Introdução

A gestão de segurança em Internet Banking é um assunto que instiga a curiosidade das pessoas, por mostrar um ponto frágil dos bancos, em um ambiente novo como a *web*. Os riscos, com os quais os bancos lidam, no mundo físico, se reproduzem, de forma particular, na Internet, onde as fraudes e crimes financeiros, bem como problemas com a imagem do banco, podem ocorrer, em uma velocidade não experimentada até pouco tempo. A Internet promoveu a redução de custos das instituições financeiras, mas, ao mesmo tempo, abriu um novo espaço para as ameaças e tentativas de invasão aos seus sistemas e aplicativos. Caso os riscos e investimentos em segurança não forem bem calculados, o banco pode sofrer perdas financeiras, em vez de ganhos com redução de custos.

O Internet Banking é o mais novo canal eletrônico explorado pelos bancos, enquanto que a ATM (*Automated Teller Machines*) e o atendimento telefônico já são utilizados desde o início da década 80, a Internet, rede pública, surgiu no mundo financeiro no final da década de 90. A área de tecnologia das instituições foi pioneira em motivar a adoção da tecnologia como um novo meio de transacionar e se relacionar com os clientes, isto em virtude da especialidade técnica necessária. O universo de usuários, clientes dos bancos, deste novo canal eletrônico, era restrito, pois além de terem acesso a um computador, este deveria estar conectado a um provedor de Internet, o que, no final da década de 90, não eram recursos democratizados, devido aos seus custos. Este cenário evoluiu, positivamente, em curto espaço de tempo, detalhe explorado mais à frente.

Os bancos, oportunamente, desenvolveram, experimentaram e testaram os recursos da Internet, ao mesmo tempo em que o meio evoluía e amadurecia. Portanto, no final da década de 90, os bancos ofereciam serviços e produtos no Internet Banking, mas o seu universo de usuários era pequeno, limitando, assim, as perdas financeiras ocasionadas pelas falhas de segurança.

A análise dos casos de gestão de Internet Banking, nos três bancos pesquisados neste trabalho, foi feita com base em 10 domínios de segurança de informação, que, por sua vez, foram agrupados em 3 camadas: física, lógica e humana.

Por meio da classificação dos domínios e das camadas é possível planejar a gestão de segurança do Internet Banking, além de compreender os três casos. Nesta gestão, há espaço para especialistas, que atuarão em um domínio ou em uma camada, e há espaço para o profissional multidisciplinar, que tenha o olhar panorâmico para orquestrar esta gestão.

A gestão de segurança envolve diversos *trade-offs*, que devem ser aderentes à estratégia da organização no quesito custo/benefício, para atender, de forma adequada, às necessidades mercadológicas e de investimento em tecnologia. O ideal é que o banco atue sempre de forma preventiva, todavia, devido aos custos e escassez de recursos humanos e tecnológicos, e até por barreiras culturais da organização e do mercado, o banco talvez decida atuar de forma detectável ou corretiva. O importante é o banco se conscientizar da necessidade de ter uma gestão transparente de segurança do seu canal Internet Banking, e buscar o ponto ótimo de gestão, que caiba no seu bolso e agrade aos seus clientes.

A estrutura desta dissertação segue o seguinte roteiro:

Neste primeiro capítulo define o canal eletrônico Internet Banking, inserindo-o no contexto bancário brasileiro. Justifica a importância deste canal, destacando as preocupações com segurança e sua gestão, para depois, definir os objetivos e o escopo de análise deste trabalho.

O segundo capítulo faz um levantamento do referencial teórico usado, destrinchando a segurança de informação no mercado bancário, a gestão de risco e segurança e as ameaças que fragilizam o Internet Banking. Nele, destaca-se a procura por um referencial bibliográfico que desvende as camadas física, lógica e humana, que envolvem a gestão de segurança, bem como os 10 domínios que abrangem este tema.

O terceiro capítulo destaca a metodologia utilizada para o estudo de casos, a abordagem com os bancos, o protocolo e a aplicação da pesquisa.

O quarto capítulo mostra os resultados da pesquisa, através da análise dos 10 domínios de gestão de segurança eletrônica, posteriormente classificados nas três camadas.

O quinto capítulo apresenta conclusões do trabalho, limitações do estudo e sugestões sobre futuros projetos de pesquisa.

Por fim, há a bibliografia utilizada e os anexos, com informações complementares.

1. Definição do problema

Os bancos, no Brasil, vêm investindo em tecnologia para ampliar a sua gama de produtos e serviços, além de diversificar os pontos de contato com o cliente. O Internet Banking é um destes pontos de contato, sendo o canal eletrônico de auto-atendimento que mais cresce (D'ANDRÉA et al, 2000). Os canais de auto-atendimento também são conhecidos como Banco Eletrônico ou canal eletrônico, compostos pelo caixa eletrônico ou ATM (*Automated Teller Machines*); atendimento telefônico URA (Unidade de Resposta Audível) ou pessoal; *home* e *office Banking*, e Internet Banking. Nas palavras de SOUZA (2000):

> *"O Banco Eletrônico é um conjunto de produtos e serviços suportado por modernas ferramentas tecnológicas e realizado com baixa interferência humana. Restrito inicialmente aos caixas eletrônicos, cresce a cada dia pela implementação de produtos como o home, o office e o Internet Banking, a ponto de não haver mais sentido pretender-se delinear suas fronteiras com o que alguns chamam de 'banco tradicional'."*
> (SOUZA, 2000, p. 5)

A viabilidade do canal eletrônico baseia-se na possibilidade dos valores monetários, expressos em papel-moeda, se converterem em informações que possam ser armazenadas e manipuladas eletronicamente. DINIZ destacou que a automação bancária tem associação estratégica com a idéia de que "o **dinheiro** caminha para se transformar exclusivamente em **informação**" (DINIZ, 1994, p. 64, grifo nosso), o que leva os bancos a estarem na vanguarda da Tecnologia de Informação (TI).

As instituições financeiras se transformaram, ao longo dos avanços tecnológicos ocorridos a partir 1965, impulsionadas pela reforma bancária, lei 4.595/64, decretada pelo governo militar brasileiro, com a qual o Estado pretendia ajustar o sistema financeiro ao estágio de desenvolvimento que já se observava na indústria (DINIZ, 1994). A reforma foi baseada na lei bancária americana, que definia que o "Brasil tivesse um sistema financeiro segmentado e com um papel preponderante para o Banco Central" (TROSTER, 2004, p. 10). Na década de 70, presenciou-se o desenvolvimento de uma "tecnologia caseira" (DINIZ, 2004, p. 56), promovida pelo "Segundo Plano Nacional de Desenvolvimento" (II PND), lançado em 1975. O plano fechou o mercado nacional para a tecnologia importada, com intuito de emancipação tecnológica na área de informática.

Conforme DINIZ, na década de 70, os bancos tiveram um papel importante no desenvolvimento tecnológico do país, por investirem em desenvolvimento da sua área de informática, "amplamente facilitada pelo ritmo acelerado do crescimento da inflação naquela época" (DINIZ, 2004, p. 57). Os clientes dos bancos, a partir da década de 70 até metade da década de 80, fim da bolha inflacionária, demandavam rapidez e eficiência do sistema financeiro para compensar a inflação galopante. Do outro lado, os bancos lucravam com a inflação e, conseqüentemente, investiam pesadamente na automação bancária, para dar sustentação ao sistema financeiro. Este benefício não ficou restrito à seara técnica, a organização e a sociedade se beneficiaram com os novos recursos e oportunidades que a tecnologia proporciona. Nos eventos mais recentes desta transformação surge o que foi denominado "Economia Digital", TAPSCOTT (1997) descreve este novo modelo, no qual a Internet, a rede pública, tem um papel fundamental na construção de novas formas de relacionamento, assim como de estrutura institucional:

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

DINIZ (2004), em seu editorial "Cinco décadas de automação" do setor bancário, ilustra uma linha temporal evolutiva do setor bancário brasileiro, demonstrado na figura 1.

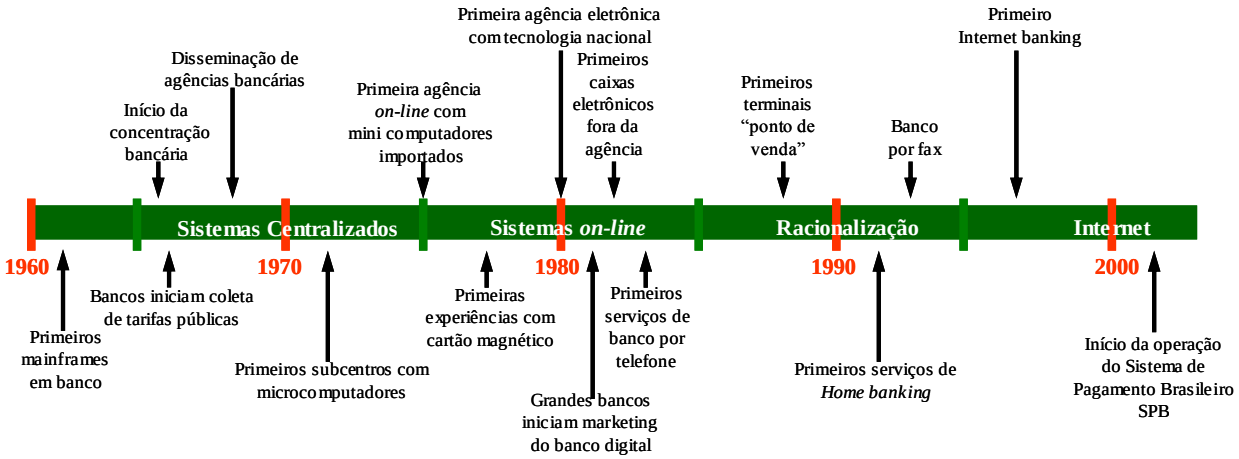


Figura 1: Fase da automação bancária no Brasil
(DINIZ, 2004, p. 58)

A transformação das organizações, ocasionada pelo surgimento da Internet, é demonstrada por TAPSCOTT (1997) por meio da figura 2, que aponta as mudanças sofridas pelas empresas conforme a evolução da TI. Num primeiro estágio, a tecnologia multimídia viabilizou o uso do computador por pessoas sem conhecimentos técnicos; em seguida, a evolução da conectividade possibilitou que a empresa se interligasse, internamente e externamente, e, num último estágio, permitiu que a empresa estivesse conectada em rede pública, com acesso aos seus clientes, concorrentes e fornecedores, gerando riqueza e desenvolvimento social.

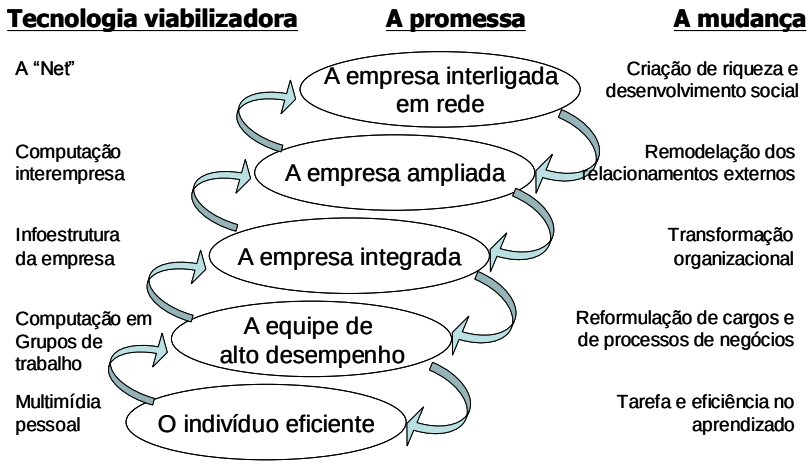


Figura 2: Transformação das empresas por meio da nova mídia (TAPSCOTT, 1997, p. 84)

A utilização de informações em rede implica, por si só, aumento da vulnerabilidade. A integração das organizações por meio da rede de computadores, na qual a sociedade se comunica, através da *web*, do protocolo TCP/IP e de e-mail, as expõem em suas fragilidades de segurança das informações e do patrimônio, vivendo, portanto, em um ambiente de risco (GARFINKEL; SPAFFORD, 1997). O Tribunal de Contas da União (2003), em seu guia de "Boas práticas em segurança da informação", bem como NAKAMURA e GEUS (2002) descrevem a influência da rede pública no quesito de segurança e seu peso nas organizações.

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

> *"O conjunto de protocolos TCP/IP e a Internet possibilitaram o avanço em direção aos ambientes cooperativos, ao tornar possíveis as conexões entre diferentes organizações, de modo mais simples e mais barato que as conexões dedicadas. Porém, essa interligação teve como conseqüência uma enorme implicação quanto à proteção dos valores de cada organização."*
> (NAKAMURA; GEUS, 2002, p. 19)

CAMERON (1997), a seguir, aumenta a amplitude da segurança, antes restrita à organização. Agora, é a organização e o meio.

> *"Security is no longer simply matter of ensuring that users within an organization use computing resources appropriately. It now extends to guarding against those skilled and savvy global users who consider it their hobby, obsession, and perhaps even mission to gain illegal access to systems and data."* [1]
> (CAMERON, 1997, p. 7)

A Internet proporciona aos clientes acesso ao seu banco, 24 horas por dia, 7 dias da semana, sem a necessidade dos funcionários do banco estarem na ativa. O processamento das vendas e transações pode ser feito em tempo real (*real-time*) ou em lotes (*batch*). Além disso, a inexistência de restrição geográfica possibilita às empresas trabalhar além da sua fronteira física (GHOSH, 1998). Com isso, os aplicativos de *home banking*, que eram disponibilizados em rede de comunicação privada, começaram a migrar para a Internet. Isto ocorreu, no Brasil, em meados de 1996 (GATES, 1999). GHOSH justifica que a ubiqüidade e as possibilidades de interação por meio de auto-atendimento levaram os bancos a criar um ambiente ainda mais competitivo. Um levantamento, realizado no mercado britânico, em 2002 (LAUDON; LAUDON, 2004), aponta que 5% do mercado bancário local era dominado por quatro bancos, que existiam, apenas, de forma virtual.

O *website* de um banco, geralmente, possui dois tipos de conteúdo: aberto, que publica informações institucionais, divulga produtos e serviços, além de comunicar campanhas promocionais e fechado, que possibilita o cliente acessar os seus dados pessoais e transacionar com o banco. D'ANDRÉA et al (2000) classificam o conteúdo aberto como institucional e o fechado como transacional.

[1] Segurança não é mais uma simples questão de garantir que os usuários dentro de uma organização usem os recursos computacionais de forma apropriada. Agora, isto se estende à guarda contra os usuários globais hábeis e experientes que consideram a quebra de segurança um passatempo, uma obsessão, e talvez até uma missão, ganhar acesso ilegal a sistemas e dados. (tradução nossa)

> *"Cabe destacar que o website de um banco é tradicionalmente formado por duas partes: sendo uma parte denominada **institucional**, de acesso público que possui informações gerais sobre o banco, seus produtos e serviços; e outra, denominada **transacional**, na qual está o Internet Banking".*
> (D'ANDRÉA et al, 2000, p. 17, nosso grifo)

O Brasil é um dos pioneiros no uso da Internet para realizar transações e distribuir serviços bancários. Segundo GATES (1999), o Bradesco, maior banco privado do Brasil, foi o quinto banco, no mundo, a lançar o Internet Banking para seus clientes, em 1996. GATES (1999) também indica que, em 1962, foi a primeira empresa, no Brasil, a usar computadores e, em 1982, o primeiro banco a oferecer caixas automáticos (ATM) e *home banking*. Com base na adoção de tecnologia do Bradesco é possível inferir o quanto a Tecnologia de Informação é importante para o crescimento e sucesso dos bancos, principalmente os de varejo, no Brasil. De acordo com LUNN (1999), os bancos são fundamentais para o crescimento dos mercados emergentes, sendo que a tecnologia é o "lubrificante" que viabiliza as engrenagens financeiras.

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

O *home banking*, versão de acesso ao banco por meio de linha dedicada (comunicação ponta a ponta entre a instituição financeira e o cliente) e *software* próprio, distribuído pela instituição, segundo SEYBOLD e MARSHAK (1998), não teve muita adesão dos clientes, como por exemplo, no caso do banco californiano, *Wells Fargo*. Todavia, quando o banco colocou à disposição, os serviços bancários na *web***,** no primeiro dia, houve a adesão de 1.500 clientes, contra 20 mil, em 7 anos (de 1989 a 1995), do home *banking*. Com a crescente adoção do Internet Banking pelo mercado, novas preocupações começaram a surgir, conforme a sua popularização.

Um fator importante, na adoção do canal, é a segurança, segundo a pesquisa "25 Melhores Serviços de Internet Banking", publicada em 2002, na revista *Business Standart* e

[2] Mercados emergentes representam a vasta maioria da população mundial e serão os mercados do próximo século. *Banking* é o lubrificante essencial para estas economias, primeiro, ajudando-as a fazer a transição inicial da agricultura de subsistência e, depois, ajudando suas empresas a negociar com o mundo; e a tecnologia é o lubrificante essencial de *banking*. (tradução nossa)

realizada pelo Centro de Excelência Bancária da Fundação Getúlio Vargas. Outro elemento importante, divulgado pela FEBRABAN (Federação Brasileira de Bancos), é que a segurança de dados é o que demandará mais investimentos pelo sistema financeiro, nos anos de 2004 em diante, sendo que, dos US$ 2 bilhões anuais investidos em atualização tecnológica, 80% do investimento está direta ou indiretamente vinculado à proteção das informações (GAZETA MERCANTIL, 02/06/2004).

O crescimento e proliferação do Internet Banking motivaram os bancos a se preocuparem com a segurança eletrônica. Segurança em Tecnologia de Informação baseia-se na tríade que assegura a preservação da integridade, confidencialidade e disponibilidade (KRUTZ; VINES, 2001). A Internet agregou a esta tríade os conceitos de privacidade, não-repúdio e autenticidade (CAMP, 2000). Estes seis componentes são trabalhados de forma a minimizar os riscos estratégicos, financeiros e operacionais, em busca da eficiência operacional com redução de custos, incremento da conquista de novos mercados, democratização da rede, e incremento nas possibilidades de relacionamento com o meio interno ou externo, devido à ubiqüidade da Internet.

Este cenário de preocupação, com relação à segurança do Internet Banking, incentivou a autora deste trabalho, a investigar como é a gestão de segurança deste canal eletrônico, nos bancos, no Brasil.

1.1. Justificativa do estudo

O setor financeiro brasileiro, particularmente os bancos de varejo, é altamente automatizado, segundo pesquisa realizada em junho de 2003, pela empresa de consultoria Accenture, publicada na revista Executivos Financeiros. A automação é fruto da reforma bancária, ocorrida no regime militar, e dos anos de inflação alta que o país viveu até o Plano Cruzado, primeiro de uma série de ações para combater a inflação. Conforme descrito por DINIZ (1994), a inflação, nos primeiros anos, tinha o objetivo funcional de financiar o crescimento da capacidade produtiva, à custa da extração da poupança dos trabalhadores, porém, após 1982, sua explosão foi uma aberração, que trouxe benefícios aos bancos.

O setor bancário brasileiro sofreu um fenômeno de concentração, ocorrido a partir de 1994 (TROSTER, 2004), impulsionado pela estabilização econômica; privatização de bancos; abertura aos bancos estrangeiros e saneamento dos bancos com problemas de solvência, propiciando o aumento dos bancos que buscavam economia de escala (tamanho do banco) e de escopo (produção conjunta de mais de um produto). Outro fator, precedente à concentração de bancos, e importante na história do setor financeiro, é a resolução 1.524, do Banco Central, que legalizou os bancos múltiplos, em 1988. No mercado bancário brasileiro, segundo o levantamento de 1989 a 2000, do Sistema Financeiro Nacional (SFN), realizado pelo Banco Central do Brasil (BACEN), o país tem os seguintes tipos de bancos, excluindo-se outros tipos de instituição financeira: Banco do Brasil; Caixa Econômica Federal; Banco Comercial; Banco de Desenvolvimento; Banco de Investimento e Banco Múltiplo, sendo que os dois primeiros são públicos e os demais podem ser controlados por capital nacional e/ou estrangeiro e podem ser privados ou públicos.

Os bancos, mercadologicamente, podem ser divididos em: de varejo, que tem como público-alvo a massa populacional bancarizável (Itaú e Bradesco); de atacado, que atende às grandes corporações (Itaú BBA); de nicho, que atende a um segmento específico da sociedade (*BankBoston*); regional, que atua em um determinado espaço geográfico (Banco do Nordeste e Nossa Caixa); globalizado, que possui uma rede internacional, efetivamente interligada (*Citibank*).

O banco de varejo, no Brasil, provavelmente se beneficia das inovações tecnológicas do comércio eletrônico, conforme KALAKOTA e FREI (1998) descrevem ocorrer no mercado norte americano, devido à sua atuação ampla e grande base de clientes.

> *"Banking as a business can be subdivided into five broad types – retail, domestic wholesale, international wholesale, investment, and trust. Of all these types, retail banking are probably the most affected by technological innovations brought about by electronic commerce."* [3]
> (KALAKOTA; FREI, 1998, p. 19)

RAMOS e COSTA afirmam: "as organizações buscam a hegemonia da tecnologia, oferecendo cada vez mais serviços acessíveis, de qualidade superior e de custo baixo". Portanto, conforme estes autores, a conseqüência disso é a evolução do auto-atendimento, que, no caso dos bancos, "enriquece a produtividade das tarefas dos escriturários em serviços e contribui para alcançar ganhos de escala pela padronização e técnicas de produção em massa" (RAMOS; COSTA, 2000, p. 139). Isto leva a crer que a forma de relacionamento entre o setor bancário e seus clientes tem migrado do atendimento pessoal para o auto-atendimento. O auto-atendimento ou auto-serviço, no mundo financeiro, é viabilizado, basicamente, através dos canais eletrônicos ou meios eletrônicos.

O BACEN, na Resolução 2.817, de 2001, considera como meios eletrônicos: a Internet, os terminais de auto-atendimento (ATM), o atendimento telefônico e outros meios de comunicação à distância, disponibilizados pela instituição para fins de relacionamento com seus clientes. Dados da FEBRABAN (Federação Brasileira de Bancos) demonstram que 75% das transações, do setor bancário, são realizadas por via eletrônica, e o auto-atendimento representa 32,3% das operações realizadas com o cliente, indicando um crescimento de 24,5% em 2003 sobre 2002. Os bancos estimulam o uso dos canais de auto-atendimento, como o Internet Banking, como estratégia de contenção de despesas, uma vez que a transação na Internet tem um custo estimado de US$ 0,01 e na agência este custo chega a US$ 1,07, conforme dados do Departamento de Comércio Americano de 1998, extraídos de DINIZ (2000 b) e representados na figura 3. Portanto, o meio transacional tem se alterado do físico e presencial para o digital e remoto, permitindo que a maior parte das transações e consultas

[3] Banco, como negócio, pode ser subdividido em cinco grandes tipos: varejo, atacado, atacado, investimento e trust. Entre todos os tipos, o banco de varejo é, provavelmente, o mais afetado pelas inovações tecnológicas, provenientes do comércio eletrônico. (tradução nossa)

possa ser feita da residência do cliente, do seu escritório ou de algum microcomputador conectado à Internet.

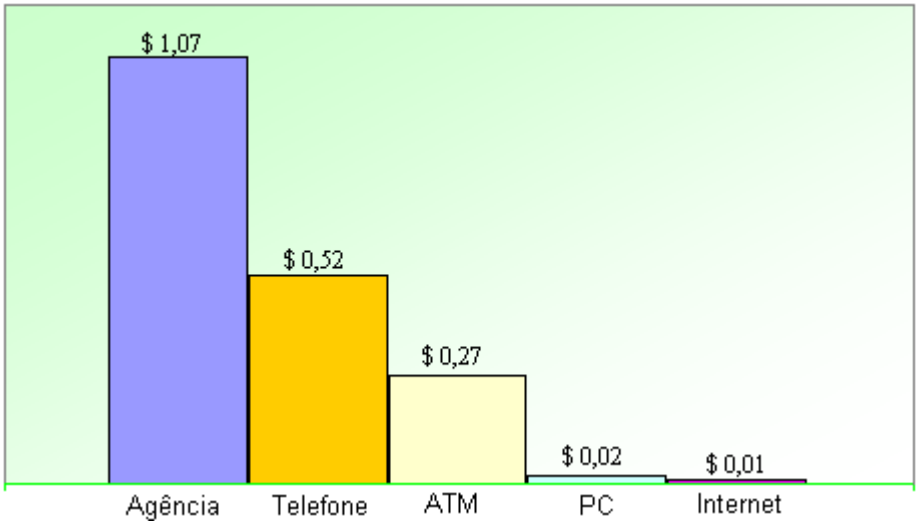


Figura 3: Custo médio por transação bancária
(DINIZ, 2000 b, p. 50)

Dados, publicados no *website* da FEBRABAN, indicam que o setor bancário pretende investir pelo menos R$ 11,5 bilhões na área de tecnologia, durante 2004, valor que representa 40% de tudo o que é investido em tecnologia no país e equivale a cerca de 4% das receitas brutas dos bancos. Outro dado importante é que, em 2002, os bancos brasileiros investiram R$3,5 bilhões em mecanismos de automação, enfatizando o processo de busca de rentabilidade e redução dos custos operacionais. ALBERTIN, em 1998, já apontava o setor bancário como um dos que mais investe em TI, devido à redução de custos e considerável vantagem competitiva que proporciona. MEIRELLES (2004), em sua 15ª pesquisa anual de administração de recursos de informática, mostra que, em 2003, o mercado brasileiro investiu, em média, 4,9% do seu faturamento líquido em informática, enquanto que o setor bancário investiu, em média, 10,4% do seu faturamento líquido.

O Internet Banking é o canal de transação e de relacionamento que mais cresce, desde 2000. Segundo dados da FEBRABAN, entre 2001 e 2002, o número de operações realizadas, via Internet, aumentou 177,9%. No período de 2002 a 2003, o número de clientes com Internet Banking também cresceu de 9,2 milhões para 9,7 milhões. Considerando que em 2002 o mercado possuía 66,7 milhões de contas correntes, distribuídas entre os bancos, e que

cada cliente podia ter mais de uma conta corrente, DINIZ (2004) estima que um quarto dos clientes bancários do país utilize o Internet Banking como meio de se relacionar com o seu banco.

A Internet, segundo McKNIGHT e BAILEY (1999), faz "parte integral" das nossas vidas, sendo que, a infra-estrutura de sua segurança é a questão mais premente a ser tratada.

> *"The Internet may not only have an impact on society, but may also become an integral part of our lives if it guides our cars, provides our entertainment, and allows us to pay our bills. Consequently, there are many questions and thorny problems – all of which interrelate in a delicate web of mutual influence. Since there are so many questions, the most important issue is which questions need to be answered now rather than later? We believe that the security infrastructure that will form the basis of new digital marketplace must be addressed now."* [4]
> (McKNIGHT; BAILEY, 1999, p. 450)

A Internet permite que os serviços e transações sejam realizados pelos clientes de forma remota, de qualquer lugar e a qualquer horário, respeitando os horários limites de cada operação e o limite financeiro estipulado por cada instituição financeira. Estas características da Internet abrem oportunidades de negócio para os bancos e brechas para as fraudes e roubos. A proteção das informações e dos dados é de vital importância para a sobrevivência das organizações, pois uma falha de segurança pode gerar perda de mercado, de negócio, de imagem e, conseqüentemente, perda financeira (NAKAMURA; GEUS, 2002).

DINIZ (2000 b) aponta, entre os diversos desafios envolvidos no Internet Banking, a segurança como uma das principais preocupações manifestadas pelos bancos e seus clientes. O autor justifica esta apreensão na crença dominante sobre a eficiência dos *hackers*. Porém, esta preocupação não deve restringir a oferta deste meio eletrônico, citando HUMPHREYS (1988), que afirma que a Internet oferece tanto risco como oportunidade:

[4] A Internet pode não só ter um impacto na sociedade, mas também se tornar parte integral de nossas vidas se puder orientar nossos carros, prover nosso entretenimento e permitir pagar nossas contas. Conseqüentemente, há muitas perguntas e problemas espinhosos – todos eles interligados em uma delicada teia de influência mútua. Já que há tantas perguntas, a questão mais importante é quais perguntas necessitam ser respondidas agora e não depois? Nós acreditamos que a infra-estrutura de segurança, que formará a base do mercado digital, deve ser endereçada agora. (tradução nossa)

> *"Financial institutions today have reason to worry that if they do not offer on-line banking services, affluent customers will be stolen away by software companies, on-line access services, brokerages, or global entertainment companies. The current situation presents both opportunities and risks."* [5]
> (HUMPHREYS, 1998, p. 73)

ALBERTIN (2004), em sua 6ª pesquisa anual sobre o comércio eletrônico no mercado brasileiro de 2003, levantou, em sua avaliação, que os aspectos mais importantes no comércio eletrônico são a segurança e a privacidade para as empresas, de diversos setores, que responderam a um questionário (figura 4). A segurança e a privacidade é reflexo da oferta de transações por meio da Internet.

