.

Isto posto, compreende-se nos sistemas bancários os seguintes sistemas: I. abertura de conta corrente; II. cadastro único de clientes; III. pagamento de folha; IV. solicitação de crédito; V. controle de restrições, de convênios; VI. devolução de cheques; VII. cobrança; VIII. inadimplência; IX. informações gerenciais; X. pedidos de material; XI. ponto eletrônico; XII. contabilidade; XIII. tesouraria; XIV. captação de recursos, (...) dentre outros. Estes sistemas ajudam os gerentes, bem como os demais profissionais, na tomada de decisões arguciosas e bem informadas sobre vários aspectos da operação.

Uma alternativa ao banco para se manter atualizado são as soluções tecnológicas fundamentadas em sistemas de atendimento ao cliente, diga-se uma chave da competitividade, uma vez que possibilita também uma melhor astúcia sobre a eficácia das intervenções e de novas abordagens na analise de rentabilidade dos clientes.

Sob esse ponto, verifica-se que a tecnologia tem permitido o alargamento de novos produtos e serviços, alterando a influencia mutua entre empresas e clientes e em particular. Essas inovações tecnológicas tem buscado várias competências,

---

[31] **ACCORSI, A.** Automação: bancos e bancários. Dissertação de mestrado. (Mestrado em Administração). Universidade de São Paulo. São Paulo-SP, 1990.

como por exemplo a entrega on line; acesso eletrônico a serviços; pagamento e apresentação eletrônica de contas; pagamento on line; transações; dentre outros[32].

Constata-se que as primeiras imissões em automação bancária deram-se inicio na década de 60, sendo acentuado na década seguinte os primeiros conhecimentos de instalação de agencia on-line. No entanto, foi na década de 80 que o setor financeiro deu os primeiros passos rumo ao auto-serviço bancário, com alguns sistemas informatizados, terminais de caixa on-line, terminais de clientes, dentre outros, permitindo a realização de aplicações em tempo real. Ao final dessa década, passou a ter necessidade de racionalização dos serviços bancários, diga-se de diminuição dos custos da mão-de-obra e obtenção de produtividade[33].

Dessa forma, foi diante desse cenário e em meados da década de 90 que se concretizaram três maneiras de automação: automação de agencia – terminais de caixa; auto-atendimento e home banking, que fora sucedido pela Internet banking, tema fundamental do trabalho em tela.

3.3. Internet Banking

A ferramenta Internet Banking foi desenvolvida com os modernos recursos de segurança voltados à Internet, assegurando seu ingresso ao Banco de forma sigilosa[34].

Com a sua vinda as intervenções financeiras, os pagamentos, as operações bancárias, como por exemplo, as transferências de dinheiro entre contas, descontos, duplicatas e faturas, passaram a ser eletrônicas, e girando em torno do meio digital tornaram-se mais eficazes as tarefas que os usuários faziam por conta própria[35].

---

[32] ALBERTIN, A. L. **Comércio eletrônico. Um estudo no setor bancário.** Resumo da Tese de Doutorado – Faculdade de Economia Administração e Contabilidade (FEA) da Universidade de São Paulo – (USP). São Paulo: FEA/USP, 1997

[33] FEBRABAN. **Atendimento e serviços.** Disponível em: http://www.febraban.org.br. Acesso em 12/5/2011, ás 10:41.

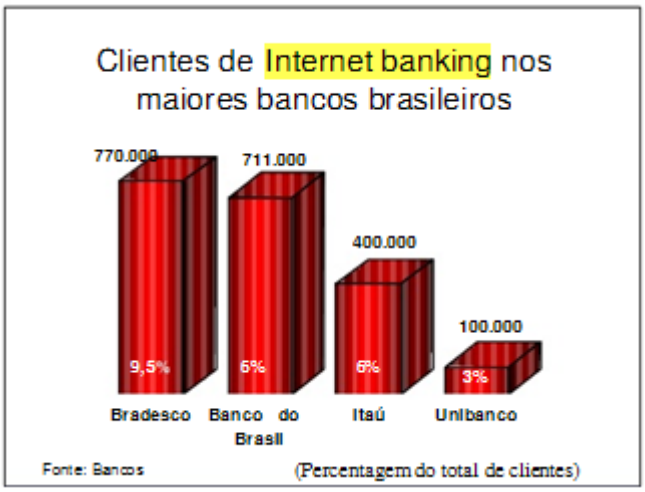
[34] SANTANDER. **Internet Banking**. Disponível em https://www.santandernet.com.br/Paginas/Ajuda/AjudaNC/iframe_PerguntasFrequentes.asp. Acesso em 12/5/2011, ás 13:01.

[35] ESTRADA, Manuel Martin Pino. **A INTERNET BANKING NO BRASIL, NA AMÉRICA LATINA E NA EUROPA.** Disponível em

O desígnio do presente trabalho é expor os aspectos da Internet Banking, sendo um dos motivos do desenvolvimento do comércio eletrônico. O assunto em tela é muito importante por tratar-se de uma poderosa ferramenta financeira. Como já mencionado, a internet tornou-se um meio indispensável na vida do homem moderno e vem alterando completamente os moldes de negócio e a história da comunicação no mundo.

Esse tema tem sido tão abordado nos últimos tempos que se pode acompanhar o crescimento do uso desse instrumento em várias instituições financeiras, devido à facilidade e comodidade que proporcionou aos seus clientes. No gráfico que se segue, tem-se um parâmetro disso nos anos 2000:

Tabela 1 - Gráfico de clientes de internet banking.
Fonte: Evolução da Internet no Brasil e no Mundo
(http://pt.scribd.com/doc/123635/Evolucao-da-Internet-no-Brasil-e-no-Mundo)



Tendo isso em vista, importante salientar que a internet banking é constituída como solução mais barata para as instituições financeiras, ficando a cargo do cliente o seu acesso, conforme tabela abaixo:

---

http://www.publicacoesacademicas.uniceub.br/index.php/prisma/article/viewFile/185/161. Acesso em 12/5/2011, ás 13:57.

Tabela 2 - Custo aos bancos nas transações.
Fonte: Associação Americana de Bancos
(www.aba.com)

Quanto Custa aos bancos a transação que o cliente faz (em dólares)	
Na agência	1,07
Pelo Telefone	0,54
No caixa eletrônico	0,27
Internet banking	010

Fonte: Associação Americana de Bancos (www.aba.com)

Não obstante, o seu crescimento tem avançado de determinada maneira que se tem visto em noticias atuais informando o crescimento dessa ferramenta. No site de notícias UOL, foi publicado recentemente um artigo dispondo que o acesso pela internet avança com rapidez, verificando-se à taxa de 27,4%, e alcançando 23% do conjunto de operações. Segundo o diretor de tecnologia da Federação Brasileira dos Bancos - Febraban, em quatro a cinco anos a internet banking vai superar os terminais de autoatendimento. É impressionante também o avanço do acesso pelo celular – móbile banking – que cresceu 72% em 2010, na comparação com o ano anterior, para 2,2 milhões de pessoas[36].

De fato, diante desses dados, pode-se constatar que os bancos irão manter as agencias abertas onde existe fluxo comercial, contudo não será para ampliar a capilaridade das transações, mas sim o nível de negócios com os clientes, uma vez que não é necessário mais ir às agencias para realizar transações[37].

3.3.1. Conceito

Com o advento dos instrumentos de informática, deu-se inicio a uma propagação de operações bancárias, deixando de lado os terminais bancários. Sob este aspecto nasceu o home banking ou office banking, isto é, permitiu-se o desenvolvimento dos negócios por intermédio de sistemas oferecido pela instituição

[36] SEABRA, Luciana. **Uso de internet banking avança 27% e número de agências se mantém**. Disponível em http://economia.uol.com.br/ultimas-noticias/valor/2011/05/04/uso-de-internet-banking-avanca-27-e-numero-de-agencias-se-mantem.jhtm. Acesso em 24/5/2011, ás 10:22.

[37] ROCHO, Gustavo – Diretor da Febraban.

bancária a computadores de seus usuários/clientes. Nessa desenvoltura é que surgiu a internet banking.

A internet banking é semelhante ao home banking, contudo diferencia-se sob a perspectiva do acesso à rede bancária, diga-se que ocorre pela internet, sendo assim, não necessita de prévia instalação de sistemas próprios dos bancos nos computadores de seus clientes como o home banking[38].

Esta ferramenta concebe uma nova forma de comércio eletrônico, pela qual o cliente, amparando-se da internet, tem acesso aos diversos serviços bancários para a efetivação de negócios e contratos, os quais são deliberados como contratos celebrados através de programas de computador e dispensados, assim, da assinatura codificada ou senha[39].

Com o uso desta o cliente aufere operosidade, já que detém todas as escolhas à distância de um "clique de mouse", sem carecer se desarticular até uma agência encarando tráfego, filas e os vários problemas ligados à segurança. Para isso, a internet banking oferece ao cliente um maior atributo nos produtos e serviços proporcionados pela instituição com segurança e praticidade.

Isto posto, constata-se que é um meio objetivo que facilita as aplicações que por ventura venha a necessitar ou realizar o cliente. Contudo, mesmo diante de vários benefícios na sua utilização há sempre que averiguar a atenção com possíveis ameaças que por ventura venham a aparecer – tema este que também será abordado brevemente.

3.3.2. Vantagens das operações bancárias na internet

Como já mencionado, este recurso – internet banking – permite ao cliente vários benefícios, tais como:

> "a) diminuição de custos fixos de manutenção de uma agência bancária, especificamente nas despesas de pessoal;

[38] GOMES, Alessandra Aparecida Calvoso. **Operações bancárias via Internet (Internet banking) no Brasil e suas repercussões jurídicas**. In Revista dos Tribunais, vol. 816, outubro de 2003.

[39] ALBERTIN, A. L. **Comércio Eletrônico – Modelo, Aspectos e Contribuições de sua Aplicação**, São Paulo Makron Books 2000.

> b) desburocratização de serviços, facilitando a vida do cliente, dispensando sua presença física no estabelecimento, evitando filas e perda de tempo realizando operações bancárias;
>
> c) o alcance geográfico, pelo fato da Internet atingir o mundo todo, podendo fornecer serviços em grande escala;
>
> d) diminuição de riscos de assaltos, porque há um menor movimento de pessoas, moeda e serviços nas agências bancárias "[40].

Cabe, contudo, ressaltar que para a fiel aplicação desses benefícios necessário tornar-se-ia a realização de algumas condições pela instituição financeira ao cliente, como por exemplo, a informação constar de forma clara e precisa; controlar o sigilo, a segurança e monitorar as movimentações na conta dos clientes; disponibilizar números de atendimento; oferecer nas paginas da internet ferramentas de envio de mensagens eletrônicas, as quais devem ter o recebimento confirmado; dentre outros.

Para tanto, frisa-se que para a concretização dessas atribuições que consequentemente trazem, com o seu usufruto pelos clientes, benefícios, imperioso realizar as políticas de segurança.

3.3.3. Políticas de segurança nas operações bancárias na internet

Como já fora abordado, a política de segurança significa um conjugado de regras que carecem ser adotadas pelos usuários das portarias de uma organização.

---

[40] ESTRADA, Manuel Martin Pino. **A INTERNET BANKING NO BRASIL, NA AMÉRICA LATINA E NA EUROPA.** Disponível em http://www.publicacoesacademicas.uniceub.br/index.php/prisma/article/viewFile/185/161. Acesso em 13/5/2011, ás 11:57

Deve, portanto, ser inserida de forma clara e precisa, determinando as áreas de responsabilidade dos usuários, do pessoal de gestão de sistemas e redes, bem como da direção. Ademais, possibilitam um ajuste para a inserção de utensílios de segurança, como também deliberam métodos de segurança apropriados, técnicas de auditoria à segurança e fundam uma base para procedimentos legais na seqüência de ataques.

Isto posto, verificam-se duas políticas que buscam evitar o surgimento de ameaças, diga-se que terceiros acessem as bases de dados relativos a transações bancárias. A primeira delas denomina-se política de segurança física, uma vez que versa sobre a implementação nas acomodações físicas dos sistemas e equipamentos de informática aproveitados pela internet banking, como por exemplo, o desígnio de um lugar adequado, com sistemas de precaução e combate à falta de energia elétrica, ou incêndio, como processamentos alternativos e cópias dos processamentos[41].

Já a segunda - política de segurança lógica - compreende a assistência dos bancos de dados contra vírus informáticos, atentando o arquivamento e manutenção dos arquivos, gerenciamento de risco, dentre outros aspectos[42].

Para efetivar essas políticas, utiliza-se de meios como o emprego da certificação digital e criptografia; o uso das senhas ou a biometria; dentre outras, e que serão explicitadas nos capítulos que logo em seguida serão expostos.

Não obstante, têm-se ainda as políticas de danos aos clientes que utilizam o recurso internet banking, que é a política de divulgação de dicas pelos bancos, diga-se aquela que informa a alteração de senha periodicamente, manter sempre atualizado o antivírus, não realizar operações em equipamentos públicos e não abrir arquivos de origem desconhecida[43].

