UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

GESTÃO DE RISCOS APLICADA AO AMBIENTE INTERNET BANKING DAS INSTITUIÇÕES FINANCEIRAS DO BRASIL

ADRIANO DE MELO POUCHAIN

ORIENTADOR: RICARDO STACIARINI PUTTINI

DISSERTAÇÃO DE MESTRADO EM ENGENHARIA ELÉTRICA

PUBLICAÇÃO: JULHO/2007

BRASÍLIA / DF: JULHO/2007

UNIVERSIDADE DE BRASÍLIA
FACULDADE DE TECNOLOGIA
DEPARTAMENTO DE ENGENHARIA ELÉTRICA

GESTÃO DE RISCOS APLICADA AO AMBIENTE INTERNET BANKING DAS INSTITUIÇÕES FINANCEIRAS DO BRASIL

ADRIANO DE MELO POUCHAIN

DISSERTAÇÃO DE MESTRADO SUBMETIDA AO DEPARTAMENTO DE ENGENHARIA ELÉTRICA DA FACULDADE DE TECNOLOGIA DA UNIVERSIDADE DE BRASÍLIA, COMO PARTE DOS REQUISITOS NECESSÁRIOS PARA A OBTENÇÃO DO GRAU DE MESTRE.

APROVADA POR:

RICARDO STACIARINI PUTTINI, DOUTOR, ENE/UNB
(ORIENTADOR)

ANDERSON CLAYTON ALVES NASCIMENTO, DOUTOR, ENE/UNB
(EXAMINADOR INTERNO)

MAMEDE LIMA MARQUES, DOUTOR, CID/UNB
(EXAMINADOR EXTERNO)

RAFAEL TIMÓTEO DE SOUSA JUNIOR, DOUTOR, ENE/UNB
(SUPLENTE)

DATA: BRASÍLIA/DF, 31 DE JULHO DE 2007.

FICHA CATALOGRÁFICA

POUCHAIN, ADRIANO DE MELO
Gestão de Riscos Aplicada ao Ambiente Internet Banking das Instituições Financeiras do Brasil [Distrito Federal] 2007.
xxi, 150p, 297 mm (ENE/FT/UnB, Mestre, Engenharia Elétrica, 2007).

Dissertação de Mestrado – Universidade de Brasília, Faculdade de Tecnologia. Departamento de Engenharia Elétrica.

1. Gestão de Riscos
2. Comportamento dos atacantes
3. Internet Banking

I. ENE/FT/UnB. II. Título (Série)

REFERÊNCIA BIBLIOGRÁFICA

POUCHAIN, ADRIANO DE MELO (2007). GESTÃO DE RISCOS APLICADA AO AMBIENTE INTERNET BANKING DAS INSTITUIÇÕES FINANCEIRAS DO BRASIL. Dissertação de Mestrado, Publicação JULHO/2007, Departamento de Engenharia Elétrica, Universidade de Brasília , Brasília , DF, 150p.

CESSÃO DE DIREITOS

NOME DO AUTOR: Adriano de Melo Pouchain
TÍTULO DA DISSERTAÇÃO: GESTÃO DE RISCOS APLICADA AO AMBIENTE INTERNET BANKING DAS INSTITUIÇÕES FINANCEIRAS DO BRASIL.
GRAU/ANO: Mestre/2007.

Adriano de Melo Pouchain
SQSW 103 bloco J apto 607
CEP 70670-310 – Brasília – DF - Brasil

DEDICATÓRIA

A minha família, pelo estímulo, apoio e compreensão, fatores essenciais para a conclusão desse projeto.

AGRADECIMENTOS

A Deus, pelo conforto nos momentos de incerteza e por permitir a conclusão dessa fase de minha vida.

Ao meu orientador Prof. Dr. Ricardo Staciarini Puttini, pela confiança e constante apoio, incentivo, dedicação e amizade essenciais para o desenvolvimento deste trabalho e para o meu desenvolvimento como pesquisador.

Aos colegas do Banco do Brasil, pelo apoio, ajuda em diversos aspectos, colaboração, compreensão e amizade.

RESUMO

O presente trabalho descreve os conceitos e a importância da gestão de riscos para as instituições financeiras. Aborda algumas das principais iniciativas na área de gestão de riscos pelas instituições financeiras do Brasil, resultando em uma proposta de metodologia a ser aplicada no ambiente internet banking. Realizamos pesquisa sobre os ataques desferidos contra as instituições financeiras instaladas no Brasil, identificando os ambientes críticos, o comportamento dos atacantes, as vulnerabilidades mais significativas e a melhor maneira de gerir os riscos identificados. Utilizamos o resultado da pesquisa como subsídio na aplicação da metodologia proposta, resultando em uma análise de riscos e proposta de gerenciamento. Assim, nos foi possível demonstrar a redução das perdas operacionais, por parte das instituições bancárias, decorrentes da consecução dos ataques, a partir da utilização dos conceitos de gerenciamento de riscos.

ABSTRACT

This work shows the necessity and advantages of using a risk management model, applied to internet banking environment for the financial institutions. We have identified the main risks of the internet banking environment and analyzed the results of a survey carried out by the author about attacks against financial institutions in Brazil. We've identified critical environments, the behavior of the hackers, the most significant vulnerabilities and the best way to manage the correspondent risks. At last, it was possible to show the reduction of operational losses due the attacks against the financial institutions, by using the concepts of risk management.

ÍNDICE

ÍNDICE DE TABELAS

ÍNDICE DE FIGURAS

1. INTRODUÇÃO

O objetivo deste trabalho consiste em demonstrar a implementação de um modelo de gestão de risco em uma situação real, vivenciada pelas instituições financeiras. Ao oferecer os serviços de *internet banking* para realização de transações bancárias, as instituições financeiras ingressaram em um ambiente repleto de incertezas e cujo domínio sobre todas as variáveis encontra-se além dessas instituições.

Aliado às incertezas advindas desse canal de relacionamento, a complexidade dos ambientes computacionais que suportam as transações financeiras, bem como as leis e regulamentos as quais as instituições devem se submeter, apresentam-se como fatores de risco, que somados podem determinam o fracasso do serviço oferecido, ou seu sucesso, dependendo da capacidade das empresas em adotarem medidas apropriadas para minimização dos riscos.

Não identificamos literatura que contemplasse de forma abrangente a abordagem apresentada nesta dissertação. As literaturas sobre o assunto estão dispersas em artigos, *sites* de segurança, livros didáticos e apresentações em congressos e cursos específicos sobre gestão de riscos e segurança, que se encontram referenciados na bibliografia desta dissertação.

Embora tenhamos identificado descrições sobre metodologias de avaliação de risco [66], não há publicação que alie a teoria com a administração de riscos em ambiente de *internet banking* das instituições financeiras.

Os administradores de empresas podem considerar o disposto neste trabalho para aprimoramento dos modelos de gestão de risco, ampliando a capacidade de tomada de decisões e influenciando diretamente as estratégias adotadas na condução dos negócios.

Assim, como primeira contribuição, apresentamos um modelo de gestão de riscos adaptado a partir do modelo do SEI – *Software Engineering Institute*, em que dividimos a gestão de risco em várias etapas. O modelo se propõe a auxiliar os gestores de processos na identificação dos riscos e no planejamento das ações de minimização de eventos indesejados.

A segunda contribuição consiste em determinar as principais ameaças e vulnerabilidades nos ambientes que constituem o *internet banking*, bem como, os tipos de ataques mais freqüentes disparados contra os clientes e as instituições financeiras no Brasil.

A terceira contribuição contempla a análise dos dados de séries temporais de quatro anos, quanto ao número de ataques sofridos pelas instituições, comparando com os períodos em que foram implementadas medidas de segurança adicionais pelos bancos. Baseado nessa comparação foi possível identificar um padrão de comportamento dos *hackers*, quando executando ataques contra as instituições e clientes.

Como quarta contribuição, identificamos as principais medidas de segurança adotadas pelas instituições financeiras, no Brasil, analisando suas vantagens e desvantagens.

A adoção de um modelo de gerenciamento de riscos atua de modo preventivo e contínuo, possibilitando a adoção de ações mais rápidas, por parte dos administradores e, conseqüentemente, a diminuição das perdas resultantes dos ataques.

1.1. SISTEMA FINANCEIRO EM NÚMEROS

Coletamos informações sobre o setor econômico em que as instituições bancárias atuam, com o propósito de ressaltar o volume de transações realizadas anualmente por meio dos diversos canais e identificar as tendências de sua utilização pelos clientes.

O quadro geral dos bancos no Brasil mostra, no decorrer dos últimos cinco anos, uma gradual diminuição de instituições autorizadas pelo Banco Central a operar no país. Este cenário sinaliza para uma estabilização e consolidação de recente processo de fusões e incorporações no mercado financeiro. Observa-se uma diminuição do número de bancos privados nacionais e uma estabilização dos bancos estrangeiros. De acordo com a Febraban – Federação Brasileira de Bancos [21] ainda há espaço para competitividade entre os bancos na busca de maiores fatias do mercado. Sob esta análise o uso da tecnologia certamente exercerá um papel decisivo na diferenciação dos produtos e serviços oferecidos, como também na gestão das estruturas das instituições financeiras. A figura 1.1 nos mostra a variação ocorrida nos últimos cinco anos.

Período	2000	2001	2002	2003	2004	2005
Número de Bancos	192	182	167	165	164	161
Bancos Privados Nacionais	105	95	87	88	88	84
Bancos Privados Estrangeiros	70	72	65	62	62	63
Bancos Públicos	17	15	15	15	14	14

Fonte: Federação Brasileira dos Bancos

Figura 1.1: Quadro de instituições financeiras no Brasil

Nos últimos cinco anos o número de agências bancárias mostra-se relativamente estável, sendo esse o mais tradicional canal de acesso dos clientes aos bancos. O número de equipamentos de auto-atendimento praticamente dobrou no mesmo período. Contudo, a mudança mais significativa concentra-se no número de correspondentes bancários. Entre 2004 e 2005 a variação foi de mais de 50%. Esse canal constitui-se na utilização da infra-estrutura de empresas parceiras (terceirizados) para atendimento de serviços bancários. A figura 1.2 ilustra o acima exposto [21].

	2000	2001	2002	2003	2004	2005	Variação 2005/2004
Número de Agências	16.396	16.841	17.049	16.829	17.260	17.515	1,5%
Postos eletrônicos	14.453	16.748	22.428	24.367	25.595	27.405	7,1%
Correspondentes bancários	13.731	18.653	32.511	36.474	46.035	69.546	51,1%

Fonte: Federação Brasileira dos Bancos

Figura 1.2: Canais de acesso às instituições financeiras

Outro dado significativo é mostrado na figura 1.3 que compara as quantidades de contas correntes com o número de contas de clientes com *internet banking*. Nos últimos três anos, a quantidade de clientes que passou a usar a *internet* para fazer suas transações bancárias praticamente triplicou.

	2000	2001	2002	2003	2004	2005
Contas correntes (1)	48,2	53,6	55,7	61,4	66,9	70,5
Clientes com Internet (2)	8,3	8,8	9,2	11,7	18,1	26,3

Em milhões

(1) Contas correntes movimentadas – Fonte Banco Central [62]
(2) Fonte Febraban [21]

Figura 1.3: Quadro de contas correntes

A figura 1.4 nos apresenta um quadro comparativo entre as transações bancárias por canal de atendimento. Alguns números são significativos quanto ao comportamento dos usuários. Primeiramente, observa-se uma expansão do número total de transações bancárias, na ordem de 17% na comparação entre o ano de 2005 em relação a 2004. Outra constatação é quanto ao crescimento de 50%, em média, do uso do *internet banking*, tanto por pessoas físicas quanto por jurídicas. Esse resultado sinaliza uma intensa migração do uso dos canais tradicionais (transações presenciais nos caixas das agências) para a *internet*.

O comportamento observado no Brasil, quanto à utilização da *internet* para realização de transações bancárias, é também observado em outros países na Europa e América do Norte. Segundo pesquisa divulgada no *site* da Global Market Insite [30], envolvendo 17,5 mil consumidores em 18 países, constatou-se que pelo menos 50% de suas transações bancárias são realizadas através de *internet banking*, com destaque para Holanda, Alemanha e Dinamarca. Os Estados Unidos e o Japão ficaram no 10º e 11º lugares, respectivamente, com 38% e 30% das transações. O Brasil aparece na sétima colocação, com 41% das transações.

	2000	2001	2002	2003	2004	2005	Variação 2005/2004
Total de transações (1)	19.760	23.444	21.617	26.302	30.035	35.122	16,90%
Transações de caixas	4.027	5.188	4.463	4.451	3.609	3.719	3,00%
Internet banking (PF)	370	820	1.139	1.457	2.045	3.167	54,90%
Internet banking (PJ)	359	664	970	1.174	1.862	2.682	44,00%
Correspondentes não bancários	-	-	-	125	187	296	58,20%

Em milhões
Fonte: www.febraban.org.br/ [62]
(1) Transações bancárias abrangendo os diversos canais de atendimento (*call center*, correspondentes não bancários, cheques compensados, *internet*, auto-atendimento, troca eletrônica de dados, transações de caixas, POS – *point of sale*)

Figura 1.4: Evolução de transações bancárias (milhões)

A pesquisa aponta a falta de confiança dos clientes americanos quanto à segurança do canal, como uma das razões pelas quais o serviço de *internet* ainda não ter atingido índices majoritários. O comportamento oposto observado nos países europeus é atribuído às medidas adicionais de segurança adotadas pelos bancos. A pesquisa detectou que os *sites* dos bancos trabalham com medidas adicionais para identificação e autenticação de usuários, como duas e até três senhas.

Contudo, independentemente da falta de confiança no canal *internet* poder ainda afastar usuários, a pesquisa revela que os consumidores de todo o mundo acreditam na irreversibilidade do movimento quanto ao uso do sistema virtual. Desta forma, cabe às instituições financeiras gerenciar os riscos inerentes ao ambiente, como forma de explorar as oportunidades oferecidas. A competitividade entre os bancos está cada vez mais acirrada e os que oferecerem diversificação nos serviços aliada a medidas de segurança mais eficazes, podem ampliar sua presença no mercado financeiro, reduzir os custos operacionais e elevar a satisfação de seus clientes.

Apresentamos na tabela 1.1 os valores médios de transações, calculados pelos bancos instalados no Brasil, que não envolvam movimentação de dinheiro, em espécie, nos canais apresentados na figura 1.4.

Tabela 1.1: Valores de Transações Bancárias

Canal de Atendimento	Valor da Transação
Internet Banking	R$ 0,30
Transação no Caixa	R$ 1,80
Correspondente não Bancário	R$ 1,20

Percebemos que transações realizadas por meio do atendimento por caixas (canal convencional) chega ser até seis vezes maior que a mesma transação, quando realizada pelo canal Internet.

Essa diferença eleva a eficiência operacional das instituições, trazendo como benefício imediato uma maior rentabilidade e retorno sobre o investimento dos acionistas. Assim, a irreversibilidade do movimento em direção ao canal eletrônico é também percebida e incentivada pelos bancos. Portanto, cabe a estes propiciar maior segurança aos clientes para que o processo migratório se intensifique cada vez mais.

1.2. ORGANIZAÇÃO DA DISSERTAÇÃO

Esse trabalho está organizado da seguinte forma: o capítulo 2 apresenta os principais conceitos que norteiam a disciplina de administração de riscos. Introduz as definições sobre o ciclo de vida dos riscos, propondo um modelo teórico de gestão de riscos. A seguir descreve as principais regulamentações internacionais e nacionais, que norteiam as ações das instituições financeiras, contemplando os conceitos sobre governança corporativa. Para finalizar descrevemos o papel desempenhado pela auditoria na avaliação de riscos.

O capitulo 3 descreve a metodologia utilizada neste trabalho.

O capítulo 4 aplica os conceitos introduzidos no modelo teórico de gestão de riscos na administração dos serviços bancários disponibilizados por meio da *internet*. Baseados na pesquisa de campo, realizada nas instituições financeiras instaladas no Brasil, seguimos aplicando cada fase do ciclo de vida dos riscos ao ambiente real das empresas. Com base nas pesquisas realizadas, caracterizamos o comportamento dos *hackers* e identificamos as principais ameaças às quais o serviço bancário está sujeito. Como conseqüência, analisamos

as soluções de segurança adotadas pelas instituições financeiras no Brasil e em alguns países estrangeiros.

O capítulo 5 destina-se a demonstrar a aplicabilidade do modelo de gerenciamento de riscos, ao reduzir o *gap* de tempo entre a detecção de uma ameaça e a adoção de medidas adicionais de segurança.

O capítulo 6 é dedicado às conclusões do trabalho.

2. GERENCIAMENTO DE RISCOS

A administração de riscos suporta diretamente a tomada de decisões, direcionando as estratégias das empresas na condução dos negócios. A dependência cada dia mais crescente dos sistemas informatizados culminou em ambientes complexos e altamente interligados. Falhas originadas em um ambiente afetam diretamente os resultados esperados em outra área negocial. Assim, o domínio sobre o universo dos riscos é de fundamental importância para a administração dos negócios de qualquer empresa.

Este capítulo trata, primeiramente, da definição de diversos conceitos que embasam a disciplina de gerenciamento de riscos. Em seguida, abordamos as etapas que constituem o modelo de gerenciamento de risco, adotado nesta dissertação. As legislações e regulamentações vigentes são apresentadas, destacando-se sua relação com o gerenciamento de riscos e a responsabilidade dos administradores perante os órgãos de fiscalização.

2.1. DEFININDO RISCO

A definição de risco não encontra unanimidade nas literaturas disponíveis sobre o assunto. Apresentamos quatro definições técnicas sobre o assunto. Contudo, antes de entrarmos nessas definições, apresentamos uma visão leiga do conceito, disposta no dicionário Houaiss: risco é a “probabilidade de insucesso, de malogro de determinada coisa, em função de acontecimento eventual, incerto, cuja ocorrência não depende exclusivamente da vontade dos interessados”.

O Instituto de Auditores Internos [60] define risco como “a possibilidade de um evento ocorrer e que pode ter impacto no atingimento dos objetivos”.

David Griffiths [31] define riscos como “um conjunto de circunstâncias que ameaça o atingimento dos objetivos”. Em um nível macro, sabemos que toda organização tem um objetivo. A partir desse objetivo macro, todos os subprocessos, pelos quais a organização foi dividida, também possuem seus próprios objetivos. Griffiths parte do pressuposto de que se não conhecemos todos os objetivos, também não conheceremos todos os riscos.

É interessante observar e aprofundar um pouco a definição de Griffiths, tomando-se o exemplo citado por ele sobre os objetivos de um fazendeiro e de um administrador de um museu. Ambos atuam em uma área próxima ao rio Nilo. Para o fazendeiro, o objetivo é cultivar terras que se fertilizam com a enchente do rio. Já para o administrador do museu, seu objetivo é preservar o acervo de obras. Assim sendo, a circunstância da enchente do rio é a mesma para ambos, contudo para o fazendeiro é uma oportunidade para fertilizar suas terras, enquanto para o administrador é um risco de danificar as obras sob seus cuidados.

A definição utilizada pela *ISO – International Organization for Standardization* [38] trata o risco como "a combinação da probabilidade de um evento ocorrer e de suas conseqüências". Em suma, a combinação da probabilidade de ocorrência com o impacto causado. Particularmente, face às demais definições sobre gerenciamento de riscos que veremos no decorrer deste trabalho, entendo que a definição da ISO estaria mais apropriada para definir o grau de exposição a um risco. Para exemplificar, tomemos como exemplo a queda de um raio sobre um *data center*. O risco de queda de um raio sempre vai existir, é o que chamamos de ameaça natural. Entretanto, a combinação de algumas atitudes como a decisão sobre a localização do *data center* e a instalação de pára-raios, que reduzem a probabilidade de queda de um raio sobre as instalações, bem como a instituição de *backups* e a existência de redundância de equipamentos, que reduzem o impacto (conseqüências), diminuem a exposição das instalações ao risco de queda de raio.

Glyn Holton [33] nos fornece uma definição de risco simplificada, mas ao mesmo tempo fascinante: "risco é expor-se a um propósito incerto", ou seja, é a exposição à incerteza.

Dos conceitos citados, a definição trazida pela ISO, aliada ao disposto por Glyn Holton, se coadunam para o meu entendimento sobre a definição de riscos. Entendo risco como a ocorrência de um evento incerto, que traz consigo conseqüências para o alcance dos objetivos determinados. Basicamente distinguimos dois elementos quando tratamos de risco: a possibilidade de ocorrência e o impacto ocasionado pela ocorrência do evento.

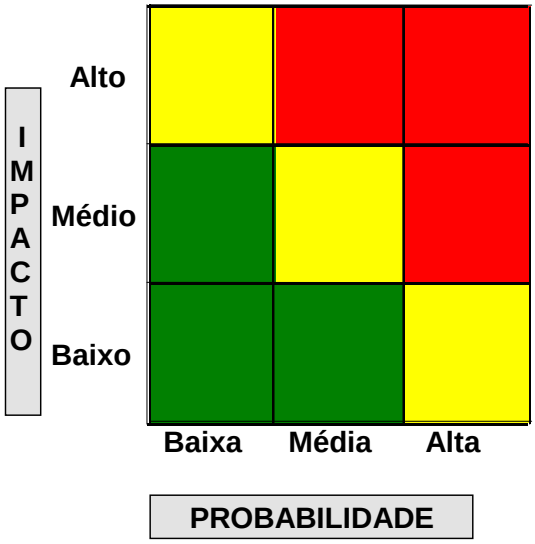


Figura 2.1: Matriz Impacto e Probabilidade

A relação impacto versus probabilidade pode ser melhor entendida à luz da figura 2.1. A região vermelha representa a área de maior exposição ao risco, resultante do cruzamento de uma alta probabilidade de ocorrência de um evento versus um impacto médio ou alto.

Outros conceitos referentes à disciplina de gerenciamento de risco encontram-se descritos no anexo I deste trabalho.

2.2. CONTROLE INTERNO

Um conceito que, imediatamente, vem associado ao risco é o de controle interno. Encontramos na literatura diversos conceitos para controle interno. O Instituto Francês de Contadores [67] o define como um conjunto de medidas de segurança que contribuem para o controle de uma companhia. Outra definição relaciona controle interno como um sistema que tem por objetivo contribuir para o controle das atividades, para assegurar a eficiência das operações e o uso racional dos recursos. Segundo o Comitê das Organizações Patrocinadoras (COSO) da *Treadway Commission* [44] controle interno é definido como “processo eficaz adotado pela direção das organizações, por gerentes e outros grupos designados para prover segurança razoável no atingimento de objetivos”.

Adoto a definição de controle interno como a tomada de ações que mitigam um determinado risco. Por exemplo, David Griffiths [31] exemplifica a ação de “reforçar uma ponte” como de minimização de um risco.

Tendo como base o disposto anteriormente, prefiro chamar de “gestão do risco” a toda ação que vise minimizar ou mesmo conviver com o risco. Convém reforçar que conviver com riscos é também uma forma de gerir riscos. Um administrador, ciente dos riscos, do impacto e da probabilidade de ocorrência, pode decidir por não adotar nenhuma atitude e “correr o risco”. A instituição de um determinado controle pode ser a resultante final do processo de análise de riscos.

Ações para mitigar riscos implicam em um custo adicional para as empresas. Contudo, no caso em que a perda ocasionada pela consecução do risco for menor que o custo do controle implementado, o administrador pode optar em conviver com a possibilidade de ocorrência do evento, sem que haja necessidade de implementar um controle.

Os controles internos podem ser de três tipos: preventivos, detectivos e corretivos [44]. Os preventivos são aqueles que agem anteriormente à consecução do risco. São exemplos deste tipo de controle: análise prévia dos antecedentes de um funcionário, quando de sua contratação; controle sobre o acesso físico de pessoas a ambientes; estabelecimento de segregação de funções em transações críticas etc. Atuam, portanto na linha das abscissas da figura 2.1, diminuindo a probabilidade de ocorrer um evento.

Os controles detectivos e corretivos entram em ação após a ocorrência de um evento e atuam em ambos os eixos da mesma figura. São exemplos desses controles: cálculos de *hash*, *check points*, planos de contingência, cópias de segurança de arquivos etc. O objetivo desses controles é detectar, o mais rápido possível, a ocorrência indesejada, procurando estancar o evento e ao mesmo tempo diminuir os impactos provocados.

2.3. CICLO DE VIDA DO RISCO

O ciclo de vida do risco compreende fases de um processo que se inicia pela identificação das situações de risco, passando pela análise de sua criticidade, adoção de

estratégias para controlar e risco e finalmente o exercício do monitoramento sobre a efetividade das medidas adotadas.

Em Continuous Risk Management Guidebook [17], uma proposta de ciclo de vida de risco nos é apresentada sob a descrição de 06 fases, quais sejam: identificação, análise, planejamento, monitoração, controle e comunicação.

Percebemos que as fases de monitoração e controle são fortemente interdependentes e, assim sendo, adotaremos uma variação do modelo em [19]. Aglutinamos na monitoração a fase de controle, reduzindo para cinco as fases do modelo a ser adotado neste trabalho – identificação, análise, planejamento, monitoração e comunicação.

Embora possamos identificar individualmente cada etapa, é interessante destacar que findada uma fase segue-se para a subseqüente, mas concomitantemente reinicializa-se a anterior. Como tratamos com incertezas sempre presentes, as fases devem giram constantemente e simultaneamente, conforme demonstrado na figura 2.2.

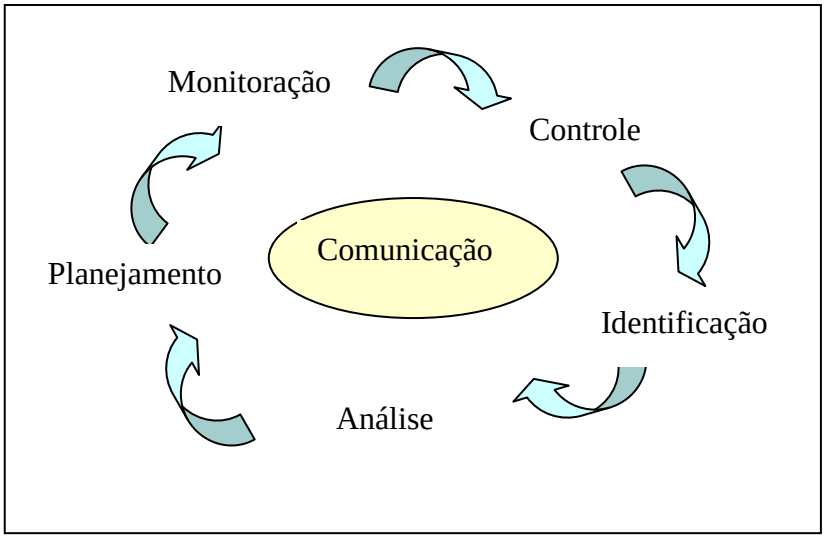


Figura 2.2: Ciclo de vida do risco
Adaptação de: Software Engineering Institute

2.3.1. IDENTIFICAÇÃO

A fase de identificação consiste na atividade de apresentar o risco sob a forma descritiva e que possa ser quantificado. Assim, procura-se identificar os mais diversos riscos,

associados ao processo sob análise, antes que se concretizem em problemas. A identificação parte, em primeiro lugar, do conhecimento do processo em curso, da determinação de seus objetivos e de suas diversas interações com os ambientes internos e externos, nos quais o processo esteja inserido.

O produto final dessa fase é a descrição ou declaração do risco, que pode e deve conter as condições de incertezas e preocupações, como também as conseqüências negativas geradas pelas condições descritas.

Mostramos a seguir um exemplo de descrição de risco para o caso de serviços *internet banking*:

"As senhas dos clientes podem ser interceptadas durante o acesso ao ambiente de *internet banking* da instituição, possibilitando o acesso de pessoas não autorizadas às contas dos usuários".

Observemos que a condição de incerteza está bem caracterizada quando se diz que "as senhas dos clientes podem ser interceptadas". As conseqüências ou impactos estão descritos em "possibilitando o acesso de pessoas não autorizadas às contas dos usuários".

A identificação de riscos é uma atividade que deve envolver diversas pessoas, com conhecimento sobre o processo que está sendo avaliado, pois possibilita juntar as mais diferentes experiências práticas e conhecimentos teóricos sobre o assunto.

Como ferramentas de identificação dos riscos são sugeridas técnicas como as seguintes:

- *brainstorming*. Esta técnica consiste em juntar as pessoas envolvidas no trabalho e colecionar as mais diversas preocupações e previsões sobre os possíveis riscos, baseadas em experiências individuais e conhecimentos teóricos;
- entrevistas, onde são colhidas, individualmente, as opiniões de várias pessoas, conhecedoras de determinado assunto;
- análises de literaturas que tratam do assunto em questão;

- experiências vivenciadas e reportadas por outras instituições; etc.

Adicionalmente à descrição dos riscos, é aconselhável que se identifique o contexto em que se encontra o risco. Trata-se de complementar o entendimento sobre todo o ambiente em que se encontra inserido e com o qual se relaciona o processo, possibilitando gerar o maior número de informações possíveis sobre os riscos identificados.

2.3.2. ANÁLISE

A atividade de análise de risco significa determinar sua dimensão, com base nas informações produzidas na fase anterior. De maneira mais detalhada, consiste na descrição e no contexto dos riscos identificados, produzindo informações que subsidiarão a tomada de decisões quanto às ações a serem adotadas para gestão dos riscos.

A descrição e o contexto identificam os riscos dentro das vertentes de impacto e probabilidade. A etapa de análise de riscos consiste, num primeiro momento, em avaliar as ameaças e vulnerabilidades, as probabilidades de concretização, em quantificar os impactos, passando, então, à classificação e priorização dos riscos.

De acordo com *Guidelines of the Management of IT Security*, ISO/IEC 13335-1:2004, o risco é caracterizado pelos seguintes elementos: ameaças, vulnerabilidades, processos e ativos.

Ameaça são quaisquer circunstâncias que podem causar danos ao ativo informação, como modificação, destruição, ou exposição indevida. Pode ser provocado por uma pessoa, um evento, um recurso defeituoso de hardware ou software. Ataques maliciosos, fraude, roubo, falhas em equipamentos são exemplos de ameaças.

Vulnerabilidades são características, ou fragilidades que podem ser exploradas por uma ameaça, para causar danos.

A análise dos riscos nos leva a concluir sobre o grau de exposição ao qual o processo se encontra sujeito. A figura 2.1 nos apresentou uma matriz de risco baseada em impacto e

probabilidade, como uma das maneiras de calcular a exposição ao risco. Existem outros tipos de matrizes e o tópico 2.3.2.1 trata do assunto.

Como resultado da identificação dos riscos é possível agrupá-los por classes ou grupos, a partir de critérios pré-estabelecidos. O objetivo desse agrupamento, ou classificação é identificar os riscos que se sujeitam às mesmas causas, os inter-relacionamentos entre eles, ou mesmo os impactos ocasionados. Isso auxilia na simplificação do processo de avaliação de risco, facilitando o planejamento quanto às ações corretivas.

Tal agrupamento pode ser melhor visualizado por meio da figura 2.3.

O objetivo final da classificação é facilitar o planejamento das estratégias de gestão, a partir de uma visão sistêmica dos riscos.

