UNIVERSIDADE DE SÃO PAULO
FACULDADE DE ECONOMIA, ADMINISTRAÇÃO E CONTABILIDADE DE
RIBEIRÃO PRETO.
DEPARTAMENTO DE ADMINISTRAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO DAS ORGANIZAÇÕES

ROSSIMAR LAURA OLIVEIRA

Gestão de fraudes financeiras externas em bancos

Orientador: Prof. Dr. Alberto Borges Matias

RIBEIRÃO PRETO

2012

Prof. Dr. Joao Grandino Rodas
Reitor da Universidade de São Paulo

Prof. Dr. Sigismundo Bialoskorski Neto
Diretor da Faculdade de Economia, Administração e Contabilidade de Ribeirão Preto

Prof. Dra. Sonia Valle Walter Borges de Oliveira
Chefe do Departamento de Administração

ROSSIMAR LAURA OLIVEIRA

Gestão de fraudes financeiras externas em bancos

Dissertação apresentada ao Programa de Pós-Graduação em Administração de Organizações da Faculdade de Economia, Administração e Contabilidade de Ribeirão Preto da Universidade de São Paulo, para obtenção do título de Mestre em Ciências. Versão Corrigida. A original encontra-se disponível na FEA-RP/USP.

Orientador: Prof. Dr. Alberto Borges Matias

RIBEIRÃO PRETO

2012

Autorizo a reprodução e divulgação total ou parcial deste trabalho, por qualquer meio convencional ou eletrônico, para fins de estudo e pesquisa, desde que citada a fonte.

Oliveira, Rossimar Laura

Gestão de Fraudes Financeiras Externas em Bancos. Ribeirão Preto, 2012.

127f.:il.;30 cm

Dissertação de Mestrado apresentada à Faculdade de Economia, Administração e Contabilidade de Ribeirão Preto da Universidade de São Paulo.

Orientador: Matias, Alberto Borges

1. Fraude Financeira. 2. Gestão de Fraude. 3. Prevenção e Detecção de Fraudes. 4. Bancos.

FOLHA DE APROVAÇÃO

Nome: Rossimar Laura Oliveira

Título: Gestão de Fraudes Financeiras Externas em Bancos.

Dissertação apresentada ao Programa de Pós-Graduação em Administração de Organizações da Faculdade de Economia, Administração e Contabilidade de Ribeirão Preto da Universidade de São Paulo como requisito para obtenção do título de Mestre em Ciências.

Aprovada em ____/____/____

Banca Examinadora

Prof. Dr. Alberto Borges Matias

Instituição: FEA-RP/USP

Julgamento: _____ Assinatura: _____

Prof. Dr. Ernesto Fernando Rodrigues Vicente

Instituição: CCN/ UFSC

Julgamento: _____ Assinatura: _____

Profa. Dra. Sonia Valle Walter Borges de Oliveira

Instituição: FEA-RP/USP

Julgamento: _____ Assinatura: _____

DEDICATÓRIA

Aos meus pais.

Aos meus irmãos.

Ao Paulo.

AGRADECIMENTOS

Agradeço ao meu orientador Prof. Alberto, por me acolher na FEARP, pela oportunidade de pertencer ao mundo da pesquisa e por apontar saídas para as minhas angústias acadêmicas.

Aos meus entrevistados, colaboradores de bancos e associações, pela disponibilidade, pelas informações prestadas e esclarecimento de dúvidas.

Agradeço ao Prof. Dr. Ernesto Fernando Vicente e à Prof. Dra. Sonia Valle W. Borges de Oliveira pelas preciosas orientações durante o exame de qualificação.

Agradeço a todos os professores da FEA-RP que conheci durante as disciplinas, principalmente ao Prof. Dr. Tabajara Pimenta e a Prof. Dra Elizabeth Krauter.

Agradeço aos meus colegas de mestrado, em especial, à minha amiga Luna e aos pós-graduandos da casa 13 pela companhia e por toda ajuda.

Agradeço aos meus familiares por entenderem a minha ausência durante muito tempo e ao Paulo por ser o grande incentivador deste projeto.

Uma das lições mais tristes da História é a seguinte: Se formos enganados durante muito tempo, temos tendência a rejeitar qualquer prova de fraude. Deixamos de estar interessados em descobrir a verdade. A fraude apanhou-nos. É demasiado doloroso reconhecer, nem que seja para nós mesmos, que fomos levados à certa. Uma vez que damos a um charlatão poder sobre nós mesmos, quase nunca o recuperamos. Por conseguinte, as velhas fraudes têm tendência a persistir, ao mesmo tempo que surgem outras novas.

Carl Sagan em *“O Mundo Assombrado pelos Demônios: A Ciência Vista como uma Vela no Escuro”*

RESUMO

OLIVEIRA, R.L. **Gestão de Fraudes Financeiras Externas em Bancos**. 2012. 127 f. Dissertação (Mestrado em Administração de Organizações) – Faculdade de Economia, Administração e Contabilidade de Ribeirão Preto, Universidade de São Paulo, Ribeirão Preto, 2012.

Segundo relatório da auditoria KPMG, 69% das empresas admitiram ser vítimas de algum tipo de fraude. Em 2010, no setor bancário foram perdidos aproximadamente R\$ 1,5 bilhões devido às fraudes financeiras cometidas em clientes considerando apenas as fraudes documentais e as perdas com fraudes bancárias eletrônicas superaram os 900 milhões neste mesmo ano. Os tipos de fraudes cometidas foram diversos, dentre eles a fraude durante a abertura de contas, cheques clonados, falsificação de documentos, alterações de códigos de barras e clonagem de cartões. A fraude é um problema frequente nas organizações e bastante discutido no mercado, porém verificou-se a existência de uma lacuna teórica quando se trata de gestão da fraude externa. O objetivo do trabalho foi a estruturação de um quadro conceitual para a Gestão da Fraude Financeira e a sua comparação com a prática. Este é um estudo qualitativo exploratório e foi realizado por meio da análise baseada na Teoria Fundamentada definindo categorias a partir da literatura disponível e a sua comparação com entrevistas feitas em um banco de varejo brasileiro e uma associação de instituições financeiras, além dos artigos jornalísticos. Com relação à utilização dos resultados esta é uma pesquisa aplicada já que seu resultado pode, além de contribuir para a discussão teórica, ser aplicada em qualquer organização interessada em gerir a fraude financeira. Os resultados da elaboração do quadro conceitual mostram que a gestão da fraude financeira externa tem quatro fases: a Contínua, a Prevenção, Detecção e a Reação e as categorias definidas estão inseridas nelas. Quanto à comparação da teoria com a prática, nem todos os aspectos verificados na literatura puderam ser encontrados nos relatos das entrevistas e nos artigos jornalísticos analisados.

PALAVRAS-CHAVE

Fraude Financeira. Gestão de Fraude. Prevenção e Detecção de Fraudes. Bancos.

ABSTRACT

OLIVEIRA, RL External Financial Fraud Management in Banks. 2012. 127 f. Dissertation (Master in Management of Organizations) - School of Economics, Administration and Accounting of Ribeirão Preto, University of São Paulo, Ribeirão Preto, 2012.

According to KPMG audit report, 69% of companies admitted being victims of some kind of fraud. In 2010, the banking sector have lost approximately R\$ 1.5 billion due to financial fraud perpetrated on customers considering only documentary fraud and the electronic banking fraud losses exceeded R\$ 900 million in the same year. The types of fraud were many, including fraud during account opening, cloned checks, forgery, alteration barcode and card cloning. Fraud is a common problem in organizations and widely discussed in the market, however it was found that there is a theoretical gap when it comes to managing external fraud. The objective of this research was to structure a conceptual framework for the Management of Fraud and its comparison with the practice. This is an exploratory qualitative study and was conducted through analysis based on Grounded Theory defining categories from the available literature and interviews with comparison to a bank and an association of financial institutions, in addition to news articles. Regarding the use of results is an applied research its result can also contribute to the theoretical discussion, and be applied to any organization interested in managing financial fraud. The results of the development of the conceptual framework shows that the management of external financial fraud has four phases: Continuous, Prevention, Detection and Reaction and the defined categories are located in them. Regarding the comparison of theory with practice, not all aspects verified in the literature could be found in the reports of interviews and newspaper articles analyzed.

KEYWORDS

Fraud. Fraud Management. Prevention and Fraud Detection. Banks

1. ÍNDICE DE ILUSTRAÇÕES

<i>Figura 1 - Localização do problema de pesquisa</i>	15
<i>Figura 2 - Delitos por computador</i>	41
<i>Figura 3 - Elementos para uma estratégia integrada de combate à fraude</i>	51
<i>Figura 4 - Componentes de um programa anti-fraude</i>	64
<i>Figura 5 - Codificação Axial</i>	69
<i>Figura 6 - Processo</i>	71
<i>Figura 7 - Representação gráfica do Framework da Gestão da Fraude</i>	111
<i>Figura 8 - O Modelo Condicional</i>	117

<i>Gráfico 1 - Tipos de Fraude por indústria</i>	16
<i>Gráfico 2 - Tipos de fraude por indústria.</i>	17
<i>Gráfico 3 - Incidentes Reportados.</i>	18
<i>Gráfico 4 - Despesas e Investimentos em TI</i>	19
<i>Gráfico 5 - Fraude Reportada por indústria</i>	31
<i>Gráfico 6 - Maior ameaça do cybercrime</i>	40
<i>Gráfico 7- Perfil dos fraudadores externos.</i>	45
<i>Gráfico 8 - Recursos interpostos contra fraudadores externos</i>	57
<i>Gráfico 9 - Métodos de Detecção de fraudes</i>	62

<i>Quadro 1 - Ameaças e possibilidades de fraude</i>	24
<i>Quadro 2 - Risco Operacional e Fraude.</i>	27
<i>Quadro 3 - Estratégias dos fraudadores</i>	44
<i>Quadro 4 - Técnicas de Identificação</i>	54
<i>Quadro 5 - Categorias da Fase "Contínua"</i>	75
<i>Quadro 6 - Categorias da Fase "Prevenção"</i>	76
<i>Quadro 7 - Categorias da Fase "Detecção"</i>	76
<i>Quadro 8 - Quadro Resumo Fases e Categorias</i>	77
<i>Quadro 9 - Framework Teórico.</i>	86
<i>Quadro 10 - Identificação Prática do Framework Teórico</i>	107
<i>Quadro 11 - Esquema para Gestão da Fraude Financeira</i>	113

<i>Tabela 1 - Fraudes Documentais Externas em 2010.</i>	35
<i>Tabela 2 - Fontes de Informações</i>	67

SUMÁRIO

1. INTRODUÇÃO E JUSTIFICATIVA	13
1.1 <i>PROBLEMA DA PESQUISA</i>	<i>14</i>
1.2 <i>OBJETIVO GERAL E OBJETIVOS ESPECÍFICOS.....</i>	<i>20</i>
2. FUNDAMENTAÇÃO TEÓRICA	21
2.1 <i>RISCO OPERACIONAL</i>	<i>21</i>
2.1.1 PESSOAS.....	23
2.1.2 PROCESSOS	24
2.1.3 TECNOLOGIA	25
2.1.4 EVENTOS EXTERNOS.....	26
2.2 <i>FRAUDES FINANCEIRAS</i>	<i>27</i>
2.2.1 HISTÓRICO DA FRAUDE	31
2.2.2 FRAUDES DOCUMENTAIS.....	33
2.2.2 FRAUDES ELETRÔNICAS E PELA INTERNET	36
2.2.3 ÓTICA PSICOLÓGICA DAS FRAUDES	42
2.2.4 ÓTICA LEGAL DAS FRAUDES	46
2.3 <i>GESTÃO DA FRAUDE FINANCEIRA</i>	<i>49</i>
2.3.1 PREVENÇÃO DA FRAUDE FINANCEIRA	51
2.3.2 DETECÇÃO DA FRAUDE FINANCEIRA	58
3. MÉTODO	65
3.1 <i>TIPO DE ESTUDO</i>	<i>65</i>
3.2 <i>MÉTODO DE COLETA.....</i>	<i>66</i>
3.3 <i>PROPOSIÇÕES</i>	<i>67</i>
3.4 <i>FONTES DE INFORMAÇÕES</i>	<i>67</i>
3.5 <i>ANÁLISE DAS INFORMAÇÕES</i>	<i>68</i>
4. RESULTADOS	73
4.1 <i>O FRAMEWORK TEÓRICO.....</i>	<i>73</i>
4.1.1 As fases	73
4.1.2 As categorias	74
4.1.3 As subcategorias	77
4.2 <i>IDENTIFICAÇÃO PRÁTICA</i>	<i>87</i>
4.2.1 As entrevistas	87
4.2.2 Artigos jornalísticos.....	94
5. DISCUSSÃO.....	109
6. CONSIDERAÇÕES FINAIS	115
7. LIMITAÇÕES E SUGESTÕES DE PESQUISAS FUTURAS	117
REFERÊNCIAS BIBLIOGRÁFICAS.....	119
APENDICE A.....	125

1. INTRODUÇÃO E JUSTIFICATIVA

A fraude financeira pode ser definida, de acordo com Mendes, Lins e Neves (1997), como o ato de agir de má-fé com a finalidade de lesar financeiramente outro agente; este outro agente podendo ser uma pessoa, empresa, organização ou governo. A fraude financeira pode ser cometida por uma única pessoa ou por um grupo, porém visando sempre a vantagem financeira sobre outrem. Segundo os autores, existem basicamente duas maneiras de a fraude financeira acontecer: mediante a alteração de dados e o desvio de numerário.

Para estudar a fraude é importante diferenciá-la do erro. Erros são perdas não intencionais ou omissões de valores ou informações financeiras. Erros podem envolver enganos de compilação ou no processamento de dados quando os relatórios financeiros são preparados, estimações incompletas da contabilidade devido à superestimação ou má interpretação de fatos ou enganos na aplicação dos princípios contábeis relatados para valores, classificação, forma de apresentação ou transparência. Por outro lado a fraude é definida como um ato intencional que resulta em perda material. (GOLDEN; SKALAK; CLAYTON, 2006).

Em seu trabalho, Clementino (2006) afirma que não é possível existir uma sociedade onde nenhum indivíduo cometa a fraude por motivações morais e éticas. Isto significa que é impossível eliminar a existência da fraude. Segundo Bergamini (2005) com o progressivo conhecimento de que os riscos são multidimensionais percebeu-se que o problema não era somente interno, surgindo a necessidade do controle externo.

Para Coque (2006; p. 5) a fraude externa pode ser entendida como as ocorrências de "perdas devido a atos com intenção de fraudar, apropriar-se indevidamente ou burlar a lei, praticados por um terceiro indivíduo". Neste caso o fraudador busca apenas o benefício pessoal e não o benefício para a instituição como pode ocorrer na fraude interna, além de não ter vínculo empregatício com a instituição. Para Fich e Shihivdasanib (2007) as fraudes financeiras são sintomáticas e são resultados de enormes deficiências na Governança Corporativa.

As empresas de auditoria são importantes pesquisadoras do tema fraude, sejam internas ou externas. Segundo relatório de pesquisa da auditoria KPMG (2009), 69% das empresas admitiram ser vítimas de algum tipo de fraude. Na pesquisa bianual feita pela PWC (2009) constatou-se que no Brasil em 2009 houve aumento de 27% nos casos de fraude financeira comparado ao ano anterior. De acordo com levantamento feito com 16 bancos nacionais e internacionais com operações no Brasil foram perdidos no ano de 2010 aproximadamente R\$ 1,5 bilhões devido às fraudes financeiras documentais cometidas por terceiros contras os clientes destes bancos. As perdas com fraudes bancárias eletrônicas superaram os 900 milhões neste mesmo ano (SOBRAL; SOBRAL,2012).¹

Mas o que justifica este estudo acadêmico? Porque este tema interessa às organizações?

De acordo com a KPMG (2009), para evitar fraudes financeiras muitas empresas adotam a máxima restrição às informações críticas e até mesmo restrição a ambientes. Os resultados da pesquisa Unisys Security Index (2011) mostram que 79% dos entrevistados no mundo todo afirmam que deixariam de se relacionar com uma organização que não garantisse a segurança de seus dados e 55% tomariam uma ação legal contra a empresa. De acordo com a mesma pesquisa o custo médio anual para uma organização mitigar apenas o crime virtual é de U\$\$ 5,9 milhões.

1.1 PROBLEMA DA PESQUISA

O assunto fraude poderia aparecer de diferentes maneiras. A figura 1 identifica algumas das principais fraudes, quais as suas respectivas origens e quem pode ser prejudicado por elas. A fraude pode acontecer no setor público, onde recursos públicos são desviados ou mal utilizados, como os esquemas de corrupção, favorecimento ilegal, propinas etc. As fraudes podem ser corporativas, onde representantes de companhias alteram informações financeiras projetando uma imagem irreal de sua situação, como os casos *Enron*, *WorldCom* (BRICKEY, 2003),

¹ SOBRAL, C. E. M e SOBRAL R. M. Os crimes Cibernéticos no Brasil: O uso da tecnologia para combate dos delitos em massa, 2012, (não publicado)

Banco Santos, Banco Panamericano etc. As fraudes financeiras podem acontecer em todos os setores, caracterizadas pelo desvio ou abuso de ativos das empresas ou de seus clientes.

A fraude tem três possíveis origens: a interna, feita por funcionários; a externa, feita por terceiros (HANSEN et al. 2005) e a mista, onde estão envolvidos agentes internos e externos. Como toda fraude tem uma vítima é possível definir os prejudicados em cada uma das possibilidades. Em casos de fraude no Setor Público toda a sociedade perde, visto que são recursos públicos envolvidos e que deixarão de ser revertidos em benefícios aos contribuintes. Na fraude Corporativa a sociedade poderia ser inserida como prejudicada, pois todos os *stakeholders* perdem com a falência de uma empresa, mas principalmente os funcionários perdem seus empregos, os clientes deixam de receber e ter disponível o produto ou serviço oferecido e os fornecedores perdem negócios futuros. Sobre a fraude Financeira os principais prejudicados são a empresa que tem perda de valores pecuniários e de imagem e seus clientes que podem ter perdas em valores pecuniários e desgaste emocional ao lidarem com os procedimentos de esclarecimento dos fatos. Isso pode ser visto na figura 1.

Fonte: Elaborado pela autora.

Figura 1 - Localização do problema de pesquisa

O foco deste trabalho foi analisar a Fraude Financeira de origem externa no setor bancário.

Existe uma razão para escolher o setor bancário para estudar a fraude. De acordo com os gráficos 1 e 2 é possível perceber que entre diversos setores, apenas as empresas de serviços financeiros e seguradoras sofreram um percentual maior de fraude externa que interna, ou seja, a fraude externa é mais frequente que a fraude interna nos bancos. No ano de 2009, 73% das fraudes em bancos foram externas e em 2011 este número foi 60% (PWC, 2011). Uma possível explicação poderia ser o fato de o setor bancário ser altamente regulado, o que pode trazer maior controle interno que nas demais indústrias.

Fonte: PWC (2011).

Gráfico 1 - Tipos de Fraude - por atividade econômica - % de fraude reportada em 2011.

Fonte: PWC (2009).

Gráfico 2 - Tipos de Fraude - por atividade econômica - % de fraude reportada em 2009.

A fraude financeira externa é uma preocupação antiga no sistema bancário. A Federação dos Bancos Brasileiros (FEBRABAN) mantém uma biblioteca onde é possível encontrar arquivos de Encontros e Congressos de Discussão sobre fraude desde a década de 1970.

Para tentar conter o avanço da fraude foi criada pela FEBRABAN a Diretoria Setorial de Prevenção às Fraudes, há aproximadamente 15 anos. Nela estão representantes de 32 bancos, responsáveis por 90% do total das transações ocorridas no Brasil.

Dentro desta Diretoria Setorial de Prevenção a Fraudes existem três subcomissões: Subcomissão de Prevenção às Fraudes Documentais que trata, por exemplo, de clonagem de cheques, falsa identidade, abertura de conta corrente com documento falso; a Subcomissão de Prevenção às Fraudes Eletrônicas que trata, por exemplo, clonagem de cartões de débito e crédito, nacionais e internacionais e a subcomissão de Prevenção às Fraudes pela Internet que trata, por exemplo, de transações realizadas pela internet e *Call Center*, invasão de contas, roubo de senhas.

A FEBRABAN alimenta um banco de dados, de acesso restrito, com os registros das perdas consolidando as informações dos bancos. Este banco de dados existe desde 2010 para fraudes documentais e desde 2007 para as eletrônicas e pela internet.

Em uma pesquisa feita com 16 bancos verificou-se que as perdas apenas com fraude documental em 2010 foram de aproximadamente R\$ 1,5 bilhão e segundo o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT) foram reportados aproximadamente 130 mil incidentes de fraude eletrônica no período entre janeiro e dezembro de 2010.

No gráfico 3 é possível verificar que os casos de incidentes reportados ao CERT tem seguido uma linha de tendência ascendente, apesar de em 2010 ter havido uma queda.

Fonte: CERT (2011).

Gráfico 3 - Incidentes Reportados.

Tentando conter esta expansão os bancos investem cada vez mais em tecnologia para garantir maior segurança às informações de seus clientes e também com a finalidade de reduzir suas perdas (LAU, 2006). De acordo com os dados da FEBRABAN as perdas com fraude realizadas eletronicamente somaram R\$ 685 milhões entre janeiro e junho de 2011. Este número é 36% maior que no primeiro

semestre do ano passado. De acordo com a pesquisa da FEBRABAN (2011) as despesas e investimentos em tecnologia das instituições brasileiras cresceram anualmente entre 2007 a 2010, 11%, 4% e 5% entre 2009 e 2010, atingindo os R\$ 22 bilhões em investimentos em TI, conforme visto no gráfico 04. Em todos os períodos os investimentos em *hardware* consomem mais recursos que os demais, mas em 2010 o crescimento dos investimentos em Telecom e Infra também foram significativos.

Fonte: FEBRABAN (2011)

Gráfico 4 - Despesas e Investimentos em TI(R\$ milhões)

Diante destas informações apresenta-se o problema de pesquisa:

O que é e como é feita a gestão da fraude financeira externa nos bancos?

1.2 OBJETIVO GERAL E OBJETIVOS ESPECÍFICOS

Para alcançar o objetivo geral de estruturar um *framework* sobre o que é e como é feita a gestão da fraude financeira externa em bancos, foi necessário investigar algumas questões essenciais, que são:

- ✓ A partir do levantamento bibliográfico, identificar as fases da gestão da fraude, assim como os aspectos relacionados a cada uma delas, que neste trabalho serão chamadas categorias.
- ✓ Analisar entrevistas e reportagens sobre o tema fraude financeira externa em bancos para confirmar se os aspectos relacionados à gestão da fraude, identificadas no framework teórico podem ser confirmados na prática.

2. FUNDAMENTAÇÃO TEÓRICA

A fundamentação teórica deste trabalho foi feita em três temas: a) Risco Operacional: Pessoas, Processos, Tecnologia e Eventos Externos. b) Fraudes Financeiras: Histórico, Fraudes Documentais, Eletrônicas e pela Internet; Óticas Gerencial, Psicológica e Legal. c) Gestão da Fraude Financeira: Prevenção e Detecção.

2.1 RISCO OPERACIONAL

A gestão de riscos financeiros diz respeito a quatro tipos de risco de perda para a empresa, sendo eles o risco de mercado, de crédito, de liquidez e o operacional. Risco de mercado é o risco de perda referente a movimentos não esperados dos preços dos títulos financeiros ou dos ativos, incluindo flutuação do valor do patrimônio, taxa de juros, commodities ou moeda estrangeira. O risco de crédito é o risco da perda pelo não recebimento e risco de liquidez é o risco de perda por não conseguir honrar pagamentos em determinado período. (JARROW, 2007).

O Comitê da Basiléia (2001, p.94) definiu risco operacional como "o risco de perda direta ou indireta, resultante de inadequações ou falhas de processos internos, pessoas e sistemas, ou de eventos externos". Assim como foi definido por Brown, Goetzmann *et al.*(2008) como as perdas causadas por problemas com pessoas, processos, eventos externos e tecnologia. Mais especificamente estão incluídos os riscos de falhas da operação interna, controle e sistemas contábeis; falhas do *compliance* e sistemas de auditoria interna; falhas do pessoal de supervisão de sistemas, ou seja, fraude e má-conduta.

No Brasil, a Resolução do Conselho Monetário Nacional (CMN) nº 3.380/06 definiu o risco operacional como "a possibilidade de ocorrência de perdas resultantes de falha, inadequação ou deficiência de processos internos, sistemas e pessoas, ou de eventos externos". Porém, nesta definição foi incluído também o risco legal, considerando as possibilidades de deficiências em contratos firmados, sanções por descumprimentos de dispositivos legais e indenizações a terceiros. Desta forma, são

considerados pelo CMN eventos de risco operacional: fraudes externas, fraudes internas, falhas em processos, falhas em sistemas, danos ao patrimônio físico, falhas nos negócios, demandas trabalhistas e interrupção dos negócios.

