UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
ESCOLA DE ENGENHARIA
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA DE PRODUÇÃO

JOÃO LUÍS SALES DE AZEVEDO

LEVANTAMENTO DE REQUISITOS PARA UM PROCESSO DE PREVENÇÃO A FRAUDES ELETRÔNICAS

Porto Alegre,
2014

JOÃO LUÍS SALES DE AZEVEDO

LEVANTAMENTO DE REQUISITOS PARA UM PROCESSO DE PREVENÇÃO A FRAUDES ELETRÔNICAS

Dissertação submetida ao Programa de Pós-Graduação em Engenharia de Produção da Universidade Federal do Rio Grande do Sul como requisito parcial à obtenção do título de Mestre em Engenharia de Produção, modalidade Profissional, na área de concentração em Sistemas de Qualidade.

Orientador: Profª Claudia Medianeira Cruz Rodrigues, Drª.

Porto Alegre,

2014

JOÃO LUÍS SALES DE AZEVEDO

LEVANTAMENTO DE REQUISITOS PARA UM PROCESSO DE PREVENÇÃO A FRAUDES ELETRÔNICAS

Esta dissertação foi julgada adequada para a obtenção do título de Mestre em Engenharia de Produção na modalidade Acadêmica e aprovada em sua forma final pelo Orientador e pela Banca Examinadora designada pelo Programa de Pós-Graduação em Engenharia de Produção da Universidade Federal do Rio Grande do Sul.

_____

Profª. Cláudia Medianeira Cruz Rodrigues, Drª.
PPGEP/UFRGS
Orientadora

_____

Prof. José Luis Duarte Ribeiro, Dr.
Coordenador PPGEP/UFRGS

Banca Examinadora:

Professor Marcelo Cortimiglia, Dr. (PPGEP/UFRGS)

Professor Diego Fettermann, *Dr.* (UESC/BA)

Professora Miriam Borchardt, Dr. (UNISINOS)

Dedicatória

Dedico este trabalho a memória de meu pai:

José Moacir Azevedo.

AGRADECIMENTOS

Um agradecimento mais que especial para a minha mãe, que mesmo com o recente falecimento de meu pai entendeu minha ausência nas ultimas semanas e manteve o suporte para que eu pudesse me manter focado no desenvolvimento deste trabalho.

Agradeço também ao meu pai, que infelizmente nos deixou antes que eu pudesse agradecer pessoalmente pelo apoio prestado ao longo destes dois anos de mestrado.

Agradeço aos meus colegas de trabalho que contribuiram significativamente para a execução desta dissertação.

Agradeço as professoras Cláudia Rodrigues e Marcia Echeveste pelo apoio e direcionamentos prestados para o desenvolvimento deste trabalho.

AZEVEDO, J. L. S. **LEVANTAMENTO DE REQUISITOS PARA UM PROCESSO DE PREVENÇÃO A FRAUDES ELETRÔNICAS.** 2014. Dissertação de Mestrado Profissional (Engenharia de produção) – Universidade Federal do Rio Grande do Sul.

RESUMO

O rumo que o mercado financeiro está tomando ao oferecer canais eletrônicos de atendimento a seus clientes traz consigo uma significativa preocupação com a segurança dos canais eletrônicos: o crescente ataque de quadrilhas fraudadoras. Neste sentido, os valores movimentados para aumentar a segurança dos canais e as perdas resultantes de ataques criminosos desta natureza exige a necessidade de disponibilizar serviços eletrônicos mais robustos e confiáveis. O presente trabalho tem como objetivo principal o levantamento de requisitos para o um processo de prevenção a fraudes eletrônicas em instituições financeiras. Para isto, o trabalho se propõe a apresentar um (i) estudo de requisitos da qualidade no processo de prevenção a fraudes eletrônicas em uma instituição financeira e (ii) a utilização de métodos qualitativos para identificação de requisitos em um processo de prevenção a fraudes eletrônicas. A principal contribuição deste trabalho é a apresentação de uma relação de requisitos, técnicos e funcionais, necessários para o estabelecimento e monitoramento de um processo de prevenção a fraudes eletrônicas para instituições financeiras que ofertam canais eletrônicos a seus clientes.

Palavras-chave: Fraudes, Fraudes eletrônicas, Requisitos

AZEVEDO, J. L. S. **LEVANTAMENTO DE REQUISITOS PARA UM PROCESSO DE PREVENÇÃO A FRAUDES ELETRÔNICAS.** 2014. Dissertação de Mestrado Profissional (Engenharia de produção) – Universidade Federal do Rio Grande do Sul.

ABSTRACT

The direction that the financial market is taking to provide electronic channels for customer services brings along a significant concern with the security of electronic channels: the growing number of attacks by fraudsters. In this sense, values mobilized to increase the security of such channels and with the losses resulting from criminal attacks of this nature require the need to provide stronger and more reliable electronic services. The main objective of the present study is the identification of requirements for a process of electronic fraud prevention in financial institutions. For this purpose, the work is proposed to submit a (i) study of quality requirements in case of electronic fraud prevention at a financial institution and (ii) the use of qualitative methods for identification of requirements into a process of electronic fraud prevention. The main contribution of this study is the presentation of an inventory of functional and technical requirements, necessary for the establishment and monitoring of a process of electronic fraud prevention for financial institutions, which provide electronic channels for their clients.

Keywords: Fraud, Electronic Frauds, Requirements

LISTA DE FIGURAS

Figura 1 - Framework de pesquisa de mercado 18
Figura 2 - Processo de Prevenção a Fraudes 23
Figura 3 - Árvore da Qualidade 25
Figura 4 - Análise Multicriterial 26
Figura 5 - Desdobramento da Função Qualidade 29
Figura 6 - Roteiro de Questões 41
Figura 7 - Situação dos Critérios 47
Figura 8 - Visão geral 53

SUMÁRIO

I INTRODUÇÃO 11
1.1 Objetivo Geral 12
1.2 Objetivos Específicos 13
1.3 Estrutura da Dissertação 13
II – ARTIGO 1: REQUISITOS DA QUALIDADE NO PROCESSO DE PREVENÇÃO A FRAUDES ELETRÔNICAS EM UMA INSTITUIÇÃO FINANCEIRA 14
Resumo 14
1 Introdução 14
2 Fraudes Eletrônicas 16
3 Procedimentos Metodológicos 18
3.1 Modelo de Pesquisa de Melhoria no Processo de Prevenção de Fraudes 19
3.1.1 Levantamento de Requisitos 19
3.1.2 Levantamento de Indicadores e Matriz da Qualidade 21
3.1.3 Levantamento de Serviços e Matriz dos Serviços 22
3.1.4 Levantamento de Recursos e Matriz de Recursos 23
3.2 Processo de Prevenção a Fraudes 23
4 Resultados e Discussões 24
4.1 Levantamento e Priorização dos Requisitos 24
4.2 Desdobramento da Qualidade 26
4.3 Desdobramento dos Serviços 27
4.4 Desdobramento dos Recursos 28
5 Considerações Finais 30
Referências 31
II – ARTIGO 2: A UTILIZAÇÃO DE MÉTODOS QUALITATIVOS PARA IDENTIFICAÇÃO DE REQUISITOS EM UM PROCESSO DE PREVENÇÃO A FRAUDES: ESTUDO DE CASO ENVOLVENDO ESPECIALISTAS DE UMA INSTITUIÇÃO FINANCEIRA 35
1 Introdução 35
2 Referencial Teórico 36
2.1 Serviços Bancários 36
2.2 Processo de Prevenção a Fraudes Eletrônicas 38

3 Procedimentos Metodológicos 40
3.1 Cenário de Pesquisa 42
3.2 Cenário de Aplicação 43
4 Resultados e Discussões 43
4.1 Indicadores 44
4.2 Serviços 45
4.3 Recursos 46
4.4 Visão Geral 47
5 Considerações Finais 48
Referências 49
IV CONCLUSÕES 52

I INTRODUÇÃO

O avanço dos chamados *e-commerces* e *e-services* permitiram que usuários transacionem sem a necessidade de interação física. A *internet* facilitou a aquisição de produtos e serviços através de meios eletrônicos, tais como: *e-mails, downloads,* portais *web,* etc. (ALFURAIH 2002).

No território nacional a adesão aos meios eletrônicos para realização de transações financeiras toma proporções significativas. A Federação Brasileira de Bancos (FEBRABAN) aponta que, no Brasil, há um aumento no número de transações em *Internet Banking* e *Point of Sales* (POS) de aproximadamente 25% ao ano. Há uma tendência mundial de mercado adotar os canais eletrônicos não só para aquisição de bens e serviços, mas também, para gerenciar a conta bancária e investimentos. Benaroch (2010) corrobora com essa ideia quando mostra que de 2001 a 2006 o aumento de usuários de *Internet Banking* foi de mais de 10 milhões somente no Reino Unido, refletindo um acréscimo de 174% sobre o número inicial de usuários. Um exemplo de que o mercado está migrando do atendimento clássico, realizado através do contato face-a-face, para as tecnologias do tipo *self-service* tipicamente eletrônicas, conforme mencionou Ericksson e Nilsson (2007), é o resultado da pesquisa realizada pelo *ICT Statistics Newslog* (2010) onde indica que o número de usuários de *mobile banking* no mundo é previsto que cresça de 55 milhões em 2009 para 894 milhões em 2015. Mahmood (2003) cita os ATM's (*automated teller machines*) como os precursores desta quebra dos paradigmas de atendimento face-a-face nas instituições financeiras.

Dentro deste contexto, na qual o contato dos clientes fica longe das dependências das instituições financeiras, surgem as quadrilhas que aproveitam esse rumo a que o mercado está se dirigindo para promover golpes e fraudes em canais eletrônicos. Dados da FEBRABAN estimam que as perdas causadas por fraudes em canais eletrônicos às instituições financeiras alcançariam o montante de R$ 1,5 bilhões no ano de 2012. Ibbett (2007) mostra que atualmente fraudes eletrônicas são um problema amplamente difundido e que geralmente custa aos empresários algo entre 3 e 8% de sua renda anual, além de comprometer sua reputação e a confiança na relação com o usuário de serviços eletrônicos. Ainda, Ibbet (2007) estima que este montante representa cerca de U$D 44 bilhões no mundo dos negócios virtuais.

Frente a esses números fica evidente a necessidade de estabelecer um processo que atue sobre este crime de maneira preventiva principalmente as instituições financeiras e seus

clientes que, segundo Ghosh (2010), estão no grupo dos mais visados pelas quadrilhas quando se trata de fraudes eletrônicas.

Para estudar o processo de prevenção a fraudes eletrônicas é necessário estabelecer claramente os requisitos necessários para evitar as falhas do ponto de vista do cliente e da instituição levando em consideração os recursos de tecnologia da informação disponíveis. A etapa de levantamento dos requisitos alicerça o estabelecimento do processo, pois estes direcionarão os trabalhos seguintes de identificação dos principais procedimentos, recursos e métricas a serem utilizadas. Young (2004) corrobora com essa ideia quando afirma que um requisito é um atributo necessário em um sistema, uma declaração que identifica um recurso, característica ou fator de qualidade de um sistema em ordem para ter valor e utilidade para um cliente ou usuário. Partindo desta prerrogativa pode-se afirmar que a identificação das necessidades dos clientes consumidores do produto ou serviço deve ser etapa fundamental no estabelecimento de um processo ou produto. Garantir que todos os requisitos, ou os mais importantes, serão considerados é parte fundamental e mandatória do processo de desenvolvimento do serviço. Os requisitos são importantes porque fornecem a base para todo o trabalho de desenvolvimento que segue. Uma vez que os requisitos são definidos, os desenvolvedores têm a possibilidade de iniciar outros trabalhos técnicos: projeto de sistema, desenvolvimento, testes, implementação e operação (YOUNG, 2004). Estes requisitos devem ser elicitados e priorizados para associar a processos e recursos na manutenção e eficiência de todo o sistema de prevenção.

1.1 Objetivo Geral

Este trabalho se propõe a apresentar um levantamento de requisitos para um processo de prevenção a fraudes eletrônicas em instituições financeiras. Como suporte para o levantamento foram utilizados o QFD (Desdobramento da Função Qualidade), o qual é um método sistemático para garantir que o desenvolvimento das características e especificações de um produto, bem como o desenvolvimento de metodologias, processo e controles, sejam orientados pela necessidade do consumidor (EUREKA; RYAN, 1992), integrado ao AHP (*Analytic Hierarchy Process*), método de análise multicriterial que usa a hierarquia para representar um problema de decisão (SAATY, 1991) e a técnica denominada grupo focal que, segundo Borges e Santos (2005), é uma dentre as várias modalidades disponíveis de entrevista grupal e/ou grupo de discussão. Os participantes dialogam sobre um tema particular, ao receberem estímulos apropriados para o debate (RESSEL et Al., 2008).