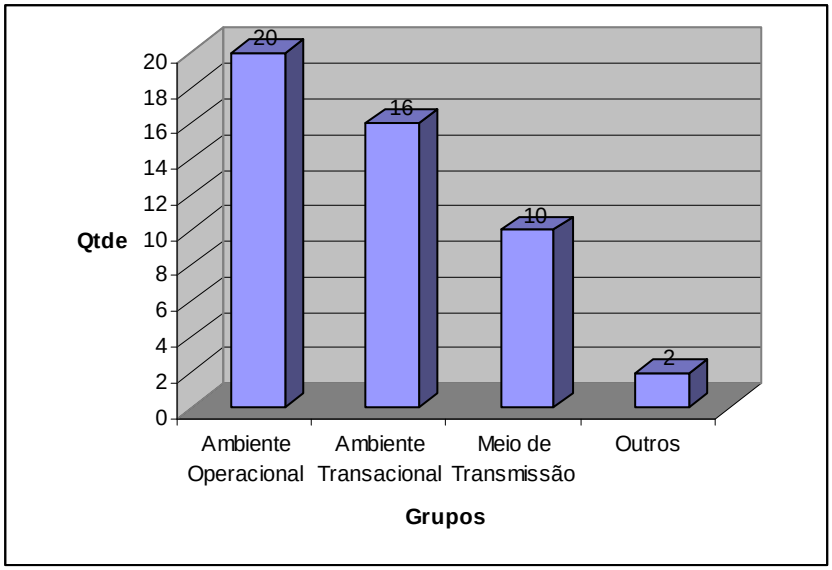


Figura 2.3: classificação de riscos
Fonte: Silas Roberto Souza [57]

A classificação dos riscos auxilia na decisão sobre a priorização daqueles que se mostrarem mais críticos ou relevantes.

2.3.2.1. Matriz de Risco

A ferramenta matriz de risco consiste em um sistema estruturado e ordenado para análise do nível de criticidade dos riscos identificados em um processo.

Identificados os riscos inerentes a cada processo, a fase de análise constitui-se em quantificar o grau de criticidade em que o risco se encontra. Uma das metodologias de análise é a matriz de riscos, que objetiva o estabelecimento de prioridades, com propósito de classificar os riscos em mais críticos e menos críticos. Dessa forma, é possível um melhor gerenciamento sobre os recursos disponíveis, estabelecendo uma estratégia de atuação a partir dos riscos mais críticos.

Para os gestores que precisam justificar a necessidade de investimentos na área de segurança, a matriz de risco fundamenta a destinação dos recursos, com base na maior criticidade dos riscos e, conseqüentemente, na necessidade de aprimoramento dos controles internos.

A figura 2.1 mostra uma matriz de riscos baseada em dois indicadores: probabilidade e impacto. Por meio do cruzamento de seus dois eixos é possível calcular o grau de exposição de um risco.

Os quadrantes em vermelho sinalizam as situações de alta exposição, os amarelos tratam dos níveis de exposição moderada, enquanto os verdes são as situações de risco baixo. Esse gráfico pode também ser ampliado para um nível de detalhamento maior, resultando nas seguintes situações, para cada eixo:

1. muito alto;
2. alto;
3. moderado;
4. baixo; e
5. muito baixo.

A resultante do gráfico é o nível de exposição ao risco que pode ser obtido pela multiplicação do impacto pela probabilidade.

A tabela 2.1 sintetiza a combinação de situações, que resulta em vários níveis de exposição:

	Probabilidade		
Impacto	Alto (3)	Moderado (2)	Low (1)
Alto (3)	Alto (9)	Alto (6)	Moderado (3)
Médio (2)	Alto (6)	Moderado(4)	Baixo (2)
Baixo (1)	Moderado (3)	Baixo (2)	Baixo (1)

Tabela 2.1: Exposição ao risco

O problema que se apresenta para avaliação do grau de exposição ao risco é como quantificar o impacto e a probabilidade do risco identificado.

Tendo em vista a quantidade de conhecimentos disponibilizados aos gestores, a subjetividade na avaliação da probabilidade e dos impactos é um fator que se faz fortemente presente quando da construção de matrizes de risco [32]. É possível, assim, identificar o grau de criticidade do risco tanto pela quantificação do impacto e das probabilidades, como pode ser utilizada uma metodologia baseada fundamentalmente na subjetividade dos avaliadores.

2.3.2.1.1 Quantificação do Impacto

A quantificação do impacto, em uma matriz de risco, consiste em identificarmos não somente as perdas financeiras para as instituições, mas os prejuízos diretos e indiretos, incluindo:

- danos à imagem da instituição, com conseqüente perda de clientes, de mercado ou de oportunidades;
- danos às pessoas (clientes, empregados, fornecedores);
- períodos de indisponibilidade e recuperação;
- degradação do desempenho de sistemas;
- descrédito sobre os serviços oferecidos;
- inter-relacionamento com outros sistemas;

- penalizações impostas pelos Órgãos de Fiscalização;
- existência de planos de contingência.

2.3.2.1.2 Quantificação da Probabilidade

A quantificação da probabilidade pode se dá por meio de cálculos probabilísticos, ou fundamentar-se em uma análise eminentemente subjetiva.

O artigo *Management of IT Auditing* [59], afirma que a quantificação da probabilidade é mais difícil de se calcular, por se tratar de incertezas – "Qual a probabilidade de um hacker invadir uma organização?". Contudo as experiências passadas e as melhores práticas podem ser usadas para auxiliar nessa estimativa.

Para o cálculo da quantificação da probabilidade, é possível utilizarmos uma avaliação numérica, com base nos cálculos de probabilidade, aliada a uma avaliação subjetiva. Neste caso, deveremos estabelecer critérios de avaliação, que fundamentarão os valores produzidos para a probabilidade.

Quando do uso dos cálculos probabilísticos, é fundamental dispormos de históricos sobre as estatísticas de ocorrência do evento. Contudo, lembrando Jacob Bernoulli, o passado não nos garante o futuro. Para esses cálculos consideramos os conceitos de média, desvio padrão, coeficiente de variância e de probabilidade.

No caso em que é necessário utilizarmos a subjetividade para quantificação das probabilidades, é necessário estabelecermos alguns critérios que fundamentarão a classificação da probabilidade nos níveis pré-definidos (alta, média, baixa, por exemplo). Assim sendo, é compreensível que utilizemos descrições qualitativas resultantes de avaliações subjetivas.

São exemplos desses critérios:

- freqüência das ocorrências dos eventos de risco (diário, várias vezes ao dia, ocasional);
- existência de controles preventivos, detectivos e corretivos;

- existência e periodicidade de monitoração dos serviços;
- grau de estabilização dos serviços – tempo que está implantado, freqüência de atualizações;
- estabilidade do ambiente de tecnologia;
- orientações/documentações disponíveis para os procedimentos executados;
- grau de treinamento dos funcionários;
- nível de intervenção manual;
- quantidade de penalizações imposta em determinado período;
- complexidade dos procedimentos;
- ocorrência de fraudes.

2.3.2.1.3 Aplicação da Metodologia AHP (*Analytic Hierarchy Process*)

Criada na década de 70 por Thomas Saaty [53], a AHP está classificada como "multicritério" ao ramo das metodologias de Pesquisa Operacional. Por essa metodologia, é possível comparar critérios de natureza diferente, para determinação do nível de criticidade de um dado risco.

A metodologia AHP é a mais difundida/utilizada das técnicas voltadas para atribuição de pesos aos critérios utilizados para classificação quantitativa e conseqüentemente para tomada de decisões.

O desafio final que se apresenta consiste em estabelecermos pesos para os mais diversos critérios, formulados para serem indicadores de impacto e probabilidade e, assim, traduzir o grau de criticidade em uma pontuação que varia entre 0 (zero) e 1 (um).

Edson de Oliveira Pamplona [50] escreve que "o método AHP pode ser usado na quantificação das características qualitativas, permitindo a ponderação de todas as características e a priorização dos critérios. A questão primordial do método é identificar com que pesos os fatores individuais influenciam os objetivos definidos. De acordo com o proposto por Saaty, os modelos têm que incluir e medir todos os fatores importantes, qualitativa e quantitativamente mensuráveis sejam eles tangíveis ou intangíveis".

Dessa maneira, a AHP [1] é um processo que permite o estabelecimento de prioridades, quando considerados aspectos qualitativos e quantitativos. Esse processo facilita a tomada de decisão pelos administradores.

Dado um determinado risco, o método AHP exige que os critérios sejam bem definidos e sem sobreposição. Uma vez definidos, esses critérios são comparados dois a dois e, em cada comparação, deve ser dito o quanto um critério é mais importante, ou "prioritário" ou, ainda, mais "grave" que um outro. Saaty propõe a utilização da escala mostrada na figura 2.4, para formação de uma matriz comparativa.

Intensidade de Importância	Definição	Explicação
1	Mesma Importância.	Duas atividades contribuem igualmente para o mesmo objetivo.
3	Importância pequena de uma sobre a outra.	A experiência e o julgamento favorecem levemente uma atividade em relação à outra.
5	Importância grande ou essencial.	A experiência e o julgamento favorecem fortemente uma atividade em relação à outra.
7	Importância muito grande ou demonstrada.	Uma atividade é fortemente favorecida; sua dominação de importância é demonstrada na prática.
9	Importância Absoluta.	A evidência favorece uma atividade em relação à outra com o mais alto grau de certeza

Figura 2.4: Escala proposta por Saaty
Fonte: Analytic Hierarchy Process [50]

A matriz mostrada na figura 2.5, nos orienta com relação à comparação entre os critérios.

	A	B	C
A		**A/B**	**A/C**
B	B/A		**B/C**
C	C/A	C/B	

Figura 2.5: Quadro comparativo entre critérios

Como exemplo, se A comparado com B for “fortemente” mais importante, a relação A/B terá valor de 5, conforme a escala proposta por Saaty.

Ao final de todas as comparações entre os critérios, obtém-se um peso para cada um deles.

O próximo passo consiste em quantificar a importância dos critérios, a qual chamamos de resposta. Determinamos o número de opções de repostas para cada critério e atribuímos graduações entre 0 e 1 para essas respostas. Por exemplo:

04 opções de resposta:

Resposta	Valor da intensidade
Intenso	1
Moderado alto	0,66
Moderado baixo	0,33
Baixo	0

Por exemplo, ao avaliarmos o critério “grau de treinamento dos funcionários” podemos assinalar a opção “Intenso”, o que faria com que fosse assumido o valor de 1 para este critério.

Assim, multiplicando-se os pesos e a intensidade de cada critério e somando os valores resultantes dessas multiplicações, chegaremos a um valor total para o risco em questão.

O processo se repete para todos os riscos identificados, fornecendo aos gestores uma classificação quanto ao grau de criticidade para cada um deles. De posse desses valores e tendo em vista os recursos disponíveis, cabe aos gestores decidir sobre a estratégia de gerenciamento a ser aplicada.

2.3.2.2. Análise S.W.O.T.

A análise SWOT é uma técnica baseada na identificação dos pontos fortes, dos pontos fracos, das oportunidades e das ameaças ajuda a identificar as fontes de recursos externas e

internas para suportar os objetivos negociais. Essa técnica é conhecida por análise S.W.O.T., ou seja, *strengths* (forças), *weakness* (fraquezas), *opportunities* (oportunidades) e *threats* (ameaças) e é utilizada na busca de riscos que possam afligir a organização. Pontos fortes e fraquezas dizem respeito ao ambiente interno, enquanto ameaças e oportunidades ao ambiente externo.

A análise S.W.O.T auxilia na determinação dos recursos e serviços internos e externos que o administrador dispõe para gerenciamento de seu negócio, através do tempo. Não importa o nível de terceirização utilizado, a responsabilidade sobre os recursos e serviços disponíveis é sempre do gestor.

As fortalezas identificam os pontos fortes da organização. Referem-se às competências que atribuem destaque às organizações quando comparadas com outras empresas concorrentes. Os pontos fortes são identificados a partir dos recursos e competências disponíveis dentro da empresa.

As fraquezas identificam os pontos deficientes das organizações, não apenas sob a perspectiva da empresa, mas sob a ótica dos clientes e fornecedores. Esses pontos podem ser definidos como “limitações ou deficiências em um ou mais recursos ou competências, quando comparados com outras empresas”. Essas fraquezas se refletem na eficiência das organizações.

As oportunidades, quando identificadas, proporcionam às empresas condições de crescimento dentro do mercado de atuação. As oportunidades são identificadas nos mais diversos segmentos, a partir de mudanças nas tecnologias, leis e regulamentos, comportamentos sociais etc.

A capacidade de perceber antecipadamente as mudanças ocorridas no ambiente em que atua pode se traduzir em elemento chave para o atingimento dos objetivos a serem alcançados pelas organizações.

As ameaças são circunstâncias ou situações desfavoráveis e que podem causar prejuízo aos ativos de uma organização ou ao atingimento de seus objetivos. Estão

classificadas dentro dos fatores externos às organizações, que precisam estar preparadas para enfrentá-las, embora possam estar fora de seu controle.

A tabela 2.2 nos apresenta exemplos dos fatores acima descritos.

Tabela 2.2: Fatores da análise S.W.O.T.

Fortalezas / Fraquezas	Oportunidades / Ameaças
Nível de treinamento dos funcionários.	Comportamento dos concorrentes
Infra-estrutura de tecnologia	Economia de mercado
Recursos disponíveis – financeiros, localização	Atendimento à legislação
Maturidade dos processos	Fraudes, roubos,
Diversidade de produtos	Falhas de aplicativos
	Erros operacionais

A técnica SWOT consiste em comparar os fatores internos com os externos, criando uma matriz estratégica para atuação da organização. Importante ressaltar que os fatores internos estão sujeitos aos controles da organização, não ocorrendo o mesmo com os fatores externos. Segundo Weihrich [64], do cruzamento desses fatores, demonstrado na fig 2.6, resultam 04 estratégias conforme a seguir.

1. Maxi-maxi (S/O). Combinação entre os pontos fortes e as oportunidades. Esta estratégia direciona a organização no aproveitamento de seus pontos fortes para explorar as oportunidades identificadas.

2. Maxi-mini (S/T). Combinação entre os pontos fortes e as ameaças. Em resumo, as organizações devem utilizar seus pontos fortes para minimizar as ameaças.

3. Mini-maxi (W/O). Cruzamento que mostra o fator ponto fraco atrelado às oportunidades. É uma estratégia de esforço para dominar as fraquezas fazendo o melhor a cada nova oportunidade.

4. Mini-mini (W/T). Esta combinação mostra o cruzamento entre os pontos fracos e as ameaças. É uma estratégia eminentemente defensiva, em que se procura evitar as ameaças externas.

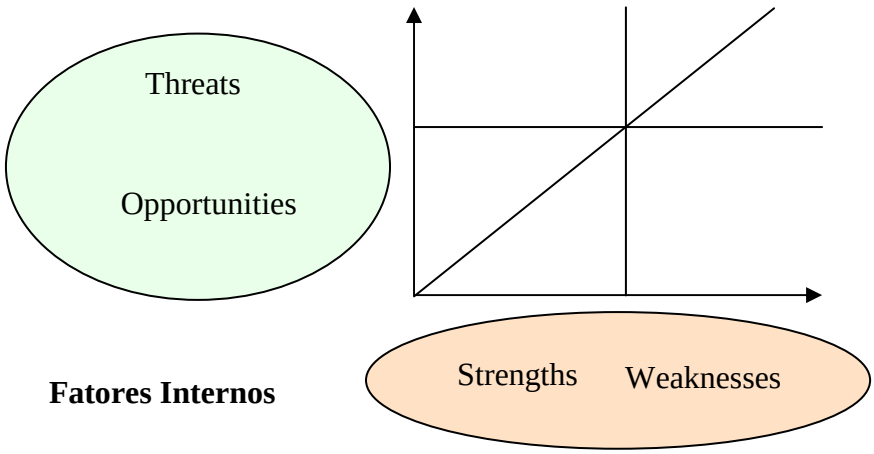


Figura 2.6: SWOT – Fatores Internos e Externos

Em uma análise SWOT o primeiro e primordial passo é a definição ou identificação dos objetivos a serem alcançados. Assim, tendo os objetivos como meta a ser alcançada, a organização deverá identificar os pontos fortes e os pontos onde há deficiências na organização. Ser capaz de monitorar o ambiente externo na busca de oportunidades de crescimento e de ganhos e na detecção de ameaças que possam por em risco os objetivos definidos. Quanto às ameaças, embora sejam fatores externos, podem surgir dentro da própria empresa, como eventos de fraudes internas, perdas de conhecimento pela saída de funcionários, dentre outros.

2.3.3. PLANEJAMENTO

A fase de planejamento é o momento em que, obtidas as informações sobre os riscos aos quais o processo se sujeita, são determinadas as ações para tratamento dos riscos. É nessa atividade que o “apetite ao risco” e as relações de custo-benefício são mais proeminentes.

Como resultado dessa fase se espera uma avaliação sobre as ameaças, vulnerabilidades e impactos, tendo em vista a adoção de medidas apropriadas para proteger as necessidades e continuidade de negócio, os recursos de informação, bem como os usuários destes recursos. O planejamento resultante deverá estabelecer as ações a serem adotadas para os riscos identificados, respeitados os resultados obtidos quanto às suas priorizações.

Ao final, algumas perguntas devem ser respondidas como forma de assegurarmos a plena consciência sobre o tratamento dispensado:

- O que será protegido?
- Do que será protegido?
- Quais as características dos riscos envolvidos?
- Qual o benefício de se proteger?
- Qual o custo estimado para se proteger?
- Qual será o impacto de não se proteger?
- Como será protegido?

Toda ação para mitigar um risco implica em um custo adicional para as empresas. Ao gerirmos riscos, adotamos basicamente as seguintes estratégias: diminuição dos impactos, diminuição da probabilidade de ocorrência, terceirização dos riscos ou aceitação dos riscos / convivência com eles.

Reportando-nos à figura 2.1, entendemos que as duas primeiras estratégias de gestão de risco buscam trazer a resultante do gráfico para mais próximo da zona de menos exposição ao risco. Assim, ao diminuirmos a probabilidade de ocorrência do risco, estamos diminuindo o grau de exposição ao risco. A mesma situação ocorre, ao diminuirmos os impactos resultantes.

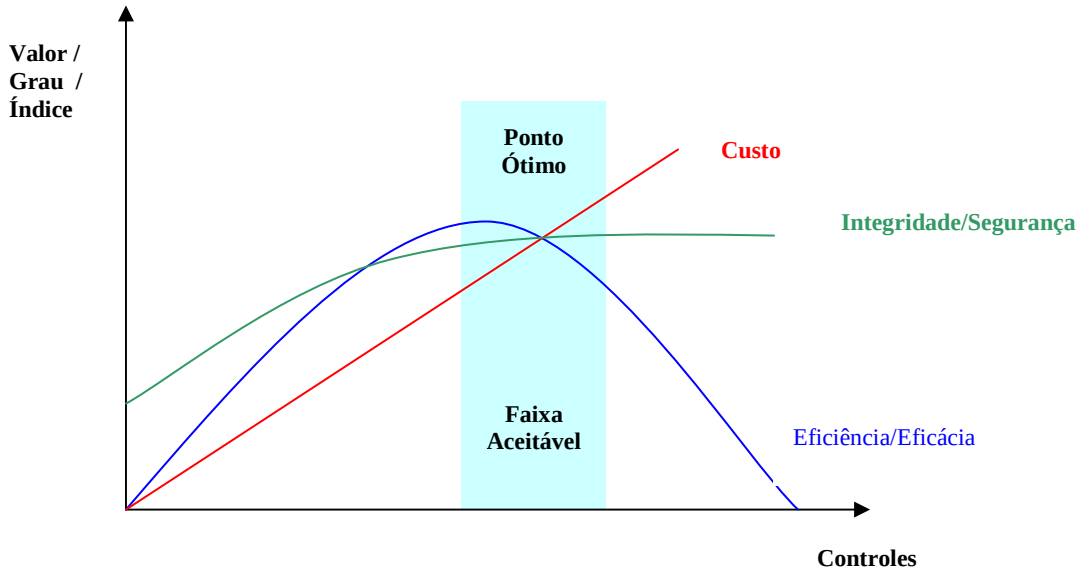
A terceira estratégia consiste em transferirmos a gestão de um risco para outra organização. O exemplo mais freqüente é o pagamento de seguros que cobrem determinados riscos, como incêndio, desmoronamento, alagamento etc. As seguradoras assumem o ressarcimento do valor segurado, mediante o pagamento de um prêmio pela empresa segurada.

Ao aceitarmos conviver com os riscos, a relação custo-benefício de implantarmos controles para minimização dos riscos deve estar representada por uma diferença positiva em favor dos custos. Nessa situação, a perda ocasionada pela efetivação do risco é avaliada como de menor valor que os custos para implementar controles.

O gráfico da figura 2.7 apresenta a relação entre a curva de eficiência/eficácia dos controles instituídos versus os custos de implantação dos controles. Verificamos que os custos de implementação de controles são sempre crescentes, enquanto a eficiência/eficácia dos controles diminui a partir de certo "ponto ótimo". Isto implica dizer que a adoção de controles sobre controles não necessariamente resulta em garantia total da minimização de um risco. A chave da questão é determinar o "ponto ótimo" de interseção entre as curvas.

O fator determinante para identificação desse ponto é justamente o custo-benefício da implementação dos controles. O benefício alcançado pelo novo controle compensa os custos associados? Se sim, é aconselhável a adoção de medidas para minimização dos riscos. Interessante observar que mesmo após a implementação dos controles, ainda restará o risco residual. Se outras medidas adicionais forem adotadas, a exposição tenderá a diminuir, até certo nível. Então resta saber se o grau de risco residual é aceito pela administração, considerado o apetite de risco.

A literatura descreve uma outra estratégia para aqueles riscos que não são passíveis de convivência, mas para os quais não identificamos ações a serem implementadas e que possam minimizá-los. Para essa situação é recomendado que se mantenha um monitoramento constante sobre esses riscos, com intuito de identificar os eventos indesejados, ainda nos estágios iniciais, adotando ações imediatas para sua correção ou diminuição dos impactos.



Fonte: ARIMA, Carlos H. Metodologia de Auditoria de Sistemas

Figura 2.7: Controles x Custos

Decidida a estratégia de mitigar os riscos, o planejamento deverá prever a adoção de medidas que visem diminuir a probabilidade de ocorrência, ou os impactos decorrentes. Essas medidas são categorizadas em três tipos:

- Medidas preventivas;
- Medidas detectivas; e
- Medidas corretivas.

As ações preventivas se prestam a detectar problemas, mesmo potenciais, antes que esses ocorram, possibilitando a adoção de medidas inibidoras. Também previnem erros, omissões ou ações maliciosas.

As medidas detectivas revelam e reportam a ocorrência de um erro, de uma omissão ou de ações maliciosas.

Já as corretivas minimizam o impacto de um fato consumado ou disparam a adoção de medidas corretivas para os problemas reportados pelas medidas detectivas. Essas ações possibilitam alterações nos processos, objetivando minimizar a recorrência dos fatos.

2.3.4. MONITORAÇÃO

A fase de monitoração consiste coletar informações precisas, relevantes e em tempo oportuno sobre o comportamento dos eventos de riscos para um processo. Essas informações servem como entrada para a fase de identificação dos riscos, dinamizando o ciclo de vida dos riscos.

Quando não nos é possível, a priori, calcular as probabilidades de ocorrência de um evento, tendo em vista não dispormos de todas as informações, o exercício do monitoramento dos fatos passados nos ajuda a identificar uma linha de comportamento dos eventos.

Em um cenário de incertezas, as informações geradas pelo monitoramento são de grande ajuda na identificação dos riscos que se apresentam.

As atividades de monitoramento exercem, grosso modo, duas grandes funções:

1. identificação de alterações nos cenários ou nos padrões de comportamento, que podem resultar no aparecimento de novos riscos; e
2. reavaliação das ações adotadas para minimização dos riscos identificados.

As informações coletadas subsidiam a avaliação da efetividade das ações em curso e possibilitam a identificação de novos padrões de comportamento, que introduzem riscos até então não imaginados, ou que elevam o grau de relevância de outros considerados de menor prioridade.

Para aquelas situações em que os riscos não são passíveis de convivência, mas não foram identificadas ações cabíveis para sua mitigação, a monitoração atua como um gatilho a disparar medidas alternativas de correção ou de contingência. Para operacionalizar esse procedimento, são estabelecidos indicadores que sejam capazes de identificar situações de risco além da desejada, ou seja, situações que extrapolem o apetite de risco da instituição.

2.3.5. COMUNICAÇÃO

A etapa prevista como comunicação trata da divulgação de informações sobre os riscos associados ao projeto ou negócio em curso por toda a equipe responsável.

Quando da identificação dos riscos, algumas técnicas foram apresentadas e objetivavam permitir que riscos fossem identificados, com base nas experiências vividas e nos conhecimentos adquiridos.

As informações produzidas em cada fase do ciclo de vida dos riscos subsidiam as etapas posteriores e ao mesmo tempo retroalimentam as anteriores, fazendo girar o ciclo.

Aplica-se então o mesmo raciocínio utilizado na identificação dos riscos. Ao comunicarmos a todos os participantes do processo as informações obtidas, contribuímos para o aprimoramento das competências individuais, que novamente são utilizadas na formação de um entendimento comum sobre os riscos, só que de uma forma mais sinérgica.

2.4. REGULAMENTAÇÃO

Toda organização, independentemente do seu tamanho ou ramo de atividade, está sujeita às leis e regulamentos estabelecidos pelos organismos de supervisão e fiscalização. Em especial, as instituições financeiras se submetem às leis não só relacionadas ao sistema financeiro, como àquelas associadas à privacidade dos dados dos clientes, e mais recentemente à lei de defesa do consumidor, dentre outras.

Após os escândalos da Enron e WorldCom, nos Estados Unidos, a qualidade das informações disponibilizadas pelos administradores passou a figurar em destaque e reforçou uma preocupação cada vez mais presente dos órgãos legisladores e de supervisão, em tornar a gestão das instituições mais transparente para o mercado e para as partes interessadas (*stakeholders*).

A dependência cada vez maior da tecnologia, associada à migração dos processos outrora manuais para sistemas informatizados, promoveu a necessidade de leis e regulamentos

ainda mais efetivos e conseqüentemente a melhoria da gestão dos riscos por parte dos administradores.

Organizações de classes, supervisores bancários e legisladores direcionam seus esforços na busca de padrões, regras e leis que garantam uma maior transparência para o mercado quanto à forma de condução dos negócios pelas instituições. Assim, vimos surgir iniciativas como os acordos Basiléia I e II, na Europa, a lei Sarbanes-Oxley, nos Estados Unidos, assim como as regras de governança corporativa e de tecnologia da informação.

No Brasil, o Banco Central divulgou as resoluções do Conselho Monetário Nacional de números 2554, 3198 e mais recentemente a 3.380, que elevam o rigor das fiscalizações, por meio do estabelecimento de critérios a serem atendidos pelas instituições financeiras instaladas no Brasil.

Nos subtópicos a seguir, resumimos os principais itens de cada legislação, procurando ressaltar as influências na área de tecnologia e na gestão dos riscos.

2.4.1. ACORDOS DA BASILÉIA I E II [2] [3]

Em 1997, o Comitê da Basiléia divulgou os “princípios essenciais da Basiléia”, em número de 25, necessários para suportar um sistema de supervisão bancária eficaz. Passam, então, a ser considerados como referências internacionais para os órgãos de supervisão bancária (Bancos Centrais) de todos os países. Entende o Comitê que a adequação de todos os países aos princípios significa o fortalecimento da estabilidade do sistema bancário internamente, em cada país, e também internacionalmente.

Os vinte e cinco princípios podem ser divididos em 06 grupos, conforme a seguir:

- precondições para uma supervisão bancária eficaz – trata das responsabilidades e objetivos dos Bancos Centrais envolvidos na supervisão de instituições bancárias;
- autorizações e estrutura – definição das atividades permitidas às instituições autorizadas a operar em cada país; autorização de funcionamento; autoridade para os Bancos Centrais examinarem propostas de transferência de controle,

bem como para examinar as aquisições e investimentos mais relevantes de um banco;

- regulamentos e requisitos prudenciais – estabelecimento de requisitos mínimos, prudentes e apropriados, de adequação de capital para os bancos. Esses requisitos devem refletir os riscos a que os bancos se submetem, definindo os componentes de capital, em função da capacidade de absorção de perdas de cada um;
- métodos de Supervisão Bancária Contínua – trata da constituição de atividades de supervisão direta ou indireta a ser exercida pelos Bancos Centrais;
- requisitos de informação – manutenção, pelos bancos, de registros que possibilitem uma avaliação precisa da real condição financeira dos bancos, aliado à publicação regular dos relatórios financeiros;
- poderes formais dos supervisores – trata da adoção de ações corretivas a serem aplicadas quando os bancos não cumprirem os requisitos prudenciais.

Destacamos os princípios 7 e 15 no que se referem à gestão dos riscos pelas instituições financeiras.

> "*Principle 7 – Risk management process: Supervisors must be satisfied that banks and banking groups have in place a comprehensive risk management process (including Board and senior management oversight) to identify, evaluate, monitor and control or mitigate all material risks and to assess their overall capital adequacy in relation to their risk profile. These processes should be commensurate with the size and complexity of the institution*".

> "*Principle 15 – Operational risk: Supervisors must be satisfied that banks have in place risk management policies and processes to identify, assess, monitor and mitigate operational risk. These policies and processes are commensurate with the size and complexity of the bank*".

O princípio 7 descreve a necessidade dos bancos adotarem um processo de gerenciamento de riscos para identificar, avaliar, monitorar e controlar ou mitigar os riscos materiais e manter capital que suporte tais riscos.

O princípio 15 determina que os bancos adotem políticas e procedimentos para identificar, avaliar, monitorar e mitigar os riscos operacionais.

Em 1998, o Comitê da Basiléia divulgou o documento “Estrutura para sistemas de controles internos em organizações bancárias”, estabelecendo 13 princípios para avaliação de sistemas de controles internos. Esse documento é a base para a Resolução 2.554, que dispõe sobre a implantação e implementação de sistema de controles internos nas instituições financeiras instaladas no Brasil.

Destacamos os princípios 4 e 5 que tratam da avaliação de riscos pelas instituições.

> “*Principle 4 – Senior management should ensure that the internal and external factors that could adversely affect the achievement of the bank’s objectives are being identified and evaluated. This assessment should cover all the various risks facing the bank (for example, credit risk, country and transfer risk, market risk, interest rate risk, liquidity risk, operational risk, legal risk and reputational risk)*”.

> “*Principle 5 – Senior management should ensure that the risks affecting the achievement of the bank’s strategies and objectives are continually being evaluated. Internal controls may need to be revised to appropriately address any new or previously uncontrolled risks*”.

O princípio 4 descreve a responsabilidade da administração superior em assegurar que fatores internos e externos que possam afetar negativamente os objetivos do banco estejam identificados e avaliados. Essa avaliação deve cobrir os mais variados riscos enfrentados pelos bancos (por exemplo, risco de crédito, risco país, risco de mercado, risco de liquidez, risco operacional, risco legal e risco de reputação).

O princípio 5 descreve a responsabilidade da administração superior em assegurar que os riscos que afetam o atingimento das estratégias e objetivos do banco sejam continuamente avaliados. Controles internos devem ser revisados como forma de identificar novos riscos ou monitorar aqueles considerados como “não controláveis”.

Desde a publicação dos treze princípios, em 1998, o chamado Acordo de Capitais da Basiléia continuou a produzir recomendações com vistas a aprimorar os controles das instituições e adequar-se às inovações financeiras e tecnológicas.

O segundo Acordo de Capitais da Basiléia, referenciado como Basiléia II, introduziu novas normas e metodologias para controle do risco operacional. Entenda-se risco operacional como “risco de perdas resultantes da inadequação dos processos internos, de falha humana e de sistemas ou decorrente de eventos externos”.

Essa definição significa que todos os processos, desde aqueles considerados como “fim” até os processos-meio, pelos quais os negócios-fim se realizam, são possíveis geradores de perdas e, assim, sujeitos aos controles internos.

O Basiléia II, que tem previsão de vigorar a partir do final de 2007, sustenta-se em três pilares: requisito mínimo de capital, processo de revisão supervisora e disciplina de mercado.

Lopes & Associados no artigo “O Novo Acordo de Capital da Basiléia” [45] descreve que “As principais mudanças estão no fim da padronização generalizada por um enfoque mais flexível, dando ênfase nas metodologias de gerenciamento de risco dos bancos, na supervisão das autoridades bancárias e no fortalecimento da disciplina de mercado. A nova estrutura pretende alinhar a avaliação da adequação de capital mais intimamente aos principais elementos dos riscos bancários e fornecer incentivos aos bancos para aumentar suas capacidades de mensuração e administração dos riscos”.