Jarrow (2007) faz uma caracterização econômica e matemática do risco operacional, originada na literatura de risco de crédito e finanças corporativas. Para ele são dois tipos de risco operacional: O risco de perda devido ao custo da agência, incluindo a fraude e má distribuição e o risco de perda devido à tecnologia de operação da firma. Estes dois tipos de risco operacional geram processos de perdas com características econômicas diferentes. Uma é baseada na produção/ processo de troca/sistema de geração de receita, o outro é baseado em incentivos gerenciais. Já Allen e Bali (2007) tratam o Risco Operacional apenas como o risco de perda causado por falhas nos processos operacionais ou nos sistemas que dão suporte a eles, incluindo qualquer adversidade que afete a reputação, aplicação legal de contratos e reivindicações.

Relacionado ao gerenciamento do Risco Operacional, Chapple et al.(2007) fazem uma revisão que envolve uma série de métodos e perspectivas para chegar ao propósito de reduzir a média de perdas e evitar perdas catastróficas. Dentre eles a aplicação das recomendações da auditoria, reorganização da linha de negócio, análise através de grandes perdas já sofridas, planejamento contínuo no negócio e a reação rápida.

A partir destas definições podemos analisar separadamente os principais aspectos que podem estar envolvidos em perdas por risco operacional: pessoas, processos, tecnologia e eventos externos.

2.1.1 PESSOAS

As pessoas podem causar perdas a uma empresa, mas estas pessoas não são apenas os funcionários. Podem ser causadas pelos funcionários ou com participação indireta destes, com ou sem intenção ou também perdas devido ao relacionamento com clientes, acionistas ou terceiros. Alguns exemplos de perdas causadas por pessoas são o desvio de recursos de contas contábeis, contas correntes ou investimentos; alteração do favorecido do crédito; acidentes envolvendo clientes ou terceiros nas dependências da instituição; fraude interna; fraude externa, etc. (FEBRABAN, 2006).

Para Figueiredo (2001) o risco humano ou risco de pessoas é possibilidade de perdas em função de falhas humanas por situações diversas, inclusive, falta de valores éticos. Os erros não intencionais podem causar prejuízos por erros na execução de tarefas em função da não definição de procedimentos, de processos distorcidos, falta de segregação de tarefas, volume de serviço, ou ainda, falta de qualificação de pessoas, incluindo capacidade, habilidade e perfil. Por fim, a possibilidade de perdas por fraude, que é em decorrência de comportamentos fraudulentos, como adulteração de controles, desvio/subtração de valores, aceitação de "incentivos" para realização de negócios etc.

De acordo com Cordeiro (1977) os efeitos do comportamento do homem podem ser controlados e evitados. As pessoas podem trazer ameaças segundo a intenção e a motivação. Quando estas ameaças são intencionais elas são deliberadas ou premeditadas, elas podem também ser fortuitas geradas pelo descuido, negligência ou pela ignorância. As ameaças segundo a motivação em geral são em benefício pecuniário próprio direto ou através de terceiros, mas também podem aparecer sem um benefício particular, nestes casos estão os ataques por vingança ou represália. Cordeiro (1977) cruzou estes aspectos e obteve como resultado a gama mais frequente de delitos apresentados no quadro 1. De acordo com o quadro 1 o risco que é fortuito, não traz benefício para a pessoa responsável e em geral são chamados acidentes. Já as ações intencionais na maioria trazem benefício para o responsável, como a espionagem, fraude e desfalque. Apenas casos de sabotagem

por vingança ou represália podem não trazer benefício pecuniário para o responsável, apesar de ser intencional.

	INTENCIONAL	FORTUITO
COM BENEFÍCIO	Espionagem	Acidente (se não se acusa o beneficiário se torna apropriação indébita)
COM BENEFÍCIO	Fraude	
COM BENEFÍCIO	Desfalque	
SEM BENEFÍCIO	Sabotagem por vingança	Acidente
SEM BENEFÍCIO	Sabotagem por represália	

Fonte: Cordeiro (1977)

Quadro 1 - Ameaças e possibilidades de fraude

2.1.2 PROCESSOS

O risco operacional em processos também é uma possível fonte de perdas para as empresas. Nele estão incluídos quaisquer erros de registro, processamento ou liquidação de transações, de contas de clientes, de negócios diários e falhas na apresentação de relatórios. São exemplos de perdas por risco operacional em processos no caso dos bancos a necessidade de indenizar ou ressarcir um cliente por causa de uma transação indevida ou liquidação de um cheque que ele tenha sustado ou que tenha alguma irregularidade, o pagamento de uma multa por perda de prazo para recolhimento de impostos e contribuições, a apresentação de uma falha no cadastro de clientes, a perda de prazo para ingresso de defesa de uma ação recebida, a perda do prazo de um recurso judicial ou homologações trabalhistas, indenizações decorrentes de processos trabalhistas, etc. (FEBRABAN, 2006).

Para Figueiredo (2001) este tipo de risco acontece devido a fragilidades ocorridas nos processos. As causas destas fragilidades podem ser uma regulamentação interna ineficiência ou falha, pode também não haver documentado os

procedimentos corretos e a política da empresa; o risco em processos pode ser devido a erros no desenho dos processos e à falta de controle interno. É possível considerar como um risco de perda em processos, falhas devido ao uso de modelos incorretos, que não representam a realidade como deveriam ou que estão inconsistentes com a realidade. Este risco de modelagem pode ser mais facilmente percebido em análise de projetos de investimentos, rentabilidade e a própria medição de risco. Outro risco de perda em processos é o risco de transação, ou seja, uma transação pode ser executada erroneamente em qualquer das suas fases, este risco fica mais claro em transações de operações e produtos complexos. Nas transações o risco pode ser de um erro no registro na operação de financiamento ou a falta de um registro, poderia ser a liquidação de operação apesar da divergência de saldos, uma operação feita com documentos incompletos, etc. Outro risco em processos é o risco de conformidade, refere-se à possibilidade da empresa sofrer alguma sanção dos órgãos reguladores se for verificada uma inobservância da legislação vigente, da mesma forma no caso dos bancos, a não observância das normas operacionais e limites que o Banco Central determina. Finalmente, o último risco em processos é o risco de controle, que são as perdas causadas pela falta de controle dos processos internos e falta de segurança. Um exemplo do risco devido à falta de controle nos processos em bancos poderia ser a falha da trava automática em liberações de crédito, esta situação poderia fazer com que volumes maiores fossem depositados pelos operadores.

2.1.3 TECNOLOGIA

As perdas por risco operacional relacionadas à tecnologia ou sistemas são as perdas decorrentes da falha destes sistemas, da indisponibilidade de infraestrutura e recursos de TI que interrompem os negócios. A falta de manutenção, a incapacidade de atendimento da demanda, a inadequação do sistema aos processos, falhas de processamento, a indisponibilidade de sistemas, a falta da criação de backups ou planos de contingência são exemplos de risco de operacional em tecnologia. Em

todos estes riscos estão incluídos os equipamentos, os softwares, aplicativos ou infraestrutura para comunicação e energia (FEBRABAN, 2006).

Para Figueiredo (2001) o risco tecnológico é qualquer situação onde os sistemas não cumprem sua finalidade de prover informações para quem toma decisão, com total confiabilidade e em tempo real. O risco tecnológico também é o risco das atividades serem interrompidas devido a problemas nos sistemas de processamento de dados, relacionados à energia e comunicação. Segundo o autor, também podem ser considerados riscos tecnológicos os erros de programação, má uso do software ou se o software não é adequado para aquela empresa; se a empresa utiliza mais que um sistema e eles não se integram, assim como sistemas vulneráveis a invasões de pessoas não autorizadas ou sistemas obsoletos.

Os equipamentos podem ser considerados parte do risco tecnológico. As falhas podem acontecer no hardware, ficando indisponível o processamento e transmissão dos dados. O disco rígido pode ser comprometido por vírus e se perderem informações importantes se não existir um backup. Os bancos têm muito de suas operações automatizadas, desta forma, estão expostos a riscos de falhas de seus sistemas, seja de relacionamento com clientes, seja interno, gerando um risco de confiabilidade de informações e continuidade de seus negócios (FIGUEIREDO, 2001).

2.1.4 EVENTOS EXTERNOS

Os bancos e todas as demais empresas são capazes de ter programas de prevenção de riscos operacionais e planos de contingência, principalmente relacionados ao controle de pessoas, processos e tecnologia. O mesmo não pode ser dito em relação aos riscos de eventos externos, pois apesar de todos os planos de contingência possíveis ainda é necessário considerar a variável acaso. Uma série de eventos externos pode causar perdas por danos ao patrimônio e ou danos ao ativo; estas perdas podem interromper o negócio por um dia ou inviabilizar a continuidade de suas operações. Os eventos naturais como tempestades, inundações, explosões, furacões e movimentos sísmicos são incontroláveis e

inevitáveis, apesar de ser cada vez mais precisa sua previsão. Outros eventos externos, não relacionados à natureza, também podem causar perdas, como por exemplo, atentados terroristas, sabotagens, guerras, tumultos, arrombamento, vandalismo, incêndios, desabamentos, acidentes viários. Para todos estes riscos de eventos externos as instituições podem ter planos de contingência, mas prejuízos são inevitáveis quando eles ocorrem (CORDEIRO, 1977; FEBRABAN, 2006).

Em síntese, o quadro 2 mostra as possibilidades de fraude considerando os Riscos Operacionais:

Risco Operacional	Possibilidade de Fraude?	Exemplos de fraude
Pessoas	Sim	Falsa identidade de clientes (externo). Roubo de ativos (interno)
Processos	Sim	O processo não inclui a necessidade de validação das informações prestadas (externo). Os pagamentos e recebimentos são feitos pela mesma pessoa (interno)
Tecnologia	Sim	Sistema vulnerável (externo). O programador deixa um comando para apagar ou capturar informações dos clientes (interna).
Eventos Externos	Não	-

Fonte: Elaborado pela autora.

Quadro 2 - Risco Operacional e Fraude.

2.2 FRAUDES FINANCEIRAS

A fraude é um risco operacional, desta forma deve ser gerida. Para Zagaris e MacDonald (1992) são crimes que permanecem em grande parte na tecnologia, que oferece meios mais sofisticados, os processos tortuosos favorecem o surgimento até mesmo de grupos organizados de fraudadores.

Existem muitos tipos de fraudes e de se caracterizar a fraude. Em uma visão de auditoria foram conceituadas por Golden, Skalak e Clayton (2006) as fraudes por funcionários ou desapropriação de ativos e a fraude em demonstrações financeiras. A fraude por funcionários pode envolver o roubo de dinheiro ou estoque. O roubo de ativos é o tipo de fraude mais comum. Pode ser por meio de esquemas com os pagamentos, reembolsos de despesas, muitas vezes existe a participação de dois ou mais funcionários. Nesta categoria podem ser incluídos os funcionários que agem como cúmplices de pessoas de fora da empresa para fraudá-la. As fraudes em demonstrações financeiras são caracterizadas pela omissão ou alteração intencional de relatórios financeiros, ou seja, a manipulação, alteração ou falsificação de demonstrações financeiras ou documentos que dão suporte a elas.

Já Mendes, Lins e Neves (1997) classificaram as fraudes como sabotagem, roubo de informações ou propriedade, venda de serviço não autorizado e a fraude financeira. Para a sabotagem foram definidos dois tipos de ocorrência, a quebra de equipamento e deleção de dados. De maneira geral quem pratica a sabotagem tem a intenção de obter algum benefício, por isso se distingue do vandalismo. A sabotagem seria o ato de danificação ou destruição de equipamentos, dados e informações. O outro tipo de fraude seria a venda de serviço não autorizado e o roubo de informação ou propriedade. O roubo de informações pode ser para uso próprio ou de terceiros e por fim a fraude financeira.

Ngai et al. (2011) classificaram a fraude financeira em quatro grandes categorias: Fraude Bancária, Fraude de Seguros, Fraude de Títulos e Commodities e Outras fraudes relatadas. A Fraude Bancária seria qualquer ação consciente ou tentativa de esquema para fraudar a instituição financeira ou para obter dinheiro, créditos, ativos, valores mobiliários ou outros bens de propriedade, custódia ou controle da instituição financeira por meio de falsas pretensões ou promessas.

A fraude financeira de Seguros pode ocorrer em muitos pontos do processo de seguro e podem ser cometidos pelos clientes, funcionários da seguradora, corretoras, beneficiários de seguro saúde etc. A fraude de Títulos e Commodities pode ser exemplificada pelo esquema Ponzi, ou Pirâmide Financeira. Definida também como qualquer roubo ou manipulação do mercado de valores mobiliários e fraude eletrônica (NGAI et al., 2011).

Finalizando as quatro categorias (NGAI et al., 2011) descrevem as “Outras Fraudes” como a falsificação de informação financeira, dirigentes empresariais que conseguem vantagens para si próprios e obstrução da justiça tentando ocultar os tipos de conduta citadas acima.

Para fins deste trabalho iremos utilizar as definições anteriormente apresentadas de fraude financeira externa documental, eletrônica e pela internet utilizadas pela FEBRABAN, visto que o trabalho busca falar o problema da fraude financeira externa nos bancos.

Gottschalk (2010) argumenta que a fraude acontece em decorrência de três condições fundamentais, conhecido como o “Triângulo da Fraude”: os incentivos, as oportunidades e a racionalização. Os incentivos podem ser muitas vezes oferecidos aos funcionários como um ambiente de muita pressão. As oportunidades são as circunstâncias onde os funcionários ou terceiros se veem com a facilidade para cometer uma fraude e por fim a racionalização que seria o pensamento e ação desonestos.

Todas as fraudes acontecem em decorrência deste Triângulo. Os incentivos são percebidos em casos de necessidade do fraudador. Os fatores de risco de fraude considerando os incentivos e pressão são circunstâncias que ameaçam a estabilidade financeira ou lucratividade do negócio, extrema pressão de investidores e credores sobre os gestores para alcance das metas, ameaça à riqueza pessoal do gestor relacionada à performance do negócio, problemas financeiros pessoais que possam motivar o roubo de ativos, adversidades de relacionamento entre a entidade e um ou mais empregados, os quais podem estar ressentidos ou sem lealdade (GOLDEN; SKALAK; CLAYTON, 2006).

A oportunidade está relacionada a alguns fatores de risco e o fraudador acredita que não será punido. Elas são criadas principalmente pela falta de controles ou controles inadequados, falta de supervisão ou inadequada segregação de funções. Algumas vezes o tipo, tamanho ou estrutura do negócio pode facilitar a fraude (GOLDEN; SKALAK; CLAYTON, 2006).

Na racionalização a efetivação da fraude depende de fatores e de características pessoais de quem a comete. Algumas pessoas são mais desonestas que outras e

alguns fatores externos podem leva-las a fraudar uma empresa. Estes fatores externos podem ser uma insegurança diante de uma redução de quadro da empresa ou devido ao clima de ressentimento no ambiente de trabalho. Um agravante da fraude feita pela racionalização é o histórico de ação dos gestores do topo diante de uma fraude do passado, se nada foi feito ou não foi dado o tratamento adequado os demais vão acreditar que podem se beneficiar da mesma forma. (GOLDEN; SKALAK; CLAYTON, 2006).

Já de acordo com Parodi (2008) as fraudes acontecem pela junção de três fatores que não são iguais ao Triângulo da Fraude (incentivos, oportunidade e racionalização), mas que possuem algumas semelhanças: a) A existência de golpistas motivados, b) a disponibilidade de vítimas adequadas e vulneráveis e a c) ausência de controles eficazes. Estes fraudadores podem ser motivados por diversas situações como as desigualdades sociais, a ineficiência das leis, falta de fiscalização ou um sistema financeiro evoluído. As vítimas em geral tem pouca informação, são ingênuas ou muitas vezes são vítimas devido à própria ganância. A falta de controles existe porque o problema não é tratado como prioritário, assim existe pouco treinamento das autoridades, falta de coordenação das ações contra os fraudadores e falta ou não clareza de leis contra estes crimes.

Krambia-Kapardis (2010) confirma parte da posição de Parodi (2008) ao argumentar que alguns fatores são os facilitadores da ocorrência de fraude nas empresas, dentre eles os mais comuns são os fracos controles internos, responsáveis por cerca de 50% das ocorrências de fraude, fatores externos como percepção do governo, economia do país, falhas no sistema bancário, policia ineficiente, etc., responsáveis por 26% das ocorrências; o tipo de negócio, conluio, substituição de gerência, incompetência e até mesmo ignorância.

No Brasil, desde a crise de 2008, tem sido intensificada a discussão a respeito do tema de fraudes financeiras. Conforme pode ser visto no gráfico 5, 44% das empresas de serviços financeiros entrevistadas (PWC, 2009; 2011) afirmaram serem vítimas de fraude nestes anos, mas ela teve início muitos anos antes, como será visto na próxima seção.

Fonte: Adaptado de PWC (2011).

Gráfico 5 - Fraude Reportada por atividade econômica (% individual)

2.2.1 HISTÓRICO DA FRAUDE

O “Triângulo da Fraude” foi criado pelo sociólogo e criminologista americano Donald Cressey² (1953 *apud* PIMENTA, 2009), formulando a hipótese que:

² CRESSEY, Donald R., “Other People’s Money: A Study in the Social Psychology of Embezzlement”, The Free Press, Glencoe, Illinois, 1953.

As pessoas, em quem se confia, tornam-se violadoras dessa confiança quando imaginam que têm um problema financeiro impossível de partilhar e que acreditam poder ser secretamente resolvido, através da violação da confiança financeira, sendo capazes de aplicar à sua conduta, naquela situação, justificações que lhes permitam ajustar o conceito, que têm de si próprios, de pessoas de confiança de utilizadores dos fundos ou propriedade que lhes foram confiados (1953).

Em seu trabalho, Robb (1993) descreve que a fraude financeira já acontecia na Inglaterra de 1850. Com as crises financeiras de 1855, 1866 e o colapso do Banco da Cidade de Glasgow em 1878 de forma semelhante, revelou a evidência da conduta criminosa no setor bancário, de falsificação da contabilidade, elementos fictícios nos balanços e práticas de gestão imperfeita.

As fraudes documentais foram as primeiras, mas as eletrônicas não são tão recentes. Já tem quase cinquenta anos de acontecido o primeiro caso de uma fraude através de um computador. De acordo com Cordeiro (1977) este fato aconteceu nos EUA no ano de 1966 quando um jovem programador de um banco quis esconder os saldos em descoberto da sua própria conta. Ele introduziu uma modificação no programa do banco de maneira que o saldo negativo da sua conta fosse ignorada. São chamadas “bombas lógicas” quando é feita uma instrução que só funciona em determinadas condições do sistema, o programa pode ser executado apenas por um período ou evento específico. Outro exemplo de bomba lógica, além deste para o programa ignorar o saldo negativo de determinada conta seria um programa que instrísse o computador a apagar todos os arquivos de pessoal de uma empresa (CLAB, 1982; LEGAL PRACTITIONER, 2012). O primeiro caso de roubo de um programa da memória do computador a partir de um terminal remoto ocorreu em 1971. Este foi o primeiro caso em que se emitiu uma ordem judicial com o fim de obter provas da memória de um computador (CORDEIRO, 1977).

Todos estes casos são uma ilustração de um problema que não é novo e parece cada vez mais de difícil solução. Os bancos e seus clientes são vítimas e estão em constante ameaça por meio ou com auxílio dos sistemas de processamento eletrônico de dados. A vulnerabilidade da atividade bancária cresce em proporção direta ao volume de dados que se deve processar. Esta vulnerabilidade é em parte resultado da massificação dos processos feitos por máquinas, que não tem a

capacidade crítica e intelectual das pessoas que faziam o trabalho (CORDEIRO, 1977).

2.2.2 FRAUDES DOCUMENTAIS

A identificação é uma necessidade social e chegamos ao extremo de converter homens em simples fichas. Uma necessidade que se impõe devido ao progresso tecnológico e aos subterfúgios de que certas pessoas se valem para fraudar diariamente o comércio, a indústria, os bancos e os cidadãos em geral. Identificação é a ação de identificar a personalidade física da pessoa a partir da primeira informação, ou seja, a antropométrica, fotográfica, fonética, grafológica, documental, datiloscopia, etc. (VELEZ ANGEL, 1985).

Segundo Velez Angel (1985) os métodos costumeiros de identificação pecam por ineficácia como a questão da assinatura e do documento de identidade. Existem muitos falsificadores de assinaturas que são calígrafos peritos, ou seja, o legítimo usuário teria dificuldade em falar que não é dele. Dependendo da qualidade da falsificação pode demorar dois dias para identificação, desta forma o funcionário do banco não teria condições de em poucos segundos decidir pelo não pagamento de um cheque porque a assinatura não é verdadeira (VELEZ ANGEL, 1985).

Os sistemas de falsificação podem ser a imitação livre ou assimilação gráfica, que consiste na repetição para assimilar as características gerais e as simulações. Na simulação o usuário legítimo deforma a própria assinatura. Este pode ser um cliente que tem sua conta e suas movimentações normais e repentinamente nega a autorização de determinado pagamento e avisa que foi roubado. A abertura de conta com documentos falsos é muito comum nas instituições bancárias e difícil de chegar ao autor já que foi antes de tudo um erro de identificação de pessoas cometido pelo funcionário do banco. O fraudador pode usar documentos falsos de uma pessoa que tenha boas referências que são confirmadas pelo telefone. No relacionamento entre grandes empresas e bancos é comum o envio das assinaturas autorizadas que são fotograficamente reduzidas para caber em algumas folhas. A redução de assinatura não é uma prática conveniente, pois não é fácil fazer uma comparação

entre assinaturas originais em tamanho original, fica ainda mais difícil comparar com uma cópia de tamanho reduzido (VELEZ ANGEL, 1985).

Existe possibilidade de fraude nas cartas de alteração de endereço. Um suposto cliente pode chegar ao banco com uma carta notificando a mudança de endereço e telefone. A carta é aceita e as alterações feitas. A partir daí os funcionários ligam para confirmar determinado pagamento, mas estão falando com o fraudador, que confirma o aceite dos cheques, ou de um novo talão, etc. O ideal é que estas cartas sejam pessoalmente verificadas por um funcionário que vá até o local confirmar as alterações. (VELEZ ANGEL, 1985)

As fraudes documentais foram divididas da seguinte forma pela FEBRABAN: Fraude no processo de abertura de conta corrente com documentos falsos; Cheques clonados; Falsificação e adulteração de cheques; Desvio da finalidade de pagamento; Ordem de pagamento com cheque (golpe); TED e DOC com cartas falsas; adulteração/ substituição do código de barras de bloquitos de cobrança; fraude em CDC; fraude em financiamento de veículos e fraude em crédito consignado, conforme será visto em mais detalhes na seção posterior.

2.2.2.1 ÓTICA GERENCIAL DA FRAUDE DOCUMENTAL

As principais fraudes documentais podem ser separadas em seis grandes grupos: Fraude na Abertura de Conta; Cheques Clonados/Falsificados e Adulterados; Fraude em TEDs, DOCs, Ordens de Pagamento e Bloquitos de Cobrança; Fraude no Crédito Direto ao Consumidor; Fraude no Crédito Consignado e Fraude no Financiamento de Veículos. A tabela 1 resume os principais tipos de fraude documentais em bancos, sua quantidade levantada no ano de 2010, o valor unitário médio e o valor total em milhões de acordo com pesquisa realizada com 16 bancos atuantes no Brasil. Analisando a tabela 1 é possível perceber que as fraudes documentais representaram uma perda de R\$1,5 bi em 2010³ para os bancos que participaram desta pesquisa em um número total de aproximadamente 825 mil

³ Dados não publicados (Comunicação pessoal).

casos. Dentre estas fraudes a de maior impacto é a linha dos cheques. Na linha dos cheques foram considerados os clonados que representam 80% do valor total perdido e 88% do total de casos de fraude. Outra linha que se destaca é a fraude relacionada ao financiamento de veículos, onde em aproximadamente 3800 casos foram perdidos R\$ 63 milhões.

Ainda de acordo com os dados desta pesquisa foi possível verificar que o valor médio unitário por caso de fraude é de R\$ 1.713,42 e a fraude com financiamentos de veículos tem um valor médio unitário de cerca da R\$ 16.744,48.

A fraude que possui o maior valor unitário médio foi a fraude por desvio de finalidade de pagamento do cheque, incluída na linha “Cheques”. Este desvio de finalidade acontece principalmente com empresas que fazem cheques para pagamentos de suas obrigações e os funcionários encarregados dos pagamentos vendem estes cheques para quadrilhas. No mesmo dia este cheque é depositado em contas abertas com documentos falsos ou de “laranjas”. Assim que o cheque é compensado o dinheiro é sacado. Para o funcionário que vende o cheque eles fazem autenticações e carimbos de pagamentos falsos nos boletos e comprovantes, assim a empresa não consegue perceber na hora, apenas muito tempo depois quando aparecem as cobranças ou processos de não recolhimento de impostos. Poderia acontecer também do encarregado pagar contas próprias com o cheque e entregar uma autenticação falsificada na empresa.