1.2 Objetivos Específicos

Como objetivos específicos, listam-se:

I) Compreender a importância do estabelecimento de um processo de prevenção a fraudes eletrônicas as instituições financeiras

II) Identificar requisitos para um processo de prevenção a fraudes eletrônicas em instituições financeiras

1.3 Estrutura da Dissertação

A organização deste trabalho apresenta o resultado de duas pesquisas, independentes entre si, mas que em conjunto contribuem para o levantamento de requisitos para um processo de prevenção a fraudes eletrônicas.

Os procedimentos metodológicos e as fontes de dados também variam em cada artigo, combinando ferramentas e métodos de aplicação. As pesquisas serão apresentadas na seguinte ordem:

- ARTIGO I: Estudo de requisitos da qualidade no processo de prevenção a fraudes eletrônicas em uma instituição financeira; e
- ARTIGO II: A utilização de métodos qualitativos para identificação de requisitos em um processo de prevenção a fraudes eletrônicas: Estudo de caso envolvendo especialistas de uma instituição financeira.

Ao final será apresentado as discussões e conclusão geral da pesquisa, levando em conta os achados de cada artigo considerando as implicações práticas das pesquisas.

II – ARTIGO 1: REQUISITOS DA QUALIDADE NO PROCESSO DE PREVENÇÃO A FRAUDES ELETRÔNICAS EM UMA INSTITUIÇÃO FINANCEIRA

Resumo

Os serviços de transações monetárias vem se tornando cada vez mais virtuais o que reforça a preocupação com segurança de dados referentes a operações financeiras. Neste sentido, as instituições tem investido altos valores para evitar fraudes eletrônicas uma vez que é crescente o número de ataques de quadrilhas especializadas nesse tipo de fraude. A necessidade de disponibilizar serviços eletrônicos mais robustos e confiáveis, além de monitorar eficientemente o comportamento fraudulento, desafia a segurança dos canais e a imagem da instituição financeira diante do mercado que deve constantemente criar novas formas de prevenção na medida em que novos mecanismos de fraudes são criados. Com o objetivo de identificar requisitos de um processo de tratamento e prevenção de fraudes eletrônicas de uma instituição financeira visando redução do impacto de perdas por fraudes eletrônicas por meio do uso de métodos de melhoria de processo da qualidade de manufatura aplicados ao processo de prevenção de fraudes eletrônicas, este trabalho apresenta um método para implementar e priorizar requisitos no processo de prevenção de fraudes utilizando técnicas conhecidas na qualidade de forma integrada como AHP (*Analytic Hierarchy Process*) para priorização e do QFD (*Quality Function Deployment*) para desdobramento dos requisitos em processos e recursos. Os resultados da aplicação do método apontam que a recuperação de valores fraudados e a identificação de transações fraudulentas são percebidos como pontos de melhoria na percepção do usuário na prevenção a fraudes, e que o contínuo desenvolvimento dos especialistas em fraudes, juntamente com o aprimoramento dos serviços de contato com o cliente e geração/atualização de regras de monitoramento contribuem significativamente para atingir os requisitos de prevenção a fraudes eletrônicas.

Palavras-chave: Fraude eletrônica; Pesquisa de Marketing; QFD; AHP

1 Introdução

Nos últimos anos a população mundial está cada vez mais utilizando de meios eletrônicos para interagir com as instituições financeiras, como exemplo o *Internet Banking.* Benaroch (2010) mostra que de 2001 a 2006 o aumento de usuários de *Internet Banking* foi de mais de 10 milhões somente no Reino Unido, refletindo um acréscimo de 174% sobre o número inicial de usuários. Outro exemplo é o apontado pela *ICT Statistics Newslog* (2010) onde indica que o número de usuários de *mobile banking* no mundo é previsto que cresça de 55 milhões em 2009 para 894 milhões em 2015. Ericksson e Nilsson (2007) apontaram uma tendência do atendimento clássico, realizado através do contato face-a-face, ser suplantado por tecnologias do tipo *self-service* tipicamente eletrônicas. A Federação Brasileira de Bancos (FEBRABAN) demonstra que no Brasil há um aumento no número de transações em *Internet Banking* e *Point of Sales* (POS) de aproximadamente 25% ao ano.

Um dos primeiros canais a romper esta barreira do contato direto entre clientes e instituições financeiras foi a disponibilização de *automated teller machines* (ATM's) para atendimentos básicos, como: saques, depósitos, transferências, pagamentos entre outros (MAHMOOD, 2013). Neste sentido, os canais eletrônicos tornaram as instituições financeiras mais próximas e, ao mesmo tempo, mais distantes dos clientes. A comodidade em poder usufruir de serviços financeiros através de aparelhos eletrônicos ligados a rede mundial de computadores vem impactando o modelo de negócio financeiro.

Dentro deste contexto, na qual o contato dos clientes fica longe das dependências das instituições financeiras, surgem as quadrilhas que promovem fraudes em canais eletrônicos visando se aproveitar deste rumo que o mercado está tomando para aplicar golpes e ganhar dinheiro de maneira ilícita. Dados da FEBRABAN estimam que as perdas causadas por fraudes em canais eletrônicos às instituições financeiras alcançariam o montante de R$ 1,5 bilhões no ano de 2012. Ibbett (2007) mostra que atualmente fraudes eletrônicas são um problema amplamente difundido e que geralmente custa aos empresários algo entre 3 e 8% de sua renda anual, além de comprometer sua reputação e a confiança na relação com o usuário de serviços eletrônicos. Ainda, Ibbet (2007) estima que este montante representa cerca de U$D 44 bilhões no mundo dos negócios virtuais.

É neste cenário que surge a necessidade de estabelecer um processo que atue de maneira proativa sobre este crime que afeta a sociedade como um todo. As instituições financeiras e seus clientes são os mais visados pelas quadrilhas quando se trata de fraudes eletrônicas. Para estudar o processo de prevenção a fraudes é necessário estabelecer claramente os requisitos necessários para evitar as falhas do ponto de vista do cliente e da instituição levando em consideração os recursos de tecnologia da informação disponíveis. Estes requisitos devem ser elicitados e priorizados para associar a processos e recursos na manutenção e eficiência de todo o sistema de prevenção. Este artigo propõe identificar requisitos de um processo de tratamento e prevenção de fraudes eletrônicas de uma instituição financeira visando redução do impacto de perdas por fraudes eletrônicas por meio do uso de métodos de melhoria de processo da qualidade de manufatura aplicados ao processo de prevenção de fraudes eletrônicas.

Como suporte a este estudo foi utilizado o QFD (Quality Function Deployment), o qual é um método sistemático para garantir que o desenvolvimento das características e especificações de um produto, bem como o desenvolvimento de metodologias, processo e controles, sejam orientados pela necessidade do consumidor (EUREKA; RYAN, 1992),

integrado ao AHP (Analytic Hierarchy Process), método de análise multicriterial que usa a hierarquia para representar um problema de decisão (SAATY, 1991). Uma aplicação integrada do QFD e do AHP permite obter as vantagens de ambos os métodos (Fiorenzo, 2001). O QFD possui um histórico de sucesso quanto a sua utilização integrada ao AHP para estabelecimento e priorização de requisitos (Moisiadis, 2002), tal afirmativa pode ser constatada nos trabalhos de Partovia e Epperly (1999), Partovi e Corredoira (2002), Bhattacharya et al. (2005) e Hanumaiah et al. (2006)

A organização do artigo acontece da seguinte maneira: a seção 1 apresenta a introdução com o objetivo geral do trabalho; após a seção 2 apresenta o referencial teórico sobre Fraudes Eletrônicas. A seção 3 evidencia os procedimentos metodológicos contemplando o levantamento de requisitos, indicadores, procedimentos e recursos utilizados em um processo de prevenção a fraudes eletrônicas, bem como, uma apresentação do processo estudado. A seção 4 ilustra os resultados do trabalho, seguida da seção 5 com as considerações finais.

2 Fraudes Eletrônicas

Definido de maneira ampla, fraudes eletrônicas tratam-se de crimes virtuais, ou seja, qualquer ato ilegal envolvendo um sistema computacional, aplicação ou transmissão de dados, onde a vítima sofre ou sofreu perdas. Neste amplo espectro inclui-se acesso não autorizado ou roubo de informações proprietárias (MILLS, 2006). Uma efetiva metodologia para detecção de fraudes pode ajudar organizações a oferecer a seus consumidores um ambiente *online* seguro e confiável que estimule a lealdade aos seus serviços. Portanto, é essencial que tecnologias de prevenção e métodos de detecção de fraude sejam continuamente desenvolvidas e atualizadas (PROVOST, 2002).

O gerenciamento de fraudes eletrônicas têm uma ampla área de atuação que geralmente engloba todos os aspectos de detecção, gestão e investigação de qualquer tentativa, com sucesso ou não, de roubo através de enganação ou violação intencional de serviços oferecidos por meio eletrônico (JACOBS, 2002). A gestão do processo de detecção de fraudes depende necessariamente da natureza e ramo do negócio, porém, de maneira geral, existem dois métodos para detecção de fraudes: análise absoluta e análise diferencial. A análise absoluta busca identificar padrões de ataques anteriores para identificar novas ocorrências destes ataques, enquanto que a análise diferencial procura por desvios no padrão de utilização do usuário (MOREAU, 1996). Ambos os métodos de detecção de fraude estão

suscetíveis a erros. Com relação aos potenciais erros na análise de detecção de fraudes, seja ela diferencial ou absoluta, estes podem ser de dois tipos: falsos positivos e falsos negativos. Um falso positivo ocorre quando um alarme é gerado embora não há um ataque. Em contrapartida, um falso negativo acontece quando um alarme não é gerado apesar do ataque (ARVIDSON, 2003).

Bella (2008) acrescenta que um processo de detecção de fraudes apresenta muitos desafios, dentre os quais estão o grande número de erros de detecção que podem ser gerados por um sistema de monitoramento de fraudes e o potencial desgaste da privacidade do usuário do serviço. Neste mesmo contexto, Bella (2008) enfatiza a questão dos falsos negativos quando afirma que, como uma fonte de perda de receitas, falsos negativos são de longe mais ameaçadores para o empresário uma vez que o valor fraudado pode ser muito superior ao trabalho despendido por um analista ao tratar um falso positivo.

As vítimas típicas de fraudes eletrônicas são consumidores, instituições financeiras e prestadoras de serviços de comunicação e empresas que oferecem serviços e venda de bens de consumo via rede internacional de computadores (GHOSH, 2010).

Dada a importância do tema, para as instituições financeiras, o Banco Central do Brasil (BACEN) determina que seja estabelecido uma estrutura de tratamento de risco operacional que contemple eventos de fraude interna e fraude externa e define como risco operacional a possibilidade de ocorrência de perdas resultantes de falha, deficiência ou inadequação de processos internos, pessoas e sistemas, ou de eventos externos (BACEN, Resolução nº 3380 Art. 2º).

As contribuições acadêmicas relacionadas à prevenção e detecção de fraudes eletrônicas no meio financeiro trazem a necessidade de antecipar as iniciativas fraudulentas. Detecção de comportamento fraudulento em meio a grandes quantidades de informação tornou-se uma extensa área de pesquisa objetivando minimizar os efeitos da fraude no mercado de serviços financeiros (KOU ET AL.,2004).

Contribuições neste sentido podem ser verificadas em estudos relacionados à detecção de fraudes em Cartão de Crédito (ALESKEROV, FREISLEBEN; RAO, 1997; BRAUSE; LANGSDORF; HEPP, 1999; GHOSH; REILLY, 1994; MAES ET AL.; MANDERICK, 2002), telecomunicações (BOUKERCHE; NOTARE, 2000; BURGE ET AL., 1997) e seguros (VIAENE; DEDENE; DERRIG, 2005) que utilizam de cenários previamente experimentados e conhecidos de fraude para prover maior eficácia na detecção de transações fraudulentas; proposição de um Sistema de Gestão de Fraudes baseado em *Internet Protocol* (IP) aliado ao

uso de Redes Neurais (BELLA, 2008) e, proposição de uso de métodos estatísticos para detecção de desvios de comportamento na utilização de cartões de crédito, tais como *data mining* (SÁNCHEZ, 2009). Também é possível encontrar na literatura trabalhos voltados à prevenção de fraudes aplicada na autenticação de transações. Tassabehhji (2012) apresenta as vantagens da aplicação de reconhecimento biométrico para autenticar transações financeiras realizadas em canais eletrônicos.

As publicações tornam evidente a necessidade de definir métodos e processos para não somente identificar eventos de fraude nos canais eletrônicos, assim como evitar que tais eventos aconteçam.