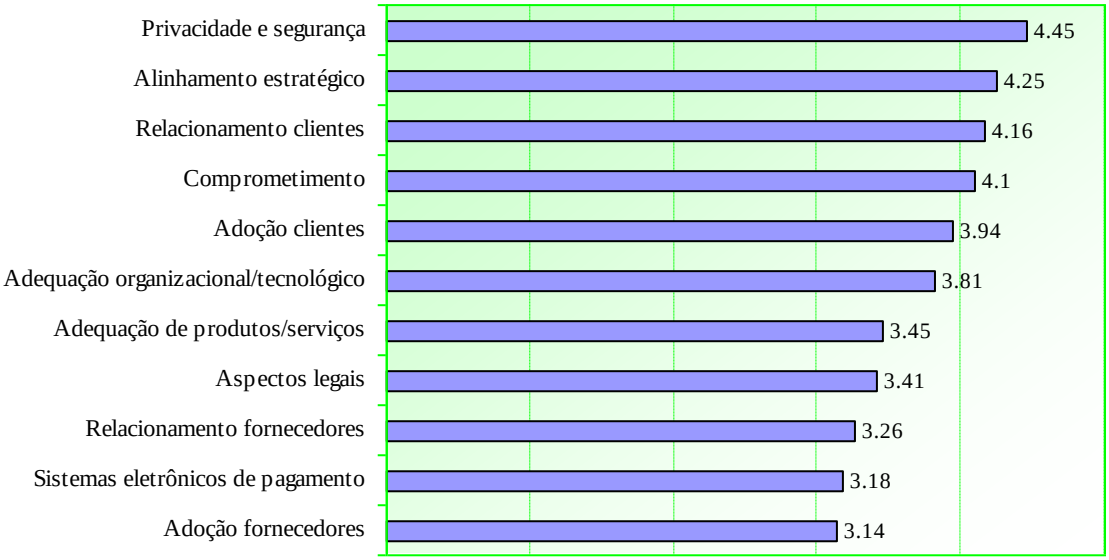


Figura 4: Avaliação de aspectos de comércio eletrônico (ALBERTIN, 2004, p. 13)

Os números das pesquisas, sobre o mercado brasileiro e americano, realizadas, anualmente, pela empresa em consultoria de segurança Módulo Security, no Brasil e pela *Computer Security Institute* (CSI), juntamente com a *Federal Bureau of Investigation* (FBI), nos Estados Unidos, apontam que a preocupação com a segurança na Internet tem aumentado, ano após ano, impulsionada pelo crescente número de fraudes e perdas financeiras. A Módulo Security está em sua 9ª edição, e a CSI/FBI está em sua 8ª edição, publicadas em 2003 e 2004, respectivamente.

[5] Hoje, as instituições financeiras têm razões para se preocuparem caso não ofereçam bancários on-line, os clientes mais afluentes serão roubados pelas empresas de software, serviços de acesso on-line, corretoras ou empresas de entretenimento global. A atual situação oferece oportunidades e riscos. (tradução nossa)

O BACEN, na resolução 2.817, de 2001, institucionalizou que os bancos devem garantir o "sigilo e a segurança dos meios eletrônicos" disponibilizados por eles. A seguir, trecho da resolução que explicita esta obrigatoriedade:

> *"As instituições financeiras (...) que tornarem disponíveis meios eletrônicos para fins de relacionamento com seus clientes devem assumir, por sua diretoria, nos termos da Resolução n. 2.554, de 24 de setembro de 1998, a responsabilidade pelos sistemas de controles que garantam o sigilo e a segurança dos meios eletrônicos tornados disponíveis, bem como o adequado monitoramento das informações relativas à movimentação das contas de depósitos de que trata esta Resolução, devendo mencionados sistemas estar devidamente avaliados e certificados mediante auditoria promovida por entidade de reconhecida capacidade técnica."*
> (BACEN, RESOLUÇÃO 2.817, 2001a)

Os bancos no Brasil, isoladamente, não divulgam o valor da perda financeira, ocasionada por fraudes na Internet, com o intuito de resguardar a própria imagem. Porém, dado divulgado em 2004, pela Revista Dinheiro, indica que os bancos, no Brasil, sofrem um desfalque de R$ 56 milhões, por ano, em golpes e fraudes ocorridos na Internet, com seus clientes. O Jornal Valor Econômico divulgou, em 2004, que as perdas na Internet, causadas por fraudadores, dobrará, a cada seis meses, e que este valor, em 2003, tenha atingido R$ 100 milhões. Apesar de não existir dado público e oficial, os bancos sinalizam uma preocupação crescente, com base no investimento alto que vêm realizando, para garantir a segurança neste meio, e na dinâmica de manobras para mitigar as brechas de segurança de seus sistemas. A Internet é um meio que minimiza os custos operacionais, abre caminho para novas oportunidades e o seu preço, para tanto, é a vulnerabilidade que o canal proporciona, por ser um meio e uma tecnologia pública.

O benefício óbvio que os bancos esperam, no curto prazo, com a adoção da Internet, é a redução de custos das operações e transações realizadas no canal eletrônico. Esta economia baseia-se na automação dos processos, conforme descrito por DINIZ (2000 a), no artigo publicado na RAC (Revista de Administração Contemporânea**)**. O estudo de caso, elaborado por GRISCI (2003), sobre uma grande instituição bancária brasileira, demonstra que ela, além de investir em tecnologia, com o objetivo de "fidelizar" seus clientes, reduzir custos e aumentar receitas, visa, também, "redirecionar o cliente da rede física para a rede virtual". KALAKOTA e FREI (1998), citados a seguir, vão um pouco à frente, ao afirmarem que as instituições financeiras devem mover-se de uma gestão centrada em custos para uma centrada em lucros, viabilizada por se tornar uma instituição de custo baixo.

> *"One of the major issues driving changes in the way financial institutions view technology is the movement from a cost to profit centered perspective. With significant competitive pressures on profit margins, one of the few ways to make a profit on a product or service is to become low cost provider."* [6]
> (KALAKOTA; FREI, 1998, p. 31)

Os bancos adotaram a Internet como um canal eletrônico por diversos motivos: redução de custo operacional e processual; vantagem competitiva, incrementando a marca (para os inovadores na adoção da Internet) ou alinhando com as ofertas dos concorrentes (para a maioria inicial e tardia); migração de serviços da rede física para a virtual. O meio eletrônico propicia diversas oportunidades, em contrapartida, há riscos que devem ser gerenciados, principalmente, os relacionados com a segurança. Portanto, este estudo se justifica pela importância do tema, gestão de segurança do Internet Banking, com a finalidade de melhor compreender como os bancos endereçam este assunto.

[6] Uma das principais questões que está impulsionando mudanças na forma como as instituições financeiras enxergam a tecnologia é o movimento da perspectiva centrada no custo voltada para obtenção de lucro. Com pressões competitivas significativas sobre as margens de lucro, uma das poucas formas de se lucrar com produtos ou serviços é tornar-se um provedor de baixo custo. (tradução nossa)

1.2. Objetivo

Os bancos, em sua maioria esmagadora, oferecem o canal eletrônico Internet Banking para os seus clientes. Um ponto importante para se disponibilizar o canal é a segurança, tanto da parte da instituição financeira, quanto do cliente. Desta forma, este trabalho visa estudar casos de gestão de segurança em bancos, no Brasil, com visão integrada de negócio e tecnologia. Serão levantadas informações relacionadas com a gestão de segurança do Internet Banking, como: modelos, padrões, práticas e documentos existentes no mercado, e, na maioria das vezes, já utilizadas pelas instituições financeiras.

O objetivo principal deste estudo é criar um material de referência acadêmica sobre a gestão de segurança em Internet Banking, que possa ser consultado pela comunidade acadêmica e pelos profissionais de organizações, sem que necessariamente as pessoas tenham formação técnica específica. A contribuição em administração de empresas que este trabalho pode oferecer é: subsidiar o administrador do canal Internet Banking com uma visão gerencial, podendo este administrador ter conhecimento, prévio ou não, de tecnologia.

1.2.1. Delimitação do Objeto

O campo de estudo deste trabalho está limitado ao setor bancário, mais especificamente, ao estudo de segurança em Internet Banking no Brasil. Todas as necessidades de segurança apresentadas são relativas ao cenário sócio-econômico brasileiro.

1.3. Classificação do Estudo

BURREL e MORGAN (1979) acreditam que as teorias organizacionais baseiem-se na filosofia da ciência e na teoria da sociedade. Os autores afirmam que a sociedade e as organizações são compreendidas por meio de diversas visões filtradas por "lentes", também tratadas como paradigmas. O paradigma é o entendimento compartilhado, é a "lente" por meio da qual as realidades organizacionais e sociais podem ser enxergadas e interpretadas. O modelo, desenvolvido pelos autores, possui quatro paradigmas, balizados por quatro dimensões: objetividade e subjetividade, elementos que norteiam a forma pela qual os fenômenos organizacionais e sociais são pesquisados (filosofia da ciência); regulação e mudança radical, componentes que permeiam a natureza do equilíbrio das relações sociais (teoria da sociedade). A figura 5 ilustra o modelo desenvolvido por BURREL e MORGAN.

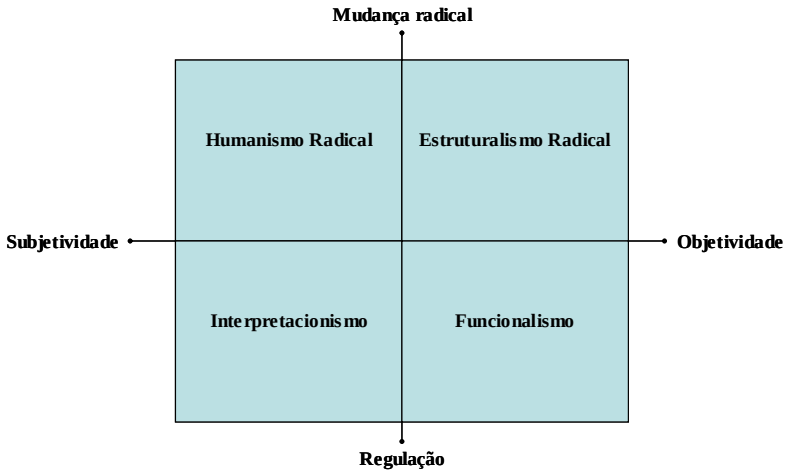


Figura 5: Modelo de análise das teorias organizacionais (BURREL e MORGAN, 1979, p. 54)

No levantamento, realizado por DHILLON e BACKHOUSE (2001), descobriu-se os seguintes trabalhos e pesquisas, existentes sobre Sistema de Informação (SI) e métodos de segurança (tabela 1):

Tabela 1: Pesquisas de SI e Segurança

Paradigma	Teoria usada	Pesquisas e trabalhos de Sistema de Informação	Pesquisas e trabalhos de Segurança
Funcionalismo	Sistemas e contingência	SI *success* (IVES et al, 1983); *Requirement identification* (BAILEY & PEARSON, 1983; DAVIS & OLSON, 1984; BAROUDI et al, 1986); *Systems development* (DEMARCO, 1978).	*Traditional risk analysis approaches* (COURTNEY, 1977; PARKER, 1981; FISHER, 1984); *Security evaluation methods* (BELL & LA PADULA, 1976; VAN DER VEEN et al, 1994).
Interpretacionista	Estruturalismo, Fenomenologia, Hermenêutica, Semiótica, Contextualismo	*Information systems strategy, system design and implementation* (BOLAND, 1985; WALSHAM, 1993); *Use of signs in system specification* (LIEBENAU & BACKHOUSE, 1990)	*Risk analysis and the communicative content* (BASKERVILLE, 1991); *Speech act theory and security development* (DOBSON, 1991); *Pragmatic consideration and security* (BACKHOUSE & DHILLON, 1996).
Humanismo Radical	Crítica	*Theory of information systems and system specification* (LYYTINEN & KLEIN, 1985).	*Strategic options for security as described by* ANGELL (1994); *Critical theoretic considerations in risk analysis* (WEBLER et al, 1992).
Estruturalismo Radical	Conflito	*Contractual view of information systems* (CIBORRA, 1987)	Não foi encontrado, exceto alguns traços nos trabalhos de LANE (1985).

(Fonte: DHILLON e BACKHOUSE, 2001, p. 146)

A maior parte dos trabalhos sobre segurança em TI é baseada na teoria Funcionalista, conforme DHILLON e BACKHOUSE (2001), que classificaram o uso deste paradigma em três tipos: *checklist*, análise de risco e avaliação.

O *checklist* responde à questão: "o que pode ser feito, em vez de o que é preciso ser feito" (DHILLON e BACKHOUSE 2001, p. 133, nossa tradução), concentrando-se nos meios e não no fim. Esta visão foca a atenção nos eventos observáveis, porém não considera a natureza humana dos eventos.

A análise de risco é feita mediante a análise das ameaças e vulnerabilidade, para justificar os custos e investimentos. A finalidade é "prever os benefícios financeiros *vis-à-vis* aos investimentos iniciais" (DHILLON e BACKHOUSE 2001, p. 134, nossa tradução).

A avaliação é uma medida que previne a divulgação não autorizada de informação, por meio de controle de acesso. “O guia de padrão de segurança, publicado pela *British Department of Trade and Industry*, adotado por algumas empresas, inclusive bancos, é uma referência deste tipo de abordagem” (DHILLON e BACKHOUSE 2001, p. 136, nossa tradução).

A teoria Interpretativa, conforme DHILLON e BACKHOUSE (2001), tem aparecido em trabalhos sobre análise de risco, com enfoque na explicação das regras, ações, objetivos e políticas. Este trabalho, na parte que discorre sobre a camada humana, não focará a análise cultural e comportamental, sugerida pela visão Interpretacionista.

Este estudo foi realizado com enfoque na abordagem Funcionalista. Este paradigma se fundamenta na filosofia Objetivista da ciência e na crença Regulacionista nas relações sociais.

2. Referencial Teórico

2.1. O advento da Internet, do comércio eletrônico e a crescente preocupação com a segurança

A Internet, segundo CASTELLS (2004), surgiu a partir da interação entre a ciência, a investigação universitária fundamental e os programas de pesquisa militar norte-americanos. O autor desvenda também o mito de que a Internet surgiu no meio militar, na realidade, ela "nunca" foi utilizada pelos militares, houve apenas um financiamento militar para os estudos e desenvolvimento do meio. A base da Internet é um protocolo de comunicação, conhecido como TCP/IP (*Transfer Control Protocol/Internet Protocol*), que faz parte de uma arquitetura de informática aberta, criada entre 1973 a 1978. A ARPANET (*Advanced Research Projects Agency Network*), considerada como a origem da Internet, foi lançada em 1969, utilizando o NPC (*Network Control Protocol*).

O comércio eletrônico, conforme ALBERTIN (1999, p. 15), "é a realização de toda a cadeia de valor dos processos de negócio num ambiente eletrônico, por meio da aplicação intensa das tecnologias de comunicação e de informação, atendendo aos objetivos de negócio."

A tecnologia viabilizou a construção de um espaço digital, inicialmente, restrito a um grupo de desenvolvimento. Em 1994, a Internet toma forma comercial, com o advento dos navegadores (*browser*) e da *world wide web* (www). Surge, então, a economia digital, o comércio eletrônico e as "empresas ponto com" (LIMA, 2000). O crescimento da Internet, desde então, é explicado por McKNIGHT e BAILEY (1999), no trecho a seguir:

> *"The growth and benefits of the Internet are explained by a combination of economic, technical, and policy factors: positive economic network externalities such as the bandwagon effect, economies of distribution and scale, and statistical sharing."* [7]
> (McKNIGHT; BAILEY, 1999, p. 445)

[7] O crescimento e os benefícios da Internet são explicados por uma combinação de fatores econômicos, técnicos e políticos: rede de economia positiva de oferta e demanda como o "efeito moda", economia de distribuição e escala e divisão estatística. (tradução nossa)

O comércio eletrônico possui a seguinte estrutura genérica, ilustrada na figura 6, desenvolvida por KALAKOTA e WHINSTON (1996), extraída de ALBERTIN (1999):

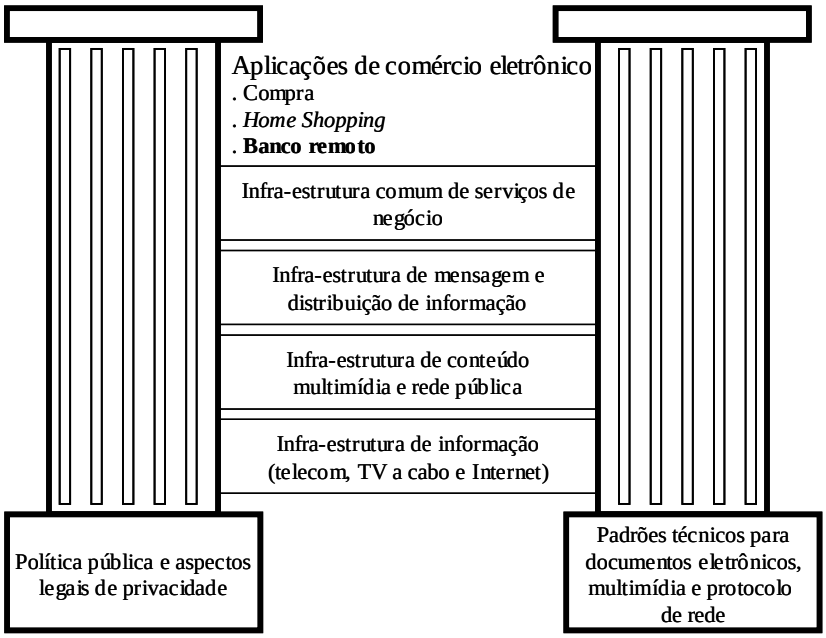


Figura 6: Estrutura genérica para comércio eletrônico
(ALBERTIN, 1999, p. 21, nosso grifo)

O ciclo de adoção de ROGERS (1983), figura 7, extraído de ALBERTIN (1999), demonstra os estágios em que uma novidade pode ser aceita por um determinado grupo, comunidade ou sociedade, por meio de uma difusão da inovação, cuja aceitação é disseminada pela comunicação. A Internet, como uma nova tecnologia e um novo meio para os bancos, pode ser inserida dentro deste ciclo, para análise. Nele, o "inovador" é o pioneiro, que adere, de imediato, à nova tecnologia, e é natural que seja uma quantidade pequena de adeptos; o "mais cedo" e a "maioria inicial" são os indivíduos que aderem após o "inovador" testar e aprovar a nova tecnologia; as duas outras categorias, "maioria tardia" e "retardatário", são das pessoas que preferem esperar uma tecnologia amadurecer, para depois adotá-la.

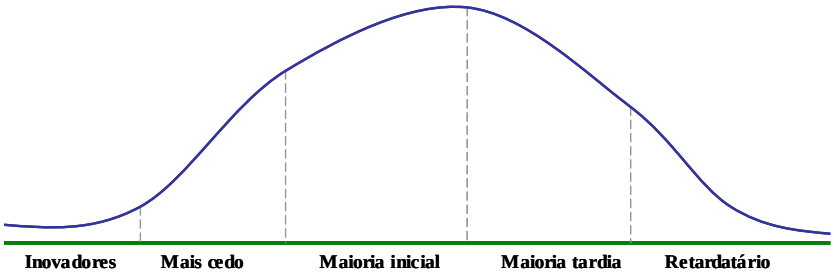


Figura 7: Ciclo de vida de adoção
(ALBERTIN, 1999, p. 136)

DINIZ, PORTO e ANGULO (2001) apontaram cinco características de análise da rapidez, na adoção do comércio eletrônico: vantagem relativa, em relação à tecnologia que está sendo substituída; compatibilidade com as necessidades, valores, comportamento e estilo de vida dos consumidores, em um mercado massificado; complexidade, que dificulta a compreensão e aceitação do novo produto e serviço; experimentação da nova tecnologia; visibilidade ou comunicabilidade dos casos de sucesso, que incentivam os novos usuários a aderirem ao comércio eletrônico. ALVES, LAMOUNIER e JABUR (2000) destacam que as empresas que conseguiram ser líderes de mercado na Internet foram também "inovadoras" na adoção da tecnologia. O Internet Banking, portanto, para os bancos, é um canal importante para a sua estratégia de liderança.

Os bancos têm a informação como insumo e produto, e seus clientes, no uso do auto-atendimento, são "co-produtores" (RAMOS; COSTA, 2000, p. 139), uma vez que precisam interagir digitando os seus dados, as solicitações de transações e consultas. BANKS (2001) descreve a natureza digital dos produtos financeiros:

> *"Financial products and services are a logical commercial business for the Internet – they are relatively homogenous, rely heavily on information and data, and require frequent customer participation; they are also easy to deliver – fulfillment of customer requirements is very straightforward, particularly when compared to consumer goods or institutional commodities which depend heavily on timely inventory management, scheduling and shipping."* [8]
> (BANKS, 2001, p. 15)

A febre das empresas ponto com teve o seu ápice no dia 10 de março de 2000, quando o índice da NASDAQ, bolsa de ações de empresas ponto com e de empresas de tecnologia, chegou ao seu maior valor já registrado, 5.048 pontos, gerando a bolha econômica da nova economia digital (BETING, 2000 e MANZONI, 2004). A bolha, no segundo semestre de 2000, entretanto, começou a murchar, chegando, em novembro, do mesmo ano, quase à metade dos pontos atingidos em março. O fim da empolgação e dos ganhos milionários incitou preocupações, encontradas no mundo físico e até então não tratadas, com ênfase, pelas empresas virtuais, existentes na Internet, a virem à tona. Uma das maiores preocupações era a

[8] Os produtos e serviços financeiros são um negócio lógico para a Internet – são, relativamente, homogêneos, baseiam-se, pesadamente, em informação e dados, e requerem a participação freqüente do cliente; são também fáceis de entregar – satisfazer as exigências do cliente é muito simples, particularmente, quando comparado aos bens e mercadorias de consumo, que dependem, pesadamente, administração de inventário oportuna, programação e remessa. (tradução nossa)

quebra da privacidade e a fragilidade da segurança das informações distribuídas em rede pública.

O avanço tecnológico e a desburocratização na área de telecomunicação que ocorreu após a privatização do setor, no Brasil, possibilitaram o aumento da base de usuários domésticos, com conexão simples ou banda larga. Segundo dados do Ibope eRatings, publicados no Jornal do Comércio, estima-se que em junho de 2003 existisse 1,9 milhão de usuários domésticos, de banda larga, no Brasil. Este número tende a avançar com o barateamento do acesso e o aumento do parque de computadores domésticos. Sendo que, o total de pessoas que tem acesso a Internet é de 26,7 milhões, 15% da população, no início de 2003, segundo dados do Comitê de Democratização da Informática (CDI), publicados na Gazeta Mercantil (27/04/2004). A banda larga possibilita conexão na Internet em tempo integral, por não utilizar uma linha telefônica convencional, e isto faz com que o computador que não tiver programas anti-*hackers* ou antivírus fique vulnerável, além da alta velocidade propiciar uma invasão rápida, a ponto do usuário não perceber.

A democratização dos computadores e um acesso de qualidade, como o da banda larga, possibilitaram a disseminação dos recursos fornecidos pela Internet (RUSSEL; GANGEMI, 1991). Este cenário propiciou, ao mesmo tempo, o aumento de fraudes, roubos e desvios de informações e de capital. O cliente do banco possui acesso aos serviços bancários pela Internet, em contrapartida, o criminoso possui acesso a programas de roubo de senhas e à informação de como proceder para quebrar a privacidade dos sistemas bancários. Desta química, surgem os *hackers*, que até criam comunidades para trocar dados, na própria Internet, de como roubar senhas e informações sigilosas. Este ambiente cibernético faz com que "segurança é uma questão que deve ser enfrentada diretamente. As empresas devem estar cientes da existência dos riscos, reconhecê-los, e desenvolver uma estratégia de segurança em resposta." (CAMERON, 1997, p. 8, tradução nossa). A tecnologia traz diversos benefícios, porém, os riscos de fraudes e crimes continuam existindo e, pior, com maior rapidez, conforme análise de GLAESSNER, KELLERMANN e McNEVIN (2002):

> *"With the benefits of new technology also come new risks. Technology facilitates more efficient and quicker ways to commit old crimes such fraud and theft. Disturbingly, as the technology becomes more complex, a perpetrador needs fewer skills to commit these crimes."* [9]
> (GLAESSNER; KELLERMANN; McNEVIN, 2002, p. 8)

Outro aspecto da segurança é que ela não é mensurável, conforme descrito por BRINEY (2004):

> *"As with quality, the benefit of security is difficult to quantify because the measure of its success is the absence of failure. As with quality, security doesn't become important until the company recognizes that it's more effective to address problems before rather than after an incident."* [10]
> (BRINEY, 2004)

2.1.1. Segurança eletrônica e suas implicações no mercado bancário

Os avanços da telecomunicação e da informática abriram caminho para o surgimento da Internet, mudando, radicalmente, a forma de uso da tecnologia (RUSSEL; GANGEMI, 1991). A Internet é uma rede de computadores de mão dupla: assim como o usuário tem acesso a milhões de informações, publicadas na rede, os criminosos e indivíduos de má índole também têm acesso aos servidores, onde as informações estão hospedadas. Somado a isso, a *web* é de fácil uso, porém, a sua tecnologia é complexa e cheia de falhas de segurança (GARFINKEL; SPAFFORD, 1997).

BRANDS (2000) indica que a sociedade, baseada em documentação física com fotos e assinaturas manuscritas, está sofrendo a transição para uma comunidade cibernética, e esta nova forma de se comunicar e transacionar só será possível se os mecanismos que suportam esta nova realidade estiverem seguras. ROSE (1999) acrescenta, no trecho abaixo, que os benefícios em agir superam os riscos de segurança:

[9] Com os benefícios da nova tecnologia também vêm novos riscos. A tecnologia facilita o surgimento de meios mais rápidos e eficientes de se cometer crimes antigos, como fraude e roubo. De modo perturbador, quanto mais a tecnologia se torna complexa, o transgressor necessita de menos habilidades para cometer estes crimes. (tradução nossa)

[10] Assim como a qualidade, o benefício da segurança é difícil de quantificar porque a mensuração do seu sucesso é a ausência do fracasso. Assim como a qualidade, a segurança não se torna importante até que a companhia reconheça que é mais efetivo administrar problemas antes do que depois de um incidente. (tradução nossa)

> *"An Internet presence must not be ignored by the financial services industry. While the Internet is an intimidating concept, it offers the opportunity to compete with others financial services providers on equal footing. Benefits of acting now outweigh the concerns of security risk."* [11]
> (ROSE, 1999, p. 32–7)

Ao se trabalhar em um sistema multi-usuário, como a Internet, no qual os computadores não são estanques, em si mesmos, e sim presentes em uma rede pública ou privada, há a preocupação com segurança. No mínimo, usam-se controles de acesso para proteger as informações (RUSSEL; GANGEMI, 1991).

O primeiro Internet Banking surgiu em Atlanta, Estados Unidos, no dia 18 de outubro de 1995. O banco, que só existia na Internet, chamava-se *Security First Network Bank*, SFNB (HUMPHREYS, 1998). No Brasil, o primeiro Internet Banking surgiu em 1996 (GATES, 1999). Desde o seu surgimento, até o início de 2003, o número de usuários cresceu, a ponto dos bancos no Brasil terem, em média, 23% de seus clientes usando Internet Banking, enquanto apenas 15% da população tem acesso a esta tecnologia, conforme levantamento realizado pelo banco Real ABN Amro Bank e a consultoria McKinsey, publicado na Gazeta Mercantil (01/04/2003). Esta taxa de uso de Internet Banking se equipara à dos bancos americanos, além de ser cinco pontos percentuais acima da média dos bancos europeus. Entretanto, há bancos, no Brasil, que extrapolam esse índice, como o BankBoston, com 42%, o Real ABN AMro Bank, com 28% e o Citibank, com 35% de usuários. Em 2004, a maioria dos bancos ultrapassava a marca dos 25% de clientes usando o Internet Banking.