Sob essa perspectiva, cabe agora abordar a respeito das ameaças, que é um importante tema e que vem gerando muitos problemas para os sistemas de

---

[41] ESTRADA, Manuel Martin Pino. **A INTERNET BANKING NO BRASIL, NA AMÉRICA LATINA E NA EUROPA.** Disponível em http://www.publicacoesacademicas.uniceub.br/index.php/prisma/article/viewFile/185/161. Acesso em 13/5/2011, ás 11:57

[42] STERN, Jim. **Serviço ao cliente na Internet**, São Paulo: Ed. Makron Books 2000.

[43] SANTANDER. **[Home page]**. Disponível em https://www.santandernet.com.br/Paginas/Ajuda/AjudaNC/iframe_PerguntasFrequentes.asp. Acesso em 13/5/2011, ás 13:01.

segurança, que tem buscado se aperfeiçoar cada vez mais devido a presença constante de novas e diferentes ameaças.

4. AMEAÇAS NA TECNOLOGIA DE INFORMAÇÃO

Diante do exposto até o presente momento, pode-se averiguar que as empresas em geral possuem softwares que gerenciam informações essenciais para organização e atendimento ao cliente. Contudo, de nada adianta a implementação de um sistema sem a devida preocupação sobre os dados armazenados e mantido nestes sistemas. Infelizmente, ficam sujeitos a várias ameaças estes sistemas de informação, sendo dentre eles a internet banking.

Essas ameaças estão interligadas a quebra dos três pilares supracitados no transcorrer desse trabalho, quais sejam: a perda da confidencialidade, da integralidade e da disponibilidade[44]. O primeiro ocorre quando há uma quebra do sigilo, como por exemplo singelo um funcionário da área de TI deixa refluir dados a respeito de um cliente, como uma senha por exemplo, que está disposta exclusivamente a determinado usuário. A perda da integridade, por sua vez, significa dizer que quando uma informação fica apresentada em mãos de uma terceira pessoa, diga-se não autorizada e que não lhe compete saber, esta faz alterações inadequadas, isto é, que não foram consentidas ou controladas pelo verdadeiro proprietário. Por fim, a perda da disponibilidade, ocorre quando a informação não está disponível a quem precise dela, seja em virtude de má intenção de terceiros, seja por boa intenção, contudo equivocada, ou por fatores externos ou internos, ou ainda por alguma falha do recurso, como é o caso, por exemplo, de a rede de cartões estarem fora do ar.[45].

Não obstante, outras volumosas ameaças apareceram com o decorrer dos tempos, diante do uso insubstituível e imprescindível da internet, que a seguir abordaremos alguns deles.

---

[44] MÉDICE, Roney. **Ameaças aos Sistemas de Informação**. Disponível em http://www.profissionaisti.com.br/2010/07/ameacas-aos-sistemas-de-informacao/. Acesso em 13/5/2011, as 12:47.

[45] Segurança em TI. **Ameaça à segurança**. Disponível em http://segurancaemti.wordpress.com/2009/07/08/ameacas-a-seguranca/. Acesso em 13/5/2011, ás 12:50.

4.1. Fraude

A fraude é um objeto que antecede o surgimento da Internet, e que deverá continuar presente no cotidiano do ser humano, independente das contribuições tecnológicas existentes ou que ainda estão por vir. É importante ressaltar que as técnicas empregadas no passado e presente para a realização da fraude, são precisas permitindo nos organizar para o desenvolvimento deste processo nos próximos anos.

Dessa forma, compreende-se que a fraude está agregada à distorção intencional de um fato que levará a obtenção de lucro ilícito, existindo a necessidade de três elementos principais para a consumação da fraude: a vítima, o fraudador e, neste caso, o canal Internet Banking[46].

A fraude está evidente em programas que detém comportamentos estranhos, devido ao desempenho de códigos criados com o fim de danificar ou modificar o seu funcionamento normal. Estes podem causar estrago nos dados de um sistema ao se incutirem em documentos sigilosos ou acessando sem autorização um sistema para hospedarem novas contas de usuário, ou alterar senhas e iludir controles de segurança normais.

Isto posto, resta-se apresentar, de forma resumida, alguns desses meios fraudulentos.

4.2. Vírus

Os vírus representam uma das maiores dificuldades para usuários de computador. Versam em pequenos programas instituídos para ocasionar algum dano ao computador infectado, seja apagando dados, seja capturando informações, seja alterando o funcionamento normal da máquina[47].

---

[46] LAU, Marcelo; SANCHEZ, Pedro Luiz Próspero. **TÉCNICAS UTILIZADAS PARA EFETIVAÇÃO E CONTENÇÃO DAS FRAUDES SOBRE INTERNET BANKING NO BRASIL E NO MUNDO.** Disponível em http://www.datasecur.com.br/academico/Tecnicas_Utilizadas_para_Efetivacao_e_Contencao_das_fraudes.pdf. Acesso em 18/5/2011, ás 09:25.

[47] ALECRIM, Emerson. **Vírus de computador: o que são e como agem**. Disponível em http://www.infowester.com/virus.php. Acesso em 16/5/2011, ás 15:41.

Esses "programas mal-intencionados" ganharam essa denominação - vírus - porque tem a particularidade de se graduar facilmente, assim como ocorre com os vírus biológicos. Verifica-se que estes se distribuem ou operam por meio de falhas de determinados programas, se disseminando como em uma infecção, como é o caso, por exemplo, de um usuário deter vírus em seu computador e ao acessar seu e-mail o vírus interage obtendo informações do login e senha e ao usuário encaminhar um e-mail – caso de spam, tema que será abordado em tópico a seguir - , neste e-mail o vírus é automaticamente também enviado[48].

Sendo assim, averigua-se que um vírus pode adulterar ou apagar dados do computador, usar o programa de e-mail para se difundir para outros computadores ou até mesmo apagar todo o disco rígido. Podem eles ser disfarçados como anexos de imagens engraçadas, cartões de felicitações ou arquivos de áudio e vídeo, bem como se espalham por meio de downloads realizados da Internet, ou ainda, estarem escondidos em softwares ilícitos ou em outros arquivos ou programas que o usuário baixar.

Sob esse aspecto, necessário torna-se, como auxilio para evitar o vírus, manter o computador sempre atualizado com as atualizações mais recentes e ferramentas antivírus, bem como deter sempre informações sobre ameaças recentes e seguir algumas regras básicas durante a navegação pela Internet, o download de arquivos e a abertura de anexos, como já mencionado.

Diante do exposto até o presente momento, pode-se observar que há um processo evolutivo nos mecanismos utilizados para efetivação do dolo junto aos clientes de serviços internet banking. Esta evolução caracteriza-se pela necessidade adaptativa de terceiros mal intencionados em razão da perda de eficácia dos ataques ou anseio no aumento de produtividade na arrecadação de credenciais que aceitam acesso a serviços financeiros dos usuários/vítimas, resultando em um volume financeiro que justifique o investimento realizado para o lançamento dos ataques[49].

---

[48] MICROSOFT. **O que é um vírus de computador?** Disponível em http://www.microsoft.com/brasil/athome/security/viruses/intro_viruses_what.mspx. Acesso em 14/5/2011, ás 16:13.

[49] LAU, Marcelo; SANCHEZ, Pedro Luiz Próspero. **TÉCNICAS UTILIZADAS PARA EFETIVAÇÃO E CONTENÇÃO DAS FRAUDES SOBRE INTERNET BANKING NO BRASIL E NO MUNDO.** Disponível em

Verifica-se que na esmagadora maioria, senão em todos, dos incidentes já registrados há claro desígnio de convencimento da vítima à concretização de uma ação que levará o fornecimento voluntário das credenciais de acesso aos serviços de internet banking. Tendo isto em vista, relata-se que a maior parcela dos ataques do convencimento dos usuários/vitimas está acoplada a curiosidade de cada um sobre o teor existente em uma mensagem, a qual pode trazer consigo matérias diversas, como recebimento de cartões virtuais, possíveis débitos pendentes junto a órgãos oficiais, oferecimento de fotos que contenham nudez, ou fatos de grande repercussão na imprensa ou mídia televisiva, entre outros, suficientes a conduzir o usuário a realizar o *download* de um programa, o qual procederá a acomodação de um executável residente em memória, competente a enlaçar dados diversos, e dentre os quais se incluem as credenciais de acesso a serviços de internet banking. Como é o caso, por exemplo, da figura que se segue:

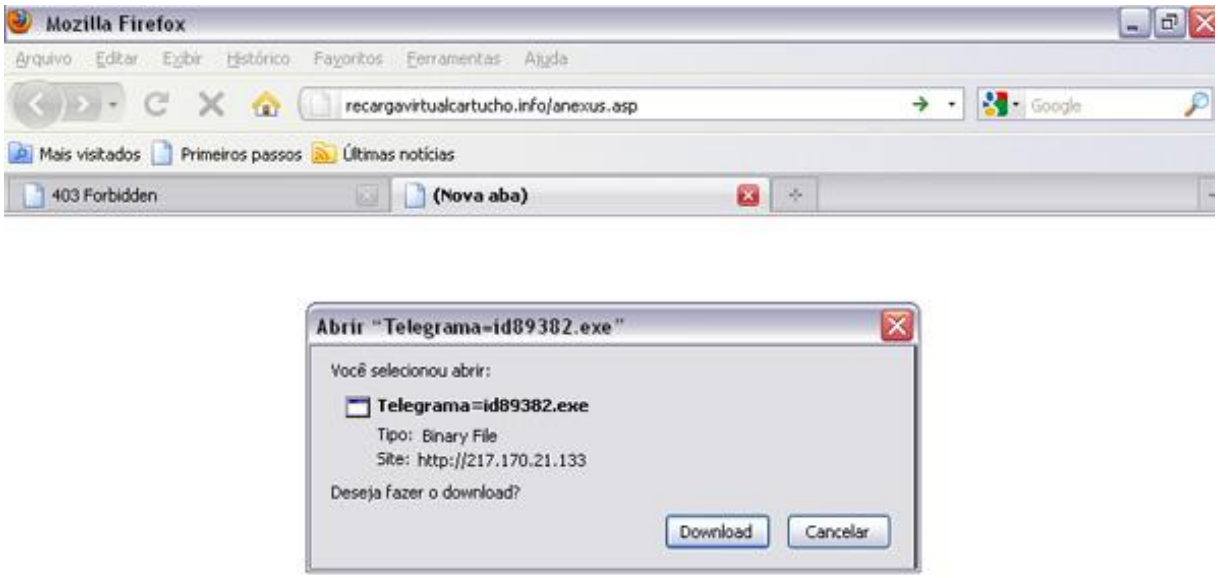


Figura 2 – Download programa

Fonte: Invasão Hacking

(http://www.invasaohacking.com/2010/12/12/saiba-como-funcionam-os-virus-que-roubam-senhas-de-banco/))

---

http://www.datasecur.com.br/academico/Tecnicas_Utilizadas_para_Efetivacao_e_Contencao_das_fraudes.pdf. Acesso em 16/5/2011, ás 12:29.

Não obstante, os clientes não são levados a erro apenas em mensagens como fora supramencionado. Mister ressaltar ainda, que um vírus, que está circulando na web, pode se infiltrar no PC do usuário, agindo de certa forma que quando o usuário digitar o endereço do site do seu respectivo banco o navegador lhe redirecionará para uma página falsa, que copia a original, levando a vítima a acreditar que está utilizando de forma segura a pagina de seu banco[50], como pode-se observar na figura abaixo:

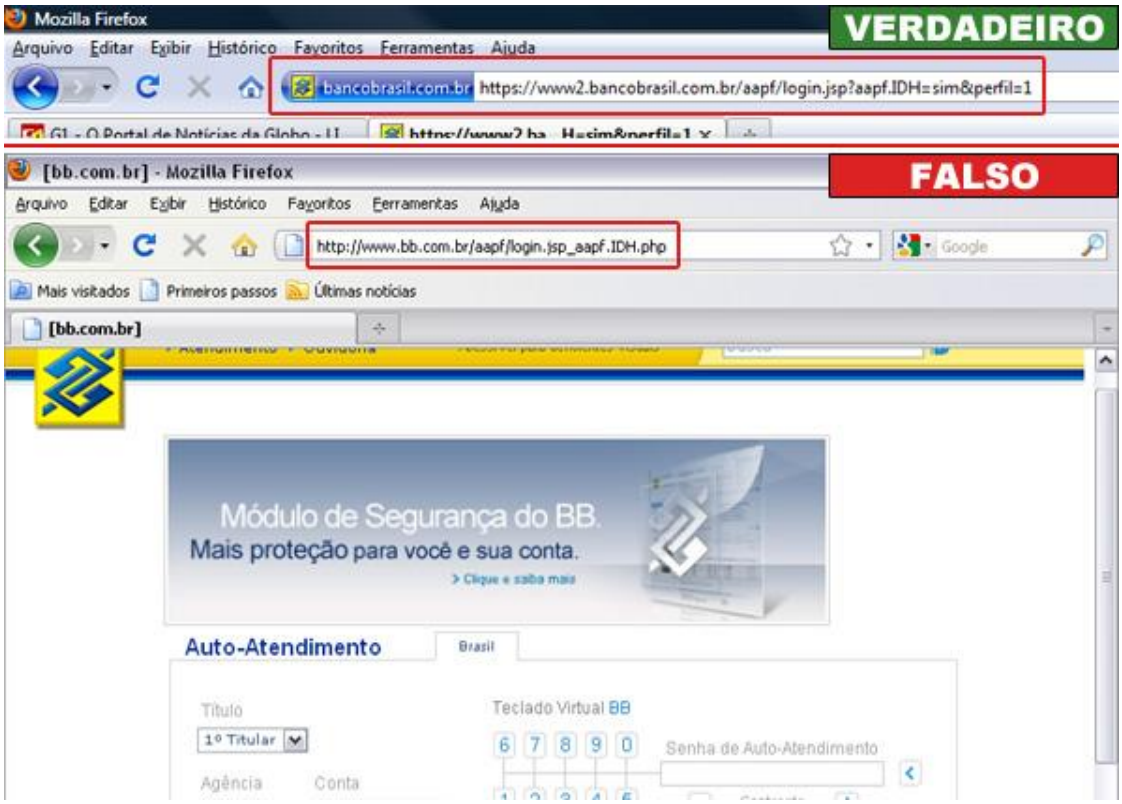


Figura 3 – Login Banco do Brasil

Fonte: Invasão Hacking

(http://www.invasaohacking.com/2010/12/12/saiba-como-funcionam-os-virus-que-roubam-senhas-de-banco/))

[50] NETO, Cláudio Ângelo. **Cuidado ao acessar seu Internet Bank. Vírus circula na Internet e atinge usuários brasileiros**. Disponível em http://www.argohost.net/blog/cuidado-ao-acessar-seu-internet-bank-virus-circula-na-internet-e-atinge-usuarios-brasileiros/. Acesso em 17/5/2011, ás 12:12.

Sob essas assertivas depara-se que muitos denominam os terceiros mal intencionados como “bankers”, denominação esta que deriva dos termos “cracker”[51] e “hacker”[52]. Esses códigos são pragas digitais que roubam fundamentalmente as senhas de acesso aos serviços de internet banking. A maioria dos bankers pode ser avaliada como um “cavalo de troia”, diga-se que eles não se disseminam sozinhos, mas sim, quem os expande é o próprio criador do vírus, que uma vez alojado no sistema da vítima, o código malicioso tentará apanhar as credenciais de acesso[53].

Averigua-se que a multiplicidade de vírus resume-se a um ou dois arquivos no disco rígido, executados automaticamente quando o sistema é iniciado, buscando sempre seu objetivo essencial, que neste caso em tela, é o roubo dos dados do internauta, seja por paginas clonadas, seja por downloads de arquivos que instalam o vírus no PC, seja a associação a endereços falsos aos de sites de instituições financeiras, seja com base em técnicas de monitoramento da janela em que são direcionadas ao infrator, dentre outros. No entanto, o fim desses criminosos, no desenvolvimento dessas pragas, é apenas para a realização de fraudes bancárias.

4.3. Spam

Efetuar pagamentos e transferências on-line empregando o site dos bancos virou o “tendão de Aquiles” da indústria financeira, na medida em que “cibercriminosos” descobrem meios de apanhar o controle dos computadores pessoais e realizar operações enviando dinheiro para lugares remotos. Outra grande ameaça aos usuários são os spams.

O termo spam é refere-se aos e-mails não requeridos, que comumente são enviados para um grande número de pessoas, mas quando o conteúdo é exclusivamente comercial, esse tipo de mensagem é chamada de UCE - Unsolicited Commercial E-mail. Este, por sua vez, é uma das práticas ruins, assim como o vírus.

---

[51] Alguém que quebra sistemas de segurança na intenção de obter proveito pessoal.

[52] São indivíduos que elaboram e modificam software e hardware de computadores, seja desenvolvendo funcionalidades novas, seja adaptando as antigas.

[53] DIABLOS. **Saiba como funcionam os vírus que roubam senhas de banco**. Disponível em http://www.invasaohacking.com/2010/12/12/saiba-como-funcionam-os-virus-que-roubam-senhas-de-banco/. Acesso em 17/5/2011, ás 12:26.

Tornou-se uma angústia para os usuários de e-mail, impactando na produtividade de funcionários e degradando o desempenho de sistemas e redes[54].

Tendo isso em vista, os usuários da ferramenta e-mail podem ser afetados de várias formas, como por exemplo, no não recebimento de e-mails, ou seja, se o usuário detiver na sua caixa de e-mail um grande numero de spams recebidos, ele corre o risco de ter sua caixa postal cheia com essas mensagens não solicitadas e com isso não irá conseguir mais receber e-mails, e até que libere espaço as demais mensagens enviadas a sua caixa serão devolvidas ao remetente.

Outra forma de afetar o usuário é o aumento de custos, ou seja, independentemente do tipo de acesso à internet, quem paga a conta pelo envio do spam é quem recebe, como por exemplo, quem utiliza o acesso discado. Ademais, aqueles que utilizam o e-mail como um instrumento de trabalho, ao receber spams, há uma perda de produtividade, pois o usuário leva certo tempo para identificar se a mensagem é ou não legitima[55].

Figura 4 – Spam

Fonte: Encyclopedia Britannica Blog (http://www.britannica.com/blogs/2010/04/to-spam-with-love-how-a-nigerian-welshed-me-in-wales-last-week/)

[54] ANTISPAM. **O que é um spam**. Disponível em http://www.antispam.br/conceito/. Acesso em 18/5/2011, ás 08:34.

[55] CARTILHA DE SEGURANÇA. **Spam**. Disponível emhttp://cartilha.cert.br/spam/sec1.html#subsec1.1. Acesso em 18/5/2011, ás 08:59.

Não obstante, o envio de spam tem causado também prejuízos financeiros, diga-se que tem sido utilizado como um meio para difundir projetos fraudulentos que levam o usuário a acessar paginas clonadas de instituições financeiras ou a instalar programas maliciosos projetados para furtar dados pessoais e financeiros, como já fora supramencionado, diga-se que o envio de um spam na caixa postal pode conter um acesso a um terminal com vírus. Nestes casos, o usuário pode sofrer grandes prejuízos financeiros, ao fornecer as informações ou realizar as instruções requeridas na mensagem dolosa recebida[56].

Com o surgimento dos spams, sobreveio os spams zombies. Estes, por sua vez, são computadores de usuários finais que foram danificados por códigos maliciosos em geral, como worms[57], bots, vírus e cavalos de tróia. Estes códigos maliciosos, uma vez instalados, possibilitam que spammers empreguem a máquina para o envio de spam, sem o conhecimento do usuário. Enquanto vale-se de máquinas comprometidas para executar suas atividades, obstam a identificação da origem do spam e dos autores também. Os spam zombies são muito explorados pelos spammers, por proporcionar o anonimato que tanto os protege[58].

Sob esses aspectos temos como exemplo um spam que se passou por uma mensagem do Banco Bradesco, tendo em vista que na mensagem continha uma imagem que informa á vitima da necessidade de recadastrar sua conta e instalar o Plugin para adquirir segurança na internet banking – conforme figura que se segue. Entretanto, dentro do spam encontrava-se um arquivo malicioso, conforme registro na Rede Nacional de Ensino e Pesquisa que fornece em seu site um catálogo de fraudes.

---

[56] CARTILHA DE SEGURANÇA. **Spam**. Disponível emhttp://cartilha.cert.br/spam/sec1.html#subsec1.1. Acesso em 18/5/2011, ás 08:59

[57] Subclasse de vírus. Geralmente se alastra sem a ação do usuário e distribui cópias completas (possivelmente modificadas) de si mesmo através das redes.

[58] ANTISPAM. **O que é um spam**. Disponível em http://www.antispam.br/conceito/. Acesso em 18/5/2011, ás 10:44.

Figura 5 – Pagina falsa banco Bradesco

Fonte: RNP - Rede Nacional de Ensino e Pesquisa

(http://www.rnp.br/)

4.4. Phishing

Assim como spam e o vírus, o phishing é um meio fraudulento que terceiros mal intencionados buscam utiliza-lo para atender o seu anseio, qual seja furtar dados pessoais e financeiros do usuário.

O termo p*hishing*, também conhecido como *phishing scam* ou *phishing/scam*, foi originalmente criado para delinear o tipo de fraude que se dá por meio do envio de mensagem não solicitada, que se passa por comunicação de uma instituição conhecida, como um banco, empresa ou *site* popular, e que procura induzir o acesso a páginas falsificadas, cogitadas para apanhar informações pessoais e financeiras das vitimas[59].

[59] CARTILHA DE SEGURANÇA PARA INTERNET.**Fraude na internet**. Disponível em: http://cartilha.cert.br/fraudes/sec2.html#subsec2.2. Acesso em 18/5/2011, ás 11:17.

Sua denominação adveio por analogia da palavra “fishing”, desenvolvida pelos fraudadores, com o fim de “pescar” as senhas e informações financeiras sigilosas dos usuários por intermédio dos e-mails enviados, considerados nesta analogia como “iscas”.

Nos dias contemporâneos a sua denominação tem sido compreendida de variadas formas, como por exemplo, referindo-se a uma mensagem que busca levar o usuário a uma instalação de códigos maliciosos, com o fim de apanhar seus dados financeiros, bem como pessoais. Ademais, pode ser compreendida como uma mensagem que em seu conteúdo dispõem formulários a serem preenchidos, sendo em seguida enviados as informações sigilosas do usuário.

Diferente das outras ameaças, os phishings não trazem anexos, ou seja, do e-mail o usuário é induzido a clicar em um link. Dessa forma, como em muitas vezes acontece, os usuários não tem pleno conhecimento das políticas de segurança das instituições financeiras, o que acaba, consequentemente, levando ao cliente clicar no link encaminhado na sua caixa de e-mail, e o conduz a informar seus dados pessoais e financeiros em uma pagina falsa. Assim, passados os dados na pagina fraudulenta, estes são reconduzidos ao terceiro mal intencionado, que os utiliza ilegalmente.

Sobre esses apontamentos podemos verificar na figura abaixo um exemplo de e-mail fraudulento, sob a denominação do banco Itaú, em que usuários recebera em sua caixa postal virtual uma mensagem com uma imagem que continha a informação de deveria ser instalado um aplicativo para a realização de operações bancárias:

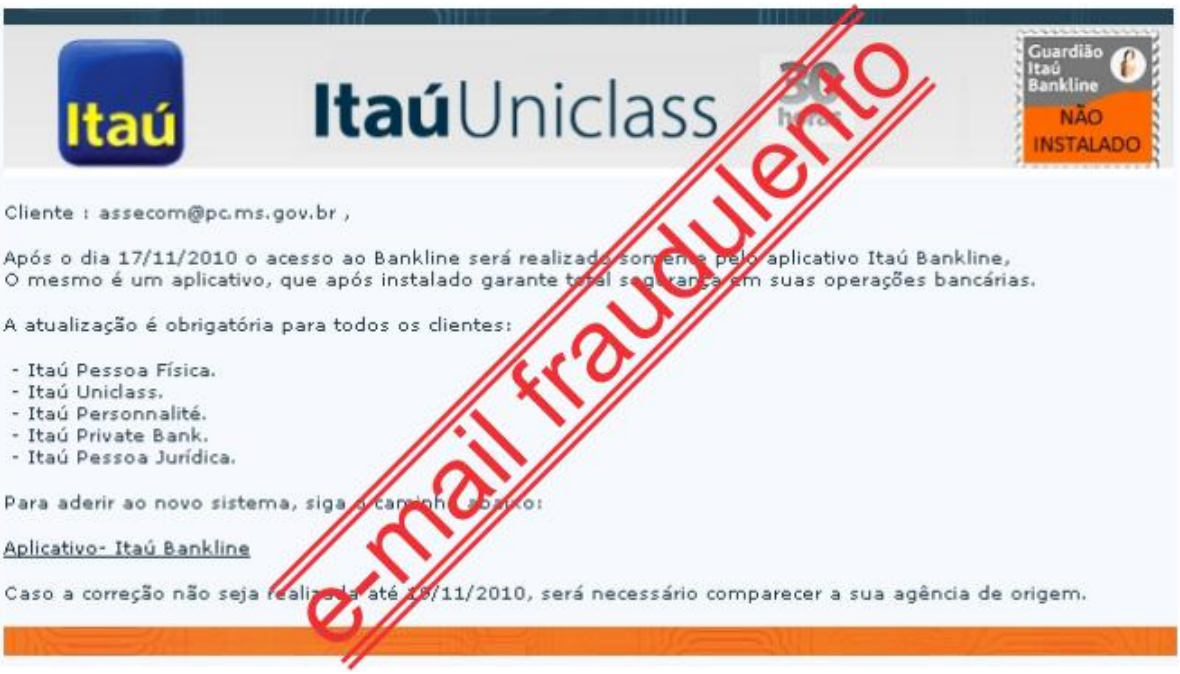


Figura 6 – E-mail fraudulento banco Itaú

Fonte: Redes e informação de segurança

(http://michelneves.blogspot.com/2010/11/aviso-aos-navegantes-e-mail-fraudulendo.html)

5. PROTEÇÃO INTERNET BANKING

Amparar sistemas de informação, como o caso da internet banking não é um trabalho fácil e econômico, já que essa proteção é impetrada ao implantar controles, estruturas de defesa cogitadas para resguardar todos os artifícios do sistema de informação como dados, software, hardware e redes.