3 Procedimentos Metodológicos

Os procedimentos metodológicos foram divididos em duas seções: a primeira com o objetivo de apresentar os passos da aplicação do *framework* utilizado para o levantamento dos requisitos, detalhando-o de maneira a identificar cada etapa utilizada (Figura 1), e a segunda seção apresentando o processo de prevenção a fraudes onde o método foi aplicado.

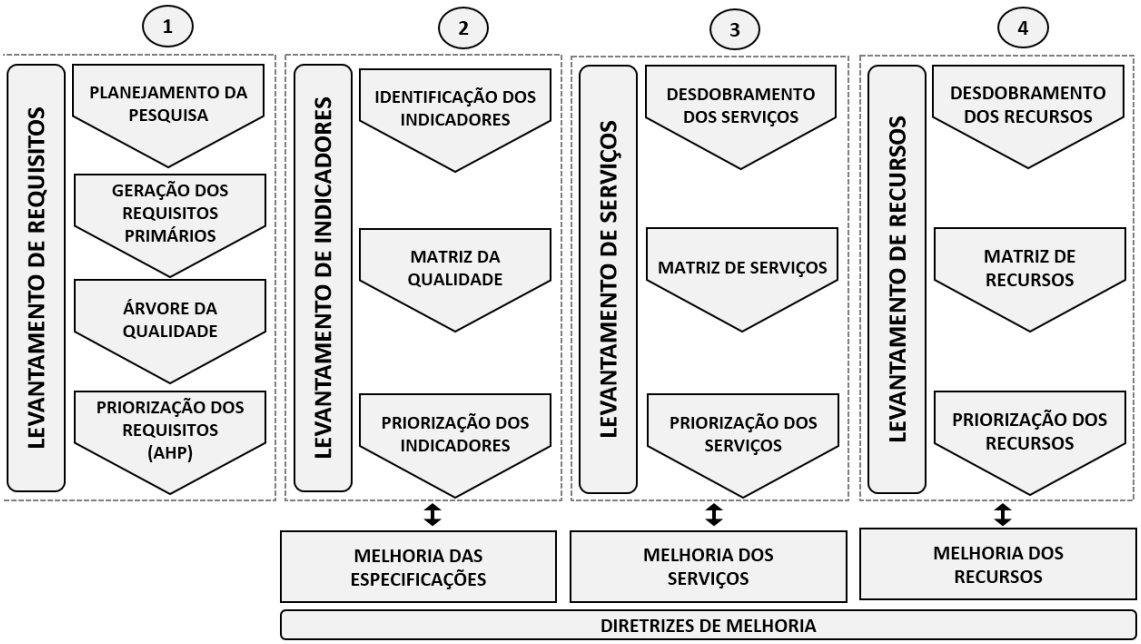

Figura 1 - Framework de pesquisa de mercado

Fonte: Adaptado de Ribeiro et Al. (2000)

3.1 Modelo de Pesquisa de Melhoria no Processo de Prevenção de Fraudes

O *framework* de pesquisa utilizado para o estudo de requisitos da qualidade do processo de prevenção a fraudes é descrito respeitando as etapas em nível macro, conforme a Figura 1. O *framework* contempla as etapas de (i) levantamento de requisitos, (ii) levantamento de indicadores, (iii) levantamento de serviços e (iv) levantamento de recursos.

Não será abordado neste trabalho o planejamento da qualidade contendo as etapas de melhoria estabelecidas no framework de pesquisa de mercado, ficando restrito ao levantamento de requisitos para o processo de prevenção a fraudes eletrônicas.

3.1.1 Levantamento de Requisitos

Como método de coleta de dados foram utilizadas técnicas tipicamente de pesquisa de mercado com o objetivo de identificar os requisitos da qualidade demandados pelos clientes, seguindo o modelo sugerido por Ribeiro et al. (2000). O **Planejamento da pesquisa** prevê as seguintes etapas: (i) Identificação do problema e objetivos da pesquisa, (ii) Planejamento da Pesquisa e, (iii) Questionário aberto e árvore da qualidade demandada, seguido da aplicação do QFD. No entanto, adaptações do modelo foram realizadas a fim de otimizar a aplicação do método, garantindo a integridade dos objetivos de cada etapa. Uma das adaptações foi a aplicação combinada do AHP ao QFD com o objetivo de melhor hierarquizar os requisitos da qualidade demandada mais relevantes para o processo

O ponto de partida para o desenvolvimento do trabalho foi a **geração dos requisitos primários** cuja premissa foi abordar de maneira direta e indireta os requisitos que fazem de um processo de prevenção a fraudes eletrônicas ser adequado para uma instituição financeira. Esta etapa do trabalho envolve não somente a consulta, através de pesquisa direta a profissionais ligados a prevenção e tratamento de fraudes eletrônicas, mas também, buscar em fontes secundárias subsídios para incrementar a lista de requisitos funcionais do processo. A etapa de geração dos requisitos primários alicerça o estabelecimento do processo, pois estes direcionarão os trabalhos seguintes de identificação dos principais serviços, recursos e métricas a serem utilizadas. Para tanto, fontes primárias e secundárias foram utilizadas para identificar os requisitos declarados e não declarados do processo. Como fontes secundárias foram utilizadas: informações advindas de produções acadêmicas no campo de fraudes eletrônicas e segurança da informação, *benchmarking* com outras instituições financeiras,

reportagens e documentários produzidos pela mídia nacional e internacional, informações privilegiadas junto à polícia civil e exigências de instituições regulamentadoras do mercado financeiro. Como fontes primárias de pesquisa foram abordados especialistas ligados ao tratamento e prevenção de fraudes eletrônicas. Tais especialistas foram expostos a uma sequência de perguntas visando coletar informações técnicas, que posteriormente, seriam utilizadas para mapear os requisitos do processo. Ao todo foram entrevistados oito profissionais distribuídos nos cargos de Gerente de Tratamento e Prevenção a Fraudes, Coordenador de Tratamento de Fraudes, Coordenador de Monitoramento de Fraudes e Analistas de Prevenção a Fraudes, que foram convidados a responder as seguintes perguntas: (i) Quais são os principais requisitos/características que um processo de prevenção e tratamento de fraudes deve possuir? (ii) Quais os principais limitantes/problemas que um processo de tratamento e prevenção a fraudes pode encontrar? (iii) Quais, em sua opinião, são as melhores práticas a serem realizadas para melhor tratar e prevenir fraudes eletrônicas?

Anteriormente a aplicação da pesquisa, ainda na etapa de planejamento, algumas hipóteses foram levantadas quanto aos requisitos requeridos ao processo. Dentre eles o de forte foco na detecção da fraude antes que o usuário o perceba, ou seja, a fraude deve ser identificada e tratada antes que o cliente perceba que uma movimentação em sua conta corrente tenha sido realizada, ou, que fraudadores estejam realizando acessos aos canais eletrônicos com suas credenciais.

Após tratar as informações coletadas nas fontes primárias e secundárias, foi possível desdobrar os requisitos em três níveis, construindo o que é denominado na literatura de QFD de uma **árvore da qualidade** demandada. A geração e organização dos requisitos possibilitou identificar os requisitos demandados ao processo, a especificação atual e a especificação desejada para cada requisito. Essa associação é facilitada quando há um conhecimento prévio a respeito das características do serviço que está sendo desenvolvido. De maneira geral, pode-se dizer que os requisitos do serviço apresentam um caráter funcional, estando associados às funções técnicas do próprio serviço, enquanto os requisitos demandados são de caráter não funcional, associados ao desempenho do serviço como um todo.

Quanto a **priorização dos requisitos** do processo, o método apresenta a utilização do AHP como suporte para estabelecer uma ordem de prioridade dos requisitos.

Uma vez identificado os requisitos do processo, um sistema de indicadores (requisitos técnicos) é estabelecido para acompanhar a qualidade demandada. A próxima etapa do

framework é identificar os indicadores necessário para o acompanhamento dos requisitos e gerar a matriz da qualidade.

3.1.2 Levantamento de Indicadores e Matriz da Qualidade

Com a finalidade de auxiliar no projeto da qualidade, a **Matriz da Qualidade** correlaciona os requisitos do cliente, com os indicadores da qualidade (requisitos técnicos). Desta associação é possível identificar quais os indicadores tem maior impacto nos requisitos do processo. Tal informação subsidia a tomada de decisão sobre o sistema de indicadores a ser utilizado.

A matriz de qualidade pondera os indicadores que tem maior impacto no atendimento dos requisitos do cliente que são uma tradução do mercado por meio do cálculo de um índice de qualidade (equação 1) que mede a importância de cada indicador. **Os indicadores** são métricas que serão utilizadas no sistema de indicadores e que produzirão o maior impacto sobre os requisitos. Para tanto, a etapa de relacionamento dos requisitos com os indicadores complementa o preenchimento da **Matriz da Qualidade**. A intensidade do relacionamento entre os requisitos e os indicadores direciona a priorização dos mesmos (DQij), essa intensidade foi expressa utilizando uma escala de 0 a 9 (0 – nenhuma influência; 3 – pouca influência; 6 – média influência; 9– forte influência).

A partir da definição do relacionamento entre os requisitos e os indicadores, foi determinada a importância de cada requisito (IQj), considerando, além desses relacionamentos, a importância relativa dos requisitos processo (IDi), conforme Equação (1):

$$IQ_j = \Sigma\, ID_i * \times DQ_{ij} \qquad (1)$$

Cabe salientar que a importância relativa dos requisitos do processo (IDi) são definidos a partir da comparação paritária dos requisitos do processo. O AHP é utilizado como métrica para definição da importância de cada requisito do processo.

Posteriormente foi avaliada a dificuldade de atuação sobre as características de qualidade (Dj), ou seja, a dificuldade de modificar as especificações das características de qualidade. Foi utilizada uma escala de 0,5 a 2,0; onde 0,5 representa muito difícil e 2,0 fácil. Este indicador é proposto por Ribeiro et al. (2000).

Conforme o indicador proposto pelos autores, é possível ajustar o indicador por meio de um fator de correção que expressa uma avaliação de mercado, comparando-se as especificações atuais das características de qualidade do produto da instituição financeira em estudo com as de instituições financeiras do mercado. A avaliação competitiva das

características de qualidade (Bj) – *benchmarking* técnico, foi realizada da mesma maneira da avaliação competitiva das demandas de qualidade, sendo utilizada a mesma escala de pontuação.

A priorização das características de qualidade (IQj*) é realizada através do índice de importância corrigido. Ele permite identificar quais são as características que, caso desenvolvidas, terão um maior impacto sobre os resultados do processo de prevenção a fraudes, conforme mostra a Equação (2):

$$IQ_j^* = IQ_i \times \sqrt{D_j} x \sqrt{B_j} \qquad (2)$$

Uma vez realizada as etapas relacionadas aos indicadores, cabe desdobrar nos serviços necessários para suportar o alcance das metas. Os detalhes deste levantamento podem ser verificados na próxima seção.

3.1.3 Levantamento de Serviços e Matriz dos Serviços

O Levantamento dos serviços tem por objetivo estabelecer o relacionamento entre os serviços prestados e os indicadores. É feito o **desdobramento dos principais serviços**, onde é possível identificar os processos críticos para a qualidade do serviço, que deverão ser monitorados e/ou otimizados.

Inicialmente, foram identificadas todas as etapas constituintes do processo de prevenção a fraudes eletrônicas, formando o cabeçalho das linhas da Matriz dos Serviços. A **Matriz de Serviços** identifica a relação de procedimentos que mais impactam nas características da qualidade.

Em seguida, foi avaliado o relacionamento dos serviços com os indicadores (PD_{ij}). Para tanto, foi utilizada a mesma escala de pontuação utilizada na avaliação do relacionamento entre as requisitos e os indicadores. Esta avaliação tem como resultado um índice de importância para cada serviço.

A **priorização dos serviços** (IP_i), é usada para avaliar quanto cada atividade contribui no atendimento dos indicadores, conforme equação (3)

$$IP_i = IQ_j \times PD_{ij} \qquad (3)$$

Nesta etapa, também foi avaliada a dificuldade de implantação dos serviços (F_i). Assim como ocorreu a priorização dos requisitos, também ocorreu a priorização dos serviços (IP_i*) utilizando a fórmula que considera além da importância dos serviços os aspectos práticos, referentes a dificuldade e tempo de execução.

Uma vez finalizada a etapa de relacionamento dos indicadores com os serviços, cabe desdobrar os recursos que oferecem suporte as rotinas e procedimentos adotados pelo processo. Os detalhes deste levantamento podem ser verificados na seção seguinte.