ROSE (1999) reforça a análise de que a segurança é um fator importante, porém, pode ser contornado, a ponto dos bancos não postergarem a sua implantação:

> *"Many industry analysts believe that Internet security concerns are greatly overrated. While security issues must be taken seriously and safety measures must be investigated and implemented, financial institutions should not postpone Internet development plans due to these fears. Secure account access can be provided for customers."* [12]
> (ROSE, 1999, p. 32–7)

[11] Uma presença na Internet não deve ser ignorada pela indústria de serviços financeiros. Ao mesmo tempo em que a Internet é um conceito intimidador, ela oferece a oportunidade de competir com outras instituições financeiras em pé de igualdade. Os benefícios em agir, agora, superam as preocupações com os riscos de segurança. (tradução nossa)

[12] Muitos analistas da indústria financeira acreditam que as preocupações sobre a segurança na Internet são excessivamente exageradas. Embora o assunto segurança deva ser tratado seriamente e medidas de segurança devam ser investigadas e implementadas, as instituições financeiras não devem postergar os planos de desenvolvimento na Internet devido a estes medos. Acesso seguro à conta pode ser oferecido para os clientes. (tradução nossa)

A utilização da Internet, como um meio para se relacionar e transacionar, foi impulsionada pela redução de custos que ela teoricamente gera, em contraste com o custo da rede física de agências, ATM ou a manutenção de redes privadas ou conexões dedicadas (KOSIUR, 1997). A partir do momento em que os bancos iniciam o relacionamento por meio da Internet, se expõem a uma situação de risco, controlável, de segurança para os seus sistemas transacionais. Com isso, a demanda por uma gestão de segurança mais complexa, que englobe mudanças organizacionais, tecnológicas, operacionais e mercadológicas, tornou-se necessária, para usufruir o benefício da Internet, sem denegrir o ativo do banco ou do cliente (D'ANDRÉA et al, 2000).

2.2. Gestão de Risco

2.2.1. O que é o risco

Risco é um conceito baseado na probabilidade de ocorrência de algum sinistro, e segurança, no sentido oposto, ocorre quando se acredita que há baixa probabilidade de risco, conforme SCHNEIER (2001). FERREIRA (1986) descreve risco como a situação em que existe certa possibilidade de perdas ou ganhos previstos; GITMAN (1997) define risco como sendo a probabilidade de que o resultado realizado seja distinto daquele esperado; e VAUGHAN (1997) denomina risco a condição na qual há um desvio do resultado esperado. O fator incerteza é a característica predominante do risco.

Independente da definição, é possível se notar que o conceito de incerteza, ganho ou perda, está explícita ou implicitamente presente, de maneira que, quando houver o risco, são possíveis dois resultados: certeza de ocorrência ou não. CAMP (2000) classifica em três, as fontes básicas de risco: falha de segurança, mau uso de dados e falha na confiabilidade.

Segundo BREI e ROSSI (2002), no relacionamento cliente e empresa, quase sempre, há uma assimetria presente, dado que a companhia tem poder econômico mais forte na relação. Um dos pontos-chave para diminuir este efeito assimétrico, em trocas relacionais de serviços, é obter a confiança do consumidor. ROUSSEAU et al (1998, p. 395) definem: “confiança é um estado psicológico que compreende a intenção de aceitar uma vulnerabilidade baseada em expectativas positivas das intenções ou comportamentos de outro”. “Uma pessoa demonstra confiança quando ela depende de outra pessoa, arrisca algo de valor no relacionamento e busca atingir um determinado objetivo” (HERNANDEZ, 2002 p. 2). A confiança pode ser selada com palavra, promessa ou declaração escrita. O risco de segurança em Internet Banking existe, todavia, pode ser mitigada pela confiança que o cliente tem no banco e em suas políticas e normas.

O risco, segundo HEALY e WALSH (1979), é composto por dois elementos: a vulnerabilidade, que se traduz pela probabilidade de ocorrência e a criticidade, que se baseia no grau de severidade do impacto desta ocorrência. A probabilidade de ocorrência depende de diversos fatores: físicos e naturais, sócios-políticos, histórico de perdas e criminais. A

severidade do impacto é baseada em custos de reposição permanente e de substituição, e de perda ou estrago do ativo ou do investimento. A vulnerabilidade possui quatro níveis: verdadeiramente certo, altamente provável, moderadamente provável e improvável; enquanto que os níveis de criticidade podem ser classificados como: fatal para a organização, muito grave, moderadamente grave e não grave ou negligenciável. À composição dos dois níveis, os autores designaram risco lógico.

Conforme GITMAN (1997), a administração financeira envolve um confronto (*trade-off*) entre o retorno e o risco, que determinam o preço da ação de uma empresa. Extrapolando este conceito para a gestão de risco em Internet, percebe-se que da mesma forma que o mercado financeiro trabalha com um *trade-off* para balancear o risco e o retorno, a gestão de segurança de Internet tem que balancear a segurança com os custos operacionais, a qualidade do serviço e o impacto mercadológico, bem como o custo de adoção da nova tecnologia e o custo para acompanhar as inovações (GLAESSNER; KELLERMANN; McNEVIN, 2002).

2.2.2. Tipos de riscos

MARSHALL (2002) classifica os riscos, em instituições financeiras, em três grupos:

1. Riscos estratégicos: são os riscos vinculados ao tipo de estratégia que a empresa adotará para atingir os seus objetivos. A estratégia é montada com base em um leque de opções táticas, direcionadas para se atingir diversas metas, que levarão a empresa a alcançar o objetivo financeiro e mercadológico. Os riscos estratégicos podem ser internos ou externos. Os internos são: o tipo de arquitetura tecnológica a ser adotada; os segmentos de mercado a serem atingidos como público-alvo; ou até o *time to market* de seus produtos e serviços. Os riscos estratégicos externos são: pressões do mercado, como a concorrência e a dinâmica dos avanços tecnológicos; falta de agilidade para se adaptar a ambientes instáveis.

2. Riscos financeiros: são os riscos associados às transações financeiras que uma empresa realiza. A precificação e a volatilidade cambial são exemplos deste tipo de risco. O risco financeiro também envolve a definição de limites financeiros e formas de transações.

3. Riscos operacionais: são os riscos ligados à integridade dos processos de negócio, bem como à condição de fornecedor de produtos e serviços, de forma consistente e oportuna. Estes riscos são subdivididos em: risco de conformidade; de processos; de tecnologia e processamento de informações; de recursos humanos; de retidão e ética.

WITTY (2002) classifica os riscos, na gestão de Tecnologia de Informação, em 5 grupos:

1. Risco financeiro: perda de receita, causada pela violação da confidencialidade, integridade, privacidade ou disponibilidade.

2. Risco estratégico: impacto no fluxo futuro de receita, através da perda de propriedade intelectual ou de clientes.

3. Risco de reputação: denegrir a confiança que o cliente e o mercado têm perante a empresa.

4. Risco operacional: impacto na entrega do negócio, devido à sabotagem, vírus de computador ou ataque de *denial of service* (negativa de serviço, quando um servidor – computador onde está o Internet Banking, por exemplo – sofre excesso de solicitações de informações de atacantes, deixando-o inoperante ou lento).

5. Risco legal, regulatório e *compliance*: penalidades financeiras, baseadas em contratos ou outros instrumentos legais, devido a falhas de segurança.

2.2.3. Gerenciamento de risco

O objetivo do gerenciamento de risco é mensurar as incertezas e o potencial, positivo ou negativo, dos eventos futuros, para implementar uma estratégia de custo e eficiência que possam maximizar os ganhos (GREENSTEIN; FEINMAN, 2000). Para BESSIS (1998), o objetivo primário da gestão de risco é mensurar os riscos para monitorá-los e controlá-los.

O gerenciamento de risco é um processo em que as organizações calculam, avaliam e decidem quais e em que nível de risco elas pretendem operar. A seguir, a explicação de CULP (2002) e BESSIS (1998):

> *"Risk management is the process by which organizations try to ensure that the risks to which they are exposed are the risks to which they think are and need to be exposed to operate their primary business."* [13]
> (CULP, 2002, p. 199)

> *"Risk management is both a set of tools and techniques and a process that is required to implement the strategy of a bank. It also includes all the management processes, and the organization design, required to implement efficiently the set of techniques and models which deal with risk measurement and control."* [14]
> (BESSIS, 1998, p. 23)

Este gerenciamento é um processo contínuo, com característica cíclica, conforme mostra a figura 2 (CULP, 2002). A Internet é uma rede pública, que utiliza tecnologia complexa, com diversas falhas ou *bugs*, conforme o jargão da área (GARFINKEL; SPAFFORD, 1997). Portanto, a constante avaliação dos processos, dos sistemas e da qualidade de recursos humanos é vital para que o banco mantenha o seu Internet Banking em um ambiente confiável e seguro.

O processo de gerenciamento, segundo CULP (2002), é dividido em cinco atividades (figura 8):

---

[13] Gerenciamento de risco é o processo pelo qual as organizações tentam assegurar que os riscos aos quais elas estão expostas são os que elas pensam que são e precisam se expor para operar seu negócio primário. (tradução nossa)

[14] O gerenciamento de risco é um conjunto de ferramentas e técnicas, bem como um processo requerido para executar a estratégia de um banco. Inclui também todos os processos de gerenciamento e desenho da organização, necessários para executar, eficientemente, o conjunto de técnicas e modelos que tratam da mensuração e do controle eficaz do risco. (tradução nossa)

1. Identificar os riscos e determinar as tolerâncias;
2. Medir os riscos;
3. Monitorar e reportar os riscos;
4. Controlar os riscos;
5. Revisar, auditar, refinar e realinhar.

Figura 8: Processo de gerenciamento de risco de CULP
(CULP, 2002, p. 200)

2.2.4. Gerenciamento de risco em bancos

No universo bancário, o risco financeiro é definido como: as incertezas que podem impactar negativamente o lucro da instituição. Este risco pode estar ligado à área de crédito, liquidez, mercado, câmbio e solvência. Outro tipo de risco que existe no setor bancário é o operacional, que cobre todas as funcionalidades de sistema de informações, relatórios e monitoramento interno, podendo gerar um grande impacto, a ponto de ser fatal para a instituição financeira, conforme BESSIS (1998).

O gerenciamento de risco operacional ocorre em dois níveis: técnico e organizacional. A configuração e a entrega dos produtos e serviços estão ligadas ao sistema de informação que, por sua vez, pertence ao nível técnico. Enquanto o monitoramento e gerenciamento do risco ocorrem no nível organizacional (BESSIS, 1998). Conforme descrito por BESSIS (1998, p. 23, tradução nossa), “o objetivo primário do gerenciamento de risco é mensurar riscos com o propósito de monitorá-los e controlá-los”.

O objetivo primário do gerenciamento de risco serve para as seguintes funções, segundo BESSIS (1998):

- ✓ Implementação da estratégia;
- ✓ Desenvolvimento de vantagens competitivas;
- ✓ Mensuração da adequação e da solvência de capital;
- ✓ Ajudar na tomada de decisão;
- ✓ Ajudar na definição de preço;
- ✓ Gerenciamento do portfólio de negócio.

A importância do gerenciamento de risco é explicada por BESSIS (1998):

> *"The importance of risk management stems from the fact that, without it, strategy implementation would be limited to commercial guidelines, with no view of their impacts on the risk reward trade-off of the bank."* [15]
> (BESSIS, 1998, p. 24)

O princípio básico da gestão de risco é a separação entre o papel do tomador de risco do papel do supervisor de risco. Os papéis desempenhados por ambos são antagônicos, pois o tomador de risco está comprometido em atingir as metas comerciais e o supervisor de risco está comprometido em minimizar os riscos, mesmo que isto signifique não fazer negócio (BESSIS, 1998). O equilíbrio entre estas duas forças contrárias é fundamental para que o banco possa desenvolver um sistema seguro de Internet Banking e que, ao mesmo tempo, atenda às suas necessidades comerciais e mercadológicas.

[15] A importância da gerência de risco baseia-se no fato de que, sem ela, a implementação da estratégia seria limitada a diretrizes da área comercial, sem nenhuma visão de seus impactos no *trade-off* da recompensa do risco do banco. (tradução nossa)

2.2.5. Gerenciamento de risco em Tecnologia de Informação

O processo de gerenciamento de risco, em Tecnologia de Informação, pode ser dividido em três grandes etapas, conforme NICOLETT et al (2002):

1. Monitoramento e descoberta: varredura do ambiente, em busca de eventos relevantes, gerando alertas, em casos de tentativas ou violação da segurança.

2. Relatório: acumular informações, ao longo do tempo, para prover histórico de acessos e transações, em diversos formatos de relatório.

3. Controle e automação: implementar alguns aspectos da política de segurança, em resposta aos eventos de violação iminente.

Para WITTY (2002), o gerenciamento de risco, para ser mais eficiente, deve estar presente em todo o ciclo de vida de um projeto de Tecnologia de Informação. Para que a segurança não se torne um aspecto marginal, ou um aspecto que só será detectado ao final do projeto, é importante que a gestão de risco esteja presente, nas oito etapas do ciclo de vida de um projeto de tecnologia:

Etapa 1 – Requisitos de negócio: define as especificações de segurança da informação, baseadas na análise dos riscos tecnológicos, com foco no negócio. Dá liga e aderência às especificações de negócio com as possibilidades de tecnologia, de forma segura.

Etapa 2 – Arquitetura do sistema: define os requisitos da arquitetura de aplicações e de infra-estrutura; administra a segurança (incluindo as regras e responsabilidades); define os acordos de nível de serviço e muda as estratégias e política de segurança, conforme a adoção de novas tecnologias.

Etapa 3 – Desenho do sistema: desenvolve a arquitetura de segurança da infra-estrutura e das aplicações; o plano de administração de segurança; o rascunho do acordo de nível de serviço e o plano de testes da segurança de informação.

Etapa 4 – Construção: constrói a arquitetura de segurança da infra-estrutura e das aplicações; o ambiente de administração de segurança; os procedimentos de testes e toda a documentação.

Etapa 5 – Testes: testa a arquitetura de segurança, baseado nas especificações técnicas e de negócio; desenvolve as informações e o treinamento sobre segurança e homologa o sistema com a área de negócios.

Etapa 6 – Implementação: implementa a arquitetura de segurança e o ambiente de administração de segurança da produção.

Etapa 7 – Pós-implementação: revisa, atualiza e finaliza a arquitetura de segurança; os acordos de nível de serviço e, eventualmente, muda a política de segurança.

Etapa 8 – Aposentadoria: assegura a remoção e destruição dos aplicativos de segurança e controle.

A Internet fez com que a fronteira entre a empresa e o mercado se expandisse, e, com isso, o gerenciamento de risco não se restringe mais ao ambiente empresarial, apenas. O gerenciamento de risco deve levar em consideração os *links* com as entidades externas, como a comunidade, os clientes, fornecedores e parceiros. Outro ponto importante são as métricas, utilizadas para que se possa avaliar e evoluir os processos de gerenciamento de risco (WITTY, 2002).

As metodologias de gestão de risco em tecnologia utilizam, no Brasil, a norma NBR ISO/IEC 17799, que define avaliação e gerenciamento de risco da seguinte forma:

> *"Avaliação de risco é avaliar as ameaças, impactos e vulnerabilidades da informação e das instalações de processamento da informação e da probabilidade da sua ocorrência."*
> (NBR ISO/IEC 17799, 2001, p. 4)

> *"Gerenciamento de risco é um processo de identificação, controle e minimização ou eliminação dos riscos de segurança que podem afetar os sistemas de informação, a um custo aceitável."*
> (NBR ISO/IEC 17799, 2001, p. 4)

Conforme análise do coronel MCCROHAN, do Centro Nacional de Proteção de Infra-estrutura do governo americano, ligado ao FBI , o setor financeiro deve encarar que possui as ameaças do ambiente físico e do ambiente cibernético também (MCCROHAN, 2003). O setor financeiro é considerado, pelos *hackers*, criminosos, anarquistas sociais, vândalos cibernéticos e até por terroristas, como um alvo estratégico. Além disso, na visão do coronel, a tecnologia, sozinha, não resolverá o problema das ameaças, a alta gerência deverá se envolver neste processo contínuo.

2.2.6. Gerenciamento de risco do Internet Banking

A organização *Bank for International Settlements*, conhecida também como Comitê da Basiléia, por estar sediada na cidade suíça de Basiléia, principal organização internacional que incentiva a cooperação entre as instituições financeiras e atua como o banco dos bancos centrais dos países, com objetivo de manter a harmonia financeira deles, publicou um manual com os princípios de gerenciamento de risco para Banco Eletrônico, sendo que, a última versão, revisada, foi publicada em julho de 2003 (BASEL COMMITTEE, 2003).

A seguir, os quatorze princípios de gerenciamento de risco para Banco Eletrônico, desenvolvidos pelo Comitê, e classificados em 3 categorias:

A. Princípios de vigilância da comissão de diretoria e gerência sênior.

1. Gerenciamento efetivo das atividades de Internet Banking.

   – Revisar, honestamente, a estratégia e a performance corrente do banco, em relação ao Internet Banking. Uma má revisão pode gerar estimativa incorreta de custo e retorno.
   – Estabelecer, claramente, qual é o apetite do banco em relação ao Internet Banking.
   – A maioria dos elementos que compõem o Internet Banking é de domínio público, portanto, fora do controle do banco, como o navegador (*browser*), a rede de conexão e alguns aplicativos.
   – Na Internet não há como restringir o raio de acesso ao serviço eletrônico, da mesma forma como é feito na rede física ou no atendimento telefônico.

2. Instituição de um processo de controle de segurança compreensível.

   – Controle físico, que impeça o acesso ao ambiente computacional.
   – Controle lógico, interno e externo, que impeça acesso indevido aos aplicativos de *software* e banco de dados.
   – Contínua revisão dos controles e das versões de *software* para *upgrades* adequados de *software* e correções de aplicativos.

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

   – Avaliação minuciosa da competência e saúde financeira da empresa parceira.
   – Definição clara do papel do banco e da parceira, documentada em contrato.
   – A empresa terceira tem que estar aderente ao gerenciamento de risco, segurança política de privacidade do banco.
   – Plano de contingência, em caso de quebra de parceria.

B. Princípios de controles de segurança:

4. Autenticação dos usuários de Internet Banking.

   – Dados de autenticação devem ser resguardados, para evitar que sejam corrompidos ou usados de forma indevida.
   – Qualquer alteração na base de dados de autenticação deve ser autorizada por um recurso autorizado.
   – Promover a segurança pelo tempo que a sessão de transação do cliente estiver ativa. Em caso de encerramento da sessão, por tempo (*time-out*), revalidar o acesso por meio de senhas.

5. Não repúdio e contabilização das transações realizadas pelo Internet Banking.

   – Validar a real intenção do cliente em realizar cada transação.
   – As partes que realizam a transação devem ser autenticadas.
   – As transações não podem ser alteradas, sem consentimento do cliente, e qualquer cancelamento ou alteração da transação deve ser registrado.

6. Medidas apropriadas para assegurar as obrigações de segregação.

   – O sistema e processo da transação devem evitar que funcionários do banco ou da empresa parceira entre no sistema e autorize e complete transações.

– Deve ser mantida a segregação entre os dados estáticos, conteúdo aberto do conteúdo individual do cliente.

– Devem ser segregados os ambientes de desenvolvimento e de administração do Internet Banking de produção.

7. Controle de autorização apropriado, dentro do sistema de Internet Banking, de banco de dados e dos aplicativos.

8. Integridade dos dados de transações, registros e informações do Internet Banking.

– O processo, como um todo, da transação eletrônica deve ser resguardado de qualquer tipo de acesso indevido.

– Política adequada de controle das alterações, incluindo monitoramento e teste dos procedimentos, visa evitar a implantação de programas errados, que possam comprometer os controles ou a confiabilidade dos dados.

9. Estabelecimento de um caminho de auditoria para as transações realizadas no Internet Banking.

– Acompanhamento da informação de abertura, alteração ou encerramento da conta corrente.

– Registrar as transações contábeis ou financeiras.

– Registrar qualquer alteração de privilégios ou alçadas de acesso.

10. Confidencialidade das informações importantes.

– Todos os dados confidenciais do banco devem estar acessíveis apenas a pessoas, agentes e sistemas autorizados.

– Todos os dados confidenciais devem estar protegidos de espionagem ou alteração indevida durante as suas transmissões públicas, privadas ou dentro das dependências do banco.

– Os padrões e os controles de uso e proteção dos dados devem ser compartilhados com terceiros.

– Todos os acessos aos dados restritos devem ser registrados e protegidos de qualquer tipo de corrupção.

C. Princípios legal e de reputação do gerenciamento de risco:

11. Apresentação apropriada dos serviços de Internet Banking.

– O banco deve publicar em seu *website* informações como localização da matriz e de suas agências; os canais de comunicação entre o cliente e a instituição; e o meio de acessar o ombudsman e demais informações dos produtos e serviços.

12. Privacidade das informações do cliente.

– A política de privacidade do banco deve estar aderente à legislação e às normas do local de atuação do banco.

– O cliente deve estar ciente da política de privacidade e das regras de uso dos produtos e serviços.

– O cliente tem a opção de permitir que seu e-mail seja usado para envio de correspondência diversa.

– Os dados do cliente não devem ser usados para fins além dos que o próprio cliente previamente autorizou.

13. Capacitação e plano de continuidade e de contingência do negócio para assegurar a disponibilidade do sistema e serviços de Internet Banking.

– A capacidade da infra-estrutura e o plano de contingência e continuidade do banco devem ser constantemente avaliados, a fim de que acompanhem a dinâmica do mercado, com o crescimento e oferta de novos produtos e serviços.

14. Plano de resposta para incidentes.

– Mecanismos para detectar incidentes e crises, assim que elas ocorram, com disparo automático de aviso para os responsáveis pelo sistema.

– Estratégia de comunicação com o público, interno e externo, em caso de incidentes.

– Manter o registro forense dos fatos, como prova de crimes e fraudes, análise futura e criação de um histórico.

2.3. Gestão de Segurança

2.3.1. Segurança, segurança eletrônica, segurança de informação

A segurança pode ser um processo de atividade ou um resultado de atividade, portanto, pode ser um processo ou um estado, conforme HEALY e WALSH (1979). O processo, na definição da autora, é a redução ou eliminação dos riscos de perdas de ativo, tangíveis ou intangíveis, causados por eventos além das fronteiras da especulação convencional, usando e aplicando os recursos humanos, equipamento e procedimentos da organização ou de parceiros. O estado de segurança é o resultado da implantação das medidas apropriadas de defesa das perdas de ativo, devido à exposição ao risco.

Uma organização deve se preocupar com a sua segurança no mundo digital da mesma forma que ela se resguarda no mundo físico. As empresas de segurança, *Internet Security Systems* e *British Department of Trade and Industry*, argumentam que os riscos no mundo físico (perda financeira ou de reputação) se repetem no meio eletrônico, resguardadas as particularidades de cada meio:

> *"Security is a business fundamental in the physical world. No organization would even consider opening operations without securing all facilities against theft, fire and vandalism. Nevertheless, companies engaging in E-commerce routinely shortchange their protection of key online asset and systems. A single security breach in the online world can be far more damaging than if would be in the physical world in terms of strategic information lost, bad publicity, loss of customer and partner confidence, and stakeholders liability."* [16]
> (*INTERNET SECURITY SYSTEMS*, 2000, p. 1)

[16] Segurança é um fundamento empresarial no mundo físico. Nenhuma organização consideraria abrir as suas operações sem assegurar sua estrutura física contra roubo, fogo e vandalismo. Não obstante, companhias engajadas em comércio eletrônico, rotineiramente, dão menos importância que o necessário à proteção dos seus recursos e sistemas chaves on-line. Uma única brecha de segurança no mundo on-line pode ser muito mais prejudicial do que no mundo físico, em termos de perda de informações estratégicas, má publicidade, perda da confiança do cliente e do sócio, e responsabilidade dos stakeholders. (tradução nossa)

> *"Information security is about safe-guarding your business's money, image, reputation and potential – perhaps its very existence. The consequences of security incidents can be disastrous – but they are avoidable. The old physical approach to security remains important, but as businesses acquire a new virtual identity, it is not enough."* [17]
> (*BRITISH DEPARTMENT OF TRADE AND INDUSTRY*, 2000, p. 3)

Segurança, conforme definição de CAMP (2000), é o controle das informações geridas pelos donos ou criadores de tecnologias implementadas, com base em uma política de segurança. Para a FEBRABAN (2000), a segurança é um processo de proteção de informações e ativos digitais, armazenados em computadores e redes de processamento de dados. SIMONDS acrescenta que deve haver "um equilíbrio entre o custo, a produtividade e o risco" (1996, p. 317, tradução nossa). Equilíbrio, para ele, significa:

> *"(...) equilibrium is what we refer to as security balance, just the right amount of security for your organization, in your context, to secure your organizational mission, taking into account your organization's culture way of doing things."* [18]
> (SIMONDS, 1996, p. 304)

O código de prática, para a gestão de segurança da informação, desenvolvido por um comitê internacional, o BS ISO/IEC 17799 (2000), é caracterizado pela tríade que assegura a preservação da:

- Integridade: garantia de que os dados não foram corrompidos no seu manuseio ou transmissão.
- Confidencialidade: forma de assegurar que os dados não foram manuseados ou lidos por pessoas não autorizadas.
- Disponibilidade: meio de tornar certa a comunicação entre os computadores, a qualquer momento que for solicitada.

[17] A segurança de informação é sobre proteger o dinheiro, a imagem, a reputação e o potencial do seu negócio – talvez sua própria existência. As conseqüências de incidentes de segurança podem ser desastrosas – mas são evitáveis. O velho enfoque físico à segurança é importante, mas quando os negócios adquirem uma nova identidade virtual, isto não é suficiente. (tradução nossa)

[18] (...) o equilíbrio é o que nós referimos como contrapeso da segurança, apenas a quantidade exata de segurança para a sua organização, dentro do seu contexto, para assegurar a sua missão organizacional, levando em consideração a sua cultura na forma de fazer as coisas. (tradução nossa)

Outras ameaças, contra a segurança na Internet, foram agregadas a esta tríade de segurança da informação (CAMP, 2000):

- Privacidade do cidadão, em relação à divulgação de suas informações ou ao seu acesso por meios eletrônicos.
- Não-repúdio, definido pela certeza de que o executor de uma transação não pode negar a ação.
- Autenticidade, que garante que a pessoa que assina o documento é ela mesma e confiabilidade no processo em si.

ALBERTIN e MOURA (1998) justificam a importância da segurança para o comércio eletrônico na citação a seguir:

> *"Os aspectos complexos de segurança, privacidade, autenticação e anonimato têm especial importância para o comércio eletrônico. Confidencialidade, confiabilidade e proteção das informações contra ameaças de segurança são pré-requisitos críticos para a funcionalidade do comércio eletrônico."*
> (ALBERTIN e MOURA, 1998, p. 50)

Conforme relato de McKNIGHT e BAILEY (1999, p. 450, tradução nossa), "o comércio na Internet paradoxalmente, requer abertura e privacidade, bem como acesso ubíquo e segurança".

A segurança eletrônica também é conhecida como segurança de informação ou segurança em TI (Tecnologia de Informação). Cada autor utiliza umas destas terminologias para indicar a segurança dos sistemas de informação no ambiente digital e no ambiente físico, além de incluir os recursos humanos envolvidos nos processos relacionados à segurança.

2.3.2. Gestão de Segurança de Informação

Segundo o guia de referência sobre ataques, via Internet, publicado em 2000, pela FEBRABAN, a segurança se baseia na avaliação de risco; nas necessidades legais, contratuais e estatutárias; nos princípios, objetivos e necessidades organizacionais e nas políticas e diretrizes organizacionais.

A capacidade essencial de gerenciamento de segurança, em Tecnologia de Informação, é prover o monitoramento e gestão de eventos, em conformidade com os requisitos de segurança em TI da organização. A gestão de segurança em TI não é apenas um assunto para os técnicos, ela também envolve as áreas administrativas, conforme argumento do departamento britânico de negócios e indústria:

> *"Technology cannot provide all the answers to what are problems posed by people. This is because information security is not a technical issue but a business and management one. The answer is to adopt tried and tested measures to counter specific threats facing the organisation, and to build these into day-to-day business operations instead of bolting it on as an optional extra."* [19]
> (*BRITISH DEPARTMENT OF TRADE AND INDUSTRY*, 2000, p. 3)

A segurança, em Internet, pode ser dividida em duas dimensões: a primeira, são as políticas, os guias de procedimentos, os processos e ações para manter as transações eletrônicas mediante riscos (falhas, invasão ou roubo) mínimos possíveis. A segunda, é composta por qualquer técnica ou processo usado para proteger as informações. O gerenciamento de segurança procura mitigar os riscos, proporcionalmente ao valor das informações para a instituição, portanto, se um banco oferece transações de valores baixos, na Internet, os riscos individuais que ele pode correr são menores que um banco com limites superiores, conforme descrito por GLAESSNER, KELLERMANN e McNEVIN (2002), na política pública de mitigação de risco das transações em meio eletrônico.