Tabela 1 - Fraudes Documentais Externas em 2010.

Fraudes Documentais	Valor em milhões de R\$	Qtde.	Valor p/unidade
Abertura de conta	R\$ 33,85	8303	R\$ 4.077,09
Cheques			
Clonados/Adulterados/Falsificados	R\$ 1.248,04	795144	R\$ 1569,58
Fraude em TEDs, DOCs, Bloquetos, OP.	R\$ 32,55	3893	R\$ 8360,18
CDC	R\$ 24,41	10317	R\$ 2.366,20
Consignado	R\$ 10,57	3120	R\$ 3.387,13
Veículos	R\$ 63,39	3786	R\$ 16.744,48

Fonte: Pesquisa com bancos atuantes no Brasil

Estas são as principais fraudes documentais, porém existem outras e as possibilidades são muitas. Cordeiro (1977) relatou o caso de um jovem que gravou com tinta magnética o número de sua conta nos formulários de depósito e distribuiu nos caixas da agência bancária. Os clientes usaram os formulários para efetuar seus depósitos durante todo o dia e o jovem tirou o dinheiro no dia seguinte tomando rumo desconhecido.

Tudo o que foi visto até agora esteve focado mais nas fraudes documentais. A opção de discutir separadamente as fraudes documentais das eletrônicas e pela Internet foi devido ao fato de apesar de representar perdas consideráveis, as fraudes documentais acontecem caso a caso, já a fraude eletrônica e pela internet tem a possibilidade de um ataque em massa e por isso tem recebido atenção especial dos gestores de fraudes.

2.2.2 FRAUDES ELETRÔNICAS E PELA INTERNET

As fraudes eletrônicas cometidas por terceiros em bancos são as que envolvem clonagem e adulteração de cartões bancários fraudes por qualquer meio e as fraudes pela internet são as fraudes onde a internet foi o principal meio para que ela acontecesse, como o roubo de senhas para violação de contas bancárias, numeração de cartões ou dados dos clientes, em outras palavras, a fraude eletrônica e pela internet visam violar contas e cartões bancários.

Nos cartões bancários existe uma série de possibilidades de fraudes, desde a duplicação da faixa magnética (fraude eletrônicas) até o bloqueio, no computador (fraude pela internet), das listas de cartões de crédito roubados ou perdidos (VELEZ ANGEL, 1985).

De acordo com a PWC (2011) Cyber crime é um crime econômico cometido usando o computador e internet. Incluindo distribuição de vírus, download arquivos ilegais, *phishing*, *pharming* e roubo de informações pessoais, por exemplo, roubo de

dados bancários. Somente pode ser chamado de cybercrime se um computador, ou computadores e a internet têm um papel central no crime, e não um acessório.

Considerando América Latina e Caribe os países mais afetadas pela fraude em cartões de crédito são Brasil, México e Caribe. Estes três somam cerca de 80% da fraude Visa na região. As principais economias, Brasil e México, foram identificados para a iniciativa de controle de riscos internacionais da Visa (GINEL, 1997). Sobre os tipos de fraude em cartões a perda, roubo e falsificação são a maior parte, sendo a falsificação 35% do total. A falsificação na América Latina merece atenção, pois nas outras regiões este número não passa de 20%.

Não será possível prosseguir sem o esclarecimento de alguns conceitos que são tratados como tipos de ataques, ou cybercrimes. As definições são técnicas, utilizadas no mercado. Sobre estes tipos de ataque Almonte (1997) lista alguns deles:

Phishing: é uma tentativa de confundir as pessoas para que forneçam suas informações confidenciais, como o número de CPF e senhas. Geralmente, essas tentativas utilizam e-mails ou mensagens instantâneas aparentemente legítimas, combinados com websites falsos, para fazer solicitações fraudulentas de informações (SYMANTEC NORTON, 2006).

Pharming: é uma tentativa de enganar os usuários da Internet roubando o nome de domínio ou a URL de um website e redirecionando seus visitantes para um website falso, pelo qual são feitas solicitações fraudulentas de informações. (SYMANTEC NORTON, 2006)

Password sniffing: O processo de capturar ativamente pacotes de informações de uma rede selecionada. A espionagem obtém todo o tráfego da rede, independente do endereço para onde os pacotes estejam endereçados. Trata-se de um método de recolher senhas monitorando os pacotes de dados no tráfego de uma rede para tirar informações que podem interessar a alguém. São softwares que realizam esta atividade automaticamente, eles podem ser comprados ou programadores podem fazer seu próprio software. Isto não significa que quem o usa sempre tem más intenções, porém pode ser uma ameaça. Qualquer senha digitada na rede está vulnerável ao *sniffing* (SYMANTEC NORTON, 2012).

Masquerading: Trata-se de uma técnica para tradução de endereços, ele permite que uma rede ou um host com IP que não existe se comunique com a internet através de um servidor válido, que pode traduzir ou mascarar este IP inválido com o IP válido do servidor que está sendo utilizado. (LINUX, 2012; COMPTECHDOC, 2012)

Eavesdropping: Significa que uma comunicação está sendo interceptada, não somente pela internet, mas rádio, telefone ou qualquer transmissão privada. Uma forma de evitar o *eavesdropping* é a criptografia da mensagem. (DIGITRO, 2012)

Man-in-the-middle: Muito parecido com o *Eavesdropping*. No “homem no meio” existe a interceptação dos dados trocados, por exemplo, entre um cliente e o banco pela internet. Neste caso, além de interceptados, estes dados poderão ser registrados, bloqueados e alterados (SECURITY, 2012).

IP spoofing: Uma técnica usada por um invasor para ganhar o acesso não autorizado à rede a um sistema de computador ou a uma rede forjando credenciais conhecidas da rede. O *spoofing* de IP é um método comum usado por invasores para ganhar acesso não autorizado a sistemas de computador ou à rede. Trata-se da troca do IP original por outro, um IP se passa por outro. Por meio do *IP Spoofing* o fraudador pode tirar proveito de hosts confiáveis e entrar em máquinas onde não é exigido senha. (PENTA UFRGS, 2012; SYMANTEC NORTON, 2012).

Data didling: Trata-se da mudança dos dados. Esta mudança pode acontecer antes, durante ou depois da entrada destes dados no sistema. Por exemplo, antes da entrada dos dados no sistema os documentos poderiam ser falsificados ou alterados ou a troca de discos e fitas válidos por outros modificados. (LEGAL PRACTITIONER, 2012)

Denial of service: São ataques de negação de serviço, ou seja, o fraudador utiliza um computador para tirar de operação outro computador ou servidor conectado à internet. Este tipo de ataque pode acontecer de diferentes maneiras, dentre elas a sobrecarga no processamento de dados, a geração de grande tráfego de dados para uma rede ou tirar o provedor de funcionamento. Todos estes ataques vão impedir que o usuário consiga usar o servido, deixando a rede indisponível (CERT, 2006).

Social engineering: A engenharia social não está apenas relacionada ao ambiente de internet, mas também está nele. Neste caso o fraudador usa suas habilidades verbais para enganar e convencer a vítima, tendo acesso facilitado a diversas informações confidenciais. Nas empresas ele também pode se fazer de funcionário e pegar informações que os demais por descuido podem ter deixado sem a proteção necessária (LEGAL PRACTITIONER, 2012).

Spyware: Trata-se de um programa invasor. Ele entra no computador sem autorização do usuário e fica oculto fazendo mudanças, gravando informações ou deixando o computador extremamente lento (TECNET, 2012)

As fraudes em cartões também tem seu vocabulário próprio como, por exemplo, o *Skimming* que é a captura não autorizada e transferência de dados de pagamento para outra fonte, para fins fraudulentos (PCISECURITY, 2009). A fraude em cartões pode acontecer por meio do comprometimento em massa de dados de cartões, pela clonagem no cartão reimpresso ou o correspondente pode fazer lavagem de cupons. Uma vulnerabilidade dos cartões é a tarja magnética que pode ser facilmente copiada, pois seus dados são estáticos (PCISECURITYSTANDARDS, 2010).

Quando a fraude é pela internet a maior ameaça está do lado de fora da empresa. De acordo com o gráfico 6, 46% das mais de 3000 empresas respondentes da pesquisa da PWC (2011) afirmaram que a maior ameaça do cybercrime são os fraudadores externos. Os próximos tópicos vão apresentar mais informações sobre estes tipos de fraude e fraudadores.

Fonte: Adaptado de PWC (2011).

Gráfico 6 - Maior ameaça do *cybercrime*

2.2.2.1 ÓTICA GERENCIAL DA FRAUDE ELETRÔNICA E PELA INTERNET

Algumas perdas podem ser intencionais ou não. No caso seguinte, relatado por Cordeiro (1977) poderia ser uma fraude, mas foi negligência dos responsáveis pelo local. Certo banco estava preocupado em atrair os jovens da cidade e convidou um grupo de escoteiros para visitar suas instalações de processamento de dados. Lamentavelmente um dos meninos levava em sua bolsa um ímã que causou danos irreparáveis nos arquivos de cintas magnéticas. Este exemplo relatado por Cordeiro há 35 anos mostra como uma fraude pode ser confundida com erro/negligência ou vice-versa, os gestores precisam estar preparados para apuração e prevenção de episódios como este.

Uma fraude comum é a mudança de dados antes ou durante o processamento, feita por qualquer pessoa com acesso aos processos de criar, gravar, transportar, codificar, examinar, verificar ou converter as informações introduzidas. A frequência das fraudes via computação eletrônica subiu junto com a automação bancária para o público e porque internamente mais pessoas estão tendo acesso a fazer alterações em sistemas. (CLAB, 1982).

Alguns outros casos de funcionários fraudando clientes foram descritos por Cordeiro (1977). Ele relata o caso de certo programador que observou que o cálculo de juros que se fazia para as contas de aplicações era habitualmente truncado do último centésimo. Ou seja, calculavam-se juros de 2,3333333 e se creditavam 2,33 desprezando o resto. Diante desta oportunidade o programador fez com que a parte restante fosse automaticamente depositada em sua conta pessoal. Esta ação do programador foi frustrada pela auditoria do banco que observou grandes pagamentos feitos por ele, mas não viam os depósitos correspondentes. Neste tipo de fraude geralmente os donos não reclamam, o que é uma vantagem para o fraudador. As aplicações são contas de pouca movimentação como a poupança ou contas feitas para não serem movimentadas, como as que os pais procuram fazer para suas crianças. Existem também possibilidades de entrar em sistemas através de “janelas clandestinas” ou portas que os programadores experientes podem utilizá-las para intercalar códigos adicionais que realizam funções não autorizadas, como pode ser visto na figura 2 (CLAB, 1982).

Fonte: Phillip Weights & Associates *apud* CLAB, 1982.

Figura 2 - Delitos por computador

Quando um *cybercrime* ocorre, especialistas devem determinar o ponto de fraqueza do sistema e implementar medidas para que esta brecha não seja atacada

novamente. Devem-se levantar quais informações ou registros foram comprometidos e procurar identificar os fraudadores. Contadores podem quantificar as perdas, que podem ser somadas com os custos para reparar, perdas de produtividade, imagem, etc. (GOLDEN; SKALAK; CLAYTON, 2006).

Geralmente estes ataques acontecem devido a servidores e firewalls mal configurados, erros de programação, servidores mal protegidos ou más políticas de gestão de senhas, que facilitam o ataque dos *crackers* (este termo é utilizado para descrever as pessoas que usam seus conhecimentos em informática para quebrar um sistema de segurança, ou seja, são hackers, mas que praticam ações ilegais que podem prejudicar terceiros); que podem facilitar também a ação dos *sniffers*, programas que farejam dados em uma rede. Em geral são usados por administradores de rede para identificarem pacotes estranhos, mas pessoas com má índole podem usá-los para descobrir senhas ou arquivos confidenciais (SYMANTEC NORTON, 2012) ou de engenheiros sociais e usuários com propensão à fraude (ALMONTE, 1997).

Até o momento é possível perceber que os fraudadores se valem de muita ousadia e criatividade nos seus ataques, mas será que existe um padrão psicológico para os fraudadores?

2.2.3 ÓTICA PSICOLÓGICA DAS FRAUDES

Muitas fraudes começam pequenas e tornam-se grandes. Pequenos furtos como longas ligações pessoais ou de longa-distância até levar suprimentos do trabalho para sua casa. Um primeiro pensamento racional deste tipo de fraudador é que esta situação é temporária, ninguém vai saber e nada vai acontecer ou pensam que não é fraude, se, por exemplo, pegar este mês e devolver no seguinte. Outro pensamento possível é achar que o gestor não se importa, que não tem um monitoramento sério dos controles internos, não sabe corrigir as deficiências dos controles e não pune este tipo de comportamento. O fraudador também pode pensar que merece, pois merecia uma promoção e não teve, pois tem um salário menor que

o mercado paga, que a empresa não tem lealdade aos funcionários e que provavelmente vai ser demitido em breve, então a fraude é apenas uma compensação por todos os benefícios que a empresa eliminou. (GOLDEN; SKALAK; CLAYTON, 2006). No caso das fraudes internas o fraudador é mais comum a partir de dois anos na empresa, isto porque ele está mais confiante, conhece bem os processos e pode explorar suas falhas (KPMG, 2009)

Chegou-se finalmente a um determinado funcionário daquele banco que ostentando padrão de vida muito acima do que lhe permitiam os vencimentos bancários, foi alvo de fundadas suspeitas de participação na trama. Interrogado, acabou confessando sua responsabilidade e denunciou os demais componentes da quadrilha, todos presos e processados. (BANCO DO BRASIL, 1980, p.162).

Dois fatores devem ser considerados para análise da psicologia e personalidade do fraudador: as qualidades biológicas do indivíduo, as quais variam amplamente influenciando o comportamento e as qualidades sociais que são derivadas do meio e podem moldar como os indivíduos lidam com as outras pessoas. (GOLDEN; SKALAK; CLAYTON, 2006).

Parodi (2008) faz um levantamento sobre os artifícios mais usados pelos fraudadores, como por exemplo, ganhar a confiança das outras pessoas por meio da reciprocidade, semelhança e simpatia. Nestes casos o fraudador pode se passar por uma pessoa muito prestativa e amiga. Outro artifício poderia ser pela intimidação ou pela inclusão de alguém com credibilidade no esquema sem que ele saiba. Todos eles podem ser acompanhados no quadro 3.

ESTRATÉGIA	DESCRIÇÃO
Reciprocidade	O fraudador se apresentará como muito prestativo e pronto a ajudar e assim pode ser mais difícil receber um "não" seu.
Escassez	Argumentos utilizados para pressionar vítimas: Oportunidade por tempo muito limitado ou que tem algum prazo a ser respeitado, limites de vagas, de produtos em promoção.
Autoridade	Forma de intimidação. Fraudadores podem alegar serem ligados a órgãos ou entidades públicas que lhe confeririam poder, ou se apresentam com cargos "importantes".

Fixação em fantasias	O fraudador se aproveita da propensão humana a subestimar a probabilidade de eventos adversos, perdendo a capacidade de duvidar de um fantástico prêmio.
Prova social	O fraudador alega que o que está sendo proposto já foi feito por diversas pessoas/empresas.
Semelhança e simpatia	O fraudador busca muitas informações sobre a vítima, criando um sentimento de semelhança e amizade.
Terceirização de credibilidade	Consiste no fraudador convencer primeiro uma pessoa com credibilidade, em quem a vítima confie, sem aplicar o golpe nele para que depois o apresente.
Autenticação por associação	Consiste no uso de um documento ou informação falsa juntamente com outros verdadeiros

Fonte: Parodi (2008) com adaptações da autora

Quadro 3 - Estratégias dos fraudadores

Ainda de acordo com Parodi (2008) existe um perfil dos fraudadores do comércio e crédito direto ao consumidor. Em geral, dentre outras características, são pessoas bem vestidas e procuram produtos fáceis de revender. Oferecem-se para levar o bem o mais rápido possível, demonstram nervosismo e dificultam a conferência dos documentos de identificação, inclusive sugerindo falar os números e não entregar o documento.

Almonte (1997) afirma que os fraudadores virtuais podem ser concorrentes de pouca ética, violadores de informações, punks cibernéticos, terroristas cibernéticos, organismos de inteligência, vírus ou os empregados (ALMONTE, 1997). De acordo com o gráfico 7 (PWC, 2011) é possível perceber que para 45% das empresas que responderam a pesquisa no ano de 2009 os fraudadores eram seus clientes e 23% outras partes terceiras. Já no ano de 2011 para 35% das empresas os fraudadores externos eram clientes, 21% outras partes terceiras e aumentou muito o número de empresas que responderam que não sabiam quem eram os fraudadores, de 2% para 17%.

Fonte: PWC (2011).

Gráfico 7- Perfil dos fraudadores externos (% reportado).

Existem dois tipos de fraudadores, o eventual e o definitivo. O eventual está em uma situação complicada e tenta conseguir dinheiro onde puder e o definitivo está convencido que sua conduta não está errada. Uma característica dos fraudadores é a de exercer domínio intelectual, usando chantagem emocional e intelectual. No caso dos fraudadores definitivos eles nunca reconhecem o crime, acreditam que se foram pegos é porque não fizeram alguma coisa certa. Foi relatado um caso de fraude onde durante o julgamento o réu ficou fazendo anotações de como melhorar seu esquema para a próxima vez (VALORECONOMICO, 2012).

Quando alguém consegue obter alguma vantagem por meio de fraude é caracterizado um crime. Saber quem ataca ou de onde vem o ataque (se virtual) à empresa é importante para que se procure mitigar os danos, seja com melhores controles ou com apoio das leis.

2.2.4 ÓTICA LEGAL DAS FRAUDES

Falsidade Ideológica é a omissão de conteúdo ou inserção de declaração falsa em um documento público ou privado. Se a forma do documento for forjada será falsidade material (PARODI, 2008). Como vimos anteriormente a fraude financeira pode ser cometida internamente e externamente e a lei as enxerga de maneira diferente. Para casos onde a fraude ocorre internamente, feita pela gestão trata-se de gestão fraudulenta ou temerária e para casos onde foi feito por terceiros trata-se de estelionato.

A gestão fraudulenta e temerária de instituições financeiras é fundamentada pela Lei n.º 7.492/1986, com pena de reclusão de 3 a 12 anos. Gestão fraudulenta em instituição financeira pode ser tida como o recurso a qualquer tipo de ardil, sutileza ou astúcia hábil a dissimular o real objetivo de um ato ou negócio, que buscam enganar as autoridades monetárias ou aqueles que mantêm relação jurídica com o agente. Já a gestão temerária está relacionada à impulsividade com que são geridos os negócios, aumentando o risco de se causar prejuízo financeiro a terceiros (MANTECCA, 1985).

Quando se trata de crime praticado por terceiros contra as instituições bancárias é chamado de estelionato. O estelionato caracteriza-se quando o agente emprega meio fraudulento, induzindo ou mantendo alguém em erro e conseguindo vantagem para si ou para outrem, vantagem ilícita, com dano patrimonial alheio (NORONHA, 1972).

Também deve ser considerada a fraude contra credores, que acontece quando o devedor desfalca seu patrimônio para evitar uma execução por dívidas e reduzindo a garantia dos credores e a fraude à execução quando o devedor danifica, destrói, desvia ou aliena o bem (PARODI, 2008), ou seja, na fraude contra o credor o devedor procura prejudicar o credor que tenta receber o que tem direito e na fraude à execução o devedor procura impedir a apreensão judicial de um bem que tenha sido dado em garantia ao credor.

O uso da internet possibilita a prática de crimes complexos (SANTOS, 2009). O Cyber crime é um campo relativamente novo, não existe consenso na definição e

gestão dos termos mais simples. Os advogados ainda tem pouco conhecimento técnico do ramo, pois a tecnologia é muito dinâmica, desta forma se faz necessária a cooperação entre a comunidade legal e técnica (ALMONTE, 1997). Pelo menos para o caso do Brasil esta afirmação de Almonte (1997) ainda é válida, como será visto a seguir.

Em relação aos crimes eletrônicos não existe no Brasil ainda uma legislação específica contra crimes feitos pela internet, como existe nos EUA e na Europa, por exemplo. Mas está em tramitação uma nova lei que tipifica e estabelece a punição para crimes eletrônicos como criação e a propagação de vírus, *phishing*, invasões de redes, acesso e divulgação indevida de dados.

Foi aprovada em 09 de julho de 2008 o projeto de lei que dispõe sobre crimes cometidos na área de informática e suas penalidades. De acordo com Botelho (2008) a PL 89/2003 compatibiliza o Brasil com o mundo que, de acordo com o autor, em 1998 foi apresentada pelo primeiro ministro britânico preocupação com o tema em uma reunião do G8 e no mesmo evento foram aprovadas as punições. Botelho (2008) mostra ainda que em 2001 surgiu a Convenção Europeia de Cyber Crimes, com 43 Estados nacionais, além da União Europeia, países como EUA, Canadá, Japão e África do Sul.

Em junho de 2010 a FEBRABAN firmou com a Polícia Federal uma parceria de combate à fraude eletrônica. Desta forma são compartilhados tecnologias e informações para proteção da sociedade e dos bancos. As vantagens principais desta parceira são maior agilidade após detecção de uma fraude e a possibilidade de mapeamento de grupos por todo o país. Como explica Botelho (2008) no texto do PL 89/2003 não há nada que comprometa o uso de conteúdos autorizados eletrônicos, pois apenas incrimina acessos a redes protegidas ou se este acesso violar sinais textuais de proibição.

Detalhadamente cada um dos dispositivos votados:

Acesso não autorizado a rede de computadores, dispositivo de comunicação ou sistema informatizado.

Art. 285-A. Acessar, mediante violação de segurança, rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso:

Pena - reclusão, de 1 (um) a 3 (três) anos, e multa.

De acordo com Botelho (2008) será punida apenas a invasão, a violação, ou seja, o cracker, quem quebra senhas e logs. Protegendo o titular da rede ou dispositivo que tenha colocado alguma restrição a seu ambiente eletrônico.

Obtenção, transferência ou fornecimento não autorizado de dado ou informação.

Art. 285-B. Obter ou transferir, sem autorização ou em desconformidade com autorização do legítimo titular da rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso, dado ou informação neles disponível:

Pena - reclusão, de 1 (um) a 3 (três) anos, e multa.

Para Botelho (2008) a lei punirá o “ladrão de dados” que obtém ou transfere dado ou informação disponibilizados em rede ou dispositivo exclusivo ou se a transferência ou obtenção se derem sem autorização do legítimo titular, ou em desconformidade com a autorização..

Divulgação ou utilização indevida de informações e dados pessoais

Art. 154-A. Divulgar, utilizar, comercializar ou disponibilizar dados e informações pessoais contidas em sistema informatizado com finalidade distinta da que motivou seu registro, salvo nos casos previstos em lei ou mediante expressa anuência da pessoa a que se referem, ou de seu representante legal:

Pena - detenção, de 1 (um) a 2 (dois) anos, e multa.

De acordo com Botelho (2008) neste caso o alvo punível é o “difusor de informações pessoais, alheias, sem comprometimento com limites impostos à difusão”, como por exemplo, violação de intimidade alheia em mídias sociais.

Dano. Art. 163. Destruir, inutilizar ou deteriorar coisa alheia ou dado eletrônico alheio:..” (NR)

Art. 5º O Capítulo IV do Título II da Parte Especial do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal) fica acrescido do art. 163-A, assim redigido:

“Inserção ou difusão de código malicioso

Art. 163-A. Inserir ou difundir código malicioso em dispositivo de comunicação, rede de computadores, ou sistema informatizado:

Pena - reclusão, de 1 (um) a 3 (três) anos, e multa.

Inserção ou difusão de código malicioso seguido de dano

§ 1º Se do crime resulta destruição, inutilização, deterioração, alteração, dificuldade do funcionamento, ou funcionamento desautorizado pelo legítimo titular, de dispositivo de comunicação, de rede de computadores, ou de sistema informatizado:

Pena - reclusão, de 2 (dois) a 4 (quatro) anos, e multa.

Para Botelho (2008) este artigo visa reprimir a difusão de vírus e tem sua forma qualificada quando este causar prejuízo para o titular ou restrição de funcionamento.

Art.171.

§ 2º Nas mesmas penas incorre quem:

Estelionato Eletrônico

VII - difunde, por qualquer meio, código malicioso com intuito de facilitar ou permitir acesso indevido à rede de computadores, dispositivo de comunicação ou sistema informatizado.

§ 3º Se o agente se vale de nome falso ou da utilização de identidade de terceiros para a prática do crime previsto no inciso VII do § 2º, a pena é aumentada de sexta parte." (NR)

Para Botelho (2008) este novo crime permite punir ao *cracker*, “que acessa a outras redes de computadores, ou uso de computadores ou dispositivos de redes, sem conhecimento do titular, para ingresso em outros níveis”.