Com o fim de suavizar as infrações, equívocos, interrupções, dentre outros fatores, essencial torna-se os bancos terem ajuste de conceitos manuais e automáticas para proteger e preservar o seu internet banking, bem como garantir o fiel funcionamento do mesmo com padrões administrativos.

Estes métodos garantem a segurança das funcionalidades da organização, com exatidão e credibilidade de seus registros contábeis e a adesão operacional aos moldes administrativos. Para isso, fundamental torna-se a prevenção diante dos erros, diga-se evitar que os erros nos sistemas de segurança ocorram, impedindo, dessa forma, que os criminosos o ataquem bem como o acessem com o fim de obter informação pessoal e financeira do usuário. Contudo se houver problema, deve este ser o quanto antes detectado, trazendo dessa forma menos danos ao cliente. Ademais, é importante também deter o controle dos danos, ou seja, minimizar perdas logo que ocorra um litígio, podendo-se realizar também a recuperação, concerto ou substituição dos componentes atingidos[60].

Isto posto, resta lembrar que há diversos meios de segurança que visam o mesmo objetivo, diga-se assegurar que as informações tanto públicas como privadas, mas ambas sigilosas, caiam nas mãos de pessoas mal intencionadas que buscam obter essas informações e utiliza-las com o fim de atender seus anseios financeiros.

5.1. Meios de segurança

Tem-se observado que o numero de infrações ocorrida pelo meio virtual tem crescido exponencialmente, tornando-se cada vez mais comum o furto de informações pessoais e financeiras. Esses atos ilegais ocorrem com tanta freqüência

[60] LAUDON, Kenneth C. & LAUDON, Jane Price. **Sistemas de informações: administrando a empresa digital.** São Paulo: Prentice Hall, 2004 – 5ª edição.

que tem ocasionado, alem das altas perdas financeiras, a desconfiança entre funcionários, a insegurança sobre a capacidade de administração ou gestão, dentre outros fatores. Os resultados dos atos ilícitos são imensuráveis, o que pode danificar a leal continuidade da instituição.

Averigua-se o aumento do numero de ocorrências dos atos ilícitos, devido ao numero crescente de clientes de internet banking, uma vez que estão diante do baixo custo e praticidade para a realização de suas operações financeiras por meio dessa ferramenta. Os riscos podem ser controlados, amenizados, mas compreende-se que jamais serão totalmente extintos. Para isso, vital torna-se a existência dos meios de segurança, como já mencionado, para conter, controlar a ocorrência desses atos fraudulentos, garantindo e assegurando a proteção dos dados dos usuários e clientes da instituição financeira.

Isto posto, os temas a seguir serão voltados para os meios de segurança, como a criptografia, certificado digital, smart card, token, plugin, teclado virtual, protocolo SSL e, por fim, selo digital.

5.2. Criptografia

Como já analisado, as instituições financeiras preocupam-se com a segurança das informações dos clientes armazenadas em seus sistemas de informação. As formas mais conhecidas de segurança dependem da criptografia. A palavra criptografia é de origem grega e tem por escopo o estudo dos princípios e técnicas pelas quais a informação pode ser escondida de forma que se torne incompreensível.

Sendo assim, compreende-se por criptografia como uma codificação dos dados com o intuito de manter a informação segura, ou seja, trata-se da arte de escrever mensagens em forma cifrada ou em código. Esse meio faz parte de um campo de estudos que trata das comunicações secretas, usadas, dentre outras finalidades, para autenticar a identidade de usuários; ou autenticar e proteger o sigilo de comunicações pessoais e de transações comerciais e bancárias; ou ainda para proteger a integridade de transferências eletrônicas de fundos[61].

[61] CARTILHA DE SEGURANÇA PARA INTERNET. **Conceitos de segurança.** Disponível em http://cartilha.cert.br/conceitos/sec8.html. Acesso em 19/5/2011, ás 09:41.

Sob essa perspectiva, averigua-se que tendo uma mensagem codificada por meio da criptografia, esta deve ser privada, isto é, apenas aquele que encaminhou e aquele que recebeu é que tem e devem ter acesso ao teor da mensagem. Ademais, essa mensagem deve ser assinada, diga-se que aquele que recebeu a mensagem deve observar se o remetente é a mesma pessoa que diz ser e ter a idoneidade de identificar se uma mensagem pode ter sido alterada.

É perceptível que a metodologia da criptografia é diligente e seguro, baseando-se no uso de uma ou mais chaves. Esta chave, por sua vez, corresponde a uma seqüência de caracteres, que pode domar letras, dígitos e símbolos - assim como uma senha -, e que é transformada em um número, empregada pelos artifícios de criptografia para codificar e decodificar mensagens[62], conforme demonstra a figura abaixo.

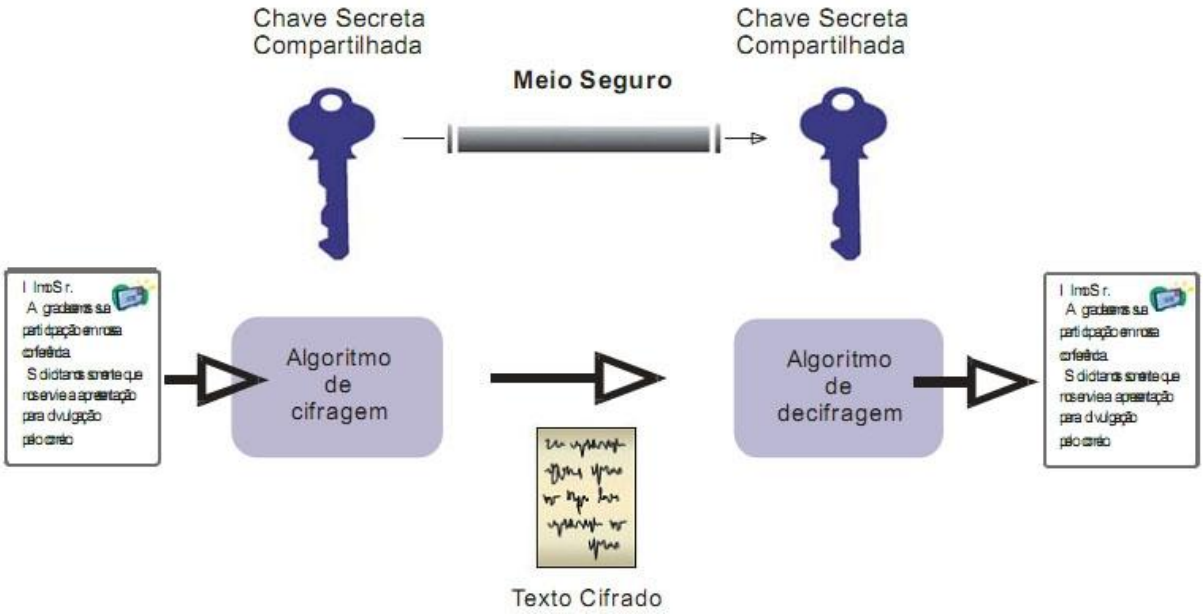


Figura 7 – Mensagem criptografia

Fonte: Public Key infrastructure– Criptografia simétrica

(http://www.gta.ufrj.br/grad/07_2/delio/Criptografiasimtrica.html)

É essencial, portanto, que esta chave seja mantida em segredo, de forma que apenas quem tem acesso a chave consiga compreender o teor da mensagem.

---

[62] CORREIA, Márcio A. S. **Segurança em Internet Banking.** Disponível em http://ximen.es/artigos/Sbseg2008_BancoDoBrasil.pdf. Acesso 19/5/2011, ás 09:53.

Nos dias atuais, pode deparar-se com duas grandes categorias de métodos criptografados, de acordo com a chave utilizada. Um deles é a criptografia de chave única, ou seja, esta utiliza a mesma chave tanto para codificar quanto para decodificar mensagens. Esse artifício é muito hábil diante do tempo de processamento, no entanto, o tempo gasto para codificar e decodificar mensagens tem como principal desvantagem a necessidade de utilização de um meio seguro para que a chave possa ser compartilhada entre pessoas ou entidades que desejem trocar informações criptografadas[63]. Vide figura abaixo:

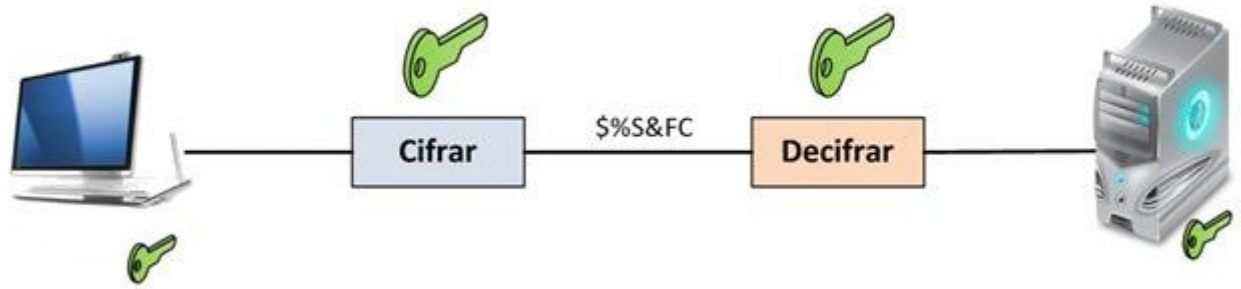


Figura 8 – Chave única

Fonte: Escreve assim.

Fonte: (http://escreveassim.com.br/2010/12/08/criptografia-simetrica-e-assimetrica/)

Nesta figura exemplificativa observa-se a funcionalidade da chave única. Na figura verifica-se que se utiliza uma única chave que é compartilhada entre o emissor da informação e o receptor, sendo possível, desta forma, criptografar (cifrar) bem como decifrar (decriptografar). Este método pode ser verificado em situações como a conexão segura estabelecidas entre um browser de um usuário e um site em transações bancárias via web.

Já a criptografia de chaves pública e privada utiliza duas chaves distintas, diga-se uma para codificar e outra para decodificar mensagens, permitindo assim que cada pessoa ou entidade mantenham duas chaves, isto é, uma pública, que pode ser divulgada livremente, e outra privada, que deve ser mantida em sigilo pelo seu proprietário. Dessa forma, as mensagens codificadas com a chave pública

[63] MUNHOZ, Felipe. **Tecnologia da informação.** Disponível em http://blog.felipemunhoz.com/criptografia/. Acesso em 19/5/2011, ás 10:08.

somente podem ser decodificadas com a chave privada correspondente. Contudo, mesmo este método apresentando desempenho bem inferior em relação ao tempo de processamento, comparado ao método de chave única supramencionado, proporciona como principal vantagem a livre distribuição de chaves públicas, não carecendo de um meio seguro para que chaves sejam combinadas antecipadamente[64].

Observando-se o exemplo supracitado em relação ao método de chave única, pode-se utiliza-lo também ao método de chave publica e privada, uma vez que as conexões seguras via web ao utilizarem o método de criptografia de chave única, implementado pelo protocolo SSL, o browser do usuário carece informar ao site qual será a chave única utilizada na conexão segura, antes de iniciar a transmissão de dados sigilosos. Para isso o browser obtém a chave pública do certificado da instituição que mantém o site. Portanto, ele usa esta chave pública para codificar e enviar uma mensagem para o site, contendo a chave única a ser utilizada na conexão segura, permitindo que o site utilize sua chave privada para decodificar a mensagem e identificar a chave única que será utilizada. Dessa forma, o browser do usuário e o site podem transmitir informações, de forma sigilosa e segura[65].

Conforme figura que se segue, pode-se fazer uma melhor análise do que foi acima exposto. Na figura abaixo, temos como exemplo o que está disponível no site InfoWester. Na imagem o “InfoWester criou uma chave pública e a enviou a vários outros sites. Quando qualquer desses sites quiser enviar uma informação criptografada ao InfoWester deverá utilizar a chave pública deste. Quando o InfoWester receber essa informação, apenas será possível extraí-la com o uso da chave privada, que só o InfoWester tem. Caso o InfoWester queira enviar uma informação criptografada a outro site, deverá obter uma chave pública fornecida por este”[66], conforme observa-se na figura abaixo:

---

[64] NUNES, Délio Silva. **Criptografia.** Disponível em http://www.gta.ufrj.br/grad/07_2/delio/Criptografiasimtrica.html. Acesso em 19/5/2011,ás 12:24.