A gestão de segurança eletrônica tem como objetivo minimizar os riscos nas transações financeiras, baseadas em *trade-off*, entre a segurança em si e o seu custo, a qualidade de serviço, os impactos mercadológicos, a inovação tecnológica e a privacidade (GLAESSNER; KELLERMANN; McNEVIN, 2002). A organização deve atentar ao balanço entre as medidas de segurança e as necessidades comerciais. McKNIGHT e BAILEY (1999) e WADLOW (2000) reforçam esta idéia, a seguir:

[19] A tecnologia não pode dar todas as respostas aos problemas vindos das pessoas. Isto porque a segurança da informação não é uma questão técnica, mas sim uma questão de negócio e gerenciamento. A resposta é adotar medidas experimentadas e testadas para se opor às ameaças específicas enfrentadas pela organização, e construir isto no dia-a-dia das operações de negócio, em vez de juntar isto como um extra, opcional. (tradução nossa)

> *"Unfortunately, information security does not necessarily exhibit positive network effects: instead, it takes knowledge, foresight, and technical skill to design an affective and secure infrastructure, which may, however, dampen growth."* [20]
> (McKNIGHT; BAILEY, 1999, p. 445–446)

> *"A segurança não pode transformar a rede em uma fortaleza, a menos que seja o único modo de realização de negócios. As medidas de segurança costumam ser inimigas da flexibilidade. Se a atividade depender de flexibilidade e a segurança de rede for inflexível, será inevitável um choque entre as duas e a segurança se perderá"*
> (WADLOW, 2000, p. 46)

A segurança, em Internet, não deve ser vista apenas como um aspecto da gestão de risco, ela deve ser aderente ao objetivo e à estratégia do banco e gerida de forma coesa, pelas áreas de negócios e tecnologia (HARRIS, 2002).

A política de segurança eletrônica do *The World Bank*, desenvolvida por GLAESSNER, KELLERMANN e McNEVIN (2002), fundamenta a gestão de segurança na Internet, em sete pilares:

1. Legislação adequada à nova realidade da Internet e política efetiva de punição.

   – A legislação deve varrer os seguintes temas:

   - transações eletrônicas e comércio eletrônico;
   - sistema seguro de pagamento;
   - privacidade;
   - crimes cibernéticos;
   - lavagem de dinheiro;
   - fiscalização de infra-estrutura.

2. Segurança eletrônica dos sistemas de pagamentos, como iniciativa governamental, com respaldo legal e intervenção regulatória.

   – A segurança deve responder a cinco questões:

[20] Infelizmente, a segurança da informação não exibe, necessariamente, efeitos em rede positivos: em vez disso, requer conhecimento, perspicácia e habilidade técnica para projetar uma infra-estrutura efetiva e segura, que pode, entretanto, amortecer o crescimento. (tradução nossa)

- falta de definição para os transferidores de dinheiro;
- falta de relatórios de requisitos;
- regulamentação limitada ou inexistente;
- garantias, indenizações, obrigações limitadas ou inexistentes;
- falta de requisitos para os provedores de serviços.

3. Supervisão e prevenção para se adequar à política global financeira.

   – Atender a requisitos de guarda e manutenção, da saúde financeira global e promover o uso de seguros, que cubram perdas financeiras, em caso de sinistro nas transações eletrônicas.

   – Compartilhar a responsabilidade da segurança com as empresas ligadas ao desenvolvimento dos *softwares*, *hardwares* e infra-estruturas utilizadas pela instituição financeira.

   – Supervisionar e examinar os processos do banco e de seus parceiros, para avaliação de riscos, monitoramento, correção, auditoria e geração de relatório.

4. Seguradora privada, como sistema complementar de monitoramento de risco, e para cobertura de eventuais danos das instituições, em caso de sinistro.

5. Setores públicos e privados cooperarem para desenvolver padrões e avalizar certificados, como forma de minimizar riscos.

   – A equalização dos requisitos e dos tipos de certificados emitidos, localmente ou internacionalmente, por órgão público ou privado, é importante para que as transações possam ocorrer sem fronteiras legais.

6. Acurácia e cooperação do setor público e privado no levantamento das informações dos incidentes.

   – A divulgação dos incidentes entre os bancos e seus parceiros é importante para que os tipos de fraudes e golpes não se repitam, em mais de uma instituição.

– Uma terceira entidade controla as informações, no caso do Brasil, a FEBRABAN, promove e controla este tipo de cooperação entre os maiores bancos que atuam no país.

7. Educação e prevenção sobre a segurança eletrônica.

– Segundo pesquisas, do MÓDULO (2003) e da CSI/FBI (2004), mais de 50% dos problemas de segurança tiveram como sujeito da ação pessoas ligadas à própria organização. O problema pode ser intencional ou não.

2.3.2.1. Estágios de conscientização do executivo sobre segurança da informação

O discurso dos executivos das organizações, principalmente dos bancos, é recheado de preocupações e considerações sobre a segurança do seu ambiente digital, mais especificamente, das transações e negócios que ocorrem no meio Internet. O quanto as organizações, efetivamente, investem, para se sentirem seguras, depende do modelo mental de segurança que o executivo da organização possui (BRINEY, 2004).

O executivo principal de uma organização pode ser enquadrado em um dos quatro estágios evolucionários de conscientização sobre a segurança, conforme estudo de BRINEY (2004):

Primeiro estágio: Segurança é um mal necessário, portanto, investe-se, o mínimo possível, para se manter dentro dos padrões exigidos por lei.

Segundo estágio: Segurança é uma necessidade básica de manutenção do negócio, portanto, a segurança não trará novos negócios ou retorno sobre os investimentos.

Terceiro estágio: Segurança é como uma apólice de seguro, portanto, ela serve para que a organização se recupere em caso de sinistro.

Quarto estágio: Segurança é qualidade, portanto, não é um item tangível, mas o seu retorno é mensurável. Assim como a qualidade, a segurança é um modelo mental, com um processo contínuo.

2.3.3. Implementando a gestão de segurança de informação

A implementação da gestão de segurança pode ser feita pela equipe interna, pela equipe externa, de parceiros e consultorias, ou de forma mista. A equipe mista é composta por recursos externos, que podem trazer as melhores práticas do mercado, e recursos internos, que incorporarão, na gestão de segurança, a visão estratégica e a idiossincrasia da própria empresa.

A seguir, esquema (figura 9) que representa o plano de ação de implementação de uma gestão de segurança de informação restrito à organização. Outro ponto relevante, questionado no final do esquema, é a segurança dos demais participantes que interagem com a organização, os clientes do banco, por exemplo. Este plano foi desenvolvido pela *British Department of Trade and Industry*.

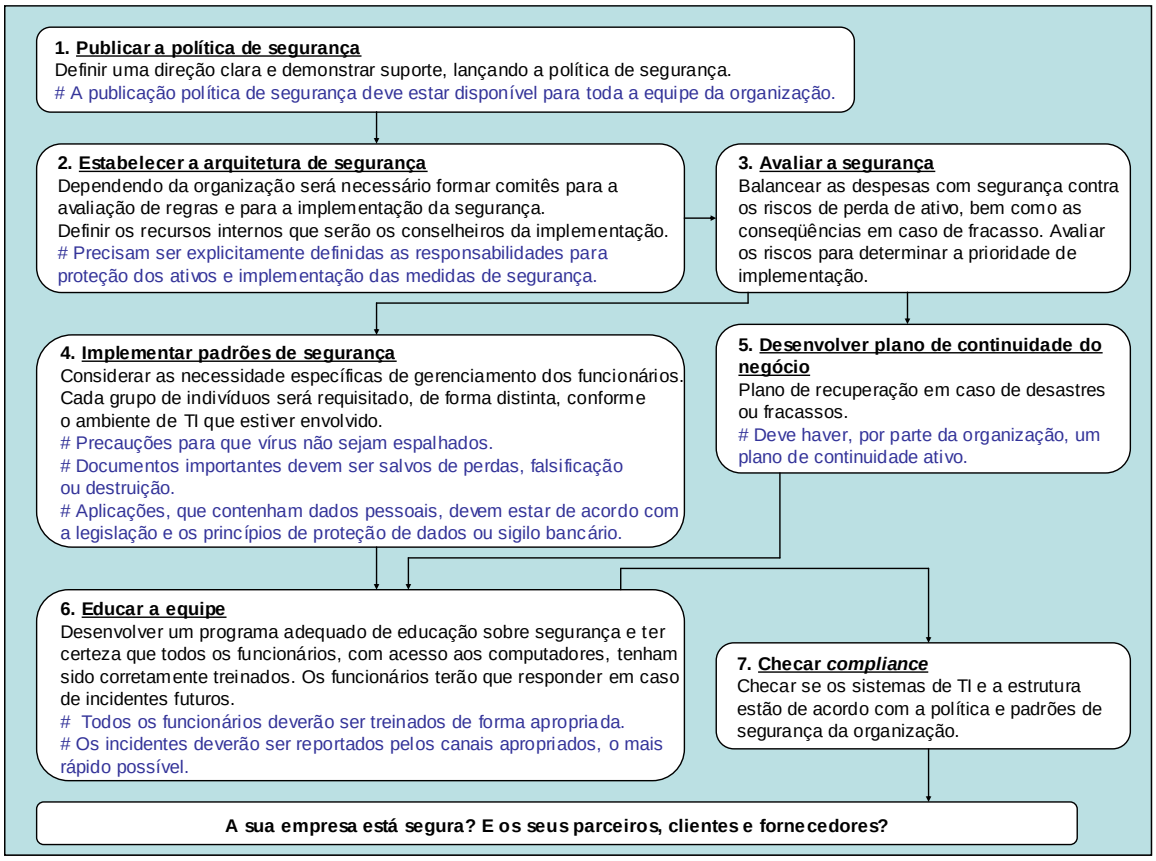


Figura 9: Plano de ação para implementação de uma gestão de segurança da informação (*BRITISH DEPARTMENT OF TRADE AND INDUSTRY*, 2000)

2.3.4. Normas, padrões e melhores práticas em gestão de segurança da informação

Uma vez que a organização se conscientiza da real necessidade em investir na minimização dos riscos de segurança da informação, ela deverá criar um guia, com as práticas necessárias para suportar a estratégia de negócio. Este documento, normalmente, é tratado como sendo a sua política de segurança, e será a base para a montagem e manutenção da arquitetura de segurança do Internet Banking.

No Brasil, existe o "Código de Prática para a Gestão de Segurança da Informação", desenvolvido pela Associação Brasileira de Normas Técnicas (ABNT). A norma, desenvolvida pela ABNT, é a NBR ISO/IEC 17799:2001, e baseia-se na norma britânica BS 17799:2000, *Information Security Management Systems: Specificaton with Guidance for Use*, desenvolvida pela *British Standards Institution* (BSI). Segundo a Associação Brasileira de Normas Técnicas, "O objetivo da política de segurança é prover à direção uma orientação e apoio para a segurança da informação." (NBR ISSO/IEC 17799, 2001, p. 4)

A norma brasileira NBR ISO/IEC 17799:2001 varre todos os temas pertinentes à gestão de segurança da informação, dividida em doze itens:

1. Objetivo
2. Termos e definições
3. Política de segurança
4. Segurança organizacional
5. Classificação e controle dos ativos de informação
6. Segurança em pessoas
7. Segurança física e do ambiente
8. Gerenciamento das operações e comunicações
9. Controle de acesso
10. Desenvolvimento e manutenção de sistemas
11. Gestão da continuidade do negócio
12. Conformidade

A Associação Brasileira de Normas Técnicas (ABNT) publica as seguintes normas, relacionadas à segurança de informação, sendo a NBR ISO/IEC 17799:2001 a mais pertinente neste estudo:

- ✓ NBR ISO/IEC 17799:2001 – *Código de prática para a gestão da segurança da informação*
- ✓ NBR 11514:1991 – *Controle de acesso para segurança física de instalações de processamento de dados*
- ✓ NBR 11515:1991 – *Critérios de segurança física, relativos ao armazenamento de dados*
- ✓ NBR 11584:1991 – *Critérios de segurança física, relativos a microcomputadores e terminais, em estações de trabalho*

O Tribunal de Contas da União (TCU) publica um manual de auditoria, denominado "Boas Práticas em Segurança da Informação", baseado na NBR ISO/IEC 17799:2001, cujo objetivo é reproduzido, a seguir:

> *"O objetivo desta publicação é apresentar, na forma de capítulos, boas práticas em segurança da informação, a qualquer pessoa que interaja de alguma forma com ambientes informatizados, desde profissionais de informática envolvidos com segurança de informações até auditores, usuários e dirigentes preocupados em proteger o patrimônio, os investimentos e os negócios de sua organização, em especial, os gestores da Administração Pública Federal."*
> (TRIBUNAL DE CONTAS DA UNIÃO, 2003, p. 10)

Em âmbito internacional, existem os seguintes órgãos que ditam as normas, padrões e melhores práticas para a gestão de segurança da informação (os documentos publicados por estas entidades encontram-se no anexo 1):

- ✓ *British Standard Institution (BSI)*

  A instituição britânica é uma das pioneiras em elaborar normas e padrões, além de ser responsável pela publicação dos guias e padrões da *British Standards*.

  BS 17799-2:2000 – *Information Security Management Systems – Specification with Guidance for Use*

- *International Organization for Standardization (ISO)*

  A organização é uma rede de institutos de padrões de 148 países, com a base de coordenação do sistema em Genebra, Suíça. A organização não é vinculada a nenhum governo e seus padrões são utilizados tanto pelo setor público, quanto privado.

  A seguir, os padrões mais relevantes, para a gestão de segurança:

- *National Institute of Standards and Technology (NIST)*

  O instituto americano é uma agência federal, não regulamentada, do departamento comercial de administração de tecnologia. A missão dele é desenvolver padrões, medidas e tecnologia que promovam o aumento de produtividade, facilite as transações e melhore a qualidade de vida.

- *Internet Engineering Task Force (IETF)*

  Este grupo de estudo é uma comunidade, aberta e internacional, que reúne designers, operadores, vendedores e pesquisadores envolvidos com a evolução da arquitetura, bem como a operação da Internet. Um dos temas de estudo é a segurança.

- *The Committee of Sponsoring Organizations of the Treadway Commission (COSO)*

  Comitê patrocinado pela comissão nacional americana de reporte de fraudes financeiras, bem como por mais cinco associações financeiras americanas, associação de contadores certificados publicamente, de executivos financeiros, de auditores internos e de gerentes contábeis.

- *Information Systems Audit and Control Association (ISACA)*

  A associação teve início com a união de alguns profissionais ligados à auditoria. O COBIT é um documento que dita as normas e padrões para uma boa segurança de informação e práticas de controles, sendo uma referência para administradores, usuários, auditores, controladores e profissionais ligados ao sistema de informação.

- *International Information Systems Security Certifications Consortium, INC. [(ISC)^2]*

  O consórcio é responsável pela emissão dos certificados de profissional de segurança, mais cobiçados no mercado.

- ✓ *Information Systems Security Association (ISSA)*

  Associação internacional que reúne profissionais de segurança. O seu papel é criar um fórum de discussão, publicações e interação entre os profissionais da área de segurança e afins. Sua finalidade é promover o enriquecimento do conhecimento e habilidade dos profissionais de segurança e membros da associação.

- ✓ *International Information Security Foundation (I^2SF)*

  Os princípios, desenvolvidos pela fundação, foram baseados em uma conferência nacional de segurança em computador ocorrida nos Estados Unidos, em 1992. A elaboração do documento foi feita por profissionais de segurança da América do Norte e da Europa Ocidental.

- ✓ *American National Standards Institute (ANSI)*

  O instituto, privado e sem fins lucrativos, administra e coordena a padronização voluntária, além de avaliar a conformidade dos sistemas nos Estados Unidos. A partir de 1974, aprovou as atividades do *X9 Standards Committee on Banking*, conhecido como padrão para facilitar operações bancárias.

- ✓ *Capability Maturity Model® for Software (SW-CMM®)*

  Este modelo foi elaborado pela comunidade de criadores de *software*, com o patrocínio da *Software Engineering Institute* da *Carnegie Mellon University*.

2.3.5. Ferramentas que auxiliam na segurança do Internet Banking

A segurança do Internet Banking possui, basicamente, três pontas: o banco, fornecedor dos serviços e transações; o cliente, usuário do canal eletrônico e a rede de comunicação, provedor de acesso à Internet. A segurança, em si, é uma responsabilidade tanto do banco quanto do cliente, pois não adianta o banco se resguardar, investindo milhões em recursos tecnológicos, processuais e humanos se o cliente escancarar suas senhas de acesso e transação. Conforme ALBERTIN e MOURA (1998, p. 58), "a segurança de qualquer conexão de rede depende dos dois lados da conexão, ou seja, o lado do cliente (browser) e o lado do servidor (www.servidor.com)."

A avaliação do nível de segurança, de um site ou serviço na Internet, pode ser mensurada pelos tipos de recursos utilizados para solucionar cada um dos seis itens descritos anteriormente (integridade, confidencialidade, disponibilidade, privacidade, não-repúdio e autenticidade). Algumas soluções são detectáveis com um simples acesso ao Internet Banking ou no uso do serviço; porém, para se avaliar o uso das outras soluções é preciso uma análise mais profunda, com a participação do responsável pelo site ou serviço.

A seguir, uma relação (tabela 2) com as principais ferramentas que podem ser usadas para garantir cada tipo de segurança esperado de um Internet Banking, dividida em: recursos utilizados pelo banco e pelo cliente usuário. As referências dos tipos de ferramentas foram extraídas dos textos de HARRIS (2002) e KRUTZ; VINES (2001).

Tabela 2: Itens de segurança do lado do banco e do cliente

Ferramentas de Segurança da Internet		
	Banco	**Cliente**
Integridade		
	- Utilizar a função *Hash* (*message digest*) para criar um código baseado nas informações da transação, que será posteriormente comparado para detectar se a mensagem foi corrompida. - Implantar um sistema de patrulha de invasão do sistema. - Controlar o acesso ao ambiente de *hardware* e *software*. - Educar, conscientizar e treinar a equipe interna e desenvolver campanhas sobre segurança para o cliente.	- Não divulgar suas senhas de acesso. - Acessar o banco de um local confiável, como sua residência ou escritório. - Utilizar provedor de acesso idôneo. -Manter atualizado o *software* antivírus.
Confidencialidade		
	- Utilizar algum tipo de encriptação. - Implantar um sistema de patrulha de invasão do sistema. - Controlar o acesso ao ambiente de hardware e *software*. - Estar de acordo com a legislação e normas do governo federal, do Banco Central e dos acordos internacionais. - Selar o uso do canal Internet Banking por meio de contrato. - Desenhar um processo de cadastramento e acesso que iniba fraudes e roubos. - Educar, conscientizar e treinar a equipe interna e desenvolver campanhas sobre segurança para o cliente.	- Não divulgar suas senhas de acesso. - Acessar o banco de um local confiável, como sua residência ou escritório. - Utilizar provedor de acesso idôneo. - Ler o contrato para evitar surpresa. - Utilizar sistema de segurança pessoal, no computador pessoal ou do trabalho, como *firewall*, que filtre vírus ou aplicativos suspeitos. - Prestar atenção nas dicas de segurança divulgadas pelo banco. - Trocar a senha regularmente. -Manter atualizado o *software* antivírus.

Ferramentas de Segurança da Internet		
	Banco	**Cliente**
Disponibilidade		
	- Montar uma arquitetura com sistema de contingência e escalabilidade imediata. - Implantar um sistema de tomada de decisão automática ou remota contra acessos de invasão em massa. - Manter redundância de ambiente e conexão. - Distribuir e balancear os acessos em diversos servidores. - Treinar e qualificar a equipe técnica, de atendimento e de vendas.	- Utilizar provedor de acesso idôneo.
Privacidade		
	- Desenvolver e divulgar uma política de privacidade. - Utilizar algum tipo de encriptação. - Utilizar sistema de segurança corporativo como *firewall*, que filtre vírus ou aplicativos suspeitos. - Controlar o acesso ao ambiente de *hardware* e *software*. - Oferecer um teclado alternativo (teclado virtual ou teclado que embaralhe as teclas), que impossibilite rastrear a digitação de senhas ou dados pessoais. - Estar de acordo com a legislação e normas do governo federal, do Banco Central e dos acordos internacionais. - Evitar ação de intrusão de terceiros, por meio de engenharia social. - Educar, conscientizar e treinar a equipe interna e desenvolver campanhas sobre segurança para o cliente.	- Ler a política de privacidade do banco. - Evitar ação de intrusão de terceiros, por meio de engenharia social. - Acessar o banco de um local confiável, como sua residência ou escritório. - Utilizar provedor de acesso idôneo. - Trocar a senha regularmente. -Manter atualizado o *software* antivírus.
Não repúdio		
	- Selar o uso do canal Internet Banking por meio de contrato. - Desenvolver um processo que valide, eletronicamente, a autenticidade das partes, como o uso de chaves privadas e certificação digital. - Documentar as transações para futuros rastreamentos de dados.	- Ler o contrato para evitar surpresa.
Autenticidade		
	- Implantar a certificação digital do banco e dos clientes usuários. - Guardar dos certificados digitais em cofres. - Implantar a assinatura digital para as transações. - Validar, por meio de senhas fortes ou por chaves pública e privada.	- Verificar o certificado digital do banco em cada acesso. -Manter atualizado o *software* antivírus.

2.3.6. Mecanismos de segurança na Internet

Os mecanismos de segurança mais difundidos, em Internet, podem ou não usar o recurso de criptografia.

A seguir, o elenco de mecanismos de segurança, classificados em: "sem criptografia" e "com criptografia" (KUHN et al, 2001).

2.3.6.1. Mecanismos de segurança SEM criptografia

1. Senhas: mecanismo tradicional de autenticação de usuário, por meio de números de identificação pessoal (PIN) ou senha secreta.

2. Medidas biométricas: utiliza características físicas, individuais, como impressão digital, desenho da íris e padrão de voz.

3. Paridade de bits e verificação de redundância cíclica: mecanismos simples de segurança projetados para assegurar a integridade dos dados transmitidos entre dispositivos, por meio de comparação de dados.
4. Assinatura manuscrita digitalizada: comparação entre assinaturas manuscritas digitalizadas, comparação entre imagens.

A tabela 3 é uma classificação dos mecanismos e do tipo de segurança garantido. Nesta classificação, não foi incluída a "disponibilidade", pois ela depende do *hardware*, *software* e infra-estrurura de telecomunicação do banco, não fazendo parte da conexão entre o cliente e o banco.

Tabela 3: Mecanismos x Tipo de segurança

Mecanismo	Integridade	Confidencialidade	Autenticação	Não Repúdio	Privacidade
1. Senhas	Não	Não	Sim	Não	Sim
2. Medidas biométricas	Não	Não	Sim	Não	Sim
3. Paridade de bits e verificação de redundância cíclica	Sim	Não	Não	Não	Sim
4. Assinatura manuscrita digitalizada	Não	Não	Não	Não	Sim

2.3.6.2. Mecanismos de segurança COM criptografia

A criptografia é um ramo da matemática aplicada que estuda a transformação dos dados, com foco em segurança. Na criptografia, um remetente transforma informação desprotegida (texto em claro) em texto codificado (mensagem cifrada). O destinatário da informação (i) decodifica a mensagem cifrada, (ii) verifica a identidade do remetente e (iii) comprova a integridade dos dados, ou uma combinação destas ações.

A seguir, os três mecanismos de criptografia mais utilizados na segurança de informação:

1. Chave Simétrica: mecanismo em que a chave de encriptação e decriptação, codificação e decodificação é a mesma. O algorítimo utilizado para embaralhar e desembaralhar os dados é o mesmo, o que implica em um compartilhamento da chave secreta entre as duas partes que estiverem se comunicando. Os algorítimos modernos são rápidos e fortes, sendo muito utilizados para autenticação.

2. Função Hash: mecanismo que destaca uma parte do documento e o reduz para um tamanho fixo, por meio de uma função matemática de mão única. O resultado é conhecido como "*message digest*", considerado uma impressão digital dos dados. Por meio do *message digest* não é possível recuperar o documento original. Recurso utilizado, principalmente, para integridade dos dados.

3. Chave Assimétrica: este mecanismo também é conhecido como criptografia de chave pública, no qual o remetente possui uma chave privada e o destinatário uma chave pública do remetente. A informação é encriptada com uma chave privada A e somente poderá ser decriptada com a chave púbica A. O algoritmo assimétrico de criptografia não é adequado para encriptar mensagens longas porque demanda recursos de processamento e é mais lento que o algoritmo simétrico. O objetivo do algoritmo assimétrico é preservar a autenticidade, a integridade, o não repúdio e a confidencialidade. Este mecanismo é usado para gerar três operações: (i) assinatura digital, (ii) transporte das chaves e (iii) "*key agreement*":

i. Assinatura digital: uso da chave privada e da função Hash, que identifica e autentica o remetente.

ii. Transporte de chave: transporte seguro das chaves simétricas.

iii. *Key agreement*: criação de um ambiente seguro entre 2 pontas que possuem as chaves públicas de cada um.

A tabela 4 é uma classificação do mecanismo criptográfico e do tipo de segurança proporcionado. Nesta classificação, também foi incluída a "disponibilidade", pelo mesmo motivo anterior.

Tabela 4: Mecanismos criptográficos x Tipo de segurança

Mecanismo	Integridade	Confidencialidade	Autenticação	Não Repúdio	Privacidade
1. Chave simétrica	Sim	Sim	Sim	Não	Sim
2. Função *Hash*	Sim	Não	Sim	Não	Não
3. Chave assimétrica:					
i. Assinatura digital	Sim	Não	Sim	Sim	Sim
ii. Transporte de chave	Não	Não	Não	Não	Sim
iii. "*Key agreement*"	Não	Não	Sim	Não	Sim

2.3.7. Funções de trabalho em uma equipe de segurança

A multidisciplinariedade é um ponto forte na formação de uma equipe de segurança, na qual nem todas as funções precisam de um profissional exclusivo, mas cada função deverá ser desempenhada por alguém na organização.

WADLOW (2000) dividiu a área de segurança em três equipes multidisciplinares: de monitoramento, de reposta e de investigação de crimes eletrônicos.

Equipe de monitoramento: cuida das tarefas rotineiras, bem como dos testes de estresse e de performance do sistema. Também deve estar preparada para lidar com certas ocorrências de gravidade leve, que não necessitam de declaração de estado de emergência.

Equipe de resposta: combate as invasões e ataques, além de estudar e implantar soluções para novas formas de ataques que surjam no mercado. Também responde pelo plano de contingência, interagindo com toda a organização.

Equipe de investigação de crimes eletrônicos: fornece pesquisa e ajuda detalhada à equipe de resposta.

A área de segurança de uma organização é composta por uma diversidade de profissionais, que elaboram, desenvolvem, gerenciam, monitoram e comunicam a segurança para a organização e seus *stakeholders* (clientes, funcionários, sociedade, governo e acionistas). Estes profissionais e funções foram classificados, por WADLOW (2000), da seguinte forma:

Administrador de sistemas: possui a suscetibilidade para levantar e detectar falhas de segurança; para gerir, no dia-a-dia, os sistemas em si.

Analista de investigação de crimes: determina a metodologia do ataque, investiga incidentes de segurança e busca métodos de invasão e danos aos sistemas.

Arquiteto de segurança: coordena e centraliza todos os aspectos de segurança, como política de segurança e novos subsistemas.

Assessor de imprensa: responde por todos os contatos sobre segurança, entre a organização e a imprensa, como cobertura da mídia sobre incidentes específicos de segurança, nos quais o banco esteja envolvido.

Auditor interno: valida sistemas implementados, conforme especificado; complementa especificação de acordo com a necessidade, para responder a novos ataques; coordena o trabalho de modernização ou conserto.

Autenticador: responde pelo sistema que permite à rede verificar as identidades dos usuários.

Comunicador: administra todas as comunicações formais, dentro e fora do grupo de segurança, e responde pela criação de mensagem clara, concisa e informativa.

Controlador de danos: avalia danos em segundo nível, coordena consertos e soluções que evitem invasão secundária, possui habilidade para trabalhar com danos em tempo real.

Documentação: redige documentos como política, procedimento e manuais para os sentinelas.

Engenheiro de desenvolvimento: responde pela integração das diversas soluções adotadas pela organização, além de programar ou modificar aplicativos.

Executor legal: administra e se relaciona com executores de leis.

Gerente da equipe de investigação de crimes: coordena a equipe de investigação.

Gerente da equipe de resposta: administra a equipe de reposta a incidentes.

Gerente de documentação: assegura que apenas pessoas autorizadas tenham acesso aos documentos, mantém a documentação atual e pertinente.

Gerente de engenharia de desenvolvimento: coordena o desenvolvimento com o arquiteto de segurança.

Gerente de operações de segurança: monitora os incidentes e as respostas, assegura relatórios e estatísticas. Age como coordenador das operações dos sistemas de informação.

Guerreiro: combate os atacantes, em tempo real, para parar a investida e estabilizar o sistema.

Operador de segurança: inclui ou exclui registros nos sistemas de autenticação, manutenção dos principais serviços e servidores de segurança, e todas as questões operacionais relacionadas à segurança.