Para o nosso estudo, entendemos ser adequado explorarmos o pilar que trata do requisito mínimo de capital. Esse pilar estabelece a quantidade mínima de capital que as entidades devem manter para suportar os riscos de crédito, de mercado e operacional. Esse requisito mínimo é conhecido como índice de Basiléia e está definido como de no mínimo 8%, cuja fórmula de cálculo é mostrada na figura 2.8. A novidade que se apresenta é quanto à necessidade de alocação de capital para enfrentar os riscos operacionais.

$$\frac{\text{Capital total}}{\text{(risco de crédito + risco de mercado + risco operacional)}} = \%\ \text{do Capital}$$

Figura 2.8: índice de Basiléia

"O risco operacional apresenta-se como uma das novidades introduzidas pela revisão do acordo. Risco operacional, definido como risco de perdas resultantes de inadequação ou falhas de processos internos, pessoas e sistemas, ou de eventos externos, inclui os riscos decorrentes de não atendimento à legislação, mas exclui os riscos de estratégia e de imagem" [4]. Em suma, são as falhas que podem ocorrer no desenvolvimento das atividades do dia-a-dia.

A partir da definição de risco operacional percebemos a necessidade da disciplina de gestão de risco aplicada ao ambiente *internet banking*. Quanto melhor gerenciado o risco operacional, maior o percentual do capital, tendo em vista a diminuição do denominador da figura 2.8, pela redução do fator "risco operacional".

Embora ainda não esteja fixado seu valor, os bancos estão adotando um percentual de 20% de seu capital para cobrir os riscos operacionais.

Os três principais critérios para mensuração de risco operacional propostos pelo comitê foram:

1. Indicador Básico – determina um percentual de capital para cobrir o risco operacional, com base em um único indicador. Por exemplo: receita bruta. Um banco terá que assegurar um capital mínimo para cobrir o risco operacional igual a um percentual da Receita Bruta. Ainda não há definição pelo comitê sobre o indicador mais apropriado.

2. Critério Padrão – o banco poderá dividir suas atividades em áreas de negócios, como por exemplo: varejo, atacado e governo, aplicando para cada uma o indicador básico. A soma dos indicadores resultantes para cada segmento determinará o percentual do capital que deverá ser alocado para cobrir o risco operacional.

3. Critério de Mensuração Interno – permite que os bancos utilizem cálculos internos para a determinação do capital proposto. Os bancos poderão considerar três indicadores: a exposição ao risco operacional, mais a probabilidade de que a perda ocorra e o total da perda causada por este evento. A este cálculo, o banco aplicará um percentual que será determinado pelo Comitê, para determinação do percentual de capital.

2.4.2. SARBANES-OXLEY

A legislação federal "*The U.S. Public Company Accounting Reform and Investor Protection Act of 2002*" [5] [39], conhecida como Sarbanes-Oxley Act of 2002 ou simplesmente SOX, é uma lei aprovada pelo governo norte americano para coibir com as fraudes contábeis. Foi criada pelos senadores americanos Paul Sarbanes e Michael Oxley. Tinha como objetivo restabelecer e aumentar a confiança do investidor e a sustentabilidade das organizações, abaladas pelos escândalos financeiros verificados em empresas como Enron e Worldcom.

Todas as empresas, inclusive estrangeiras, com ações negociadas nas bolsas de valores dos EUA devem se submeter a SOX. Além do aperfeiçoamento dos padrões contábeis, a lei introduziu mudanças na responsabilidade dos administradores, na forma com que as empresas tratam os acionistas minoritários e nos relatórios de prestação de contas. A responsabilidade pela correta avaliação e monitoramento dos controles referentes aos processos internos fica atribuída aos principais administradores das empresas, que se irregular estão sujeitas a multas de milhões de dólares e seus administradores a penas de 10 a 20 anos de prisão.

A seção 302 da SOX trata da responsabilidade pessoal dos diretores executivos e financeiros, enquanto a seção 404 determina a avaliação anual dos controles e procedimentos internos para fins de emissão do relatório financeiro. Sendo assim, a que mais impacta a área de TI. A incorporação dos processos de negócios aos sistemas de tecnologia da informação faz com que a aplicabilidade da lei recaia diretamente sobre esse segmento.

De acordo com Rodney de Castro Peixoto [52] "A Seção 404 da lei é o principal foco de atenção das empresas neste particular, por trazer os mandamentos sobre os controles de processos internos e sistemas contábeis. Esta Seção determina uma avaliação anual dos

controles e processos internos para a realização de relatórios financeiros, com a obrigação de emissão de relatório, a ser encaminhado a SEC – *Security Exchange Comission*, órgão regulador das empresas de capital aberto dos EUA, que ateste estes parâmetros". Dentre outros itens, o relatório deverá conter atestado de responsabilidade dos administradores da empresa e manutenção da estrutura dos controles internos.

Ainda segundo Peixoto "temos, por força da Sarbanes-Oxley, a obrigatoriedade da observância de práticas de segurança de redes e critérios rígidos para uso de aplicações terceirizadas por companhias que se encontram ao alcance da presente lei".

Invasões em sistemas, vírus, roubo de dados, fraudes de senhas e demais ameaças à segurança das informações podem, se não houver prova suficiente de adoção de medidas preventivas, implicar em responsabilidade direta dos administradores, com possibilidades de sanções civis e penais.

Peixoto levanta a preocupação com dois pontos quanto à tecnologia da informação:

1. Segurança de sistemas de informação – as políticas de segurança da informação devem ser adaptadas ao teor da Sarbanes-Oxley, contemplando inclusive a responsabilidade pela segurança do ambiente de *Internet*.

2. Controle de registros – estabelecimento de procedimentos que garantam a integridade, a confiabilidade e a guarda e recuperação dos registros das operações, quer sejam em papel, quer em mídia eletrônica. Na lei encontram-se disposições que penalizam severamente a falsificação, destruição e perda de documentos e registros, bem como a inobservância dos prazos para armazenamento.

A constituição de um comitê de auditoria é uma novidade introduzida pela SOX, atribuindo a esse comitê a responsabilidade de supervisionar o trabalho dos auditores.

A SOX requer que, além de desenvolver os controles internos, os executivos analisem e certifiquem o funcionamento desses mecanismos de controle. Exige, ainda que o auditor externo certifique a avaliação feita pela administração e emita relatório. Assim é

indispensável o perfeito funcionamento dos controles internos, fornecendo segurança aos administradores e auditores.

Como forma de auxiliar as empresas na missão de desenvolver um sistema de controles internos, o COSO – (*Commitee of Sponsoring Organizations of the Treadway Commission*) [44] – apresenta uma estrutura baseada em cinco componentes, conforme a seguir:

1. Ambiente de controle – estabelece a forma de atuação de uma empresa e constitui a base para um sistema de controles internos eficiente. Compreende o estabelecimento, pela administração, de um ambiente ético de controle e cultura;

2. Avaliação de riscos – estabelecimento de mecanismo que identifique, analise e administre os riscos relacionados ao negócio da empresa;

3. Atividades de controle – políticas e procedimentos de controle devem ser estabelecidos e executados, a fim de assegurar que as ações adotadas pela administração para gerir os riscos estejam sendo, efetivamente, executadas;

4. Informação e comunicação – os sistemas de comunicação e informação devem permitir que as pessoas da empresa obtenham e forneçam informações adequadas à condução, ao gerenciamento e ao controle das operações.

5. Monitoramento – o processo inteiro deve ser monitorado e as modificações introduzidas, assegurando que o sistema de controle interno mantenha a sua efetividade.

2.4.3. LEGISLAÇÃO BRASILEIRA

O Sistema Financeiro Nacional e em especial o sistema bancário é um dos mais avançados do mundo em tecnologia. Os canais eletrônicos são responsáveis pela maioria das transações efetuadas pelos clientes, superando àquelas executadas pelos meios tradicionais,

com o uso dos caixas “manuais” nas agências. Documentos outrora existentes, como a transferência de fundos com uso dos “DOC”, em papel, praticamente inexistem, tendo sido substituídos pelas TED (Transferência Eletrônica Disponível) ou pelos DOC eletrônicos.

Como conseqüência natural dessa evolução, as leis e regulamentos tiveram que ser adaptados, ou mesmo criados para amparar o funcionamento eficaz e transparente das instituições financeiras.

Como vimos na seção 2.4.1, o Comitê da Basiléia conjuntamente com os Bancos Centrais mundiais enfatizam cada vez mais a importância dos controles internos nas instituições, descrevendo não só as medidas regulatórias, mas dando ênfase ao desenvolvimento efetivo de atividades de supervisão.

O princípio 13 da Basiléia determina que “os supervisores bancários devem se assegurar de que os bancos adotam um processo abrangente de administração de risco (incluindo a supervisão adequada pelo conselho de diretores e pela administração sênior), para identificar, medir, monitorar e controlar todos os demais riscos materiais e, quando necessário, para manter capital contra tais riscos” [2].

A resolução 2.554 é a resposta a esse princípio.

2.4.3.1. Resolução 2.554

A Resolução 2.554 [7] dispõe sobre a implantação e implementação de sistema de controles internos. O Banco Central do Brasil, em setembro de 1998, tornou pública a resolução do CMN – Conselho Monetário Nacional que contemplou medidas quanto:

- a supervisão gerencial e cultura de controles;
- a identificação, avaliação e tratamento dado aos riscos;
- aos procedimentos de controle e segregação de funções;
- a informação e comunicação;
- as atividades de monitoramento e correção de deficiências; e
- a avaliação do sistema de controles internos pelas autoridades.

O artigo 2º desta resolução contempla as diretrizes relacionadas à gestão de riscos em seus incisos III e V e parágrafo 1º.

> "Art. 2º Os controles internos, cujas disposições devem ser acessíveis a todos os funcionários da instituição de forma a assegurar que sejam conhecidas a respectiva função no processo e as responsabilidades atribuídas aos diversos níveis da organização, devem prever":
> III – meios de identificar e avaliar fatores internos e externos que possam afetar adversamente a realização dos objetivos da instituição;
> V – a contínua avaliação dos diversos riscos associados às atividades da instituição;
>
> Parágrafo 1º Os controles internos devem ser periodicamente revisados e atualizados, de forma a que sejam a eles incorporadas medidas relacionadas a riscos novos ou anteriormente não abordados.

2.4.3.2. Resolução 3.198

A lei Sarbanes-Oxley determinou a constituição de um comitê de auditoria, atribuindo a este a responsabilidade de supervisionar o trabalho dos auditores.

A resolução do Banco Central do Brasil de número 3.081, de maio de 2003, criou a exigência de que as instituições financeiras possuam comitê de auditoria, com as atribuições de monitorar a efetividade dos processos operacionais e o cumprimento das normas legais. A resolução 3.198 [8], de maio de 2004, altera e revoga a 3.081.

O capítulo V, artigo 10 trata da criação e do funcionamento do comitê de auditoria e assim descreve:

> "Art. 10. Devem constituir órgão estatutário denominado comitê de auditoria as instituições referidas no art. 1º, inciso I, alínea ´a´, que tenham apresentado no encerramento dos dois últimos exercícios sociais:
> I - Patrimônio de Referência (PR) igual ou superior a R$ 1.000.000.000,00 (um bilhão de reais); ou

II - administração de recursos de terceiros em montante igual ou superior a R$ 1.000.000.000,00 (um bilhão de reais); ou

III - somatório das captações de depósitos e de administração de recursos de terceiros em montante igual ou superior a R$ 5.000.000.000,00 (cinco bilhões de reais)".

§ 4º As instituições devem ter o comitê de auditoria em pleno funcionamento até o dia 31 de março do exercício subseqüente aos exercícios previstos no caput, cumprindo suas atribuições inclusive no que se refere às demonstrações contábeis daquela data-base.

§ 5º Para as instituições que se enquadrem no disposto no caput ou no § 1º, relativamente aos exercícios de 2002 e 2003, o comitê de auditoria deve estar instalado e em pleno funcionamento até 1º de julho de 2004.

Dentre as funções previstas para o comitê de auditoria destacamos, no artigo 15, os incisos VI e VII:

"VI – estabelecer e divulgar procedimentos para recepção e tratamento de informações acerca do descumprimento de dispositivos legais e normativos aplicáveis à instituição, além de regulamentos e códigos internos, inclusive com previsão de procedimentos específicos para proteção do prestador e da confidencialidade da informação;

VII – recomendar, à diretoria da instituição, correção ou aprimoramento de políticas, práticas e procedimentos identificados no âmbito de suas atribuições".

O art. 17. prevê que ao final dos semestres findos em 30 de junho e 31 de dezembro, o comitê de auditoria deva elaborar, documento denominado relatório do comitê de auditoria contendo diversas informações, dentre as quais destacamos os incisos II, III e IV:

"II – avaliação da efetividade dos sistemas de controle interno da instituição, com ênfase no cumprimento do disposto na Resolução 2.554, de 24 de setembro de 1998, e com evidenciação das deficiências detectadas;

III – descrição das recomendações apresentadas à diretoria, com evidenciação daquelas não acatadas e respectivas justificativas;

IV – avaliação da efetividade das auditorias independente e interna, inclusive quanto à verificação do cumprimento de dispositivos legais e normativos aplicáveis à

instituição, além de regulamentos e códigos internos, com evidenciação das deficiências detectadas".

2.4.3.3. Resolução 3.380

O Banco Central do Brasil [9], através da resolução 3.380, tornou público que o Conselho Monetário Nacional resolveu determinar às instituições financeiras a implementação de estrutura de gerenciamento do risco operacional. Entre os eventos de risco operacional destacamos:

I. fraudes internas;
II. fraudes externas;
III. aqueles que acarretam a interrupção das atividades da instituição;
IV. falhas em sistemas de tecnologia da informação;

A estrutura de gerenciamento do risco operacional deve prever, dentre outras medidas:

I. identificação, avaliação, monitoramento, controle e mitigação do risco operacional;
II. documentação e armazenamento de informações referentes às perdas operacionais;
III. elaboração e disseminação da política de gerenciamento de risco operacional ao pessoal da instituição;
IV. existência de plano de contingência;

A estrutura de gerenciamento do risco operacional deve estar capacitada a identificar, avaliar, monitorar, controlar e mitigar os riscos associados a cada instituição.

2.4.4. GOVERNANÇA CORPORATIVA

No intuito de tornar a gestão das organizações mais transparente para o mercado e para todas as partes interessadas, o conceito de Governança Corporativa ganhou aceitação e difundiu-se entre as empresas, como práticas referenciais de gestão a serem adotadas e

principalmente como subsídio na decisão dos investidores em colocar ou não seus ativos financeiros nessas empresas.

O IBGC – Instituto Brasileiro de Governança Corporativa [34] assim a define:

"Governança corporativa é o sistema pelo qual as sociedades são dirigidas e monitoradas, envolvendo os relacionamentos entre Acionistas/Cotistas, Conselho de Administração, Diretoria, Auditoria Independente e Conselho Fiscal. As boas práticas de governança corporativa têm a finalidade de aumentar o valor da sociedade, facilitar seu acesso ao capital e contribuir para a sua perenidade".

Ressalte-se que Governança não é uma legislação a qual as organizações devam se submeter, mas boas práticas a serem utilizadas na administração dos recursos disponíveis para condução e continuidade dos negócios. Essas boas práticas estão calcadas principalmente no fornecimento ao mercado de informações precisas e transparentes, na igualdade de direitos entre os acionistas e na atuação independente do Conselho de Administração.

É de se esperar que as empresas com uma estrutura de governança corporativa mais adequada às boas práticas obtenham melhores resultados e tenham suas ações mais valorizadas pelo mercado financeiro.

Em Governança Corporativa, Desempenho e Valor da Empresa no Brasil, Alexandre Di Miceli da Silveira [54] discorre que "a discussão sobre governança corporativa envolve a criação de mecanismos externos e internos que assegurem que as decisões corporativas serão tomadas no melhor interesse dos investidores, de forma a maximizar a probabilidade dos fornecedores de recursos obterem para si o retorno sobre seu investimento". Assim, a empresa que quiser sobreviver com responsabilidade terá como objetivo maior a maximização do retorno aos seus acionistas. Contudo, sem prejudicar o conjunto da sociedade e/ou o meio ambiente, ou ainda tendo como base a violação dos princípios legais e éticos que orientam o seu negócio.

Um dos principais mecanismos de governança é o Conselho de Administração, ao qual compete, entre outras, controlar a alta administração, fiscalizar e avaliar o desempenho da gestão.

O IBGC foi responsável pela elaboração, no Brasil, do Código das Melhores Práticas de Governança Corporativa. O Código está dividido em seis capítulos e aborda o Conselho de Administração e temas relativos à propriedade/acionistas, gestão, auditoria independente, Conselho Fiscal e conflito de interesses.

Quanto ao gerenciamento de riscos, o código estabelece em seu capítulo 2 que "o Conselho de Administração deve assegurar-se de que a Diretoria identifique preventivamente – por meio de sistema de informações adequado – e liste os principais riscos aos quais a sociedade está exposta, sua probabilidade de ocorrência, bem como as medidas e os planos adotados para sua prevenção ou minimização".

Ainda no capítulo 2, o código prescreve que "a auditoria interna deve reportar-se ao Comitê de Auditoria ou, na falta deste, ao Conselho de Administração. Sua competência é verificar o funcionamento dos controles internos e se os regulamentos, instruções e políticas estão sendo observados".

2.5. O PAPEL DA AUDITORIA NA AVALIAÇÃO DE RISCOS

Uma primeira definição a ser reforçada é quanto à responsabilidade da administração das empresas na gestão dos riscos. É sim atribuição destes estabelecer processo de gerenciamento de riscos, estabelecendo estratégias e atribuindo aos gestores as suas implementações. A existência e funcionamento de uma efetiva gestão de riscos contribuem decididamente para o atingimento dos objetivos definidos.

A crescente importância que a gestão dos riscos vem suscitando nas empresas reflete-se nas funções desempenhadas pela auditoria. As orientações de Turnbull, divulgadas pela Bolsa de Valores de Londres, estabelecem que todas as pessoas dentro de uma organização possuem, em graus diferentes, responsabilidades pela gestão do risco. Neste sentido, a auditoria, no papel de supervisão, contribui em garantir que o processo de gestão de risco esteja efetivamente funcionando. Para que o trabalho desenvolvido pela auditoria se revista de um caráter de agregação de valor, é adequado que ela emita parecer sobre a condução do processo de gestão de riscos pelos gestores.

Encontramos em "*The Role of Internal Audit in Risk Management*" [61] o papel da auditoria assim traduzido:

Focar o trabalho da auditoria interna nos riscos mais relevantes que a organização enfrenta, identificados pelos gestores, e auditar o processo de gestão de riscos, assegurando à organização que esses estão minimizados a níveis aceitáveis, ou não.

Segundo David M Griffiths "A auditoria fornece a garantia independente e objetiva, à direção da Organização, de que seus riscos estão mitigados a um nível aceitável e relata onde não estão".

De acordo com o *The Institute of Internal Auditors*, o papel da Auditoria é rever o processo de gestão de riscos que está sendo adotado na redução do nível de riscos aceitáveis pela Administração (apetite de risco).

Esses conceitos representam o que há de mais moderno quanto ao papel a ser desempenhado pela auditoria. Um papel de assessoramento à alta administração quanto ao desenvolvimento e condução dos processos de gestão de riscos na organização, contemplando a identificação, análise e ações de mitigação dos riscos.

3. METODOLOGIA

O objetivo desse trabalho consiste em demonstrar a aplicabilidade de um modelo de gerenciamento de riscos em uma situação real vivenciada por instituições financeiras, instaladas no Brasil.

Assim, partimos da identificação da situação real, qual seja o ambiente de *internet banking*, que se constitui na disponibilização para os clientes de um canal eletrônico para realização de transações bancárias.

Identificamos alguns modelos de gerenciamento de riscos para, então, adotarmos aquele que consideramos mais próximo à realidade das instituições e, conseqüentemente, mais factível à sua utilização. Esse modelo é constituído das seguintes fases ou etapas: identificação de riscos, análise dos riscos identificados, planejamento das ações para gestão dos riscos, monitoração do ambiente das instituições e comunicação dos resultados.

A metodologia, descrita a seguir, possibilita atingir o objetivo inicialmente proposto podendo ser utilizada por qualquer instituição financeira.

3.1. IDENTIFICAÇÃO DOS RISCOS

Essa etapa se inicia pelo mapeamento do processo de *internet banking* disponibilizado aos clientes das instituições financeiras. Nesta etapa, são identificados os ambientes que constituem o *internet banking*, ou seja, o ambiente do cliente, a rede *internet* e o ambiente da instituição.

Identificados os ambientes, determinamos os possíveis riscos que podem impedir a disponibilização dos serviços bancários. Esses riscos foram categorizados em: operacionais, legais e de imagem. Não significa que essas três categorias abranjam todo o conjunto de riscos. Para esse trabalho, limitamos a abordagem para melhor demonstrar a aplicabilidade da metodologia. O leitor poderá ampliar as categorias, de acordo com suas necessidades. A identificação dos riscos é feita para cada um dos ambientes que constituem o *internet banking*.

Para que os riscos se tornem realidade é necessário que uma ameaça explore uma determinada vulnerabilidade do ambiente, causando impacto nos serviços oferecidos. Assim, apresentamos as principais ameaças e as mais significativas vulnerabilidades para os ambientes de *internet banking*.

3.2. ANÁLISE DOS RISCOS IDENTIFICADOS

Nessa etapa, os riscos identificados são classificados de acordo com sua criticidade para a instituição. Essa classificação é realizada por meio da adoção de uma matriz de risco, que neste trabalho, baseia-se em dois indicadores: impacto e probabilidade.

Os impactos podem ser de diversas ordens, desde prejuízos financeiros até prejuízos de imagem, retratada em danos à marca da organização.

A outra vertente consiste em determinar a probabilidade do risco ocorrer, tendo em vista os controles instituídos.

De posse desses dois indicadores, é possível determinar o nível de exposição que a organização se encontra perante o risco avaliado.

Outras formas de medir o nível de criticidade de um risco podem ser adotadas. Nesse sentido, apresentamos a metodologia AHP – *Analytic Hierarchy Process* [55].

Analisamos os diversos tipos de ameaças para cada ambiente, com base em séries históricas de ataques disparados contra os serviços de *internet banking*.

Com base nos dados colhidos, procedemos às análises conclusivas com objetivo de identificar padrões de comportamento e comprovar a efetividade da adoção de modelo de gerenciamento de riscos. Historicamente, sabe-se que as instituições bancárias quase sempre combateram as fraudes de forma reativa.

O resultado da análise das séries históricas possibilita determinar a efetividade e a tempestividade das ações adotadas pelas instituições.

A adoção de um modelo de gerenciamento de riscos atua de modo preventivo e contínuo, possibilitando ações mais rápidas e, conseqüentemente, estancar as perdas resultantes dessas fraudes.

3.3. PLANEJAMENTO DE AÇÕES PARA GESTÃO DOS RISCOS

A fase de planejamento se resume na adoção de medidas, por parte dos administradores, para minimização dos riscos identificados e analisados.

A matriz de riscos fornece o direcionamento das ações a serem adotadas, tendo por base o nível de criticidade de cada risco identificado.

Apresentamos as seguintes estratégias para gerir os riscos: diminuição dos impactos, diminuição da probabilidade de ocorrência, terceirização da gestão dos riscos e convivência com o risco. Para cada uma dessas estratégias são adotadas medidas de caráter preventivo, detectivo e corretivo.

Como forma de aprimorar o gerenciamento das ações adotadas apresentamos, no anexo II, planilha para controle dos riscos identificados. A planilha constitui-se em um excelente instrumento gerencial para o planejamento e acompanhamento das ações instituídas para gerenciamento dos riscos.

3.4. MONITORAÇÃO

A fase de monitoração identifica e relata os ataques disparados contra os ambientes que constituem o *internet banking*. O exercício dessa atividade é fundamental para o sucesso da metodologia aqui apresentada.

Acompanhamos, durante trinta dias, os trabalhos das equipes responsáveis pelo monitoramento dos ambientes das instituições financeiras. Ao final desse período, identificamos as principais ameaças lançadas contra os Bancos e seus clientes.

De acordo com a metodologia, aqui proposta, essas informações servirão de insumo para as etapas de identificação, análise e planejamento das ações de gerenciamento de riscos.

Os relatos provenientes desse monitoramento informam, dentre outros, a evolução dos riscos mapeados, a eficácia dos controles instituídos, o aparecimento de novas ameaças, o comportamento dos atacantes etc.

3.5. COMUNICAÇÃO

A fase de comunicação age como catalisador de todas as demais etapas. Mantém os responsáveis pelas demais etapas cientes sobre as mudanças no ambiente monitorado, divulga o aparecimento de novas ameaças, fornece informações que subsidiam a avaliação das medidas adotadas e dissemina o conhecimento entre os diversos atores responsáveis por cada etapa.

O processo de comunicação deve ser claro e conhecido por todos os integrantes das diversas equipes responsáveis pelas demais etapas. Dessa forma, é possível agir com maior rapidez na adoção de medidas de segurança, minimizando os impactos advindos de uma ameaça.

4. APLICAÇÃO DO MODELO DE GERENCIAMENTO DE RISCOS AO AMBIENTE DE INTERNET BANKING

Este capítulo é dedicado à aplicação dos conceitos apresentados e do modelo de gerenciamento de riscos quando gerenciados os riscos inerentes ao serviço de *internet banking*.

Percorremos cada etapa do modelo de gerenciamento de risco proposto, apresentando os resultados obtidos durante a pesquisa e nas fases que compõem o modelo.

4.1. IDENTIFICAÇÃO DE RISCOS NO AMBIENTE INTERNET BANKING

À medida que a sociedade humana evolui, novas ferramentas e tecnologias surgem como conseqüência natural, levando a sociedade a uma dependência crescente dessas inovações. Essa sujeição é percebida nas organizações de todos os portes, na medida em que a operacionalização dos negócios é vista como impraticável sem o auxílio dos sistemas computadorizados. Durante todas as fases da evolução humana, a presença de pessoas de boa e má índole é observada rotineiramente. Falamos isso para ressaltar a forte influência que os maus elementos exercem na exploração não só das vulnerabilidades dos artefatos, como das outras pessoas, usuárias das ferramentas e tecnologias.

O canal *internet banking* tem sido a “bola da vez” dentro da evolução dos serviços bancários. Muito se fala de suas vulnerabilidades, do volume de fraudes perpetradas e dos recursos investidos pelas instituições financeiras na busca de maior segurança para seus clientes. Contudo, o elo humano, a capacitação dos clientes na utilização das tecnologias é uma vertente nem sempre bem observada por algumas instituições, quando da avaliação dos riscos desse ambiente. É bom lembrar que as fraudes bancárias não surgiram com o advento dos serviços de *on-line banking*. Até poucos anos atrás, o instrumento de “contra-ordem” de cheques inexistia em grandes bancos ingleses. A premissa usada pelas instituições era de que a responsabilidade pela segurança dos cheques é dos clientes. No Brasil, nas décadas de 80 e

90, quando a utilização de cheques era bastante elevada, o número de fraudes com cheques era também bastante preocupante.

A complexidade e, antagonicamente, as facilidades advindas das interconexões das redes mundiais trouxeram consigo um aumento significativo nos riscos de segurança e no acesso a ferramentas de ataque, utilizadas antigamente apenas por agências de inteligência.

De *spans* à infestação de vírus, o uso dos computadores domésticos como "zumbis" é cada vez mais crescente. Cada computador que possa ser infectado e usado para propósitos malévolos é um alvo em potencial, tanto para destino final dos ataques, como para lançamento de ataques do tipo *Distributed Denial of Service* (DoS).

Da página da British Bankers´ Association [12] extraímos uma preocupação das autoridades com a fraude bancária. O volume de perdas com as fraudes e os gastos investidos pelas instituições para combatê-las estão representadas como um custo a mais para a sociedade. Os reflexos podem ser percebidos no aumento das tarifas bancárias e nos procedimentos adicionais de controle sobre as transações. Essa mesma preocupação existe no setor bancário brasileiro. Embora o Brasil possua um dos sistemas bancários mais avançados do mundo, não está imune às ações criminosas de pessoas que utilizam o canal *internet* para cometerem delitos, antes praticados dentro das agências.

Sabedores das facilidades proporcionadas aos seus clientes – na economicidade de tempo e comodidade de acesso às transações – bem como na redução de seus custos operacionais, os bancos investem cada vez no aprimoramento da tecnologia e nas medidas de segurança. Por sua vez, as modalidades de golpes crescem a cada dia em volume e em diversidade, desafiando não só os especialistas da área de tecnologia, mas a sociedade e as autoridades públicas.

Destarte, é imprescindível que os bancos exerçam uma gestão sobre os riscos inerentes ao canal *internet banking*, como forma de reduzir sua exposição, por meio da identificação das ameaças e das vulnerabilidades a que estão sujeitos, contribuindo para o alcance dos objetivos estratégicos estabelecidos, com conseqüente elevação do nível de satisfação de seus clientes.

4.2. A PRÁTICA DO MODELO DE GERENCIANDO DE RISCOS

Neste ponto, entendemos ser necessário equalizarmos os conceitos e objetivos do *internet banking*. Afinal, o primeiro passo na gestão de riscos consiste na compreensão dos objetivos a serem atingidos.

Também chamado de *on-line banking* ou *e-banking*, trata-se de disponibilizar aos usuários canal eletrônico de comunicação para entrega automática de produtos e serviços bancários diretamente aos clientes. Dentre os diversos produtos e serviços, hoje disponíveis, destacamos o acesso às contas correntes e de investimento, pagamentos de contas e compras de serviços (a exemplo de recarga de celulares e aquisição de ações).

A operacionalização desses produtos e serviços se dá por meio do uso de dispositivos eletrônicos por parte dos clientes (computadores, *palms*, celulares) que se conectam aos servidores dos bancos através da rede mundial de computadores. Resumidamente, o objetivo do *e-banking* é fornecer produtos e serviços bancários aos seus clientes, por meio do uso da *internet*.

Com esse objetivo, é fundamental que os bancos possam identificar positivamente seus clientes, apresentar ao usuário o local verdadeiro do *site* da instituição para realização das transações e garantir a segurança dos dados armazenados.

No segundo capítulo deste trabalho, apresentamos a gestão de riscos como um processo para disciplinar nossa convivência com a possibilidade de ocorrer um evento que pode causar danos. Para os serviços de *internet banking*, a gestão de riscos é o processo que possibilita a conciliação entre o fornecimento de um serviço considerado diferencial de mercado e a exposição aos mais diversos riscos para as instituições e seus clientes. A seguir propusemos um ciclo de vida para a gestão de riscos dividido em cinco fases, quais sejam: identificação, análise, planejamento, monitoração e comunicação.

Aliado a este estudo e como subsídio às proposições aqui apresentadas, realizamos pesquisa sobre os ataques desferidos contra as instituições financeiras instaladas no Brasil, bem como as medidas de defesa implementadas. O monitoramento dos ataques foi realizado no período de 01/05/2006 a 31/05/2006.

Ressalte-se que algumas instituições financeiras no Brasil exercem uma atuação conjunta no monitoramento, análise e comunicação dos eventos maliciosos detectados, contribuindo para o fortalecimento e aprimoramento do canal *internet banking*. Esse monitoramento aponta eventos maliciosos detectados não somente contra o respectivo banco, mas contra os demais bancos co-participantes.

A seguir conciliamos a teoria exposta no capítulo 2, com a realidade enfrentada pelos bancos no gerenciamento dos riscos para o ambiente *internet*, por meio da aplicação do modelo de gestão de riscos apresentado neste trabalho, contemplando cada uma das fases do ciclo de vida dos riscos.