2.3 GESTÃO DA FRAUDE FINANCEIRA

Gerir a fraude significa ter estratégias que possam identificar fraudes existentes e evitar que novas fraudes aconteçam. Inicialmente é necessário que seja designado um responsável ou um departamento responsável para este trabalho. Por meio deles a organização vai procurar entender quais são os tipos de risco de fraude que a ameaçam, saber quem a comete, como e quando acontece e quanto se é perdido. Identificadas estas variáveis serão definidas metas e a monitoração da performance em avaliações periódicas da escala de ameaça de fraude. Durante a monitoração será possível identificar quais são as medidas mais efetivas e focar mais recursos nelas (FEE, 2005).

Quando o assunto é a fraude uma ação recomendada é o trabalho em conjunto com outras organizações que sofrem os mesmos tipos de problemas. No caso dos bancos e financeiras brasileiros este trabalho é uma realidade, sendo realizado por exemplo, através das Comissões de Combate à Fraude da FEBRABAN, da Comissão Base de Inconsistência da Associação Nacional das Instituições de Crédito, Financiamento e Investimento (ACREFI) e também, de acordo com Sobral e

Sobral(2012)⁴, existe desde 2009 um acordo de cooperação entre a Polícia Federal e a FEBRABAN para montagem de um banco de dados, os bancos que aderiram encaminham online as informações sobre as fraudes que sofreram.

São muitos os benefícios de se trabalhar juntos contra a fraude, as boas práticas podem ser divididas e a troca de informações pode acontecer de forma mais eficiente. As organizações participantes podem desenvolver habilidades, sistemas e um escopo mais consistente juntas, podendo testar também a consistência das informações passadas por clientes, além do benefício de se construir confiança e entendimento entre elas (FEE, 2005; NATIONAL, 2008).

De acordo com a FEE (2005) além do trabalho em conjunto, para lidar com as fraudes é importante impor sanções para casos acontecidos, como mover ações penais e de recuperação de ativos. É preciso avaliar a efetividade destas sanções, investigar os casos e esclarecê-los por completo usando para detecção vários métodos diferentes, cruzando informações e as confirmando. A figura 3 ilustra o método apresentado pela FEE para o processo de gestão da fraude.

⁴ SOBRAL, C. E. M e SOBRAL R. M. Os crimes Cibernéticos no Brasil: O uso da tecnologia para combate dos delitos em massa, 2012, (não publicado)

Fonte: FEE - *Federation des Experts Comptables Europeens*, 2005

Figura 3 - Elementos para uma estratégia integrada de combate à fraude

2.3.1 PREVENÇÃO DA FRAUDE FINANCEIRA

Todo programa de prevenção à fraude deve começar pelo comprometimento do topo da empresa, que vai implementar e seguir um código de ética e conduta. O sistema de controles internos deve ser claro e os funcionários devem ser constantemente treinados para cumpri-lo. As organizações devem aderir à prática de verificar o histórico dos funcionários, dos fornecedores e dos clientes e divulgar a todos as consequências para um ato de fraude (LOZZANO, 2009). Assim será possível criar uma cultura anti-fraude, fortalecer os controles e a conformidade com as normas internas (FEE, 2005).

2.3.1.1 PREVENÇÃO DA FRAUDE DOCUMENTAL

Hollein (2010) apresenta os três passos para atenuação das condições que podem levar à ocorrência da fraude. Primeiro, seria a definição de um forte tom ético no topo, que consiga permear a cultura corporativa. De acordo com a autora, se for passada a mensagem de que todos que participam na companhia fazem “a coisa certa” são grandes as chances de que a coisa certa realmente seja feita, ou seja, desenvolver um efetivo programa de gerenciamento de risco de fraude. Ceticismo saudável é o segundo elemento chave. Não há substituto para mentalidade questionadora, mas é necessário caminhar na linha entre investigações que são sondagem, apropriados e com algum fundamento e aqueles que foram criados em um ambiente de trabalho hostil. Para quem tem a função na empresa de investigar suspeitas de fraude nunca é um processo fácil, porque alguns que se envolvem em comportamento fraudulento na empresa frequentemente são amigos de longa data e colegas de trabalho. A comunicação efetiva através de toda estrutura facilitada pela partilha regular de informação e identificação de brechas na monitoração da fraude fornece a terceira linha de potencial mitigação das fraudes.

De acordo com consultoria Kroll e a Economist Intelligence Unit as empresas devem disseminar os seus valores com treinamentos. Estes treinamentos não devem ser apenas para os funcionários, mas também para os fornecedores e terceirizados, evitando assim os danos à imagem da empresa e as perdas financeiras causadas pela fraude. De acordo com esta pesquisa os casos de fraudes custaram às empresas 2,1% do faturamento ao longo de 2011. Isto significa que para 18% das companhias, a perda chegou a 4% dos ganhos.(VALOR ECONOMICO, 2012)

De acordo com a Serasa (2011) as perdas com fraude são irre recuperáveis e é prejuízo líquido e certo, o que não acontece com a inadimplência. Para evitar perdas com a fraude de roubo de identidade existe no mercado um serviço de alerta de identidade, onde com uma consulta pelo CPF é possível cruzar esta informação com um banco de dados de óbitos, documentos e cheques roubados, endereços, telefones, etc. e sendo informada uma nota de risco.

Também para evitar os problemas de identificação foi sugerido no Seminário Latino-Americano de Segurança Bancária (1985) a utilização da identificação datiloscopia,

isto porque este seria o único confiável dentre todos os sistemas no mundo. O sistema de identificação datiloscópica, ou por digitais, é infalível devido ao fato de serem perenes já que foi comprovado que as cristas papilares aparecem no “sexto mês da vida intrauterina e permanecem em número, situação, forma e direção, até que o cadáver se decompõe e destrua a peça” (VELEZ ANGEL, 1985; p. 19). Elas não podem ser alteradas fisiológica, voluntária ou patologicamente. Um famoso exemplo é o do pistoleiro americano John Dellinger, célebre por ter iniciado os assaltos a bancos por volta de 1936. Ele pediu a um médico que raspasse suas digitais até o osso e foi colocado enxerto da pele das costelas, quando tirada as ataduras ele não tinha digitais, mas toda vez que era detido e verificavam que não tinha digitais já sabiam exatamente quem era, pois ele era o único que não as tinha.

Outras vantagens desta utilização foram apresentadas, como o fato de haver intercâmbio de digitais em todo o mundo e nunca foi verificado que duas são iguais, inclusive as pessoas tem dez digitais, todas diferentes entre si. Segundo relatado por Velez Angel (1985) um banco que adotou este sistema na Colômbia nunca mais teve um caso de fraude em abertura de conta. Outros sistemas foram criticados, o baseado na íris do olho, o sistema biométrico, o sistema fotográfico, pois em todos estes já se conseguiu comprovar que existem duas ou mais pessoas com características iguais. Desta forma a sugestão era que a impressão digital seja usada em todas as transações feitas.

Este argumento já não seria totalmente válido nos dias de hoje. Parodi (2008) afirma que existem meios de enganar estes leitores de digitais, como a criação de próteses plásticas então seria necessário um sistema que verificasse a composição do material. Apesar disto, entre as tecnologias biométricas disponíveis, a impressão digital é o mais utilizado no mundo, representando cerca de 50% dos produtos do gênero, porque é barata e bastante segura. A chance de duas pessoas terem a mesma digital é de uma em cem bilhões. O leitor de íris é ainda mais seguro que a impressão digital, segundo Parodi (2008), mas não tão barato. O maior inconveniente é que 11% da população do mundo tem íris inaptas ao sistema. O leitor de veias da palma da mão lê um mapa que não é igual nem em casos de gêmeos idênticos. Este sistema vai funcionar apenas se a pessoa estiver viva. O reconhecimento da dinâmica da assinatura é a análise da dinâmica do traço que forma um padrão. Esta análise inclui velocidade, aceleração, pressão etc. Por fim, a

identificação da voz reconhece a dicção de uma determinada frase como uma senha; neste caso não é totalmente segura, pois a voz muda com idade, problemas de saúde, uso anterior da voz (PARODI, 2008). A comparação destas técnicas pode ser vista no quadro 04.

Tecnologia Biométrica	Precisão	Falhas em Operação	Melhor uso	N Identificações (1:N) em 2 seg	Possibilidade de Falsificação
Veias da Palma da Mão	Ótima	Baixa	Massivo	200	Praticamente Nula
Íris	Ótima	Baixa	Massivo	300.000	Praticamente Nula
Impressão Digital	Boa	Média	Pessoal	15.000	Média
Geometria da Face	Boa	Baixa	Massivo	1 milhão	Média
Dinâmica da Assinatura	Boa	Média	Massivo/Pessoal	-	Média
Geometria da Mão	Regular	Média	Massivo	-	Média
Voz	Regular	Média	Massivo/Pessoal	-	Média

Fonte: Parodi (2008)

Quadro 4 - Técnicas de Identificação

2.3.1.2 PREVENÇÃO DAS FRAUDES ELETRÔNICAS E PELA INTERNET

Para a prevenção, uma medida tomada no nível administrativo em algumas instituições foi a criação de comitês de processamento de dados. Em outras procuram separar definitivamente funções que nos centros tradicionais de processamento de dados se confundem com as partes de desenvolvimento, de manutenção dos sistemas e de operação. Algumas empresas fizeram alterações que colocaram a parte de entrada de dados hierarquicamente separada da de operação. Também tem dado maior ênfase às auditorias de processamento de

dados (CLAB, 1982) outras empresas ainda começaram a restringir ambientes (KPMG, 2009). Em 1982 começaram a aparecer produtos desenhados especificamente para combater fraudes por computador: Imaspzap, Incorzap, Command (CMD), Spy, Debugger.

Mas a prevenção também tem evoluído, atualmente usam-se firewalls, que são programas para impedir que usuários da internet não autorizados acessem uma rede privada (SYMANTEC NORTON, 2012); certificados digitais, que são arquivos usados como prova de identidade pelos sistemas criptográficos (SYMANTEC NORTON, 2012); firma digital, que consiste na aplicação de algoritmos de encriptação de dados, assim o destinatário pode comprovar a autenticidade do remetente e do documento (PAIVA, 2002) e a encriptação, que é a conversão de dados em algoritmos para que sejam lidos apenas por pessoas autorizadas (SYMANTEC NORTON, 2012; GINEL, 1997). Cordeiro (1977) nos traz que cada tipo de delito precisa de determinada medida de precaução e de controle, porém antes de fazer esta opção é necessário fazer a avaliação dos riscos aos quais o sistema está exposto. O autor sugere um exame de consciência para determinar os perigos para o sistema:

1. Pessoas estranhas ao serviço têm acesso ao sistema?
2. Pessoas estranhas ao serviço têm acesso a partes vulneráveis do sistema?
3. A vulnerabilidade do sistema pode se dar por acidente?
4. Alcançar a parte vulnerável exige conhecimentos especiais?
5. Pessoas de baixo nível de confiança e com suficiente nível de conhecimento tem acesso às partes vulneráveis do sistema?
6. Alguma circunstância poderia alterar o nível de confiança das pessoas que tem acesso às partes vulneráveis do sistema?
7. O sistema tem ou produz algo que possa interessar a outros?
8. Os pontos de interesse para outros são acessíveis a pessoas estranhas ao serviço?
9. O acesso a pontos de interesse para terceiros dependem de conhecimentos especializados?

Certamente cada uma destas perguntas com resposta positiva vai gerar outras, aumentando o nível de segurança do sistema, apesar das perguntas iniciais serem

primárias e genéricas. O autor alerta que é preciso recordar da chamada lei básica de Dansinger segundo a qual sempre que se inventa algo, alguém, em algum lugar, começa imediatamente a pensar em meios de burlar a invenção (CORDEIRO, 1977).

De acordo com Ginel (1997) existem algumas recomendações para controlar as fraudes por cartões. Os cupons de venda devem ser revistos e feito o controle das numerações destes cupons. É preciso saber exatamente que numeração foi entregue a um estabelecimento de maneira que este comércio não possa apresentar um cupom que não corresponda.

A monitoração de autorizações se refere basicamente a utilizar o histórico de autorizações que tenha sido processado pelo adquirente e fazer um rastreamento. Buscando casos nos quais o cartão tenha sido utilizado várias vezes em um estabelecimento ou aqueles casos em que um mesmo cartão foi usado em dois lugares diferentes com uma diferença de tempo que não poderia ser real, por exemplo, o mesmo cartão ser usado no mesmo dia na Alemanha e na República Dominicana. Assim é possível seguir e desenvolver uma série de parâmetros que ajudam a identificar casos em que as transações têm um nível de suspeitas altas e merecem ser confirmada para verificar a natureza da transação, se feita pelo verdadeiro titular ou não (GINEL, 1997).

É preciso também fazer a monitoração de depósitos de um estabelecimento, vendo em que caso o volume destes depósitos, o percentual de devoluções, a quantidade média, supera os parâmetros habituais do estabelecimento. Para fraudes com manipulação de banda magnética as operadoras precisam assegurar que estão produzindo a transmissão íntegra da informação que está na banda magnética, assegurando que o adquirente não manipule ou reforme. Um sistema faz com que o comerciante introduza os quatro primeiros dígitos manualmente e quando passado o cartão se o número não conferir na leitura magnética a transação é bloqueada. (GINEL, 1997)

Quanto ao *skimming* que alcançava 10% do total de falsificações antes dos cartões com chip é possível aderir a seguintes medidas: forte ênfase na proteção de informações dentro das entidades financeiras, a informação do cartão e principalmente relativa à composição de banda magnética deve estar estritamente

protegida, se possível criptografada para que ninguém possa ter acesso, copiar ou carregá-la. A monitoração de utilizações de cartões fora do seu padrão de uso comum por meio de redes neurais e a verificação de informações impressas no cartão, a validação da data de validade e da existência real do plástico é muito importante. Em casos de compras por telefone ou internet a operadora deve confirmar a existência deste plástico em sua base de dados, pois muitos fraudadores usam programas de geração de números de cartões para fazer compras desta forma (GINEL, 1997).

Quando a fraude externa acontece algumas medidas podem ser tomadas. De acordo com o gráfico 8, baseado na pesquisa da PWC (2011), a maioria das empresas faz uma acusação criminal ou movem uma ação civil (77% em 2011 e 59% em 2009) notificam a autoridade regulatória ou apenas cortam suas relações de negócios, 5% das empresas não tomam nenhuma atitude.

Fonte: PWC (2011).

Gráfico 8 - Recursos interpostos contra fraudadores externos (% dos respondentes)

Quanto à fraude interna, lembrando o “Triângulo da Fraude” as ações de prevenção devem procurar evitar os três tipos de motivação. Para mitigar a fraude feita pelos incentivos, a empresa pode implementar códigos de conduta, ter um plano de salários adequado ao mercado ou superior, ter respeito e proximidade com

os funcionários e manter relações éticas com os clientes e demais agentes externos. Em relação à fraude por oportunidades a empresa deve dar mostras de que as fraudes serão identificadas, isto consiste em ter controles internos e externos, auditorias, sistemas de detecção, punição, publicidade de fraudes e de políticas anti-fraude. Para evitar a fraude feita pela racionalização a empresa deve manter um bom clima organizacional, iniciativas de responsabilidade social e fazer com que os funcionários tenham um sentimento de pertencimento. (MOURA, 2010)

Em síntese, de maneira geral, de acordo com Downing (2010) a prevenção à fraude passa pelos estágios de a) Consciência: os envolvidos devem estar treinados e monitorados; b) Controles Internos, com destaque para a segregação de funções e c) Análise dos Riscos, pelo menos uma vez por ano fazer a identificação dos possíveis riscos e classificá-los quanto à sua gravidade. Algumas medidas práticas são recomendadas pelo autor como a criação de um meio de comunicação para receber denúncias anônimas (elas devem ser investigadas), o uso da tecnologia, como softwares que ajudam no monitoramento dos processos e a realização de auditorias. Estas medidas não só ajudam a prevenir com também a detectar fraudes que não estavam sendo percebidas, como será visto a seguir.

2.3.2 DETECÇÃO DA FRAUDE FINANCEIRA

Medidas muito parecidas com as sugeridas por Downing (2010) para a prevenção da fraude foram apresentadas por Lozzano (2009) para a detecção. Por exemplo, o uso de softwares como ferramenta de trabalho, a realização de auditorias internas e externas, criação de uma forma de receber denúncias e seguir as suspeitas. Pode ser disponibilizado um telefone de ligação grátis ou e-mail para receber estas denúncias e divulgá-los, deixando claro que o informante não precisa se identificar e de que maneira serão tratados determinadas fraudes, além da existência de um departamento que monitore os casos de fraude e suas possibilidades.

Para Downing (2010) as medidas de detecção da fraude devem ser separadas pela origem interna ou externa. Para detectar fraudes internas todos os funcionários

devem ser obrigados a saírem em férias, as reconciliações bancárias devem ser feitas frequentemente, as contas bancárias não utilizadas devem ser fechadas e as informações prestadas pelos fornecedores devem ser checadas. Para detectar a fraude externa devem ser realizadas diligências em qualquer parte terceira que se associar ao negócio, sejam clientes, fornecedores, novos parceiros etc. Deve existir esforço para conhecer o cliente e suspeitar de algumas *red flags* comuns como a residência do cliente ser fora da área ou muito distante da companhia, suas ações são inconsistentes com os objetivos que ele diz ter com o negócio, grandes movimentações financeiras sem explicação. Podem ser implementados controles para evitar e detectar a engenharia social, como a destruição de documentos, acesso controlado a informações sensíveis, gerenciamento de identificação e senhas, controle de acesso de visitantes e o uso de computadores fora da companhia. Outras ações podem ser úteis para descoberta de mais *red flags* como as auditorias surpresa, ouvir reclamações de clientes e fornecedores, relatórios e análise financeira.

2.3.2.1 DETECÇÃO POR MEIO DOS CONTROLES E COMPLIANCE

Lofton (2010) em sua pesquisa com 500 executivos concluiu que 80% dos bancos não conseguem detectar a fraude antes de fundos serem transferidos para fora da instituição e em 87% dos ataques de fraude o banco não consegue recuperar plenamente os ativos.

Alguns fatores são os facilitadores da ocorrência de fraude nas empresas. Dentre eles o principal fator são os fracos controles internos (KRAMBIA-KAPARDIS, 2010). De acordo com a pesquisa da KPMG (2009) esta é a principal causa de fraude representando 64% do total, seguido pelas peculiaridades de cada ramo de empresa com 21%.

A adequação dos controles refere-se à habilidade de prevenir ou detectar roubos de ativos, devido ao desenho, implementação e monitoramento destes controles (GOLDEN; SKALAK; CLAYTON, 2006). Controles internos são procedimentos ou normas internas e formas de acompanhamento que verificam se os mesmos estão sendo efetivamente seguidos. Diferencia-se de auditoria externa, pois tem uma frequência maior e tem maior grau de profundidade (MATIAS, 2007). Também pode

ser definido como um “conjunto de procedimentos, métodos ou rotinas com os objetivos de proteger os ativos, produzir dados contábeis confiáveis e ajudar a administração na condução ordenada dos negócios da empresa” (ALMEIDA, 1996, p. 50).

Eles estão divididos entre contábeis e administrativos. Os contábeis estão relacionados aos sistemas de conferência, aprovação e autorização; à necessidade de segregação de funções, ao controle físico de ativo. Já os administrativos são os relacionados ao controle de qualidade, treinamento de pessoas, análises das variações entre os valores orçados e incorridos, etc. (MATIAS, 2007).

Alguns dos objetivos da supervisão bancária estão relacionados à avaliação da qualidade dos controles internos das instituições e, em especial, avaliar a efetividade do processo de supervisão feito pelo Conselho de Administração e dos controles internos desenhados para detectar e mitigar possíveis conflitos de interesse e fraudes, avaliar se as estruturas organizacionais estabelecidas pelas instituições incluem controle e supervisão, se enfatizam a prestação de contas e a abertura de informações e se as funções de auditoria interna e externa são conduzidas de forma independente e que efetivamente avaliem o sistema de controles internos da instituição (CORAZZA, 2000).

A maioria dos bancos elabora uma série de manuais de processos que padronizam os trâmites operacionais das agências e dos demais serviços, porém os empregados tem a tendência de aplicar seus próprios métodos de trabalho, “procurando agilizar e ganhar tempo no seu trabalho”, muitas vezes sem considerar a segurança, pensando em atender bem os clientes e sem conhecer como agem os fraudadores (VELEZ ANGEL, 1985,p.23).

A avaliação de riscos deve ser feita regularmente e com alto detalhamento, examinando os processos empregados pelos funcionários (VELEZ ANGEL, 1985). Além da segregação de funções e definição clara das responsabilidades de todas as áreas, o controle do nível de exatidão de detalhes dos documentos, controle das alterações dos documentos e acesso a eles também são medidas em geral eficientes de controle interno (CORDEIRO, 1977).

Algumas medidas práticas de controle em TI foram sugeridas por Almonte (1997) dentre elas a definição de políticas realistas, identificação e valoração dos ativos, observar o que pode dar errado, a utilização de um software maduro, contratação de pessoas honestas, encriptação de dados, back-ups, manterem-se informados sobre novos métodos de ataque e a realização de estudos de penetração no sistema. “Um sistema de informação é seguro somente quando sua integridade puder ser mantida, sua disponibilidade assegurada, sua confidencialidade preservada, sua informação consistente e seu acesso controlado” (ALMONTE, 1997, p. 195).

Hoje as empresas contam com ferramentas modernas de detecção de fraude. Os chamados *data mining* tem grande capacidade de tratamento massificado, ou seja, conseguem processar uma quantidade muito superior de informações que um cérebro humano em um curto período de tempo, muitas vezes em tempo real. Eles encontram informações, correlacionam, analisam padrões e detectam se algo não está de acordo com o que deveria ser (PIMENTA, 2009). Trata-se de um processo de seleção, exploração e modelagem de grande volume de dados para revelar aspectos antes não conhecidos, comportamentos, tendências e relacionamentos os quais podem ajudar a identificar casos de fraude (FEE, 2005).

Data matching envolve uma varredura computadorizada dos dados de diferentes arquivos da mesma organização ou não. Isto pode ser usado para gerenciamento de muitos propósitos, inclusive a fraude e as Redes Neurais que são computadores baseados em sistemas de multiprocessamento, designados para conectar dados vindos de múltiplos recursos para identificar estruturas, padrões e exceções. Isto pode facilitar o trabalho da empresa, que vai focar seus esforços nestas exceções (FEE, 2005).

Compliance significa cumprir o que foi imposto, estar em conformidade e fazer cumprir normas internas e externas (ABBI, 2009). Para evitar a fraude interna algumas medidas são críticas. Por exemplo, a clara comunicação interna sobre os valores e ética da empresa e o frequente reforço destes valores, não ignorar o risco da fraude e ter medidas efetivas no caso de aparecimento de casos de fraude (GOLDEN; SKALAK; CLAYTON, 2006).

Após os escândalos corporativos das últimas décadas os funcionários das empresas têm sido cada vez mais encorajados a monitorar a ética corporativa por meio de denúncias internas anônimas (GOLDEN; SKALAK; CLAYTON, 2006). No gráfico 9 é possível perceber a importância da cultura corporativa na detecção das fraudes. Porém apesar do importante papel da cultura corporativa são as medidas de controle corporativo, como a auditoria interna e monitoramento de transações suspeitas que mais detectam as fraudes nas empresas.

Fonte: PWC (2011).

Gráfico 9 - Métodos de Detecção de fraudes (% das fraudes reportadas)

Para ABBI- FEBRABAN (2009, p. 9) a missão de *compliance* é

Assegurar, em conjunto com as demais áreas, a adequação, fortalecimento e o funcionamento do Sistema de Controles Internos da Instituição, procurando mitigar os Riscos de acordo com a complexidade de seus negócios, bem como disseminar a cultura de controles para assegurar o cumprimento de leis e regulamentos existentes. Além de atuar na orientação e conscientização à prevenção de atividades e condutas que possam ocasionar riscos à imagem da instituição.

Gottschalk e Saether (2011) afirmam que os executivos são mais competentes quando introduzem mecanismos de controle e procedimentos de rotina em esforços de prevenção. Eles são menos competentes quando precisam realizar entrevistas, investigar documentos e procurar evidências eletrônicas em casos de fraude financeira. Para eles a tecnologia da informação é usada para coletar informação sobre procedimentos de rotina em grande quantidade, mas raramente em procedimentos de investigação, ou seja, prevenir ainda é mais fácil que remediar, já que o custo de detecção, investigação e ações judiciais para recuperação de bens adquiridos por meio de operações fraudulentas em geral são maiores que o valor da fraude em si, além dos casos que não são detectados (MOURA, 2010).

Na figura 4 são apresentados quais os componentes necessários na gestão da fraude, segundo a Ernest & Young (2010). A primeira fase de configuração e ajuste é onde se localiza a prevenção; neste período serão implementados o código de ética, as políticas de prevenção e os treinamentos. Na segunda fase, a proativa, está localizada a detecção; neste período os riscos de fraude serão avaliados, controlados e monitorados. A terceira fase é a de reação à fraude; qual ação tomar se identificada a fraude.