[65] CARTILHA DE SEGURANÇA PARA INTERNET. **Conceitos de segurança.** Disponível em http://cartilha.cert.br/conceitos/sec8.html. Acesso em 19/5/2011.

[66] INFOWESTER. **Criptografia.** Disponível em http://www.infowester.com/criptografia.php. Acesso em 19/5/2011, ás 10:31.

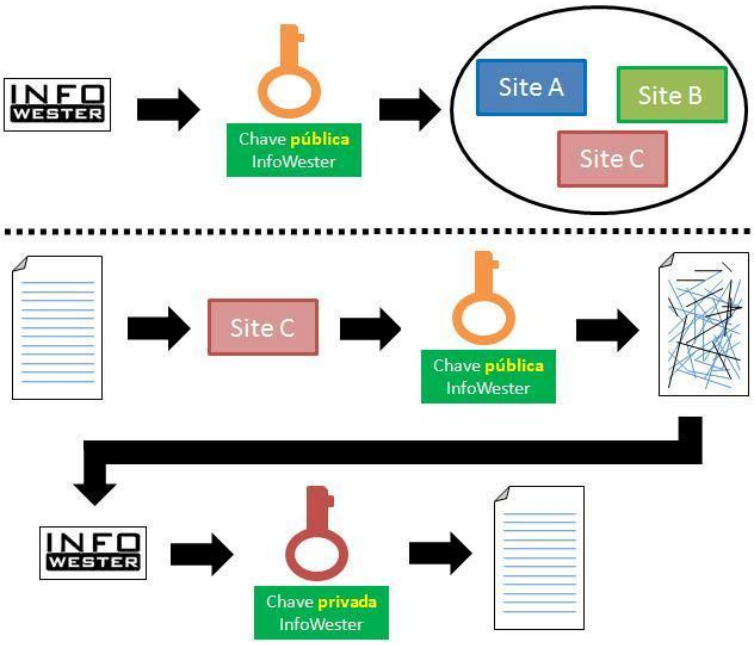


Figura 9 – Criptografia – chave publica e privada.

Fonte: InfoWester

(http://www.infowester.com/criptografia.php)

Diante desses aspectos, fica perceptível que por meio dos algoritmos criptográficos é admissível tornar a informação enigmática aos olhos de um terceiro estranho a relação de troca de informações, ou a qualquer ente que não possua o segredo indispensável para a correta transformação e compreensão do dado ilegível. Por esse motivo, os bancos têm buscado esses recursos com o fim de suavizar ao máximo os danos de dinheiro causados por uso indevido da informação.

5.3. Certificado digital

Como se pode observar até o presente momento, os computadores e a internet são vastamente consagrados para o processamento de dados e para o intercâmbio de mensagens e documentos entre os usuários. Contudo, como já mencionado, estas transações eletrônicas carecem da adoção de mecanismos de segurança competentes a garantir autenticidade, confidencialidade e integridade aos dados eletrônicos. A certificação digital é a tecnologia que provê estes mecanismos.

Com o uso dessa ferramenta, foi possível a presença de inúmeros benefícios para os cidadãos e para as instituições que a adotam, diga-se que com ela é admissível utilizar a internet como meio de comunicação alternativo para a

disponibilização de diversos serviços com uma maior agilidade, facilidade de acesso e substancial redução de custos.

No que cerne a certificação digital, pode-se observar que é um tipo de tecnologia de identificação que permite que transações eletrônicas dos mais variados tipos sejam desempenhadas considerando sua integridade, sua autenticidade e sua confidencialidade, de forma a impedir que falsificação, captura de informações privadas ou outros tipos de atos inconvenientes ocorram[67].

Sob essa perspectiva, entende-se que o certificado digital é um documento eletrônico assinado digitalmente e cumpre o desempenho de integrar uma pessoa ou entidade a uma chave pública. É comum, portanto, um certificado digital oferecer informações tais como o nome da pessoa ou entidade a ser associada à chave pública; o período de validade do certificado; a chave pública; o nome e assinatura da entidade que assinou o certificado; bem como o número de série[68].

Dessa forma, podemos observar na figura que se segue um exemplo comum do uso de certificados digitais que é o serviço bancário provido via Internet, diga-se que os bancos possuem certificado para autenticar-se perante o cliente, assegurando que o acesso está realmente ocorrendo com o servidor do banco, permitindo, assim, que o cliente, ao solicitar um serviço, possa utilizar o seu certificado para autenticar-se perante o banco:

---

[67] INFOWESTER. **Entendendo a certificação digital.** Disponível em http://www.infowester.com/assincertdigital.php. Acesso em 19/5/2011, ás 15:45.

[68] LANIWAY. **Certificados digitais.** Disponível em http://www.laniway.com.br/br/corporativo/certificado.do. Acesso em 19/5/2011, ás 16:46.

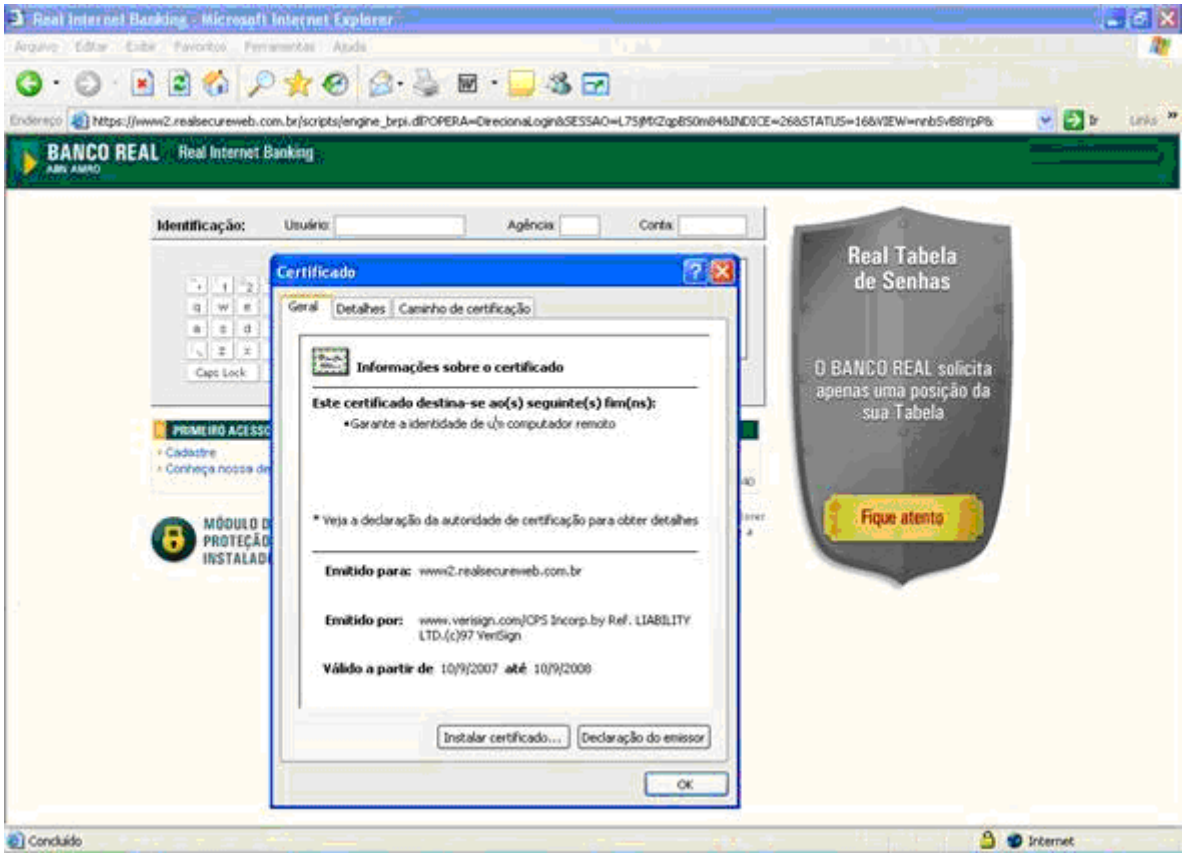


Figura 10 – Certificado digital banco.

Fonte: Informática Jurídica

(http://www.informatica-juridica.com/trabajos/A_responsabilidade_dos_bancos_pelos_prejuizos.asp)

É perceptível, dessa forma, que o certificado digital sendo um arquivo eletrônico que armazena dados é um arquivo que identifica quem é seu usuário, diga-se que é um meio de comprovar a identidade de um cliente ou instituição financeira, podendo ser armazenado em um computador ou em outra mídia.

Ao acessar um navegador, este reconhece automaticamente as empresas que detém o certificado digital e as aceitam concomitantemente os certificados por elas assinados, verificando-se em seguida a sua autenticidade e a da pagina correspondente. Para tanto, averigua-se isso, por exemplo, quando um cliente acessa a internet banking de seu banco. Ao acessá-la ira verificar um cadeado que informa que aquele site é seguro, uma vez que, se clicar neste cadeado aparecerá o certificado de habilitação do site, sendo confirmado sua autenticidade pela

concessão dada pelo certificador internacional, contendo também as informações sobre o nível de criptografia utilizada[69].

Cabe destacar, ainda, que entre as áreas imprescindíveis do certificado digital depara-se a identificação e a assinatura da entidade que o emitiu, os quais possibilitam examinar a autenticidade e a integridade do certificado. Dessa forma, aquela que emitiu é conhecida como Autoridade Certificadora ou meramente AC. Esta, por sua vez, é a parte basilar de uma infra-estrutura de chaves públicas, bem como responsável pela emissão dos certificados digitais[70].

Para compreender melhor essa situação supramencionada, apresenta-se em figura a seguir uma analogia feita ao documento de identidade da pessoa física – RG -, com o certificado digital. Na figura abaixo, averigua-se que “o certificado digital é emitido por uma Autoridade de Certificação - AC, que pode ser uma empresa, instituição ou indivíduo, tanto público quanto privado. A Autoridade de Registro – AR - opera como tabelião para examinar e autenticar a identidade dos usuários de um sistema criptográfico de chave pública. Posto isto, uma AC, que pode fazer o papel de uma AR, responsabiliza-se pela distribuição da chave pública e pela garantia de que uma determinada chave pública esteja seguramente atrelada ao nome de seu proprietário”[71].

---

69 CARTILHA DE SEGURANÇA PARA INTERNET. **Conceitos de segurança.** Disponível em http://cartilha.cert.br/conceitos/sec8.html. Acesso em 20/5/2011, ás 09:17.

70 INFOWESTER. **Entendendo a certificação digital.** Disponível em http://www.infowester.com/assincertdigital.php. Acesso em 20/5/2011, ás 09:28.

71 PUBLIC KEY INFRASTRUCTURE. **Estrutura hierárquica de certificação.** Disponível em http://www.gta.ufrj.br/grad/07_2/delio/Estruturadeumcertificadodigital.html. Acesso em 20/5/2011, ás 09:57.

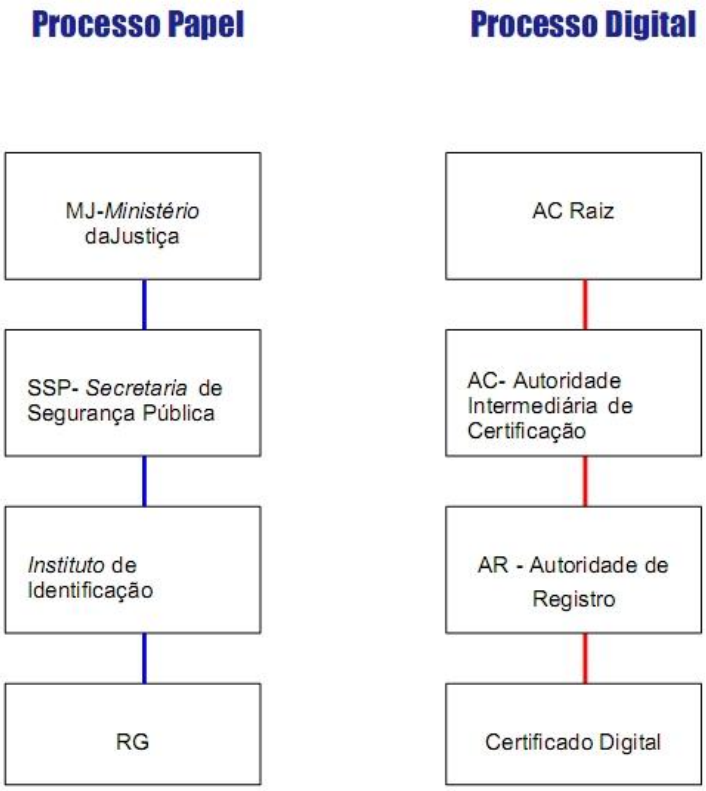


Figura 11 – Estrutura de um certificado digital.