4.2.1. IDENTIFICAÇÃO DE RISCOS NO AMBIENTE DE INTERNET BANKING

A fase de identificação de riscos parte, em primeiro lugar, do conhecimento do processo em curso, da determinação de seus objetivos e de suas diversas interações com os ambientes internos e externos, nos quais o processo esteja inserido. A análise S.W.O.T auxilia na determinação dos recursos e serviços internos e externos que o administrador dispõe para gerenciamento de seu negócio.

De acordo com Kevin Knight [43], “o segredo da gestão de riscos está em identificar os riscos que precisam ser gerenciados efetivamente para que os objetivos estratégicos da companhia não sejam ameaçados”. A estratégia para se obter uma gestão efetiva é concentrar-se na administração dos riscos mais críticos, ou seja, nos que possam impactar o atingimento dos objetivos. A fase de identificação tem como propósito mapear esses riscos de forma contínua. Não devemos imaginar que uma vez terminada essa fase, não haja mais necessidade de retomá-la. O ciclo de fases (fig. 2.2) gira continuamente e o monitoramento está constantemente retroalimentando as fases iniciais.

Somente a constante revisão dos riscos garante seu gerenciamento ao:

- maximizar as oportunidades advindas;
- explorar os pontos fortes e dominar as fraquezas mapeadas na organização; e
- minimizar as ameaças identificadas.

As instituições financeiras continuamente enfrentam os riscos inerentes a cada canal de comunicação com seus clientes. O ambiente de *internet*, como um canal adicional, trouxe comodidade e facilidade no acesso pelos clientes aos serviços bancários. Contudo, potencializou a exposição ao risco de roubo de informações sobre a identidade dos clientes e quanto à autenticação dos clientes, perante as instituições, na execução das transações bancárias.

Assim, o primeiro passo desta etapa consiste em conhecer o ambiente no qual as transações de *internet banking* se realizam, sendo vigilante na identificação proativa de ameaças, possibilitando implementar medidas de ajustes em seus sistemas para desta forma proteger a integridade, confidencialidade e disponibilidade das informações armazenadas.

As instituições financeiras podem optar por ter seus serviços de *internet banking* suportados pela própria organização, ou de forma alternativa, podem terceirizar qualquer parte desse serviço.

Ao adotar a solução terceirizada a instituição tem o mesmo objetivo a ser atingido, ou seja: disponibilizar aos usuários canal eletrônico de comunicação para entrega automática de produtos e serviços bancários. A alternativa se faz viável para:

- redução de custos;
- direcionamento dos esforços da organização para seu "*core business*", ou seja, manter o foco nos negócios;
- melhoria da solução, tendo como premissa que a empresa terceirizada é especialista na sua área de atuação;

Entretanto, ao se decidir por uma solução terceirizada, a instituição não se isenta do gerenciamento de riscos, pois aos clientes a disponibilização dos serviços é feita de forma transparente, como se fosse pelo próprio banco. Assim, outros riscos se somam aos já presentes na solução on-line. Esse adicional de risco está ligado aos seguintes fatores, dentre outros:

- confidencialidade dos dados trafegados, processados e armazenados no ambiente terceirizado;

- continuidade da empresa terceirizada, ou seja, capacidade da empresa terceirizada manter-se atuante no mercado;
- dependência da instituição ao terceirizado. A instituição fica totalmente dependente de outra no fornecimento dos serviços, podendo acarretar dificuldades quando das negociações para renovação de contrato;
- procedimentos de encerramento de contrato e transferência dos serviços para outra empresa;

No site da FFIEC [25] encontramos a figura 4.1 que nos apresenta o ambiente de *internet* no caso de processamento "*in-house*", ou seja, o próprio banco fornece o serviço de hospedagem de seu *site*. Esse tipo de ambiente é o mais freqüente entre as maiores instituições bancárias instaladas no Brasil e sobre o qual esse trabalho se baseia.

Desse diagrama identificamos, basicamente, três ambientes: o ambiente do usuário que engloba o fluxo da transação desde o computador do cliente até a entrega dos pacotes tcp/ip na *internet*. O segundo ambiente compreende o recebimento e a entrega dos pacotes tcp/ip através da rede mundial. Por fim, o ambiente de processamento das transações na própria instituição financeira.

A pesquisa realizada nos bancos brasileiros, para fundamentação deste trabalho, abordou os ataques nos ambientes do usuário (primeiro ambiente) e das instituições financeiras (terceiro ambiente).

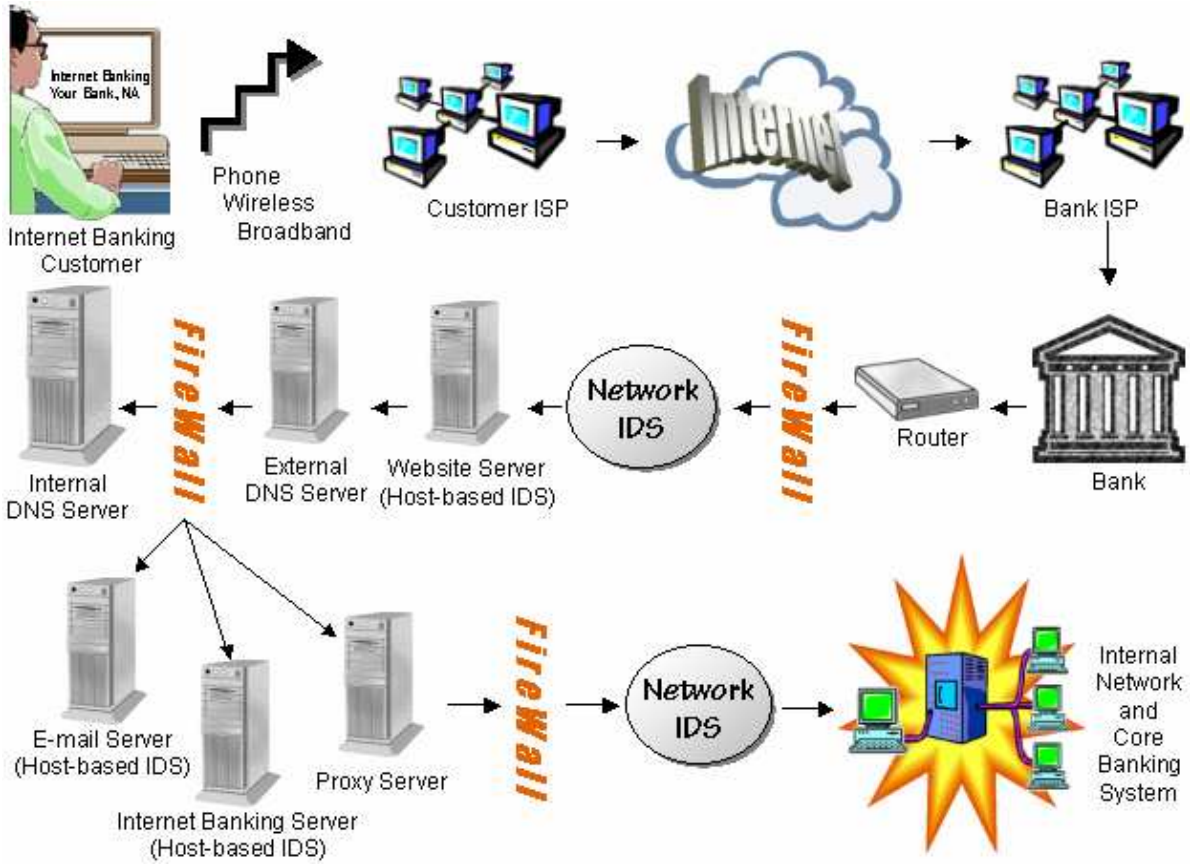
Embora sejam conhecidos os riscos quanto à monitoração e captura dos dados em transferência (segundo ambiente), os bancos adotam o uso de criptografia para os dados transmitidos e partem do pressuposto de que o nível de criptografia usado é suficiente para desestimular os ataques nesse ambiente.

O pressuposto reside na confiança depositada nos algoritmos criptográficos de mercado que asseveram que mesmo que os dados sejam capturados, sua compreensão não será possível, a não ser pela quebra da criptografia. Ao adotar algoritmos compatíveis com os padrões de mercado, as instituições financeiras transferem as iniciativas de monitoração de riscos e melhoria das soluções criptográficas para organismos mundiais ligados às ações de

segurança nessa área. Em suma, a estratégia consiste em manter-se atualizado quanto aos padrões mundiais de criptografia.

Essa abordagem está perfeitamente aderente às estratégias de gestão de riscos, descritas na seção 2.3.3, ou seja: diminuição dos impactos, diminuição da probabilidade de ocorrência, terceirização dos riscos ou aceitação dos riscos / convivência com eles. Neste caso, as instituições transferem a gestão do risco de quebra dos algoritmos criptográficos para outras entidades.

O ambiente de *internet banking* compreende dois tipos de *web sites*: os que fornecem informações aos usuários, não obrigatoriamente clientes e os que disponibilizam as transações bancárias para os clientes. É evidente que a análise de riscos para cada um deles tem abordagens diferentes, face aos objetivos a que se destinam.



Fonte: FFIEC – Federal Financial Institutions Examination Council's

Figura 4.1: Diagrama ambiente internet banking

4.2.1.1. Web sites Institucionais

Os *web sites* destinados ao fornecimento de informações possibilitam acesso de qualquer usuário às chamadas páginas institucionais, ou seja, provêm informações sobre as empresas, seus produtos e serviços, dicas de segurança, resultados financeiros etc.

Na identificação dos riscos inerentes a esse serviço, devem ser considerados os seguintes fatores:

- Fornecimento de informações imprecisas ou incompletas sobre produtos, serviços e tarifas, podendo a instituição ser responsabilizada por infringir a lei de defesa do consumidor. Em alguns países europeus, como a Itália, a legislação sobre defesa do consumidor impõe pesadas sanções que podem culminar no fechamento de instituições, por desrespeito aos direitos dos consumidores;
- Possibilidade de acesso não autorizado a informações financeiras da instituição ou de clientes, caso o *web site* não esteja devidamente apartado da rede interna que armazena os dados financeiros;
- Possibilidade de envio de vírus ou outros códigos maliciosos aos computadores conectados ao *web site* da instituição;
- Possibilidade de "pichação" das páginas institucionais, decorrente de invasão, afetando negativamente a imagem do banco perante o público em geral. Esse ataque é conhecido como *Web Site Defacement*;
- Possibilidade de indisponibilidade da página do banco, em virtude de ataques externos, a exemplo do DoS (*denial of service*), ou de problemas de origem interna, como erros operacionais, falhas em aplicativos ou equipamentos, desastre natural etc.

Dos exemplos acima relatados podemos identificar riscos legais, de imagem e operacionais. Não distinguimos riscos relacionados à identificação e autenticação do usuário perante a instituição, tendo em vista tratar-se apenas da disponibilização de informações institucionais.

Contudo, vislumbramos a possibilidade de um ataque muito comum até pouco tempo e que raramente vêm sendo utilizadas: as famosas páginas falsas.

As páginas falsas usam endereços parecidos com o do *site* original, mas com pequenas alterações em seu nome ou na extensão, como, por exemplo: www.banco.com.br.info (extensão info no final). Geralmente, as páginas falsas estão associadas a e-mails maliciosos, ou partem de atalhos indicados em outros *sites*, que não os dos bancos.

A recomendação para os usuários é para sempre acessar seu banco digitando o endereço diretamente na janela do navegador. Como exemplo citamos as recomendações disponibilizadas no link “acesso e segurança”, do *site* do Banco do Brasil, em que aconselha ao usuário evitar atalhos para acessar o *site* da instituição, especialmente os obtidos em *sites* de pesquisa. A orientação é para sempre digitar www.bb.com.br no campo de endereço dos *browsers* de navegação. Aliada às ações educativas, os bancos implantaram *pluggins* que cadastram os endereços de seus servidores, possibilitando a detecção das páginas falsas.

4.2.1.2. Web sites Transacionais

Os *web sites* transacionais são os responsáveis por disponibilizar aos clientes dos bancos ambiente propício para realização de suas transações bancárias. As grandes instituições financeiras, instaladas no Brasil, oferecem aos clientes praticamente todos os serviços disponíveis nas agências bancárias, ou nos terminais de auto-atendimento, com exceção daqueles em há necessidade de entrega física de documentos ou saques de dinheiro.

Dos *sites* do Banco do Brasil [10] e do Bradesco [6], identificamos os principais grupos de serviços e produtos disponíveis aos clientes:

- ✓ Gerenciamento das contas corrente, de investimento e de poupança:
  Consultas, extratos e transferências;
- ✓ Gerenciamento de Cartões de crédito:
  Extratos, pagamentos de faturas, programa de fidelidade;
- ✓ Aplicações financeiras:
  Fundos de investimento e carteira de ações;
- ✓ Empréstimos e Financiamentos;

- ✓ Pagamentos de boletos de cobrança, impostos, taxas e outros convênios;
- ✓ Débito automático;
- ✓ Consórcios;
- ✓ Seguros, previdência e capitalização;
- ✓ Além de outros serviços.

Como em todo canal de comunicação disponível para realização de transações bancárias, o *internet banking* também tem como procedimento inicial a identificação positiva do cliente. Entretanto, em face da virtualização do ambiente, esse problema se manifesta de forma mais intensa. Como os bancos podem se assegurar de que o cliente que se apresenta é realmente quem se diz ser? A que tipos de riscos estão expostos o cliente e a instituição financeira? A seguir identificamos os principais riscos nesses dois ambientes.

4.2.2. IDENTIFICANDO RISCOS NOS AMBIENTES DO CLIENTE E DA INSTITUIÇÃO

Os sistemas de *e-banking* para efetivação dos serviços estão suportados por recursos e processos, dentro de uma complexidade cada vez mais crescente. Destacamos os seguintes:

- ✓ Recursos de infra-estrutura de tecnologia da informação: servidores de *internet banking*, servidores da rede interna, sistema de processamento central, *firewall*, *intrusion detection system* ou IDS etc;
- ✓ Processo de administração e gerenciamento de redes;
- ✓ Sistemas aplicativos que suportam as transações bancárias;
- ✓ Sistemas operacionais e gerenciadores de bancos de dados;
- ✓ Monitores de transações.

Conhecido o ambiente e identificados os objetivos a serem alcançados, a fase de identificação de riscos prossegue com o mapeamento das possíveis ameaças as quais as instituições estão sujeitas e que podem inviabilizar o êxito do negócio.

4.2.2.1. Riscos Operacionais

São riscos de perdas resultantes de fraudes, inadequação ou falhas de processos internos, pessoas e sistemas, ou de eventos externos. O impacto resultante da consecução desse risco está diretamente relacionado à incapacidade da instituição em disponibilizar os serviços de banco eletrônico para os clientes. Este risco existe para todo produto ou serviço oferecido.

As principais ameaças dizem respeito à segurança da informação, ou seja, abrangem os aspectos de confidencialidade, disponibilidade e integridade. Destruição, danificação da informação ou de outros recursos; modificação da informação; furto, remoção ou perda de informação ou de outros recursos; revelação de informação a pessoas não autorizadas; interrupção de serviços de servidores ou estações de trabalho [13].

Um tipo de ataque envolve vasculhar informações sobre uma rede de computadores ou sobre o computador de um usuário. É a chamada ameaça passiva, ou seja, o atacante busca informações sobre dados dos usuários ou sobre a configuração da rede, disponibilizada pelos bancos para prover informações ou realizar transações, que poderão ser usadas para atingir um sistema ou conjunto de sistemas, em um ataque real. Não resultam em qualquer modificação nas informações dos sistemas, ou na sua forma de operação.

Um exemplo desse tipo de ataque, lançado contra os servidores dos bancos, é a análise de rede (*Network analysis*). O atacante aplica uma abordagem sistemática e metódica conhecida como *footprinting* para constituir um perfil sobre a infra-estrutura de segurança da rede de uma instituição. Nessa fase de reconhecimento, são obtidas informações sobre endereços de rede, localização de *gateways* e *firewalls*, bem como analisa os números de portas mais conhecidos para detectar informações ou serviços em execução no sistema. A análise do conjunto de informações obtidas possibilita identificar vulnerabilidades a serem exploradas.

Pelo lado do cliente, esse tipo de ataque pode levar ao vazamento de informações sobre dados bancários que serão usadas para possibilitar ao atacante realizar transações fraudulentas. Interessante observar que o atacante não tem interesse em alterar ou destruir as

informações dos usuários. Para o atacante, é necessário que a passividade e a "invisibilidade" do ataque sejam seus pontos fortes, pois caso o cliente não perceba que está sendo monitorado, as chances de sucesso do ataque e conseqüente utilização dos dados capturados se potencializam. De posse dos dados bancários obtidos por meio dessas técnicas, o atacante terá condições de realizar transações "em nome" do verdadeiro cliente.

Monitoramos, no período de 01/05/2006 e 31/05/2006, o envio de *trojans* aos clientes dos bancos instalados no Brasil e apresentamos o resultado na tabela 4.1. Essas instituições financeiras constituem um grupo que atua de forma conjunta na monitoração de incidentes de segurança. Por razões de segurança deixamos de nomear as entidades. Os números ali dispostos representam a quantidade total de códigos maliciosos enviados aos clientes, por dia e detectados pelas ferramentas disponíveis. Não necessariamente significam novos *trojans*. Às vezes é o mesmo código, mas com novo apelo, do tipo:

- "você está sendo traído, clique aqui para ver as fotos";
- "sua declaração de imposto de renda está na malha da Receita Federal, clique aqui para saber mais informações";
- "seu título de eleitor foi cancelado, clique para informações";
- "seu nome está no Serasa, informe-se clicando em...".

Os *trojans* atuando por trás desses "cliques" têm como objetivo capturar informações bancárias e/ou induzir o cliente a executar ações que acabam por revelar e permitir o envio dos dados dos clientes ao atacante.

Tabela 4.1: Quantidade de Trojans enviados a clientes de bancos

5/1/2006	178	5/17/2006	115
5/2/2006	419	5/18/2006	133
5/3/2006	163	5/19/2006	86
5/4/2006	81	5/20/2006	97
5/5/2006	85	5/21/2006	20
5/6/2006	23	5/22/2006	61
5/7/2006	8	5/23/2006	149
5/8/2006	96	5/24/2006	65
5/9/2006	24	5/25/2006	200
5/10/2006	144	5/26/2006	129
5/11/2006	137	5/27/2006	95
5/12/2006	157	5/28/2006	51
5/13/2006	2	5/29/2006	195
5/14/2006	38	5/30/2006	56
5/15/2006	190	5/31/2006	98
5/16/2006	139	Total	3434

Outra estatística sobre a ocorrência de *trojans* nas instituições financeiras do Brasil nos é apresentada pela empresa GAS Informática e demonstrada acumuladamente na tabela 4.2. O valor apontado no mês de maio difere do valor obtido na pesquisa de campo. A explicação reside na utilização de fontes de pesquisas diferentes entre a monitoração realizada por este autor e a procedida pela empresa GAS informática. Entretanto, acreditamos que uma não invalida a outra, tendo em vista a materialidade do número de ocorrências apontadas.

Tabela 4.2: Acumulado de Trojans enviados a clientes de bancos

Mês	Acumulado	No mês
Setembro/2005	12.267	
Outubro/2005	14.072	1.805
Novembro/2005	16.208	2.136
Dezembro/2005	18.225	2.017
Janeiro/2006	24.104	5.879
Fevereiro/2006	25.785	1.681
Março/2006	27.539	1.754
Abril/2006	30.822	3.283
Maio/2006	35.485	4.663
Até 08 de Junho de 2006	36.150	665

Graficamente podemos representar os números acima conforme a seguir:

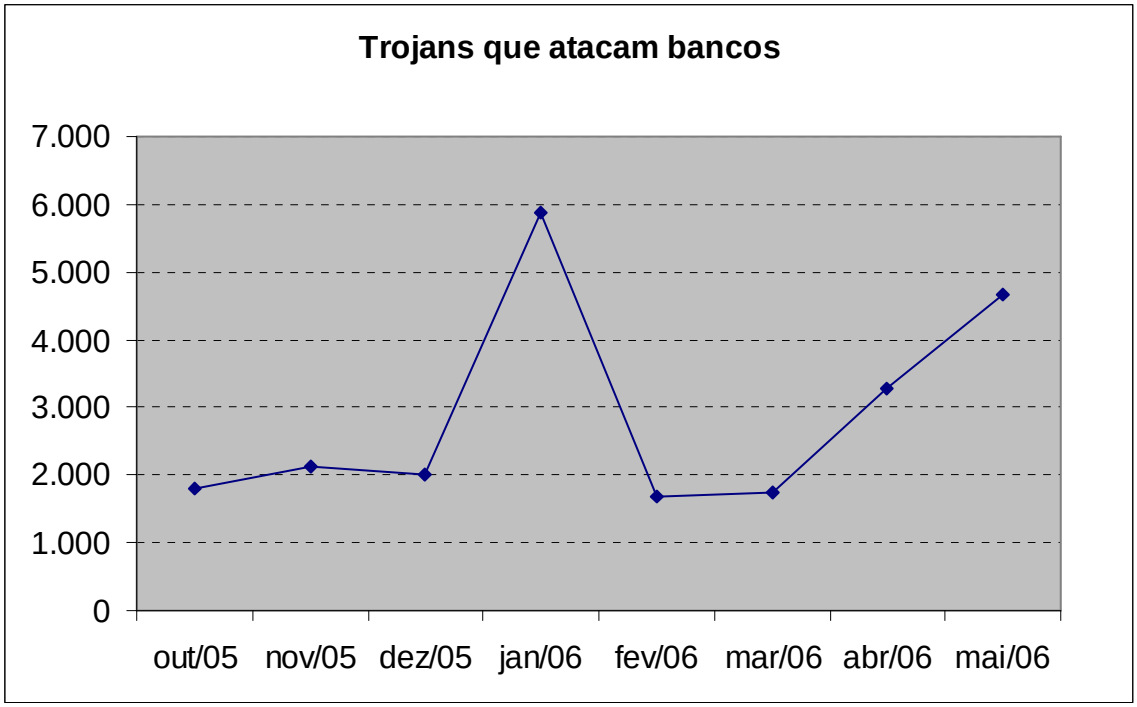


Figura 4.2 – Variação dos ataques por trojans

Uma vez obtidas as informações sobre o ambiente dos bancos e sobre seus clientes, os atacantes iniciam os chamados ataques ativos. Estes envolvem a alteração da informação contida no sistema ou modificações em seu estado ou operação. Também consideramos como

ataques ativos, a consecução de transações fraudulentas, com uso dos dados bancários capturados nos ataques passivos.

O intruso lança um ataque real contra a rede da instituição ou contra o cliente, com intuito de obter controle sobre o sistema, possibilitando a materialização da ameaça. Isto pode abranger desde o acesso não autorizado para modificar dados ou programas, até deixar o *site* da instituição indisponível, caracterizando um ataque de *denial of service,* ou seja, negação de serviço.

A figura 4.3 e a tabela 4.3 apresentam o resultado do monitoramento realizado no período de 05/05/2006 a 05/06/2006, onde mapeamos os ataques realizados contra os bancos participantes do grupo de monitoramento anteriormente referenciado. Também esses dados refletem a população dos ataques detectados pelas ferramentas disponíveis nas instituições.

Tabela 4.3: Ataques contra os servidores dos bancos

Identification of the attack	Ocurrences	%
synflood	1.758.020	25,90
HTTP_Cross_Site_Scripting	714.457	10,52
IP_Unknown_Protocol	534.306	7,87
Stream_DoS	469.548	6,92
BGP_Route_Unreachable	449.138	6.62
DNS_Query_All	274.311	4,04
TCP_Port_Scan	223.576	3,29
HTTP_IIS_Unicode_Wide_En-coding	150.952	2,22
RealSecure_Kill	140.230	2,07
Email_Outlook_URL_Spoof	131.296	1,93
Other	1.942.847	28,62
Total	6.788.681	100,00

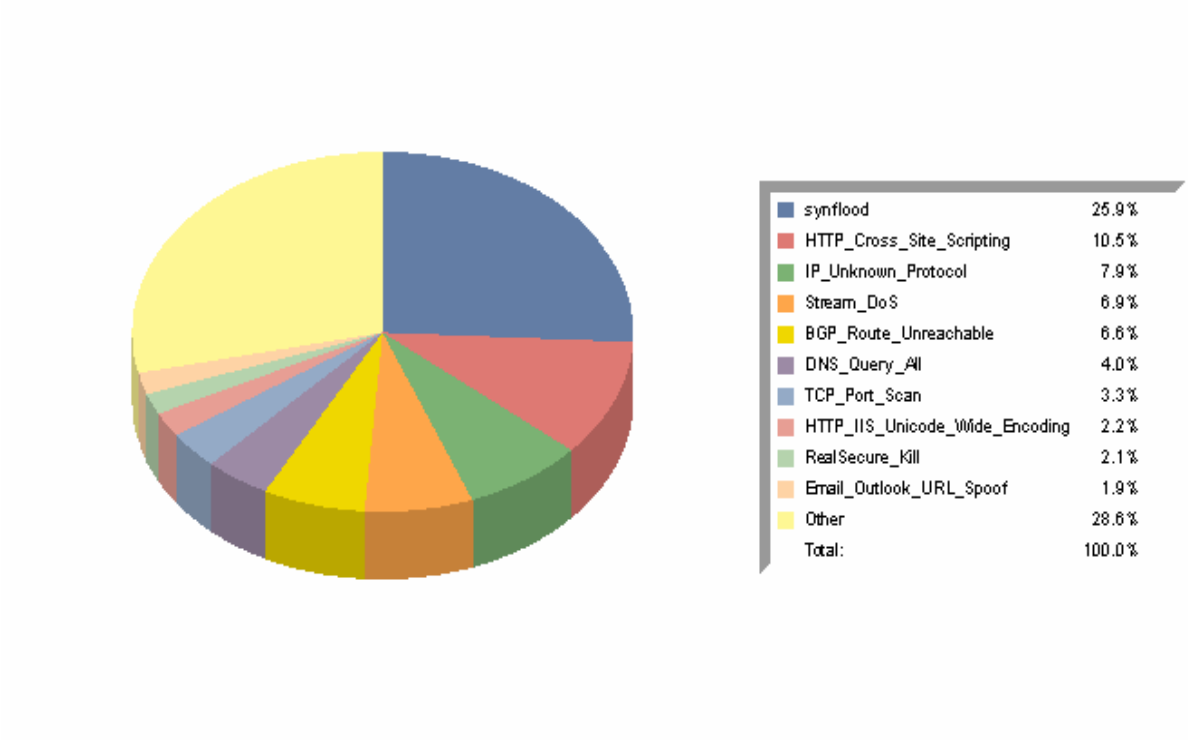


Figura 4.3: Estatística dos ataques contra os servidores dos bancos

A tabela 4.4 nos apresenta o número de incidentes reportados ao CERT – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil [14] no período de janeiro a dezembro de 2006. Os incidentes estão distribuídos entre *worms*, incidentes de invasão, ataques a servidor *web*, ocorrências de *denial of service* (DoS), varredura de portas (*scan*) e consecução de transações fraudulentas.

Tabela 4.4: Incidentes reportados ao CERT – Janeiro a Dezembro de 2006
Totais mensais e trimestral classificados por tipo de ataque

Mês	Total	Worm (%)		DoS (%)		Invasão (%)		Aw (%)		Scan (%)		Fraude (%)	
jan	**8446**	1358	16	71	0	24	0	32	0	3274	38	3687	43
fev	**7742**	1223	15	33	0	59	0	54	0	2737	35	3636	46
mar	**11945**	4062	34	41	0	112	0	29	0	2925	24	4776	39
abr	**14126**	7327	51	3	0	61	0	28	0	2742	19	3965	28
mai	**18204**	11139	61	81	0	24	0	29	0	3153	17	3778	20
jun	**17470**	11036	63	24	0	44	0	43	0	3127	17	3196	18
jul	**18754**	12833	68	11	0	57	0	46	0	2823	15	2984	15
ago	**17501**	8961	51	4	0	44	0	37	0	5160	29	3295	18
set	**23321**	13499	57	4	0	26	0	38	0	5507	23	4247	18
out	**18592**	8944	48	3	0	21	0	35	0	6823	36	2766	14
nov	**23414**	16355	69	0	0	43	0	51	0	3777	16	3188	13
dez	**18377**	12939	70	2	0	8	0	27	0	3143	17	2258	12
Total	**197892**	109676	55	277	0	523	0	449	0	45191	22	41776	21

Legenda:
DoS: *Denial of Service* AW: Ataque a servidor WEB

Diversas formas de ataques aos serviços de *internet banking* são identificadas todos os dias. Com base no resultado do monitoramento mostrado na figura 4.3, bem como nas conseqüências advindas pela efetivação do *trojans* lançados contra os clientes, descrevemos, a seguir, os principais tipos de ameaças contra os serviços de *internet banking*, atualmente observadas com mais intensidade. Não pretendemos esgotar todas as formas de ataque, mas enfatizar as estatisticamente mais utilizadas, no período da pesquisa, dentro da filosofia de otimizar os recursos disponíveis na minimização dos principais riscos. Lembremo-nos de que o constante monitoramento possibilita identificar novos riscos e conseqüentemente desenvolver ações direcionadas ao seu combate e minimização.

Informamos que as descrições, plataformas afetadas e contra-medidas referentes aos ataques descritos a seguir foram obtidas a partir do *site* da *Internet Security Systems* [37] e livremente traduzidas pelo autor deste trabalho.

4.3.2.1.1 Ataques Passivos

Objetivo do ataque

Obter informações sobre a configuração de uma rede ou sobre dados dos usuários, que possibilitem a utilização dessas informações em ataques ativos.

4.3.2.1.1.1 Decod-dns

Médio Risco

Descrição

Uma requisição de DNS para todos os registros disparada contra um *host* pode indicar um ataque passivo de sondagem sobre uma rede. Com ferramentas do tipo “dig”, um atacante poderá executar esse tipo de ataque e obter informações sobre uma determinada rede. Esse tipo de ataque pode ser confundido com uma requisição legítima de DNS.

Um programa do tipo “dig” é um sistema de indexação e procura por *intranets* e pequenos domínios. Esse programa, em algumas distribuições linux pode permitir um atacante obter arquivos de forma remota.

Plataformas afetadas:

- DNS: qualquer versão de DNS.
- Qualquer aplicação em qualquer versão.

Contramedidas

Eventos deste tipo são em sua maioria partes de requisições normais e não maliciosas de DNS. Os sites requisitantes dessas informações devem ser monitorados quanto a estes eventos, na tentativa de se identificar eventos que possam caracterizar um ataque passivo de sondagem de rede.

4.3.2.1.1.2 IP-Portscan

Médio Risco

Descrição

Um ataque de *portscan* é uma tentativa de determinar quais serviços estão sendo executados em um sistema, por meio da sondagem de portas, obtida quando das respostas a requisições enviadas.

Plataformas afetadas

- Qualquer aplicação em qualquer versão.

Contramedidas

Identificar a fonte do ataque de *port scan*. Correlacionar a fonte do *scan* com os serviços que estão sendo executados no *host* sobre ameaça. Mapear a fonte e a intenção da varredura. Verificar os *logs* de acesso buscando identificar acessos não autorizados. Se forem constatados esses acessos considere seu sistema comprometido e adote as medidas cabíveis.

4.3.2.1.1.3 Trojans, Spywares, Códigos Maliciosos

Alto Risco

Descrição

Esse conjunto de programas tem como objetivo o roubo de informações, como, por exemplo, números de contas, senhas, números de cartões de créditos, certificados digitais etc. Genericamente são programas de computador que, ao serem instalados, fazem com que outra pessoa possa controlar virtualmente a máquina infectada, ou executar funções sem o conhecimento do usuário, como as sobrescritas.

Dentro dessa categoria, destacamos três tipos de ataques diretamente relacionados com ataques passivos ao ambiente *internet banking* do usuário.