Em todas as três fases haverá sobre o processo de gestão a constante comunicação e monitoração considerando dados analíticos e se os elementos do programa estão sendo efetivos, avaliando se estes elementos estão sendo executados e se eles cumprem seu objetivo. Sempre que necessário, o processo será aperfeiçoado. As mudanças devem auxiliar na implementação e execução do programa.

Fonte: ERNEST & YOUNG, 2010.

Figura 4 - Componentes de um programa anti-fraude

3. MÉTODO

Este trabalho foi baseado na abordagem da *Grounded Theory* ou Teoria Fundamentada, utilizando o levantamento teórico anterior, entrevistas com gestores de segurança de um banco de varejo brasileiro, com uma associação de instituições financeiras e documentos para análise de seus conteúdos, principalmente casos reais de fraudes financeiras contra clientes já veiculados pela mídia. Neste capítulo será apresentado o tipo de estudo, o método de coleta, as proposições, as fontes de informações e análise.

A *Grounded Theory* é indicada quando o pesquisador se propõe a obter *insights* sobre um fenômeno, desenvolvendo uma teoria e também para entender um processo pelo qual os atores constroem significados e o modo como a realidade é compreendida (GLASER; STRAUSS, 1979; SUDDABY, 2006 *apud* COSTA, 2011)⁵.

A decisão de utilizar a *Grounded Theory* foi inspirada no trabalho de Costa (2011). Em sua tese de doutorado defendida na FGV SP, Costa (2011) utilizou os casos do Boi Gordo e do Banco Santos para analisar os antecedentes, os aspectos simbólicos e substantivos encontrados nas fraudes Corporativas. Em sua conclusão, por meio da teoria fundamentada, chegou-se à categoria central chamada "negócio baseado na confiança", respondendo quais as características estavam presentes nestas fraudes corporativas e como se deu a relação entre variáveis que criaram o contexto favorável à fraude.

3.1 TIPO DE ESTUDO

Trata-se de uma pesquisa qualitativa que discute este evento contemporâneo que é a fraude financeira externa em bancos. A análise lida com certa variedade de evidências como literatura, entrevistas e reportagens.

⁵ SUDDABY, Roy. From the editors: what grounded theory is not. **Academy of Management Journal**, vol. 49, no. 4, p. 633–642, 2006.

As entrevistas foram feitas em condições e com participantes escolhidos para representar situações típicas (YIN, 2010). Considera-se que o Banco brasileiro escolhido e a associação de bancos podem representar um banco típico e que as análises feitas podem em algum grau se estender aos demais.

A pesquisa foi descritiva à medida que pretende discorrer sobre o contexto onde a fraude acontece e exploratória, pois a situação avaliada pode não ter um único e claro conjunto de resultados (YIN, 2010). Uma das justificativas para um estudo em parte exploratório é que a base de conhecimento existente é pobre e a literatura disponível não fornece estrutura conceitual ou hipóteses notáveis. Mesmo neste caso é imprescindível a realização de uma revisão teórica relacionada a colaborar em uma possível “generalização analítica” (YIN, 2010).

3.2 MÉTODO DE COLETA

Para realização desta pesquisa foram utilizadas múltiplas fontes de evidências, não apenas uma, pois desta forma oferece maior poder de convencimento em qualquer achado ou conclusão (YIN, 2010) as quais são: 1) Literatura: a revisão teórica inicial deve ser base para a identificação das categorias relacionadas à gestão da fraude financeira externa. 2) Entrevistas; entrevista semi-estruturada perguntando aos respondentes-chave sobre os fatos relacionados ao tema, de maneira conversacional. 3) Observações diretas: Observação da organização, pesquisador estará pessoalmente nos locais e os artefatos físicos; deve-se verificar as tecnologias empregadas para gerenciamento da fraude ou qualquer outra evidência física e 4) Reportagens relacionadas ao tema da pesquisa.

3.3 PROPOSIÇÃO

O projeto de um estudo que seja exploratório deve declarar qual a sua finalidade, em vez de escrever proposições e também quais os critérios que vão dizer se a exploração pode ser julgada sucedida. (YIN, 2010). A proposição central deste trabalho é:

Analisar as formas de gestão da fraude financeira de um banco comercial típico, que oferece diversas formas de atendimento e financiamento, ou seja, diversas oportunidades para diversos tipos de fraude externa contra uma mesma organização.

3.4 FONTES DE INFORMAÇÕES

O estudo foi realizado nas seguintes unidades de análise: Diretoria de Segurança de um dos maiores bancos brasileiros, Associação de Bancos e documentação não técnica.

A literatura não técnica pode fornecer questões, conceitos iniciais e ideias para a amostragem teórica. Ela também pode ser usada como fonte de dados (primários e complementares) ou para fazer comparações, e pode agir como base para desenvolvimento da teoria geral (STRAUSS; CORBIN, 2008). O investigador analisa fatos e incidentes e não pessoas ou organizações. Pessoas, locais e documentos são apenas os meios para obter estes dados e continua até a saturação das categorias (STRAUSS e CORBIN, 2008).

Tabela 2 - Fontes de Informações

Fontes	Número
Entrevistas com respondentes-chave/ visitas	2
Artigos jornalísticos	102

Fonte: Elaborado pela autora

3.5 ANÁLISE DAS INFORMAÇÕES

Dentre as estratégias gerais de análise a pesquisa é norteadada pelo objetivo do trabalho: “Desenvolver um quadro conceitual sobre como é feita a gestão da fraude financeira externa”, que foi desenvolvido por meio da teoria fundamentada, baseada nas fontes de informações disponíveis.

Na teoria fundamentada fazer a microanálise é um passo importante. Por meio do exame minucioso dos dados o pesquisador deve descobrir novos conceitos e relações, desenvolvendo as categorias sistematicamente em termos de propriedades e dimensões. Formular perguntas e fazer comparações de maneira flexível e criativa permite ficar acima do lugar comum e desenvolver uma teoria inovadora e embasada (STRAUSS; CORBIN, 2008).

3.5.1 Codificação Aberta

A codificação aberta consiste em conceituar, definir categorias e desenvolver categorias em termos de propriedades e dimensões e depois relacionar as categorias por meio de hipóteses ou de declarações de relações. Conceituação é o processo de agrupar itens similares segundo algumas propriedades definidas e dar aos itens um nome que represente associação comum. Ao conceituar reduzimos grandes quantidades de dados a blocos de dados menores, mais administráveis. Ao obter as categorias é necessário especificar suas propriedades e mostrar como os conceitos (categorias) variam dimensionalmente ao longo destas propriedades. Por meio de especificação e de dimensionamento é possível começar a ver padrões. Assim, temos a base e a estrutura para a construção da teoria. (STRAUSS; CORBIN, 2008).

3.5.2 Codificação Axial

O processo de relacionar categorias às suas subcategorias chama-se axial por que ocorre em torno de um eixo de uma categoria, associando categorias ao nível de propriedade e dimensões, acrescentando a ela profundidade e estrutura. (STRAUSS e CORBIN, 2008). A figura 5 traz uma exemplificação do que é esta codificação axial. Trata-se dos relacionamentos das categorias “Tipo de fraude” e “Perdas com fraude” com suas subcategorias. No caso do “Tipo de fraude” é possível perceber que nos seus dois extremos estão as fraudes internas e externas à empresa, cabendo ao pesquisador analisar estes dois pontos e o que mais poderia estar entre eles, por exemplo, de que maneira poderia surgir a fraude mista. No caso da categoria “Perdas com fraude” está relacionada com as subcategorias extremas “Ativos” e “Imagem”. Para uma empresa pode ser fácil medir quanto foi perdido em valor pecuniário no caso de um roubo de ativo, desvio de pagamento por um funcionário, mas deve ainda mensurar o valor perdido pelo comprometimento de sua imagem caso seus sistemas sejam vulneráveis a um ataque fraudulento.

Fonte: Adaptado de Strauss e Corbin (2008)

Figura 5 - Codificação Axial

3.5.3 Codificação Seletiva

Este é o passo de integração e de refinamento da teoria. Na integração, as categorias são organizadas em torno de um conceito explanatório central. A integração ocorre com o tempo, começando com os primeiros passos da análise, e geralmente não termina até a redação final. Uma vez que se consiga um comprometimento com a ideia central, as principais categorias são relacionadas a ela por meio de declarações explanatórias de relações (STRAUSS; CORBIN, 2008).

3.5.4 Codificação para o processo

Estrutura e processo estão intimamente ligados. A estrutura tende a mudar com o tempo (avanços tecnológicos de segurança, procedimentos, treinamentos), a ação/interação tem que mudar para ficar em linha com a estrutura. Nem tudo que é um processo pode ser reduzido a estágio ou fases (STRAUSS e CORBIN, 2008). Esta relação pode ser percebida pela figura 6, onde os contextos estão em interação ao longo do tempo, mas apesar desta sequência de interação evolutiva acontecer, ao mesmo tempo existem variações inesperadas que podem levar a outros processos ou alteração nestes. Ao analisar os dados da pesquisa sobre a fraude financeira em busca de um processo serão observados movimento, sequência e mudança ou que se manteve, apesar das mudanças no contexto e condições (STRAUSS; CORBIN, 2008).

Fonte: STRAUSS e CORBIN, (2008, pág. 164).

Figura 6 - Processo

Legenda: Linhas retas: inter/ação evolutiva / **Círculos:** contexto para a interação/ **Sobreposição nos círculos:** intersecção de condições e consequências resultando na mudança de variação no contexto e ajustes feitos na interação para manter o fluxo.

4. RESULTADOS

4.1 O *FRAMEWORK* TEÓRICO

A estruturação de um *framework* teórico é o objetivo deste trabalho. É parte fundamental para sua conclusão, pois a partir dele serão comparadas as entrevistas realizadas e os artigos jornalísticos selecionados. Inicialmente, a partir da literatura mencionada no capítulo do referencial teórico intitulado Gestão de Fraudes: Prevenção e Detecção foi identificado que a Gestão da Fraude obedece a uma determinada sequência, que serão chamadas de fases, além da existência de ações que estão presentes em todas elas.

Para cada uma das fases (Codificação para o processo) foram identificadas as categorias (Codificação aberta) e subcategorias (Codificação Axial) com a utilização da Teoria Fundamentada, também a partir da literatura utilizada.

4.1.1 As fases

A partir do referencial teórico foram identificadas as seguintes fases: Prevenção, Detecção e Reação, além de ações que permeiam estas três fases, as quais estarão na fase chamada “Contínua”.

Na fase “Contínua” estão incluídas ações relacionadas à implantação da Gestão da Fraude, identificação das responsabilidades, a importância da comunicação, da avaliação e monitoração constantes, visando o aperfeiçoamento dos processos.

Na fase da Prevenção estão incluídas as ações institucionais para conscientização dos envolvidos, implantação de controles internos e avaliação dos riscos que a instituição está sujeita.

Na fase da Detecção a instituição determina que métodos serão utilizados para investigar suspeitas de fraude e confirmar as existentes. Nesta fase se encontram

também as ações que a empresa deve manter para que os indícios de fraude sejam imediatamente percebidos.

A última fase é a Reação. Nesta fase, após comprovada a fraude, a instituição deve decidir que medida tomar, como será sua postura diante de um caso de fraude. É importante que estejam claros que procedimentos seguir para cada tipo de fraude.

4.1.2 As categorias

Para cada fase foram definidas de 1 a 3 categorias para melhor explicá-las. As categorias são palavras que sintetizam uma ideia e buscam expressá-la de maneira clara. Uma categoria é um conjunto de ações que possuem muitas características comuns e podem ser abrangidas ou referidas por um conceito ou concepção genérica (HOUAISS, 2001)

Para a fase “Continua” foram definidas três categorias: 1) Responsabilidade. 2) Sinergia. 3) Aperfeiçoamento.

Na categoria Responsabilidade devem estar representadas tanto as responsabilidades pela gestão da fraude quanto as responsabilidades pela perpetração da fraude. Esta categoria está relacionada à fase “Contínua”, pois durante qualquer fase, prevenção, detecção ou reação, as responsabilidades devem estar definidas - é necessário que exista um dono do problema, seja um gestor ou um departamento. Saber quem ataca, de quem se prevenir ou contra quem reagir também são passos básicos da gestão da fraude.

Na categoria Sinergia devem estar representadas as relações externas - sinergia quer dizer que a soma dos esforços conjuntos de 1+1 é maior que os esforços individuais somados. Quando se trata de fraude não existem concorrentes, pois as fraudes em geral são muito parecidas e unir forças pode ser uma saída para mitigar o problema. Esta categoria foi alocada na fase “Continua”, pois a comunicação não deve cessar, independente se a instituição está na fase das ações de prevenção, de detecção ou reação.

Na categoria “Aperfeiçoamento” devem estar representadas as ações visando acompanhar a dinâmica do problema. A fraude não é estática, assim que um sistema de segurança é criado um fraudador pode estar criando uma forma de contorná-lo. Nesta categoria devem estar representadas a inteligência da gestão da fraude, a criação de relatórios, avaliação da efetividade das ações e correção dos rumos diante de resultados negativos. Esta categoria foi alocada na fase “Contínua” por um único motivo: o gestor da fraude precisa estar à frente do fraudador em qualquer circunstância. Assim o aperfeiçoamento das ações precisa ser uma preocupação constante.

Fase	Categorias relacionadas
Continua	Responsabilidade
	Sinergia
	Aperfeiçoamento

Fonte: Elaborado pela autora

Quadro 5 - Categorias da Fase "Contínua"

Para a fase “Prevenção” foram identificadas 2 categorias; 1) Instituição. 2) Identificação.

Na categoria Instituição deve estar representado o papel institucional para evitar qualquer tipo de fraude. O clima anti-fraude pode ser ditado pelo topo da Organização a partir da implementação de procedimentos de conduta e controles internos, garantindo que sejam efetivos e que as normas sejam cumpridas. A categoria Instituição está alocada na fase “Prevenção”, pois prevenir a fraude, ou seja, evitar que ela aconteça, é interesse maior da Instituição, que quer evitar perdas pecuniárias ou de imagem e tem meios para que a prevenção à fraude seja parte da cultura corporativa.

Na categoria Identificação devem estar representadas as ações para que uma mensagem seja enviada aos fraudadores, que nesta instituição a fraude será identificada. Para se identificar as fraudes financeiras inicialmente é preciso saber qual é a ameaça, treinar os funcionários para que as percebam e monitorar constantemente. A categoria Identificação foi alocada na fase “Prevenção”, pois o

intuito é representar como prevenir a fraude adiantando-se a ela e não deixar que aconteça para depois identificá-la.

Fase	Categorias relacionadas
Prevenção	Instituição
	Identificação

Fonte: Elaborado pela autora

Quadro 6 - Categorias da Fase "Prevenção"

Para a fase “Detecção” foram identificadas duas categorias; 1) Manutenção. 2) Investigação.

A categoria Manutenção deve representar as ações que tornem uma fraude pública rapidamente. Nesta categoria estão incluídas a definição de parâmetros e padrões de avaliação, a utilização de auditorias, a manutenção de registros e também o papel da estrutura funcional na detecção de fraudes. A categoria Manutenção está alocada na fase “Detecção”, pois apesar das ações de prevenção, possivelmente algumas fraudes ainda vão acontecer e a instituição precisa manter mecanismos para que não sejam levadas adiante.

A categoria Investigação deve representar ações para tratar suspeitas de fraudes que podem ter passado pelos mecanismos de manutenção. Nesta categoria estão incluídos meios de recebimento de denúncias e o tratamento delas com o uso da tecnologia. Esta categoria está alocada na fase “Detecção” porque a investigação é a maneira mais direta e mais usual de detectar uma fraude.

Fase	Categorias relacionadas
Detecção	Manutenção
	Investigação

Fonte: Elaborado pela autora

Quadro 7 - Categorias da Fase "Detecção"

Para a fase “Reação” foi identificada apenas uma categoria; 1) Sanções.

As sanções devem representar as decisões tomadas pela Instituição após a constatação de um caso de fraude. Existem vários tipos de fraude, desta forma são várias as possíveis reações ou sanções, sejam tratados com apoio das leis, acordos ou assumindo o prejuízo. A categoria “Sanções” está alocada na fase “Reação”, pois apenas será possível reagir depois de detectada a fraude.

Fase	Categorias relacionadas
Continua	Responsabilidade
	Sinergia
	Aperfeiçoamento
Prevenção	Instituição
	Identificação
Detecção	Manutenção
	Investigação
Reação	Sanções

Fonte: Elaborado pela Autora

Quadro 8 - Quadro Resumo Fases e Categorias

4.1.3 As subcategorias

Apesar das categorias tentarem exprimir uma ideia a partir de apenas uma palavra é possível identificar subcategorias que podem mostrar possíveis variações desta ideia. Desta forma, para cada uma das categorias foram identificadas de 2 a 5 subcategorias.

Na fase “Contínua”, categoria “Responsabilidade” foram identificadas duas subcategorias: 1) Gestor. 2) Fraudador.

A subcategoria “Gestor” deve representar a figura de quem trabalha pensando na gestão da fraude, o gestor ou seu departamento. O Gestor da Fraude é quem define as estratégias e avalia os riscos sobre os quais a Instituição está sujeita. O trabalho

do Gestor é garantir a segurança nos processos, verificar se as normas de segurança estão sendo cumpridas e se as atuais são efetivas.

A subcategoria “Fraudador” representa qualquer ameaça sofrida pela Instituição, seja um ataque individual ou por um grupo. A identificação do fraudador é a responsabilidade inicial do gestor da fraude.

Na fase “Contínua”, categoria “Sinergia” foram identificadas quatro subcategorias: 1) Comunicação. 2) Confiança. 3) Troca de Informações. 4) Comitês.

A subcategoria “Comunicação” está alocada na categoria “Sinergia” devido ao fato de representar a condição fundamental do trabalho em grupo: uma comunicação contínua e sem ruídos entre os interessados.

A subcategoria “Confiança” deve representar a construção do relacionamento sinérgico, onde o conhecimento gerado entre as partes possa ser difundido e utilizado em benefício de todos.

A subcategoria “Troca de Informações” deve representar o fluxo de informações entre as partes que estão trabalhando juntas. Um exemplo poderia ser a montagem de um banco de dados único para o grupo, alimentado por todos os componentes.

A subcategoria “Comitês” deve representar a realidade deste trabalho sinérgico. Os comitês podem ter uma política e um calendário de reuniões, para colocar em prática as subcategorias anteriores de comunicação, troca de informações e construção da confiança.

Na fase “Contínua”, categoria “Aperfeiçoamento” foram identificadas quatro subcategorias: 1) Dados analíticos. 2) Efetividade. 3) Regularidade. 4) Mudança.

A subcategoria “Dados Analíticos” deve representar a necessidade da utilização de dados para tomada de decisões em qualquer fase que o Gestor esteja concentrado. Os dados analíticos vão além de embasar a tomada de decisão, dizer em que medida a Instituição está sendo eficiente no combate à fraude.

A subcategoria “Efetividade” quer mostrar que as ações de gestão da fraude devem ser acompanhadas com o objetivo de garantir retorno ou resultado.

A subcategoria “Regularidade” deve representar esta necessidade de acompanhamento em qualquer uma das fases, por este motivo está dentro da categoria “Continua” e na categoria “Aperfeiçoamento”. Deve existir uma rotina de verificação - a efetividade não deve ser medida apenas em momentos críticos.

A subcategoria “Mudança” representa o caráter dinâmico da gestão da fraude diante da dinâmica da própria fraude. Visto que as fraudes mudam rapidamente, as estratégias institucionais podem ter que mudar da mesma forma para acompanhá-la.

Na fase “Prevenção”, categoria “Instituição” foram identificadas três subcategorias: 1) Código de Ética. 2) Controles Internos. 3) Conformidade.

A subcategoria “Código de Ética” representa o documento institucional que define a conduta dos seus funcionários e fornecedores. Nele deve estar expressa que postura a Instituição espera de quem se associa a ela. A instituição deve se certificar que estas partes tenham lido e entendido o Código.

A subcategoria “Controles Internos” representa a implantação de medidas práticas que minimizem os riscos de fraude. Os controles internos devem ser claros, aplicáveis e revistos sempre que necessário.

A subcategoria “Conformidade” representa a busca pela realização dos processos e negócios de acordo com as normas internas e externas. A conformidade dos processos deve ser checada com regularidade e devem ser definidas sanções em caso de descumprimento delas.

Na fase “Prevenção”, categoria “Identificação” foram identificadas quatro subcategorias: 1) Análise de Risco”. 2) Treinamento. 3) Monitoração. 4) Restrições.

A subcategoria “Análise de Risco” representa que a Instituição conhece suas fragilidades. O mapeamento dos riscos, inclusive a fraude, inerentes ao negócio possibilita a criação de mecanismos e ações para preveni-los. A instituição precisa saber contra o que está trabalhando.

A subcategoria “Treinamento” representa o papel da equipe na prevenção à fraude. Uma única pessoa não é capaz de combater a fraude. Toda a equipe deve estar ciente dos riscos que a instituição corre e estar preparada para identificá-los e alguns para tratá-los.

A subcategoria “Monitoração” representa a vigilância. O que é vigiado constantemente e de forma correta tem muito menos chances de ser atacado. Esta subcategoria poderia ser relacionada à subcategoria Regularidade da fase “Contínua”.

A subcategoria “Restrições” representa medidas de proteção de ativos. Estas restrições podem aparecer em forma de acesso restrito a ambientes físicos, virtuais e/ou alçadas de aprovações.

Na fase “Detecção”, categoria “Manutenção” foram identificadas cinco subcategorias: 1) Auditorias. 2) Histórico. 3) Parâmetros. 4) Padrões. 5) Segregação de Funções.

A subcategoria “Auditorias” representa uma metodologia de monitoração, seja interna ou externa, desta forma está alocada na fase de “Detecção”, mas não exclui a possibilidade da Organização se beneficiar do uso de Auditorias na fase de “Prevenção”.

A subcategoria “Histórico” representa a prática de manter encadeadas todas as informações a respeito de uma parte que se associar à Instituição, seja um cliente, funcionário ou fornecedor. E cada informação nova deve ser incluída e analisada.

A subcategoria “Parâmetros” representa faixas de variação possíveis para determinados comportamentos ou ações. Por exemplo, um cliente de banco, de acordo com seu histórico utiliza em média R\$ 500,00 do cheque especial por mês, com desvio padrão de R\$ 100,00. Se em determinado mês o valor estiver acima do desvio padrão será necessário verificar o motivo.

A subcategoria “Padrões” representa a análise de comportamento das partes associadas. Por exemplo, às 8 da manhã foi feita uma compra com cartão de crédito em Manaus e 3 horas depois foi feita uma compra com o mesmo cartão em Curitiba. Ou ainda, o histórico mostra que o cliente apenas usa seu cartão de crédito em lojas de roupas e determinado dia aparece uma grande compra neste cartão em um supermercado. Estas situações fogem ao padrão e é um motivo para verificação.

A subcategoria “Segregação de Funções” aparece em Manutenção, pois dentro da empresa pode haver um funcionário realizando fraude sozinho ou ajudando um

terceiro a cometê-la. Os processos devem ser desenhados para dificultar a realização das fraudes, por exemplo, o comprador não deve ser responsável pelo pagamento das contas. A instituição deve obrigar que seus funcionários saiam em férias e desconfiar de quem reluta em passar suas atribuições aos colegas.

Na fase “Detecção”, categoria “Investigação” foram identificadas cinco subcategorias: 1) Cruzamento de Informações. 2) Tecnologia. 3) Denúncias. 4) Diligências. 5) *Red Flags*.

A subcategoria “Cruzamento de Informações” representa a parte da categoria “Investigação” onde as informações obtidas pela manutenção do Histórico (subcategoria) serão analisadas considerando os parâmetros (subcategoria da categoria Manutenção da fase Detecção) definidos pela Instituição e os padrões (subcategoria da categoria Manutenção da fase Detecção) de comportamento do investigado. Este cruzamento de informações pode ser feito também com as informações trocadas (subcategoria da categoria Sinergia da fase Continua) com os pares nos Comitês (subcategoria da categoria Sinergia da fase Continua).

A subcategoria “Tecnologia” representa a utilização de recursos tecnológicos para maximizar a capacidade de análise da Instituição, permitindo que um número maior de informações seja analisada mais rapidamente e com maior precisão, mas não exclui a possibilidade da Organização se beneficiar do uso de Tecnologia na fase “Prevenção”.

A subcategoria “Denúncias” representa uma forma de a Instituição seguir pistas. Ela deve manter meios para que quem souber de alguma informação relevante possa denunciar sem se identificar e definir estratégias para averiguação destas denúncias recebidas.

A subcategoria “Diligências” representa a necessidade de se verificar fisicamente as informações recebidas. Significa que o ideal seria que um representante da Instituição fosse pessoalmente verificar, por exemplo, se o endereço residencial que um novo cliente informou existe e se ele realmente reside naquele local.

A subcategoria “*Red Flags*” representa a definição de sinais de que alguma coisa está errada e pode ser uma fraude. Está ligada aos padrões (subcategoria da

categoria Manutenção da fase Detecção), porém mostra que durante a investigação estes sinais serão procurados.