Fonte: Public Key Infrastructure

(http://www.gta.ufrj.br/grad/07_2/delio/Estruturadeumcertificadodigital.html)

Sob esses pontos de vista, nota-se que a escolha de acreditar em uma AC é semelhante ao que ocorre em transações convencionais, as quais não empregam o meio eletrônico. Para ilustrar melhor esse apontamento observa-se a figura abaixo:

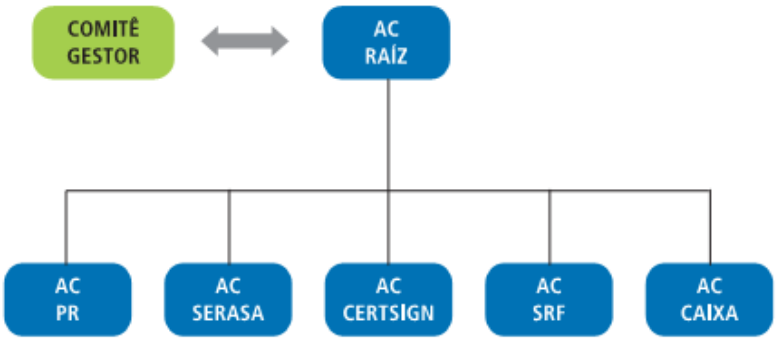


Figura 12 – Autoridade Certificadora (AC).

Fonte: YRoss

(http://yross.wordpress.com/2010/07/14/certificado-digital/)

Na figura, pode-se analisar a situação de uma empresa, por exemplo, que ao vender parcelado aceita determinados documentos para identificar o comprador antes de efetuar a transação. Usualmente, esses documentos são emitidos pela Secretaria de Segurança de Pública e pela Secretaria da Receita Federal, como o RG e o CPF. Neste momento, verifica-se a existência de uma relação de confiança já estabelecida com esses órgãos, o mesmo ocorrendo com os usuários que escolher uma AC à qual desejam confiar à emissão de seus certificados digitais[72].

Isto posto, verifica-se que para a emissão dos certificados, as ACs detém obrigações que são descritos em um documento chamado de Declaração de Práticas de Certificação – DPC. Este, por sua vez, tem que ser pública, com o fim de possibilitar que as pessoas possam saber como foi emitido o certificado digital, o qual deve debelar informações seguras que permitam a verificação da identidade do seu titular[73].

Dessa forma, são por estes motivos, que quanto mais bem definidos e mais compreensivos os procedimentos adotados por uma AC, maior será sua confiabilidade, e para isso, existe um Comitê Gestor da ICP-Brasil que especifica os procedimentos que devem ser adotados pelas ACs. Havendo o cumprimento dos procedimentos, é ele auditado e fiscalizado, envolvendo, por exemplo, exame de documentos, de instalações técnicas e dos sistemas envolvidos no serviço de certificação, como também seu próprio pessoal. Contudo, caso contrário, diga-se a não concordância com as normas, fica sujeito a penalidades, como o descredenciamento, por exemplo[74].

5.4. Protocolo SSL

Como se pode observar até o presente momento, a preocupação dos usuários está voltada à segurança e garantia do sigilo de suas informações contidas

---

[72] ROSSY, Ythalo. **Certificado digital.** Disponível em http://yross.wordpress.com/2010/07/14/certificado-digital/. Acesso em 20/5/2011, ás 10:54.

[73] CARTILHA. **O que é certificado digital.** Disponível em http://www.iti.gov.br/twiki/pub/Certificacao/CartilhasCd/brochura01.pdf. Acesso em 20/5/2011, as 11:07.

[74] Câmara brasileira do comércio eletrônico. **Comitê Gestor.** Disponível em ftp://ftp.cefetes.br/Especificos/CertificacaoDigital/Guia%20Certifica%E7%E3o%20Digital.pdf. Acesso em 20/5/2011, ás 11:22.

no meio eletrônico – internet banking - para obter sucesso em suas aplicações financeiras.

No item anterior compreendeu-se do que se trata o certificado digital, ou seja, uma garantia fornecida por uma entidade certificadora, que confirma a identificação do titular do certificado e o nível de segurança que está sendo utilizado nas páginas que estão sendo acessadas[75]. Frisa-se isso porque o protocolo SSL trata-se de uma espécie de certificado digital.

Ressalta-se, assim, que os certificados digitais SSL proporcionam uma autenticidade de que o site que o cliente está acessando é realmente de quem ele pensa ser. Ademais, o protocolo garante, por meio da criptografia dos dados, de que as informações ministradas não poderão ser interceptadas no trajeto entre o computador do usuário e o servidor da empresa[76].

Portanto, SSL – Secure Sockets Layer (Camada Segura de Sockets) – é um padrão de segurança que tem função de instituir uma conexão segura entre o navegador do usurário e a instituição financeira, de forma a impedir a interceptação dos dados sigilosos que comerciam entre os dois pontos, ou seja, o protocolo previne que os dados trafegados possam ser capturados, ou mesmo alterados no seu curso entre o browser do usuário e o site do banco com o qual está se relacionando, assegurando a proteção das informações confidenciais, como por exemplo, os dados de cartão de crédito.

São perceptíveis estes apontamentos quando o usuário acessa o browser, conectando-se a um servidor que está utilizando o protocolo SSL. Sendo assim, observa-se na barra de endereços que o protocolo passa a ser HTTPS://, ao invés do HTTP:// padrão. Junto a isso, a pluralidade de browsers apresenta um habitual cadeado, que demonstra ao cliente que os dados pessoais bem como financeiros fornecidos não poderão ser interceptados no seu procedimento[77]. Abaixo se apresenta figuras para ilustrar a explicação:

---

[75] SANTANDER. **O que é certificado de segurança.**Disponível em https://netbanking2.banespa.com.br/Paginas/Ajuda/ajuda_seguranca_3.asp Acesso em 22/5/2011, ás 23:40.

[76] LANIWAY. **Certificados seguros SSL.** Disponível em http://www.laniway.com.br/br/corporativo/certificado.do. Acesso em 22/5/2011, ás 23:53.

[77] COMODOBR. **O que é SSL.** Disponível em http://www.comodobr.com/ssl_o_que_e.php. Acesso em 23/5/2011, ás 00:46.

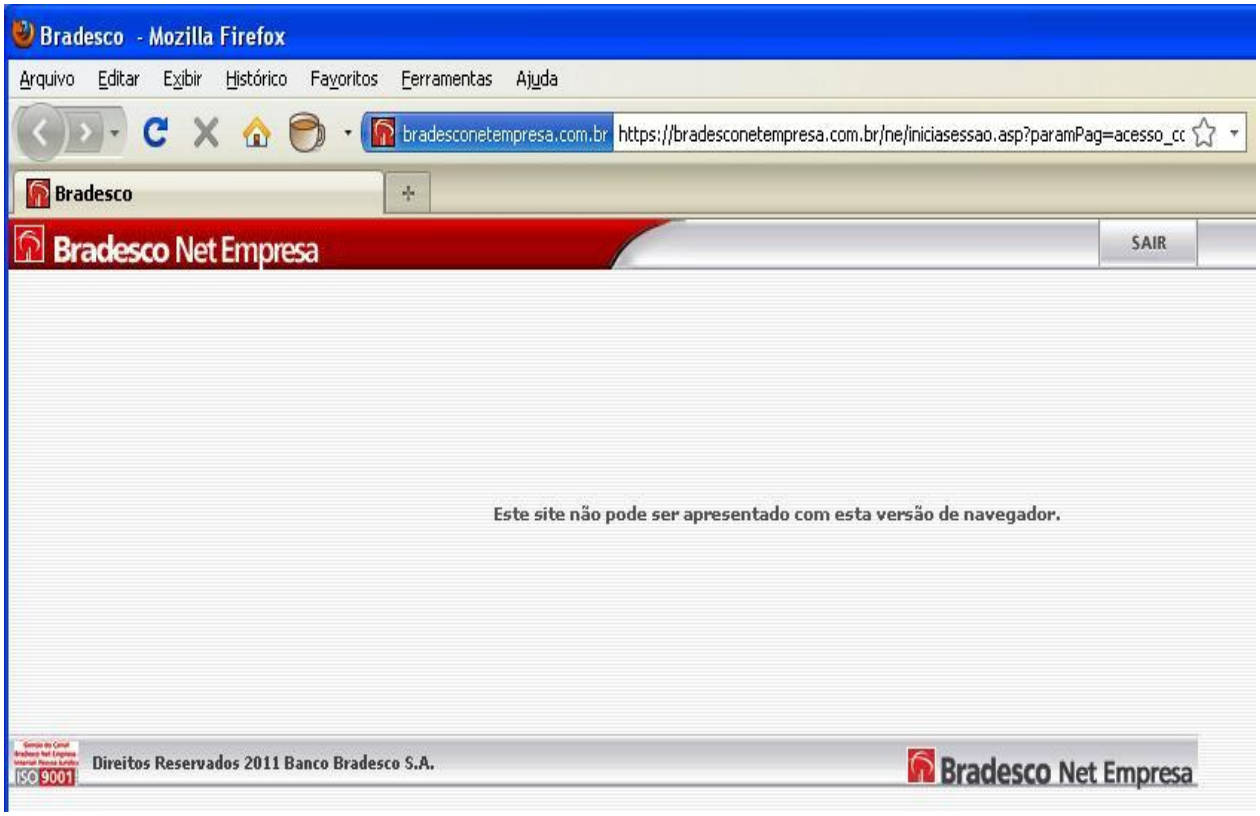


Figura 13 – Protocolo SSL HTTPS:// Bradesco.

Fonte: Bradesco

(http://www.bradesco.com.br/)

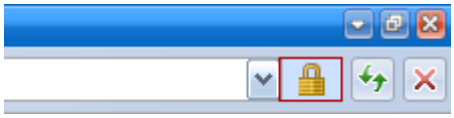


Figura 14 – Cadeado certificado digital.

Fonte: Caixa Geral de Depósitos

(http://www.cgd.pt/Seguranca/Internet-Banking/Pages/Seguranca-CGD-Certificados-Digitais.aspx)

Insta salientar que protocolo SSL é desenvolvido pela Netscape Communications Corporation, com o fim, como já fora supracitado, de transmitir documentos privados pela internet por meio de um canal de comunicação codificado. Dessa forma, o SSL funciona empregando uma chave privada para encriptar as informações que são diferidas através da conexão SSL[78]. Com efeito, o

[78]RABELLO, Nelson. **O básico do protocolo.** Disponível em http://www.webartigos.com/articles/51248/1/O-basico-do-protocolo-SSL/pagina1.html. Acesso em 23/5/2011, ás 09:22.

SSL age como uma camada adicional, garantindo a segurança dos dados, situada entre a camada aplicação e a camada transporte, conforme figura abaixo:

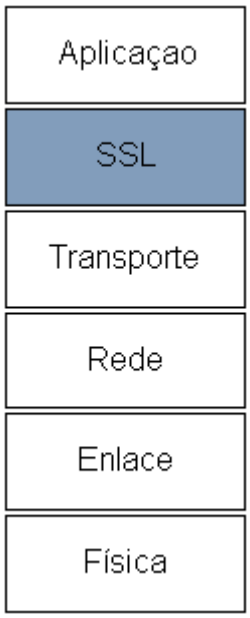


Figura 15 – Camada SSL.
Fonte: SSL – Secure Socket Layer
(http://www.gta.ufrj.br/grad/00_2/ssl/ssl.htm)

Ademais, o certificado digital SSL subdivide-se em duas camadas, quais sejam handshake e record. O SSL suporta vários protocolos de alto nível, e um deles é o protocolo handshake. Este, por sua vez, é utilizado com o fim de ordenar os estados entre cliente e servidor, tendo em vista que no decorrer do seu procedimento, os certificados são transmitidos entre o cliente e o servidor para comprovar suas identidades. Assim sendo, o cliente cria um grupo de chaves aleatórias, as quais serão empregadas para a criptografia dos dados, bem como para a geração dos MACs. Estas, assim, são criptografadas usando a chave pública do servidor e enviadas para o servidor[79].

Já a camada record, conglomera vários protocolos de alto nível, e utiliza a acepção de estado corrente para eleger os algoritmos de compressão e criptografia adequados. Dessa forma, todas as informações são protegidas utilizando-se os

[79] RABELLO, Nelson. **O básico do protocolo.** Disponível em http://www.webartigos.com/articles/51248/1/O-basico-do-protocolo-SSL/pagina1.html. Acesso em 23/5/2011, ás 10:09.

algoritmos de criptografia e MAC definidos no Cipher Spec - ferramenta usada para notificar uma das partes a respeito de mudanças na estratégia de criptografia[80].

Portanto, fica perceptível que o protocolo SSL é uma tecnologia considerada como o padrão de segurança na transmissão de dados pelo meio virtual, uma vez que, se terceiro não autorizado receber determinados dados não conseguirá decifra-los bem como lê-los, o que significa a garantia da seguridade e privacidade das informações dos clientes.

Figura 16 – Protocolo SSL.