Pesquisador: informa sobre as brechas de segurança e as investidas mais recentes de atacantes; ensina soluções novas; trabalha coordenado com o auditor interno.

Políticas e procedimentos: administra e monitora os documentos de política de segurança, em conjunto com a área de recursos humanos.

Registro: mantém registros válidos de todos os sistemas e soluciona problemas.

Resposta a incidente – nível 1: tria pós-incidentes de segurança, cuida dos incidentes básicos, mantém ativo o sistema, foca a quantidade de eventos processados.

Resposta a incidente – nível 2: cuida dos incidentes mais complicados, foca a qualidade dos eventos processados.

Segurança da rede: responde pelo projeto e implementação da arquitetura de segurança, e pela configuração de cada componente.

Segurança do *host*: responde pelo projeto e implementação de sistema de segurança e *softwares*, residentes em computadores em geral.

Segurança física: responde por crachás, mecanismos de controle de acesso, registro de transações de controle de acesso físico e chaves.

Sentinela: monitora os vários sensores e ferramentas de análise de ataque, aciona especialistas em caso de incidente.

2.4. Ameaças que fragilizam a segurança na Internet

2.4.1. As ameaças

A sociedade está, cada vez mais, interligada em rede pública pela tecnologia da Internet, que possibilita acesso, em tempo real, a dados e informações armazenados em computadores, de alguma forma, abertos em rede. A partir do momento em que um computador esteja aberto na rede, para receber informações e dados, ele também está aberto para enviar informações armazenadas em sua própria memória. O ponto forte da Internet, que é a conexão em rede, pode ser também o mais vulnerável, pois abre brechas para algumas ameaças de invasões, ataques e escravização da máquina.

A ameaça, conforme KUMAR (1995), é a possibilidade potencial de que uma tentativa, desautorizada e deliberada, alcance as informações, manipule-as ou deixe o sistema não confiável e inutilizável. A segurança existe para proteger os ativos contra as ameaças, segundo PELTIER (2001).

A ameaça é composta pelos seguintes elementos (PELTIER, 2001): agente que catalisa e executa a ameaça, podendo ser um indivíduo, uma máquina ou a natureza; motivo que incentiva o agente a atuar, acidental ou intencional; e resultado que é o efeito causado pela execução da ameaça.

Segundo a SYMANTEC (2001), a ameaça pode ser dividida em três grandes categorias, ilustradas na figura 10.

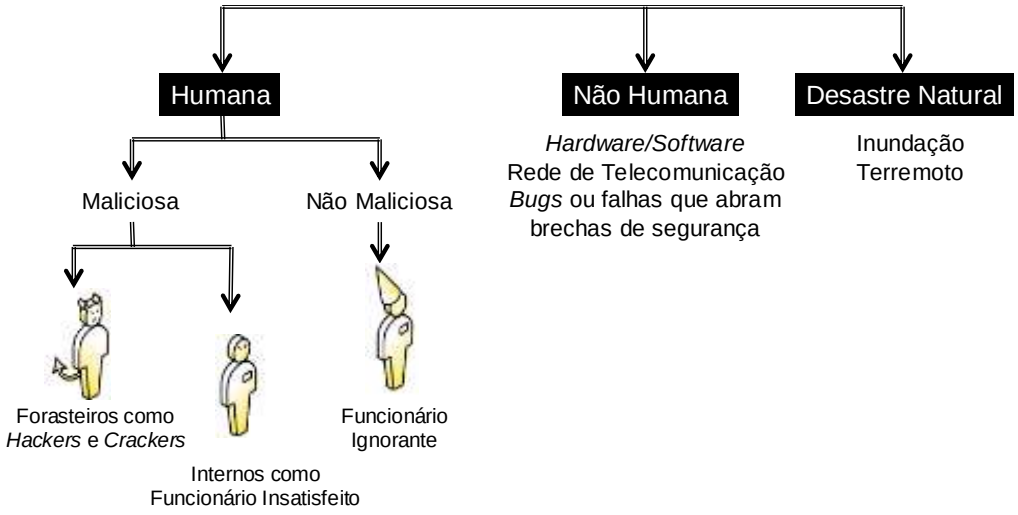


Figura 10: Categorias de ameaças
(SYMANTEC, 2001)

As ameaças estão, intrinsecamente, ligadas às vulnerabilidades. A seguir, nove eventos que tornam o sistema mais vulnerável (SYMANTEC, 2001):

1. senha fácil de ser adivinhada;
2. *software* desatualizado;
3. má administração do sistema;
4. não manter sigilo, escrevendo ou divulgando a senha, ou trafegando a senha, em claro, na Internet;
5. recursos humanos, não treinado e conscientizado sobre as ameaças de segurança;
6. rodar serviços confiáveis, em redes não confiáveis;
7. confiar em protocolos, sem autenticação;
8. confiar em coisas adquiridas de terceiros, sem checar;
9. cair em truques estúpidos de vendedores ou fornecedores.

Conforme pesquisa desenvolvida pelo coronel MCCROHAN (2003), as ameaças que rondam o mercado financeiro podem ser traduzidos nos seguintes tópicos:

- ✓ O mundo cibernético é o alvo, de espionagem e fraudes, mais comum.
- ✓ Os ataques aos centros de dados e de telecomunicação, das instituições financeiras, terão grande impacto.
- ✓ A perda de recurso humano, em algumas áreas, terá um impacto significativo.

- ✓ A tecnologia, sozinha, não resolverá o problema das ameaças.
- ✓ A gerência sênior, das áreas de tecnologia, negócios e comercial, deve estar ciente e agir em conjunto.
- ✓ Compartilhar informações, entre os bancos e os órgão ligados às instituições financeiras, é um componente crítico. Sem este compartilhamento não haverá defesa, eficiente e rápida.
- ✓ Preocupações com a "quarteirização" sem controle. Por exemplo, terceirizar o desenvolvimento de *software* com uma empresa da Índia, e esta empresa indiana "quarterizar" o serviço com empresas da China ou do Oriente Médio, sem o conhecimento da empresa compradora do serviço.
- ✓ Sofisticação dos *hackers*, da Eurasia e do Brasil, continua a crescer.

A Internet propiciou o surgimento de um novo ambiente digital de relacionamento, entre o banco e seus clientes, sendo que, neste ambiente há também ameaças de fraudes e crimes. SCHNEIER (2001, p. 27) afirma: "As ameaças do mundo digital espelham as ameaças do mundo físico."

2.4.2. As invasões

A invasão é baseada em uma violação da política de segurança do sistema. A política de segurança deve definir os objetivos a serem atingidos, traduzindo-os em um conjunto bem definido de ações. A ruptura da política de segurança caracteriza a violação (KUMAR, 1995).

A invasão pode se dividida em seis tipos, conforme SMAHA (1988):

1. Tentativa de arrombamento: detectado, freqüentemente, por perfis atípicos ou por violações atípicas das restrições de segurança.
2. Ataque mascarado: também detectado, freqüentemente, por perfis atípicos ou por violações atípicas das restrições de segurança.
3. Penetração no sistema de controle de segurança: detectado, geralmente, pelo monitoramento de padrões específicos da atividade.
4. Vazamento: detectado, freqüentemente, pelo uso atípico de recursos.

5. Negação de serviço ou DoS (*Denial of Service*): detectado, freqüentemente, pelo uso atípico de recursos de sistema.
6. Uso malicioso: detectado, freqüentemente, por perfis atípicos de comportamento, por violações de restrições da segurança, ou por uso de privilégios especiais.

2.4.3. Tipos de crimes eletrônicos

A segurança da Internet e da rede pública é fragilizada com o crescente aumento de crimes eletrônicos. O impacto destes crimes, muitas vezes, não é mensurado, porque nunca foram detectados ou reportados. Segundo WADLOW (2000, p. 40): "Saber que está sendo atacado representa mais da metade da batalha." Os crimes podem ocorrer com um computador atacando um ou vários computadores, ou um computador escravizando vários computadores que são utilizados, involuntariamente, para atacar outro (KRUTZ; VINES, 2001).

Os crimes digitais, que englobam invasões, ataques, disseminações de vírus, spams, entre outras atividades consideradas, custaram, aproximadamente, US$ 666 milhões às empresas norte-americanas em 2003, segundo pesquisa conduzida pela revista CSO (*Chief Security Officer*) (2004), com apoio do Serviço Secreto dos Estados Unidos e do *CERT Coordination Center*, da Universidade de Carnegie Mellon. Esta pesquisa foi realizada com empresas de diversos setores, sendo 13%, instituições financeiras. As perdas se concentraram em operacionais, com 56%, e financeiras, 25%. As tecnologias mais utilizadas para combater os crimes foram: *firewalls*, 98% das empresas, seguidos por sistemas de segurança física (94%), gerenciamento manual de correções de sistemas (91%), criptografia de dados críticos trafegados (63%) e armazenados (56%). Dentro dos processos de segurança, a auditoria é listada como o método mais eficiente por 51%, seguidos de contratação de executivos de segurança (CSO), testes periódicos de penetração no sistema, monitoramento das conexões de Internet e avaliação periódica dos riscos, indicados por mais de 45% dos participantes da pesquisa.

A seguir, lista com os tipos de crimes mais comum na Internet, descritos por KRUTZ; VINES (2001) e HARRIS (2002):

- ✓ *Denial of Service* (DoS): sobrecarregar o servidor de um banco para indisponibilizar serviços e informações, caracterizando um ataque de negação de serviço.

- ✓ Engenharia social: usar a habilidade social para conseguir informações privilegiadas.

- ✓ Códigos maliciosos: vírus, cavalos de Tróia e vermes que causam DoS, destruição ou modificação de informações.

- ✓ *Spoofing* de endereço IP ou de e-mail: forjar o endereço IP de um *website* para dar aparência de um *website* oficial de algum banco. Por exemplo, forjar o endereço de remetente de e-mail para dar credibilidade a um SPAM ou a um *HOAX*.

- ✓ *Sniffing* de senhas: captura de informações que trafegam na rede. O mais comum é a busca de senha não encriptadas.

- ✓ *HOAX:* mensagem falsa sobre vírus ou, mais usualmente, de promoções, geralmente na forma de e-mail, com um link para um endereço que na realidade é uma armadilha para coletar senhas. Por exemplo, o endereço do *website* do banco é www.bancoX.com.br e na mensagem de e-mail enviada para os clientes o endereço falso é www.promocaobancoX.com. Este é o golpe mais comum, aplicado pelos *hackers*, para colher informações de usuário e senha de Internet Banking.

- ✓ *Phishing and scam*: e-mail que, aparentemente, foi enviado por uma entidade legitimada na Internet, porém, com intuito de enganar e coletar dados pessoais ou informações de senha bancária.

- ✓ Pirataria: copiar *software*s privados sem licença de uso.

2.4.4. Tipos de fraudes em Internet Banking

O Internet Banking possui duas partes principais que atuam nas transações: uma parte é o banco, a outra, o cliente. A ponta mais frágil no relacionamento, via Internet Banking, é o cliente, portanto, os criminosos concentram os seus esforços em ameaçar, atacar e fraudar o cliente do banco. A mira das fraudes, portanto, está centrada no cliente.

A seguir, tipos de fraudes que mais ocorrem, via Internet Banking, conforme NIC BR (2003):

1. O cliente recebe um *e-mail*, ou ligação telefônica, de um suposto funcionário do banco, e neste *e-mail* ou ligação o cliente é persuadido a fornecer informações sigilosas, como senhas de acesso ou número de cartões de crédito.

2. O cliente recebe um *e-mail*, cujo remetente pode ser um suposto funcionário, gerente, ou até mesmo uma pessoa conhecida, sendo que, este *e-mail* contém um programa anexado. Este programa pode capturar as informações digitadas no teclado; obter as posições do cursor na tela e a tela apresentada no monitor; ou controlar o *webcam* e enviar imagens coletadas.

3. O criminoso redireciona todos os acessos ao Internet Banking para um *website* falsificado, semelhante ao *website* do banco. Desta forma, ele pode monitorar todas as ações do cliente, incluindo, por exemplo, a digitação de sua senha ou do número de seu cartão de crédito. É importante ressaltar que nesta situação, normalmente, o cliente aceitou um novo certificado do *website* falso e o endereço do *website* pode ser diferente do endereço do *website* do banco.

4. O cliente pode ser persuadido a acessar o *website* do banco, por meio de um *link* recebido por *e-mail*, ou em uma página de terceiros. Este *link* pode direcionar o cliente para um *website* falso, semelhante ao do banco. A partir daí, o criminoso monitora todas as suas ações, por exemplo, a digitação da senha bancária ou do número de seu cartão de crédito.

5. O cliente, ao utilizar computadores de terceiros para acessar o Internet Banking, pode ter todas as suas ações monitoradas, por programas especificamente desenvolvidos para este fim.

É importante ressaltar que nos tipos de fraudes 3 e 4, normalmente, o cliente aceitou um novo certificado do *website* falso e o endereço do *website* pode ser diferente do endereço do *website* do banco.

2.4.5. As qualidades que impulsionam o ataque

A segurança na Internet pode ser quebrada quando um atacante, ou mais, dispuser de habilidade, motivação e oportunidade suficientes (WADLOW, 2000).

A habilidade do atacante pode ser classificada em: geral ou personalizada. A habilidade geral é o conhecimento básico que o profissional técnico de Internet possui, e pode ser combatida com a instalação adequada dos aplicativos e suas prováveis correções ou *patches* (ajuste de um pequeno defeito no programa), reduzindo, ao mínimo, o número de entradas dos sistemas e atualizando-os, conforme o estado-da-arte em medidas de segurança. Por outro lado, a habilidade personalizada representa o conhecimento de uma rede específica, cuja configuração ou arquitetura contenha recursos não padronizados pelos *softwares*, aplicativos ou *hardwares*.

A motivação que ameaça a segurança é gerada por três fatores: primeiro, a satisfação em invadir um sistema após uma “luta” insistente, interessante e/ou lucrativa. A forma de se defender deste fator é impedir qualquer tipo de satisfação do invasor e maximizar o nível de frustração, em caso de invasão, como a baixa lucratividade. Segundo, a tenacidade em continuar investindo tempo e paciência em tentativas frustradas de invasão, ou a grande quantidade de etapas que o invasor deve percorrer até atingir seu alvo principal. E o terceiro, corresponde ao ego que pode ser despertado quando o ataque tem valor pessoal, ou se o atacante, em algum momento, se sentir caçoado pelo sistema, aumentando, assim, o seu empenho em invadi-lo.

A oportunidade pode ser interpretada como um meio de acesso a uma rede que poderá ser operada ou danificada pelo atacante. Este risco pode ser minimizado com as seguintes providências: parcimônia em oferecer o mínimo possível de oportunidades, por meio de uma configuração e arquitetura do sistema enxuto, o suficiente para operar de forma ótima, porém, sem instalações ou aplicativos supérfluos que possam gerar brechas de segurança; justificativa para acessar o sistema de fora, ou por terceiros ou estranhos ao sistema; perfeição em manter o estado-da-arte em medidas de segurança, através de atualizações constantes; atenção para detectar qualquer violação ao sistema e notificar as pessoas competentes; e, por fim, robustez em reproduzir, no sistema inteiro, limitações pontuais.

2.5. Camadas de segurança da Internet

A gestão de segurança de um canal de relacionamento, como o Internet Banking, envolve diversas áreas e uma gama vasta de desafios multidisciplinares, dentro de um banco. O escopo de atuações para se manter um ambiente, como o da Internet, seguro, minimizando os riscos de perda de ativo e credibilidade de uma instituição financeira, é vasto, abrangendo desde a gestão de infra-estrutura tecnológica até o apelo mercadológico, a ser adotado pelo banco. Para facilitar o entendimento do panorama que abrange, a gestão de segurança pode ser classificada em três camadas – física, lógica e humana (DINIZ; PORTO; ADACHI, 2003).

A camada física é composta pelo ambiente em que os equipamentos e periféricos estão fisicamente no banco, residência ou escritório do usuário, ou ainda no espaço público de um cibercafé, escola, biblioteca. É o local onde está instalado o *hardware* – computadores, servidores, o meio de telecomunicação utilizado – linha de conexão e de transmissão (HARRIS, 2002). Uma das formas de gerir a segurança desta camada é o controle de acesso, que pode ser através de senhas, documentos ou medidas biométricas (MEIRELLES, 1994).

A camada lógica é caracterizada pelo *software*, que é um conjunto de instruções, arranjadas logicamente, para serem interpretadas e executadas por um *hardware*, necessário para usufruir toda a capacidade de processamento do computador (MEIRELLES, 1994 e ALBERTIN 2002). O *software* pode ser classificado como básico, que coordena e gerencia a utilização do sistema e de aplicativos, programas para resolver uma aplicação específica (MEIRELLES, 1994). Os programas são responsáveis por efetuar e administrar as transações realizadas na base de dados dos bancos até a encriptação e decriptação de senhas e mensagens.

A camada humana é formada pelos recursos humanos que permeiam todo o ambiente da Internet na sua execução, manutenção ou uso. Segundo SCHNEIER (2001) é o elo mais fraco na corrente da segurança, sendo, cronicamente, responsável pela falha dos sistemas de segurança. Os aspectos importantes desta camada são a percepção do risco pelas pessoas: como elas lidam com os sinistros que ocorrem raramente; se são usuários confiantes ou ignorantes no uso do computador; o perigo dos intrusos maliciosos ou ingênuos; e a engenharia social, da qual os *hackers* conseguem informações por meios lícitos (SCHNEIER,

2001). Esta camada engloba, além dos recursos humanos da empresa e do usuário final, os processos operacionais, a política de segurança adotada pelo banco e a conscientização e treinamento destes recursos humanos (HARRIS, 2002).

A segurança no Internet Banking é a soma das três camadas, que se permeiam e geram um ambiente de negócio aberto em rede. A gestão destas camadas pode ser feita de diversas formas: centralizada, por camada e especialidade; interdisciplinar, que atinge mais de uma camada e por processos, que permeiam um item como cadastramento de usuário e acesso final. A idéia central da divisão por camadas é categorizar os temas, ou domínios a serem abordados, em uma gestão de segurança.

A definição de como será o acesso ao Internet Banking, pelo usuário final, envolve desde o local em que o computador se encontra, residência, estabelecimento público ou escritório; a qualidade de segurança do ambiente do usuário (camada física) até o tipo de encriptação/decriptação a ser utilizada (camada lógica) e o fluxo e os tipos de validação utilizados no processo de cadastrar e acessar o banco, via Internet Banking (camada humana).

A visão por camadas auxilia a gestão de segurança, uma vez que define o tipo de expertise que cada profissional deve ter, ao atuar em uma ou mais camadas. A gestão de segurança do Internet Banking requer um profissional multidisciplinar, que seja capacitado a enxergar o todo de forma coerente, para tomar as melhores decisões, que harmonizem as forças técnicas com as forças de negócio, em busca de sinergia e qualidade do canal Internet Banking.

2.5.1. A camada física

A camada física representa o ambiente em que se encontram os computadores e seus periféricos, bem como a rede de telecomunicação com seus *modems*, cabos e a memória física, armazenada em disquetes, fitas ou CDs. Esta camada está presente em todo o processo de conexão: o banco, com seu ambiente de desenvolvimento e de produção; o cliente, com seu computador e conexão doméstica ou corporativa e o meio de comunicação, em si, representado por cabos ou ondas.

> *"A segurança física é uma parte importante da segurança global da rede, mas é um dos aspectos mais mal compreendidos da segurança de rede. Com muita freqüência, a imagem associada à segurança física é semelhante àquela mostrada no filme Missão Impossível, no qual uma equipe de agentes se infiltra furtivamente em um centro de computadores (...)"*
> (WADLOW, 2000, p. 98)

Esta camada sofre as seguintes ameaças, no lado do banco, conforme descrito por WADLOW (2000):

- ✓ Funcionário manipulando de forma errada ou indevidamente o equipamento;
- ✓ Acesso impróprio às mídias de *back-up*;
- ✓ Desligar ou desconectar, acidentalmente, o equipamento de produção;
- ✓ Problemas ou não mensuração da capacidade de energia elétrica, necessária para alimentar o equipamento de produção;
- ✓ Falta de energia e de equipamento de *no-break*;
- ✓ Danos causados por água, como enchente, alagamento ou extintor de incêndio, como *sprinkler* disparado, acidentalmente;
- ✓ Roubo.

O cliente do banco sofre outros tipos de ameaças, detectadas nas campanhas de segurança de Internet Banking, divulgadas pelo BankBoston e HSBC:

- ✓ Não utilizar computadores comunitários ou de terceiros, como os do cibercafé;
- ✓ Evitar acessar o Internet Banking em ambiente público, onde uma outra pessoa possa gravar seus dados e sua senha bancária.

A Fundação Internacional de Segurança da Informação classifica as ameaças físicas no meio eletrônico:

> *"Physical threats to information systems fall into two broad categories: extreme environmental events and adverse physical plant conditions. Extreme environmental events include earthquake, fire, flood, electrical storms, and excessive heat and humidity. The information system may be housed in a building, in which, in addition to computers and communication lines located throughout the building, there may be dedicated computer rooms and data storage rooms. Connections for power supply and communication may lead to and from the building. Adverse physical plant conditions may arise from breach of physical security measures, power failures or surges, air conditioning malfunction, water leaks, static electricity and dust. An organization may be affected by lapses either*

> *directly at its premises or indirectly at a vital point outside the organization, such as power supply or telecommunication channels."* [21]
> (*INTERNATIONAL INFORMATION SECURITY FOUNDATION*, 1999, p. 52)

As questões importantes de segurança desta camada, são, segundo WADLOW (2000):

- ✓ Controle de acesso ao ambiente em que se encontram as máquinas, computadores e mídias com dados;
- ✓ Níveis de acesso às áreas de alta segurança;
- ✓ Registro de acesso;
- ✓ Administração de visitante;
- ✓ Prevenção contra incêndio;
- ✓ Acesso indevido ao computador do cliente.

A arquitetura e modelos de segurança, os sistemas de controle de acesso e a segurança em telecomunicação e redes são os componentes principais desta camada. Sendo que, o controle de acesso para o usuário final, cliente do banco, é a parte mais conhecida, devido ao processo de cadastramento e acesso ao Internet Banking.

BANKS (2001), a seguir, argumenta que a segurança desta camada deve ser "robusta o suficiente" para evitar sinistro, mas não tão rígida que inviabilize o canal.

> *"Security design must achieve at least two broad goals simultaneously: it must be sufficiently robust to prevent unauthorized Access to, or release of, information, but not so complex that it renders the website inefficient."* [22]
> (BANKS, 2001, p. 12)

[21] As ameaças físicas aos sistemas de informação caem em duas grandes categorias: eventos ambientais extremos e condições físicas adversas da planta. Os eventos ambientais extremos incluem terremoto, incêndio, inundação, tempestades elétricas, calor e umidade excessivos. O sistema de informação pode ser abrigado em um edifício, em que, além dos computadores e das linhas de comunicação situados ao longo do edifício, pode haver salas exclusivas de computadores e armazenamento de dados. Conexões para provisão de energia e comunicação podem sair ou entrar no edifício. As condições físicas adversas da planta podem surgir de brechas nas medidas de segurança física, falha elétrica ou aumento de voltagem, mau funcionamento do ar condicionado, vazamento de água, eletricidade estática e pó. Uma organização pode ser afetada por problemas diretamente em suas instalações ou indiretamente, em um ponto vital fora da organização, tal como fonte de energia ou canais de telecomunicação. (tradução nossa)

[22] O projeto da segurança deve atingir, ao menos, dois grandes objetivos, simultaneamente: deve ser suficientemente robusto para prevenir acesso ou liberação desautorizada da informação, mas não tão complexo que torne o website ineficiente. (tradução nossa)

2.5.2. A camada lógica

A camada lógica é composta por programas e aplicativos que podemos denominar *softwares.* Esta camada é o "cérebro" do Internet Banking, na qual estão as regras, normas, protocolo de comunicação e onde, efetivamente, ocorrem as transações e consultas.

Software é um programa ou conjunto de instruções e dados que comandam o *hardware* FORESTER (1987). Instruções do que, como e quando realizar alguma tarefa específica HUTCHINSON e SAWYER (1988). Pode ser dividido em duas grandes categorias: *software* de sistema ou de aplicação. O de sistema é composto de programas que não realizam tarefas específicas, ele controla, integra e gerencia os componentes do *hardware*. Faz parte desta categoria o sistema operacional, gerenciador de arquivos, rede de comunicação, gerenciador de ferramentas e controle de dispositivos. O de aplicação, por outro lado, realiza tarefas específicas, e pode consistir em um único programa ou em uma coletânea pequena ou grande de programas, como o pacote *Office* da *Microsoft*.

O banco, geralmente, possui os seus dados e aplicativos transacionais em *mainframe* (alta plataforma), onde o acesso é restrito, por não ser conectado diretamente a uma rede pública. Além disso, o *mainframe* concentra as transações e consultas para todos os canais de um banco, desde a agência física até o atendimento telefônico. O Internet Banking é um aplicativo (baixa plataforma) que requisita as consultas e transações para o *mainframe*. Esta ação, na maioria das vezes, é intermediada por um *middlerange* (plataforma média), que resguarda o banco de invasões, *hackers* e negação de serviço. Todo este fluxo ocorre na camada lógica, por meio de aplicativos e sistemas.

O mundo financeiro se tornou digital, passando do dinheiro em espécie para o dinheiro digitalizado. A partir desta mudança, de físico para lógico, os avanços tecnológicos impactaram, fortemente, o mundo financeiro. O que antes era realizado por pessoas, foi migrado para as máquinas (*hardwares*), que pensam conforme foram programadas (*softwares*), portanto, a camada lógica está sempre sendo ameaçada e é um dos pontos focais para ataques. Os ataques, à distância, ocorrem na camada lógica, por meio de vírus, cavalos-de-tróia e e-mails maliciosos. Esta camada é um "terreno fértil" para ataques, conforme a *International Information Security Foundation*:

> *"Computer programs are an important element of information systems and a potentially fertile terrain for threats to information systems. A program containing a virus that is introduced into an information system may affect the availability, confidentiality and integrity (...) Disclosure of proprietary information may damage an organization's competitive position."* [23]
> (*INTERNATIONAL INFORMATION SECURITY FOUNDATION*, 1999, p. 53)

Nesta camada, conforme o guia desenvolvido pela *Interpol* sobre segurança e métodos de prevenção de crimes de TI (INTERPOL, 2000), podem ser implantadas as seguintes medidas de precauções, do lado do banco:

- ✓ Registro (*log*) de quem, quando, o que e onde foi realizado um evento (este dado é o material mais importante em uma investigação);
- ✓ *Back-up* dos dados e redundância dos sistemas e aplicativos;
- ✓ *Firewall* para filtrar as informações que entram e saem;
- ✓ Sistema para detectar intrusão nos sistemas e programas.

Do outro lado, o cliente se previne das seguintes formas:

- ✓ Usar navegadores (*browser*) homologados pelo banco;
- ✓ Instalar e atualizar, constantemente, o sistema de *firewall* e de antivírus;
- ✓ Manter atualizado os aplicativos com as correções (*patches*) sugeridas pelos fornecedores idôneos de *softwares*;
- ✓ Não instalar no computador programas suspeitos.

Na camada lógica ocorrem três grandes categorias de ações: leitura, criação e modificação de *software* e de dados do sistema; transporte por meio da rede de comunicação privada ou pública, e mídias como CD ou disquete; armazenamento dos dados e das informações (INTERPOL, 2000). Em cada uma destas categorias existem ameaças, como: corrompimento do *software*, na primeira, manipulação indevida dos dados, no transporte, e perda de dados, no armazenamento.

[23] Programas de computadores são elementos importantes no sistema de informação e um terreno fértil para ameaças aos sistemas de informação. Um programa que contenha vírus introduzido no sistema de informação pode afetar a sua disponibilidade, confidencialidade e integridade. (...) A revelação de informações privadas pode danificar a posição competitiva da organização. (tradução nossa)

2.5.3. A camada humana

A camada humana é composta pelo recurso humano, envolvido no processo global do Internet Banking, desde o analista responsável pela programação técnica; o operacional, que cuida da infra-estrutura; a gerência e diretoria, que administram o canal; até o cliente, seu usuário final. Das três camadas, esta é a mais difícil de se avaliar os riscos e gerenciar a segurança, pois envolve o fator humano, com características psicológicas, sócio-culturais e emocionais, que variam de forma individual (SCHNEIER, 2001). A primeira impressão que se tem ao mencionar segurança, em Internet Banking, é que este assunto pertence ao mundo de tecnologia, mas, conforme WADLOW (2000, p. 92): "A segurança é um problema que envolve pessoas e não tecnologia".

Ao analisar a literatura sobre segurança, de forma geral, o fator humano é um dos principais agentes responsáveis por acidentes (LEVESON, 1995). Muitas tarefas humanas, realizadas por pessoas, estão sendo, cada vez mais, substituídas por máquinas, *softwares* e *hardwares*, isto ocorre por interesse relacionado à economia de custos, ganho em escala, necessidade de gerenciamento e também para minimizar os riscos de erros ou falhas humanas. Todavia, em todos os processos, sempre haverá um recurso humano, podendo ser desde o criador até o usuário final.