Keyloggers: Programas que visam capturar dados digitados pelo usuário, durante a execução de transações bancárias. Depois, o *trojan* envia a lista de informações para o endereço do autor do programa invasor. Como no Brasil as grandes instituições financeiras adotaram os teclados virtuais, que utilizam o mouse para entrada dos dados críticos (em especial as senhas), esses programas não representam maiores problemas. Contudo, muitos bancos internacionais ainda utilizam o teclado para entrada dos dados bancários, tornando eficaz a utilização de *keyloggers*.

Mouseloggers: Programas adaptados para interceptarem cada clique do mouse. Essa técnica se tornou mais freqüente com o advento do uso de teclados virtuais. Uma vez detectado o clique do mouse, o programa captura a imagem sob o cursor. Com isso, os programas de monitoração conseguem determinar a seqüência de imagens clicadas que correspondem aos dados que normalmente seriam digitados pelo usuário.

Screenlogger: ataque de monitoramento da tela. Como numa seqüência lógica crescente de exploração a vulnerabilidades, esse tipo de ataque veio imediatamente após os bancos terem adotado o uso de teclados virtuais. Agora, esses *trojans* agem por meio da captura de telas, vigiando e monitorando as ações dos clientes, quando do acesso ao *site* dos bancos. Ao obter as informações dos usuários, esses códigos maliciosos as enviam para seus "donos" remotos.

No *site* da SOPHOS [56] encontramos uma série de exemplos de *trojans* destinados a capturar informações sobre dados de clientes, quando transacionando com seus respectivos bancos. Fazem parte dessa gama de códigos:

- Troj/Banker-AJ – Aliases: PWSteal, Revcuss.A, Win32.Recvuss.H;
- Troj/Banker-JJ – Aliases: Trojan-Spy.Win32.Banker.jj, PWS-Banker.f, TROJ_BANKER.EY. Esse trojan destinado a capturar senhas de bancos, monitora os acessos do usuário a *internet*. Quando determinados bancos são acessados, ele captura e armazena as atividades do usuário, enviando os dados para um *web site* remoto.

- Troj/Banker-HS é um *trojan* de captura de senhas que tem como alvo os web *sites* de bancos brasileiros. Aliases: Trojan-Spy.Win32.Banker.ri, PWSteal.Bancos, W32/Bancos.AIQ, W32/Banker.CNE e PWS-Banker.gen.b.

Da lista sobre alertas quanto a *trojans* e □cess divulgada para setembro de 2006, identificamos dentre os dez mais detectados, a presença de 03 códigos destinados a captura de dados bancários: Troj/Bancos-AWI, Troj/Bancos-AWG e Troj/Banker-DNM.

1. W32/Sdbot-CRR – Sun, 24 Sep 2006 04:26:46 Z

2. Troj/Lineag-ABA – Sat, 23 Sep 2006 15:52:58 Z

3. Troj/WowPWS-Z – Sat, 23 Sep 2006 06:25:46 Z

4. Troj/Bancos-AWI – Sat, 23 Sep 2006 01:39:36 Z

5. Troj/WOW-HH – Fri, 22 Sep 2006 19:29:28 Z

6. Troj/Bancos-AWG – Fri, 22 Sep 2006 14:50:02 Z

7. W32/WinLose-A – Fri, 22 Sep 2006 14:23:05 Z

8. W32/Stration-AE – Fri, 22 Sep 2006 11:09:48 Z

9. Troj/LowZone-CX – Fri, 22 Sep 2006 09:52:47 Z

10. Troj/Banker-DNM – Fri, 22 Sep 2006 09:16:38 Z

4.3.2.1.2 Ataques Ativos

4.3.2.1.2.1 Ataques de Invasão

Alto Risco

Objetivo do ataque

Enganar os controles de segurança para obtenção de acesso não autorizado ao sistema gerenciador de serviços do *site* da instituição financeira.

4.3.2.1.2.1.1. IIS_Cross_Site_Scripting (HTTP_Cross_Site_Scripting)

Baixo Risco

Descrição

As versões 4.0 e 5.0 do serviço IIS da Microsoft (*Internet Information Server*) são vulneráveis ao *Cross-Site Scripting* (CSS), que afeta diretamente os servidores *web* responsáveis pela geração automática de páginas HTML. *Cross-Site Scripting* pode ser usado de forma maliciosa por um operador de um *web site* para introduzir e executar um código em outra sessão *web* de usuário.

Plataformas afetadas

- Microsoft Corporation: Microsoft IIS 4.0
- Microsoft Corporation: Microsoft IIS 5.0
- Microsoft Corporation: Microsoft Personal Web Server 4.0
- Microsoft Corporation: Windows 2000 Qualquer versão
- Microsoft Corporation: Windows NT Qualquer versão

Contramedidas

Atualizar o sistema com as correções disponibilizadas no *site* da Microsoft.

4.3.2.1.2.1.2. IP-Unknown

Low Risk

Descrição

Existem diversos protocolos “padrão de mercado” usados no topo da arquitetura tcp/ip para transmitir dados. São exemplos desses protocolos o tcp, o udp e o igmp.
Contudo os usuários podem criar seus próprios protocolos e transmitir dados usando suas customizações. Essas aplicações que usam seus próprios formatos de protocolo tornam difícil, ou mesmo impossível, determinar o que está sendo transmitido, a não ser diretamente pelo exame dos dados. Por essa razão, protocolos customizados são,

algumas vezes, usados por atacantes para evitar detecção enquanto transmitem dados pela rede.

Muitas ferramentas de segurança ignoram protocolos que elas não entendem. Assim sendo, é comum se estabelecer canais de comunicação dissimulados usando protocolos desconhecidos. Um canal escondido pode indicar a presença de uma “porta dos fundos” (*backdoor*) dentro de uma rede de comunicação.

Plataformas afetadas

- Qualquer aplicação em qualquer versão.

Contramedidas

Se há suspeitas sobre atividades anormais, é aconselhável utilizar ferramentas de análise para capturar e verificar o tráfego dentro da rede.

4.3.2.1.2.1.3. HTTP-Apache-Cookie

 Alto Risco

Descrição

O servidor Apache EM possui um módulo opcional (mod_cookies) que pode permitir a um atacante remoto provocar sobrecarga (*overflow*) de buffer interno no servidor *web*, possibilitando a execução arbitrária de códigos no servidor. Esse módulo é compilado no servidor *web*, não sendo instalado por *default* em nenhuma versão do Apache. Esses servidores de http, até a versão 1.1.1, podem estar vulneráveis a ataque de *overflow*, se o módulo descrito tiver sido compilado no servidor.

Plataformas afetadas

- Apache Software Foundation: Apache EM Server – qualquer versão
- Data General: DG/UX qualquer versão
- Hewlett-Packard Company: HP-UX qualquer versão
- Hewlett-Packard Company: Tru64 UNIX qualquer versão
- IBM: AIX qualquer versão

- Linux: Linux qualquer versão
- Santa Cruz Operation, Inc.: SCO Unix qualquer versão
- SGI: IRIX qualquer versão
- Sun Microsystems: Solaris qualquer versão
- Wind River Systems, Inc.: BSD qualquer versão

Contramedidas

Essa vulnerabilidade somente afeta *sites* que executam Apache versão 1.1.1 ou inferior com módulos *cookies* compilados no servidor. A recomendação é para atualizar o servidor com as devidas correções.

4.3.2.1.2.1.4. IIS-Unicode-Wide-Encoding

 Alto Risco

Descrição

O serviço de Internet Information Server (IIS) da Microsoft possibilita que caracteres sejam codificados no padrão “Unicode” em requisições URL, dentro de um formato que use “%u”. Essa codificação aparece como “%uXXXX”, onde “XXXX” representa caracteres hexadecimais (0-9, A-F). Por exemplo, a letra ‘a’ pode ser codificada como “%u0061”. Um atacante remoto pode usar essa forma de codificação para tentar burlar os sistemas de detecção de intrusos.

Muitos ataques do tipo “.ida” (incluindo os *worms* do tipo CodeRed) usam esse tipo de codificação quando executam tentativas de buffer *overflow* .

Plataformas afetadas

- Cisco Systems, Inc.: CiscoSecure IDS qualquer versão
- Enterasys Networks, Inc: Dragon Sensor 4.x
- *Internet* Security Systems, Inc.: RealSecure Network Sensor 5.x
- *Internet* Security Systems, Inc.: RealSecure Network Sensor 6.0
- *Internet* Security Systems, Inc.: RealSecure Network Sensor 6.5
- *Internet* Security Systems, Inc.: RealSecure Server Sensor 5.5
- *Internet* Security Systems, Inc.: RealSecure Server Sensor 6.0

- Microsoft Corporation: Microsoft IIS 4.0
- Microsoft Corporation: Microsoft IIS 5.0
- Snort: Snort anterior à versão 1.8.1

Contramedidas

Para RealSecure Network Sensor 5.x, 6.x: aplicar a última atualização do RealSecure Network Sensor X-Press (XPU 3.2 ou posterior).

Para RealSecure Server Sensor 6.0: atualizar a última versão do RealSecure Server Sensor (6.0.1 ou posterior).

Para IDS Cisco Secure (Netranger): aplicar o mais recente *service pack* conforme indicado em "Cisco Systems Field Notice, September 5, 2001".

Para Snort anterior a 1.8.1: atualizar com a última versão do Snort (1.8.1 ou posterior) disponível em: http://www.snort.org/downloads.html.

4.3.2.1.2.1.5. Database-Ida-Portable-Executable-Bo

Alto Risco

Objetivo do ataque

Obter acesso a sistema, fraudando a segurança através de artifícios de burla do IDS (*Intrusion Detection System*).

Descrição

DataRescue IDA Pro é um "multi-processor disassembler" para Linux e Microsoft Windows. DataRescue IDA Pro versões 4.6 Service Pack 1, 4.7, e possivelmente outras versões são vulneráveis a *stack-based buffer overflow* na análise gramatical de longas listas de nomes de bibliotecas importadas. Um atacante remoto pode provocar uma sobrecarga (*overflow*) em um buffer e executar códigos arbitrários no sistema, pelo uso de privilégios de usuários.

Plataformas afetadas

- IDA Pro Disassembler: DataRescue IDA Pro 4.6 Service Pack 1

- IDA Pro Disassembler: DataRescue IDA Pro 4.7
- Jibz, Qwerton, snaker and xineohP.: PeiD prior to 0.93
- Linux: Linux Qualquer versão
- Microsoft Corporation: Windows 95
- Microsoft Corporation: Windows 98
- Microsoft Corporation: Windows 98 Second Edition
- Microsoft Corporation: Windows Me
- Microsoft Corporation: Windows 2000 Qualquer versão
- Microsoft Corporation: Windows 2003 Qualquer versão
- Microsoft Corporation: Windows NT 4.0
- Microsoft Corporation: Windows XP Qualquer versão

4.3.2.1.2.1.6. Ataques de DOS – Denial of Service (Interrupção de Serviço)

Alto Risco

Esse tipo de ataque tem por objetivo interromper um serviço ou impedir totalmente que usuários ou entidades autorizadas o utilizem. Seu objetivo principal é “tirar do ar” (não deixar disponível) um serviço ou o sistema, apenas para causar prejuízo, transtorno ou eliminar um serviço de proteção que possa permitir que se tenha acesso a outros serviços não autorizados.

4.3.2.1.2.1.7. Synflood

Médio Risco

Descrição

Uma conexão padrão TCP se estabelece pelo envio de pacotes com sinalização do bit SYN (*Synchronous Idle*, ou *Synchronize sequence number* – caractere de controle utilizado para manter o sincronismo na ausência de dados trafegando pela rede) ao *host* de destino. Caso esteja preparado para esperar por conexões em uma porta específica, ele responderá com um pacote SYN/ACK (SYN-Acknowlegment – código de comunicação reconhecendo que os dados transmitidos foram recebidos sem erros, ou que o *host* de destino está preparado para receber mais dados). Então, a estação que

iniciou a conexão (*host* de origem) responde com um pacote ACK para estabelecimento da conexão.

Quando um pacote SYN/ACK é enviado de volta à origem, um bloco de memória no *host* destino é alocado para aguardar pela informação sobre o estado da conexão que está sendo estabelecida. Até que o pacote ACK final seja recebido, a partir da origem, ou o *timeout* seja alcançado, esse bloco de memória permanece alocado, esperando por mais informações a serem recebidas.

O ataque de DoS se concretiza pelo envio de numerosos pacotes SYN a um *host* de destino, com objetivo de esgotar a porção de memória destina a abrir conexões. Quando essa memória é exaurida, nenhuma conexão, mesmo as legítimas, poderá ser estabelecida.

Essa situação pode ser detectada pelo monitoramento do fluxo de pacotes SYN que não tiveram respostas. Para corrigi-la, enviam-se pacotes RST, ao *host* destino, correspondentes aos pacotes SYN enviados pela origem. O resultado dessa ação é a liberação da porção de memória alocada para aguardar por mais informações sobre o estabelecimento da conexão.

Contramedidas

Atualizações dos sistemas operacionais trazem correções para ataques baseados em "SYN *flood*". Adicionalmente os administradores dos *hosts* de destino devem considerar a possibilidade de elevar o limite *default* de *buffers* de conexão.

4.3.2.1.2.1.8. Stream-Dos

Médio Risco

Descrição

O "stream.c" é um ataque de *denial of service* projetado para derrubar um sistema operacional pelo envio de pacotes TCP, adulterados (*spoofs*) pela marcação do sinalizador de ACK, a várias portas do *host* de destino. Essa situação pode causar, em certas versões do FreeBSD e possivelmente de outros sistemas, reações descontroladas e derrubada do *kernel* do sistema operacional. Essa forma de ataque é também utilizada no software de ataque "Mstream" que reúne todas as ferramentas utilizadas

para “tirar do ar” vários sites como Yahoo e Amazon, como por exemplo: Trin00, Tribal Flood Network, TFN2K ou Stacheldraht.

Spoofs – Tem como objetivo a falsificação ou disfarce de identidade. Existem várias formas de *spoofs*:
- IP Address Spoofing – Falsificação de endereço IP: utiliza um endereço IP válido e aceito pelo sistema de validação para ter acesso à determinada rede.

Plataformas afetadas

- Qualquer aplicação em qualquer versão.

Contramedidas

Atualizar os sistemas operacionais com as correções disponíveis para esse tipo de ataque.

4.3.2.1.2.1.9. BGP-Route-Unreachable

 Baixo Risco

Descrição

Uma rota é anunciada como inalcançável em uma mensagem de protocolo BGP – *Border Gateway Protocol*. Esse ataque impede o acesso do usuário ao serviço legítimo.

Plataformas afetadas

- Qualquer aplicação em qualquer versão.

Contramedidas

Essa mensagem não necessariamente significa um ataque. O monitoramento do *host* deve procurar por repetições constantes em um curto período de tempo e tratá-las na medida adequada.

4.3.2.1.2.1.10. Ataques de Envenenamento de Transação

Alto Risco

Esse tipo de ataque tem por objetivo capturar e adulterar a mensagem original, sem que o cliente e o sistema de segurança da instituição financeira percebam. Essa situação é uma das formas de ataque conhecido como "*man in the middle*", ou mais recentemente "*man in the browser*".

O ataque de MIM – *Man in the middle* é uma técnica de se colocar no meio da comunicação entre a estação do cliente e o servidor de e-*banking*. Geralmente, o atacante captura a transmissão e procede a alterações nas transações antes de reenviá-las ao destino final.

O que se vem observando no ambiente de *internet banking* é a instalação de aplicativos na estação do cliente para adulterar as transações efetuadas pelo cliente. Como exemplo descrevemos a seguinte situação: o usuário se autentica normalmente no banco, tendo inclusive utilizado todos os dispositivos de segurança disponibilizados pela instituição (teclado seguro, *browser defence* etc). O cliente procede então uma transferência de valores entre contas correntes. Ao enviar a transação, o aplicativo residente no computador intercepta a mensagem e procede a alterações nos dados de agência e conta de destino, bem como no valor a ser transferido. O banco recebe a solicitação e envia um pedido de confirmação. O aplicativo também monitora esse pedido, altera novamente a transação e apresenta ao cliente os dados originais. Ao confirmar a transação, o banco efetua a transferência para a conta indicada pelo atacante. Na seção sobre análise e planejamento de ações para gestão do risco retomaremos esse tipo de ataque e as contramedidas adotadas.

4.3.2.1.2.1.11. Ataques Internos

Alto Risco

Administradores de segurança devem considerar esse tipo de ataque quando do monitoramento do ambiente de *internet banking*. Por se encontrarem dentro das instituições, os funcionários ou contratados já ultrapassaram várias barreiras impostas

aos atacantes externos, elevando o risco de efetuarem acesso a ambientes ou aplicações não autorizadas para eles.

O fator “confiança”, neste tipo de ataque, é bastante explorado pelos usuários mal intencionados. Por considerarem confiáveis os colegas de trabalho, os administradores muitas vezes concentram sua atenção nos ataques que vêm de fora da instituição. O ambiente interno fica assim mais fragilizado quanto a medidas de segurança a serem implementadas na preservação das informações trafegadas e armazenadas internamente.

Destarte, ferramentas de defesa e de monitoração necessitam ser instaladas de modo a detectar a execução de aplicativos não autorizados ou inadequados ao desempenho das funções, com objetivo de burlar a segurança ou mesmo capturar dados de clientes e de outros usuários internos.

Destacamos da ISO-27001 no item 6.3 – Respondendo aos incidentes de segurança e ao mau funcionamento:

> “Devem estar claramente definidos os procedimentos a serem adotados nas diversas ocorrências indesejáveis no ambiente de processamento de informações da empresa.
>
> Incidentes que afetam a segurança devem ser relatados, o mais rapidamente possível, aos níveis gerenciais adequados.
>
> Devem ser do conhecimento de todos os funcionários e contratados os procedimentos para relatar os diversos tipos de incidentes (quebras de segurança, ameaças, fraquezas e mau funcionamentos) que podem impactar a segurança dos ativos da instituição.
>
> Processo disciplinar deve ser instaurado para investigar casos de falhas relacionadas ao descumprimento da Política de Segurança da Informação”.

4.3.2.1.2.1.12. Ataques de Engenharia Social

Alto Risco

Este tipo de ataque merece um destaque todo especial. Com certeza representa o maior desafio para as instituições financeiras, pois esse ataque trabalha com o comportamento das pessoas, usuárias dos serviços de *internet banking*. Já escrevemos sobre o despreparo das pessoas quanto ao uso da rede mundial de computadores. Alie-se, então, a exploração por parte dos atacantes dos desejos de ganhos e da curiosidade dos usuários, para dissimular as ações de ataque.

As instituições financeiras, no Brasil, destacam-se pelos altos investimentos financeiros na área de tecnologia. A área de segurança, em especial a questão de proteção está entre as maiores preocupações dos administradores. Diversas camadas de segurança são implementadas, abrangendo desde a autenticação do cliente, passando pela proteção aos sistemas, aos dados dos clientes e chegando até o ambiente pessoal do usuário. E é justamente esse ambiente que mais preocupa os executivos das instituições.

As camadas de segurança implementadas nos ambientes de *e-banking* das instituições financeiras proporcionam um nível confortável de exposição ao risco de invasão, levando os atacantes a investirem justamente no elo mais fraco do sistema. O que observamos como resultado da pesquisa realizada é uma concentração de ações muito mais relacionadas com “engenharia social” do que com tecnologia. São métodos não-tecnológicos para se obter acesso a um sistema, constituindo-se em um processo de convencimento, em que o cliente é iludido com intuído de fornecer ou revelar seus dados bancários.

As técnicas são as mais diversas e criativas possíveis. Neste item, é de se destacar a criatividade dos atacantes. Durante a pesquisa realizada por este autor, conseguimos recolher alguns exemplos, que anexamos nas figuras a seguir.

Figura 4.4: Trojan concurso Petrobrás

Figura 4.5: Trojan cartão Petrobrás

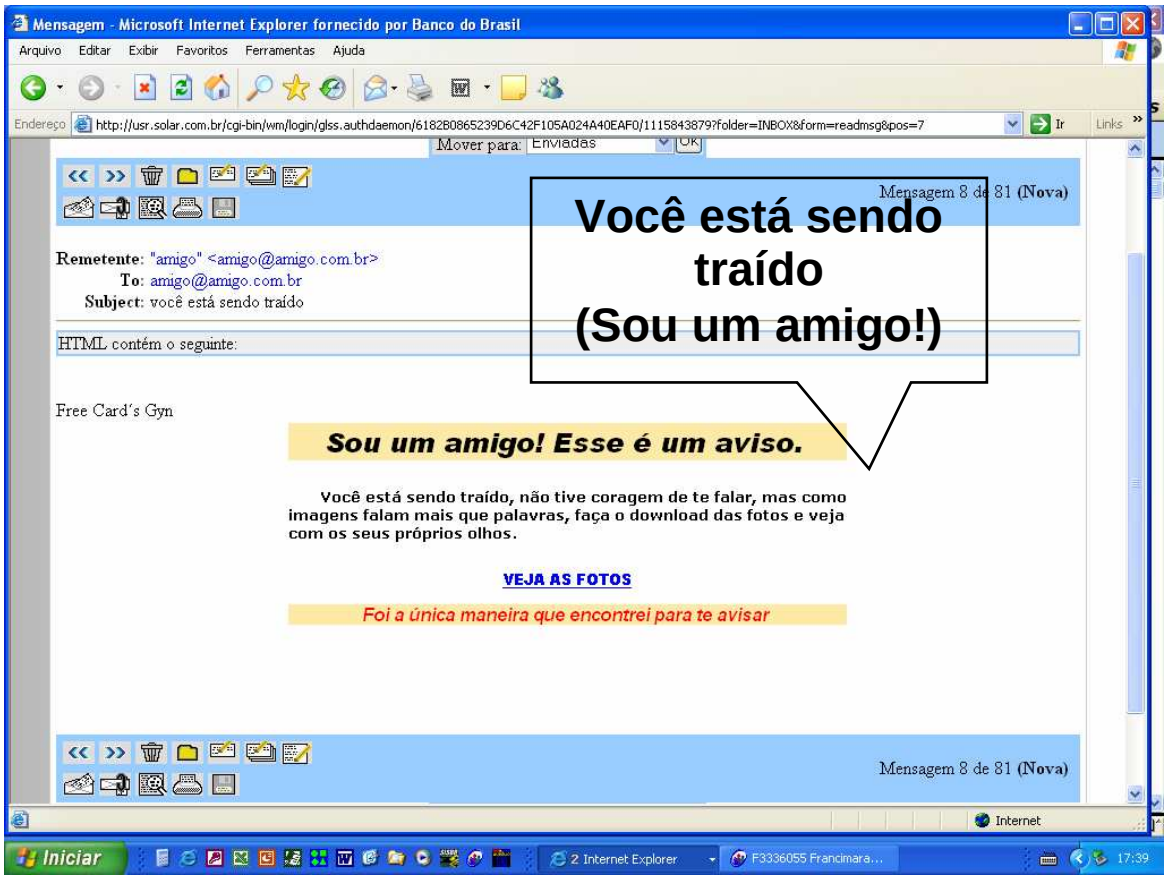


Figura 4.6: Trojan via e-mail

Figura 4.7: Trojan via aviso bancário

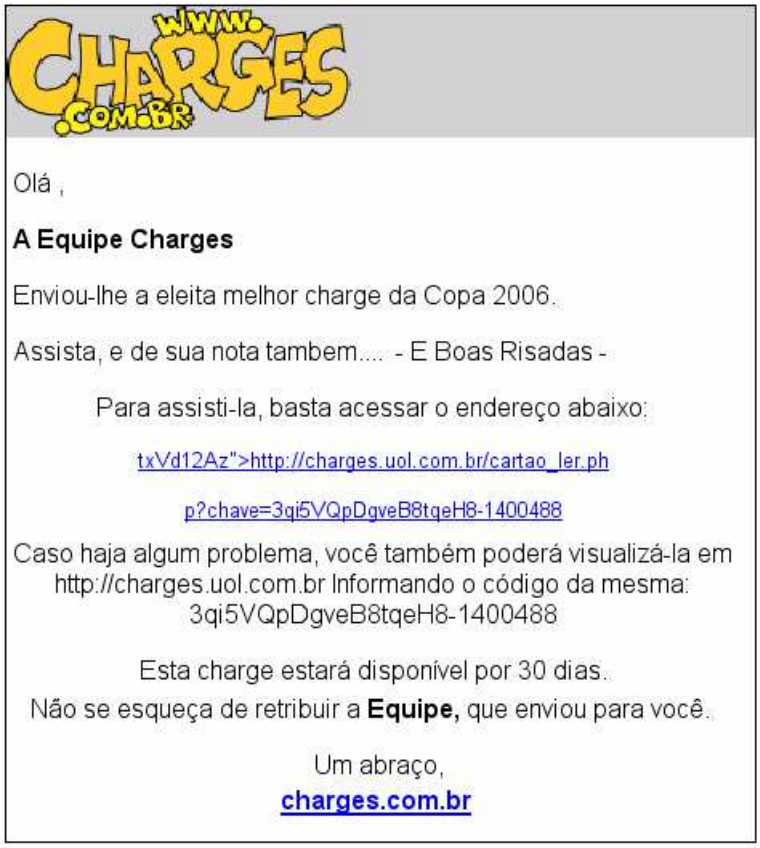


Figura 4.8: Trojan via site de charges

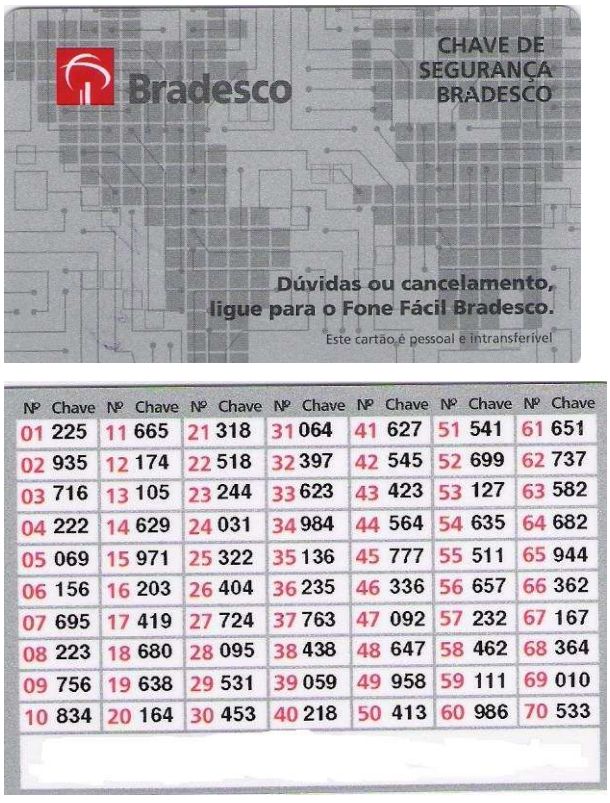
Os apelos, as promessas de ganhos, as ajudas oferecidas ou mesmo a exploração de *sites* de diversão são os mais diversos possíveis. Observamos, em todos, a indicação para acessar determinado endereço, figura ou *link*s na própria página apresentada, de forma a possibilitar ao usuário baixar ou visualizar arquivos.

A medida em que os bancos foram implementando soluções de segurança, novas formas de engenharia social foram aparecendo. Vejamos, por exemplo, dois grandes bancos nacionais.

O Banco do Brasil, em sua mais recente medida de segurança, implementou o cadastramento de computadores para identificação de seus clientes. Ao aderir à solução de cadastramento de computadores, as transações de pagamentos e de transferências ficam restritas aos computadores previamente cadastrados. Se o cliente tiver necessidade de cadastrar outros computadores, poderá fazê-lo por meio da opção de cadastramento de computadores, gerando um código de quatro números que deverá

ser informado em um computador previamente cadastrado, na agência de relacionamento, nas centrais de atendimento ou nos terminais de auto-atendimento. O ataque de engenharia social para essa solução consiste em solicitar ao cliente, em troca de alguma premiação, via e-mail supostamente enviado pelo banco, que faça o cadastro de um determinado código de cadastramento de computador. Ao fazê-lo, o cliente estará cadastrando o equipamento do atacante que, de posse de seus dados bancários poderá transacionar com o banco.

O Bradesco implementou a solução de senha dinâmica, para possibilitar a execução de transações críticas. Assim, além das senhas e contra-senhas tradicionais, uma adicional é solicitada para cada transação. As senhas dinâmicas são distribuídas aos clientes por meio de um cartão contendo 70 senhas de três dígitos, conforme fig 4.9.



Nº	Chave	Nº	Chave	Nº	Chave	Nº	Chave	Nº	Chave	Nº	Chave	Nº	Chave
01	225	11	665	21	318	31	064	41	627	51	541	61	651
02	935	12	174	22	518	32	397	42	545	52	699	62	737
03	716	13	105	23	244	33	623	43	423	53	127	63	582
04	222	14	629	24	031	34	984	44	564	54	635	64	682
05	069	15	971	25	322	35	136	45	777	55	511	65	944
06	156	16	203	26	404	36	235	46	336	56	657	66	362
07	695	17	419	27	724	37	763	47	092	57	232	67	167
08	223	18	680	28	095	38	438	48	647	58	462	68	364
09	756	19	638	29	531	39	059	49	958	59	111	69	010
10	834	20	164	30	453	40	218	50	413	60	986	70	533

Figura 4.9: Cartão Bradesco de senhas dinâmicas

O ataque de engenharia social consiste em solicitar ao cliente, também via e-mail supostamente enviado pelo banco, que digite suas 70 senhas. O que constatamos é que há usuários que o fazem.

O grande desafio enfrentado pelos bancos do mundo inteiro é auxiliar seus clientes no gerenciamento de seus ambientes, quanto ao nível de segurança implementado. Como as instituições não possuem controle sobre o ambiente do cliente, essa atividade é ainda mais onerosa. Observamos diversas iniciativas adotadas para minimizar os riscos no ambiente dos clientes. Essas iniciativas serão abordadas no decorrer deste trabalho. Contudo, face à diversidade de leis e regulamentos, muitas das medidas de segurança esbarram em leis que se prestam a defender a privacidade das pessoas, impedindo uma atuação mais eficiente dos aplicativos no ambiente dos clientes.

4.2.2.2. Riscos Legais

Risco associado ao não atendimento a leis e regulamentos aos quais a organização se encontra submetida. Tem como impactos, sanções aplicadas pelos órgãos reguladores, que podem, dependendo do país, levar à desautorização para funcionamento das organizações.

De acordo com o *site* do Federal Financial Institutions Examination Council [23] [24], os serviços de banco on-line é um novo canal de negociação onde as leis e regulamentos podem ser ambíguos ou ainda em desenvolvimento. Esses regulamentos incluem:

- Procedimentos quanto à entrega/exigência de documentação para efetivação das transações;
- Identificação de operações com indícios de lavagem de dinheiro;
- Confidencialidade dos dados dos clientes;
- Medidas quanto ao ressarcimento de clientes, por transações fraudulentas;
- Armazenamento das informações e condições negociais disponibilizadas na *internet*;

Leis e regulamentos que governam as transações disponibilizadas aos clientes requerem tipos específicos de divulgação, notícias e requerimentos de guarda de registro. Esses requerimentos também se aplicam ao *e-banking* e os órgãos supervisores continuam a

atualizar as leis e regulamentos para refletir o impacto do *e-banking* e relacionamentos com os clientes virtuais. Alguns dos requerimentos legais e normativos nos Estados Unidos [63] que freqüentemente se aplicam aos produtos e serviços *e-banking* incluem:

- Solicitação, coleta e reporte de informação monitorada pelo governo para aplicações e empréstimos, conforme requerida pelos regulamentos *Equal Credit Opportunity Act* (*Regulation* B) e *Home Mortgage Disclosure Act* (*Regulation* C).