Fonte: Santander

(http://www.santander.com.br/portal/wps/script/templates/GCMRequest.do?page=6687)

5.5. Smart card

O smart card surge como um fantástico instrumento de segurança. Este, por sua vez, é um cartão contendo um chip responsável pela geração e o armazenamento de certificados digitais, diga-se arquivamento de informações que

[80] BETO. **SSL – Secure Socket Layer**. Disponível em http://www.gta.ufrj.br/grad/00_2/ssl/ssl.htm. Acesso em 23/5/2011, ás 10:25.

dizem respeito ao respectivo usuário. Conhecido como cartão inteligente, este se assemelha a um cartão de credito diante do seu tamanho e formato, sendo seu inferior totalmente distinto, já que em seu interior há um microprocessador embutido[81].

Frisa-se, assim, que este microprocessador fica sob uma placa de contato de ouro em uma das faces do cartão. Este microprocessador tem como fim garantir a segurança das informações ali armazenadas. Isto posto, é como se o computador e o leitor de cartão interagissem com o microprocessador, que por sua vez permite o acesso aos dados contidos no cartão[82].

Um dos papeis fundamentais dessa ferramenta, entretanto, não é evitar que se tenha acesso ao micro, mas admitir ou não o acesso à rede na qual o micro está conectado. Dessa forma, o servidor da rede autoriza ou não o uso da rede dependendo do conteúdo existente no smart card.

Ressalta-se, ainda, que como o smart card é singular, o único modo de terceiro mal intencionado utilizar a rede por meio do micro de outro usuário, será literalmente furtando o cartão.

Podem estes ser utilizados com leitores conectados em um computador pessoal a fim de autenticar um usuário, bem como por meio de softwares de navegação na internet com o fim de complementar SSL e melhorar a segurança em transações na internet, ou seja, é possível a transmissão de informações por dois meios: com ou sem contato com o smart card. Aqueles que precisam de contato ocorrem quando há um leitor com conexão direta a um micromódulo na superfície do cartão. Já o cartão sem contato exige somente a proximidade do leitor, pois tanto o cartão quanto o leitor têm antenas e por meio destas fazem a conexão conseguindo se comunicar[83].

Diante do exposto até o presente momento, verifica-se que os smart cards oferecerem mais segurança e confidencialidade que outros tipos de informação ou armazenamento de informação, já que se trata de um local seguro para

---

[81] COMO TUDO FUNCIONA. **O que é um leitor smart card.** Disponível em http://www.hsw.uol.com.br/questao332.htm. Acesso em 20/5/2011, ás 12:40.

[82] TORRES, Gabriel. **Smart card.** Disponível em http://www.clubedohardware.com.br/artigos/665. Acesso em 20/5/2011, ás 12:52.

[83] MATOS, Conrado Leiras. **Smart card.** Disponível em http://www.gta.ufrj.br/grad/01_2/smartcard/smartcard.html. Acesso em 20/5/2011, ás 15:19.

armazenamento de informação como chaves privadas, números de contas, e informações pessoais, ou então para executar demais processos, tanto o é que observamos suas aplicações em diversos modos como cartões de crédito, dinheiro eletrônico, sistemas de segurança por computador, comunicação sem fio, operações bancárias, identificação de membros do governo, dentre outros.

Figura 17 – Smart card.

Fonte:Smart Card Basics

(http://www.smartcardbasics.com/smart-card-types.html)

5.6. Token

O token, ou a chave eletrônica, é um dispositivo de segurança criado para garantir a proteção das transações realizadas pelos clientes que usufruem do meio internet banking. Esse dispositivo gera automaticamente senhas instantâneas. Sendo assim, é um instrumento que arquiva as chaves privadas e os certificados digitais, contendo normalmente em sua estrutura uma bateria e um chip que ao ser pressionado um botão gera as chaves aleatórias e temporárias dentro de um espaço de tempo determinado. Portanto, esse código, sendo temporário e aleatório, é de

uso singular para os serviços no acesso ao internet banking, diga-se para qualquer transação realizada por este meio virtual[84].

A denominação denota “passe”, compreendendo-se que trata de dispositivos geradores de códigos aleatórios, necessários para acessar a conta bancária ao lado da senha individual, impossibilitando, assim, a intercepção de terceiros mal intencionados.

Como já mencionado, o código é valido por poucos segundos, o que obsta ainda mais a ação dos criminosos. O token tem a estrutura semelhante a um pequeno chaveiro, parecido com um pendrive, conforme figura abaixo:

Figura 18 – Token.

Fonte: Tecmundo

(http://www.tecmundo.com.br/3077-o-que-e-token-.htm)

Existe também token para deficientes visuais, em que especificamente o Banco Bradesco desenvolveu. Este dispositivo tem a mesma finalidade do token convencional, contudo ele fornece as chaves de segurança por meio do áudio, ou seja, as informações são verbalizadas e ouvidas pela caixa de som embutidas ou fone de ouvido, conforme figura que se segue:

[84] FONSECA, Willian. **O que é token.** Disponível em http://www.tecmundo.com.br/3077-o-que-e-token-.htm. Acesso em 23/5/2011, ás 10:59.

Figura 19 – Token para deficientes visuais.

Fonte: Bradesco

(http://www.bradescosegurança.com.br)

Alem desses, há, ainda, o token list. Este, por sua vez, é um cartão com uma lista de senhas numéricas e enumeradas, geradas para trazer mais uma opção de segurança aos clientes dos bancos.

Figura 20 – Token list.

Fonte: Secure list

(http://www.securelist.com/en/analysis/204792084/Brazil_a_country_rich_in_banking_Trojans)

Isto posto, fica perceptível, portanto, que essas peculiaridades incluindo-se o bom uso do computador, diga-se obtendo cuidados essenciais com fraudes, spam e phishing, bem como evitar a utilização da internet banking em redes públicas, são a melhor forma de prevenir os possíveis danos com invasões de contas bancárias.

5.7. Plugin

Este é mais um meio de segurança que as instituições financeiras utilizam para garantir o fiel uso pelos seus usuários/clientes da ferramenta internet banking. Como os demais recursos já apontados, o plugin vem também com o objetivo de impedir os atos ilícitos realizados pelos fraudadores.

O plugin é um programa instalado, diga-se um software, que executa-se de forma integrada com os navegadores, como internet explorer e firefox, com o fim de amenizar os riscos dos programas maliciosos, que são instalados no computador do usuário sem o seu consentimento, com o objetivo de apanhar os dados pessoais bem como financeiros do cliente.[85]

Este dispositivo é perceptível quando o cliente acessa o site do banco, e ao realizar o login colocando o usuário e senha, a página da internet banking informa a possibilidade de instalar o plugin. Ressalta-se, ainda, que tem como desígnio na atuação de detectar softwares maliciosos, como por exemplo, o cavalo-de-troia. Para isso, o plugin só irá agir no computador o qual ele fora instalado, ou seja, caso o cliente utilize computador diverso daquele o qual ele já tenha instalado o plugin, terá que instalar também nesse outro.

Imprescindível frisar, contudo, que esse dispositivo não exime o uso do antivírus convencional, para tanto, deve o cliente mantê-lo sempre atualizado, bem como o aplicativo firewall.

5.8. Teclado virtual

O teclado virtual foi projetado para alargar a segurança dos dados transmitidos ao utilizar a internet banking, ou seja, adveio com o objetivo de incrementar a proteção contra vírus, por exemplo, que vigiam a digitação no teclado convencional, bem como os campos de digitação das paginas web e informações antes de serem criptografadas[86].

---

[85]BRADESCO. **Segurança.** Disponível em http://www.bradescoseguranca.com.br/html/content/seguro/ib_elementos_plugin.asp. Acesso em 23/5/2011, ás 11:55.

[86]SANTANDER. **Teclado virtual.** Disponível em https://www.santandernet.com.br/Paginas/Ajuda/AjudaNC/iframe_teclado.asp. Acesso em 23/5/2011, ás 12:55.

Com o uso desse meio, é possível impedir que os dados de acesso sejam enviados a outros computadores por intermédio de ameaças cibernéticas ou softwares que podem ser instalados no computador sem o consentimento do usuário.

Será obrigatório o seu uso sempre que o cliente digitar a senha de acesso ao internet banking, bem como quando digitar a senha do cartão para confirmar as transações realizadas.

Não obstante, frisa-se que o teclado virtual emprega a ambigüidade, isto é, cada caractere da senha é apresentado junto a um grupo de dois ou três outros caracteres, tendo em vista que a ordem dos números dentro de cada botão muda aleatoriamente toda vez que o cliente utiliza o teclado virtual[87].

Seu objetivo, portanto, é limpar os campos onde a senha é digitada, não as arquivando em disco ou memória, impossibilitando, dessa forma, que os campos de digitação sejam monitorados. Há teclados, contudo, que não detém somente essa função, como é o caso, por exemplo, do Banco Bradesco, em que o teclado virtual serve também para escrever perguntas sigilosas, tendo em vista que se trata de um teclado alfanumérico e com outros caracteres semelhantes a um teclado convencional.

Figura 21 – Teclado alfanumérico.

Fonte: Bradesco

(www.bradescoseguranca.com.br/.../ib_elementos_teclado.asp)

[87]CAIXA ECONOMICA FEDERAL. **Teclado virtual.** Disponível em http://www.caixa.gov.br/seguranca/seguranca_internet_banking_pg5.asp. Acesso em 22/5/2011, ás 13:02.

6. SELO DIGITAL

O selo digital é conhecido como uma imagem constituída por cinco subsídios combinados de certo modo que formam uma imagem de um selo singular para cada cliente. Sendo assim, seu fundamental objetivo é a aprovação para o cliente que ele está de fato acessando o site de sua instituição financeira. Para tanto, ele é composto por: I. um número de dois dígitos; II. uma imagem inserida ao fundo; III. uma cor de fundo; IV.uma forma de selo; V. uma forma e posição de "carimbo" impresso sobre o selo[88].

Frisa-se que sendo o selo único e pessoal, deve todos os seus elementos ser memorizados, uma vez que a mesma imagem deverá aparecer em todos os seus acessos. Portanto, o cliente só deverá digitar sua senha depois de confirmado o selo.

Imprescindível ressaltar que mesmo apresentando a vantagem de ser personalizado, trata - se de um meio de segurança que garante a veracidade do site acessado, pois por mais que uma página falsa consiga imitar um determinado selo legítimo, não poderá associar os cinco elementos de cada selo para cada cliente, conforme informação disposta no site do banco HSBC. A figura abaixo ilustra a explicação:

Figura 22 – Selo digital.
Fonte: HSBC
(http://www2.hsbc.com.br/common/seguranca/artigo-seguranca-selo-digital.shtml)

[88] HSBC. **Selo digital.** Disponível em http://www2.hsbc.com.br/common/seguranca/hsbc-faz-ib-selo.shtml. Acesso em 23/5/2011, ás 19:33.

7. CONSIDERAÇÕES FINAIS

Tendo em vista as informações expostas no desenvolvimento deste trabalho é possível averiguar que com o avanço tecnológico foi possível à criação de dispositivos de segurança que garantissem a proteção de dados pessoais e financeiros conforme a necessidade que foi surgindo no decorrer dos tempos. É perceptível que os fraudadores não são piedosos, uma vez que não medem esforço algum na obtenção do maior lucro possível ao cometer um ato ilícito. Para tanto, a informática é uma ferramenta em que a instituição financeira utiliza para se tornar cada vez mais eficiente e eficaz, atendendo de forma adequada os seus clientes, com o fim de proporcionar e garantir a segurança de suas informações.

A captação do uso da ferramenta internet banking é um desafio, já que se trata de um meio que dispõe de tecnologia e está sujeito a sofrer mudanças constantes. Dessa forma, o seu objetivo deve ser fundado em uma ferramenta eficiente para a instituição financeira alcançar suas metas. Para isso, esse instrumento deve proporcionar confiança tanto para os bancos, como também para os seus clientes.

Ademais, salienta-se que o uso cumulativo de uma senha padrão - digitada por teclado virtual -, frases secretas e o uso da denominada tabela contendo posição de senhas (chaves de segurança) conduz à diminuição de ocorrência de fraudes, de certo modo que o terceiro mal intencionado não logrará êxito na concretização de transferências e pagamentos sem deter todo o conjunto de informações a serem dispostas em duas ou três telas do computador.

Dessa forma, por óbvio que é mais benéfico perder certo tempo para a realização de uma operação virtual, tendo o acréscimo de segurança, do que arriscar a realizar operações virtuais simples e rápidas podendo ter como resultado um grande prejuízo financeiro, bem como pessoal.

Por derradeiro, imprescindível torna-se a importância de mostrar os mecanismos de segurança que as instituições financeiras dispõem, tendo em vista que não se safistaz o objetivo das instituições financeiras oferecendo apenas os recursos de proteção, devendo, assim, instruir o usuário a se precaver contra fraudes, pois a segurança sem um treinamento não basta, ou seja, é como entregar arma carregada a quem não sabe atirar.

REFERENCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Citação**: NBR-10520/ago - 2002. Rio de Janeiro: ABNT, 2002.

_____. **Referências**: NBR-6023/ago. 2002. Rio de Janeiro: ABNT, 2002.

ACCORSI, A. **Automação: bancos e bancários**. Dissertação de mestrado. (Mestrado em Administração). Universidade de São Paulo. São Paulo-SP, 1990.