HEALY e WALSH (1979) apontam que a conscientização sobre a segurança é desejada pela organização. Primeiro, a segurança afeta todos os funcionários, de forma restrita ou não; segundo, ela afeta o desempenho e as negociações coletivas, pois a organização e os funcionários podem sofrer processos legais ou de pequenas causas devido à conseqüência de algum sinistro; terceiro, impacta a alta gerência, envolvida com este aspecto da empresa; e por fim, afeta o processo de seleção, porque a maioria dos problemas de segurança é gerada pelo recurso humano interno.

WADLOW (2000) descreveu três qualidades que podem levar uma pessoa a atacar um sistema: habilidade, motivação e oportunidade. Os funcionários da empresa possuem duas das três qualidades: habilidade e oportunidade, basta ter uma motivação para ameaçar, invadir, fraudar ou roubar, quebrando a segurança da empresa. Desta forma, o processo e as condições de contratação de recursos humanos, internos ou externos, deve ser rigoroso, seguindo a política de segurança elaborada pela empresa. Uma política de segurança clara, largamente

disseminada e incutida em todos os recursos humanos, é importante para zelar pela segurança da empresa e de seus clientes. Além disso, é importante que na política de segurança sejam discriminadas as penalidades, conforme infrações, e que elas sejam efetivamente executadas, conforme julgamento de um conselho de análise de incidentes.

O *hacker*, Kevin Mitnick, preso em 1995 por ter invadido diversos sistemas de informação, tinha como um dos maiores trunfos a engenharia social. A engenharia social consiste em fingir ser uma pessoa que você não é para levantar informações, como por exemplo, entrar em contato com uma pessoa de uma organização e fingir ser funcionário de uma empresa terceirizada para obter alguns dados privilegiados. O *hacker* entendia, obviamente, de tecnologia e telecomunicação, porém, o seu ponto forte era a arte de enganar as pessoas para ganhar a sua confiança e depois utilizar as informações coletadas para fins ilícitos (MITNICK; SIMON, 2003).

A engenharia social é uma ferramenta poderosa para os *hackers* descobrirem informações privilegiadas, de forma um tanto quanto simples. O combate a este tipo de ação baseia-se na conscientização, dos funcionários e terceiros, a respeito da segurança dos dados. Esta conscientização pode ser feita por meio de treinamentos periódicos dos funcionários e de empresas terceirizadas, além de campanhas internas, alertando sobre a periculosidade de algumas atitudes, aparentemente simples e ingênuas.

Os bancos aproveitaram a popularização da Internet para terceirizar parte do trabalho bancário para os clientes, ou seja, o cliente digita a sua conta a pagar, consulta seu extrato, remotamente, fazendo o trabalho que antes era do caixa ou do atendimento telefônico, minimizando erros de digitação. BANKS (2001, p. 144, tradução nossa), afirma que “o futuro do *e-finance*, invariavelmente, focará, atentamente, o ‘elemento humano’ dos serviços financeiros”.

> *"Human beings and the institutions they establish to reflect their values, whether social, economic or political, as well as the lack of such institutions, all contribute to security problems. The diversity of system users – employees, consultants, customers, competitors or the general public – and their various levels of awareness, training and interest compound the potential difficulties of providing security."* [24]
> (*INTERNATIONAL INFORMATION SECURITY FOUNDATION*, 1999, p. 53)

Outro aspecto importante de se levantar, na camada humana, é o programa de treinamento, conscientização e educação.

> *"Lack of training and follow-up about security and its importance perpetuate ignorance about proper use of information systems. Without proper training, operators and users may not be aware of the potential for harm from system misuse. Poor security practice abound. Operators and users may not take even the most rudimentary security measures."* [25] (GASSP, 1999, p. 53)

[24] Seres humanos e as instituições que eles estabelecem para refletir seus valores, sejam sociais, econômicos ou políticos, bem como a falta de tais instituições, tudo contribui para os problemas de segurança. A diversidade de usuários dos sistemas – empregados, consultores, clientes, concorrentes ou público em geral – e seus vários níveis de conscientização, treinamento e interesse compõem as dificuldades potenciais para prover segurança. (tradução nossa)

[25] A falta de treinamento e acompanhamento sobre segurança e sua importância perpetua a ignorância sobre o uso apropriado de sistemas de informação. Sem treinamento adequado, os operadores e usuários não podem estar cientes do potencial de dano do emprego incorreto do sistema. A prática pobre da segurança é comum. Os operadores e usuários podem não tomar, nem sequer as medidas mais rudimentares de segurança. (tradução nossa)

2.6. Os 10 domínios

A restrição de profissionais capacitados para gerir a segurança dos sistemas de informação, de forma holística (abrangendo conhecimento técnico, processual, administrativo e de negócio), inspirou a criação do consórcio internacional de certificação de profissionais de segurança de sistema de informação (ISC)² (*International Information Systems Security Certifications Consortium, Inc.*), em 1986. Este consórcio definiu um corpo de conhecimento geral, desde a terminologia a ser aplicada na área de segurança até os dez domínios que o conhecimento de segurança deve abranger (KRUTZ; VINES, 2001). O certificado CISSP (*Certified Information Systems Security Professional*) é a forma de comprovar que um profissional tem conhecimento geral suficiente para fazer a gestão de segurança de um sistema de informação, como o Internet Banking, por exemplo. A certificação abrange todas as áreas envolvidas com segurança em sistema de informação, divididas em 10 domínios (HARRIS, 2002).

Os dez domínios foram descritos e classificados em camadas, para facilitar a compreensão do papel de cada profissional envolvido na gestão de segurança. A classificação foi realizada com base no julgamento da autora deste trabalho, dando ênfase à camada mais influente dentro de cada domínio. A maioria dos domínios possui características de mais de uma camada, porém, na classificação, as características predominantes foram as razões decisivas para a classificação. O escopo de cada domínio foi extraído dos textos de HARRIS (2002) e KRUTZ; VINES (2001), já as classificações em camadas foram realizadas pela autora deste trabalho.

Tabela 5: A abrangência de cada um dos 10 domínios

Domínio	Escopo	Camada
1. Arquitetura e modelos de segurança	– Define a política, a arquitetura e a metodologia de segurança, para depois implementar e comparar com critérios iniciais, para mensurar a aderência entre o planejado e o realizado. – A arquitetura compõe-se de todas as partes do sistema computacional, como sistema operacional, memória, circuitos, discos rígidos, componentes de segurança, canais e componentes de rede. – Escolha de modelos de segurança, como Bell-LaPAdula, que protege a confidencialidade dentro do sistema; Biba, que protege a integridade dentro do sistema; Clark-Wilson, que previne usuários autorizados a realizar ações fora da sua alçada.	**Física**
2. Sistemas de controle de acesso	– Define, monitora e controla as políticas e procedimentos de acesso, bem como promove treinamento e conscientização sobre o acesso seguro aos sistemas, dados e informações. – Define a metodologia de acesso por meio de senhas, documentos digitais, *smart cards*, medidas biométricas ou qualquer outro mecanismo de autenticidade.	**Física**
3. Segurança em telecomunicação e redes	– Elabora e monitora a segurança de comunicação dos sistemas analógicos, digitais, ou *wireless*, em meio físico ou aéreo, que transmitem voz, dados e imagens em um local restrito ou público, de forma remota ou local. – Previne ataques, detecta intrusos e corrige erros, para manter a integridade, confidencialidade e disponibilidade da comunicação. – Define e monitora os filtros de acesso (*firewall*), roteadores, portas de acesso e protocolos da Internet, Extranet e Intranet. – Administra o uso dos diversos protocolos (TCP/IP, PAP, SMTP, PPP), que são um conjunto de regras padronizadas que ditam como os computadores se comunicarão na rede. – Elabora e controla a segurança e capacidade da infra-estrutura de comunicação.	**Física**
4. Segurança física	– Controla, administrativamente, tecnicamente e fisicamente a segurança física dos recursos e informações sensíveis. – Gerencia a segurança, controla as ameaças e define as medidas preventivas que protegem o ativo físico, como o espaço, a construção e os equipamentos. – Autentica indivíduos e detecta invasores.	**Física**

Domínio	Escopo	Camada
5. Desenvolvimento de sistemas e aplicativos	– Gerencia os diversos tipos de *softwares* de controle e as suas implementações. – Cria e administra os bancos de dados e cerca-os de segurança, para evitar problemas. – Administra o ciclo de vida dos processos de desenvolvimento i. Estudo e definição do projeto; ii. Planejamento, análise e desenho das funcionalidades; iii. Especificação do desenho do sistema; iv. Desenvolvimento do *software*; v. Instalação; vi. Manutenção e suporte; vii. Revisão e substituição).	**Lógica**
6. Criptografia	– Elabora e implementa a forma de encriptar e decriptar dados, informações e senhas, para que a mensagem siga de forma confidencial, íntegra, e confiável e a autentica, em alguns casos. – Avalia a intensidade de segurança necessária para os diferentes tipos de funcionalidades e níveis de acesso. – Desenvolve a encriptação simétrica ou assimétrica, com ou sem assinatura digital, com ou sem função *hash*, para garantir a integridade da mensagem.	**Lógica**
7. Práticas de gerenciamento de segurança	– Desenvolve a política dos padrões, guias e procedimentos de segurança. – Promove a conscientização, educação e treinamento sobre segurança. – Gerencia o risco. – Define e monitora o papel e as responsabilidades da administração de segurança.	**Humana**
8. Segurança de operação	– Mantém as soluções implementadas e os sistemas, monitora as mudanças, institui padrões necessários e segue as práticas e tarefas de segurança. – Gerencia a administração da segurança das operações, principalmente os recursos humanos envolvidos, para que uma única pessoa não possa comprometer os ativos e a imagem da empresa. – Auditora os registros operacionais e monitora os problemas.	**Humana**
9. Legislação, investigação e ética	– Conhece e compreende como se aplicam as leis para crimes em ambiente eletrônico, como se detecta se houve crime, como se preserva as evidências, os princípios básicos de conduta e investigação e as obrigações perante a lei. – Conhece e age conforme a ética.	**Humana**

Domínio	Escopo	Camada
10. Plano de continuidade do negócio e plano de recuperação em caso de desastre	– Analisa o impacto no negócio, nas operações e na contabilidade, em casos de desastre natural ou falhas humanas. – Seleciona, desenvolve e implementa planos de contingência e de desastre. – Responde pelo *back-up* e site de contingência, fora da organização.	**Humana**

3. Metodologia

3.1. Método de Estudo de Casos Múltiplos

A parte empírica deste trabalho foi realizada por meio do método de Estudo de Caso, nos moldes propostos por YIN (1994). Este método pode ser realizado pela análise de um caso único ou de múltiplos casos. A autora optou pelo estudo de múltiplos casos, para checar e fortalecer as evidências por meio da replicação da análise, em diferentes contextos.

O estudo de caso é inserido no grupo de métodos qualitativos, com o objetivo de ampliar o foco de compreensão dos fatos, em detrimento da sua mensuração (LAZZARINI, 1995). O método é mais apropriado à fase exploratória da pesquisa, na qual se busca formular teorias, a partir de uma visão mais contextual e abrangente do fenômeno (BONOMA, 1985).

O método de estudo de caso tem se revelado capaz de empregar diferentes tipos de evidências empíricas, além de ser usado para testar teorias (EISENHARDT, 1989). Esta metodologia pode ser usada para diversos propósitos de pesquisa, da fase exploratória ao teste, desde que atenda a três condições de aplicabilidade (YIN, 1994):

1. Quanto ao tipo de questão empregada na pesquisa. Segundo YIN (1994), o método de estudo de caso é indicado para responder questões de natureza explanatória, do tipo "como?" e "por que?".

2. Quanto ao grau de controle do pesquisador sobre o evento estudado. O estudo de caso é indicado quando o pesquisador não tem controle sobre o evento estudado, não podendo, assim, manipulá-lo ou reproduzi-lo fora do seu contexto original.

3. Quanto ao foco temporal. O estudo de caso é aplicável para examinar eventos contemporâneos à pesquisa, não sendo apropriado para examinar eventos históricos.

Quanto à aplicabilidade do método de estudo de caso, neste trabalho, pode-se afirmar que as condições, levantadas por YIN (1994), foram atendidas:

1. O estudo proposto pela autora visou responder questões explanatórias sobre a forma de gestão de segurança, usando como guia os “10 domínios”.

2. O objeto da pesquisa não é reproduzível fora do seu contexto.

3. A segurança em Internet é um fenômeno contemporâneo.

Na definição de YIN, o estudo de caso é:

> *"(...) uma pesquisa empírica que investiga um fenômeno contemporâneo dentro do seu contexto real, especialmente quando as fronteiras entre esse fenômeno e o seu contexto não são claramente evidentes."*
> (YIN, 1994, p. 13)

As evidências levantadas pelo estudo de caso múltiplo, conforme YIN (1994), são consideradas mais fortes do que o estudo de caso único. O estudo de casos múltiplos é considerado mais “robusto”, pois há a possibilidade de checar e fortalecer as evidências, por meio da replicação da análise, em diferentes contextos.

A opção pelo estudo de casos múltiplos se justifica pelo fato deste trabalho não tratar de uma teoria estruturada e pronta, que se queira provar, testar. Apesar da dificuldade das organizações bancárias tratarem este assunto de forma pública, três bancos, representativos, se propuseram a participar do estudo e nenhum deles possui, isoladamente, caráter revelador.

A parte empírica deste estudo constituir-se-á da análise da gestão de segurança de três bancos representativos.

3.2. Amostra

O universo de tipos de instituições financeiras, existentes no Brasil, é vasto, e o escopo de montagem da amostra é:

- ✓ Banco Múltiplo
- ✓ Banco Comercial
- ✓ Caixa Econômica

A amostra previu o estudo de casos de bancos com controles acionários distintos. A seguir, os tipos de controle acionário existentes no setor financeiro brasileiro:

- ✓ Público federal
- ✓ Público estadual
- ✓ Público nacional
- ✓ Privado nacional
- ✓ Privado com controle estrangeiro
- ✓ Privado com participação estrangeira

No levantamento da amostra, foram relacionadas instituições financeiras para cada tipo de controle acionário. Por restrição de acesso às áreas que cuidam, especificamente, de segurança, foram abordados apenas seis bancos, com os seguintes controles acionários: dois privados nacionais, dois privados de controle estrangeiro, um público federal e um público nacional. Destes, apenas três, de controles acionários distintos, retornaram o questionário: um público federal, um privado nacional e um privado com controle estrangeiro. As empresas, no trabalho, serão denominadas de: banco A no caso do banco privado de controle estrangeiro; banco B o privado nacional; e banco C o público federal.

Dada a complexidade em acessar os profissionais responsáveis pela área de segurança dos bancos e convencê-los a abrir informações sensíveis à estratégia das organizações, e ao tamanho do mercado bancário no Brasil, a escolha de apenas três casos excluiu instituições relevantes, que seriam dignas de análise. Contudo, operacionalmente, analisar mais casos seria inviável, porque o tema segurança em Internet Banking é tratado de forma sigilosa, pela maioria dos bancos.

3.3. Protocolo de pesquisa

A coleta dos dados foi realizada por meio de uma pesquisa estruturada, aplicada aos profissionais responsáveis por segurança de Internet dos bancos. O guia utilizado para o questionário foi os "10 domínios", com o qual se procurou entender como o banco se comporta em relação a cada um dos domínios.

A seguir, o guia para a montagem do questionário:

Domínio	Escopo
1. Arquitetura e modelos de segurança	– Averiguar se o banco possui uma política de segurança. Caso afirmativo, verificar se a política foi desenvolvida pelo banco ou foi baseada em algum padrão de mercado. – Investigar a definição da arquitetura de segurança, se foi feita por uma equipe multidisciplinar ou pela área técnica, apenas. – Levantar como é a gestão da arquitetura e da política de segurança, bem como o perfil dos profissionais envolvidos neste domínio.
2. Sistemas de controle de acesso	– Verificar quais são os pontos de acesso controlados no fluxo completo do Internet Banking. – Desenhar como são os controles e a administração das senhas e alçadas. – Levantar como é a gestão dos sistemas de controle de acesso, bem como o perfil dos profissionais envolvidos neste domínio.
3. Segurança em telecomunicação e redes	– Identificar o papel do gestor de negócio dentro deste domínio, caso haja. – Descobrir se as alçadas de decisão, dentro do domínio, são da área técnica, apenas, ou são colegiadas com a área de negócios. – Levantar como é a gestão de segurança em telecomunicação e redes, e verificar se este domínio é tratado apenas pela equipe técnica.
4. Segurança física	– Investigar se há uma preocupação com a segurança dos espaços físicos, onde estão as máquinas, e se há cofres ou política de armazenamento das mídias com as informações sigilosas. – Investigar como é a gestão de segurança física, bem como o perfil dos profissionais envolvidos neste domínio.
5. Desenvolvimento de sistemas e aplicativos	– Compreender o grau de envolvimento da área de negócios neste domínio. – Descobrir se as decisões de compra de *software* ou terceirização de desenvolvimento são feitos de forma isolada, na seara técnica, ou a área de negócios está envolvida.

Domínio	Escopo
6. Criptografia	– Compreender o grau de envolvimento da área de negócios neste domínio. – Investigar se a definição do tipo de encriptação é feita de forma colegiada com a área de negócios, que sofrerá os impactos desta decisão no momento em que o cliente tiver acesso ao Internet Banking.
7. Práticas de gerenciamento de segurança	– Descobrir se há política de padrões, guias e procedimentos de segurança e quem são os responsáveis. – Detectar se há um trabalho de conscientização, educação e treinamento sobre segurança. – Identificar quem é responsável e como é feito o gerenciamento de risco. – Investigar se há um esquema de monitoramento da administração de segurança. – Levantar como é a gestão das práticas de gerenciamento de segurança, bem como o perfil dos profissionais envolvidos neste domínio.
8. Segurança de operação	– Identificar se há uma área específica, que cuide da parte operacional do fluxo como um todo, ou se cada passo do processo é monitorado e mantido por áreas isoladas. – Verificar se há auditoria interna e externa. – Levantar como é a gestão de segurança de operações, bem como o perfil dos profissionais envolvidos neste domínio.
9. Legislação, investigação e ética	– Verificar se os conhecimentos, legais e éticos, são compartilhados com todas as áreas envolvidas na segurança, inclusive a área técnica. – Identificar se há um guardião do histórico de sinistros, bem como material forense para análises e eventuais processos. – Levantar como é a posição do banco perante o mercado, em caso de sinistros.
10. Plano de continuidade do negócio e plano de recuperação em caso de desastre	– Levantar o perfil dos profissionais envolvidos neste domínio e se são internos ou terceiros. – Identificar se há manutenção e testes periódicos dos planos. – Verificar qual é a área responsável por este domínio.

3.4. Aplicação da pesquisa

A pesquisa foi aplicada por meio de um questionário estruturado, por se tratar de um assunto amplo e delicado. O questionário foi elaborado com base nos "10 domínios", cada domínio possui um grupo de questões que varrem o assunto, com foco em gestão de negócio. As questões estavam agrupadas por domínio, e a ordem dos temas levantados foi a seguinte: introdução da área que cuida da segurança; descrição da metodologia (padrão e modelo utilizados); os responsáveis pela área; desenho da arquitetura de segurança; desenvolvimento, manutenção e controle de acesso do canal; e, por fim, legislação e planos de contingência.

A aplicação do questionário começou por meio de uma investigação do melhor meio de abordar este tema, nos bancos. A FEBRABAN foi o canal escolhido para encabeçar a tarefa de aplicar o questionário, pois possui um comitê, do qual participam os maiores bancos, com foco na discussão e troca de experiências sobre segurança e fraude nos canais eletrônicos. O questionário sobre segurança, abordando os "10 domínios", foi enviado por meio do correio eletrônico (e-mail), para participantes deste comitê, que representam quatro bancos distintos, além de um banco ser abordado por intermédio de um executivo do setor bancário, para auxiliar a coleta de três casos distintos e significativos para o estudo.

No dia 8 de julho de 2004, o questionário foi enviado para um banco privado de controle estrangeiro, para um pré-teste da forma de abordagem. Por meio do correio eletrônico, no dia 11 de julho, o questionário retornou, com todas as questões respondidas. Outros dois bancos, privado nacional e público federal, foram abordados no dia 12 de julho de 2004 e, uma semana depois, a solicitação foi reforçada com novo e-mail, sem retorno. Outros dois bancos, público estadual e privado nacional, que participam do comitê da FEBRABAN, foram abordados, no dia 19 de julho de 2004, por meio do correio eletrônico, e, na mesma data, o banco privado nacional devolveu o questionário inteiramente preenchido. No próprio dia 19 de julho, o banco público federal foi abordado novamente, e, no dia 14 de agosto de 2004, respondeu o questionário. Por fim, no dia 26 de julho de 2004, um executivo do setor bancário enviou o questionário para o quinto banco, solicitando que o respondesse. O questionário foi respondido e devolvido no dia 10 de agosto.

Os questionários foram respondidos por gestores da área de segurança, dos bancos em que atuam, sendo que, o foco principal destes profissionais é a segurança em Internet.

4. Resultados da pesquisa

4.1. Análise descritiva dos 10 domínios

O questionário foi estruturado com base nos "10 domínios" e sua análise respeitará esta classificação. A seqüência das questões, na análise, é a mesma do questionário aplicado.

O banco privado estrangeiro será denominado **Banco A**; o banco privado nacional será tratado como **Banco B** e o banco público federal será chamado **Banco C**.

I. Práticas de gerenciamento de segurança

Os três bancos possuem uma área específica, que administra a segurança de Tecnologia de Informação. Em cada um, a área de segurança possui denominações próprias, que serão tratadas, neste trabalho, como área de segurança da informação. Nos três bancos, esta área é subordinada à hierarquia de tecnologia, e, em nenhum deles, a área de segurança da informação está ligada diretamente à presidência.

Os **Bancos A** e **B** possuem as seguintes práticas: política de segurança, plano de contingência, guia de procedimentos de segurança e plano de continuidade, em caso de incidentes ou desastres. O **Banco C** possui as mesmas práticas, com exceção do guia de procedimentos de segurança. Estas práticas, nos três bancos, foram desenvolvidas por eles próprios, sem auxílio de consultorias externas.

No **Banco A**, a política de segurança e o plano de continuidade, em caso de incidentes, foram desenvolvidos com base na experiência e expertise do banco; o guia de procedimentos de segurança e o plano de contingência foram elaborados com base no padrão ou modelo de mercado. Sendo que, o responsável pela política de segurança e pelo guia de procedimentos de segurança está vinculado à área de segurança de informação; o plano de contingência é responsabilidade da área de segurança de informação, juntamente com a área de negócios, responsável pelo Internet Banking; por fim, o plano de continuidade, em caso de incidentes ou desastres, é responsabilidade das áreas de segurança de informação e Tecnologia de Informação.

No **Banco B**, a política de segurança foi fundamentada no padrão ou modelo de mercado; o guia de procedimentos de segurança foi também baseado no padrão ou modelo de mercado, além da experiência e expertise de empresa de consultoria; o plano de contingência foi desenvolvido com base na experiência e expertise do banco e o plano de continuidade, em caso de incidentes, foi alicerçado também na experiência e expertise do banco no uso de padrão ou modelo de mercado. Sendo que, o responsável por todos estes fatores, em caso de incidentes ou desastres, é a área de tecnologia, apenas.

No **Banco C**, a política de segurança e o plano de continuidade, em caso de incidentes, foram desenvolvidos com base na experiência e expertise do banco e uso de padrão ou modelo de mercado; e o plano de contingência foi fundamentado na experiência e expertise do banco. Sendo que, as áreas responsáveis pelos planos de contingência e continuidade, em caso de incidentes, são as de Tecnologia de Informação e negócios de Internet Banking. A política de segurança é responsabilidade da área de segurança de informação ("gestão de segurança").

Existe, nos três bancos, um trabalho de conscientização, educação e treinamento sobre segurança em Tecnologia de Informação que abrange o Internet Banking, sendo que, este trabalho é contínuo, no **Banco A**, e pontual, nos **Bancos B** e **C**. No **Banco A**, a área responsável por desenvolver este trabalho é a de segurança de informação, sendo que, o trabalho de conscientização também é responsabilidade da área de recursos humanos. No **Banco B**, a conscientização e educação são responsabilidades da área de Tecnologia de Informação e o treinamento é terceirizado. No **Banco C**, a conscientização é responsabilidade da área de Tecnologia de Informação e a educação, bem como o treinamento, são responsabilidades da área de recursos humanos.

Tanto no **Banco A**, quanto no **Banco B**, há uma área que cuida, especificamente, do gerenciamento de risco do Internet Banking. No **Banco A**, esta área está subordinada à tecnologia e no **Banco B**, está vinculada a produtos que cuidam do canal.

II. Arquitetura e modelos de segurança

A arquitetura de segurança do Internet Banking dos bancos estudados foi definida pela área de tecnologia, nos três casos (**A**, **B** e **C**). No caso do **Banco B**, a área de produtos, gestora do canal Internet Banking, também participou da elaboração da arquitetura de segurança.

A área responsável pela manutenção da arquitetura de segurança do Internet Banking, no **Banco A**, é a de segurança de informação; no **Banco B**, as áreas de tecnologia e produtos é que gerenciam o canal Internet Banking; e, no **Banco C**, apenas a área de tecnologia responde pela arquitetura de segurança.

III. Sistemas de controle de acesso

Os ambientes de desenvolvimento, homologação, produção e o espaço, onde é armazenada a base de dados (mídias), possuem controle de acesso físico nos **Bancos B** e **C**. No caso do **Banco A**, apenas o ambiente de produção não tem um controle de acesso físico.

Ao se questionar quem são os responsáveis pela administração das senhas de acesso aos ambientes e base de dados do Internet Banking, o **Banco A** indicou a área de segurança de informação, e os **Bancos B** e **C**, a área de tecnologia do próprio banco. Nenhum dos bancos terceiriza esta administração ou delega a responsabilidade para a área de *help desk*, própria do banco.

A terceira questão sobre este domínio investigou a responsabilidade pela administração de alçadas de cada usuário, o que ele pode consultar, alterar, incluir ou excluir no fluxo de desenvolvimento, homologação e produção do Internet Banking. No **Banco A**, a administração de alçadas é realizada pelos superiores de cada funcionário e pelo dono da informação. Os **Bancos B** e **C** responderam que a área de tecnologia do próprio banco realiza esta administração. Em nenhum dos bancos, a área de recursos humanos interfere na administração de alçadas.

IV. Segurança física

A segurança do ambiente físico, no qual se encontram os equipamentos de produção do Internet Banking, tem, para os **Bancos A** e **B**, acesso restrito às pessoas que trabalham na produção; é controlado por crachás e senhas; registrado (nome do funcionário, horário de entrada e saída) e vigiado por câmeras e sensores. No caso do **Banco C**, o acesso ao ambiente físico é registrado (nome do funcionário, horário de entrada e saída) e vigiado por câmeras e sensores, apenas.

Nos três bancos, o responsável pelo controle do acesso físico ao ambiente de produção do Internet Banking é a área de segurança do prédio.

V. Segurança em telecomunicação e redes

As áreas envolvidas na gestão de segurança em telecomunicação e redes, usadas pelo Internet Banking, são: para o **Banco A**, a de tecnologia do próprio banco, de telecomunicação e redes terceirizados e a de segurança de informação; para o **Banco B**, apesar de ter terceirizado sua telecomunicação, a segurança é realizada pela área de tecnologia do próprio banco; no caso do **Banco C**, a área de tecnologia do próprio banco também cuida da segurança da rede de telecomunicação.

Apenas no **Banco A**, a área de negócios (que cuida do canal Internet Banking) participa na tomada de decisão sobre os riscos na gestão de segurança em telecomunicação e redes do Internet Banking.

VI. Desenvolvimento de sistemas e aplicativos

No **Banco A**, a área de negócios, responsável pelo Internet Banking, é envolvida apenas no desenho do sistema, na fase de desenvolvimento dos aplicativos do Internet Banking. Para o **Banco B**, a área de produtos, que cuida do Internet Banking, é envolvida apenas na especificação do negócio. E no **Banco C**, a área de negócios participa no desenvolvimento de sistemas e aplicativos do Internet Banking em dois momentos: na especificação do negócio e no desenvolvimento.

Nenhum dos bancos declarou que a área de negócios participa das seguintes etapas de desenvolvimento do sistema e aplicativo: decisão entre desenvolver, com recursos internos ou externos; decisão de compra de *softwares* ou pacotes de mercado; definição de requisitos da arquitetura de aplicações e de infra-estrutura; aposentadoria ou remoção e destruição dos aplicativos; testes; implantação; e pós-implantação.