3.1.4 Levantamento de Recursos e Matriz de Recursos

Após o desdobramento dos serviços, foi realizada uma avaliação dos recursos necessários para o funcionamento dos processos, ou seja, o **desdobramento dos recursos** que é realizado de maneira a identificar os recursos necessários ao andamento do processos. Essas informações foram organizadas na **Matriz de Recursos**, que contempla tanto os itens referentes a recursos humanos como os itens referentes a infraestrutura. Essa matriz relaciona os serviços com os recursos (equipamentos, os componentes da estrutura física e o pessoal) necessário para atender as rotinas que constituem o processo. O relacionamento dos serviços com os itens de recursos (PRij), foi avaliado utilizando-se uma escala de 0 a 9.

$$IR_j = IP_i \times PR_{ij} \quad (4)$$

A priorização dos recursos (IRj), apresentada na equação (4) permite avaliar o quanto eles contribuem para a melhoria dos serviços e, portanto, para a melhoria da qualidade dos requisitos do processo.

3.2 Processo de Prevenção a Fraudes

O processo avaliado (Figura 2) tem por objetivo tratar unicamente fraudes realizadas utilizando-se de canais eletrônicos. Dentre os canais eletrônicos que são abordados por este processo estão: *Internet Banking*, POS's (*Point of Sale*) que aceitam cartões de débito e ATM's. Lembrando que o processo em questão na pesquisa não é responsável por fraudes documentais ou qualquer outra espécie de fraude.

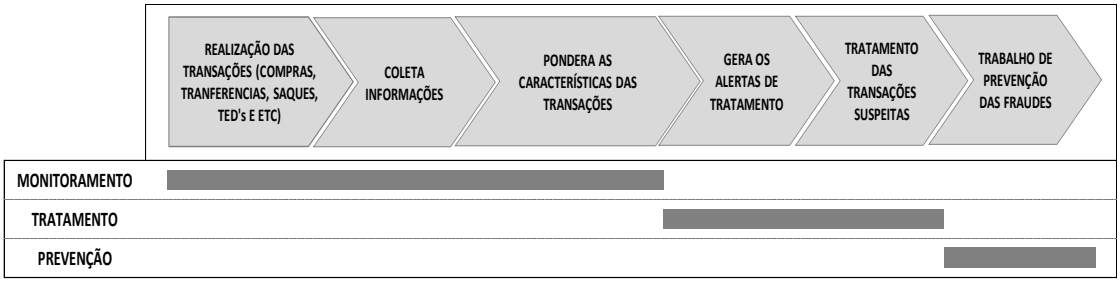

Figura 2 - Processo de Prevenção a Fraudes

Fonte: Elaborado pelos autores

De maneira geral e abrangente o processo pode ser descrito inicialmente com a (i) Realização das Transações nos canais eletrônicos por parte dos clientes da instituição financeira onde os registros das transações são mantidos por um sistema central que, por sua vez (ii) Coleta as Informações da transações e ao mesmo tempo (iii) Pondera as Características das Informações de maneira a identificar padrões de fraudes eletrônicas utilizados por quadrilhas. Desta ponderação o mesmo sistema (iv) Gera os Alertas de Tratamento para as transações que apresentaram algum padrão comportamental anteriormente registrado nas transações tipicamente fraudulentas. Para as transações que tiveram algum tipo de alerta, estas sofrem uma avaliação mais rigorosa que, muitas vezes, contempla contato com o cliente para confirmar a transação. Existe uma equipe especifica para o (v) Tratamento das Transações Suspeitas que neste momento assume a responsabilidade de validar a transação.

A etapa de (vi) Prevenção das Fraudes é na verdade um trabalho de definição das novas estratégias de combate às quadrilhas. Neste momento o histórico das fraudes é levado em consideração a fim de direcionar as ações de contenção das fraudes. O contato com as demais instituições financeiras também contribui para o aprimoramento do processo e alocação dos recursos. Técnicas mais elaboradas de detecção de fraudes são exigidas neste contexto.

4 Resultados e Discussões

Os resultados serão apresentados em quatro seções de maneira a identificar as conclusões de cada etapa utilizada no método. As discussões serão baseadas na Figura 5 que demonstra os resultados, de uma maneira global, da aplicação do método.

4.1 Levantamento e Priorização dos Requisitos

Ao analisar e organizar as informações coletadas na pesquisa de marketing foi possível gerar a **árvore da qualidade demandada** (Figura 3), onde é possível identificar a qualidade primária, secundária, suas especificações e indicadores utilizados para monitoramento. Para melhor compreensão dos requisitos, estes foram agrupados em três estratos, que são especificados na Figura 3: (i) Monitoramento das transações, (ii) Tratamento das transações e, (iii) Inteligência e Prevenção.

Qualidade Primária	Qualidade Secundária	Característica da Qualidade	Especificação Atual	Meta
Monitoramento de Transações	Identificar a transação fraudulenta antes do cliente	% de transações fraudulentas identificadas	60%	80%
	Assertividade na identificação das transações fraudulentas	% falso negativo	30%	20%
Tratamento das Transações	Rapidez no tratamento das transações fraudulentas	Tempo de tratamento da fraude	6 dias	4 dias
	Minimizar o impacto financeiro das fraudes	% de recuperação	45%	55%
Inteligência e Prevenção	Reduzir o número global de fraudes	Número global de fraudes	1/10000 transações	1/15000 transações

Figura 3 - Árvore da Qualidade

Fonte: Elaborado pelos autores

O objetivo de **monitorar as transações** é identificar padrões e comportamentos conhecidos e historicamente utilizados por fraudadores, de maneira a sinalizar o evento e tratá-lo rapidamente mitigando perdas financeiras e comprometimento da imagem da instituição. É neste contexto que entram as **ferramentas computacionais** para análise das transações e comparação com padrões conhecidos de comportamento fraudulento. Para tanto, é importante acompanhar o desempenho das regras de monitoramento no que se refere a quantidade de falsos negativos com o objetivo de tornar mais eficientes as regras de identificação de fraudes.

O **tratamento de transações fraudulentas** consiste em identificar novos *modus operandi* de fraudes utilizados pelas quadrilhas que ainda não são conhecidos pela organização, gerando informações e subsídios para o monitoramento de transações. A reação é um dos aspectos mais importantes do tratamento de fraudes. Em uma analogia, o tratamento dos eventos seria uma espécie de termômetro do processo, pois nesta etapa são identificados os falsos negativos, que por sua vez, implicam em perdas consideráveis de receita.

A inteligência e prevenção a fraudes abrange não somente o monitoramento dos eventos, mas, uma visão mais ampla do negócio. Entender para onde o mercado está se dirigindo com novos produtos financeiros e tecnologias de acessos aos serviços. É neste sentido que a área de inteligência deve atuar, ou seja, corroborando para que produtos financeiros e canais eletrônicos sejam disponibilizados para os clientes com segurança mínima para autenticar as transações e garantir o mínimo de perdas financeiras.

Indicador	Qualidade Demandada (Critérios)
(i)	Identificar transações fraudulentas antes do cliente
(ii)	Assertividade na identificação das transações fraudulentas
(iii)	Rapidez no tratamento de transações fraudulentas
(iv)	Minimizar o impacto financeiro das fraudes
(v)	Reduzir o número global de fraudes

Matriz de Comparações						Peso
Critérios	**(i)**	**(ii)**	**(iii)**	**(iv)**	**(v)**	
(i)	1,00	0,20	5,00	0,20	3,00	**13,82%**
(ii)	5,00	1,00	7,00	0,33	5,00	**30,59%**
(iii)	0,20	0,14	1,00	0,14	0,33	**3,81%**
(iv)	5,00	3,00	7,00	1,00	3,00	**42,78%**
(v)	0,33	0,20	3,00	0,33	1,00	**9,01%**

Figura 4 - Análise Multicriterial

Fonte: Elaborado pelos autores

O resultado da análise multicriterial (Figura 4) permitiu identificar que o impacto financeiro foi o requisito do cliente que mais se destacou dentre todos. Dado os resultados, é possível perceber que o item **prejuízos financeiros resultantes de ataques fraudulentos** é o maior ofensor na visão dos especialistas. Os prejuízos de fraudes podem inviabilizar um produto, e até mesmo, comprometer fatalmente a saúde financeira da organização. No segundo plano dos resultados ficou a **assertividade na identificação das transações fraudulentas**, que por sua vez, corrobora com a afirmação de Abramonwicz (2002) quando diz que, tipicamente, falsos negativos resultam em perdas de receita enquanto falsos positivos geram uma maior carga de trabalho para os analistas de fraude. Implicitamente, a assertividade da identificação de transações fraudulentas aumenta as chances de recuperação de valores e com isso **minimizar o impacto financeiro das fraudes**, pois permite que a operação realizada sob má-fé tenha uma resposta mais rápida quando esta não foi identificada imediatamente a sua ocorrência.

4.2 Desdobramento da Qualidade

Após o relacionamento dos requisitos com os indicadores foi possível perceber um maior impacto do **percentual de transações fraudadas identificadas pelo monitoramento** e o **percentual de falsos negativos** como os indicadores de maior significância para satisfazer a "voz do cliente" (Figura 5, (a) Matriz da Qualidade). O resultado do relacionamento entre os indicadores e os requisitos do processo corroborou com as conclusões identificadas na etapa de levantamento dos requisitos, uma vez que, a identificação das operações fraudulentas pelo

sistema de monitoramento propicia uma chance maior de resgate do valor fraudado. A identificação rápida permite ações reativas serem executadas exatamente após o evento fraudulento. O mesmo acontece com o **percentual de falsos negativos**, esta métrica exibe o quão eficiente são as regras aplicadas no monitoramento. Partindo da premissa que falsos negativos são transações fraudulentas não identificadas pelo sistema de monitoramento, essas, por sua vez, possuem um baixo potencial de resgate uma vez que são dadas inicialmente como transações legitimas realizadas pelos clientes, mas na verdade, são transações realizadas por fraudadores e que não tiveram a devida atenção pela instituição financeira.

O **número global de fraudes**, relação entre o número de transações legitimas e o número de transações fraudulentas, reflete uma série de frentes de prevenção a fraudes. Desde o esforço para prevenir fraudes aumentando a segurança de canais e serviços eletrônicos, como as iniciativas de conscientização dos clientes quanto a usabilidade dos canais eletrônicos. Este pode ser um indicador a ser utilizado de maneira global, envolvendo todos os tipos de transações eletrônicas, ou, de maneira especifica, por tipo de transação ou produto. A vantagem da utilização de maneira especifica sobre a de maneira global, é a possibilidade de identificação de produtos ou canais financeiros mais frágeis.

4.3 Desdobramento dos Serviços

A relação entre os indicadores e os serviços resultou na identificação dos procedimentos críticos do processo, que por sua vez, definirão parte da estratégia para satisfazer a qualidade demandada (Figura 5, (b) Matriz de Serviços).

Os resultados deste relacionamento apontaram para a **geração/atualização das regras de monitoramento** como fundamental para a satisfação do cliente, uma vez que este serviço demonstrou-se ser de forte impacto nos indicadores da qualidade. A geração/atualização de regras de monitoramento deve estar alinhada com o **tratamento das fraudes**, pois as fraudes tratadas devem servir de "*inputs*" para o monitoramento das transações. Percebe-se uma interdependência entre o tratamento das fraudes, também identificado como um serviço que impacta significativamente o processo de prevenção a fraudes, e a geração/atualização das regras de monitoramento uma vez que os "*modus operandi*" não englobados pelas regras são identificados no tratamento destas, que por sua vez, deve fornecer informações para tornar as regras mais eficazes e evitar o falso negativo. O impacto deste procedimento nos indicadores foi considerado para todas as características do processo. Entende-se que este seja um

processo que deve ser avaliado de maneira mais detalhada uma vez que fica evidente o seu considerável impacto nas características da qualidade.

O **contato com o cliente** é importante para a detecção da fraude. Um exemplo desta afirmativa é a utilização dos chamados Serviços de Mensagem Curta (SMS – *Short Message Service*) que hoje são largamente utilizados para notificar o cliente sobre alguma transação atípica identificada nos canais eletrônicos (O'SULLIVAN, 2008). O contato com o cliente é realizado após a suspeita de que alguma transação tenha sido realizada em seu nome. A confirmação da transação fraudulenta implica em ganho de tempo para recuperação dos valores fraudados, ou, bloqueio das credenciais deste cliente para que novas transações fraudulentas não sejam realizadas.