A.I.S.A. **História da Internet.** Disponível em http://www.aisa.com.br/historia.html. Acesso em 21/03/2011.

ALBERTIN, A. L. **Comércio eletrônico. Um estudo no setor bancário.** Resumo da Tese de Doutorado – Faculdade de Economia Administração e Contabilidade (FEA) da Universidade de São Paulo – (USP). São Paulo: FEA/USP, 1997.

ALECRIM, Emerson. **Endereço IP**. Disponível em http://www.infowester.com/internetprotocol.php. Acesso em 21/03/2011.

ALECRIM, Emerson. **Vírus de computador: o que são e como agem**. Disponível em http://www.infowester.com/virus.php. Acesso em 16/5/2011.

ARAUJO, Nonata Silva. **Segurança da Informação (TI).** Disponível em http://www.administradores.com.br/informe-se/artigos/seguranca-da-informacao-ti/23933/. Acesso em 07/5/2011.

ANTISPAM. **O que é um spam**. Disponível em http://www.antispam.br/conceito/. Acesso em 18/5/2011.

BETO. **SSL – Secure Socket Layer**. Disponível em http://www.gta.ufrj.br/grad/00_2/ssl/ssl.htm. Acesso em 23/5/2011.

BOGO, Kellen Cristina. **História da Internet.** Diponível em http://www.kplus.com.br/materia.asp?co=11&rv=Vivencia. Acesso em 21/03/2011.

BRADESCO. **Segurança.** Disponível em http://www.bradescoseguranca.com.br/html/content/seguro/ib_elementos_plugin.asp. Acesso em 23/5/2011.

Câmara brasileira do comércio eletrônico. **Comitê Gestor.** Disponível em ftp://ftp.cefetes.br/Especificos/CertificacaoDigital/Guia%20Certifica%E7%E3o%20Digital.pdf. Acesso em 20/5/2011.

CARTILHA. **O que é certificado digital.** Disponível em http://www.iti.gov.br/twiki/pub/Certificacao/CartilhasCd/brochura01.pdf. Acesso em 20/5/2011.

CARTILHA DE SEGURANÇA PARA INTERNET. **Conceitos de segurança.** Disponível em http://cartilha.cert.br/conceitos/sec8.html. Acesso em 19/5/2011.

CARTILHA DE SEGURANÇA PARA INTERNET. **Fraude na internet**. Disponível em: http://cartilha.cert.br/fraudes/sec2.html#subsec2.2. Acesso em 18/5/2011.

CARTILHA DE SEGURANÇA. **Spam**. Disponível emhttp://cartilha.cert.br/spam/sec1.html#subsec1.1. Acesso em 18/5/2011.

CASTELLS, Manuel. **A Galáxia da Internet.** Disponível em http://www.edrev.info/reviews/revp49.pdf. Acesso em 21/03/2011.

CAIXA ECONOMICA FEDERAL. **Teclado virtual.** Disponível em http://www.caixa.gov.br/seguranca/seguranca_internet_banking_pg5.asp. Acesso em 22/5/2011.

CLESIO, Fabio. **Segurança da Informação**. Disponível em http://info.abril.com.br/forum/viewtopic.php?f=122&t=371. Acesso em 10:5/2011.

COMO TUDO FUNCIONA. **O que é um leitor smart card.** Disponível em http://www.hsw.uol.com.br/questao332.htm. Acesso em 20/5/2011.

COMODOBR. **O que é SSL.** Disponível em http://www.comodobr.com/ssl_o_que_e.php. Acesso em 23/5/2011.

CORREIA, Márcio A. S. **Segurança em Internet Banking.** Disponível em http://ximen.es/artigos/Sbseg2008_BancoDoBrasil.pdf. Acesso 19/5/2011.

DIÁRIO DIGITAL. **Primeira mensagem de correio electrónico enviada há 40 anos.** Disponível em http://diariodigital.sapo.pt/news.asp?section_id=18&id_news=417591. Acesso em 21/03/2011 ás 10:24.

ÉDIPO, Luciano. **Internet**. Disponível em http://www.marketing.com.br/index.php?option=com_content&view=article&id=374:no-primeiro-trimestre-de-2008-a-internet-acompanhou-a-taxa-de-crescimento-trimestral-de-2007&catid=43:midias-digitais&Itemid=106. Acesso em 21/03/2011.

ESTRADA, Manuel Martin Pino. **A INTERNET BANKING NO BRASIL, NA AMÉRICA LATINA E NA EUROPA.** Disponível em http://www.publicacoesacademicas.uniceub.br/index.php/prisma/article/viewFile/185/161. Acesso em 12/5/2011.

FEBRABAN. **Atendimento e serviços.** Disponível em: http://www.febraban.org.br. Acesso em 12/5/2011.

FONSECA, Willian. **O que é token.** Disponível em http://www.tecmundo.com.br/3077-o-que-e-token-.htm. Acesso em 23/5/2011.

GOMES, Alessandra Aparecida Calvoso. **Operações bancárias via Internet (Internet banking) no Brasil e suas repercussões jurídicas**. In Revista dos Tribunais, vol. 816, outubro de 2003.

HSBC. **Selo digital.** Disponível em http://www2.hsbc.com.br/common/seguranca/hsbc-faz-ib-selo.shtml. Acesso em 23/5/2011.

INFOWESTER. **Criptografia.** Disponível em http://www.infowester.com/criptografia.php. Acesso em 19/5/2011.

INFOWESTER. **Entendendo a certificação digital.** Disponível em http://www.infowester.com/assincertdigital.php. Acesso em 20/5/2011.

KENN, Peter G. W. **Guia Gerencial para a tecnologia da informação: Conceitos essenciais e terminologia para empresas e gerentes**. Rio de Janeiro: Campus, 1996,p.XLIX.

LAUREANO, Marcos Aurelio Pchek. **Gestão de Segurança da Informação**. Disponível em http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf. Acesso em 10/5/2011.

LAURINDO, Fernando José Barbin; DE CARVALHO, Marly Monteiro; JR, Roque Rabechini, SHIMIZU, Tamio. **O PAPEL DA TECNOLOGIA DA INFORMAÇÃO (TI) NA ESTRATÉGIA DAS ORGANIZAÇÕES**. Disponível em http://www.scielo.br/pdf/gp/v8n2/v8n2a04.pdf, acesso em 09/5/2011.

LAUDON, Kenneth C. & LAUDON, Jane Price. **Sistemas de informações: administrando a empresa digital.** São Paulo: Prentice Hall, 2004 – 5ª edição.

LAU, Marcelo; SANCHEZ, Pedro Luiz Próspero. **TÉCNICAS UTILIZADAS PARA EFETIVAÇÃO E CONTENÇÃO DAS FRAUDES SOBRE INTERNET BANKING NO BRASIL E NO MUNDO.** Disponível em http://www.datasecur.com.br/academico/Tecnicas_Utilizadas_para_Efetivacao_e_Contencao_das_fraudes.pdf. Acesso em 16/5/2011.

LANIWAY. **Certificados digitais.** Disponível em http://www.laniway.com.br/br/corporativo/certificado.do. Acesso em 19/5/2011.

LANIWAY. **Certificados seguros SSL.** Disponível em http://www.laniway.com.br/br/corporativo/certificado.do. Acesso em 22/5/2011.

MATOS, Conrado Leiras. **Smart card**. Disponível em http://www.gta.ufrj.br/grad/01_2/smartcard/smartcard.html. Acesso em 20/5/2011.

MÉDICE, Roney. **Ameaças aos Sistemas de Informação**. Disponível em http://www.profissionaisti.com.br/2010/07/ameacas-aos-sistemas-de-informacao/. Acesso em 13/5/2011.

MICROSOFT. **O que é um vírus de computador?** Disponível em http://www.microsoft.com/brasil/athome/security/viruses/intro_viruses_what.mspx. Acesso em 14/5/2011.

MICROSOFT. **O que são vírus, worms e cavalos de Tróia**. Disponível em: http://www.microsoft.com/brasil/athome/security/viruses/virus101.mspx#EDD. Acesso em 18/5/2011.

MOREIRA, Ademilson. **A importância da segurança da informação**. Disponível em http://www.oficinadanet.com.br/artigo/1124/a_importancia_da_seguranca_da_informacao. Acesso em 10/5/2011.

MUNHOZ, Felipe. **Tecnologia da informação.** Disponível em http://blog.felipemunhoz.com/criptografia/. Acesso em 19/5/2011.

NETO, Cláudio Ângelo. **Cuidado ao acessar seu Internet Bank. Vírus circula na Internet e atinge usuários brasileiros.** Disponível em http://www.argohost.net/blog/cuidado-ao-acessar-seu-internet-bank-virus-circula-na-internet-e-atinge-usuarios-brasileiros/. Acesso em 17/5/2011.

NUNES, Délio Silva. **Criptografia.** Disponível em http://www.gta.ufrj.br/grad/07_2/delio/Criptografiasimtrica.html. Acesso em 19/5/2011.

OLIVEIRA, Bruno de. **Déficit de profissionais de TI chegará a cerca de 750 mil vagas em 2020**. Disponível em http://www.dci.com.br/noticia.asp?id_editoria=9&id_noticia=372580. Acesso em 11/5/2011.

PACHECO, Roberto C.S; TAIT, Tania Fatima Calvi. **Tecnologia de Informação: Evolução e Aplicações.** Disponível em: http://www.upf.br/cepeac/download/rev_n14_2000_art6.pdf. Acessado em 06/5/2011.

PUBLIC KEY INFRASTRUCTURE. **Estrutura hierárquica de certificação.** Disponível em http://www.gta.ufrj.br/grad/07_2/delio/Estruturadeumcertificadodigital.html. Acesso em 20/5/2011.

RABELLO, Nelson. **O básico do protocolo.** Disponível em http://www.webartigos.com/articles/51248/1/O-basico-do-protocolo-SSL/pagina1.html. Acesso em 23/5/2011.

RASKIN, Sara. **Uma arquitetura de tecnologia de informação**. XXV SEMINÁRIO NACIONAL DE INFORMÁTICA PÚBLICA, Anais, Salvador, Bahia, 1997.

RFTecnologia. **História da tecnologia**. Disponível em: http://www.rftecnologia.hd1.com.br/historiadatecn.htm. Acesso em 04/5/2011.

ROSE, Lílian. **A Ética da Internet Anonimato e Impunidade, Liberdade e Censura**. Disponível em http://www.adtevento.com.br/INTERCOM/2007/resumos/R0211-1.pdf. Acesso em 21/03/2011.

ROSSY, Ythalo. **Certificado digital.** Disponível em http://yross.wordpress.com/2010/07/14/certificado-digital/. Acesso em 20/5/2011.

SANTANDER. **Internet Banking**. Disponível em https://www.santandernet.com.br/Paginas/Ajuda/AjudaNC/iframe_PerguntasFrequentes.asp. Acesso em 12/5/2011.

SANTANDER. **[Home page]**. Disponível em https://www.santandernet.com.br/Paginas/Ajuda/AjudaNC/iframe_PerguntasFrequentes.asp. Acesso em 13/5/2011.

SANTANDER. **O que é certificado de segurança.** Disponível em https://netbanking2.banespa.com.br/Paginas/Ajuda/ajuda_seguranca_3.asp Acesso em 22/5/2011.

SANTANDER. **Teclado virtual.** Disponível em https://www.santandernet.com.br/Paginas/Ajuda/AjudaNC/iframe_teclado.asp. Acesso em 23/5/2011.

SEGURANÇA EM TI. **Ameaça à segurança**. Disponível em http://segurancaemti.wordpress.com/2009/07/08/ameacas-a-seguranca/. Acesso em 13/5/2011.

SEABRA, Luciana. **Uso de internet banking avança 27% e número de agências se mantém**. Disponível em http://economia.uol.com.br/ultimas-noticias/valor/2011/05/04/uso-de-internet-banking-avanca-27-e-numero-de-agencias-se-mantem.jhtm. Acesso em 24/5/2011.

STERN, Jim. **Serviço ao cliente na Internet**, São Paulo: Ed. Makron Books 2000

TADEU, Erivelto. **Gastos dos bancos com TI crescem 15% e somam R$ 22 bi.** Disponível em http://www.tiinside.com.br/04/05/2011/gastos-dos-bancos-com-ti-crescem-15-e-somam-r-22- bi/ti/223001/news.aspx. Acesso em 10/5/2011.

TORRES, Gabriel. **Smart card.** Disponível em http://www.clubedohardware.com.br/artigos/665. Acesso em 20/5/2011.

WALTON, Richard E. T**ecnologia de informação - o uso de TI pelas empresas que obtêm vantagem competitiva**. Trad. Edson Luiz Riccio. São Paulo: Atlas, 1994.

ZEVALLOS, Ruben. **A História da Internet.** Artigonal Diretório de Artigos Gratuitos. Disponível em http://www.artigonal.com/ti-artigos/a-historia-da-internet-737117.html. Acesso em 21/03/2011.