- Requerimentos de propaganda, divulgação aos clientes, ou notícias requeridas pelos regulamentos *The Real Estate Settlement Procedures Act* (RESPA), *Thruth in Lending* (*Regulation* Z) e *Truth in Savings* (*Regulation* DD) e *Fair Housing*;

- Exibição apropriada e destacada de informações sobre seguros do FDIC (Federal *Deposit Insurance Corporation*) ou NCUA (*National Credit Union Administration*);

- Divulgação destacada nas páginas *web* indicando que certos tipos de investimento, corretagem e produtos de seguro oferecidos têm alguns tipos de riscos associados, incluindo não estarem cobertos por seguros do FDIC ou NCUA;

- Programas e procedimentos de identificação de clientes, bem como guarda de registros e requerimentos de notificação aos clientes, requeridas pelo *Bank Secrecy Act*;

- Processos de identificação de clientes para determinar se as transações efetuadas são proibidas pelo *the Office of Foreign Asset Control* (OFAC) e, quando necessário, se os clientes aparecem em alguma lista de terroristas suspeitos ou conhecidos ou organizações terroristas providenciadas por qualquer órgão do governo;

- Requerimentos de guarda de registros conforme os regulamentos dispostos no: *The Equal Credit Opportunity Act* (*Regulation B*) and *Fair Credit Reporting Act.*

Instituições que oferecem serviços de *e-banking*, tanto informacionais como transacionais, assumem um alto risco de conformidade em virtude da natureza mutável da tecnologia, da velocidade com a qual os erros se propagam e a freqüência das mudanças de regulação para direcionar as questões de *e-banking*. O potencial para violações é sobrepesado

pela necessidade de assegurar consistência entre propagandas em papel e eletrônicas, divulgações e notícias. Informações adicionais sobre requerimentos de conformidade para *e-banking* podem ser encontradas nos *web sites* das agências reguladoras.

4.3.2.2.1 Legislação Brasileira

Há muito se discute sobre a lacuna existente na legislação brasileira no que se refere à tipificação dos crimes virtuais. Essa lacuna obriga os juízes a adaptarem suas decisões e conseqüentemente as penas impostas tomando como base outras legislações. Não queremos afirmar que em países onde existe legislação específica os crimes virtuais não ocorram. Contudo, a situação atual da legislação brasileira favorece a proliferação de crimes da espécie, provavelmente pela sensação de impunidade percebida pelos autores.

A iniciativa mais recente para o tratamento do tema com mais profundidade reside no Substitutivo de Projeto de Lei de autoria do senador Eduardo Azeredo, do ano de 2003 [51]. Há uma expectativa quanto ao seu envio para sanção do presidente da república ainda neste ano.

Antes dessa, outras iniciativas também trataram do assunto, sem que fossem implementadas. Resumimos a seguir as principais medidas propostas anteriormente.

Projeto de Lei do Senado no. 76, de 2000.
Senador Renan Calheiros

- Divide os crimes virtuais em sete categorias: contra a inviolabilidade de dados e sua comunicação; contra a propriedade e o patrimônio; contra a honra e a vida privada; contra a vida e a integridade física das pessoas; contra o patrimônio fiscal; contra a moral pública e opção sexual; e contra a segurança nacional.

Projeto de Lei do Senado no. 137, de 2000.
Senador Leomar Quintanilha

- Visava alterar o código penal para que se aumentasse, em até 03 vezes, a pena prevista para os crimes contra a pessoa, o patrimônio, a propriedade imaterial e intelectual, os

costumes, e a criança e o adolescente, na hipótese de tais crimes serem cometidos por meio da utilização da tecnologia da informação e telecomunicações.

Projeto de Lei da Câmara no. 89 de 2003, anteriormente PLC 84 de 1999.
Deputado Luiz Piauhylino.

Visava criar tipos penais tanto para delitos cometidos contra sistemas de computador, quanto por meio de computador. Destacam-se:

- acesso indevido a meio eletrônico (art. 154-A);
- manipulação indevida de informação eletrônica (art. 154-B);
- definição de meio eletrônico e sistema informatizado, para efeitos penais (art. 154-C);
- difusão de vírus eletrônico (art. 163 §3º.);
- pornografia infantil (art. 218-A);
- falsificação de telefone celular ou meio de acesso a sistema informático (art. 298-A);

De acordo com as declarações do Senador Eduardo Azeredo à revista "Security Review – edição número 08" a tipificação das penas de acordo com o delito eletrônico culminará em uma realidade mais factível aos juízes. "Por mais que seja um instrumento válido, definir as penas por analogia é muito difícil para os juízes que estão num cenário ainda sem clareza. O criminoso se safa por não haver a definição clara dos crimes, nem das punições que deve receber" declara o senador.

Destacamos alguns pontos do Substitutivo ao Projeto de Lei nº 89, de 2003:

- Art. 163, parágrafo segundo: Dano em dado ou informação eletrônica, base de dados ou sistema informatizado decorrente da difusão de vírus eletrônico. Pena: reclusão de um a três anos e multa

- Inserir no Código Penal (CP) o artigo 163-A para tipificar o crime de dano por difusão de vírus eletrônico;

- Inserir no CP os artigos:

- Art. 154-A: Acessar indevidamente ou sem autorização dispositivo de comunicação ou sistema informatizado. Pena: reclusão de dois a quatro anos e multa.
- Art. 154-B: Manter, transportar ou fornecer indevidamente ou sem autorização dado ou informação obtidos em dispositivo de comunicação ou sistema informatizado. Pena: reclusão de dois a quatro anos e multa.
- Art. 154-D: Difundir, por qualquer meio, sistema informatizado com o propósito de induzir alguém a fornecer, espontaneamente e por qualquer meio, dados ou informações que facilitem ou permitam o acesso indevido ou sem autorização a dispositivo de comunicação ou a sistema informatizado. Pena: reclusão de dois a quatro anos e multa.
- Art. 154–F tipificando a conduta de permitir acesso por usuário não identificado e autenticado. Este último item fez emergir calorosas discussões nos diversos meios da sociedade, sobre a liberdade de navegação na *internet*, culminando, em 07/11/2006, com o adiamento da votação.
- Art. 154-H: Utilizar, de forma anônima, dispositivo de comunicação ou sistema informatizado para o envio de mensagem eletrônica de qualquer tipo. Pena: reclusão de um a dois anos e multa.

- Acrescentar, ainda no CP, o art. 183–A, para equiparar à coisa todo dado ou informação em meio eletrônico; a base de dados armazenada em dispositivo de comunicação e o sistema informatizado, a senha ou qualquer meio que proporcione acesso aos mesmos;

- Alterar o art. 265 do CP, para incluir como objeto do crime de atentado os serviços de comunicação e telecomunicação;

- Alterar o art. 266 do CP, para prever o crime de perturbação ou interrupção de serviço telemático ou de telecomunicação;

- Acrescentar no CP o art. 266–A para definir o crime de difusão maliciosa de código;

4.2.2.3. Riscos de Imagem

Risco associado ao impacto negativo da opinião pública sobre uma organização, decorrente de envolvimento da empresa com operações ilícitas, danos ao meio ambiente, notícias sobre sua saúde financeira, falhas operacionais e de sistemas etc.

O risco de imagem vem associado à consecução de algum risco operacional ou legal e reflete-se diretamente no resultado dos negócios, quer pela perda de clientes, quer pela diminuição de negócios realizados. Assim, além dos prejuízos advindos do impacto de outros riscos, a organização vê sua imagem "arranhada" perante seus clientes.

Ao disponibilizar os serviços de *internet banking* aos clientes, as instituições elevam o grau de exposição do risco de imagem. Isto procede em virtude do fornecimento de mais um canal de negociação, e para o qual são requeridas ações específicas de gerenciamento de seus riscos inerentes. Situações, como as listadas a seguir, são decorrentes de outros riscos, mas contribuem para elevação do risco de imagem, a partir da diminuição da confiança dos clientes pela:

- efetivação de transações não autorizadas em contas de clientes;
- exposição ou roubo de informações confidenciais de clientes;
- constante indisponibilidade dos serviços oferecidos;
- dificuldades quanto à usabilidade das transações eletrônicas;
- sanções impostas por órgãos de supervisão bancária; dentre outras.

A etapa de identificação de riscos é uma atividade permanente em que a coleta de informações subsidia a fase subseqüente de análise e gestão dos riscos. Destaque-se a importância quanto ao estabelecimento de um procedimento contínuo de identificação de

riscos, tendo em vista a constante alteração nas formas de ataques, na identificação de novas vulnerabilidades e de novos códigos maliciosos.

4.2.3. ANÁLISE E PLANEJAMENTO DE AÇÕES PARA GESTÃO DOS RISCOS

De posse dos dados resultantes da monitoração dos ambientes dos clientes e dos bancos, e identificados os riscos a que a instituição está exposta, iniciam-se as fases de análise dos riscos e planejamento das ações de gestão.

Remetendo ao item 2.3.2, o administrador pode utilizar várias técnicas para analisar os riscos identificados, com o objetivo de mapear aqueles de maior criticidade. Desta forma, os gestores poderão direcionar seus esforços e recursos para minimizá-los, a partir dos níveis mais altos de exposição.

Importante relembrar que adotamos basicamente as seguintes estratégias para gerir os riscos: diminuição dos impactos, diminuição da probabilidade de ocorrência, terceirização dos riscos ou aceitação dos riscos / convivência com eles.

O planejamento deverá prever a adoção de medidas que visem diminuir a probabilidade de ocorrência, ou os impactos decorrentes. Essas medidas são categorizadas em três tipos:

- Medidas preventivas;
- Medidas detectivas; e
- Medidas corretivas.

Para as situações em que a estratégia é de convivência com os riscos, a monitoração atua como um gatilho a disparar medidas alternativas de correção ou de contingência. Neste caso, os indicadores de risco são fundamentais na identificação das situações de risco que extrapolem o apetite da instituição.

Nesta fase de análise e planejamento é de suma importância o exercício do controle sobre os riscos identificados. Assim, como forma de sugestão quanto à prática dessa

atividade, apresentamos, no anexo II, planilha para análise, planejamento e monitoração de riscos, na qual é possível identificar todos os elementos anteriormente citados.

A planilha concentra as informações resultantes da fase de identificação dos riscos, avaliando o grau de exposição pela medição do impacto versus a probabilidade de ocorrência. As etapas de análise e planejamento estão representadas pela definição e acompanhamento dos controles necessários para minimização dos riscos identificados. Por fim, as fases de monitoração e controle se prestam ao acompanhamento da evolução das medidas implementadas e gerenciamento dos riscos, identificando os responsáveis pelas providências a serem adotadas, bem como a situação atual de exposição ao risco, face à implementação das medidas de controle.

Aplicando-se as orientações acima para os serviços de *internet banking*, percebe-se que, atualmente, o maior risco existente e conseqüentemente grande foco de ataques está na monitoração passiva desenvolvida pelos atacantes. É cada vez mais crescente o número e a diversidade de *trojans* enviados aos clientes com objetivo de capturar os dados pessoais (agência, conta e senha de bancos, senha de MSN, *orkut*, *gmail* etc).

É importante ressaltar que embora o ataque de monitoração seja passivo é de alto risco, pois possibilita a captura dos dados bancários dos usuários e na seqüência efetuar transações fraudulentas por *spoofing* de autenticação.

Analisando-se a tabela 4.1, obtemos uma média de 111 ocorrências de *trojans* por dia enviados aos clientes. São ocorrências diversas, mas com o mesmo intuito de obter os dados dos usuários. Em suma, é uma diversidade muito grande de “armadilhas”, que distribuídas em um universo de aproximadamente 26 milhões de contas correntes (figura 1.3) elevam as probabilidades sucesso desse tipo de ataque.

O quadro apresentado torna-se mais preocupante quando juntamos o despreparo das pessoas para utilizar a *internet*, por desconhecimento dos riscos inerentes ao ambiente em que estão atuando, como também por parte dos administradores de rede e de sistemas, que demoram em atualizar os ambientes, ou não possuem habilitação suficiente para tal.

4.2.3.1. O COMPORTAMENTO DAS FRAUDES

Paralelamente à pesquisa sobre os ataques sofridos pelas instituições financeiras, procedemos com uma pesquisa sobre o comportamento dos atacantes, quanto ao *modus operandi* empregado nos ataques.

A conclusão a que chegamos é de que o atacante busca sempre o caminho mais fácil para seu ataque. Não encontramos materialidade suficiente relacionada com ataques a criptogramas, por exemplo. Esse tipo de ataque demanda um investimento muito alto tanto financeiramente, quanto de tempo e de conhecimento. O atacante busca sempre a forma mais simples para consecução de seus objetivos. Percebe-se que em todos os momentos em que há implementação de ações de segurança por parte das instituições financeiras, os ataques decrescem imediatamente, sinalizando uma "fuga" para outros bancos que ainda não implementaram medida adequada.

Pesquisa divulgada pelo Gartner Group [27], em 02 de junho de 2006, retrata o acima exposto. De acordo com a pesquisa, o mercado bancário brasileiro sempre esteve à frente na luta contra o *cybercrime*. Os bancos brasileiros têm presenciado todo tipo de ataque em seus serviços de *internet banking*, conforme figura 4.10. Por essa representação, percebemos a evolução dos ataques nos últimos quatro anos, desde os *keyloggers* até o mais recente tipo de ataque – *man in the middle*. Contudo, todas as formas apresentadas atuam no ambiente do cliente, ou seja, no elo mais fraco da cadeia de segurança. A ausência de legislação específica para o combate dos crimes virtuais contribui como motivador para o número de ocorrências registradas.

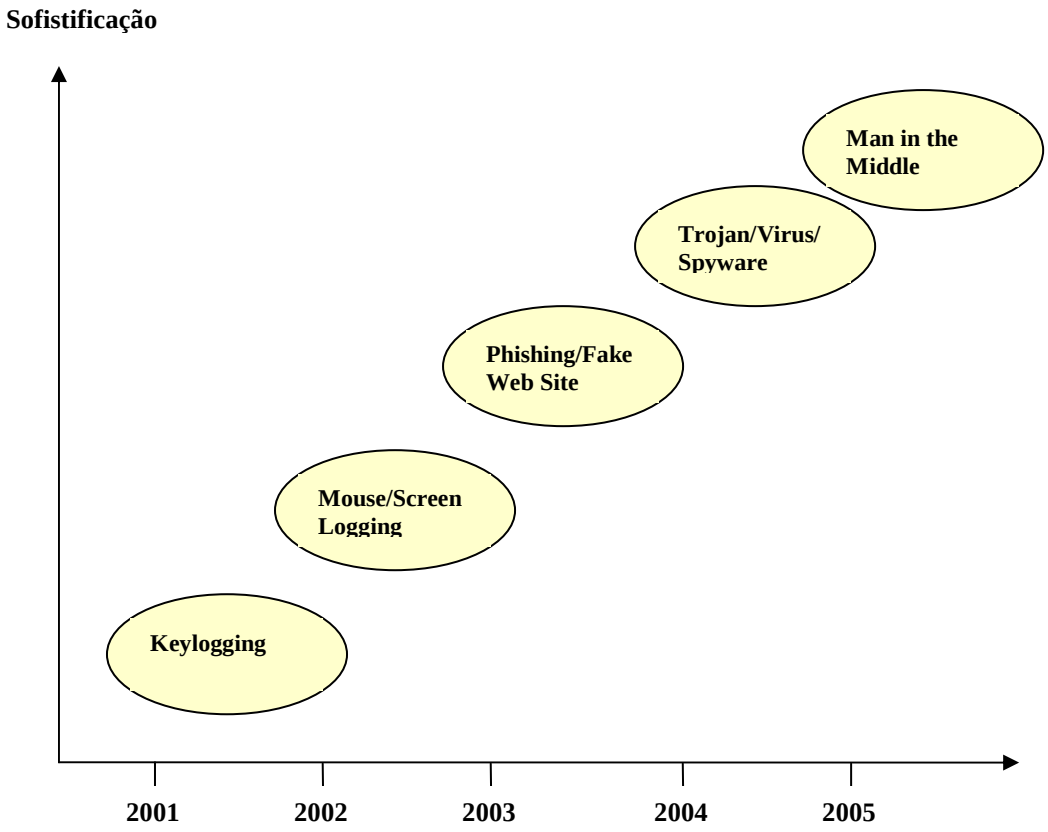


Figura 4.10: Ataques na internet

As figuras 4.11 e 4.12 corroboram com a afirmação quanto ao comportamento dos atacantes. O gráfico apresentado na figura 4.11 faz parte da pesquisa divulgada pelo Gartner Group, aplicado no banco HSBC, enquanto a 4.12 é fruto da pesquisa realizada por este autor. Percebe-se que cada vez que as instituições adotam medidas de segurança adicionais, a incidência de ocorrências diminui de imediato, voltando a crescer, quando os atacantes mudam a estratégia ou descobrem alguma outra vulnerabilidade.

Essa variação é notória e pode ser comprovada quando da implementação do teclado virtual, de sua randomização, do clique oculto, dos limites de transações, da monitoração ativa, do cadastramento de clientes e de computadores.

Como exemplo mais recente, o cadastramento de computadores realizado pelo Banco do Brasil, reduziu significativamente as ocorrências de fraudes no ambiente de *internet*. O que

se percebeu, logo em seguida, foi a migração dos ataques para o ambiente de *internet banking*, que não exigia cadastramento prévio para realização de transações financeiras.

Cada queda verificada nos gráficos é associada com a implementação de medida de segurança adicional pelos bancos. Não significa, contudo, que o ataque cessou. Provavelmente foi direcionado a outro banco, ou continuou surtindo efeito nos clientes que não adotaram as novas ferramentas de segurança.

Este fato, também vem a ser um problema a mais para os bancos. Embora disponíveis para uso pelos clientes, alguns optam por não as utilizarem, por motivos diversos. Assim, os ataques ainda continuam a surtir efeito, embora em menores grandezas.

Ao juntarmos as figuras 4.10, 4.11 e 4.12, conforme mostrado na tabela 4.5, podemos observar as ameaças e as medidas de segurança adotadas pelos bancos. Percebemos o atraso que existe entre a detecção de um novo tipo de ameaça e a adoção da solução de segurança. Esse atraso pode ser explicado por alguma falha no processo de gerenciamento de riscos – algumas etapas podem não estar sendo conduzidas apropriadamente.

Como exemplo de medida de segurança, apresentamos o teclado virtual do Banco do Brasil – figura 4.13.

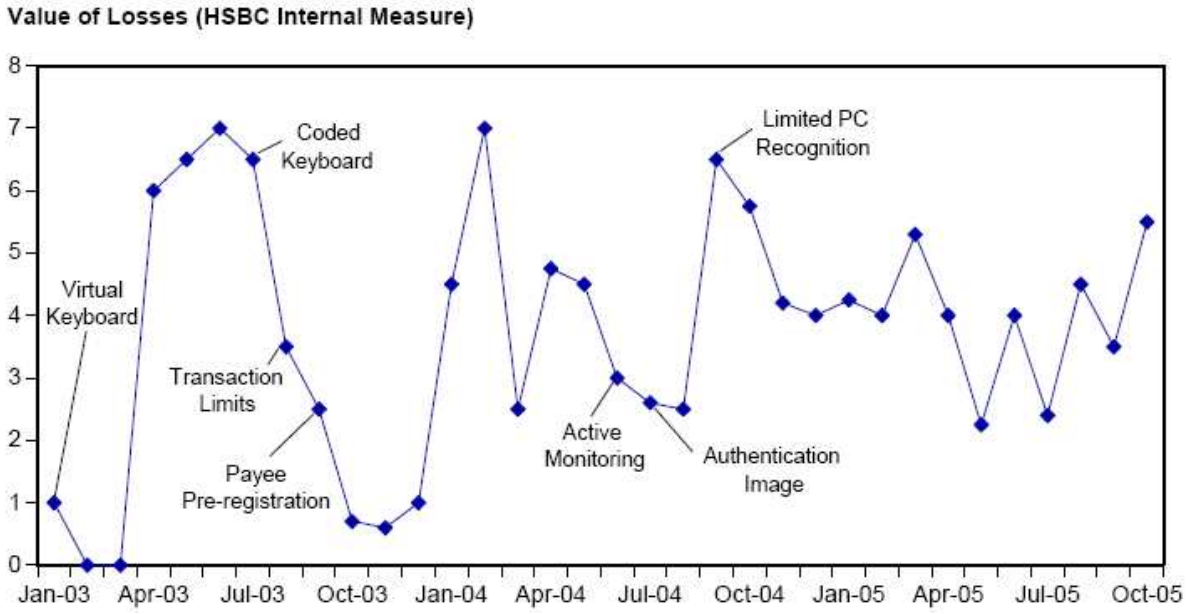


Figura 4.11: Ataques praticados versus solução adotada.

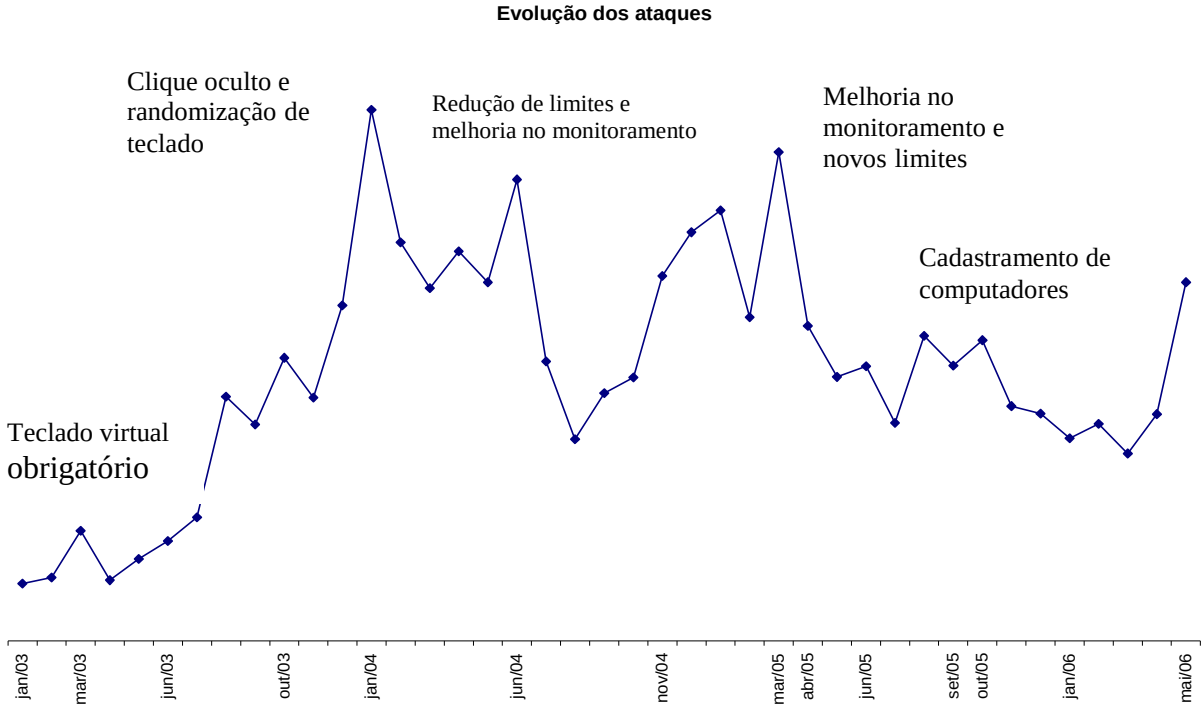


Figura 4.12: Evolução dos Ataques versus implantação de solução de segurança

Tabela 4.5: Detecção das ameaças versus implementação de medida de segurança

Ameaça	Detecção	Medida de Segurança	Implementação
Keylogger	2001-2002	Virtual keyboard	2003
Screen Capture	2002-2003	Browser defense	2004
Fake web site	2003-2004	Monitoring	2004
Trojan	2004-2005	Monitoring	2005
Man in the middle	2005-2006	cryptography	2006

Legenda:

Keylogger – ataque de captura das teclas digitadas
Screen Capture – ataque de captura das telas, buscando identificar a posição do teclado virtual.
Fake web site – páginas falsas de bancos
Man in the middle – ataque de envenenamento da transação
Virtual keyboard – teclado virtual
Browser defense – programa que blinda o browser do cliente quanto à ataques de captura de teclado e tela.
Monitoring – monitoramento exercido pelos bancos sobre as transações dos clientes.
Cryptography – uso de criptografia como solução de autenticação e confidencialidade

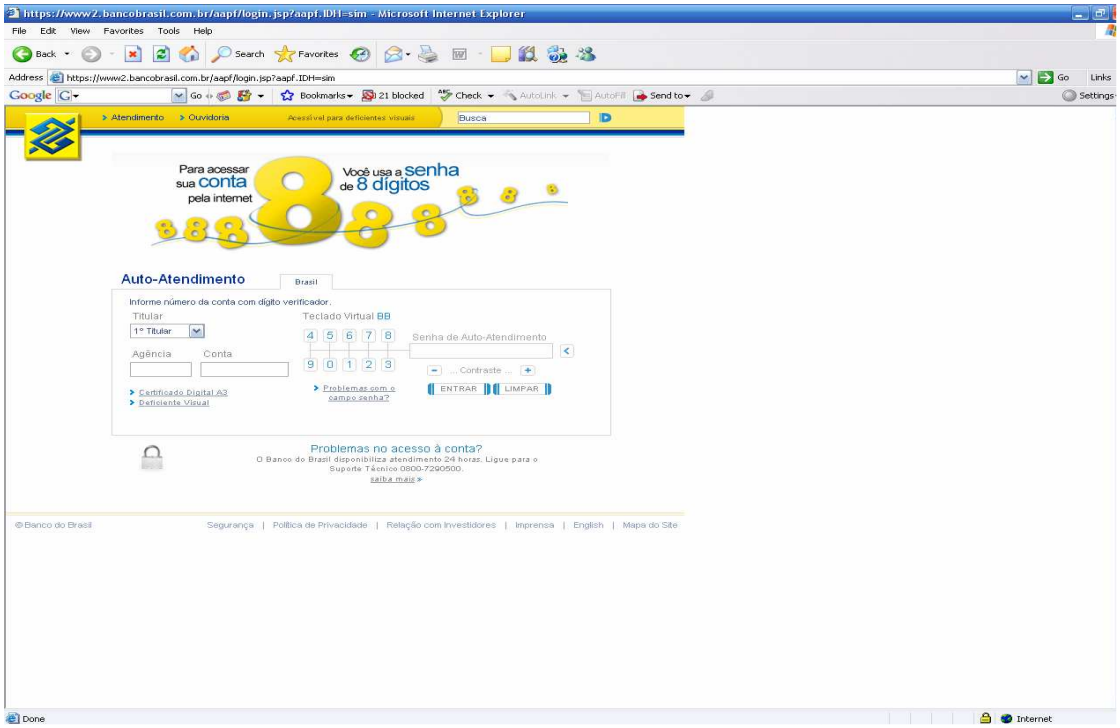


Figura 4.13: Teclado Virtual

Uma avaliação do ex-conselheiro da Casa Branca para segurança em TI, Howard Schmidt, divulgada no *site* da empresa Módulo [47], sinaliza que pequenas empresas devem tomar cuidados extras com a segurança de suas redes, pois vão tornar-se o principal alvo de *crackers* num futuro próximo. Em situação oposta encontram-se as grandes corporações que investem em soluções avançadas, tornando-se pouco atrativas para invasões. A explicação está diretamente relacionada ao fato de que, segundo Schimidt, poucos *crackers* são tecnicamente habilidosos a ponto de criarem mecanismos para driblar as medidas de segurança adotadas nos ambientes das instituições bancárias.

4.2.3.2. O PROBLEMA DA AUTENTICAÇÃO DOS CLIENTES

Conforme exposto nos parágrafos anteriores, a característica marcante nos ataques aos ambientes que compõem o *internet banking* das instituições financeiras é o caminho mais fácil. Assim, observamos que o “roubo” de senhas bancárias reutilizáveis, dentro da arquitetura atualmente em uso pelos bancos, vem se mostrando ser o meio mais fácil de

perpetrar fraudes. A gestão desse risco vem sendo tratada de diversas formas pelas instituições, na busca de elevar o nível de segurança do processo de autenticação.

O Federal Financial Institutions Examination Council (FFIEC) editou um guia [22] abordando os controles para gerenciamento de riscos e autenticação de clientes em ambientes baseados em *web*. Esse guia utiliza uma abordagem baseada em riscos para o gerenciamento de transações e recomenda que os bancos utilizem tecnologias de autenticação compatíveis com o risco das aplicações disponibilizadas aos clientes. O FFIEC é o órgão responsável pela uniformização da supervisão bancária nos Estados Unidos.

Embora não determine qual tecnologia deva ser adotada, promove a discussão sobre diversas formas de autenticação, como por exemplo, a biometria e os *smart cards*. O guia dá ênfase ao fato de que a adoção de senhas reutilizáveis não é mais suficiente para proteger os usuários das ameaças do mundo virtual, bem como das fraudes eletrônicas. A publicação desse documento é visto como um fator de motivação para que as instituições promovam melhorias quanto à segurança dos acessos de seus clientes aos serviços on-line.

De forma semelhante o FDIC – Federal Deposit Insurance Corparation vem editando artigos e publicações orientando os usuários sobre os riscos e cuidados a serem adotados quando utilizando serviços de *on-line banking* [18] [19].

A adoção de autenticação baseada unicamente em senhas é também observada em outros países. A solução de *internet banking*, fornecida pela empresa Misys, sediada em Londres, fundamentava-se na utilização de uma única senha para autenticar os clientes. Em raras situações, uma contra-senha era solicitada para realização de algumas transações.

Adicionalmente, analisamos os seguintes serviços de *internet banking*, disponibilizados por bancos estrangeiros:

1. Banco de Boston na Argentina - www.bankboston.com.ar
   O *site* oferece, em caráter opcional, o uso de teclado virtual para seus clientes. São exigidos código do usuário e senha.
2. Barclays Bank – www.barclays.co.uk

Não utiliza teclado virtual. O acesso não se dá pela conta, mas por combinação de nome e código de oito dígitos. A senha tem tamanho de 04 dígitos.

3. Citibank – www.citi.com

   Não utiliza teclado virtual. O código do usuário e a senha são informados via digitação dos caracteres. O código do usuário é cadastrado *online* informando o número do cartão de crédito ou débito e da conta. Nos acessos subseqüentes só usa o código do usuário, não precisa mais do número da conta ou cartão.

4. Bank of America – www.bofa.com

   Sem utilização de teclado virtual. São usados código do usuário, figura e senha. No primeiro acesso, o usuário escolhe, além do código e da senha *internet*, uma figura, supostamente para garantir a origem do *site*. Ao fazer o *sign-on* é informado o código do usuário e, antes de informar a senha, é apresentada a figura para que o usuário confirme se é a previamente escolhida.

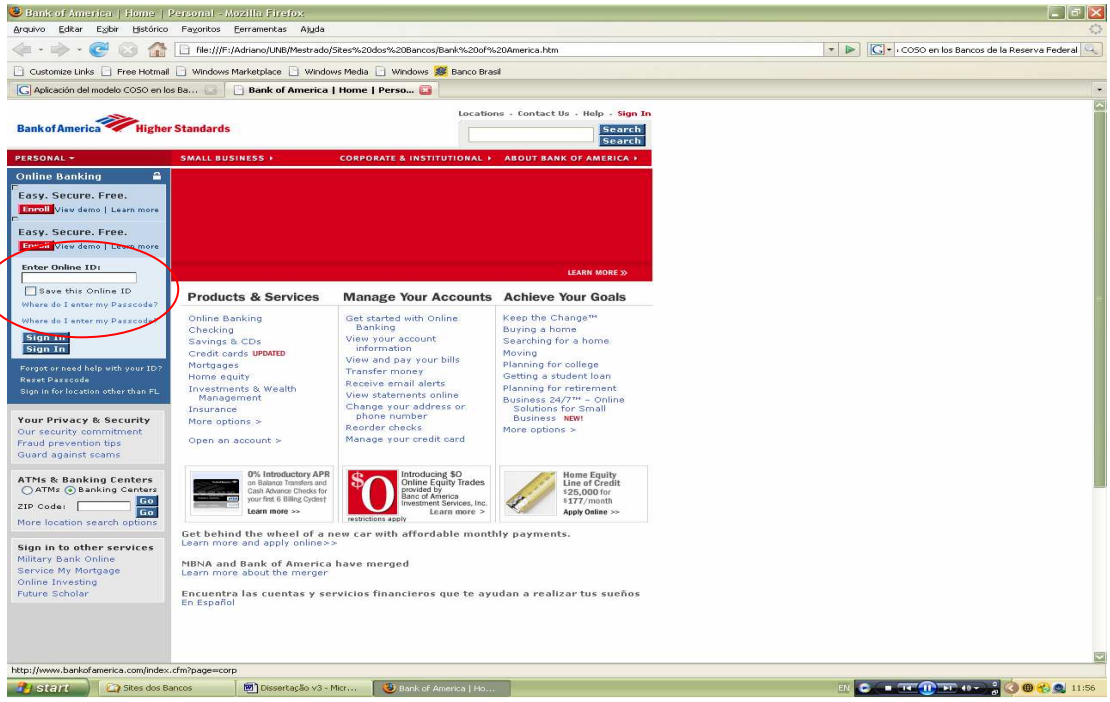


Figura 4.14: Site do Bank of America

5. Banco da Malásia – Maybank2u.com

Não utiliza teclado virtual. O acesso se dá pela conta e senha.