Na fase “Reação, categoria “Sanções” foram identificadas cinco subcategorias: 1) Crime. 2)Notificação. 3) Recuperação. 4)Fim de relação. 5)Perda.

A subcategoria “Crime” representa a decisão da Instituição de acionar judicialmente os responsáveis após a identificação da fraude, por exemplo, a montagem de notícia crime por estelionato caso um cliente utilize identidade falsa.

A subcategoria “Notificação” representa a decisão da Instituição de comunicar a órgãos superiores em caso de identificação de fraude, por exemplo, quando um caso de lavagem de dinheiro é notificado ao Conselho de Controle de Atividades Financeiras (COAF).

A subcategoria “Recuperação” representa a decisão da Instituição reaver o que foi perdido, por exemplo, a busca do ativo quando existe garantia no contrato.

A subcategoria “Fim da Relação” representa a decisão da Instituição de apenas encerrar o relacionamento com a parte que a fraudou e evitar ações de recuperação ou punição ao responsável.

A subcategoria “Perda” representa a decisão da Instituição de mensurar o prejuízo da fraude e lançar como perdas. Uma observação na categoria “Sanções” é que todas as subcategorias poderiam ser utilizadas em um único caso.

O quadro 6 mostra o Framework Teórico da Gestão da Fraude Financeira.

FRAMEWORK TEÓRICO DA GESTÃO DA FRAUDE FINANCEIRA			IDENTIFICAÇÃO TEÓRICA	
Fase	CATEGORIAS	SUBCATEGORIAS	REFERÊNCIAS	EXEMPLOS
Continua	Responsabilidade	Gestor	(FEE,2005)	[...] Inicialmente é necessário que seja designado um responsável ou um departamento responsável para este trabalho.[...]
		Fraudador	(FEE,2005)	[...]a organização vai[...] saber quem a comete.[...]
	Sinergia	Comunicação	(FEE,2005)	[...] São muitos os benefícios de se trabalhar juntos contra a fraude, as boas práticas podem ser divididas. [...]
		Confiança	(FEE,2005; NATIONAL, 2008)	[...] além do benefício de se construir confiança e entendimento entre elas [...]
		Troca de informações	(FEE,2005)	[...] e a troca de informações pode acontecer de forma mais eficiente.[...]
		Comitês	(CLAB,1982)	[...]uma medida tomada no nível administrativo em algumas instituições foi a criação de comitês de processamento de dados[...]
	Aperfeiçoamento	Dados analíticos	(ALMONTE,1997)	[...] identificação e valoração dos ativos [...]
		Efetividade	(CORAZZA,2000; FEE,2005)	[...] avaliar a efetividade do processo de supervisão feito pelo Conselho de Administração e dos controles internos desenhados para detectar e mitigar possíveis conflitos de interesse e fraudes.[...]
		Regularidade	(FEE,2005)	[...] serão definidas metas e a monitoração da performance em avaliações periódicas da escala de ameaça de fraude[...]
		Mudança	(ALMONTE,1997)	[...] manterem-se informados sobre novos métodos de ataque e a realização de estudos de penetração no sistema[...]

FRAMEWORK TEÓRICO DA GESTÃO DA FRAUDE FINANCEIRA			IDENTIFICAÇÃO TEÓRICA	
Fase	CATEGORIAS	SUBCATEGORIAS	REFERÊNCIAS	EXEMPLOS
Prevenção	Instituição	Código de Ética	(LOZZANO,2009; HOLLEIN,2010; ERNEST & YOUNG, 2010)	[...] Todo programa de prevenção à fraude deve começar pelo comprometimento do topo da empresa, que vai implementar e seguir um código de ética e conduta. 2- “a definição de um forte tom ético no topo, que consiga permear a cultura corporativa.”[...]
		Controles Internos	(LOZZANO,2009; KRAMBIA-KAPARDIS,2010; KPMG,2009; GOLDEN, SKALAK, CLAYTON, 2006; GOTTSCHALK e SAETHER,2011; ERNEST & YOUNG, 2010)	[...]O sistema de controles internos deve ser claro. “Alguns fatores são os facilitadores da ocorrência de fraude nas empresas, dentre eles o principal fator são os fracos controles internos”[...]
		Conformidade	(ABBI-FEBRABAN, 2009)	[...]missão de <i>compliance</i> é(...)atuar na orientação e conscientização à prevenção de atividades e condutas que possam ocasionar riscos à imagem da instituição.[...]
	Identificação	Análise de risco	(FEE,2005; DOWNING 2010; VELEZ ANGEL,1985; ERNEST & YOUNG,2010)	[...] a organização vai procurar entender quais são os tipos de risco de fraude que a ameaçam. pelo menos uma vez por ano fazer a identificação dos possíveis riscos e classifica-los quanto a sua gravidade. “A avaliação de riscos deve ser feita regularmente e com alto detalhamento”[...]
		Treinamento	(DOWNING, 2010; ERNEST & YOUNG, 2010)	[...]os envolvidos devem estar treinados e monitorados [...]
		Monitoração	(FEE,2005; PWC,2011; GOTTSCHALK e SAETHER,2011;ERNEST & YOUNG, 2010)	[...] Durante a monitoração será possível identificar quais são as medidas mais efetivas e focar mais recursos nelas.2- “a auditoria interna e monitoramento de transações suspeitas é que mais detectam as fraudes”[...]

		Restrições	(KPMG,2009)	[...] outras empresas ainda começaram a restringir ambientes (KPMG, 2009). [...]
--	--	------------	-------------	--

FRAMEWORK TEÓRICO DA GESTÃO DA FRAUDE FINANCEIRA			IDENTIFICAÇÃO TEÓRICA	
Fase	CATEGORIAS	SUBCATEGORIAS	REFERÊNCIAS	EXEMPLO
Detecção	Manutenção	Auditorias	(MOURA,2010;PWC,2011; DOWNING,2010; LOZZANO,2009; CLAB,1985)	[...] deve dar mostras de que as fraudes serão pegas, isto consiste em ter controles internos e externos, auditorias, [...]
		Histórico	(GINEL,1997; LOZANNO,2009)	[...] utilizar o histórico de autorizações que tenha sido processado [...]
		Parâmetros	(GINEL,1997)	[...] é possível seguir e desenvolver uma série de parâmetros que ajudam a identificar casos em que as transações têm um nível de suspeitas altas [...]
		Padrões	(VELEZ ANGEL,1985; FEE,2005; PIMENTA,2009; PARODI,2008)	[...] 1- recursos para identificar estruturas, padrões e exceções 2- A maioria dos bancos elabora uma série manuais de processos que padronizam os trâmites operacionais das agências e dos demais serviços [...]
		Segregação de funções	(CLAB,1982;CORDEIRO,1977)	[...] em outras procuram separar definitivamente funções que nos centros tradicionais de processamento de dados se confundem com as partes de desenvolvimento, de manutenção dos sistemas e de operação. segregação de funções e definição clara das responsabilidades de todas as áreas [...]
	Investigação	Cruzamento de Informações	(FEE,2005; SERASA,2011)	[...] usando para detecção vários métodos diferentes, cruzando informações e as confirmando [...]
		Tecnologia	(DOWNING,2010; PIMENTA,2009; PARODI,2008; MOURA,2010; ALMONTE ,2009; LOZZANO,2009)	[...] o uso da tecnologia, como softwares que ajudam no monitoramento dos processos. contam com ferramentas modernas de detecção de fraude [...]
		Denúncias	(DOWNING,2010; GOLDEN; SKALAK; CLAYTON,2006)	[...] criação de um meio de comunicação para receber denúncias anônimas. 2-“Após os escândalos corporativos das últimas décadas os funcionários das empresas têm sido cada vez mais encorajados a monitorar a ética corporativa por meio de denuncias internas anônimas [...]

	Investigação	Diligências	(DOWNING,2010)	[...] devem ser realizadas diligências em qualquer parte terceira que se associar ao negócio, sejam clientes, fornecedores, novos parceiros etc.[...]
		<i>Red flags</i>	(DOWNING,2010)	[...] Deve existir esforço para conhecer o cliente e suspeitar de algumas <i>red flags</i> comuns como a residência do cliente ser fora da área ou muito distante da companhia [...]

FRAMEWORK TEÓRICO DA GESTÃO DA FRAUDE FINANCEIRA			IDENTIFICAÇÃO TEÓRICA	
Fase	CATEGORIAS	SUBCATEGORIAS	REFERÊNCIAS	EXEMPLO
Reação	Sanções	Crime	(FEE,2005; PWC,2011; ERNEST & YOUNG,2010)	[...] para lidar com as fraudes é importante impor sanções para casos acontecidos “a maioria das empresas faz uma acusação criminal ou movem uma ação civil” [...]
		Notificação	(PWC,2011; ERNEST & YOUNG, 2010).	[...] notificam a autoridade regulatória [...]
		Recuperação	(ERNEST & YOUNG,2010; MOURA,2010)	[...]ações judiciais para recuperação de bens adquiridos por meio de operações fraudulentas em geral são maiores que o valor da fraude em si. [...]
		Fim de relação	(PWC,2011; ERNEST & YOUNG, 2010)	[...] apenas cortam suas relações de negócios. [...]
		Perda	(ERNEST & YOUNG,2010; SERASA,2011; GOLDEN; SKALAK; CLAYTON ,2006).	[...] as perdas com fraude são irre recuperáveis e é prejuízo líquido e certo. 2- Contadores podem quantificar as perdas, que podem ser somadas com os custos para reparar, perdas de produtividade, imagem, etc [...]

Fonte: Elaborado pela autora.

Quadro 9 - *Framework* Teórico.

4.2 IDENTIFICAÇÃO PRÁTICA

Na identificação prática o intuito é comparar informações reais com as categorias e subcategorias obtidas no *framework* teórico. As informações práticas foram obtidas a partir de entrevistas feitas com um banco de varejo, com uma associação de bancos e também foram utilizadas reportagens jornalísticas relacionadas ao tema.

4.2.1 As entrevistas

As entrevistas foram realizadas entre julho de 2011 e agosto de 2012, com o auxílio de um roteiro semi-estruturado (vide Apêndice A) aplicado a gestores de segurança do banco de varejo e um representante da Associação de Instituições Financeiras.

4.2.1.1 Banco de Varejo

Entrevista realizada em 11/08/2011 com os representantes da Diretoria de Segurança de um grande banco de varejo brasileiro. Relato validado pelos entrevistados em junho 2012.

O Banco conta com agências em todo Brasil e em quatro continentes no mundo. É proprietário de outros bancos na Argentina, nos Estados Unidos e na Europa. Para esses bancos estrangeiros a Instituição apresenta políticas, mas as normas e os procedimentos são feitos de acordo com a legislação local, não existindo, portanto, uma padronização global.

De acordo com os entrevistados, foi percebida a necessidade de se ter uma diretoria de Segurança desde os anos 80, porém em meados dos anos 2000 foi totalmente reestruturada.

O intuito e objetivo da área é proteger os ativos e as pessoas que se relacionam com a instituição. Desde então a atribuição da diretoria de segurança é pensar e desenvolver soluções para segurança de canais, produtos, serviços e processos.

Não existe um marco no tempo, mas os entrevistados afirmaram que a tecnologia trouxe consigo a necessidade de maior segurança. Atualmente mais de 90% das transações são realizadas eletronicamente, abrindo espaço para as mais diversas fraudes.

Os entrevistados afirmam ter dificuldade em encontrar bibliografia relacionada aos problemas e rotinas da sua área, principalmente devido à dinâmica do assunto, mas o banco incentiva a pesquisa em todos os seus setores. Desta forma, a área de segurança mantém uma área de P&D. Alguns funcionários são pesquisadores, doutorandos de universidade federal.

De acordo com os entrevistados, para a instituição uma fraude financeira são os atos voluntários que lesam o patrimônio do banco ou mesmo as tentativas, vindas de agentes internos ou externos. Para eles a fraude financeira é um risco operacional, ligado a processos, pessoas e tecnologia.

Na estrutura do banco existe a Diretoria de Riscos, que acompanha as informações referentes aos diversos riscos: mercado, crédito, operacional, liquidez, etc.

Segundo os entrevistados, o fundamental em termos de segurança antifraude é ter um pessoal com conhecimento profundo sobre o assunto. As diversas tecnologias existentes para combater fraudes não substituem o pessoal altamente capacitado.

Cerca de 500 funcionários, espalhados no país, trabalham para garantir a segurança das operações na Instituição. Para ingresso na área, deve ser um funcionário selecionado internamente através de um rigoroso processo. Geralmente o funcionário inicia sua carreira na área de segurança em um cargo da base. A área tem um trabalho constante de formação destes funcionários.

O treinamento destes funcionários é feito por meio de cursos que são oferecidos internamente, relacionados às mais diversas matérias bancárias, e externamente, por meio inclusive de cursos exclusivamente desenvolvidos para a Instituição. No mercado não existem cursos que atendam completamente as necessidades da área.

Os resultados tem sido satisfatórios, o volume relativo de fraudes não tem crescido na mesma proporção do aumento das transações nos últimos 10 anos.

Além da própria auditoria interna, a instituição contrata empresas de auditoria externa para realizar a avaliação do processo.

Todas as decisões importantes são registradas em documentos e atas de reunião. Com isso, o conhecimento gerado na área durante estes anos está registrado. Se um novo procedimento de segurança é adotado, os motivos, implementação, histórico, resultados estão registrados.

Não existe um modelo de prevenção à fraude definitivo na Instituição. Os entrevistados desconhecem um banco que o utilize um modelo fixo, isto porque a área é muito dinâmica, não há como fazer prevenção de fraude com um modelo.

Alguns sistemas são utilizados para ajudar na prevenção à fraude, como por exemplo, os sistemas de bloqueio de transações suspeitas com cartões. Trata-se de um sistema de identificação de padrões por meio da análise feita pela técnica computacional conhecida por redes neurais artificiais, que de modo simplificado pode ser definido como um modelo matemático de processamento de informações. Estes sistemas de bloqueios na instituição são altamente eficientes, acima de 90% de efetividade.

Na data da entrevista também foi comentado a respeito do uso de certificados digitais A3 da ICP Brasil, que alguns clientes e funcionários já têm acesso. De acordo com informações disponíveis no site do banco, ele é um dispositivo que atesta a identidade de pessoas físicas e jurídicas virtualmente.

Na demonstração foi usado um cartão com chip, mas por ser do tipo A3 poderia ser também um *token* USB. Com este dispositivo não apenas transações bancárias podem ser feitas, mas também assinatura de contratos, declarações de Imposto de Renda, processos judiciais e administrativos, entre outros, com alto nível de segurança e validade jurídica.

Existe um esforço para que aconteça a comunicação interbancos a respeito do tema fraude contra clientes, os entrevistados reconhecem que poderia ajudar no combate à fraude. O que já começa a acontecer é uma união dos principais bancos com autoridades policiais para montar um banco de dados dos fraudadores.

O risco de fraude tecnológica é mais preocupante que o risco de fraude envolvendo pessoal, porque o potencial de prejuízo é muito maior na primeira. O risco envolvendo erro de pessoal é chamado no banco de falha e também é tratado na área.

O Código de ética e normas de conduta são lidos via sistema nos primeiros dias do funcionário no Banco, não é possível realizar outra atividade sem ter confirmado a leitura, assim todo o público interno conhece as práticas de segurança de informação. Uma forma efetiva de registrar quantas vezes o funcionário leu e uma forma do Banco se resguardar no caso do funcionário afirmar que desconhecia qualquer parte do Código.

Os produtos/serviços da Instituição são muito parecidos com todos os outros bancos, desta forma, os procedimentos antifraude são parecidos entre eles, de acordo com os entrevistados. Para eles, o que difere a segurança da Instituição são as pessoas, isto por ser um banco onde as pessoas tem muitas chances de crescimento na carreira, o que poucos podem oferecer.

Já se verificou funcionários fraudando clientes, mas pelo tamanho do banco não são números expressivos. O funcionário que é pego fraudando é demitido por justa causa, o que o impede de ingressar novamente na Instituição. Exemplos citados foram saque de conta de cliente e aumento do próprio limite de crédito feito pelo funcionário.

Nunca foi feita a contratação de um “consultor” (por exemplo, empresa contrata os serviços de um *hacker* para achar brechas em seu sistema) para verificar constantemente quais são as possibilidades de fraudar os clientes, mas na área existem pessoas altamente qualificadas cujas funções são as de monitoramento dos canais.

A fraude em *call center* não é a grande preocupação visto que é feito de um em um. A fraude mais danosa é a feita quando um único computador ataca ao mesmo tempo uma série de contas.

A maioria das tecnologias de segurança não são patenteadas, desta forma, alguma tecnologia testada por um banco pode ser copiada por outro. O tempo em média para um dispositivo de segurança ser violado é de 1,5 a 2 anos, depois deste

período geralmente ela é ultrapassada. Por exemplo, o código de letras utilizado pelos bancos nos terminais de autotendimento demorou 1,5 ano para que fosse violado.

Apesar de o banco de dados referente aos clientes que pertencem ao banco ser um recurso valioso, não existe seguro. No caso da Instituição, deveria ser uma empresa do mesmo tamanho ou maior para segurá-la.

No Brasil não existe uma legislação específica para crimes feitos pela internet, mas está em tramitação a tipificação de crimes eletrônicos. No caso desta Instituição, as ocorrências são relatadas à autoridade policial como notícia crime, mesmo sem a tipificação específica independente do risco de imagem, ou seja, não haverá influência na ocorrência deste tipo fraude.

4.2.1.1 Associação de Instituições Financeiras

Entrevista realizada em 29/07/2011 com o representante da Associação de Instituições Financeiras. Relato da entrevista validado pelo entrevistado em 11/08/2011.

Esta Associação Nacional de Instituições Financeiras, com mais de 50 anos, congrega as empresas do setor, defende seus interesses, fortalece as relações entre os associados e promove o desenvolvimento de suas atividades. Com sede em São Paulo – SP funciona por meio de Comissões Técnicas compostas por representantes de cada Instituição associada. São comissões para Assuntos Jurídicos, *Compliance*, Contábil e Tributária, Veículos e outros.

Dentre as diversas comissões existentes verificou-se no ano de 2007 a necessidade da criação da Comissão Base de Inconsistências, que reúne os responsáveis pela prevenção e detecção de fraudes em 42 Instituições de Crédito do país, o que representa boa parte do total das 59 que aqui atuam. O objetivo principal desta comissão é evitar perdas, por meio do compartilhamento do conhecimento sobre as práticas de fraude existentes no mercado e os meios mais eficazes de combatê-las, em um esforço conjunto contra fraudadores dos mais diferentes perfis, que segundo

o entrevistado não obedece a um perfil pré-definido - existem fraudadores de todas as idades, cores, regiões, nota-se apenas uma quantidade maior de fraudadores do sexo masculino.

A comissão realiza reuniões mensais para debater e reunir informações a respeito da ocorrência de fraude. Pelas reuniões é frequentemente verificado que um mesmo fraudador pode aplicar o mesmo golpe em diversas financeiras. Todas as reuniões são registradas em ata.

Pelo estudo da Comissão estima-se que de 3 a 5% do valor financiado no mercado são tentativas de fraudes. Das fraudes documentais e eletrônicas existentes pode-se expandir em quatro grupos principais tratados pela Comissão Base de Inconsistências: a fraude nos contratos de Crédito Direto ao Consumidor (CDC Consumo), em Financiamentos de Veículos, Cartões e Empréstimo Consignado (Aposentados e pensionistas).

Na fraude em contratos de CDC percebe-se em muitas vezes a participação do cliente verdadeiro, onde ele fraudava dados cadastrais, por exemplo, aumentando o valor de sua renda ou apenas já realizando a compra sem a intenção de pagar.

Na fraude em veículos, apesar da garantia contratual pelo gravame no bem já foram verificados financiamentos em que o veículo pertence a um terceiro, não pertencendo ao estoque da loja “parceira” da Instituição financeira, onde denominamos no mercado como “terceiro de boa fé”, ou seja, a garantia não existe, uma evidência clara de que o agente lojista foi conivente ou totalmente responsável pela fraude. A relação entre as Instituições que fornecem o crédito e os agentes lojistas também é regida por um contrato de responsabilidade, mas não é totalmente eficaz devido à preocupação inicial com o comissionamento pela venda, desta forma, fraudes grosseiras podem passar despercebidas pelo agente comercial e lojista. De acordo com o entrevistado uma prática adequada para aprovação do crédito é a visita *in loco*, onde um agente faz a averiguação das informações prestadas pelo proponente pessoalmente, verificando local de residência, trabalho, se ela reconhece o financiamento, padrão de renda do bairro, dentre outras informações. Existem empresas especializadas que realizam este trabalho, mas o alto custo e o tempo de resposta são empecilhos para que seja realizado em cada

contrato, por isso cada instituição define um valor para o qual seja indispensável a visita.

A fraude com cartões hoje é a preocupação central da Comissão Base de Inconsistências, porque o volume tem crescido vertiginosamente e as possibilidades de fraude crescem em igual proporção. O Brasil foi pioneiro na implantação do chip em cartões, uma tecnologia cara, mas que já se mostrou vulnerável. Uma modalidade de fraude que ganhou destaque na entrevista foi a invasão de conta, onde o fraudador acessa a conta de um cliente e realiza pagamentos e alterações.

A busca por aumento da segurança nas Instituições de Crédito deve continuar, porque não foi inventado ainda um dispositivo que não fosse violado em pouco tempo. Uma prática no setor é a contratação de pessoas que buscam brechas no próprio sistema, testando sua segurança e tentando resolvê-las antes que um fraudador consiga.

De acordo com o entrevistado não existe uma receita contra a fraude. Na atual conjuntura onde a renda do brasileiro vem crescendo, puxando o consumo e os produtos de crédito, não há como evitar totalmente a ocorrência de fraudes, porém uma empresa com pessoal treinado pode fazer a diferença. Chamou-se a atenção para a área comercial, que deve estar mais alinhada com a prevenção à fraude, os vendedores preferem correr o risco de serem fraudados do que perderem a venda.

Em relação ao volume nominal de tentativa de fraude percebe-se aumento, mas como foi dito anteriormente o volume de crédito subiu mais que proporcionalmente. A existência da Base de Inconsistência tem ajudado no controle da fraude. Há esforço para contabilizar quanto em reais evitou-se perder com fraude devido à existência da Comissão Base de Inconsistência - estima-se aproximadamente R\$ 700 milhões no primeiro semestre de 2011.

Os fraudadores são pessoas que cometem crimes, mas não existe no Brasil ainda uma legislação específica contra crimes feitos pela internet, como existe nos Estados Unidos, por exemplo. O entrevistado não acredita que a tipificação dos crimes pela internet que está em tramitação possa reduzir o número de fraudes, pois em diversos casos, para preservação da imagem e por não obterem resultado

satisfatório na justiça quando a procuraram, as Instituições de crédito preferem arcar com a perda a se desgastarem em um processo.

Como o volume de negócios é muito grande, o auxílio de softwares inteligentes pode ajudar a mitigar o problema da fraude, mas as pessoas ainda não são substituíveis nesta área. Os fraudadores são pessoas e podem cometer pequenas e decisivas falhas, como insegurança na voz, uma assinatura suspeita, comportamento que não condiz com a renda informada, entre outros indícios que apenas uma pessoa bem treinada pode perceber. Resumindo, como fundamental em termos de prevenção à fraude seria uma área na empresa específica para Prevenção à Fraude que reporte direto à Presidência, atuação conjunta e não conflitante entre Área Comercial e Prevenção à Fraude e equipe muito bem treinada.

Assim como os entrevistados, Cordeiro (1977) já alertava sobre a necessidade de se concentrar esforços na preparação do pessoal. Segundo ele, os erros de operação não causam interrupções frequentes, mas podem ocasionar problemas delicados e de difícil solução.

4.2.2 Artigos jornalísticos

Para seleção dos artigos jornalísticos foram filtradas notícias com as seguintes palavras-chaves: “fraude”, “fraude financeira”, “crime eletrônico”, “fraude bancária”, “fraude pela internet”. Dos resultados encontrados foi feita uma seleção inicial para não considerar alguns tipos de notícias relacionadas à fraude no setor público, violações de imagem e corrupção. Foram escolhidos um número de 102 notícias aproveitáveis para o estudo.

Estas reportagens foram analisadas para identificação prática das categorias subcategorias definidas no framework teórico. Nestas reportagens verificou-se a predominância sobre casos de fraudes pela internet, mas também foram encontrados artigos sobre clonagem de cartões, sobre a participação policial na

resolução de alguns casos, sobre as estratégias utilizadas pelos fraudadores e apresentação de recursos tecnológicos para combate à fraude.

O quadro 7 demonstra esta identificação prática a partir das entrevistas descritas e destas reportagens veiculadas pela internet.