4.4 Desdobramento dos Recursos

A relação dos recursos com as características da qualidade possibilitou identificar o desenvolvimento e aprendizagem como fator principal de investimento para prevenir as fraudes (Figura 5, (c) Matriz de Recursos). Neste caso, o desenvolvimento representa o apetite da instituição financeira em querer entender os potenciais "*modus operandi*" de fraude, bem como, identificar os métodos que estão sendo utilizados, ou que podem ser utilizados, para mitigar tais riscos. Dentre as fontes de informação estão: Benchmarkings, fóruns de prevenção a fraudes, comitês interempresariais do ramo financeiro, congressos, etc. Quando se trata de combater quadrilhas de fraudadores, as instituições financeiras não devem considerar o fator "concorrência" como um limitador para esse processo de troca de experiências. Neste momento deve estar claro que as instituições financeiras, e a sociedade, são as vítimas e nada melhor como um trabalho em conjunto, baseado na troca de experiências, pode conter o avanço dos criminosos.

Quanto ao apontamento de **equipamentos de tecnologia da informação e *softwares*** como recursos para prevenção a fraudes (ver etapa 4, figura 5), as ferramentas computacionais e tecnológicas permanecem como componentes chaves para o estabelecimento de Processo de Prevenção a Fraudes Eletrônicas. O serviço financeiro não depende da utilização destes artifícios somente para acelerar processos ou ganhar maior capacidade transacional e sim para evitar perdas de natureza fraudulenta. O volume transacional utilizando-se de canais eletrônicos tende a aumentar significativamente no Brasil e no mundo, logo, sistematizar esse processo torna-se mandatório para evitar perdas desta natureza.

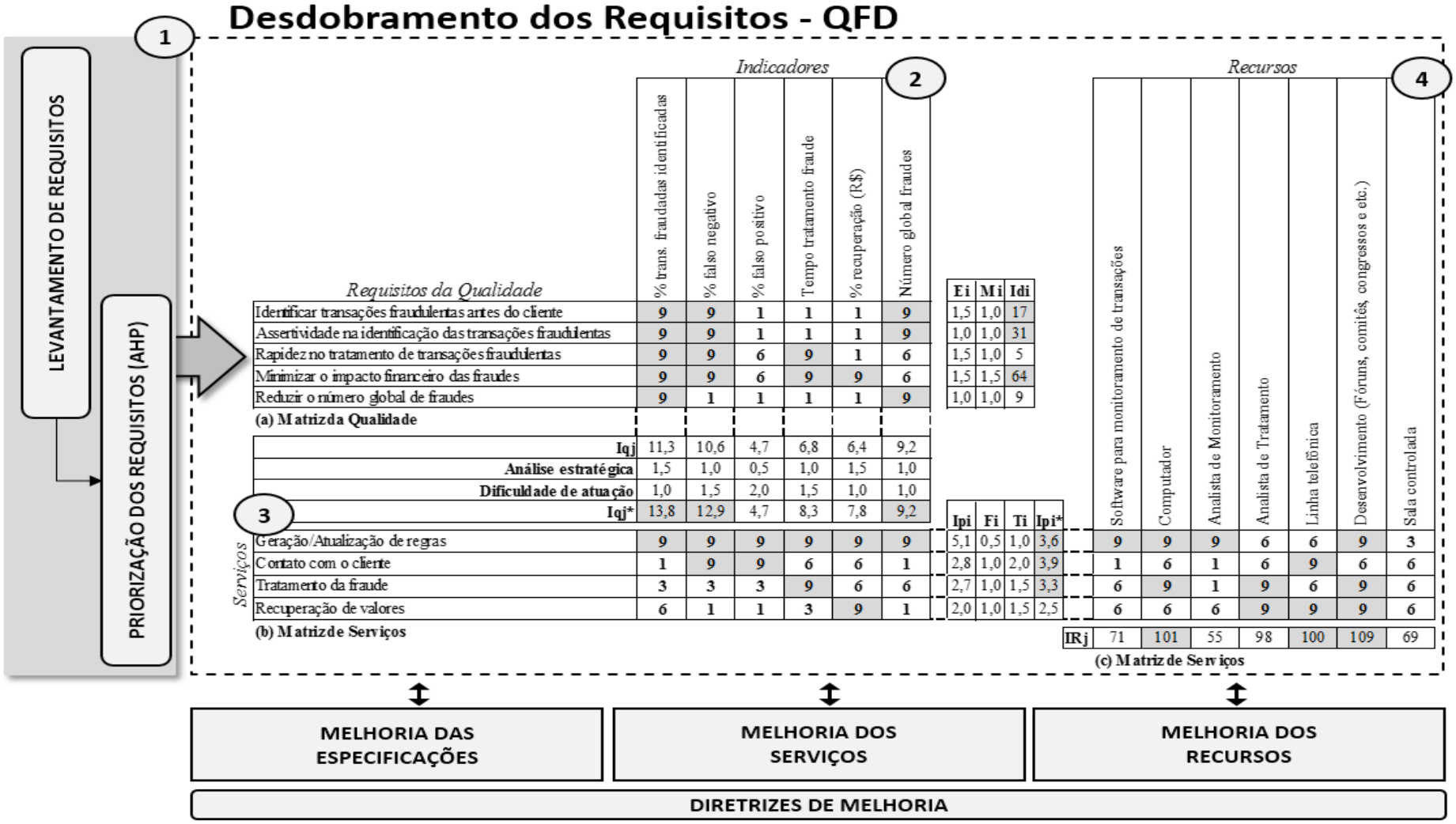

Figura 5 - Desdobramento da Função Qualidade

Fonte: Elaborado pelos autores

5 Considerações Finais

Este artigo teve como objetivo identificar requisitos de um processo de tratamento e prevenção de fraudes eletrônicas de uma instituição financeira visando redução do impacto de perdas por fraudes eletrônicas por meio do uso de métodos de melhoria de processo da qualidade de manufatura aplicados ao processo de prevenção de fraudes eletrônicas. Para tanto, foi realizado inicialmente uma pesquisa de mercado solicitando a opinião de especialistas na área de prevenção a fraudes e priorizando esses resultados por meio do AHP. A pesquisa permitiu identificar as necessidades de um processo de prevenção para posterior utilização como qualidade demandada no QFD integrado ao AHP. Como requisitos do cliente, a matriz da qualidade apontou que o "percentual de transações fraudulentas identificadas pelo monitoramento" e o "percentual de falsos negativos" foram os indicadores mais importantes no processo de prevenção de fraudes. Ambas as métricas implicam em maior possibilidade de resgate do volume financeiro fraudado, bem como, as chances de evitar que o cliente perceba o ato fraudulento, o que corrobora com a os primeiros itens de maior impacto na qualidade demandada: "Assertividade na identificação das transações fraudulentas" e "Minimizar o impacto financeiro das fraudes".

Para melhoria dos procedimentos relacionados aos indicadores, por meio da matriz de serviços, foi possível identificar a geração de regras para o monitoramento de fraudes como o procedimento de maior impacto nas características da qualidade. Tal resultado se deve ao foco de uma área de prevenção a fraudes mitigar as chances de ocorrer fraudes. O fato de identificar os eventos fraudulentos quando estes ocorrem, ou muito próximo de sua ocorrência, permitem que o tratamento seja mais efetivo, as chances de descontinuar a transação ou recuperar os valores fraudados aumentam significativamente para atender estes procedimentos, a matriz de recursos trouxe resultados que apontaram desenvolvimento e atualização trazem grandes vantagens para a instituição financeira. Como os métodos de fraudes são dinâmicos e cada vez mais elaborados, cabe a organização estar informada sobre estes métodos de maneira a antecipar-se aos ataques.

Como sugestão para trabalhos futuros indica-se ampliar o estudo de requisitos para um processo de prevenção a fraudes eletrônicas através da realização de reflexões críticas sobre indicadores, serviços e recursos que possam contribuir reduzindo o impacto financeiro causado pelas fraudes em canais eletrônicos.

Referências

ABREU, F. S.; **QFD - desdobramento da função qualidade - estruturando a satisfação do cliente**. Rev. adm. empres. [online]. 1997, vol.37, n.2, pp. 47-55. ISSN 0034-7590.

AKAO, Y.; **Quality function deployment: integrating costumer requirements in product design**. New York: Productivy Press, 1990.

ALFURAIH, S. Using Trusted Email to Prevent Credit Card Frauds in Multimedia Products. **World wide web**, v.5, n. 3 p. 245 -256. 2002.

ALESKEROV, E., FREISLEBEN, B., Rao, B. CARDWATCH: A neural network based database mining system for credit card fraud detection. **IEEE/IAFE 1997 computational intelligence for financial engineering (CIFEr)** p. 220–226. 1997

ARVIDSON, M.; CARLBARK, M.; Intrusion detection systems – technologies, weaknesses and trends. **Department of Electrical Engineering, Linko ping University**. 2003.

BHATTACHARYA, A., Sarkar, B. and Mukherjee, S.K., "Integrating AHP with QFD for robot selection under requirement perspective", **International Journal of Production Research**, Vol. 43 No. 17, pp. 3671-85. 2005

BACEN – BANCO CENTRAL DO BRASIL. **Resolução Nº 3380.** Disponível em: http://www.bcb.gov.br/pre/normativos/res/2006/pdf/res_3380_v2_P.pdf Acessada em: 20/01/2014.

BELLA, M.A.; ELOFF, J.H.P.; OLIVER, M.S.; A fraud management system architecture for next-generation networks. **Forensic science international**. v. 185 n. 1 – 3 p. 51 – 58. 2008.

BENAROCH, M. Pricing e-service quality risk in financial services. **Electronic commerce research and applications** v.10 n. 5 p. 534 -544. 2011

BHATLA, T. P., VIKRAM, P., & DUA, A. Understanding Credit Card Frauds. **Cards Business Review 1**. 2003

BOUKERCHE, A.; NOTARE, M. S. M. A. Neural fraud detection in mobile phone operations. **Lecture Notes in Computer Science**, p. 636–644. 2000

BRAUSE, R.; LANGSDORF, T.; & HEPP, M. Neural data mining for credit card fraud detection. **11th IEEE international conference on tools with artificial intelligence** p. 103–106. 1999

BURGE, P.; SHAWE-TAYLOR, J.; COOKE, C.; MOREAU, Y., PRENEEL, B.; STOERMANN, C. Fraud detection and management in mobile telecommunications networks. **European conference on security and detection, ECOS 97** p. 91–96. 1997

COELHO, L. S.; RAITTZ, R. T.; TREZUB, M.. FControl®: sistema inteligente inovador para detecção de fraudes em operações de comércio eletrônico. **Gest. Prod. [online]**. vol.13, n.1, pp. 129-139. 2006.

DONG, W. et al. A feature extraction method for fraud detection in mobile communication networks. **Fifth world congress on intelligent control and automation** (pp. 1853–1856). 2004.

FIORENZO, F. (2001), Advanced Quality Function Deployment, St Lucie Press, New York, NY. Govers, C.P.M. (2001), "QFD not just a tool but a way of quality management", **International Journal of Production Economic**, Vol. 69 No. 2, pp. 151-9.

FEBRABAN – Federação Brasileira de Bancos. – **FEBRABAN dá Dicas de Segurança Eletrônica**. Disponível em: http://www.febraban.org.br/Noticias1.asp?id_texto=1886&id_pagina=60&palavra= Acesso em: 22/01/2012

FEBRABAN – Federação Brasileira de Bancos. – **Pesquisa FEBRABAN de Tecnologia Bancária**. Disponível em: http://www.febraban.org.br/7Rof7SWg6qmyvwJcFwF7I0aSDf9jyV/sitefebraban/Pesquisa%20FEBRABAN%20de%20Tecnologia%20Banc%E1ria%202013.pdf Acesso em: 20/02/2014

GHOSH, M. Telecoms Fraud. **Computer fraud and security** v. 2010 n. 7 p. 14 -17. 2010.

GHOSH, S.; REILLY, D. L. Credit card fraud detection with a neural-network. **Twenty seventh Hawaii international conference on system science** v. 3 p. 621–630). 1994

GIL, A. C.. **Como elaborar projetos de pesquisa**. São Paulo. Atlas. 1991

HANUMAIAH, N., Ravi, B. and Mukherjee, N.P., "Rapid hard tooling process selection using QFD-AHP methodology", Journal of Manufacturing Technology Management, Vol. 17 No. 3, pp. 332-50. 2006

ICT Statistics Newslog - **Report Predicts 894 Million Mobile Banking Users by 2015. News Related to ITU Telecommunication/ICT Statistics** . Disponível em: http://www.itu.int/ITU-D/ict/newslog/Report+Predicts+894+Million+Mobile+Banking+Users+By+2015.aspx Acesso em: 15/02/2014

IBBETT, G. Top Telco Frauds and How to Stop them. **Billing World and OSS Today Magazine**, Disponível em: http://www.billingworld.com/secondary.cfm?page=detail&archiveId=7824 Acessado em: 22/01/2014

JACOBS, R. **Telecommunications Fraud, Dimension Data White Paper**. Disponível em: http://www.didata.com/services/white_papers/Fraud_White_Paper. pdf Acessado em: 15/01/2014

Kou, Y.; Lu, C.-T.; SIRWONGWATTANA, S.; HUANG, Y. Survey of fraud detection techniques. **In 2004 IEEE international conference on networking, sensing and control**, V. 2 p. 749–754). 2004

MAHMOOD, T.; SHAIKH, G. M.; Adaptive Automated Teller Machines. **Expert systems with applications** v. 40 n. 4 p.1152 -1169. 2013

MAES, S.; TUYLS, K., VANSCHOENWINKEL, B.; MANDERICK, B.: Credit card fraud detection using bayesian and neural networks. **NF 2002**. p. 16-19 2002

MILLS, J E Cybercrimes against Consumers: Could Biometric Technology Be the Solution? **Internet Computing** v. 10 n. 4 p. 64 -71. 2006.