VII. Criptografia

A decisão pelo tipo de padrão criptográfico, a ser utilizado no Internet Banking, não é colegiada entre as áreas de tecnologia e negócios, em nenhum dos três bancos, é apenas tecnológica:

VIII. Segurança de operação

A parte operacional do Internet Banking é realizada pelas áreas operacional e de tecnologia, nos **Bancos A** e **B**. No caso do **Banco C**, a parte operacional é realizada pelas áreas de tecnologia, infra-estrutura e logística. Nos três bancos, a área comercial não está envolvida com a parte operacional do Internet Banking.

A auditoria, nos sistemas e processos do Internet Banking, é realizada no **Banco A** por uma equipe externa. Nos **Bancos B** e **C**, por uma equipe interna.

IX. Legislação, investigação e ética

Os conhecimentos legais e éticos são compartilhados com todas as áreas envolvidas na segurança do Internet Banking, inclusive a área técnica, nos **Bancos A** e **B**. O **Banco C** não soube responder à questão.

Os três bancos estudados responderam que existe um guardião do histórico de ocorrências e material forense, para serem utilizados em futuras análises de sinistros que, porventura, ocorram no Internet Banking.

Em caso de sinistro com o Internet Banking, o **Banco A** interage com o cliente por meio das áreas: comercial; assessoria de imprensa; produto, que cuida do canal; segurança de

informação e marketing/qualidade. A interação com o mercado e com os outros bancos é feita pela área de segurança de informação.

O **Banco B**, em caso de sinistro com o Internet Banking, interage com o cliente por meio das áreas comercial e de fraudes. A assessoria de imprensa atua com o mercado e a área de fraudes atua com os outros bancos.

O **Banco C** interage com o cliente, em caso de sinistro com o Internet Banking, por meio das áreas comercial e auditoria. A comunicação com o mercado é realizada pelas áreas comercial, auditoria e assessoria de imprensa. Outros bancos são acionados pelas áreas comercial e de auditoria.

X. Plano de continuidade do negócio e plano de recuperação em caso de desastre

Os três bancos possuem um plano de continuidade do negócio e um plano de recuperação em caso de desastre, sendo que, os três responderam que realizam testes periódicos dos planos de contingência e continuidade.

Os três bancos realizam também, periodicamente, testes de estresse. E a responsabilidade por este teste é da área de tecnologia. Entretanto, para o **Banco A**, a área de negócios também é responsável pelos testes de estresse.

Os três bancos possuem sites de contingência, sendo que, o **Banco A** possui um site de contingência terceirizado e os **Bancos B** e **C** possuem sites de contingência próprios.

4.2. Análise da pesquisa por meio de camadas

4.2.1. Camada física

A camada física é composta, predominantemente, dos seguintes domínios:

- Arquitetura e modelos de segurança
- Sistemas de controle de acesso
- Segurança em telecomunicação e redes
- Segurança física

A arquitetura de segurança define como será composta toda a plataforma de *hardware* e *software*, que dará sustentação ao Internet Banking. Este domínio é uma seara exclusiva da área de tecnologia para os **Bancos A** e **C**. O **Banco B** possui uma decisão multidisciplinar, com a participação da área técnica e da área de produtos, responsável pela gestão do canal.

A definição e manutenção da arquitetura de segurança do Internet Banking interfere nos custos e investimentos do canal, decisão que compõe a gestão de segurança. Alguns impactos, para as áreas de negócios e produtos, são: crescimento da base de clientes usuários do canal (escalabilidade); fluxo de cadastramento e acesso ao canal (processo); diversificação e criação de novos produtos e serviços ofertados no canal (portfólio de produtos e serviços); rapidez e economia de custo no desenvolvimento e implementação de novos produtos e serviços (modularização de componentes).

O espaço físico, no qual ocorrem o desenvolvimento, a homologação e a produção do Internet Banking, bem como as bases de dados, possui o acesso controlado e administrado pela área de tecnologia ou de segurança de informação, nos três bancos estudados. Apenas o ambiente de desenvolvimento, no **Banco A**, não é controlado. Este ponto, na gestão de segurança, é mais coerente estar centrado nas mãos da área de tecnologia. Entretanto, a participação da área de negócios é também importante, para que a arquitetura do canal esteja alinhada com as necessidades e definições da área de negócios e produtos.

A responsabilidade pela segurança em telecomunicação e redes está centrada na área de tecnologia, nos três bancos pesquisados, sendo que, no caso do **Banco A**, a área de

negócios participa na tomada de decisão sobre os riscos. Apesar de telecomunicação e rede serem, essencialmente, assuntos técnicos, a gestão de segurança pode ser compartilhada com as áreas de negócios e produtos, para tomada de algumas decisões como terceirização ou redundância de redes com fornecedores parceiros.

A segurança física do Internet Banking é administrada pela segurança do prédio, onde estão os recursos e as informações sensíveis, nos três bancos. Eles possuem recursos de controle e registro de acesso físico sugeridos pelos modelos de segurança padrão. Este domínio é importante para zelar pela manutenção e continuidade do canal, pois os serviços e produtos são digitais, todavia, estão armazenados em algum espaço físico. Este domínio não tem um apelo estratégico forte, mas é um ponto a ser trabalhado com cuidado, pois, no ambiente físico, podem ocorrer: vazamento de informações, desconexão de cabos de energia e de rede, e as idiossincrasias dos seres humanos, que atuam neste ambiente. Uma alternativa, em caso de problemas, é o site de contingência que os três bancos já possuem.

4.2.2. Camada lógica

A camada lógica é composta, predominantemente, pelos seguintes domínios:

- Desenvolvimento de sistemas e aplicativos
- Criptografia

O desenvolvimento de sistemas e aplicativos é um domínio centrado na área de tecnologia, nos três bancos estudados, com pouco envolvimento das áreas de negócios e produtos. No ciclo de desenvolvimento, estas áreas poderiam estar mais envolvidas, para haver uma gestão, realmente, multidisciplinar, pois todas as decisões impactarão o Internet Banking e sua segurança.

A escolha do tipo de padrão criptográfico, utilizado pelo Internet Banking, não é uma decisão colegiada entre as áreas de tecnologia e negócios, nos três bancos. Este cenário impede que as áreas de negócios e produtos avaliem e decidam pelo melhor processo de cadastramento e acesso ao canal. A criptografia é um domínio importante para se definir o nível de segurança do canal, e, conseqüentemente, o grau de complexidade ou simplicidade

do processo de cadastramento e acesso. Se a segurança é alta, o canal poderá possibilitar transações de valor financeiro maior, mas, provavelmente, terá um processo complexo de cadastramento e acesso, e vice-versa. Portanto, apesar deste domínio ser técnico, gera grandes impactos no posicionamento mercadológico do Internet Banking.

4.2.3. Camada humana

Por fim, a camada humana é composta, predominantemente, pelos seguintes domínios:

- Práticas de gerenciamento de segurança
- Segurança de operação
- Legislação, investigação e ética
- Plano de continuidade do negócio e plano de recuperação em caso de desastre

A segurança em Tecnologia de Informação e do Internet Banking é importante para os bancos. Um dos indicadores desta importância é a existência, nos três bancos, de uma área que faça a gestão especificamente deste assunto, denominada, neste trabalho, segurança de informação. Há alguns anos, a área de segurança de informação não existia, na maioria dos bancos. O fato motivador para se criar uma área específica foi o *bug* do milênio, o dado ano era tratado apenas com os dois dígitos finais, em vez de quatro dígitos. O *bug* do milênio motivou a criação de metodologias e o uso das melhores práticas nos bancos. O **Banco A**, por incentivo e definição da matriz estrangeira, possui esta área desde o início da década de 90, porém, os bancos nacionais, **B** e **C**, vieram a constituir a área, nos anos 2000. Devido a este histórico do *bug* do milênio, é compreensível a área de segurança de informação estar subordinada à tecnologia, nos três bancos.

A política de segurança, o plano de contingência, o guia de procedimentos de segurança e o plano de continuidade em caso de incidentes ou desastres, nos três casos, foram desenvolvidos pelos próprios bancos, com base nos padrões de mercado, bem como na experiência e expertise do banco. Os três bancos responderam que as práticas surgiram internamente, porém, uma das referências fortes para as equipes eram as práticas publicadas nos sites, mundo afora. As primeiras práticas surgiram no mercado norte-americano, portanto, o mercado tem diversos *websites* que são referências na *world wide web* (www).

As práticas de gestão de segurança são responsabilidade, no **Banco A** e **B**, da área de tecnologia. No **Banco C**, a área de negócios é co-responsável por algumas práticas. Neste estudo de casos, não foi detectada a multidisciplinaridade na gestão das práticas de segurança, nos **Banco**s **A** e **B**.

Os três bancos estudados possuem um trabalho de conscientização, educação e treinamento sobre segurança, sendo que, apenas no **Banco A**, este trabalho é contínuo. Nele, a área de segurança da informação tem uma atuação expressiva e apoio da área de recursos humanos. Isto se deve ao fato da área existir desde o início da década de 90. Nos bancos nacionais, **B** e **C**, o trabalho é pontual, sendo que, no **Banco B**, o treinamento é terceirizado e no **C** é desenvolvido, apenas, pela área de recursos humanos. O **Banco A** tem um trabalho mais focado e contínuo porque tem que estar alinhado com as normas brasileiras e as normas da matriz estrangeira.

Os **Bancos A** e **B** possuem uma área especifica, que gerencia os riscos do Internet Banking, sendo que, no **Banco A**, esta área está subordinada à tecnologia e, no **Banco B**, está subordinada à área de produtos. Isto indica que, no **Banco B**, a gestão de segurança está mais centrada na área de negócios do canal.

A auditoria, nos sistemas e processos do Internet Banking, é realizada por equipe externa, no **Banco A**, e por equipe interna, nos **Bancos B** e **C**. Os **Bancos B** e **C**, devido ao grande porte, possuem uma estrutura interna de auditoria. O **Banco A**, que é de porte médio, prefere terceirizar a auditoria do canal, devido aos custos e, principalmente, à imparcialidade e experiência de seus parceiros.

Os conhecimentos legais e éticos são compartilhados com todas as áreas envolvidas na segurança do Internet Banking, nos três bancos. A divulgação da legislação e da ética é importante para que todos os funcionários estejam de acordo com as normas do país e da organização. No caso do **Banco A**, esta postura é reforçada pela continuidade nos trabalhos de conscientização sobre segurança.

O histórico de ocorrências de sinistros, no Internet Banking, é importante para se criar uma jurisprudência para ocorrências futuras; formando uma massa de dados para análise e simulação de situações e especificação de novas características do canal. Os três bancos

possuem este histórico e material forense para subsidiar novas decisões, em caso de sinistro ou desenho de novos produtos e serviços.

Os três bancos possuem uma estrutura para atender e comunicar o cliente, o mercado e outros bancos, em caso de sinistro. Esta estruturação demonstra o amadurecimento dos bancos em lidar com este tipo de adversidade. O **Banco A** utiliza sua área de segurança da informação para atender e comunicar o cliente, o mercado e os outros bancos, demonstrando que esta área é mais madura e disseminada, dentro da estrutura do banco, se comparada com os outros dois casos. O **Banco B** utiliza mais a sua área de fraudes, para atuar e se comunicar com o cliente e outros bancos, indicando que existe uma área apartada da de segurança da informação para cuidar dos sinistros. O **Banco C** utiliza sua estrutura de auditoria, em parceria com a área comercial, para atuar com o cliente, o mercado e os outros bancos, em caso de sinistro.

Os três bancos realizam testes periódicos dos planos de contingência e continuidade, sendo que, apenas no **Banco A**, a área de negócios tem uma participação mais efetiva. Ele possui um site de contingência terceirizado, devido aos custos de replicação de *hardware*, *software* e ambiente.

5. Considerações finais

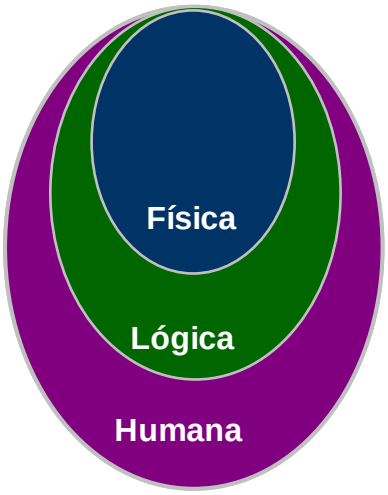
5.1. Conclusão

Discorrer e investigar a gestão de segurança de Internet Banking, dos bancos no Brasil, pode auxiliar a compreender as influências que a TI trouxe para a administração de empresa contemporânea. A tecnologia é, cada vez mais, uma das vertentes da administração, portanto, enveredar pelo tema de segurança de TI, com foco em segurança do canal eletrônico, possibilita a percepção da amplitude da disciplina de negócio, a gestão de TI.

A disseminação da Internet e, conseqüentemente, o aumento de usuários de Internet Banking, somados aos avanços da tecnologia bancária e da tecnologia de fraudes, incentivaram os bancos a definirem uma estrutura de segurança de informação. A Internet possibilitou a criação de um novo canal eletrônico, o Internet Banking, por outro lado, trouxe também preocupações sobre a sua segurança nas transações bancárias com os clientes, uma vez que o ambiente, até então restrito aos domínios do banco, se torna público, levando os bancos a reestruturarem suas áreas de segurança para suportar os riscos de atuarem na *web*. A Internet, portanto, forçou uma nova cultura de segurança, diferente das praticadas em ambiente interno fechado, do *mainframe*, da conexão privada com o cliente, das agências e demais canais interligados apenas aos computadores do banco ou de seus parceiros. A nova cultura da Internet implica em ambiente aberto, com acesso por meio de rede pública e aplicativos (*browser*) desenvolvidos por terceiros e compartilhados com os concorrentes.

A análise dos casos de gestão de Internet Banking, em três bancos brasileiros, foi feita com base nos 10 domínios, agrupados em 3 camadas: física, lógica e humana. Estas três camadas de segurança foram ordenadas, pela autora, conforme o grau de amadurecimento dos domínios nos bancos. A fundação do Internet Banking é a camada física, a infra-estrutura que suporta os produtos e serviços, transações e relacionamento entre o banco e seus clientes. A camada seguinte é a lógica, que proporciona inteligência à infra-estrutura, são os sistemas e aplicativos que, efetivamente, realizam as transações, acesso às informações e à segurança lógica. A última camada, que envolve as demais, é a humana, que abrange desde a definição da arquitetura de *hardware* até o desenho dos processos mercadológico de conquista de clientes e novos negócios.

A seguir, na figura 11, a classificação dos domínios, por camadas:



Camada Física
1.Sistemas de controle de acesso
2.Segurança em telecomunicação e redes
3.Arquitetura e modelos de segurança
4.Segurança física
Camada Lógica
5.Criptografia
6.Desenvolvimento de sistemas e aplicativos
Camada Humana
7.Práticas de gerenciamento de segurança
8.Segurança de operação
9.Plano de continuidade do negócio e plano de recuperação em caso de desastre
10.Legislação, investigação e ética

Figura 11: Os 10 domínios classificados em camadas
(elaborada pela autora)

Cada uma destas camadas sofreu uma reestruturação, para acomodar as novas necessidades de segurança que a Internet impõe. A seguir, quadro comparativo, na figura 12:

Antes da Internet	**Com a Internet**
Camada Física	**Camada Física**
1. Restrito ao ambiente controlado pelo banco	1. Acesso público e irrestrito
2. Rede privada	2. Rede pública
3. Fechada ao ambiente interno	3. Aberta e global
4. Restrito ao espaço do banco	4. Espaço múltiplo, banco, cliente, cibercafé, etc.
Camada Lógica	**Camada Lógica**
5. Tráfego interno, não necessitando deste recurso	5. Uso intenso deste recurso
6. Aplicativos próprios	6. Aplicativos de mercado
Camada Humana	**Camada Humana**
7. Ambiente interno	7. Ambiente ampliado que atinge os *stakeholders*
8. Ambiente fechado e controlado	8. Ambiente aberto com controle restrito
9. Sem meio alternativo (apenas o físico)	9. Pode ser um meio alternativo
10. Legislação e ética vigente	10. Auto regulamentado

Figura 12: Quadro comparativo dos impactos de segurança antes da Internet e com a Internet
(elaborada pela autora)

Nos três casos estudados, os bancos têm uma área específica que cuida da segurança de informação, como indicador positivo de maturidade. As camadas física e lógica são as mais bem sedimentadas, por tratarem de assuntos com soluções mais cartesianas, e estarem

concentradas na área de tecnologia, devido ao perfil dos profissionais da área técnica. A camada lógica lida com seres humanos e suas idiossincrasias, o que poderia ser um empecilho para o amadurecimento da gestão de segurança, porém, as metodologias e padrões de segurança de TI, disponíveis no mercado, auxiliam os bancos a criarem suas próprias políticas de segurança.

Os domínios das camadas física e lógica são geridos, na maior parte, pelas equipes de TI, com pouca participação da área de negócios. Esta realidade, provavelmente, é reflexo do tipo de conhecimento necessário para tomada de decisão, técnica, somado à manutenção do poder político, proveniente do alto orçamento para investimentos, que a área de TI possui em um banco. Este cenário vem se alterando, um pouco, à medida que os profissionais técnicos migram para a área de negócios, em busca de exposição, ascensão hierárquica, e melhores salários, na maioria das vezes, traduzidos em participação nos lucros ou em bônus, geralmente distribuídos apenas para as áreas comercial, de negócios e produtos. Os profissionais, que responderam o questionário, são, todos, oriundos na área de tecnologia dos bancos.

A camada humana concentra os domínios administrados pela área de segurança de informação, esta é, das camadas, a que a área de negócios encontra-se um pouco mais envolvida. A área de segurança de informação é formada, em sua maioria, por profissionais técnicos, com visão de negócio e, principalmente, com linguagem não técnica, facilitando a integração entre as possibilidades técnicas, com as necessidades mercadológicas, alinhadas à estratégia do banco.

O estudo de casos indica que os 10 domínios de segurança são abrangentes, sendo que um único profissional, dificilmente, concentrará conhecimento profundo de todos os assuntos envolvidos na segurança do Internet Banking. A multidisciplinariedade, nesta gestão, é fundamental, para que as três camadas sejam cobertas de forma eficiente e, também, sejam adequadas às expectativas do cliente. O profissional de tecnologia, ciente dos riscos técnicos, deve interagir com o homem de negócio, para estudar a melhor forma de aproveitar as oportunidades do meio eletrônico. Por sua vez, o profissional de negócio deve procurar compreender as possibilidades, restrições, vantagens e desvantagens de determinadas decisões técnicas. A soma dos dois conhecimentos poderá construir um canal eletrônico mais competitivo e alinhado à estratégia do banco; com custos menores e ganho de produtividade; além de poder propiciar um aumento na participação no mercado bancário.

O tema segurança em TI permeia os bancos através de ações, pontais ou contínuas, de treinamento, conscientização e prevenção. Este cenário se fortalece com a adoção das diversas práticas de segurança, utilizadas nos três casos estudados. Os bancos, atualmente, lidam com segurança de forma pró-ativa, preventiva, e não mais reativa, corretiva. O gerenciamento de segurança é, de fato, uma atitude praticada pelos bancos estudados, além de, comprometido em promover um canal, efetivamente, seguro para os clientes.

No início de 2001, quando o tema deste trabalho foi definido, a gestão de segurança era um assunto polêmico, explorado de forma sensacionalista pela mídia de massa. Praticamente, em menos de três anos, esta ramificação da gestão de TI cresceu nas organizações, na velocidade da Internet, formando profissionais especializados em gerir a segurança, com discernimento entre os seus riscos e oportunidades, criando um ambiente preventivo, bem como políticas de atuação em caso de sinistro.

Concluindo, os bancos estão comprometidos em preservar a segurança do meio eletrônico para si, bem como para o cliente, perdas em qualquer um dos lados são ruins, principalmente, para a imagem da instituição financeira. A tendência da gestão de segurança de informação é estar, cada vez mais, integrada à área de negócios, para melhor alinhamento com a estratégia do banco, otimizando os recursos investidos. O insumo dos bancos é a informação, portanto, o lado de negócio precisa estar preparado tomar decisão sobre temas que envolvam TI.

Os objetivos definidos no início do trabalho refletem nas principais contribuições deste estudo que são:

- ✓ Levantamento de referencial teórico, que poderá auxiliar na compreensão da gestão de segurança de TI, com foco principal em Internet Banking;
- ✓ Estudo de casos, de bancos com atuação no país, que indica a divisão de trabalho entre as áreas de tecnologia e negócios.

5.2 Limitações

A segurança do canal eletrônico, Internet Banking, é um tema difícil de ser abordado com os bancos, principalmente, por envolver questões como fraudes, perda financeira e problemas com a imagem da instituição financeira. Conseguir três bancos que participassem da coleta de dados para o estudo de casos, foi um trabalho árduo, e contou com a colaboração de diversas pessoas, politicamente influentes, nas empresas. Esta complexidade, no levantamento de dados, para o estudo de casos, se reflete em, basicamente, três limitações impostas ao trabalho:

A primeira limitação foi não poder realizar uma entrevista em profundidade com os bancos. Os profissionais não se dispuseram a uma entrevista, apenas concordaram em responder um questionário, devido à restrição de tempo e, principalmente, exposição de um assunto delicado.

A segunda limitação foi não poder contextualizar o banco no trabalho. O compromisso selado, entre a autora e o banco respondente, era que apenas o tipo de controle acionário seria aberto, na dissertação. Impedindo, desta forma, trazer à tona algumas informações relevantes na análise dos casos.

Duas outras etapas do trabalho sofreram limitações: a primeira, foi a investigação teórica e a segunda, a quantidade pequena de casos estudados.

A investigação acadêmica sobre os 10 domínios foi pobre, pois os domínios, concentrados nas camadas física e lógica, requerem acesso a informações técnicas. A autora pesquisou informações em bibliotecas de computação e engenharia, porém sem muito êxito de análise.

A quantidade de casos estudados não foi suficiente para montar um quadro comparativo, uma vez que os três bancos possuem a gestão de segurança muito parecida. Isto pode ter ocorrido por diversas razões: adoção de práticas de mercado; normas e regulamentos do BACEN e comitês da FEBRABAN; ou falta de uma entrevista, que viabilizasse a investigação em profundidade.

5.3. Sugestões para pesquisas futuras

Este estudo pode ser enriquecido com diversas pesquisas futuras. Uma delas é a análise mais aprofundada nos impactos que o segmento de grandes corporações tem na globalização do canal Internet Banking, tanto do lado da instituição financeira quanto da cadeia produtiva, relacionamento com os fornecedores e compradores. A Internet possibilita que filiais, espalhadas pelo mundo, de uma empresa multinacional, solicitem as transações e a matriz as aprovem, conforme fluxo de caixa global, legislação e norma internacionais. A segurança em um relacionamento global deve ser mais criteriosa, todavia, o banco tem que aproveitar as oportunidades, ou, muitas vezes, atender as necessidades do cliente para não perdê-lo para a concorrência.

Outros aspectos importantes, que poderiam melhorar este trabalho, são os levantamentos do perfil dos profissionais de segurança de informação: sua formação, especialidade, nível de conhecimento técnico versus conhecimento de negócios; e se o papel deles é o de assessorar e sugerir, ou definir e implementar as regras do canal. Até onde a segurança define o canal, e até onde a área de negócios pode se expor, como é feito este *trade-off*.

Por fim, a sugestão mais complexa, no ponto de vista da autora, é a análise da co-responsabilidade do cliente na segurança do Internet Banking. A Internet é segura, desde que as partes que transacionam neste meio sejam responsáveis pelos seus ambientes: físico, lógico e humano. O cliente do banco é também co-responsável por sua segurança, no ambiente Internet, assim como tem esta co-responsabilidade no mundo físico. No mundo físico, o cliente não deve andar com sua carteira exposta, se descuidar do cartão de crédito, ou sacar em caixa automático onde haja algum suspeito rondando. Desta mesma forma, na Internet, ele deve tomar alguns cuidados básicos, como não criar senhas fáceis ou divulgá-las, utilizar recursos de antivírus e *personal firewalls* (programa de defesa, que protege o computador contra a invasão de *hackers* e vírus).

Bibliografia

ALBERTIN, Alberto L. *Administração de Informação*: funções e fatores críticos de sucesso. 4ª ed. São Paulo : Editora Atlas, 2002.

_____. *Comércio Eletrônico*: modelo, aspectos e contribuições de sua aplicação. São Paulo : Editora Atlas, 1999.

_____. *Comércio Eletrônico*: um estudo no setor. In: XXII Encontro Anual da ANPAD, 22, 1998, Foz do Iguaçu (Brasil). ANAIS DA ENANAPD 1998, p. 01–15, Setembro/1998.

_____. *Pesquisa de Comércio Eletrônico no Mercado Brasileiro*. 6ª ed. São Paulo : FGV–EAESP–CIA (Centro de Informática Aplicada), 2004.

ALBERTIN, Alberto L.; MOURA, Rosa M. Comércio Eletrônico: seus aspectos de segurança e privacidade. *Revista de Administração de Empresas*, São Paulo : FGV–EAESP, v. 38, n. 2, p. 49–61, Abril/Junho, 1998.

ALVES, Mauro F.; LAMOUNIER, Ana B.; JABUR, Fábio P. Internet – adicionando valor por meio de inovações descontínuas: a experiência brasileira. *Revista de Administração*, São Paulo : v. 35, n. 2, p.30–36, abril/junho, 2000.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *Código de Práticas para a Gestão da Segurança da Informação (NBR ISO/IEC 17799)*. Rio de Janeiro : ABNT, 2001.

BACEN. *RESOLUÇÃO 2.817* Brasília, 2001 (a). Disponível em: <http://www5.bcb.gov.br/pg1Frame.asp?idPai=NORMABUSCA&urlPg=/ixpress/correio/correio/DETALHAMENTOCORREIO.DML?N=101032661&C=2817&ASS=RESOLUCAO+2.817> Acesso em: 17/08/2004.

BACEN. *Sistema Financeiro Nacional* – 1989 a 2000. Brasília, 2001(b). Disponível em: <http://www.bcb.gov.br/htms/Deorf/e88-2000/texto.asp?idpai=relsfn19882000> Acesso em: 27/09/2004.

BANKS, Erik. *E-Finance the Electronic Revolution*. England : John Wiley & Sons, 2001.

BASEL COMMITTEE. *Risk Management Principles for Electronic Banking*. Basel Committee Publication, Suíça, 2003.

BESSIS, Joël, *Risk Management in Banking*. Chichester : John Wiley & Sons, 1998.

BETING, Joelmir. *A Bolha Murchou.* Santa Catarina, 24/11/2000. Disponível em: <http://an.uol.com.br/2000/nov/24/0joe.htm> Acesso em: 13/04/2004.

BONOMA, Thomas V. *Case Research in Marketing:* Opportunities, Problems and Process. Journal of Marketing Research, vol. XXII. p. 199–208, 1985.

BRANDS, Stefan A. *Rethinking Public Key Infrastructures and Digital Certificates Building in Privacy*. United States of America : The MIT Press, 2000.

BREI, Vinícius A.; ROSSI, Carlos V. *Confiança, Valor Percebido e Lealdade em Trocas Relacionais de Serviço*: Um Estudo com Usuários de Internet Banking no Brasil. In: XXVI Encontro Anual da ANPAD, 26, 2002, Salvador (Brasil). ANAIS DA ENANAPD 2002, p. 01–15, Setembro/2002.

BRINEY, Andrew. *What is "enough" Security*. Junho, 2004. Disponível em: < http://infosecuritymag.techtarget.com/ss/0,295796,sid6_iss407_art819,00.html> Acesso em: 26/06/2004.

BRITISH DEPARTMENT OF TRADE AND INDUSTRY. *Managing Information Security Solutions from the UK Contents.* Inglaterra, 2000. Disponível em: <http://www.dti.gov.uk/industry_files/pdf/solutions.pdf> Acesso em: 20/04/2003.

BRITISH STANDART INSTITUTION. *Code of Practice for Information Security Management (BS ISO/IEC 17799).* England : BSI, 2000.

BURREL, Gibson; MORGAN, Gareth. *Sociological paradigms and organizational analysis*. London : Heinemann Educational Books, 1979.

CAMERON, Debra. *Security Issues for the Internet and the World Wide Web*. Computer Technology Research Corp., Revised Edition, 1997.

CAMP, Jean L. *Trust and Risk in Internet Commerce*. 1st ed. United States of America : MIT PRESS, 2000.

CAMPBELL, Joseph. *O Poder do Mito*. São Paulo : Editora Palas Athena, 2000.

CASTELLS, Manuel *Internet y la sociedad red.* Espanha, 2004. Disponível em: http://www.uoc.edu/web/esp/articles/castells/castellsmain3.html. Acesso em: 28/10/2004.