FRAMEWORK TEÓRICO DA GESTÃO DA FRAUDE FINANCEIRA			IDENTIFICAÇÃO PRÁTICA			
Fase	CATEGORIAS	SUBCATEGORIAS	Entrevista Banco de Varejo	Entrevista Associação	Notícias e Reportagens nacionais	Fonte
Continua	Responsabilidade	Gestor	O intuito e objetivo da área é proteger os ativos e as pessoas que se relacionam com a instituição. Desde então a atribuição da diretoria de segurança é pensar e desenvolver soluções para segurança canais, produtos, serviços e processos.	como fundamental em termos de prevenção à fraude seria uma área na empresa específica para Prevenção à Fraude que reporte direto à Presidência[...]	1- “No Brasil, os fraudadores miram preferencialmente sites de bancos e de empresas de telecomunicações”	ibahia.com
		Fraudador	união dos principais bancos com autoridades policiais para montar um banco de dados dos fraudadores	Um esforço conjunto contra fraudadores dos mais diferentes perfis, que segundo o entrevistado não obedece a um perfil pré-definido, existem fraudadores de todas as idades, cores, regiões, nota-se apenas uma quantidade maior de fraudadores do sexo masculino.	“Os perpetradores muitas vezes iniciam com pequenos roubos ou falsificações e gradualmente aumentam em tamanho e frequência.” 2-“ Um jovem, de boa aparência, vestindo calça, camisa social e gravata, que se passava por funcionário do Banco do Brasil de Itapeverica da Serra e, tinha por função “ajudar” as pessoas no caixa eletrônico da agência foi preso em flagrante na última segunda-feira, dia 02, pela polícia militar, após o senhor perceber a ação do acusado.” 3- “Na casa da dupla foram apreendidos aproximadamente 100 cartões de crédito falsos, cheques, documentos, celulares e R\$ 156 mil [...]”	Decisionreport.com.br/ jornalnananet.com.br Globo.com
	Sinergia	Comunicação	Existe um esforço para que aconteça a comunicação interbancos a respeito do tema fraude contra clientes, os entrevistados reconhecem que poderia ajudar no combate à fraude.	A comissão realiza reuniões mensais para debater e reunir informações a respeito da ocorrência de fraude. Pelas reuniões é frequentemente verificado que um mesmo fraudador pode aplicar o mesmo golpe em diversas financeiras.		

Continuação:

FRAMEWORK TEÓRICO DA GESTÃO DA FRAUDE FINANCEIRA			IDENTIFICAÇÃO PRÁTICA			
Fase	CATEGORIAS	SUBCATEGORIAS	Entrevista Banco de Varejo	Entrevista Associação	Notícias e Reportagens nacionais	Fonte
Continua	Sinergia	Confiança	-	-	-	
		Troca de informações	O que já começa a acontecer é uma união dos principais bancos com a PF para montar um banco de dados dos fraudadores.	Por meio do compartilhamento do conhecimento sobre as práticas de fraude existentes no mercado e os meios mais eficazes de combatê-la	“Fraudes e segurança da Informação são temas prioritários do CIAB 2012, maior evento de Tecnologia da Informação nos bancos”	Convergenciadigital.uol.com.br
		Comitês		Verificou-se no ano de 2007 a necessidade da criação da Comissão Base de Inconsistências, que reúne os responsáveis pela prevenção e detecção de fraude em 42 Instituições de Crédito do país		
	Aperfeiçoamento	Dados analíticos	Incentiva a pesquisa em todos os seus setores	Pelo estudo da Comissão estima-se que de 3 a 5% do valor financiado no mercado são tentativas de fraudes.	“houve, no segundo trimestre, um aumento de 89% no número de notificações de páginas falsas de instituições financeiras e de portais de comércio eletrônico. 2- De acordo com dados da Febraban, em 2011, os bancos brasileiros perderam cerca de R\$ 1,1 bilhão com fraudes eletrônicas.”	Techlider.com.br/convergenciadigital.uol.com.br
		Efetividade	Estes sistemas de bloqueios são altamente eficientes neste banco, acima de 90% de efetividade.	Há esforço para contabilizar quanto em reais evitou-se perder com fraude devido à existência da Comissão Base de Inconsistências	“Nossa capacidade de detecção é de 99%”	Computerworld.uol.com.br

Continuação:

FRAMEWORK TEÓRICO DA GESTÃO DA FRAUDE FINANCEIRA			IDENTIFICAÇÃO PRÁTICA			
Fase	CATEGORIAS	SUBCATEGORIAS	Entrevista Banco de Varejo	Entrevista Associação	Notícias e Reportagens nacionais	Fonte
Continua	Aperfeiçoamento	Regularidade	Todas as reuniões decisivas são registradas em ata, assim o conhecimento gerado sobre Gestão de Segurança durante estes anos está registrado. Se um novo procedimento de segurança é adotado os motivos, implementação, histórico, resultados são registrados.	A comissão realiza reuniões mensais		
		Mudança	Não existe um modelo de prevenção à fraude neste banco, os entrevistados desconhecem um banco que o utilizem, isto porque a área é muito dinâmica, não há como fazer prevenção de fraude com um modelo.	A busca por aumento da segurança nas Instituições de Crédito deve continuar, porque não foi inventado ainda um dispositivo que não fosse violado em pouco tempo.	“Se antes os cibercriminosos direcionavam vítimas brasileiras para sites fraudulentos para roubar dados bancários, agora uma nova modalidade de golpe burla sistemas antifraude e é aplicada direto no computador das vítimas.” 2- Rapidez dos fraudadores em modificar seus comportamentos assim que um padrão de atividade é descoberto. Nestes casos, utilizam outras técnicas ou migram seus ataques para outros departamentos;	Cssti.wordpress.com.br Administradores.com.br

Continuação:

FRAMEWORK TEÓRICO DA GESTÃO DA FRAUDE FINANCEIRA			IDENTIFICAÇÃO PRÁTICA			
Fase	CATEGORIAS	SUBCATEGORIAS	Entrevista Banco de Varejo	Entrevista Associação	Notícias e Reportagens nacionais	Fonte
Prevenção	Instituição	Código de Ética	O código de ética e normas de conduta são lidos via sistema nos primeiros dias do funcionário no Banco, não é possível realizar outra atividade sem ter confirmado a leitura, assim todo o público interno conhece as práticas de segurança de informação. Uma forma efetiva de registrar quantas vezes o funcionário leu e uma forma do Banco se resguardar no caso do funcionário afirmar que desconhecia qualquer parte do código.			
		Controles Internos			1- “esse potencial fraudador começa por procurar oportunidades na empresa onde ele possa perpetrar a fraude. Ele vai atrás de onde não existem controles, ou onde os controles internos são frágeis para poder agir com segurança e se dar bem.”2- “A falta de controles internos é a principal circunstância facilitadora com 64% dos casos, seguido das particularidades do ramo em que a empresa atua, com 21%.”	Decisionreport.com.br Administradores.com.br

FRAMEWORK TEÓRICO DA GESTÃO DA FRAUDE FINANCEIRA			IDENTIFICAÇÃO PRÁTICA			
Fase	CATEGORIAS	SUBCATEGORIAS	Entrevista Banco de Varejo	Entrevista Associação	Notícias e Reportagens nacionais	Fonte
Prevenção	Instituição	Conformidade	-	-	-	
	Identificação	Análise de risco	Fraudes financeiras são os atos voluntários que lesam o patrimônio do banco ou mesmo as tentativas, vindas de agentes internos ou externos. Para eles a fraude financeira é um risco operacional, ligado aos processos, às pessoas e à tecnologia.	Das fraudes documentais e eletrônicas existentes pode-se expandir em quatro grupos principais tratados pela Comissão Base de Inconsistências da ACREFI: a fraude no CDC Consumo, em Financiamentos de Veículos, Cartões e Empréstimo Consignado (Aposentados e pensionistas)	1- “Entre as metas dos hackers, constata ainda o levantamento da Check Point/Ponemon, estão as fraudes financeiras - 57%, interrupção das operações - 42% e roubo de dados dos clientes - 35%. 2- Há que estar atento para a segurança física e para a segurança lógica. “E agora temos também a mobilidade”	Cobertura CIAB 2012 convergencialdigital.uol.com.br
		Treinamento	Segundo os entrevistados o fundamental em termos de segurança antifraude é ter um pessoal com conhecimento profundo sobre o assunto. O treinamento destes funcionários é feito por meio de cursos que são oferecidos internamente. No mercado não existem cursos que atendam as necessidades da área.	[...]pessoal treinado pode fazer a diferença.	1- “Nas aulas, os policiais conhecem os meios técnicos adequados para a compreensão das evidências digitais deixadas pelos criminosos e como rastreá-los, por meio de ferramentas disponíveis e informações constantes na web e com os provedores de internet. 2- Além de equipes bem treinadas para responder em tempo às ameaças.” 3- Parte das ações que podem contribuir para a diminuição do número de fraudes passa pela gestão de pessoas, diz o diretor.	Correiodopovo-al.com.br/ convergencialdigital.uol.com.br valor.com.br

Continuação:

FRAMEWORK TEÓRICO DA GESTÃO DA FRAUDE FINANCEIRA			IDENTIFICAÇÃO PRÁTICA			
Fase	CATEGORIAS	SUBCATEGORIAS	Entrevista Banco de Varejo	Entrevista Associação	Notícias e Reportagens nacionais	Fonte
Prevenção	Identificação	Monitoração	Na área existem pessoas altamente qualificadas cujas funções são as de monitoramento dos canais		“os bancos devem contar com um perímetro bem configurado e monitorado”	Convergenciadigit al.uol.com.br
		Restrições		Chamou-se a atenção para a área comercial, que deve estar mais alinhada com a prevenção à fraude, os vendedores preferem correr o risco de serem fraudados do que perderem a venda, enquanto a postura de quem previne a fraude pode ser contrária.		

Continuação:

FRAMEWORK TEÓRICO DA GESTÃO DA FRAUDE FINANCEIRA			IDENTIFICAÇÃO PRÁTICA			
Fase	CATEGORIAS	SUBCATEGORIAS	Entrevista Banco de Varejo	Entrevista Associação	Notícias e Reportagens nacionais	Fonte
Detecção	Manutenção	Auditorias	Além da própria auditoria interna, a instituição contrata empresas de auditoria externa para realizar a avaliação do processo.		“Fraudes em instituições financeiras podem desacreditar as auditorias independentes”	Administradores.com.br
		Histórico	Todas as decisões importantes são registradas em documentos e atas de reunião. Com isso, o conhecimento gerado na área durante estes anos está registrado. Se um novo procedimento de segurança é adotado, os motivos, implementação, histórico, resultados estão registrado	Na fraude em contratos de CDC (Crédito Direto ao Consumidor) percebe-se em muitas vezes a participação do cliente verdadeiro, onde ele fraudava dados cadastrais, por exemplo, aumentando o valor de sua renda ou apenas já realizando a compra sem a intenção de pagar.		
		Parâmetros			“Ontem, Lenilson retornou a agência para desbloquear o cartão de débito e os talões de cheque, que recebeu pelo Correio, mas ao verificar o sistema do banco, o gerente constatou o alerta de fraude e informou a Polícia.”	Nominuto.com.br/noticias

FRAMEWORK TEÓRICO DA GESTÃO DA FRAUDE FINANCEIRA			IDENTIFICAÇÃO PRÁTICA			
Fase	CATEGORIAS	SUBCATEGORIAS	Entrevista Banco de Varejo	Entrevista Associação	Notícias e Reportagens nacionais	Fonte
Detecção	Manutenção	Padrões			1- “Falta de estatística e dados históricos para permitir o mapeamento dos padrões de fraudes ou modus operandi”	Administradores.com.br
		Segregação de funções	-	-	-	
	Investigação	Cruzamento de Informações			<p>1- “Segundo os policiais, eles chegaram até Querubim Pupu da Silva Filho cruzando dados do setor de inteligência da unidade com os do setor de segurança do banco, gerando um mapeamento de dias e horários em que o equipamento costumava ser instalado naquela agência. Com essas informações, os policiais monitoraram a entrada e saída de pessoas no banco, até flagrarem o criminoso instalando o equipamento.”</p> <p>2- “Com cruzamento de dados, corretora consegue identificar cliente para evitar fraudes”</p>	Portal Terra Exame.com.br

FRAMEWORK TEÓRICO DA GESTÃO DA FRAUDE FINANCEIRA			IDENTIFICAÇÃO PRÁTICA			
Fase	CATEGORIAS	SUBCATEGORIAS	Entrevista Banco de Varejo	Entrevista Associação	Notícias e Reportagens nacionais	Fonte
Detecção	Investigação	Tecnologia	Alguns sistemas são utilizados para ajudar na prevenção à fraude, como por exemplo, os sistemas de bloqueio de transações suspeitas com cartões.	Como o volume de negócios é muito grande o auxílio de softwares inteligentes pode ajudar a mitigar o problema da fraude.	1- “A análise aponta que os bancos, sozinhos, não são capazes de lidar com todas as ameaças e que os provedores de acesso devem fazer a parte deles.” 2- “A solução, que inclui o maior radar de detecção de fraudes do mundo, um sistema de decisões e consultoria especializada, tem a capacidade de detectar, com precisão, uma tentativa de fraude on-line em tempo real, em praticamente todos os métodos de pagamento (cartões de crédito e débito, boleto bancário, moedeiros etc).” 3- Se um cheque for modificado, a área tratada previamente com a tinta UV apresenta-se distorcida ou apagada.	Convergencialdigit al.uol.com.br Exame.com.br Prnewswire.com.br
		Denuncias		Como o volume de negócios é muito grande o auxílio de softwares inteligentes pode ajudar a mitigar o problema da fraude.	1- “De qualquer modo, um amplo e eficiente trabalho de captação de informações deve ser desenvolvido, de forma que as pessoas se sintam seguras para colaborar. Elas devem perceber que a empresa vai atuar.”	Administradores.c om.br

FRAMEWORK TEÓRICO DA GESTÃO DA FRAUDE FINANCEIRA			IDENTIFICAÇÃO PRÁTICA			
Fase	CATEGORIAS	SUBCATEGORIAS	Entrevista Banco de Varejo	Entrevista Associação	Notícias e Reportagens nacionais	Fonte
Detecção	Investigação	Diligências		De acordo com o entrevistado uma prática adequada para aprovação do crédito é a visita in loco, onde um agente faz a averiguação das informações prestadas pelo proponente pessoalmente, verificando local de residência, trabalho, se ela reconhece o financiamento, padrão de renda do bairro, dentre outras informações.		
		<i>Red flags</i>			1- “Todas as fraudes foram precedidas dos sinais de alerta que se fosse percebidas pelas diretorias; elas não teriam ocorrido.” 2- Algumas situações após a venda ter sido realizada podem apontar que a fraude já aconteceu: o cliente ligar reclamando que não realizou a compra do produto; se após a compra efetivada, não for paga nenhuma das parcelas; se o cliente não for encontrado; caso encontre o titular dos documentos, ele comprova que nunca esteve no estabelecimento.	Administradores.com.br Nominuto.Com/noticias

Continuação:

FRAMEWORK TEÓRICO DA GESTÃO DA FRAUDE FINANCEIRA			IDENTIFICAÇÃO PRÁTICA			
Fase	CATEGORIAS	SUBCATEGORIAS	Entrevista Banco de Varejo	Entrevista Associação	Notícias e Reportagens nacionais	Fonte
Reação	Sanções	Crime	Os casos de fraude são feitos em notícia crime mesmo sem a tipificação específica independente do risco de imagem, ou seja, não haverá influencia na ocorrência deste tipo fraude.		1 -“O "chupa-cabra" foi apreendido e Querubim foi preso em flagrante por tentativa de furto mediante fraude e interceptação de comunicação telemática sem autorização judicial. 2- Vinte e quatro pessoas de 13 países de quatro continentes foram detidas numa vasta operação do FBI que desmantelou uma organização internacional que se dedicava ao roubo e tráfico de números de cartões de crédito. Mais de 400 mil contas bancárias ficaram comprometidas com a ação criminosa desta rede agora desmantelada. 3 - As fraudes eletrônicas podem ser enquadradas como crime de interceptação de dados, de falsidade ideológica e de estelionato.” 4- Suspeitos de fraudar financiamentos de veículos são presos no AM, pela PF	Portal Terra/ Portal RTP / paraiba.com.br Acrítica.com.br
		Notificação			“o STJ emitiu nesta sexta-feira a súmula 479, segundo a qual "as instituições financeiras respondem objetivamente" pelos danos gerados por fraudes praticadas por terceiros em operações bancárias”	Exame.com.br/ veja.com.br

Continuação:

FRAMEWORK TEÓRICO DA GESTÃO DA FRAUDE FINANCEIRA			IDENTIFICAÇÃO PRÁTICA			
Fase	CATEGORIAS	SUBCATEGORIAS	Entrevista Banco de Varejo	Entrevista Associação	Notícias e Reportagens nacionais	Fonte
Reação	Sanções	Recuperação			1- Dificuldade em tomar uma decisão quando constatada a fraude, principalmente em andamento; Os valores recuperados não foram apontados. Na minha experiência constato que em poucos casos existe a recuperação de perdas.	Administradores.com.br
		Fim de relação	O funcionário que é pego fraudando é demitido do Banco por justa causa.		1- Em algumas empresas, após a descoberta das fraudes, ocorreram demissões (muitas sem justa causa).	Administradores.com.br
		Perda	O potencial de prejuízo é muito maior na fraude tecnológica	em diversos casos, para preservação da imagem e por não obterem resultado satisfatório na justiça quando a procuraram as instituições de crédito preferem arcar com a perda a se desgastarem em um processo.	“Além dos prejuízos financeiros as fraudes detectadas causaram perdas nas reputações das diretorias dos envolvidos.” 2- “Uma fraude, principalmente envolvendo grandes bancos, pode fazer o sistema financeiro perder confiança e, mais do que isso, perder dinheiro.”	Administradores.com.br istoedinheiro.com.br

Fonte: Elaborado pela autora

Quadro 10 - Identificação Prática do Framework Teórico

5. DISCUSSÃO

É possível perceber, analisando o *framework* teórico deste trabalho, que na fase “Contínua” a principal referência é a Fédération des Experts-comptables Européens (FEE). A Federação dos Contabilistas Europeus é uma organização internacional sem fins lucrativos com sede em Bruxelas que representa 45 institutos de profissionais contabilistas e auditores de 33 países europeus, incluindo todos os 27 Estados Membros da União Europeia, de acordo com o website da Federação.

Esta fase, que permeia as demais, representa por meio de suas categorias a necessidade de estarem claros quem são os responsáveis pela gestão da fraude e por sua perpetração, além da importância do trabalho em conjunto e do permanente aperfeiçoamento e avaliação deste processo de gestão.

Na identificação prática da fase “Contínua” foi possível localizar as categorias e subcategorias tanto nas entrevistas com o Banco de Varejo quanto com a Associação, assim como em reportagens nacionais. Apesar de em algumas subcategorias não ter sido possível encontrar nas três fontes de análise, por exemplo, a subcategoria “Fraudador” foi localizada nas entrevista com a Associação de Instituições e em reportagens, porém não foi mencionado o perfil do fraudador durante a entrevista com o Banco de Varejo.

Na fase “Contínua” apenas na subcategoria “Confiança” (vinculada à categoria “Sinergia”) não foi possível encontrar evidências práticas. Esta subcategoria deveria retratar a construção da confiança entre Instituições que trabalham juntas contra a fraude financeira externa ou como um benefício do trabalho em equipe.

Na fase de Prevenção do *framework* teórico o número de referências aumenta em comparação com a fase “Contínua”. Entre as referências destas fases estão autores, empresas de consultoria e auditoria e a Federação de Bancos Brasileiros. Esta fase, por meio de suas categorias, representa o papel da Instituição na prevenção da fraude como também os meios para sua identificação. Na fase da “Prevenção”, na

categoria “Instituição” é possível perceber que recebe destaque a subcategoria “Controles Internos” identificada em seis referências deste trabalho, ou seja, existe uma concordância a respeito da importância de fortes controles internos para prevenção de fraudes. Porém na identificação prática este assunto não foi encontrado nas entrevistas feitas com o Banco de Varejo e com a Associação de Instituições, apenas nas reportagens nacionais.

Na fase “Prevenção” apenas foi possível encontrar indícios práticos nas três fontes de pesquisa nas subcategorias “Treinamento” e “Análise de Risco” ambas vinculadas à categoria “Identificação”. Para a subcategoria “Conformidade” não foram encontrados indícios práticos nas entrevistas ou em reportagens. Esta subcategoria deveria representar a busca por estar de acordo com normas internas e externas.

Na fase “Detecção” do framework teórico, representada pelas categorias “Manutenção” e “Investigação”, é possível perceber que as subcategorias “Auditoria” e “Tecnologia” são as que possuem mais referências. Fica evidente a importância das auditorias interna e externa na detecção de fraudes, assim como é altamente recomendável que sejam utilizados recursos tecnológicos em processos de investigação de fraude.

Na identificação prática, apenas a subcategoria “Tecnologia” foi encontrada tanto nas entrevistas quanto nas reportagens. Nas entrevistas a tecnologia aparece como sistemas inteligentes que possuem a capacidade de analisar um grande volume de informações e transações, já nas reportagens aparece também como ferramenta que analisa alterações em documento físico.

Na fase “Detecção” apenas para a subcategoria “Segregação de Funções”, vinculada a categoria “Manutenção” não foram encontrados indícios práticos nas entrevistas e reportagens. A segregação de funções está relacionada a controles internos, porém é uma subcategoria à parte devido a importância de evitar que uma única pessoa seja responsável por todo um processo.

Na fase “Reação”, representada pela categoria “Sanções” as principais subcategorias referenciadas são “Crime” e “Perda” com três referências em cada

uma delas. Nesta fase, para todas as subcategorias foram encontrados indícios práticos em pelo menos uma entrevista ou reportagem. Apenas a subcategoria “Perdas” foi encontrada nas três fontes de evidencia. Apesar da possibilidade de se fazer uma notícia crime, encerrar a relação ou tentar buscar recuperar o prejuízo, a instituição vítima, em geral, arca com consideráveis perdas, principalmente a perda de reputação e de confiança.

A figura 7 é uma representação gráfica do *framework* da Gestão da Fraude elaborado neste trabalho. A seta representa a fase “Contínua” e suas categorias: Responsabilidade, Sinergia e Aperfeiçoamento, que devem estar presentes em todas as demais fases: Prevenção, Detecção e Sanções, que aparecem nos círculos. Abaixo de cada uma das fases (ou círculos) estão as suas respectivas categorias.

Fonte: Elaborado pela autora

Figura 7 - Representação gráfica do *Framework* da Gestão da Fraude

Ao final deste trabalho, como propõe a Teoria Fundamentada, é necessário chegar a uma categoria central do problema estudado. Considerando a dinâmica das fraudes financeiras externas, o nível de criatividade dos fraudadores em um setor tão visado como bancário é possível afirmar que a fraude é um problema inerente a esta atividade, confirmada pelo fato de até hoje não ter sido criado um dispositivo de segurança que não tenha sido violado. Desta forma, é possível mitigar a fraude financeira externa por meio da gestão da fraude, de acordo com as fases expostas no framework criado, porém sem perspectiva de eliminação total do problema, ou seja, a fraude financeira externa causa prejuízos, deve ser gerida para evitar que os ataques se tornem tão frequentes e as perdas insuportáveis para a organização, porém não há a garantia de uma solução definitiva.

Desta forma, chega-se ao final deste trabalho com a categoria central da discussão, que será chamada “Ação sobre a Crise Ininterrupta” A palavra crise, neste caso, quer representar a fraude como um momento difícil, uma situação de anormalidade que obriga a Instituição a se recompor, ou seja, ciclos de feedback positivos ou negativos no sentido de minimizar perdas, por meio de rotinas relacionadas à prevenção, detecção e sanções às fraudes externas.

Assim, tem-se no quadro 11 o esquema proposto para entendimento da gestão da fraude financeira por meio da teoria fundamentada.

Categoria Central	Categorias	Subcategorias	Descrição
Ação sobre a Crise Ininterrupta	Responsabilidade	Gestor/Fraudador	Representam tanto a responsabilidade tanto pela gestão quanto pela perpetração da fraude
	Sinergia	Comunicação, Confiança, Troca de Informações, Comitês.	Representam a sinergia, as relações externas. Quando o assunto é fraude não existem concorrentes, unir forças pode ajudar a mitigar o problema.
	Aperfeiçoamento	Dados Analíticos, Efetividade, Regularidade, Mudança.	Ações para acompanhamento da dinâmica do problema. Devem estar representadas a inteligência da gestão da fraude e a avaliação da efetividade das ações.
	Instituição	Código de Ética, Controles Internos, Conformidade.	Representa o papel institucional para evitar qualquer tipo de fraude. Deve ser criada uma cultura de prevenção à fraude.
	Identificação	Análise de Risco, Treinamento, Monitoração, Restrições.	Representa como prevenir a fraude adiantando-se a ela, identificando os sinais e não deixar para identificá-la apenas após o acontecimento.
	Manutenção	Auditoria, Históricos, Parâmetros, Padrões, Segregação de Funções.	São ações que tornem uma fraude pública rapidamente. Apesar das ações de prevenção, algumas fraudes vão acontecer, desta forma devem haver mecanismos para que não sejam levadas adiante.
	Investigação	Cruzamento de Informações, Tecnologia, Denúncias, Diligências, <i>Red Flags</i> .	São ações para tratar suspeitas de fraude que tenham passado pelos mecanismos de manutenção. A investigação é a maneira mais direta e usual de detectar uma fraude.
	Sanções	Crime, Notificação, Recuperação, Fim de Relação, Perda.	Representam as ações tomadas após a constatação de uma fraude. Apenas é possível definir uma sanção após esclarecida uma fraude.