MOISIADIS, F., "The fundamentals of prioritizing requirements", paper presented at: **Systems Engineering: Test and Evaluation Conference**, Sydney, October. 2002

MOREAU, Y.; PRENEEL, B.; BURGE, P.;SHAWE-TAYLOR, J.; STOERMANN, C.; COOKE, C.; Novel techniques for fraud detection in mobile telecommunication networks. **ACTS (Advanced Communications Technologies and Services)**. 1996.

MOREAU, Y.; VANDERWALLE, J. Detection of mobile phone fraud using supervised neural networks: A first prototype. **International Conference on Artificial Neural Networks** – p. 1065–1070. 1997

PARTOVIA, F.Y. and Corredoira, R.A. "Quality function deployment for the good of soccer", **European Journal of Operational Research**, Vol. 137, pp. 642-56. 2002

PARTOVIA, F.Y. and Epperly, J.M., "A quality function deployment approach to task organization in peacekeeping force design", **Socio-Economic Planning Sciences**, Vol. 33, pp. 131-49. 1999

PROVOST, F. Statistical fraud detection: A review Statistical Science. **Statistical science** v. 17 n. 3. p. 235–255. 2002.

RIBEIRO, J. L. D., A utilização do QFD na otimização de produtos, processos e serviços. **FEENG/UFRGS – Fundação Empresa Escola de Engenharia da Universidade federal do Rio Grande do Sul**. 2001

SÁNCHEZ, D. Association rules applied to credit card fraud detection. **Expert systems with applications**. v.36 n.2 p. 3630 -3640. 2009

TASSABEHJI, R.; KAMALA, M. A. Evaluating biometrics for online banking: The case for usability. **International journal of information management** v.32 n.5 p.489 -494. 2012

VIANE, S.; DEDENE, G.; DERRIG, R. Auto claim fraud detection using Bayesian learning neural networks. **Expert Systems with Applications: An International Journal**, p. 653–666. 2005

YIN, R.. **Case study research: Design and methods** (2nd ed.). Beverly Hills, CA: Sage Publishing, 1994.

II – ARTIGO 2: A UTILIZAÇÃO DE MÉTODOS QUALITATIVOS PARA IDENTIFICAÇÃO DE REQUISITOS EM UM PROCESSO DE PREVENÇÃO A FRAUDES: ESTUDO DE CASO ENVOLVENDO ESPECIALISTAS DE UMA INSTITUIÇÃO FINANCEIRA

Resumo

O objetivo deste trabalho é ampliar o estudo de requisitos de um processo de prevenção a fraudes através da consulta direta a especialistas da área em uma instituição financeira. Esta reflexão crítica sobre um processo de prevenção a fraudes eletrônicas visa identificar indicadores, serviços e recursos utilizados e desejados por uma instituição financeira que oferece canais eletrônicos de atendimento a clientes. A técnica utilizada para o estudo foi um grupo focal, formado por seis especialistas da área de prevenção a fraudes eletrônicas seguindo um roteiro pré-definido. Os resultados do grupo focal permitiram verificar quanto a (i) Indicadores: identificação da primeira transação fraudulenta, volume financeiro fraudado e percentual de eventos fraudulentos identificados pelo monitoramento; (ii) Serviços: que incluam análise de *malwares*, monitoramento de páginas falsas (*phishing*), contato com o cliente, tratamento de eventos fraudulentos e análise preventiva de produtos e canais eletrônicos, e (iii) Recursos: *software* de monitoramento, linha telefônica e especialistas em prevenção a fraudes.

Palavras-chave: Fraudes eletrônicas; grupo focal; serviços financeiros; eficiência; métodos qualitativos

1 Introdução

Os bancos têm investido cada vez mais em tecnologia, procurando permitir o acesso do cliente aos seus serviços através de canais como: *internet*, telefone, celulares, *palm-tops*, fax, centrais de atendimento, entre outros (SOUZA NETO; FONSECA; OLIVEIRA, 2005). A tecnologia promoveu mudanças significativas na prestação de serviços financeiros, exemplo disso são os diversos estudos relacionados a *mobile banking* (Lin 2011), *internet banking (Calisir, 2008)*, ATM's (*Automated Teller Machine*)(MAHMOOD 2013).

O viés desta quebra dos paradigmas de atendimento e prestação de serviços foi o surgimento das quadrilhas especializadas em fraudes eletrônicas. Estudos da Federação Brasileira de Bancos (FEBRABAN) apontaram uma estimativa de R$ 1,5 bilhões em perdas a instituições financeiras nacionais no ano de 2012, deixando claro que fraudes eletrônicas passaram a ser um dos maiores ofensores a eficiência das instituições financeiras. Ibbett (2007) mostra que atualmente fraudes eletrônicas são um problema amplamente difundido e que geralmente custa aos empresários algo entre 3 e 8% de sua renda anual, além de comprometer sua reputação e a confiança na relação com o usuário de serviços eletrônicos. Ainda, Ibbet (2007) estima que este montante representa cerca de U$D 44 bilhões no mundo dos negócios virtuais. É neste contexto que as técnicas de prevenção a fraudes eletrônicas,

bem como, os métodos utilizados para gerenciamento e acompanhamento devem ser constantemente reavaliados objetivando a redução de seu impacto e aumento dos resultados.

Este trabalho se propõe a ampliar o estudo de requisitos de um processo de prevenção a fraudes através da consulta direta a especialistas da área em uma instituição financeira. Esta reflexão crítica sobre um processo de prevenção a fraudes eletrônicas visa identificar indicadores, serviços e recursos utilizados e desejados por uma instituição financeira que oferece canais eletrônicos de atendimento a clientes. Para tanto, foi utilizado o grupo focal como ferramenta de apoio. Grupo focal, segundo Borges e Santos (2005), é uma dentre as várias modalidades disponíveis de entrevista grupal e/ou grupo de discussão. Os participantes dialogam sobre um tema particular, ao receberem estímulos apropriados para o debate (RESSEL et Al., 2008).

A organização do artigo acontece da seguinte maneira: a seção 2 apresenta o referencial teórico, contendo os resultados de pesquisa sobre Fraudes Eletrônicas e Serviços Bancários, a seção 3 apresenta os procedimentos metodológicos contemplando o roteiro com as perguntas utilizadas para o grupo focal juntamente com uma apresentação do cenário onde o método foi aplicado, na seção 4 estão apresentados os resultados e discussões da aplicação do grupo focal seguido da seção 5 com as considerações finais do trabalho.

2 Referencial Teórico

O referencial teórico deste artigo está dividido em duas seções. A primeira seção aponta para os resultados de pesquisas relacionados ao tema Serviços Bancários. Na seção seguinte, o tema abordado é Processo de Prevenção a Fraudes Eletrônicas.

2.1 Serviços Bancários

Moori, Marcondes e Ávila (2002) afirmam que a constante recriação de processos produtivos e as mudanças nas expectativas dos consumidores em relação ao surgimento de novos produtos são mais frequentes. Uma consequência prática disso é que os ciclos de vida dos produtos são cada vez menores e isso pressiona as empresas a terem ciclos de desenvolvimento de produtos e de serviços mais rápidos, reforçando, assim, as atividades de desenvolvimento e de inovação simultaneamente. Ser inovador está deixando de ser uma alternativa de risco elevado e passando a ser uma obrigação. Na verdade, inovar está

tornando-se um risco menor do que não inovar. Nesse caso, a portabilidade no setor pode ser um aspecto relevante na inovação e na adoção de estratégias diferenciais (ENSSLIN 2013).

As constantes mudanças do cenário financeiro exigem deste setor um desempenho, muitas vezes, acima da média dos demais setores. Fatores econômicos, políticos e mercadológicos afetam significativamente o setor, que por sua vez, exige flexibilidade e constante monitoramento do desempenho. Schiehll e Morissette (2000) corroboram com esta ideia de constante análise do desempenho em ambientes de constante mudança afirmando que os novos ambientes de produção, de competição global e de revolução da informação são alguns dos aspectos que estão sendo usados para aumentar a relevância do assunto e o argumento de que as organizações precisam mudar a maneira de avaliar os seus desempenhos. Neste sentido, no entender de Paiva, Barbosa e Ribeiro (2009), ainda há uma carência de estudos sobre o tema, os quais considerem variáveis como os setores da economia, segmentos de consumidores ou regiões geográficas a fim de possibilitar maior precisão nas estratégias para conquistar, de forma duradoura, a preferência de consumo do cliente, então, focando seus negócios atuais e futuros.

Muitos bancos têm direcionado suas estratégias para aumentar a satisfação e a lealdade de seus clientes melhorando a qualidade dos serviços, uma vez que o oferecimento do serviço correto é um fator alinhado com o objetivo de aumentar as taxas de retenção e, consequentemente, os lucros da empresa. (LEVESQUE; MCDOUGALL, 1996).

O investimento em serviços mais eficientes é uma vantagem competitiva, principalmente no setor bancário, com tanta similaridade entre os produtos e serviços ofertados, o diferencial para o cliente passa a ser a qualidade com que os serviços são prestados, já que estes se assemelham tanto, que é possível, de forma geral, tratar o mercado de varejo dos bancos como um mercado de *commodities* (CAMPELLO; COSTA NETO, 2004).

Com o objetivo de aumentar a eficiência dos serviços prestados pelo sistema bancário nacional, o Banco Central do Brasil (BACEN) definiu através da resolução nº 3380 que todas as instituições financeiras devem estabelecer uma estrutura de gerenciamento de riscos e perdas operacionais. Segundo a resolução, enquadram-se como fontes de perdas operacionais: (i) fraudes internas; (ii) fraudes externas; (iii) demandas trabalhistas e segurança deficiente do local de trabalho; (iv) práticas inadequadas relativas a clientes produtos e serviços; (v) danos a ativos físicos próprios ou em uso pela instituição; (vi) aqueles que acarretem a interrupção das

atividades da instituição; (vii) falhas em sistemas de tecnologia da informação; e (viii) falhas na execução, cumprimento dos prazos e gerenciamento das atividades na instituição.

Conforme mencionado, as fraudes são tratadas como perdas operacionais e afetam diretamente a eficiência operacional dos serviços financeiros. Logo, trabalhos específicos de prevenção e tratamento devem ser continuamente desenvolvidos visando mitigar as perdas desta natureza e maximizar os resultados da organização. Na próxima seção será apresentada uma abordagem teórica sobre o tema fraudes eletrônicas.

2.2 Processo de Prevenção a Fraudes Eletrônicas

Estabelecer e melhorar continuamente um processo de prevenção a fraudes eletrônicas se faz necessário. Segundo Ghosh (2010), as vítimas típicas de fraudes eletrônicas são: consumidores, instituições financeiras e prestadoras de serviços de comunicação e empresas que oferecem serviços e venda de bens de consumo via rede internacional de computadores. Dentro deste conjunto de potenciais vítimas, encontra-se uma parcela considerável de entidades que são alvo de quadrilhas fraudadoras. Para tanto, uma efetiva metodologia para detecção de fraudes pode ajudar as organizações a oferecer a seus consumidores um ambiente *online* seguro e confiável que estimule a lealdade aos seus serviços. Portanto, é essencial que tecnologias de prevenção e métodos de detecção de fraude sejam continuamente desenvolvidas e atualizadas (PROVOST, 2002).