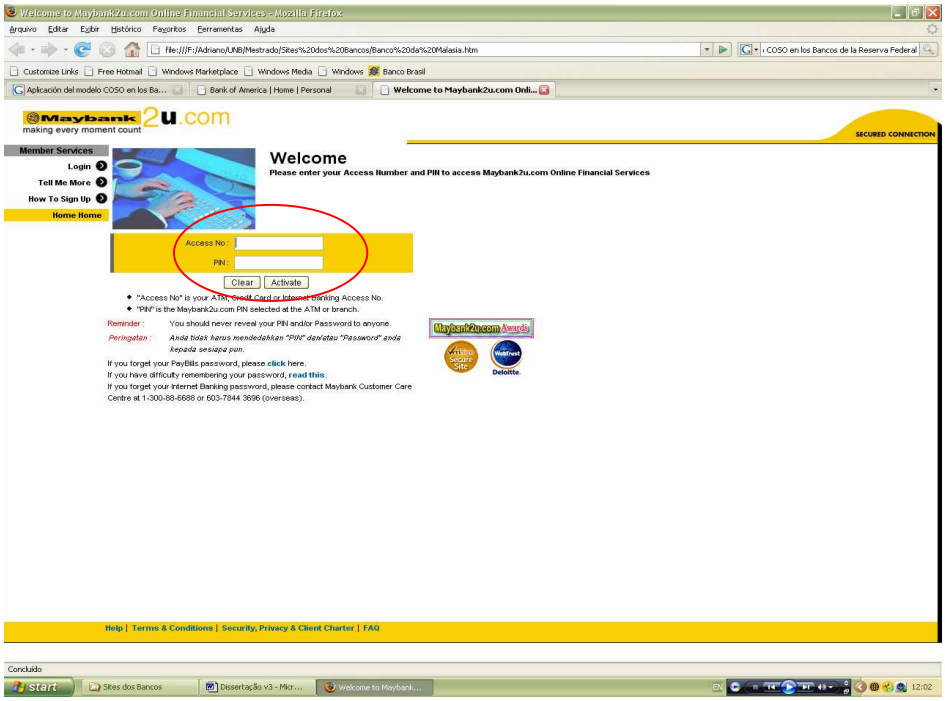


Figura 4.15: Site do Banco da Malásia

A Módulo Security [48] divulgou, em 20/10/2006, pesquisa conduzida pela empresa uSwitch, especializada em pesquisa de mercado, relatando que "O número de incidentes envolvendo a prática do *phishing* contra computadores pessoais no Reino Unido aumentou 800% em um ano. De agosto de 2005 a agosto de 2006, os registros saltaram de 160 ocorrências para 1.484".

Um fator que deve ser considerado é a influência da cultura no comportamento das pessoas. No período de outubro de 2006, em que estivemos desenvolvendo trabalhos de auditoria em Londres, percebemos que prevalece a premissa de confiar nas pessoas. Quando alguém se identifica verbalmente, presume-se que ela esteja falando a verdade. Contudo, as penalidades são severas para os casos em que se comprovem o fornecimento de informações falsas. Acontece, que não se pode transportar essa cultura para o ambiente virtual, em que os

atacantes não obrigatoriamente estão localizados em território inglês e sujeitos à legislação local. Sob essa análise, os resultados apresentados pela uSwitch se justificam.

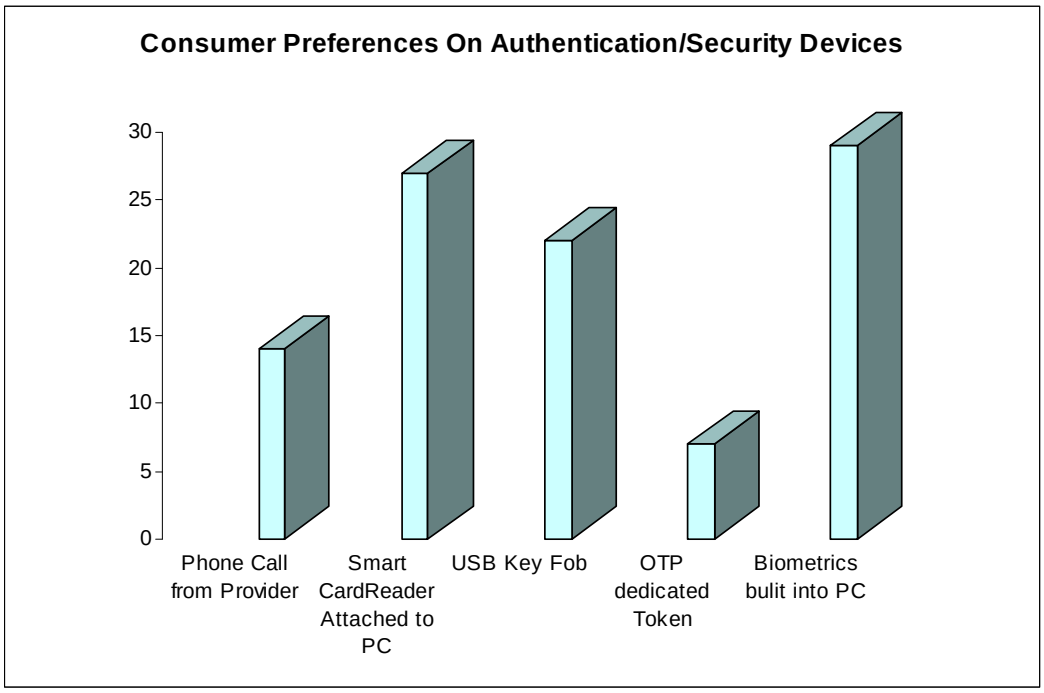
O Brasil, talvez por falta de uma legislação mais eficiente, está à frente desses países em termos de adoção de soluções de autenticação. Teclados virtuais, *browser defense*, senhas dinâmicas, cadastramento de computadores, biometria e mais recentemente a certificação digital são medidas já adotadas por vários bancos.

A questão da autenticação contínua, em contra-partida com a realizada uma única vez, destaca-se atualmente, tendo em vista que os ataques de *man in the middle* ou *man in the browser* podem executar aplicativos, escondidos nos computadores do usuário, após a identificação e autenticação inicias do usuário. Como a autenticação é realizada apenas no início, o ataque se aproveita para "envenenar" as transações realizadas subseqüentemente à autenticação.

Sobre o guia do FFIEC, o Gartner publicou, em 2005, artigo intitulado "*Regulators Tell U.S. Banks to Adopt Stronger Risk-Based Authentication*" [28] em que tece algumas considerações sobre a implementação de ações de segurança pelos bancos americanos, em resposta à referida publicação. De acordo com o artigo, as instituições estariam dispostas a adotar autenticação forte, mais para aumentar a confiança do cliente e atender à regulamentação, do que para reduzir as ameaças de fraude. A expectativa é de até o final de 2006, 85% dos bancos americanos adotassem autenticação de usuários mais fortes que as baseadas unicamente em senhas, como: teclados virtuais, ou autenticação por desafio (*knowledge-based*). As instituições que dispõem de mais recursos poderão adotar medidas complementares como monitoração de transações fundamentadas em "redes bayeseanas". Esse método implementa monitoração de comportamento anormal das transações.

Supõe-se que o comportamento resultante seja de migração dos ataques, primeiramente para as instituições que não adotam algum tipo de autenticação forte, depois para as instituições com soluções menos seguras. O Gartner acredita que em 2007 os ataques mais freqüentes serão predominantemente de "*man in the middle*", burlando as autenticações que não são contínuas e não suportadas por detecção de transações anormais.

Sobre o uso de autenticação por certificação digital (*tokens, smart-card*) ou mesmo biometria, os bancos estariam mais propensos pelos dispositivos de *tokens* ao invés de biometria, pelos custos associados. Os clientes, entretanto, preferem o uso da biometria, como demonstrado pela pesquisa realizada pelo Gartner [29], em maio de 2005 – figura 4.16.



Fonte: State of the Art for Online Consumer Authentication.pdf [29]

Figura 4.16: Preferência dos clientes quanto aos dispositivos de segurança para autenticação de transações on-line.

O artigo "*State of the Art for Online Consumer Authentication*" [29], publicado pelo Gartner Group, em 05/05/2006, trata do problema enfrentado pelas instituições financeiras, no mundo todo, quanto à identificação e autenticação de seus clientes, usuários dos serviços de *internet banking*. De acordo com esse artigo, autenticação forte é necessária, mas nunca será suficiente, por si só, mas apenas uma camada em uma arquitetura que demanda outros níveis de proteção.

Como exemplo dessa complementação de camadas, são apresentadas as ações de monitoração sobre as anomalias dos padrões de transações dos clientes (redes bayeseanas), autenticação interativa com os usuários e verificação de transações. Os bancos americanos e

brasileiros destacam-se, perante o resto do mundo, na adoção de medidas complementares de segurança.

Dentro da linha de raciocínio explicitada na análise sobre o comportamento dos atacantes, pode-se prever que os bancos que não investirem em autenticação forte e subseqüentemente aqueles que investirem tão somente nessa camada de defesa serão, nesta ordem, alvos de ataques contra seus clientes, o que com certeza elevará o risco de imagem da instituição, refletindo em perda de confiança e "fuga" de clientes.

Analisaremos, a seguir, as principais medidas de segurança quanto à autenticação dos clientes, adotadas pelos principais bancos brasileiros. Essa análise tomou como base o artigo acima citado, o conhecimento e a experiência deste autor em auditoria de sistemas e do orientador dessa dissertação.

4.2.3.3. SOLUÇÕES DE AUTENTICAÇÃO DE CLIENTES

4.2.3.3.1. Senhas Simples

Senhas são palavras ou combinações de caracteres, de conhecimento exclusivo do usuário, que são digitadas por meio do teclado do computador para validar a autenticação dos clientes. Essas senhas são cifradas e assim enviadas aos bancos para autenticação.

Esse tipo de autenticação, embora bastante simples, é universalmente utilizada e seu uso é facilmente compreendido pelos usuários. São vulneráveis aos ataques de *phishing scan* e *trojans* de *keylogger*.

Esse tipo de autenticação ainda é bastante utilizado pelos bancos nos Estados Unidos e outros países fora do Brasil. Vide exemplos indicados na seção anterior.

4.2.3.3.2. Teclados Virtuais

A utilização dos teclados virtuais veio para incrementar a segurança do uso de senhas, não permitindo sua digitação pelo teclado do computador e sim por meio de um teclado exibido na tela de entrada dos *web sites* dos bancos. Assim, o usuário faz uso do *mouse* para digitar sua senha, clicando sobre os respectivos caracteres.

Embora proteja o usuário contra ataques de *keyloggers*, é vulnerável aos *mouseloggers* e *screenloggers*, ou seja, *trojans* que capturam as telas acessadas e conseqüentemente o movimento e clique dos mouses.

4.2.3.3.3. Senhas cognitivas

As senhas cognitivas são aquelas baseadas no conhecimento de informações adicionais por parte dos usuários. Assim, previamente, o usuário cadastra algumas informações que são solicitadas, randomicamente, quando de sua autenticação perante a instituição financeira.

As senhas cognitivas, embora sejam de fácil utilização pelos clientes, estão sujeitas aos ataques de engenharia social e *trojans* que capturam teclados ou telas. Após um certo número de observações é possível ao atacante constituir banco de dados com as informações dos clientes.

Esse tipo de senha é geralmente usado complementarmente ao uso de senhas simples, ou teclado virtual.

4.2.3.3.4. Senhas dinâmicas

As instituições financeiras entregam aos clientes uma lista de números que serão solicitados, seqüencialmente ou não, a cada transação. São as chamadas "OTP – *One Time Password*". Para efetivação de uma transação ou para autenticar o cliente, o banco solicita um determinado número, dentro da lista entregue previamente ao cliente. Esse tipo de senha é utilizado complementarmente à solicitação da senha do cliente.

Essa solução, de baixo custo de implementação é vulnerável a ataques de engenharia social. O uso pelo cliente demanda medida adicional de segurança, pois não é aconselhável que a lista de senhas seja guardada em conjunto com o cartão bancário. Como normalmente o usuário faz uso da *internet* no trabalho, em *notebooks* e na residência, eleva-se a dificuldade da guarda e transporte seguros da lista gerada. A administração pelo cliente também é considerada como dificultador para essa solução, pois ele deve ir, a cada utilização, eliminando os números solicitados.

Como a instituição usa uma lista pré-definida, o atacante pode utilizar-se dos ataques de *spoofing* e *phishing*. Apresenta ao cliente um *site* forjado do *internet banking* da instituição

e solicita os dados dos clientes, inclusive um número da lista. Em resposta aos dados digitados, o atacante pode alegar que o número já foi utilizado, induzindo o cliente a digitar outro número. Assim, o atacante obtém um número válido de senha dinâmica.

Também é susceptível ao ataque de "*man-in-the-browser*".

4.2.3.3.5. Cartões de Grid

Essa solução já foi apresentada nesse trabalho e corresponde àquela utilizada pelo banco Bradesco. Os clientes recebem um cartão com números dispostos randomicamente por linhas e colunas. A cada autenticação, o usuário é solicitado a digitar o número correspondente a determinada posição.

Baixo custo e fácil utilização são os pontos fortes dessa solução. Contudo, está sujeita a ataques de engenharia social, conforme já detalhado em "Ataques de Engenharia Social". Também possui os mesmos inconvenientes quanto à guarda e transporte seguros do cartão. Como o cartão não possui proteção para encobrir os números, a cópia do seu conteúdo é facilitada, por meio de scanner ou fotocopiadoras.

4.2.3.3.6. Autenticação baseada em Tokens

Dispositivos OTP (*One Time Password*). Esse método utiliza *tokens* pessoais para gerar as OTP que são enviadas, via *browser*, para as instituições financeiras. Caracteriza-se por ser uma tecnologia já testada e aprovada, mas possui um alto custo como fator desestimulante. Outra desvantagem dessa tecnologia diz respeito ao fato do *token* ser exclusivo para um determinado banco. Assim, caso o usuário possua contas em vários bancos, deverá possuir vários *tokens*.

Dispositivos de *smart tokens* ligados aos computadores. Nesse método, os clientes dispõem de *smart cards* ou *tokens* com dispositivos de *smart chip* que armazenam as senhas criptográficas. Possui como vantagem as características de segurança associadas ao uso da criptografia, mas os altos custos e a mobilidade ainda são fatores que não permitem o uso maciço dos dispositivos. A questão da mobilidade refere-se à disponibilidade de leitores e software de suporte operacional nos computadores a serem utilizados pelos clientes.

Alguns bancos brasileiros, dentre os quais o Banco do Brasil, já disponibilizam aos seus clientes a solução de certificação digital para autenticação forte [20].

A certificação digital implementa um nível mais avançado de segurança, por meio de uma solução que utiliza uma chave privativa do certificado do cliente, que é de seu uso exclusivo, secreto e intransferível, e uma chave pública. No processo de autenticação, o banco desconhece a chave privativa de criptografia do cliente, armazenada no chip do *smart card*.

A solução aqui descrita utiliza certificados vinculados a ICP-Brasil, dentro do padrão e-CPF (Figura 4.17) e e-CNPJ. Essa utilização traz como vantagem o uso de um cartão único para todas as instituições financeiras, não havendo necessidade de adotar cartões individuais para cada banco.

Figura 4.17: e-CPF

4.2.3.3.7. Identificação de dispositivos dos clientes

Esse método, utilizado pelo Banco do Brasil, consiste em cadastrar previamente os dispositivos utilizados pelos clientes para efetuarem suas transações financeiras. O cadastramento restringe o acesso a serviços bancários aos dispositivos previamente cadastrados.

O cadastramento pode se dar pela utilização de diversas características inerentes aos dispositivos usados pelos clientes, como números de endereços IP, configurações de hardware ou software.

O ponto forte consiste em impedir que os atacantes utilizem seus próprios equipamentos para efetuarem as transações financeiras em nome de clientes legítimos. No item dedicado aos ataques de engenharia social, descrevemos a forma que os atacantes usam

para enganar os usuários e cadastrarem seus próprios computadores. A mobilidade também se apresenta como fator de desvantagem, pois para efetuar as transações financeiras, os clientes devem, a priori, cadastrar os computadores.

4.2.3.3.8. Detecção de transações anômalas

Esse método é complementar ao uso de autenticação forte. Um perfil de uso é criado para cada cliente. Ao realizar uma determinada transação, essa é comparada com o perfil armazenado. Caso a transação seja considerada “anormal” é disparada alguma ação preventiva por parte da instituição, podendo contemplar a realização de uma ligação de confirmação, ou o envio de mensagem solicitando confirmação.

Não há necessidade de instalação de aplicativos nos dispositivos dos clientes. Mas, o elevado índice de ocorrências do tipo falso-positivo (transações verdadeiras consideradas espúrias) impõe um gerenciamento mais rigoroso sobre as travas à realização das transações. Também não garante a autenticidade do usuário que está realizando a transação, sendo usada como método complementar aos de autenticação.

4.2.3.3.9. Autenticação Biométrica

Esse método usa traços biométricos dos usuários para realizar a autenticação nos servidores das instituições. Os traços mais comuns são as digitais, a voz, a palma da mão, o mapeamento das veias sanguíneas, a íris e a face.

Tem como principais desvantagens, os custos e a mobilidade, pois necessitam que os computadores, a serem utilizados para realização das transações, possuam dispositivos biométricos de autenticação. Também devemos considerar os aspectos de intrusão, como as radiações emitidas pelos dispositivos.

4.2.4. MONITORAÇÃO E COMUNICAÇÃO

O processo de monitoração consiste no acompanhamento dos eventos que possam por em risco a segurança dos serviços financeiros disponibilizados pelos bancos, a segurança dos dados dos clientes armazenados nas instituições e a própria segurança dos sistemas bancários.

A ISO 17799 [36] dispõe no capítulo 9, item 9.7 que: “Convém que os sistemas sejam monitorados para detectar divergências entre a política de controle de acesso e os registros de eventos monitorados, fornecendo evidências no caso de incidentes de segurança”.

O meio encontrado pelas instituições financeiras para exercer um monitoramento eficiente sobre os riscos de segurança no ambiente de *internet banking* foi a instituição dos CSIRT – *Computer Security Incident Response Team*, que em português é traduzida como Grupo de Resposta a Incidentes de Segurança. Além de exercer uma atividade de reação aos eventos detectados, essa equipe desenvolve um trabalho preventivo na detecção dos riscos e das ameaças ao ambiente de *internet*.

Este grupo é capacitado a prover rápida recuperação dos sistemas, em casos de incidentes de segurança, com a vantagem de preservar suas evidências e causas, tendo assim maiores condições de avaliar a extensão do problema.

Foi justamente como base no trabalho desenvolvido pelos CSIRT das instituições financeiras, que desenvolvemos nossas pesquisas. Esse grupo mantém uma ação conjunta na identificação de eventos maliciosos e troca de informações, contribuindo para uma maior agilidade na adoção das ações corretivas.

O monitoramento do ambiente do cliente é executado por meio de agentes instalados nos computadores pessoais. Os agentes baseiam-se em padrões de assinatura e métodos heurísticos. Ao detectar comportamentos não previstos, os agentes informam ao servidor dos Bancos a ocorrência de ataque. As equipes de monitoração adotam, então as medidas apropriadas para controle da ameaça.

A monitoração no ambiente das Instituições é feita pelo acompanhamento dos *logs* de segurança para os *firewalls* e IDS (*Intrusion Detection System*). Estes equipamentos são ajustados para detectar padrões de comportamentos diferentes das regras estabelecidas.

Dentro da etapa de monitoração, uma das atividades mais importantes é a coleta de informações relevantes para um determinado risco. Durante a etapa de planejamento das ações de gestão dos riscos identificados, informações de acompanhamento ou mesmo indicadores de risco são estabelecidos de forma a observar o progresso dos riscos mapeados,

como forma de medir a eficácia dos controles estabelecidos. Lembremo-nos, que para aqueles riscos classificados dentro da estratégia de “convivência”, o acompanhamento da evolução do nível de criticidade é fundamental e pode influenciar na reavaliação da estratégia adotada pelos administradores.

O resultado da etapa de monitoração é consolidado por meio de relatórios que informam, dentre outros fatores, a evolução dos riscos mapeados, a eficiência dos controles estabelecidos, as mudanças significativas no ambiente de *internet banking*, bem como no comportamento dos atacantes e as tendências identificadas para ameaças e vulnerabilidades. Esses relatos retroalimentam as etapas anteriores do ciclo de gerenciamento dos riscos, sendo fundamentais na identificação, análise e planejamento das ações de gestão de riscos.

Decisões como replanejamento, encerramento de risco, ativação de plano de contingência ou mesmo continuação do monitoramento e execução do plano corrente são tomadas com base nas informações coletadas e reportadas pela equipe de monitoração.

Aqui, cabe-nos aprofundar as razões para as decisões acima explicitadas. O replanejamento se dá quando da necessidade de alterar ou mesmo criar planos de ação. Quando os indicadores de riscos são extrapolados há uma sinalização de que os controles instituídos se mostram ineficazes. Outra situação é a identificação de novas vulnerabilidades ou tendências de ataques, requerendo uma ação de replanejamento para ambas as situações.

O encerramento de um risco se justifica quando aquele não mais se apresenta, ou a relação custo x benefício não mais se justifica em face da redução da probabilidade de ocorrência ou dos impactos advindos a índices toleráveis pela organização.

Recorremos aos planos de contingência quando os indicadores de risco são excedidos e há a necessidade de adoção de medidas emergenciais. Importante frisar que mesmo após a retomada das atividades normais, os riscos que causaram a ativação dos planos de contingência voltam a ser monitorados, dentro do planejamento em curso.

Por fim, a decisão pela continuidade dos planos atuais se justifica quando os relatos da monitoração indicam que todos os fatores estão se comportando dentro do planejado.

Quanto ao processo de comunicação, este se destina a prover informações sobre os riscos identificados, bem como sobre o aparecimento de novas situações.

O processo deve ser exercido em via de mão dupla, ou seja, tanto pelos responsáveis por garantir a segurança dos serviços de *internet banking*, como pelos funcionários e clientes de um modo geral. Sem a participação ativa dos funcionários, e dos clientes, através de relatos sobre incidentes de segurança, a eficácia da gestão de riscos pode diminuir significativamente. Assim, torna-se imprescindível que usuários saibam da importância de relatar incidentes de segurança, assim como a forma e o local de envio dos relatos.

5. APLICAÇÃO DA PROPOSTA

A proposta de utilização de um modelo de gerenciamento de riscos para ambientes de *internet banking*, como forma de minimizar os riscos de fraudes e de perdas financeiras foi aplicada com base nas séries históricas de perdas ou de ataques e na efetiva monitoração dos eventos de segurança.

Dentre as fases que constituem o modelo de gerenciamento apresentado, destacamos as de monitoramento e de análise e planejamento de soluções como essenciais para seu sucesso, considerando-se seu caráter preventivo.

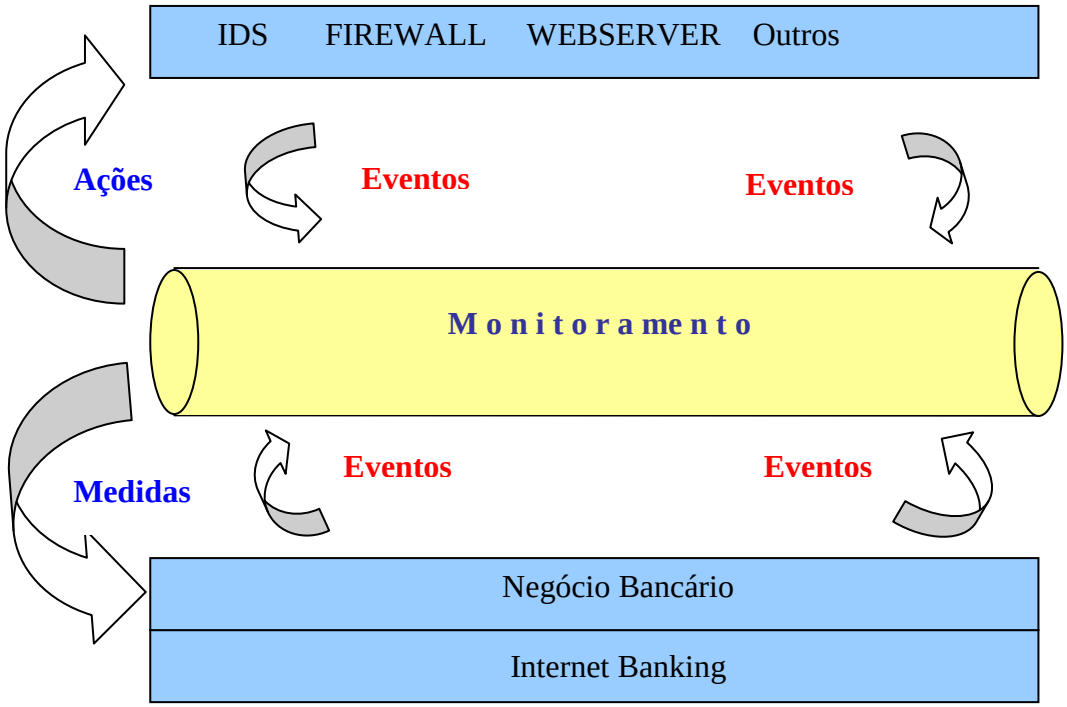


Figura 5.1: Gestão integrada de Riscos

A figura 5.1 nos apresenta o processo de monitoramento, em que os eventos de segurança, bem como as transações de negócio são acompanhadas pela equipe de monitoramento. Como base em regras pré-estabelecidas e considerando-se o apetite ao risco, estabelecido pela administração, são adotadas ações corretivas e medidas de segurança, como resposta aos eventos monitorados.

Pela figuras 5.2 percebemos, de forma clara, que até início de 2004 o "*gap*" de tempo entre a detecção de eventos maliciosos e a adoção de medidas adicionais de segurança possibilitava um número elevado de fraudes bancárias.

A partir de 2004, as equipes de monitoramento (CSIRT) passam a exercer suas funções de forma mais efetiva, aliada à instituição do consórcio de bancos. Observa-se, então, uma diminuição no tempo decorrido entre a detecção de eventos de fraude e a adoção de soluções, que passaremos a chamar de Δt.

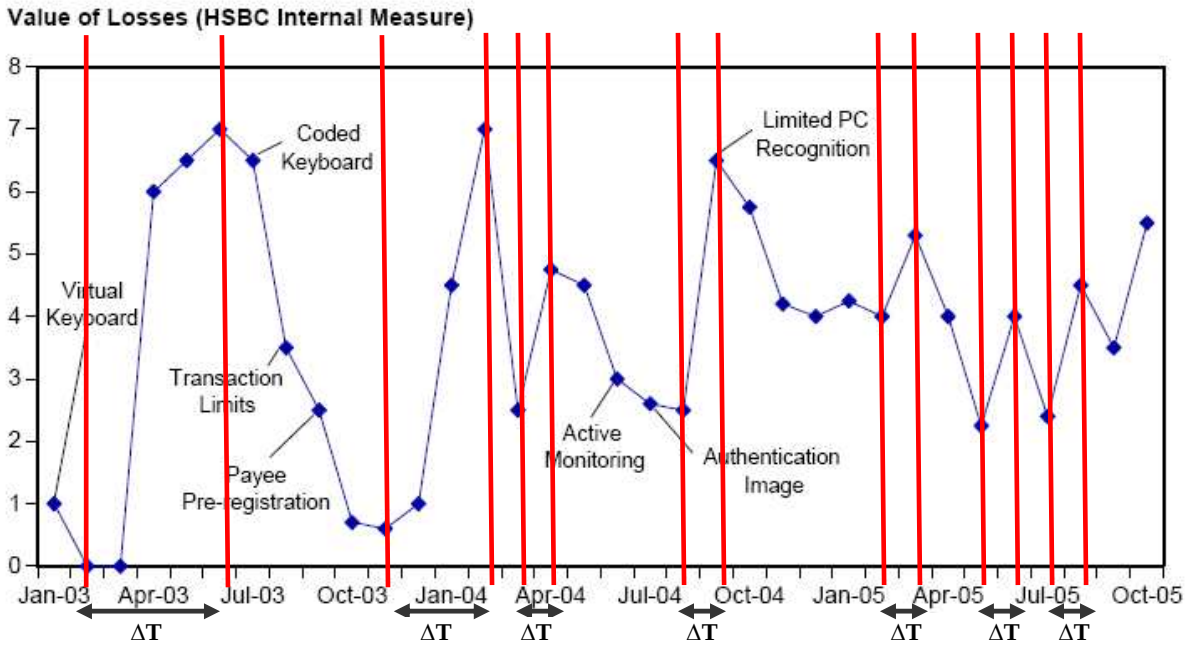


Figura 5.2: Variação de ΔT na adoção de soluções de segurança

A conjugação dos fatores: definição do apetite de riscos pela administração, efetivo exercício do ciclo de gerenciamento de riscos, em destaque as fases de monitoramento e análise e planejamento influenciam significativamente na diminuição do intervalo de tempo decorrido entre a observação de eventos, a análise e entendimento do ataque e a implantação de camadas adicionais de segurança. A atuação colaborativa dos bancos também contribui na diminuição desse tempo.

A figura 5.3 apresenta a curva 2 como representação da variação de tempo desejável, quando aplicados os conceitos de gerenciamento de riscos. O uso disciplinado e maduro possibilita a redução do tempo de resposta aos ataques detectados. A diminuição representa uma atuação mais rápida pelas instituições, implicando na redução das fraudes e conseqüentemente no número de ataques com sucesso.