CSO MAGAZINE; CERT COORDINATION CENTER; U.S. SECRET SERVICE. *E-Crime Watch survey*. United States of America, 2004. Disponível em: <http://www.csoonline.com/releases/052004129_release.html> Acesso em: 26/06/2004.

COMPUTER SECURITY INSTITUTE (CSI); FEDERAL BUREAU OF INVESTIGATION (FBI). *Computer crime and security survey*. 8th Annual. San Francisco, 2004. Disponível em: <http://visionael.com/products/security_audit/FBI_CSI_2003.pdf > Acesso em: 15/05/2004.

CULP, Christopher L. *The Art of Risk Management* – Alternative Risk Transfer. United States of América : John Wiley & Sons, 2002.

D'ANDRÉA, Edgar R. P. et al. *Segurança em Banco Eletrônico*. Coordenador: D'ANDRÉA, Edgar R. P. 1ª ed. São Paulo : PricewaterhouseCoopers, 2000. 181 p.

DHILLON, Gurpreet; BACKHOUSE, James. Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal*, United Kingdom, Blackwell Science Ltd., n. 11, p. 127–153, 2001.

DINIZ, Eduardo H. Cinco décadas de automação. *GV–Executivo*. Editorial Era Digital. Edição especial 50 anos. FGV–EAESP, São Paulo, v. 3, n. 3, p. 55–60, ago./out. 2004.

_____. Evolução do uso da web pelos bancos. *RAC – Revista de Administração Contemporânea*, Curitiba, v. 4, n. 2, p. 29–50, Maio/Ago. 2000 (a).

_____. *Redes locais e downsizing de sistemas de informação*: um estudo em bancos brasileiros. 108 f. Dissertação (Mestrado em Administração), FGV–EAESP, São Paulo, 1994.

_____. *Uso da Web pelos bancos*: comércio eletrônico nos serviços bancários. 287 f. Tese (Doutorado em Administração de Sistemas de Informação), FGV–EAESP, São Paulo, 2000 (b).

DINIZ, Eduardo H.; PORTO, Roseli; ADACHI, Tomi. *Internet Banking sob a Ótica da Funcionalidade, Confiabilidade e Usabilidade.* In: Conselho Latino Americano de Escolas de Administração, 38, 2003, Peru (Lima). ANAIS DO CLADEA 2003, p. 01–15, Outubro/2003.

DINIZ, Eduardo H. PORTO, Roseli M.; ANGULO, Marcelo J. *Uso da Web nos serviços financeiros.* FGV–EAESP–NPP (Núcleo de Pesquisa e Publicações), Série Relatórios de Pesquisa, São Paulo, 183 f., 2001.

EISENHARDT, Katheleen M. *Building Theories from Case Study Research*. Academy of Management Review, vol. 14, nº 4, p. 532–550, 1989.

EXECUTIVOS FINANCEIROS. Setor Financeiro Brasileiro está entre os mais competitivos do mercado. *Revista Executivos Financeiros*, São Paulo, junho de 2003.

FEBRABAN. *Em 2003 os bancos investiram R$ 4,2 bilhões em TI*. São Paulo : FEBRABAN, 2004. Disponível em: http://www.febraban.org.br/Arquivo/Servicos/Dadosdossetor/tecnologia_2003_dadossetor.asp. Acesso em: 27/09/2004.

FEBRABAN. *Guia de Referências sobre Ataques via Internet.* São Paulo : FEBRABAN, 2000.

FERREIRA, Aurélio B. de H. *Novo Aurélio – O Dicionário da Língua Portuguesa.* 2ª ed. (revista e aumentada), Rio de Janeiro : Nova Fronteira, 1986.

FORESTER, Tom. *High-tech society*. Great Britain : First MIT Press edition, 1987.

GARFINKEL, Simson; SPAFFORD, Gene. *Web Security & Commerce.* United States of América : O'Reilly & Associates Inc, 1997.

GATES, Bill. *Business at the Speed of Thought*. 1ª ed. United States of America : Warner Books, 1999.

GAZETA MERCANTIL. Bancos investem US$ 1,6 bi para proteger dados. *Jornal Gazeta Mercantil*. São Paulo, 02/06/2004.

GAZETA MERCANTIL. Serviços Bancários: Brasil já é o segundo do mundo em Internet Banking. Dados do IDC e levantamento Real ABN Amro Bank e McKinsey, *Jornal Gazeta Mercantil*. São Paulo, 01/04/2003.

_____. Tecnologia é arma para redução de custos. *Jornal Gazeta Mercantil*. São Paulo, 27/04/2004.

GHOSH, Anup K. *E-commerce Security:* Weak, Links, Best Defense. United States of America : John Wiley & Sons, 1998.

GLAESSNER, Thomas; KELLERMANN, Tom; McNEVIN, Valerie. *Electronic Security:* Risk Mitigation in Financial Transactions. United States of America : The World Bank, 2002.

GITMAN, Lawrence J., *Princípios de Administração Financeira.* 7ª ed. São Paulo : Harbara Editora, 1997.

GREENSTEIN, Marilyn; FEINMAN, Todd M. *Eletronic Commerce:* Security, Risk Management and Control. United States of America : McGraw-Hill Higher Education, 2000.

GRISCI, Carmen I. Dos corpos em rede às máquinas em rede: reestruturação do trabalho bancário e constituição do sujeito. *RAC – Revista de Administração Contemporânea*, Curitiba, v. 7, n. 1, p. 87–108, Jan./Mar. 2003.

HARRIS, Shon. *CISSP Certification:* all-in-one. United States of America : McGraw-Hill/Osborne, 2002.

HEALY, Richard J.; WALSH, Timothy J. Translating Security into Business Terminology. 1979. In: GALLERY, Shari M. *Security Management:* Readings from Security Management Magazine. United States of America : Butterworth Publishers. 1984. Cap. 5, p. 37–45.

HERNANDEZ, José M. *Entendendo Melhor o Processo de Decisão de Compra na Internet*: Uma análise Sobre o Papel da Confiança em Diferentes Situações de Risco. In: XXVI Encontro Anual da ANPAD, 26, 2002, Salvador (Brasil). ANAIS DA ENANAPD 2002, p. 01–15, Setembro/2002.

HUMPHREYS, Kim. Banking on the Web: Security First Network Bank and the development of virtual financial institutions. In: CRONIN, Mary J. *Banking and Finance on the Internet*. Canada : John Wiley & Sons, 1998. p. 75–104.

HUTCHINSON, Sarah E.; SAWYER, Stacey C. *Computers: the user perspective*. 2nd ed., Boston : Irwin, 1988.

INTERNATIONAL INFORMATION SECURITY FOUNDATION. *Generally Accepted System Security Principles* (GASSP). United States of América. Revisto em julho/1999. Disponível em: <http://web.mit.edu/security/www/GASSP/gassp021.html> Acesso em: 05/06/2004.

INTERNET SECURITY SYSTEMS. *Creating, Implementing and Managing the Information Security Lifecycle*. United States of América, 2000. Disponível em <http://documents.iss.net/whitepapers/securityCycle.pdf> Acesso em: 20/04/2003.

INTERPOL. *IT Security and crime prevention methods*. United States of América, 2000. Disponível em: < http://www.modulo.com.br/index.jsp>. Acesso em: 30/09/2004.

JORNAL DO COMÉRCIO. *Pesquisa IBOPE eRatings* – Segurança Parcial no e-banking. 23/6/2003.

KALAKOTA, Ravi; FREI, Frances. Frontiers of On-Line Financial Services. In: CRONIN, M. J. *Banking and Finance on the Internet*. Internet Management Series. Canada : John Wiley & Sons Inc., 1998. p. 19–74.

KOSIUR, David. *Understanding Eletronic Commerce.* United States of America : Microsoft Press, 1997.

KRUTZ, Ronald L.; VINES, Russell D. *The CISSP Prep Guide:* Mastering the Ten Domains of Computer Security. United States of America : Wiley Computer Publishing, 2001.

KUMAR, Sandeep. *Classification and detection of computer intrusions*. 1995. 165 f. Tese (Doctor of Philosophy) – Purdue University, United States of America, 1995.

KUHN, Richard et al. *Introduction to Public Key Technology and the Federal PKI Infrastructure*. United States of America : National Institute of Standards and Technology, U.S. Government publication, 26/02/2001.

LAUDON, Kenneth C.; LAUDON, Jane P. *Management Information Systems* – Managing the Digital Firm. 8ª ed., United States of America : Pearson Prentice Hall, 2004.

LAZZARINI, Sérgio G. *Estudos de Caso:* Aplicabilidade e Limitações do Método para Fins de Pesquisa. São Paulo : Economia & Empresa, vol.2, nº 4, outubro/dezembro de 1995.

LEVESON, Nancy, G. *Safeware:* System Safety and Computer, 1st edition. United States of America : Addison-Wesley Publishing Company, 1995.

LIMA, Marcelo B. *Provisão de Serviços Inseguros Usando Filtros de Pacotes com Estados*. 128 f. Dissertação (Mestrado em Ciência da Computação) Instituto de Computação da UNICAMP, Campinas, 2000.

LUNN, Bernard. Banking Technology in Emerging Markets. In: KEYES, Jessica. *Banking Technology Handbook*. United States of America : CRC Press LLC. Cap. 2, p. 2.1–2.6, 1999.

MANAGEMENT Review, vol. 14, nº 4, p. 532–550. 1989.

MANZONI, Ralphe Jr. *O início do fim da Nova Economia*. São Paulo : IDG Now: 10/04/2004. Disponível em: <http://idgnow.terra.com.br/idgnow/business/2004/03/0031> Acesso em: 13/04/2004.

MARSHALL, Christopher. *Medindo e gerenciando riscos operacionais em Instituições Financeiras*. São Paulo : Qualitymark Ed., 2002.

McCROHAN, Kevin. *Banking and Finance Threats*. United States of America : National Infrastructure Protection Ceter – FBI, 14 fev. 2003. Disponível em: <www.clusit.it/infosecurity2003/mccrohan.pps> Acesso em: 05/04/2003.

McKNIGHT, Lee; BAILEY, Joseph P. Information Security for Internet Commerce. In: _____. *Internet Economics*. MIT Workshop on Internet Economics, United States of America, 1999. p. 435–452.

MEIRELLES, Fernando S. *Informática:* novas aplicações com microcomputadores. São Paulo : Editora Makron Books, 1994.

_____. *Pesquisa Anual de Administração de Recursos de Informática*. 15ª ed. São Paulo : FGV–EAESP–CIA (Centro de Informática Aplicada), 2004.

MITNICK, Kevin D.; SIMON, William L. *A Arte de Enganar*. São Paulo : Editora Pearson Brasil, 2003.

MÓDULO SECURITY. Pesquisa Nacional de Segurança da Informação. 9ª ed. São Paulo, 24/11/2003. Disponível em: <http://www.modulo.com.br/pdf/nona_pesquisa_modulo.pdf> Acesso em: 10/03/2004.

NAKAMURA, Emilio T.; GEUS, Paulo L. de. *Segurança de Redes em Ambiente Cooperativos.* São Paulo : Editora Berkeley, 2002.

NIC BR. *Cartilha de Segurança para Internet*. NIC BR Security Office – Brazilian Computer Emergency Response Team. Versão 2.0, 11/03/2003. Brasil : Disponível em: <http://www.nbso.nic.br/docs/cartilha/#copyright> Acesso em: 17/08/2004.

NICOLETT, Mark et al. *Enterprise IT Security Management Defined*. Gartner Research, 2002.

PELTIER, Thomas R. *Information Security Risk Analysis.* United States of America : Auerbach Pub., 2001.

RAMOS, Anatália M.; COSTA, Fabrício R. Serviços bancários pela Internet: um estudo de caso integrando a visão de competidores e clientes. *RAC – Revista de Administração Contemporânea*, Curitiba, v. 4, n. 3, p. 133–154, Set./Dez. 2000.

REVISTA BUSINESS STANDART. 25 Melhores Serviços de Internet Banking. *Revista Business Standart*. Edição especial, IDG – Coputerworld do Brasil. São Paulo, abril/2002.

REVISTA DINHEIRO. HSBC contra hackers. *Revista Dinheiro*. São Paulo, 26/05/2004.

ROGERS, Everett M. *Diffusion of Innovations.* 3rd ed. New York : The Free Press, 1983.

ROSE, Mary. Internet Security Analysis Report: an executive overview. In: KEYES, Jessica. *Banking Technology Handbook*. United States of America : CRC Press LLC, Cap. 32, p. 32.1–32.7, 1999.

RUSSEL, Deborah; GANGEMI Sr., G. T. *Computer Security Basics.* United States of América : O'Reilly & Associates Inc., 1991.

SCHNEIER, Bruce. *Segurança.com* – segredos e mentiras sobre a proteção na vida digital. 1ª ed. Rio de Janeiro : Campus, 2001.

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

SIMONDS, Fred. *Network Security:* data and voice communications. United States of America : McGraw-Hill Series on Computer Communications, 1996.

SMAHA, Stephen E. Haystack: An Intrusion Detection System. In: *Proceedings of the Fourth Aerospace Computer Security Applications Conference*. Tracor Applied Science Inc., Austin, Texas. December, 1988. p. 37–44.

SOUZA, Luis H. C. Mensagem FEBRABAN. In: D'ANDRÉA, Edgar R. P et al. *Segurança em Banco Eletrônico*. 1ª ed. São Paulo: PricewaterhouseCoopers, 2000.

SYMANTEC ENTERPRISE SECURITY. *Security Reference Handbook:* A comprehensive categorization of security technologies and their relative threats. United States of América : Symantec Corporation, agosto/2001.

TAPSCOTT, Don. *Economia digital*. São Paulo : Makron Books, 1997.

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

TROSTER, Roberto L. *Concentração bancária.* São Paulo : FEBRABAN, junho/2004. Disponível em: <http://www.febraban.com.br/Arquivo/Servicos/Imprensa/Conc0404.pdf> Acesso em: 20/10/2004.

VALOR ECONÔMICO. Bancos buscam novas tecnologias para coibir as fraudes na Internet. *Jornal Valor Econômico.* São Paulo, 17/05/2004.

VAUGHAN, Emmett J. *Risk Management*. New Baskerville. John Wiley & Son, 1997.

YIN, Robert K. *Case Study Research:* design and methods. New York : Sage Publications, 1994.

WADLOW, Thomas A. *Segurança de Rede:* Projeto e gerenciamento de redes seguras. São Paulo : Editora CAMPUS, 2000.

WITTY, Roberta. *Elements of a Successful IT Risk Management Program***.** Gartner Research, 2002.

ANEXO 1

Lista de entidades internacionais, com suas normas, padrões e melhores práticas para a gestão de segurança em TI:

- ✓ *British Standard Institution (BSI)*

  BS 17799-2:2000 – *Information Security Management Systems – Specification with Guidance for Use*

- ✓ *International Organization for Standardization (ISO)*

  ISO/IEC TR 13335-1:1996 – *Guidelines for the Management of IT Security – Part 1: Concepts and Models for IT Security*

  ISO/IEC TR 13335-2:1997 – *Guidelines for the Management of IT Security – Part 2: Managing and planning IT Security*

  ISO/IEC TR 13335-3:1998 – *Guidelines for theMmanagement of IT Security – Part 3: Techniques for theMmanagement of IT Security*

  ISO/IEC TR 13335-4:2000 – *Guidelines for the Management of IT Security – Part 4: Selection of safeguards*

  ISO/IEC TR 13335-5:2001 – *Guidelines for the Management of IT Security – Part 5: Management Guidance on Network Security*

  ISO/IEC 15408-1:1999 – *Evaluation Criteria for Information Technology Security (Common Criteria) – Part 1: Introduction and General Model*

  ISO/IEC 15408-2:1999 – *Evaluation Criteria for Information Technology Security (Common Criteria) – Part 2: Security Functional Requirements*

  ISO/IEC 15408-3:1999 – *Evaluation Criteria for Information Technology Security (Common Criteria) – Part 3: Security Assurance Requirements*

  ISO/IEC 18044:2004 – *Information Security Incident Management*

  ISO/IEC 13569:1997 – *Banking and Related Financial Services – Information Security Guidelines*

- ✓ *National Institute of Standards and Technology (NIST)*

  SP 800-2 – *Public-Key Cryptography*

  SP 800-9 – *Good Security Practices for Electronic Commerce, Including Electronic Data Interchange*

SP 800-10 – *Keeping Your Site Comfortably Secure: An Introduction to Internet Firewalls*

SP 800-12 – *An Introduction to Computer Security: The NIST Handbook*

SP 800-13 – *Telecommunications Security Guidelines for Telecommunications Management Network*

SP 800-14 – *Generally Accepted Principles and Practices for Securing Information Technology Systems*

SP800-16 – *Information Technology Security Training Requirements: A Roleand Performance-Based Model*

SP 800-18 – *Guide for Developing Security Plans for Information Technology Systems*

SP 800-26 – *Security Self-Assessment Guide for Information Technology Systems*

SP 800-30 – *Risk Management Guide for Information Technology Systems*

SP 800-34 – *Contingency Planning Guide for Information Technology Systems*

SP 800-35 – *Guide to Information Technology Security Services*

SP 800-46 – *Security for Telecommuting and Broadband Communications*

SP 800-50 – *Building an Information Technology Security Awareness and Training Program*

SP 800-55 – *Security Metrics Guide for Information Technology Systems*

SP 800-61 – *Computer Security Incident Handling Guide*

SP 800-64 – *Security Considerations in the Information System Development Life Cycle*

- ✓ *Internet Engineering Task Force (IETF)*

  RFC 3631 – *Security Mechanisms for the Internet*

  RFC 2504 – *Users' Security Handbook*

  RFC 2350 – *Expectations for Computer Security Incident Response*

  RFC 2196 – *Site Security Handbook*

- ✓ *The Committee of Sponsoring Organizations of the Treadway Commission (COSO)*

  COSO Enterprise Risk Management Framework – Released for Comment

  Report of the National Commission on Fraudulent Financial Reporting

- ✓ *Information Systems Audit and Control Association (ISACA)*

  Control Objectives for Information and Related Technology (COBIT)

- ✓ *International Information Systems Security Certifications Consortium, INC. [(ISC)^2]*
  Certified Information Systems Security Professional (CISSP)
  System Security Certified Practitioner (SSCP)

- ✓ *Information Systems Security Association (ISSA)*
  Generally Accepted Information Security Principles (GAISP)

- ✓ *International Information Security Foundation (I^{2}SF)*
  Generally Accepted System Security Principles (GASSP)

- ✓ *American National Standards Institute (ANSI)*
  X9D-Securities Processing
  X9F-Data & Information Security

- ✓ *Capability Maturity Model® for Software (SW-CMM®)*

ANEXO 2

Tabulação do questionário:

I. Práticas de gerenciamento de segurança

1. O banco possui uma área específica que administra a segurança de TI?

	Estrangeiro (A)	Nacional (B)	Público (C)
Sim	x	x	x
Não			

1.a. Se sim, esta área está subordinada a qual diretoria ou vice-presidência?

	Estrangeiro (A)	Nacional (B)	Público (C)
Tecnologia	x	x	x
Auditoria			
Produtos			
Diretamente à presidência			
Organização e métodos			
Financeiro			
Outra. Qual?			

2. O banco possui quais das práticas abaixo?

	Estrangeiro (A)	Nacional (B)	Público (C)
Política de segurança	x	x	x
Plano de contingência	x	x	x
Guia de procedimentos de segurança	x	x	não soube responder
Plano de continuidade em caso de incidentes ou desastres	x	x	x

2.a. Esta(s) prática(s) foi (foram) desenvolvida(s) por quem?

	Estrangeiro (A)		Nacional (B)		Público (C)	
	Próprio banco	Empresa terceiri-zada	Próprio banco	Empresa terceiri-zada	Próprio banco	Empresa terceiri-zada
Política de segurança	x		x		x	
Plano de contingência	x		x		x	
Guia de procedimentos de segurança	x		x		x	
Plano de continuidade em caso de incidentes ou desastres	x		x		x	

2.b. Qual(is) foi (foram) a(s) base(s) ou fundamento(s) utilizado(s) no(s) seu(s) desenvolvimento(s)?

	Estrangeiro (A)			**Nacional (B)**			**Público (C)**		
	1. Padrão ou modelo de mercado	**2.** Experiência e expertise do banco	**3.** Experiência e expertise de empresa de consultoria	**1**	**2**	**3**	**1**	**2**	**3**
Política de segurança		x		x			x	x	
Plano de contingência	x			x		x			
Guia de procedimentos de segurança	x				x			x	
Plano de continuidade em caso de incidentes ou desastres		x		x	x		x	x	

2.c. O profissional responsável por cada prática está vinculado a qual área?

	Estrangeiro (A)	**Nacional (B)**	**Público (C)**
Política de segurança	Segurança Informação	Tecnologia	Gestão de segurança
Plano de contingência	Segurança Informação + Dono do negócio	Tecnologia	TI + negócio
Guia de procedimentos de segurança	Segurança Informação (SI)	Tecnologia	
Plano de continuidade em caso de incidentes ou desastres	Segurança Informação + TI	Tecnologia	TI + negócio

3. O banco possui um trabalho de conscientização, educação e treinamento sobre segurança em TI?

	Estrangeiro (A)	**Nacional (B)**	**Público (C)**
Sim	x	x	x
Não			

3.a. Se sim, este trabalho é:

	Estrangeiro (A)	**Nacional (B)**	**Público (C)**
Pontual		x	x
Contínuo	x		

3.b. Quem são os responsáveis por desenvolver este trabalho?

	Estrangeiro (A)				**Nacional (B)**				**Público (C)**			
	RH	TI	3º	Outros	RH	TI	3º	Outros	RH	TI	3º	Outros
Conscientização	x			SI		x				x		
Educação				SI		x			x			
Treinamento				SI			x		x			

RH = Recursos Humanos; **TI** = Tecnologia de Informação; **3º** = terceiros.

4. Existe uma área que cuida especificamente do gerenciamento de risco do Internet Banking?

	Estrangeiro (A)	Nacional (B)	Público (C)
Sim	x	x	não sabe
Não			

4.a. Se sim, esta área está subordinada a qual diretoria ou vice-presidência?

	Estrangeiro (A)	Nacional (B)	Público (C)
Tecnologia	x		–
Auditoria			–
Produtos		x	–
Financeiro			–
Organização e métodos			–
Diretamente à presidência			–
Outra. Qual?			–

II. Arquitetura e modelos de segurança

5. A arquitetura de segurança do Internet Banking foi definida por qual área do banco?

	Estrangeiro (A)	Nacional (B)	Público (C)
Área de tecnologia	x	x	x
Área de negócios			
Diversas áreas. Quais?		Produtos	

6. Quais são as áreas responsáveis pela manutenção da arquitetura de segurança do Internet Banking?

	Estrangeiro (A)	Nacional (B)	Público (C)
Áreas responsáveis	–	Tecnologia e produtos	Tecnologia

III. Sistemas de controle de acesso

7. Quais são os pontos de acesso físico* controlados no fluxo completo do Internet Banking?

	Estrangeiro (A)	Nacional (B)	Público (C)
Ambiente de desenvolvimento		x	x
Ambiente de produção	x	x	x
Ambiente de homologação	x	x	x
Base de dados (mídias)	x	x	x

*Acesso ao ambiente físico, onde estão os servidores, computadores e mídias (*hardware* em geral).

8. Quem administra as senhas de acesso aos ambientes e bases de dados do Internet Banking?

	Estrangeiro (A)	Nacional (B)	Público (C)
Área de tecnologia do próprio banco		x	x
Empresa terceirizada com expertise em segurança			
Área de *help desk* do próprio banco			
Outras. Quais?	Segurança de Informação		

9. Quem administra as alçadas de cada usuário, o que cada usuário pode consultar, alterar, incluir ou excluir no fluxo de desenvolvimento, homologação e produção do Internet Banking?

	Estrangeiro (A)	Nacional (B)	Público (C)
Área de tecnologia do próprio banco		x	x
Os superiores de cada funcionário	x		
Área de recursos humanos			
Outras. Quais?	Dono da informação		

IV. Segurança física

10. O ambiente físico onde estão os equipamentos de produção do Internet Banking tem acesso:

	Estrangeiro (A)	Nacional (B)	Público (C)
Restrito às pessoas que trabalham na produção	x	x	
Controlado por crachás e senhas	x	x	
Registro de acesso, nome do funcionário, horário de entrada e saída	x	x	x
Restrito às pessoas que trabalham na produção	x	x	

11. Qual a área responsável pelo controle do acesso físico ao ambiente de produção do Internet Banking?

	Estrangeiro (A)	Nacional (B)	Público (C)
Área de segurança do prédio	x	x	x
Área de recursos humanos			
Área de tecnologia			
Área de organização e métodos			
Outras. Quais?			

V. Segurança em telecomunicação e redes

12. Quais são as áreas envolvidas na gestão de segurança em telecomunicação e redes que são utilizados pelo Internet Banking?

	Estrangeiro (A)	**Nacional (B)**	**Público (C)**
Área de tecnologia do próprio banco	x	x	x
Telecomunicação e redes serviços terceirizados no banco	x		
Outras. Quais?	Segurança de Informação		

13. A área de negócio participa, em algum momento, na gestão de segurança em telecomunicação e redes do Internet Banking?

	Estrangeiro (A)	**Nacional (B)**	**Público (C)**
Sim		x	x
Não	x		

13.a. Se sim, em qual momento?

Estrangeiro (A)	**Nacional (B)**	**Público (C)**
Tomada de risco – decisão		

VI. Desenvolvimento de sistemas e aplicativos

14. Em quais momentos do desenvolvimento de sistemas e aplicativos do Internet Banking a área de negócios do banco está envolvida?

	Estrangeiro (A)	**Nacional (B)**	**Público (C)**
Especificação do negócio		x	x
Desenvolver com recursos internos ou externos			
Compra de *software* ou pacotes de mercado			
Requisitos da arquitetura de aplicações e de infra-estrutura			
Aposentadoria ou remoção e destruição dos aplicativos			
Desenvolvimento			x
Testes			
Implantação			
Pós-implantação			
Desenho do sistema	x		

VII. Criptografia

15. A decisão pelo tipo de padrão criptográfico, a ser utilizado no Internet Banking, é uma decisão colegiada entre as áreas de tecnologia e de negócios?

	Estrangeiro (A)	Nacional (B)	Público (C)
Sim			
Não	x	x	x

VIII. Segurança de operação

16. A parte operacional do Internet Banking é realizada por qual(is) áreas?:

	Estrangeiro (A)	Nacional (B)	Público (C)
Operacional	–	x	
Tecnologia	–	x	x
Comercial	–		
Outras. Quais?	–		Infra-estrutura e logística

17. A auditoria, nos sistemas e processos do Internet Banking, é realizada por equipe:

	Estrangeiro (A)	Nacional (B)	Público (C)
Interna		x	x
Externa	x		

IX. Legislação, investigação e ética

18. Os conhecimentos legais e éticos são compartilhados com todas as áreas envolvidas na segurança do Internet Banking, inclusive a área técnica?

	Estrangeiro (A)	Nacional (B)	Público (C)
Sim	x	x	não respondeu
Não			

19. Existe um guardião do histórico de ocorrências e material forense para serem utilizados em futuras análises de sinistros que porventura ocorram no Internet Banking?

	Estrangeiro (A)	Nacional (B)	Público (C)
Sim	x	x	x
Não			

20. Qual é a área responsável em interagir em caso de sinistro no Internet Banking?

	Estrangeiro (A)					**Nacional (B)**					**Público (C)**				
	1. Comer-cial	**2.** Audito-ria	**3.** Assesso-ria de imprensa	**4.** Frau-des	**5.** Outros	**1**	**2**	**3**	**4**	**5**	**1**	**2**	**3**	**4**	**5**
Cliente	x		x		Produto, SI, MKT qualidade	x			x		x	x			
Mercado					SI			x			x	x	x		
Outros bancos					SI				x		x	x			

SI = Sistema de Informação; **MKT =** marketing.

X. Plano de continuidade do negócio e plano de recuperação em caso de desastre

Responda as questões 21 a 23, caso o banco possua um plano de continuidade do negócio e plano de recuperação em caso de desastre.

21. O banco possui plano de continuidade do negócio e plano de recuperação, em caso de desastre?

	Estrangeiro (A)	**Nacional (B)**	**Público (C)**
Sim	x	x	x
Não			

22. O banco realiza testes periódicos dos planos de contingência e de continuidade?

	Estrangeiro (A)	**Nacional (B)**	**Público (C)**
Sim	x	x	x
Não			

22.a. Se sim, quem é o responsável pelos testes?

	Estrangeiro (A)	**Nacional (B)**	**Público (C)**
Tecnologia	x	x	x
Auditoria			
Negócio	x		
Outras. Quais?	TI		

23. O banco possui:

	Estrangeiro (A)	**Nacional (B)**	**Público (C)**
Sites de contingência própria		x	x
Sites de contingência terceirizados	x		