O gerenciamento de fraudes eletrônicas tem uma ampla área de atuação que geralmente engloba todos os aspectos de detecção, gestão e investigação de qualquer tentativa, com sucesso ou não, de roubo através de enganação ou violação intencional de serviços oferecidos por meio eletrônico (JACOBS, 2002). Quanto a utilização de ferramentas computacionais para auxiliar a detecção e prevenção a fraudes eletrônicas, Bella (2008) estabelece os principais requisitos de tal sistema: (i) flexibilidade, ou seja, deve detectar fraudes independente do tipo de serviço e da tecnologia subjacente, bem como, permitir a adição, remoção e atualização de algoritmos de detecção de fraude; (ii) capacidade analítica dos dados trocados independentemente do canal utilizado e do volume de informações trafegadas e (iii) escalabilidade, ou seja, que possa ter condições de ser atualizado continuamente de maneira a acomodar os novos canais e novos *modus operandi* de fraudes. Definida de maneira ampla, fraudes eletrônicas tratam-se de crimes virtuais, ou seja, qualquer ato ilegal envolvendo um sistema computacional, aplicação ou transmissão de dados, onde a vítima sofre ou sofreu perdas. Neste amplo espectro inclui-se acesso não autorizado ou roubo

de informações proprietárias (MILLS, 2006). A gestão do processo de detecção de fraudes eletrônicas depende necessariamente da natureza e ramo do negócio, porém, de maneira geral, existem dois métodos para detecção de fraudes: análise absoluta e análise diferencial. A análise absoluta busca identificar padrões de ataques anteriores para identificar novas ocorrências destes ataques, enquanto que a análise diferencial procura por desvios no padrão de utilização do usuário (MOREAU, 1996). Ambos os métodos de detecção de fraude estão suscetíveis a erros. Com relação aos potenciais erros na análise de detecção de fraudes, seja ela diferencial ou absoluta, estes podem ser de dois tipos: falsos positivos e falsos negativos. Um falso positivo ocorre quando um alarme é gerado embora não há um ataque. Em contrapartida, um falso negativo acontece quando um alarme não é gerado apesar do ataque (ARVIDSON, 2003).

Bella (2010) enfatiza a questão dos falsos negativos quando afirma que, como uma fonte de perda de receitas, falsos negativos são de longe mais ameaçadores para o empresário uma vez que o valor fraudado pode ser muito superior ao trabalho despendido por um analista ao tratar um falso positivo. Neste mesmo contexto, Bella (2010) acrescenta que um processo de detecção de fraudes apresenta muitos desafios, dentre os quais estão o grande número de erros de detecção que podem ser gerados por um sistema de monitoramento de fraudes e o potencial desgaste da privacidade do usuário do serviço.

Um dos maiores desafios das organizações que tratam de fraudes eletrônicas é a detecção de comportamento fraudulento em meio a grandes quantidades de informação. Prevenção a fraudes eletrônicas tornou-se uma extensa área de pesquisa objetivando minimizar os efeitos da fraude no mercado de serviços financeiros (KOU ET AL.,2004). Contribuições neste sentido podem ser verificadas em estudos relacionados à detecção de fraudes em Cartão de Crédito (ALESKEROV, FREISLEBEN; RAO, 1997; BRAUSE, LANGSDORF; HEPP, 1999; GHOSH & REILLY, 1994; MAES ET AL.; MANDERICK, 2002), telecomunicações (BOUKERCHE; NOTARE, 2000; BURGE ET AL., 1997) e seguros (VIANE, DEDENE; DERRIG, 2005) que utilizam de cenários previamente experimentados e conhecidos de fraude para prover maior eficácia na detecção de transações fraudulentas; proposição de um Sistema de Gestão de Fraudes baseado em *Internet Protocol* (IP) aliado ao uso de Redes Neurais (BELLA, 2008) e, proposição de uso de métodos estatísticos para detecção de desvios de comportamento na utilização de cartões de crédito, tais como *data mining* (SÁNCHEZ, 2009).

Também é possível encontrar na literatura trabalhos voltados à prevenção de fraudes aplicada na autenticação de transações. Tassabehhji (2012) apresenta as vantagens da aplicação de reconhecimento biométrico para autenticar transações financeiras realizadas em canais eletrônicos.

Diante do avanço tecnológico e da dinâmica do mercado financeiro, a reavaliação continua do processo de prevenção a fraudes eletrônicas objetivando o ganho de eficiência e o aumento da segurança nos canais torna-se mandatório.

3 Procedimentos Metodológicos

Esta seção tem por objetivo descrever um caso real de práticas utilizadas para prevenção a fraudes eletrônicas em uma instituição financeira privada da região sul do Brasil, comparando-as com alguns achados em outros estudos de caráter exploratório. Desta forma, o estudo caracteriza-se como sendo um estudo de caso que segundo Yin (2005) é uma estratégia de pesquisa que visa responder questões do tipo "como" ou "por quê", em situações em que o evento estudado é contemporâneo à pesquisa e em que o pesquisador não detém controle sobre o evento estudado (não podendo reproduzi-lo fora do seu contexto original). Essas condições se aplicam a este estudo, uma vez que as questões de pesquisa envolvidas são do tipo "como" – como são realizadas as práticas de prevenção a fraudes eletrônicas –, e "por quê" – enumerando as vantagens e desvantagens da utilização de determinadas práticas –, o evento estudado é contemporâneo à pesquisa e não reprodutível fora do seu contexto.

Esse trabalho é de natureza aplicada, uma vez que os conhecimentos gerados servem de base para a solução de problemas práticos (GIL, 1991). O levantamento dos dados foi realizado por meio da técnica de grupo focal o qual, segundo Borges e Santos (2005), é uma dentre as várias modalidades disponíveis de entrevista grupal e/ou grupo de discussão. Os participantes dialogam sobre um tema particular, ao receberem estímulos apropriados para o debate (RESSEL et. al., 2008).

A vantagem das entrevistas em grupos focais é que elas não requerem muito planejamento prévio, permitindo que o pesquisador vá a campo tão logo tenha definido os objetivos da pesquisa. No entanto, segundo Ribeiro e Milan (2004), apesar de não exigirem muito planejamento, há aspectos que precisam ser verificados, entre os quais se destacam: **1) Escolha dos entrevistados** – Sendo uma abordagem qualitativa, as entrevistas não precisam reunir um grupo de pessoas que seja estatisticamente representativo da população. Contudo, os entrevistados devem ser escolhidos da forma que possam fornecer informações úteis a

respeito da população de interesse. **2) Agenda e horário** – Para diminuir os problemas de falta de agenda, é importante programar as entrevistas com um bom prazo de antecedência e confirmar alguns dias antes da entrevista propriamente dita. **3) Local das entrevistas** – Cabe ao moderador assegurar que estará disponível uma sala agradável para o encontro (climatização, mesa e cadeiras confortáveis, chá ou café são bem vindos). **4) Roteiro das questões** – No caso de entrevistas não estruturadas, o entrevistador explica os objetivos da pesquisa, confirma a intenção do entrevistado em colaborar e solicita que se inicie a discussão sobre o assunto. Nas entrevistas semiestruturadas, existirá um roteiro, o qual deverá ser coberto durante a entrevista. **5) Forma de registro dos dados** – é muito difícil escrever acompanhando o ritmo em que uma pessoa está falando. Ainda mais lembrando que o entrevistador deve estar prestando atenção, pronto para fazer questões que não estão no roteiro, caso necessário. Assim, a forma mais recomendada para o registro das informações é a gravação ou a filmagem.

Com relação ao roteiro de questões, o grupo obedeceu ao roteiro estabelecido na Figura 1.

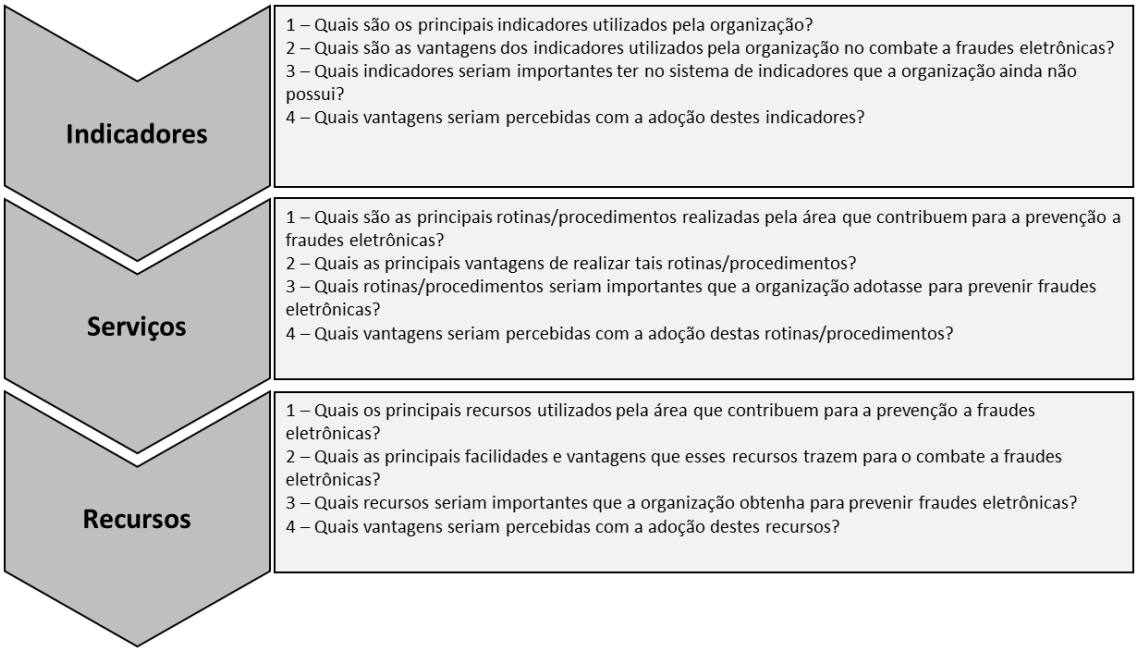

Figura 6 - Roteiro de Questões

Fonte: Elaborado pelos autores

O roteiro das perguntas foi elaborado levando em consideração três aspectos: (i) indicadores, (ii) serviços e, (iii) recursos. Os aspectos relacionados foram baseados no trabalho desenvolvido por Azevedo (2014) resultado da aplicação do QFD (*Desdobramento*

da Função Qualidade) integrado ao AHP (*Analytic Hierarchy Process*) com o objetivo de identificar requisitos para um processo de prevenção a fraudes eletrônicas. Quanto as perguntas, estas foram elaboradas com o objetivo de não somente mapear quais indicadores, serviços e recursos são utilizados pela organização e como os mesmos contribuem para a prevenção a fraudes mas, também, identificar quais indicadores, serviços e recursos há o anseio de serem adotados pela organização.

Para a realização do grupo focal, selecionou-se um grupo de 6 especialistas do setor de prevenção a fraudes eletrônicas. A seção de discussão ocorrida no primeiro trimestre de 2014 foi dirigida por uma pessoa, também especialista do setor, que exerceu a função de moderador. A discussão foi gravada para fins de avaliação posterior dos argumentos e ideias expressas pelos especialistas. Procurou-se registrar aspectos como: experiências, ideias, observações, descrições e necessidades apresentadas pelos participantes. O moderador tinha como funções: incentivar a participação de todos, buscando evitar o predomínio de algum participante sobre os demais, e manter a discussão nos limites dos tópicos de interesse.

A duração de cada uma das duas sessões de discussão realizadas foram de uma hora. Os participantes foram informados, no início das sessões, pelo moderador, da finalidade e do formato da discussão, do caráter informal da reunião e da necessidade da participação de todos. As sessões foram realizadas em ambiente de harmonia apropriado às finalidades propostas. Procurou-se contribuir para que as naturais divergências de opiniões não interferissem no desenvolvimento das discussões.

Os dados obtidos foram anotados, registrando-se a fala de cada participante e procurando refletir sobre o conteúdo da discussão. Posteriormente à realização da sessão de discussão, a equipe envolvida reuniu-se para analisar os dados obtidos mediante leitura cuidadosa dos registros. Na análise dos dados, procurou-se verificar as tendências e padrões das opiniões apresentadas.

3.1 Cenário de Pesquisa

A instituição financeira utilizada para a análise é uma organização que atua a mais de 20 anos no mercado financeiro nacional fornecendo aos seus clientes serviços financeiros através de canais eletrônicos. Com agências de atendimento distribuídas pelo Brasil, a organização possui mais de 3 milhões de clientes ativos, sendo aproximadamente 25% destes usuários, clientes frequentes de *Internet Banking* e 70% possuem cartões magnéticos de débito e crédito. É, segundo a FEBRABAN, uma das maiores instituições financeiras do

Brasil em ativos, possui um parque de aproximadamente cinco mil ATM's (*Automated Teller Machine*) para atendimento distribuído em agências, agentes credenciado e postos avançados.

O caso de estudo foi realizado no centro administrativo da instituição financeira onde os serviços de monitoramento de transações, bem como, estratégias de prevenção a fraudes são desenvolvidas.