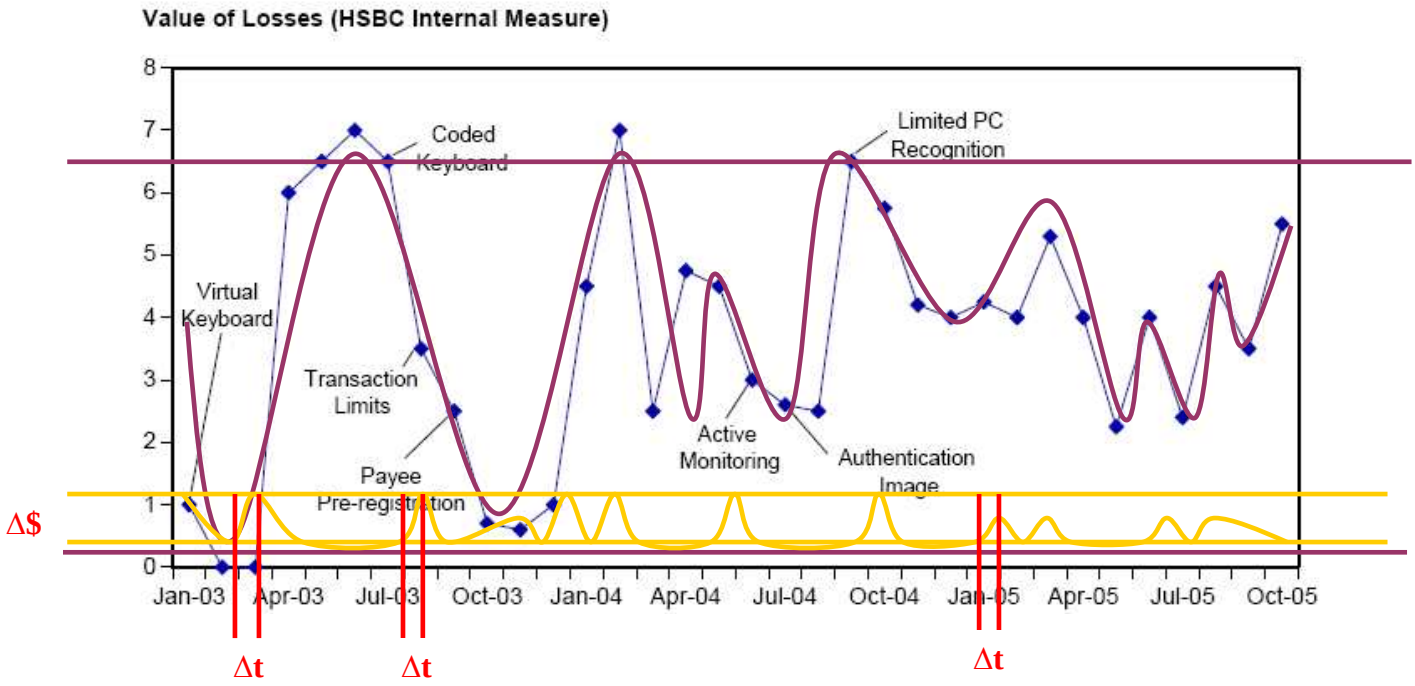


Figura 5.3: Diminuição da curva de tempo na adoção de soluções

Legenda: Curva 1
Curva 2

6. CONCLUSÃO

Administrar riscos é administrar incertezas. O modelo apresentado neste trabalho propôs a adoção de cinco fases dentro de um ciclo contínuo de gerenciamento de riscos. O ponto central da adoção de um modelo de gerenciamento de riscos consiste em uma cuidadosa identificação de riscos, como forma de classificar e ranquear todas as ameaças de acordo com suas relevâncias. Essa classificação possibilita uma atuação preventiva no combate aos riscos.

Ao seguir as etapas propostas, é possível reduzir o tempo decorrido entre a identificação de uma nova ameaça e a adoção de ações corretivas. Conforme verificamos na tabela 4.5, existe um atraso entre a percepção de uma ameaça e a adoção de medidas corretivas. Na medida em que o modelo se torne maduro, as ações hoje adotadas pelas instituições também se aprimorarão, possibilitando a adoção de soluções de segurança cada vez mais rápidas. Acreditamos que um modelo maduro de gerenciamento dos riscos pode permitir uma antecipação aos atacantes, impedindo a consecução de uma nova ameaça.

Nesse contexto, as fases de monitoração, pela atuação conjunta das equipes de CSIRT – *Computer Security Incident Response Team* e a análise dos eventos detectados exercem papéis fundamentais para o amadurecimento do modelo apresentado.

Ao adotar um modelo de gerenciamento de riscos, a instituição pode reduzir o número de fraudes e de perdas financeiras. Algo bastante apreciado pelos acionistas e órgãos reguladores. Ademais, reduz os riscos operacionais, legais e de imagem, elevando a satisfação dos clientes com a segurança implementada pela instituição.

De acordo com Liliana Rojas-Suárez [58], “uma das características do futuro do setor bancário pelo mundo é a de melhorar as técnicas de avaliações de risco e o Brasil não é exceção”.

Os principais riscos identificados foram de ordem operacional, legal e de imagem. Os riscos operacionais estão diretamente relacionados à segurança da informação, nos aspectos de confidencialidade, integridade e disponibilidade.

No Brasil, a deficiência nas leis quanto à tipificação de crimes virtuais e das respectivas penas é considerada como um dos fatores que favorecem o crescente número de ataques.

Quanto ao risco de imagem, é essencial que os clientes tenham uma clara percepção de segurança, quando transacionando com seus bancos. A adoção de soluções seguras favorece esse objetivo e contribui para a fidelização dos usuários.

Algumas instituições financeiras exercem atuação conjunta no monitoramento, análise e comunicação dos eventos maliciosos detectados. As equipes de CSIRT interagem entre si e entre as diversas entidades de segurança (inclusive a força policial), possibilitando a troca de informações e a adoção imediata de medidas corretivas. Sobre a atuação desse grupo, efetuamos pesquisas sobre os principais ataques desferidos contra esses bancos.

As conclusões resultantes dessa pesquisa apontaram o ambiente pessoal dos clientes como de maior criticidade e alvo predileto dos ataques contra os serviços de *internet banking*. A forma de ataque mais comum e de maior efetividade é a engenharia social. Esse tipo de ameaça representa o maior desafio para os bancos, pois trabalha com o comportamento das pessoas e os clientes dos bancos vêm demonstrando ingenuidade, quando submetidos a esses ataques, facilitando a descoberta de seus dados pessoais e bancários.

Quanto aos ataques desferidos contra o ambiente das instituições, concluímos que são todos conhecidos e suas correções disponíveis nos *web sites* dos fornecedores dos aplicativos. Aqui, a vulnerabilidade consiste na demora, ou despreparo por parte dos administradores de rede em atualizar os ambientes.

Outra importante ameaça identificada está relacionada ao “envenenamento” de transações. Nesse tipo de ataque, as transações bancárias são interceptadas e modificadas antes de seu envio aos Bancos. A solução que mais se adequa ao combate a esse tipo de ataque é a utilização de *tokens*.

Sobre o comportamento dos atacantes, ficou evidenciado que esses buscam sempre o caminho mais fácil. Em todos os momentos em que os bancos implementam medidas adicionais de segurança, percebe-se uma diminuição do número de ataques. Essa diminuição

pode significar a migração dos ataques para outros bancos que ainda não implementaram medidas semelhantes.

Outra vulnerabilidade apontada refere-se ao despreparo dos usuários em utilizar o *internet banking*. Por desconhecerem os riscos e as ameaças que se fazem presentes, os clientes são vítimas mais fáceis para os fraudadores. É essencial que as instituições, bem como a federação de bancos, invistam cada vez mais forte em campanhas educativas. Já se percebe alguma movimentação nesse sentido, contudo incipientes e não contínuas. Acreditamos que a medida em que os usuários estejam mais preparados, os atacantes terão mais dificuldades em obter sucesso.

Em resposta às ameaças identificadas, os bancos implementam soluções cada vez mais sofisticadas e criativas, dentre as quais destacamos: o cadastramento de computadores, a utilização de senhas dinâmicas, autenticação baseada em *tokens* e certificados digitais, bem como a detecção de transações anômalas.

Os resultados das pesquisas realizadas nos mostraram a queda do número de ocorrências, quando da implantação de medidas adicionais de segurança, trazendo uma diminuição dos prejuízos por parte dos bancos.

Da parte das instituições, apresentamos na tabela 1.1 um comparativo entre os valores das transações, quando efetuadas nos canais *internet banking*, agência e correspondente não bancário. Os custos para os bancos é de longe favorável ao canal *internet*.

Assim, entendemos que as instituições financeiras devam alinhar os interesses pelo uso do canal eletrônico com a adoção de medidas adicionais de segurança. Ousamos propor uma estratégia aos bancos quanto ao uso de certificados digitais. Primeiramente, identificar os nichos negociais mais atraentes e também de maior incidência de ataques. Distribuir, sem custos adicionais, certificados digitais a esses clientes. Comparar os ganhos obtidos pela redução do número de fraudes com os valores dos certificados distribuídos. Sabendo que o custo de um certificado varia em torno de duzentos reais, acredito que esse custo total se pagaria somente com o obtido com a redução nos valores das fraudes.

Essa estratégia é fruto da utilização efetiva do modelo de gerenciamento de riscos, onde percebemos a utilização direta das fases de identificação, análise, planejamento e monitoração.

O ambiente de *internet banking* trouxe facilidade e comodidade aos usuários e abriu perspectivas de novos negócios para os bancos, resultando no incremento de seus resultados financeiros. Fraudes e roubo de informações sempre existiram, mesmo antes do surgimento desse novo canal de atendimento.

A facilidade proporcionada aos atacantes reside no acesso a uma amostra de clientes muito superior ao que se conseguiria ao abordar os clientes dentro das agências bancárias. Ao lançar *trojans* ou *loggers* sobre esse universo de possibilidades, quer seja para infecção dos computadores pessoais, quer para obtenção dos dados bancários, as probabilidades de sucesso são muito maiores.

Alie-se a isto, uma aparente impunidade proporcionada pelas deficiências na legislação brasileira. O que deve ficar claro para todos os clientes desse tipo de serviço é que, embora os bancos estejam trabalhando na melhoria das soluções disponibilizadas, cabe a cada um fazer sua parte, protegendo seu patrimônio da forma mais adequada. O conhecimento prévio sobre os riscos no ambiente de *internet* e a adoção de medidas básicas de segurança pode contribuir para a diminuição do número de ocorrências hoje registradas.

BIBLIOGRAFIA

[1] Analytic Hierarchy Process, disponível em http://www.expertchoice.com/markets/index.html#AHP. Acessado em 03/08/2007.

[2] ACORDO DA BASILÉIA I – Basel Committee On Banking Supervision. Core Principles For Effective Banking Supervision.pdf, abril 2006

[3] ACORDO DA BASILÉIA II – Basel Committee on Banking Supervision. International Convergence of Capital Measurement and Capital Standards.pdf, novembro2005.

[4] ACORDO DA BASILÉIA II – BASEL COMMITTEE ON BANKING SUPERVISION. International Convergence of Capital Measurement and Capital Standards.pdf Tradução livre – p.129.

[5] AICPA- CENTER For PUBLIC COMPANY AUDIT FIRMS, Summary of Sarbanes-Oxley Act of 2002, http://cpcaf.aicpa.org/Resources/Sarbanes+Oxley/Summary+of+the+Provisions+of+the+Sarbanes-Oxley+Act+of+2002.htm, □cessã acesso em 03.08.2007.

[6] BANCO BRADESCO – www.bradesco.com.br – diversas opções disponíveis após o login do cliente. Acessado em 15/03/2007

[7] BANCO CENTRAL DO BRASIL , Resolução 2554, http://www5.bcb.gov.br/normativos/detalhamentocorreio.asp?N=098186548&C=2554&ASS=RESOLUCAO+2.554. Acessado em 03.08.2007

[8] BANCO CENTRAL DO BRASIL , Resolução 3198, http://www5.bcb.gov.br/normativos/detalhamentocorreio.asp?N=104080599&C=3198&ASS=RESOLUCAO+3.198, último acesso em 03.08.2007

[9] BANCO CENTRAL DO BRASIL , Resolução 3380, http://www5.bcb.gov.br/normativos/detalhamentocorreio.asp?N=106196825&C=&ASS=RES. Acessado em 03.08.2007.

[10] BANCO DO BRASIL S.A. – www.bb.com.br – diversas opções disponíveis após o login do cliente. Acessado em 15/03/2007.

[11] BERNSTEIN, PETER L. Desafio aos Deuses: a fascinante história do risco. Rio de Janeiro, 1997, p.01.

[12] BRITISH BANKERS´ ASSOCIATION, http://www.bba.org.uk/bba/jsp/polopoly.jsp?d=146&a=568. Acessado em 03.08.2007.

[13] CALDEIRA, RENATA MARTINO e VIEIRA NETO, AMÉRICO CORDEIRO- Dissertação Autenticação De Usuário Em Serviços Web de Instituições Financeiras – Projeto Final de Graduação em Engenharia de Redes de Comunicação, UNB 2005.

[14] CERT – Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, http://www.cert.br/stats/incidentes/2006-jan-dec/total.html, último acesso em acessado em 03.08.2007

[15] COSTA, FERNANDO, Desafio aos Economistas, http://www.eco.unicamp.br/artigos/artigo49.htm, acessado em 03/08/2007.

[16] CUNHA, GILBERTO R. – O paradoxo de São Petersburgo. http://www.agrolink.com.br/colunistas/pg_detalhe_coluna.asp?Cod=1170,

acessado em 10/08/2006
[17] Dorofee, Andrey J., Walker, Julie A., Alberts, J.Christopher, Higuera, Ronald P., Murphy, Rochard L., Williams, Ray C. Continuous Risk Management Guidebook, SEI – Software Engineering Institute da Carnegie Mellon University.
[18] FDIC – FEDERAL DEPOSIT INSURANCE CORPORATION Authentication in an Electronic Banking Environment.pdf
[19] FDIC – FEDERAL DEPOSIT INSURANCE CORPORATION, Tips for Safe Banking Over the Internet. Disponível em: http://www.newyorkfed.org/education/addpub/safeinternet.pdf. Acessado em 03/08/2007
[20] FEBRABAN – Federação Brasileira de Bancos, *CIAB – 2006* – Apresentação sobre "Uso da Certificação Digital no Banco do Brasil S.A.", proferida pela Sra. Francimara Viotti em junho/2006.
[21] FEBRABAN – Federação Brasileira de Bancos, http://www.febraban.org.br/. Artigo "Bancarização". Artigo restrito aos bancos associados à federação. Disponível com o autor desta dissertação.
[22] FFIEC – Federal Financial Institutions Examination Council´s, *FFIEC*-authentication_guidance.pdf.
[23] FFIEC – Federal Financial Institutions Examination Council´s, http://www.ffiec.gov/ffiecinfobase/booklets/e_banking/ebanking_01_risks.html
[24] FFIEC – Federal Financial Institutions Examination Council´s, http://www.ffiec.gov/ffiecinfobase/booklets/e_banking/ebanking_00_intro_def.html. Acessado em 03/08/2007.
[25] FFIEC – Federal Financial Institutions Examination Council's, http://www.ffiec.gov/ffiecinfobase/booklets/e_banking/e_banking.pdf – IT Examination Handbook E-Banking – agosto 2003.
[26] Gartner Group – Conduct a SWOT Analysis to Shape Your Sourcing Practice, September 2004.
[27] Gartner Group – Artigo: HSBC Bank Brasil Turns to Back-End Fraud Detection to Curb Cybercrime.
[28] Gartner Group – Regulators Tell U.S. Banks to Adopt Stronger Risk-Based Authentication.pdf, Publication date: 27 October 2005.
[29] GARTNER GROUP – Publicação: State of the Art for Online Consumer Authentication.pdf
[30] GLOBAL MARKET INSITE, Online Banking Gaining Worldwide Momentum, Disponível em: http://www.gmi-mr.com/gmipoll/release.php?p=20051019. Acessado em: 01.03.2007
[31] GRIFFITHS DAVID, Risk Based Internal Auditing. Disponível em: http://www.internalaudit.biz/files/introduction/Internalauditv2_0_3.pdf.Acessado em 07/09/2006.
[32] GTAG – GLOBAL TECHNOLOGY AUDIT GUIDE, Publicação: Management of IT Auditing.pdf
[33] HOLTON, GLYN. Defining Risks – Financial Analysts Journal Volume 60 Number 6, page 22 (2004, November)
[34] IBGC – INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA, Governança Princípios IBGC , http://www.ibgc.org.br/ibConteudo.asp?IDArea=2. acessado em 03/08/2007.

[35] INSTITUTE Of CHARTERED ACCOUNTANTS In ENGLAND & WALES, Policy – Risk Management and Reporting, "Risk Management in Small and Medium Sized Enterprises.pdf. Disponível em http://www.icaew.com/index.cfm?route=120062. Acessado em 03/08/2007.
[36] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, Publicação ISO 17799.pdf
[37] INTENET SECURITY SYSTEMS, Disponível em https://gtoc.iss.net/issEn/delivery/gtoc/index.jsp. Acessado em 03/08/2007.
[38] ISO – International Organization For Standardization / IEC Guide 73 – Risk Management Standards page 03, Ferma – Federation of European Risk Management Associations, 2003
[39] IT Control Objectives for Sarbanes-Oxley, 2nd Edition
[40] Kawano, Carmen. http://revistagalileu.globo.com/Galileu/0,6993,ECT705269-2680,00.html. Acessado em 03/08/2007.
[41] KEYNES, JOHN MAYNARD. A Treatise on Probability. Londres, 1921.
[42] KNIGHT, FRANK. Risk, Uncertainty and Profit. New York, 1921.
[43] KNIGHT, KEVIN, Revista Security Review, março/abril de 2006 – páginas 8,9, 10 e 12
[44] LIVRO-TEXTO PARA O EXAME CISA, Estrutura de Controles Internos – COSO – Commitee of Sponsoring Organizations of the Treadway Commission – Comitê das Organizações Patrocinadoras da Treadway Commission.
[45] LOPES & ASSOCIADOS. O Novo Acordo de Capital da Basiléia, boletim Risk Bank, de 21/08/2002.
[46] LORENZONNI, PABLO. http://www.propus.com.br/articles/alt/1/1.html. Acessado em 03/12/2006.
[47] Módulo Security – http://www.modulo.com.br/index.jsp?page=3&catid=7&objid=4954&pagenumber=0&idiom=0, acessado em 03/12/2006.
[48] MÓDULO SECURITY, www.modulo.com.br – documento: "Ataques com phishing a computadores domésticos no Reino Unido crescem 800% em um ano". acessado em 29/10/2006.
[49] O'CONNOR J. J. e ROBERTSON E. F. http://www-history.mcs.st-andrews.ac.uk/Biographies/Bernoulli_Jacob.html. Acessado em 03/08/2007.
[50] PAMPLONA, EDSON DE OLIVEIRA. Avaliação Quantitativa de Cost Drivers pelo método AHP, http://www.iepg.unifei.edu.br/edson/download/Artavalahp.pdf. Acessado em 03.08.2007.
[51] Pareceres da Comissão de Constituição, Justiça e Cidadania e da Comissão de Educação sobre o Substitutivo de Projeto de Lei de autoria do senador Eduardo Azeredo, 2006.
[52] PEIXOTO, RODNEY De CASTRO, Módulo Security Magazine, 12 de abril de 2004.
[53] SAATY ,THOMAS. Apostila do Banco do Brasil sobre Analytic Hierarchy Process.
[54] SILVEIRA, ALEXANDRE DI MICELI Da, Governança Corporativa – Desempenho e Valor da Empresa no Brasil, Tese de Mestrado em Administração apresentada à Faculdade de Economia, Administração e Contabilidade, USP - Universidade de São Paulo, 2002

[55] SIMONIS, ADILSON. Em://www.ime.usp.br/~asimonis/probmagna.html. Acessado em 03.08.2007.
[56] SOPHOS, Security Information, http://www.sophos.com/security/. Acessado em 01/05/2007
[57] SOUZA, SILAS ROBERTO. Macroavaliação de Riscos em Auditoria Interna. Apostila do seminário de Formação de Auditores Internos da gerência de auditoria de sistemas do Banco do Brasil, junho 2006.
[58] SUÁREZ LILIANA ROJAS, Center for Global Development. Apresentação "O Futuro das Operações Bancárias: Perspectivas Globais e o Brasil", Brasília 28 de julho de 2007.
[59] THE INSTITUTE OF INTERNAL AUDITORS. Global Techonology Audit Guide BROCHURE_Mar10__1.pdf
[60] THE INSTITUTE OF INTERNAL AUDITORS. http://www.theiia.org/download.cfm?file=42122 – Putting COSO Theory into Practice," *Tone at the Top*, The Institute of Internal Auditors, November 2005 (PDF). Disponível em 03/08/2007.
[61] THE INSTITUTE OF INTERNAL AUDITORS. The Role of Internal Audit in Risk Management, Disponível em http://www.iia.org.uk/cms/IIA/uploads/-38c9a362-ed71ce5fa5--7770/PositionStatementRiskManagement.pdf. Acessado em 03/08/2007.
[62] Transações Bancárias e Automação. Disponível em: http://www.febraban.org.br/Arquivo/Servicos/Dadosdosetor/2006/item05.asp. Accessado em 01.03.2007. Área restrita – necessário senha de acesso. Disponível com o autor desta dissertação.
[63] U.S. GOVERNMENT PRINTING OFFICE, The text of the law http://www.access.gpo.gov/index.html. Acessao em 03/08/2007.
[64] Weihrich, H. (1982) The TOWS matrix: a tool for situational analysis, Journal of Long Range Planning, Vol. 15 Issue 2, pp.12-14.
[65] WIKIPEDIA. http://en.wikipedia.org/wiki/Law_of_large_numbers, acessado em 01/05/2007
[66] Guía para la realización del análisis del Riesgo medioambiental.pdf, editado pelo Ministério do Interior da Espanha; Norma de Gestão de Riscos, editada pela Federacion of European Risk Management Associantions; Auditoria Interna: Um Negócio Arriscado.pdf, David M Griffiths; Macroavaliação de Risco em Auditoria Interna, Silas Roberto de Souza; Specchio Silvia Reina Astorino Matriz de Riscos IBCB – Instituto Brasileiro de Ciência Bancária; Kaplan Robert S.; Norton David P. – A Estratégia em Ação, Editora Campus, 1997; Continuous Risk Management Guidebook, SEI – Software Engineering Institute
[67] The Internal Control System.pdf. Working Group set up by the AMF –Financial Markets Authority.

ANEXO I

Glossário sobre Gestão de Riscos

O gerenciamento de riscos é um processo que, mesmo de forma inconsciente, vem sendo executado pelas organizações, há algum tempo, como forma de maximizar as chances de alcançar os objetivos estratégicos definidos. Contudo, somente recentemente, tem surgido a necessidade de definir uma linguagem comum para a gestão de riscos.

Este glossário contém os termos mais usuais em se tratando da disciplina de gerir riscos, abordando também a definição de metodologias e a descrição dos principais regulamentos. Entretanto, não se destina a usuários iniciantes na busca de tutoriais sobre o assunto. O foco está centrado no fornecimento de informações concisas para aqueles já iniciados na disciplina. Assim, os leitores obterão um melhor uso deste documento como referência, após o estudo dos textos apresentados.

A

AHP – *Analytic Hierarchy Process*

> Metodologia voltada para atribuição de pesos para os mais diversos critérios, formulados para serem indicadores de matrizes de risco, e, assim, traduzir o grau de criticidade de um risco, em uma pontuação que varia entre 0 (zero) e 1 (um).

Ameaça (*Threat*)

> Evento ou circunstância que possa causar dano aos ativos de uma organização, como captura, destruição, alteração ou exposição de informações. Tipos de ameaças: erros operacionais, ataques maliciosos, fraude, roubo e falhas de aplicativos e equipamentos, dentre outros.

Amostragem (*Sampling*)

> Técnica estatística que se baseia não no universo de informações, mas nas amostras em quantidade suficiente para conclusão sobre o todo.

Análise S.W.O.T. (S.W.O.T. *Analysis*)

Técnica utilizada no planejamento estratégico das organizações, com objetivo de identificar os pontos fortes (*strenghts*), as vulnerabilidades (*weaknessess*), as oportunidades (*oportunities*) e as ameaças (*threats*), na busca de riscos que possam afligir a organização.

Apetite ao risco (*Appetite for risk*)

Nível de risco residual que os administradores consideram aceitável. Decisão de se expor mais ou menos aos riscos, em função da quantidade de controles instituídos.

C

COBIT (Control Objectives for Information and related Technology)

Modelo (*framework*) que descreve uma estrutura de controle para a área de tecnologia da informação. Identifica uma lista de objetivos de controle e um conjunto de diretrizes de auditoria. Descreve 04 domínios de atuação: Planejamento e Organização, Aquisição e Implementação, Entrega e Suporte e Monitoração.

Comitê de Basiléia (*Basel Comitee*)

Composto pelos representantes dos bancos centrais e das autoridades supervisoras dos principais países industrializados foi constituído em 1974. Os acordos firmados pelo Comitê são balizadores para a supervisão bancária mundial.

Controle corretivo (*Corrective Control*)

Controle projetado para corrigir erros, omissões, usos não autorizados e intrusões, após serem detectados, minimizando os impactos da ocorrência.

Controle detectivo *(Detective Control*)

Controle implementado para detectar e reportar as ocorrências de erros, omissões, uso não autorizado ou intrusões.

Controle interno (*Internal Control*)

Medida adotada para diminuição da exposição a riscos, pela prevenção ou redução da probabilidade de ocorrer o evento de risco, em detectar a ocorrência do evento indesejado e em minimizar o impacto da ocorrência. Qualquer medida de gestão de risco, com intuito de minimizar a probabilidade de ocorrência, minimizar o impacto ou transferir o risco para outra empresa. Os controles internos são desenvolvidos para auxiliar o atingimento dos objetivos das organizações, pela prevenção ou detecção e correção de eventos indesejados.

Controle Operacional *(Operacional Control*)

Controle relacionado às operações do dia-a-dia das organizações e que assegura o atingimento de seus objetivos.

Controle preventivo (*Preventive Control*)

Controle projetado para prevenir ou restringir a ocorrência de eventos indesejados, provendo os devidos ajustes. Esse controle atua de forma a evitar a ocorrência dos eventos indesejados.

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

Metodologia que define controles internos descreve seus componentes e fornece critérios para avaliar os sistemas de controle instituídos pelas organizações.

E

Exposição (*Exposure*)

Potencial resultado ou conseqüência adversa a ser considerado quando da avaliação dos controles internos instituídos. Um forte sistema de controles internos pode reduzir a exposição a riscos, mas raramente eliminá-la.

F

Fragilidade (*weakness*)

Vulnerabilidade identificada nos controles internos instituídos por uma organização, ou ausência de controles que possam contribuir para a minimização de um risco.

G

Gerenciamento de risco *(Risk Management*)

Processo de identificação dos riscos aos quais a empresa está exposta, sua probabilidade de ocorrência, bem como as medidas e os planos adotados para sua prevenção ou minimização.

Governança Corporativa (*Corporate Governance*)

Sistema pelo qual as organizações são dirigidas e controladas. Compreende as políticas, normas e procedimentos instituídos com o objetivo de otimizar o desempenho das empresas e facilitar o acesso ao capital. Governança Corporativa também inclui os relacionamentos entre todas as partes interessadas (*stakeholders*) e os objetivos instituídos para a organização. Entenda-se *stakeholders* como: acionistas, conselho de administração, conselho diretor, empregados, clientes, fornecedores, reguladores, sociedade em geral.

I

Impacto (*Impact*)

Perdas decorrentes da consecução de uma ameaça ao explorar uma vulnerabilidade existente. Exemplo: perdas financeiras, descumprimento de legislação, danos à imagem da organização, perda de confiança dos clientes, interrupção de operações, perda de dados de clientes etc.

M

Materialidade (*Materiality*)

Conceito de auditoria que representa a relevância ou importância de um determinado item ou assunto. Por exemplo, a detecção de falhas isoladas, dentro de uma grande

quantidade de operações, pode não ter materialidade suficiente para representar uma vulnerabilidade.

Matriz de risco (*Risk Matrix*)

Cruzamento de indicadores com propósito de classificar os riscos em mais críticos e menos críticos. O impacto e a probabilidade podem representar indicadores dentro de uma matriz de risco.

P

Ponto de Controle (*Point of control*)

Ponto ou local, dentro de um processo, considerado ideal pelos gestores para implementação de controles internos.

Probabilidade (*Probability*)

Possibilidade de ocorrência de um evento.

R

Risco (*Risk*)

Possibilidade de perda, ou grau de incerteza a respeito de um evento. Potencial de uma ameaça explorar uma vulnerabilidade causando perdas ou danos aos ativos de uma organização.

Risco de controle (*Control Risk*)

Risco de que uma falha possa ocorrer e que não seja prevenida ou detectada a tempo, pelo sistema de controles internos.

Risco inerente (*Inherent risk*)

Risco próprio do processo ou negócio. Risco de um erro ocorrer, supondo que não haja controles instituídos.

Risco Legal (*Legal Risk*)

Risco associado ao não atendimento a leis e regulamentos aos quais a organização se encontra submetida. Tem como impactos, sanções aplicadas pelos órgãos reguladores, que podem, dependendo do país, levar à desautorização para funcionamento das organizações.

Risco de Imagem (*Reputation Risk*)

Risco associado ao impacto negativo da opinião pública sobre uma organização, decorrente de envolvimento da empresa com operações ilícitas, danos ao meio ambiente, notícias sobre sua saúde financeira, falhas operacionais e de sistemas etc. As conseqüências do risco de imagem podem ser percebidas por: queda do valor das ações, perda de clientes, diminuição da quantidade de negócio realizada, dentre outras. O risco de imagem está presente por toda a organização e significa agir com preocupação no trato com clientes e com a sociedade.

Risco Operacional (*Operational Risk*)

Risco de perdas resultantes de inadequação ou falhas de processos internos, pessoas e sistemas, ou de eventos externos. Esta definição inclui os riscos decorrentes de não atendimento à legislação.

Risco remanescente ou residual (*Residual risk*)

Nível de conforto aceitável quanto à exposição ao risco, face à relação custos versus benefícios da implementação de controles adicionais. Está diretamente relacionado com o apetite de risco da organização.

S

Segurança dos dados (*Data security*)

Controles que buscam manter a confidencialidade, integridade e disponibilidade das informações.

SOX – Sarbanes Oxley

Lei aprovada pelo governo norte americano para coibir as fraudes contábeis, elevando a credibilidade das informações constantes nas demonstrações financeiras de empresas que operam no mercado financeiro americano. Assim, todas as empresas que transacionam suas ações na Bolsa de Valores de Nova Iorque (EUA) estão obrigadas a atenderem o disposto nessa Lei. A SOX descreve 11 títulos, ou seções, e foca principalmente a Responsabilidade Penal da Diretoria. As seções 302 e 404 são as mais discutidas. A 302 trata da responsabilidade pessoal dos Diretores Executivos e Diretores Financeiros, enquanto a 404 determina avaliação anual dos controles e procedimentos internos para fins de emissão do relatório financeiro.

U

Utilidade (*Utility*)

Motivação que rege o comportamento das pessoas, perante um risco, baseada em desejo, proveito ou satisfação.

V

Vulnerabilidade (*Vulnerability*)

Característica inerente a um processo, ou ativo organizacional que pode ser explorada por uma ameaça. Exemplos: treinamento insuficiente de usuários, ausência de funcionalidades de segurança, aplicativos não testados, transmissão de informações sem utilizar dispositivos de confidencialidade, uso de senhas fracas etc.

ANEXO II

Planilha gerencial para identificação, análise, planejamento e monitoração de riscos

IDENTIFICAÇÃO					ANÁLISE E PLANEJAMENTO					MONITORAMENTO E CONTROLE		
Risco Identificado	Categoria	Probabil.	Impacto	Severidade	Ação Preventiva	Ação Detectiva	Ação Corretiva	Indicadores de Risco	Providência	Responsável	Status	Controle

Categoria:
Risco Operacional, Legal, Imagem
Probabilidade: (1) Baixa; 2 (Média); 3 (Alta); (4) Muito Alta
Impacto: (1) Baixo; (2) Médio; (3) Alto; (4) Muito Alto
Severidade: Impacto x Probabilidade
Ação Preventiva: detectar problemas, mesmo potenciais, antes que esses ocorram
Ação Detectiva: revela e reporta a ocorrência de um erro, de uma omissão ou de ações maliciosas.
Ação Corretiva: minimizam o impacto de um fato consumado ou disparam a adoção de medidas corretivas para os problemas reportados pelas medidas detectivas
Indicadores de Risco: fatores capazes de identificar situações de risco além da desejada.
Providência: medidas alternativas de correção ou de contingência, para os casos oriundos dos indicadores de risco.
Status: situação em que se encontra o risco, podendo assumir valores como mitigado, controlado ou contingenciado.
Controle: Campo auxiliar para acompanhamento do planejamento. Exemplo: Mantido o Controle; Retirado o Controle