Fonte: Elaborado pela autora.

Quadro 11 - Esquema para Gestão da Fraude Financeira

Este esquema, além de ser uma proposta para ordenar ou organizar o conhecimento existente sobre o tema gestão de fraudes, pode ser a base para a estruturação de um programa de gestão de fraude ou de um departamento de gestão de fraude em qualquer tipo de Organização.

6. CONSIDERAÇÕES FINAIS

Este trabalho procurou discutir a fraude financeira, que são os atos voluntários que podem lesar financeiramente outros agentes. As principais fraudes financeiras tratadas neste trabalho foram as referentes à alteração ou falsificação de documentos, as fraudes cometidas via internet, como a perpetração em ambientes virtuais e as fraudes eletrônicas que utilizam alterações e manipulação de sistemas eletrônicos.

Estas fraudes podem ser internas, cometidas por funcionários, externas, cometidas por terceiros sem relação trabalhista com a organização, ou mistas, onde existe cumplicidade entre pelo menos um agente interno e outro externo. As fraudes financeiras externas foram escolhidas como foco do trabalho.

As fraudes financeiras externas podem acontecer em qualquer tipo de organização, porém os bancos são os principais alvos destes fraudadores pela natureza do seu negócio: a movimentação financeira. Conforme foi verificado nesta pesquisa, entre todos os setores, apenas os bancos e seguradoras tem mais incidência de fraudes externas que fraudes internas.

Após esta constatação de que os bancos são alvos de fraudadores surgiu a dúvida de como eles fazem a gestão da fraude financeira externa. Para esclarecer esta dúvida foram realizadas duas entrevistas, uma com um banco de varejo de grande porte e outra com uma Associação de Instituições Financeiras.

Ainda para procurar entender melhor o assunto foi feita a revisão bibliográfica tratando do problema da fraude financeira como um risco operacional e verificou-se que está relacionado a pessoas, aos processos e à tecnologia. Esta revisão bibliográfica abordou também trabalhos sobre o histórico da fraude financeira, as fraudes documentais, pela internet e as eletrônicas. Houve a preocupação de se levantar também trabalhos que tentaram definir o perfil dos fraudadores e como a lei pode ser aplicada aos casos de fraude. Por fim, foram encontrados trabalhos, muitos deles publicações técnicas de empresas de auditoria sobre métodos de prevenção e detecção de fraudes, que podem ser aplicados às fraudes internas e externas.

A pesquisa bibliográfica foi a base para alcançar o objetivo geral deste trabalho foi estruturar um *framework* teórico sobre como é feita a gestão da fraude financeira externa em bancos, organizando e interligando as ideias dos trabalhos encontrados. Após análise do material bibliográfico foi percebido que a gestão da fraude poderia seguir um processo ou ter determinadas fases.

Após a organização do material em fases foi utilizado o método conhecido como Teoria Fundamentada ou *Grounded Theory*, para uma nova análise do texto, para entender o processo e para definição de categorias que pudessem exprimir as principais características encontradas em cada uma destas fases. As categorias definidas para a Gestão da Fraude foram: Responsabilidade, Sinergia, Aperfeiçoamento, Instituição, Identificação, Manutenção, Investigação e Sanções. Porém, algumas categorias podem ter variações dentro delas mesmas, por isso, ainda de acordo com a Teoria Fundamentada, foram definidas subcategorias para explicar, com mais minúcia, cada propriedade nas categorias.

Um objetivo específico deste trabalho também foi verificar se era possível encontrar na prática os aspectos relacionados à gestão da fraude identificados no *framework* teórico relatado. Assim, além das entrevistas com o banco de varejo e a associação de bancos foram encontradas reportagens veiculadas na internet sobre o assunto para elaboração do quadro de comparação da teoria com a prática. Esta comparação mostrou que nem todas as categorias e subcategorias teóricas puderam ser encontradas na prática, assim como não foram encontradas na prática possíveis categorias que não apareceram na análise da revisão bibliográfica.

A Teoria Fundamentada propõe que seja elaborada uma Categoria Central após análise de todo material disponível e da definição das categorias. Conclui-se que na fraude financeira externa a Categoria Central adequada seria a “Ação sobre a Crise Ininterrupta”, porque não existe perspectiva de eliminação total das fraudes, algumas podem ser mitigadas, porém outras novas vão surgir, o que remete e explica a escolha da epígrafe deste trabalho.

Espera-se que este trabalho contribua de alguma forma para a continuidade da discussão acadêmica do tema “Fraudes Financeiras” e que possa também contribuir com todas as Organizações, não somente bancos, que pretendam implementar ou ampliar programas de gestão da fraude.

7. LIMITAÇÕES E SUGESTÕES DE PESQUISAS FUTURAS

A falta de identificação de evidências práticas em algumas categorias propostas pode ter duas explicações: 1) nem todas as categorias e subcategorias estão em evidência na gestão da fraude ou 2) elas realmente existem, mas por alguma falha metodológica não foram identificadas. Uma forma de verificar esta limitação seria expandir a pesquisa e, a partir do *framework*, ser feita uma nova pesquisa com mais bancos.

A respeito deste tema muitas outras perguntas de pesquisa podem ser feitas. Uma sugestão de pesquisa seria a partir do modelo condicional/consequencial, também da Teoria Fundamentada, analisar a interação entre condições, resposta dos atores e as consequências resultantes. A figura 8 é a representação gráfica do que seria este modelo. Devemos imaginar que estas são bolas de bilhar, onde o movimento de uma delas pode alterar as condições das demais, ou seja, uma tomada de decisão a nível nacional relacionada ao fenômeno estudado pode alterar a posição regional e institucional.

Fonte: Adaptado de Strauss e Corbin (2008)

Figura 8 - O Modelo Condicional

No caso da fraude financeira a nível global ou internacional, poderia ser decidida uma cooperação entre países ou uma legislação única entre eles, poderiam surgir pesquisas multinacionais para redução das perdas com fraudes. Um país influente pode também alterar a disposição atual, por exemplo, nos Estados Unidos o combate ao *Cybercrime* tem recursos financeiros menores apenas que o terrorismo.

No âmbito nacional, como a nova lei contra crimes na internet pode alterar as relações entre as demais áreas? A aprovação desta lei terá impacto nos casos de fraude financeira em clientes de bancos? Será que a imagem atual dos bancos no Brasil tem influência por sofrerem tantas fraudes? Uma mudança desta imagem reduziria a incidência das fraudes?

Institucionalmente é possível dizer que a fraude afeta todos os bancos da mesma maneira? As diferenças de estruturas, controles e processos afetam a incidência da fraude externa?

Internamente, no nível sub-organizacional, a seleção, treinamento e clima organizacional podem afetar a incidência ou mitigar as fraudes? É possível analisar o perfil dos funcionários e evitar possíveis fraudadores em cargos de confiança?

Estas são apenas algumas perguntas ainda não respondidas a respeito da fraude e sua gestão. Com este trabalho procurou-se dar uma pequena contribuição para que o tema continue a ser discutido pelos acadêmicos da administração.

REFERÊNCIAS BIBLIOGRÁFICAS

ALLEN, L.; BALI, T. G. Cyclicalities in catastrophic and operational risk measurements. **Journal of Banking & Finance**, v. 31, n. 4, p. 1191-1235, April 2007.

ALMEIDA, M.C. **Auditoria**: um curso moderno e completo. São Paulo, Atlas, 1996.

ALMONTE, J.A. La function de seguridad en informática y en ambiente Internet in **Anais XII Congresso Latino Americano de Seguridad Bancária**. República Dominicana, p. 183-190, 1997.

ASSOCIAÇÃO BRASILEIRA DE BANCOS INTERNACIONAIS (ABBI) - FEBRABAN. Documento Consultivo “Função de Compliance”, 2009. **ABBI**. Disponível em: <http://www.abbi.com.br/download/funcaoodecompliance_09.pdf>. Acesso em: 12 ago. 2011

BANCO DO BRASIL S.A. Cheques Fraudulamente Impressos. **FELABAN**, Bogotá, 1980.

BASEL COMMITTEE ON BANKING SUPERVISION. **The New Basel Capital Accord**, 2001. Disponível em: <<http://www.bis.org/publ/bcbsca03.pdf>>. Acesso em: 28 fev. 2012.

BERGAMINI JR, S. Controles internos como um Instrumento de Governança Corporativa. **Revista do BNDES**, Rio de Janeiro, v.12, v.24, Dez/2005.

BOTELHO, F.N. O Brasil dos Crimes Eletrônicos, 2008. **Alice Ramos**. Disponível em <<http://www.aliceramos.com/view.asp?materia=1440>>. Acesso em: 28 fev. 2012.

BRICKEY, K. F. From Enron to WorldCom and Beyond: Life and Crime After Sarbanes-Oxley. **Washington University Law Quarterly**, Vol. 81, 2003.

BROWN, S. et al. Mandatory disclosure and operational risk: Evidence from hedge fund registration. **Journal of Finance**, v. 63, n. 6, p. 2785-2815, Dec 2008.

[CERT. Cartilha de Segurança para Internet, 2006. CERT. Disponível em <http://cartilha.cert.br/conceitos/sec7.html>](http://cartilha.cert.br/conceitos/sec7.html). Acesso em: 30 abr. de 2012.

CHAPELLE, A. et al. Practical methods for measuring and managing operational risk in the financial sector: A Clinical study. **Journal of Banking & Finance**, n. 32, p. 1040-1061, Oct 2007.

CLAB – IX Congresso Latino Americano de Automação Bancária. Os delitos por computador. **Revista Dados e Ideias**. Dez. 1982.

CLEMENTINO, M e NÓBREGA, E. Fraudadores Oportunistas: Sugestões para o combate in **Revista Brasileira de Risco e Seguro**, Rio de Janeiro, v.2, n.3, p.85-124, abr/set, 2006.

COMPTECHDOC. IP Masquerading. **COMPTECH**. Disponível em<<http://www.comptechdoc.org/independent/networking/guide/netipmasq.html>> . Acesso em: 29 abr. 2012.

CONSELHO MONETÁRIO NACIONAL(CMN). Resolução 3.380, 2006. Disponível em:<<https://www3.bcb.gov.br/normativo/detalharNormativo.do?method=detalharNormativo&N=106196825>>. Acesso em: 28 fev. 2012.

COQUE JR, M.A. **Base de Dados Interna FEBRABAN**. São Paulo, 2006

CORAZZA, G. **Os dilemas da supervisão bancária**. Indicadores Econômicos FEE. Disponível em: <<http://revistas.fee.tche.br/index.php/indicadores/article/view/1659/2027>>

CORDEIRO, P. R. El delito tecnico, algunos ejemplos y definiciones. **Revista FELABAN** /BOGOTA /(27)303-324 /7, 1977.

COSTA, A.P.P. **Casos de Fraudes Corporativas Financeiras: antecedentes, recursos substantivos e simbólicos relacionados**. Tese de Doutorado em Administração da FGV/SP, 176p., 2011.

DÍGITRO Tecnologia. Glossário Tecnológico na área de telecomunicações. **DÍGITRO**. Disponível em: <<http://www.digitro.com/pt/index.php/sala-imprensa/glossario>>. Acesso em: 30 abr. 2012

DOWNING, J. Fraud Prevention and Detection, **CHEEVERS and Company, INC**, 2010.

ERNEST & YOUNG. Fraud Detection Tools and Methods: Integrating fraud analytics into your work plans. **ERNEST & YOUNG**. Isaca, 2010.

FEDERAÇÃO BRASILEIRA DE BANCOS (FEBRABAN). **O setor bancário em números**. Disponível em <<http://www.febraban.org.br/>>. Acesso em: 17 out. 2011.

FEDERAÇÃO BRASILEIRA DE BANCOS (FEBRABAN). **Melhores práticas na gestão do risco operacional**, 2006. Disponível em<http://www.febraban.org.br/p5a_52gt34++5cv8_4466+ff145afbb52ffrtg33fe36455li5411pp+e/sitefebraban/GTMP_documento_finalago2006.pdf>. Acesso em: 28 fev. 2012.

FEDERATION DES EXPERTS COMPTABLES EUROPEENS (FEE). Good Practice in Tackling External Fraud. **Federation des Experts Comptables Europeens**, 2005.

FICH, E SHIHIVDASANIB, A. Financial fraud, director reputation, and shareholder wealth. **Journal of Financial Economics**. Vol. 86, Issue 2, November 2007.

FIGUEIREDO, R.P. **Gestão de riscos operacionais em instituições financeiras**, 2001. Dissertação de Mestrado em Administração - Universidade da Amazônia, Belém, 2001.

GINEL, F. Fraudes en Tarjetas de Crédito in Anais **XII Congresso Latino Americano de Seguridad Bancária**. República Dominicana, p. 183-190, 1997.

GLASER, B. G.; STRAUSS, A. **The discovery of grounded theory: strategies for qualitative research**. New York: Aldine Publishing Company, 1979.

GOLDEN, T.W. SKALAK, S. L. CLAYTON, M. **A Guide to Forensic Accounting Investigation**. ISBN-13: 978-0471469070, Edition: 1, Hardcover, 2006

GOTTSCHALK, P. Theories of financial crime. **Journal of Financial Crime**. Vol. 17. N°2. 2010.

GOTTSCHALK, P; SAETHER, H.S. Financial crime in business organizations: an empirical study. **Journal of Financial Crime**, vol. 18 Iss:1 pp. 76-92, 2011

HANSEN, R; THEMBILE, P; KILLRON, D. E CHIKANZA, S. **Fraud Prevention Handbook**. Pact, Zimbabwe, 2005

HOLLEIN, M. Fighting Financial Reporting Fraud: a Team Effort. **Financial Executive**. Publisher: Financial Executive Institute. Morristown, NJ 07961-1938, n°9, 2010.

HOUAISS. Dicionário Houaiss da Língua Portuguesa. **Instituto Antonio Houaiss**. Rio de Janeiro: Objetiva, 2001.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA (IBCG). Disponível em <<http://www.ibgc.org.br>>. Acesso em: 19 jun. 2011.

JARROW, R. Operational Risk. **Journal of Banking & Finance**, n. 32, p. 870-879, Sep 2007.

KPMG. A fraude no Brasil. Relatório de Pesquisa **KPMG**, São Paulo, 2009.

KRAMBIA-KAPARDIS, M. Fraud Victimization of Companies: The Cyprus Experience. **Journal of Financial Crime**. Vol. 10. N°2. 2010.

LAU, M. **Análise das Fraudes aplicadas sobre o ambiente Internet Banking**, dissertação de mestrado apresentada à Escola Politécnica da USP, sob orientação do Prof. Dr. Pedro Luís Próspero Sanchez, 2006.

LEGAL PRACTITIONER. A Guide To Computer Crime. **LEGAL PRACTITIONER**. Disponível em <<http://legal.practitioner.com/computer-crime/index.htm>>. Acesso em: 30 abr. 2012.

LINUX. IP Masquerading. **LINUX** Disponível em <http://br-linux.org/artigos/rede_ipmasq.htm>. Acesso em: 29 abr. 2012.

LOFTON, L. Fraud Prevention. **Mississippi Business Journal**. Vol. 32, No 32. August, 2010

LOZZANO, F.J. **Fraud and its Effects**, Whitley Penn, 2009.

MANTECCA, Paschoal. **Crimes Contra a Economia Popular e Sua Repressão**, São Paulo: Saraiva, 1985.

MATIAS, A.B. **Finanças Corporativas de Longo Prazo: Criação de Valor com Sustentabilidade Financeira**, São Paulo: Atlas, 2007.

MENDES, J.B.; LINS, L.S.; NEVES, M.R. Fraudes por computador. **Contabilidade Vista & Revista**. Belo Horizonte, v.8, n.1, p26-32, jun, 1997.

MOURA, P.S. Ditados e Fraude, 2010. **Portal Sapo**. Disponível em <<http://visao.sapo.pt/ditados--fraude=f573179#ixzz1psbijsQx>>. Acesso em: 28 fev. 2012.

NATIONAL AUDIT OFFICE .Tackling external fraud. **Good Practice Guide**. HM Treasury, UK, 2008.

NGAI, E. W. T. et al. The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. **Decision Support Systems**, v. 50, n. 3, p. 559-569, Feb 2011.

NORONHA, E.M. **Direito Penal**, 2º V. 7ª ED., P. 358, São Paulo: Saraiva, 1972.

NORTON SYMANTEC. Glossary. **NORTON**. Disponível em <http://br.norton.com/security_response/glossary>. Acesso em: 30 abr. de 2012.

NORTON SYMANTEC. O que são phishing e pharming? **SYMANTEC**. Disponível em <<http://service1.symantec.com/SUPPORT/INTER/ncointl.nsf/0/215a7595200ab15b88257204004cb008?OpenDocument>>. Acesso em: 30 abr. 2012.

PAIVA, M.A.L A firma digital e entidades de certificação. **Jus Navigandi**. Disponível em <<http://jus.com.br/revista/texto/2945/a-firma-digital-e-entidades-de-certificacao>>. Acesso em: 03 mai. 2012

PARODI, L. **Manual das Fraudes**. 2ª edição. São Paulo: Brasport, 2008.

PCI SECURITY STANDARDS COUNCIL. Skimming Prevention – Best Practices for Merchants. **PCI SECURITY STANDARDS COUNCIL**. Disponível em <https://www.pcisecuritystandards.org/documents/skimming_prevention_IS.pdf>. Acesso em: 30 abr. 2012.

PENTA UFRGS. IP Spoofing. **PENTA UFRGS**. Disponível em <<http://www.penta.ufrgs.br/gere96/segur/ipspooft.htm>>. Acesso em: 29 abr. 2012.

PIMENTA, E. Sistemas de informação: Redutores ou impulsionadores da fraude? **Portal Sapo**, 2009. Disponível em <<http://visao.sapo.pt/sistemas-de-informacao-redutores-ou-impulsionadores-da-fraude=f541728>>. Acesso em: 28 fev. 2012.

PRICEWATERHOUSECOOPERS (PWC) Cybercrime: protecting against the growing threat . **Global Economic Crime Survey**. PWC. UK, Nov/2011.

PRICEWATERHOUSECOOPERS (PWC). **Pesquisa de Crimes Econômicos**. São Paulo, Novembro/2009.

SANTOS, C.A.A.C. **As múltiplas faces dos crimes eletrônicos e dos fenômenos tecnológicos e seus reflexos no universo jurídico**. OAB/SP, 2009

SECURITY .A técnica do Man-in-the middle, 2012. **Security Hacker**. Disponível em <<http://www.securityhacker.org/artigos/item/a-tecnica-man-in-the-middle>>. Acesso em 30 de abril de 2012.

SERASA. Indicador Serasa Experian de Cheques sem fundos. **Serasa Experian**. Disponível em <http://www.serasaexperian.com.br/release/indicadores/cheques_devolvidos.htm>. Acesso em: 04 nov. 2011.

SERASA. Serasa Experian da dicas para o comércio evitar prejuízo com fraudes, 2011. **Serasa Experian**. Disponível em <<http://www.nominuto.com/noticias/economia/serasa-experian-da-dicas-para-o-comercio-evitar-prejuizo-com-fraudes/82998/>>. Acesso em: 28 fev. 2012

ROBB, G. White-Collar Crime in Modern England: Financial Fraud and Business Morality, 1845-1929. **Business History Review**. Boston, vol. 67, Iss. 4, winter 1993.

STRAUSS, A. CORBIN, J. **Pesquisa qualitativa - Técnicas e procedimentos para o desenvolvimento de teoria fundamentada**. São Paulo: Artmed, 2008.

TECHENET. Como não ser enganado na internet, 2012. **TECHENET**. Disponível em <http://www.techenet.com/2012/03/como-nao-ser-enganado-na-internet/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+Technet-blogsobretecnologiaeinternet+%28TECH%26NET+-+blog+sobre+tecnologia+e+internet%29> Acesso em: 28 fev. 2012.

UNISYS SECURITY INDEX. Brazil Security Index Report. **UNISYS** Disponível em <<http://www.unisyssecurityindex.com/usi/brazil/reportshttp://marcosassi.com.br/fraudes-de-r-900-mi-estimulam-bancos-a-investir-em-seguranca>>. Acesso em: 20 mar 2012.

VALORECONOMICO. De olhos bem abertos dentro das empresas. **VALOR ECONOMICO** Disponível em<<http://www.valor.com.br/carreira/2496426/de-olhos-bem-abertos-dentro-das-empresas>>. Acesso em: 28 fev. 2012.

VALORECONOMICO. Cresce o número de fraudes realizadas por funcionários. **VALOR ECONOMICO**. Disponível em

<<http://www.valor.com.br/carreira/2496424/cresce-o-numero-de-fraudes-realizadas-por-funcionarios>>. Acesso em: 28 fev. 2012.

VELEZ ANGEL, A. Defraudações Bancárias por falhas operativas e sua prevenção in **Seminário Latino Americano de Segurança e Proteção de Bancos**. São Paulo, 1985.

YIN, R. **Estudo de Caso: planejamento e métodos**. 10º Ed. 205p .Porto Alegre: Bookman, 2010,

ZAGARIS, B. and MacDonald, S. B. Money laundering, financial fraud, and technology: The perils of an instantaneous economy. **The George Washington Journal of International Law and Economics**, 26(1), 61, 1992.

2. APENDICE A

O Apêndice A refere-se ao roteiro utilizado durante as visitas. As respostas não foram gravadas, mas os entrevistados receberam o relato da entrevista para validação.

GESTÃO DA FRAUDE FINANCEIRA EXTERNA.

1. Quando foi percebida a necessidade de se ter gerir a fraude? Quando surgiu sua área?
2. Quais são as suas atribuições específicas? Quais são as suas atividades e da sua área?
3. Para esta organização qual é o conceito de fraudes financeiras? O que é considerado uma fraude financeira em clientes? Quantos tipos de fraudes financeiras vocês consideram?
4. Fraude financeira é risco operacional? Se sim, em que área se localiza: de processos, de pessoas, de tecnologia ou de eventos externos? Exemplos.
5. Que área cuida de riscos operacionais?
6. Existe algum material bibliográfico utilizado?
7. O que o senhor considera fundamental em termos de segurança anti-fraude?
8. Quantos funcionários trabalham para garantir a segurança das operações?
9. De que maneira é feito o treinamento destes funcionários? Existem cursos efetivos no mercado? Existem cursos oferecidos internamente?
10. Qual tem sido resultado alcançado? O volume nominal e/ou relativo de fraudes tem recuado ou aumentado nos últimos 10 anos?
11. Vocês realizam a Auditoria de Processamento de Dados? Interna ou Externa?
12. O conhecimento gerado sobre Gestão de Segurança durante estes anos está registrado?

13. Qual tecnologia empregada? Existem sistemas desenvolvidos no Banco para segurança? Quais são os programas utilizados para auxílio na detecção e prevenção da fraude contra clientes? Existe um modelo de prevenção e detecção de fraude?
14. Como o banco realiza investimentos na área? Qual montante anual?
15. Existe comunicação com outros bancos a respeito do tema fraude contra clientes? Existe um banco de dados interbancário sobre fraudes contra clientes? Já foi verificado que um mesmo fraudador aplica o mesmo golpe em mais de um banco?
16. O risco de fraude tecnológica é mais preocupante que o risco de fraude envolvendo erro de pessoal?
17. Todo o público interno conhece as práticas de segurança de informação? De que maneira são divulgadas? Existe alguma maneira de se certificar que a divulgação atingiu o objetivo?
18. Os seus produtos/serviços tem alguma característica anti-fraude que os difere dos demais e os tornam mais difíceis de fraudar?
19. Já se verificou funcionários fraudando clientes? Como o caso foi tratado?
20. Existe a prática de se verificar constantemente quais são as possibilidades de fraudar os clientes deste Banco? (Por exemplo, empresa contrata os serviços de um hacker para achar brechas em seu sistema)
21. Existe um tempo médio para um dispositivo de segurança ser violado? De quanto em quanto tempo são revistos os métodos de identificação de clientes?
22. O banco de dados referente aos clientes que pertencem a um banco é um recurso valioso. Existe seguro para estas informações?
23. No Brasil não existe uma legislação específica para estes crimes feitos pela internet, mas está em tramitação a tipificação de crimes eletrônicos. De que maneira isto pode influenciar na ocorrência deste tipo fraude?

24. As medidas de controle de segurança podem reduzir os ganhos do Banco? Por exemplo, um sistema de identificação de padrões bloqueia uma compra verdadeira por cartão de crédito. Qual o percentual de bloqueios efetivos? De alguma maneira é medido o impacto negativo ao se bloquear um cliente realizando uma transação verdadeira.