3.2 Cenário de Aplicação

A área de prevenção a fraudes é composta por 10 integrantes distribuídos nas funções de gestão, monitoramento e tratamento de fraudes eletrônicas e integra uma superintendência de segurança juntamente com áreas de segurança patrimonial, numerários e da informação. A área não atua sobre fraudes de caráter documental ou internas, ou seja, o trabalho preventivo realizado pela área é estritamente relacionado aos canais eletrônicos.

No que tange as atividades, a composição da área e dividida em três blocos distintos, sendo eles: **(1) Tratamento de ocorrências:** Recuperar valores fraudados com outras instituições financeiras e avaliar as contestações de fraudes eletrônicas. **(2) Monitoramento de transações:** Contatar o cliente para confirmação de transações e monitorar transações realizadas nos canais eletrônicos. **(3) Estratégia e projetos:** Coordenar ações emergenciais e projetos de combate a fraudes, analisar os resultados de tratamento e monitoramento a fim de identificar comportamentos e tendências e, por fim, definir a estratégia de prevenção a fraudes.

Quanto a lotação da área, segue a seguinte estrutura:I - Gerente de Prevenção e Tratamento a Fraudes: Responsável por representar a área pela gestão da equipe, direcionamentos estratégicos a nível de prevenção a fraudes e corporativos. II – Coordenador de Prevenção e Tratamento a Fraudes: Gerenciamento operacional da equipe de analistas. III – Analista de Prevenção e Tratamento a Fraudes: Responsável por operacionalizar as rotinas de prevenção a fraudes.

4 Resultados e Discussões

Os resultados serão apresentados a seguir representando uma síntese das análises feitas pelo moderador do grupo focal. Os resultados são divididos conforme estrutura proposta na Figura 1.

4.1 Indicadores

Foi possível observar que os indicadores são tratados pela organização de maneira específica para cada canal ou produto financeiro. A principal razão, segundo os especialistas, para essa prerrogativa é o apontamento dos produtos financeiros mais frágeis, bem como, o acompanhamento exclusivo de cada produto ou serviço eletrônico oferecido pela instituição financeira. Além disso, os produtos financeiros possuem diferentes *modus operandi* de fraudes, logo, controlá-los de maneira agrupada pode trazer perdas à análise. Um exemplo desta afirmativa são os diferentes tipos de ataques que acontecem com o canal *internet banking* e com o cartão magnético. Enquanto com o primeiro a modalidade de ataque é tipicamente roubo de credenciais através de páginas falsas, o segundo é clonagem da trilha do cartão.

Dentre os indicadores citados pelos especialistas, o **volume financeiro fraudado, recuperado e prejuízo** é monitorado uma vez que para a maioria dos casos é possível a recuperação parcial ou total dos valores fraudados. O que define a recuperação parcial do volume fraudado é a natureza do produto financeiro, uma vez que diferentes produtos financeiros possuem diferentes controles aplicados. Identificar os controles e o quão eficiente estes são, trazem subsídios para a tomada de decisão e até mesmo a alocação de recursos para incrementar a segurança do produto financeiro. O prejuízo de cada produto financeiro serve de amparo para a tomada de decisão de investimento em segurança, pessoas, infraestrutura e até mesmo descontinuação do produto em certos casos.

O controle sobre a **primeira transação fraudulenta**, segundo os especialistas, é importante, pois verifica se ações tomadas no passado surtiram o efeito desejado, uma vez que a identificação da fraude pode ocorrer algum tempo depois de sua ocorrência tornando a análise da eficácia das ações mais complicada. É importante controlar esta "inércia" dos resultados, acompanhar a evolução pela data de detecção da fraude pode levar a constatações errôneas do cenário de fraudes.

Outro indicador que ocupou espaço nas discussões foi o **percentual de fraudes identificadas pelo monitoramento.** Este indicador é uma versão global do índice de eficiência das regras de monitoramento. Todas as transações eletrônicas devem ser avaliadas de maneira a haver uma comparação com comportamentos conhecidos de fraude. Quando uma transação fraudulenta não é identificada tem-se um falso negativo, e, na maioria das

vezes, a transação não é tratada em tempo hábil, o que minimiza as chances de resgate dos valores.

Os indicadores de monitoramento do processo de prevenção a fraudes trazem informações que direcionarão a tomada de decisão no curto, médio e longo prazo. Para o atingimento das metas definidas para os indicadores, procedimentos são estabelecidos para alcançar as metas estabelecidas para os indicadores. Na próxima seção será abordado os serviços que refletem diretamente nos indicadores.

4.2 Serviços

Na seção alocada para discussão dos principais serviços utilizados e desejados de prevenção a fraudes eletrônicas, os especialistas citaram atividades como: análise de *malwares*, monitoramento de páginas falsas *(phishing)*, contato com o cliente para confirmação de transações, tratamento dos eventos de fraudes, geração e atualização de regras de monitoramento e análise preventiva de produtos e canais financeiros. Dentre as atividades desejadas pela organização estão a análise de *malware* e o monitoramento de páginas falsas (*phishing*).

Segundo os especialistas, a **análise de *malware*** é uma prática não muito comum nas instituições financeiras devido a sua complexidade, pois exige conhecimento relativamente alto sobre reengenharia de *software*. Segundo os mesmos, atualmente, existem poucas instituições que desenvolvem esta atividade no mercado financeiro. Esta rotina visa buscar em repositórios de *malwares* ou em *links* disponibilizados por fraudadores contendo *softwares* maliciosos. Analisar constantemente estes artefatos implicaria em coletar informações de como esses *softwares* se comportam ao atacar os clientes, o que poderia ser revertido em maior segurança nos canais eletrônicos como: *Internet Banking e Mobile Banking*. Com relação ao **monitoramento de páginas falsas (*Phishing*)** esta é uma prática de prevenção a fraudes, pois busca na rede mundial de computadores *sites* que ludibriam os clientes e roubam suas credenciais de acesso. Atualmente existem ferramentas que proporcionam uma avaliação de páginas das quais foram desenvolvidas com o objetivo de enganar o cliente, fazendo com que o mesmo insira suas credenciais de acesso aos canais eletrônicos e estes sejam interceptados por fraudadores que o utilizarão para realizar fraudes em nome do cliente. Este serviço visa identificar as páginas e tomar ações para bloqueá-las ou impedi-las de roubar as informações dos clientes.

Na relação de atividades realizadas pela instituição, o **contato com o cliente** ainda é uma das práticas reativas mais eficazes do ponto de vista de bloqueio ou recuperação de valores fraudados. A instituição em pesquisa possui somente o contato realizado via telefone através de contato direto com o cliente, porém, há a sistemática de envio de mensagem SMS solicitando a confirmação de transações financeiras realizadas através de canais eletrônicos.

Para os casos onde a fraude eletrônica foi consumada, com ou sem prejuízo financeiro, cabe um trabalho de avaliação das fragilidades do canal eletrônico utilizadas pelo fraudador de maneira a propor medidas que aumentem a segurança dos canais. Este serviço, chamado **tratamento dos eventos de fraude**, subsidia a definição da estratégia a ser adotada. A **geração ou atualização de regras de monitoramento** têm forte influência do **tratamento dos eventos de fraude**, pois esta atividade é uma espécie de termômetro onde é possível perceber onde estão sendo realizados os ataques e com isso incrementar as regras de análise das transações. Logo, a geração ou atualização de regras de monitoramento é fortemente dependente dos resultados encontrados no **tratamento de eventos fraudulentos**.

No processo de desenvolvimento de produtos financeiros uma análise, sob a ótica de prevenção a fraudes, é realizada com o objetivo de identificar fragilidades no produto que ainda não foi disponibilizado para o cliente. Esta **analise preventiva de produtos e canais financeiros** corrobora para que cenários de fraudes acontecidos no passado, em produtos financeiros similares, sejam levados em consideração na etapa de desenvolvimento e tornem-se requisitos para os novos produtos e canais. Além disso, a experiência nas tratativas de eventos fraudulentos também ajuda na análise crítica de novos desenvolvimentos.

Uma vez identificados os serviços prestados pela instituição financeira, cabe identificar os recursos que suportam essas atividades. Na seção seguinte, serão apresentados os recursos utilizados pela organização para suportar as atividades de prevenção a fraudes.

4.3 Recursos

No que diz respeito aos recursos utilizados pelo processo de prevenção a fraudes eletrônicas foi possível perceber a forte dependência de um ***software*** **de monitoramento** utilizado para analisar as transações realizadas através dos canais eletrônicos. As funcionalidades deste *software* contemplam a possibilidade de geração de regras de monitoramento de transações. Essas regras são padrões de comportamento utilizados pelos fraudadores das quais, quando detectados, geram alertas de tratamento que, por sua vez, devem ser avaliados se trata-se de uma fraude ou um chamado falso positivo (transação que

tem características fraudulentas, porém, é lícita). Em alguns casos é necessário o contato com o cliente para solicitar a confirmação da transação, e para isso, o meio de contato é ativo e por **telefone**.

Todas as atividades realizadas por prevenção a fraudes são dependentes da avaliação de um especialista. Logo, o **especialista de prevenção a fraudes eletrônicas** é responsável por uma parte significativa da avaliação dos casos, estratégia de prevenção a fraudes e proposição de melhorias na segurança dos produtos e canais eletrônicos. Com isso, o contínuo desenvolvimento dos especialistas através de participação em fóruns, comitês, *benchmarkings*, etc. torna-se necessário a ponto de incluí-lo na relação de recursos essenciais ao processo de prevenção a fraudes eletrônicas.

4.4 Visão Geral

A relação dos critérios identificados no decorrer das sessões de grupo focal realizado com os especialistas em prevenção a fraudes eletrônicas podem ser verificadas na Figura 7.

Critérios		**Situação**	
		Integrado	**Desejado**
Indicadores	*Primeira transação fraudulenta*	X	
	Volume financeiro fraudado recuperado e perdido	X	
	*Percentual de fraudes identificadas pelo monitoramento**		X
Serviços	*Análise de Malware*		X
	Monitoramento de páginas falsas		X
	Contato com o cliente	X	
	Tratamento dos eventos de fraudes	X	
	Geração/Atualização das regras de monitoramento	X	
	Analise preventiva de canais e produtos financeiros	X	
Recursos	*Software de monitoramento*	X	
	Especialistas em prevenção a fraudes eletrônicas	X	
	Linha telefônica	X	

Figura 7 - Situação dos Critérios

Fonte: Elaborado pelos autores

Percebe-se que uma parcela dos indicadores e serviços não estão integrados ao processo de prevenção a fraudes, porém, há o anseio de integrar tais rotinas e indicadores ao processo. Segundo os especialistas, a análise de *malware* e monitoramento de páginas falsas trariam retorno no curto prazo. Ambas as atividades não previnem o ataque, porém, atuam de maneira proativa sobre um dos meios geradores de fraudes. Quanto ao percentual de fraudes identificadas pelo monitoramento, existe uma ressalva, pois o monitoramento geral a organização utiliza. O monitoramento específico por regra ainda não está integrado ao sistema de indicadores.

5 Considerações Finais

Este trabalho apresentou os resultados da aplicação de um grupo focal, objetivando ampliar o estudo de requisitos de um processo de prevenção a fraudes através da consulta direta a especialistas da área em uma instituição financeira. Esta reflexão crítica sobre um processo de prevenção a fraudes eletrônicas visa identificar indicadores, serviços e recursos utilizados e desejados por uma instituição financeira que oferece canais eletrônicos de atendimento a clientes. Para tanto, foi definido um roteiro de perguntas com o objetivo de direcionar o grupo focal e identificar os principais atributos que esse processo de prevenção a fraudes possui, bem como os desejados, para prevenir fraudes.

Na realização do grupo focal foi possível identificar os principais atributos utilizados pela instituição financeira para prevenção a fraudes eletrônicas no que tange a indicadores, serviços e recursos utilizados. Quanto aos indicadores, a utilização de métricas para acompanhamento de volume financeiro fraudado relacionado a valores recuperados e prejuízo, acompanhamento da primeira transação fraudulenta e percentual de fraudes identificadas pelo monitoramento foram listados como utilizados pela área. No que tange a principais serviços prestados pela área, foram listados análise de *malwares*, monitoramento de páginas falsas (*Phishing*), tratamento de eventos de fraudes, geração e atualização de regras de monitoramento e análise preventiva de produtos e canais eletrônicos. Quanto as questões relativas a recursos necessários para suportar os serviços de prevenção a fraudes, foram citados o *software* de monitoramento de transações eletrônicas, que contemple as funcionalidades de geração de alertas de monitoramento, uma linha telefônica para contato ativo com clientes, especialistas de prevenção a fraudes para tratamento dos casos e a participação continua em eventos (fóruns, comitês, *benchmarkings*, etc.) para troca de experiências com demais instituições financeiras e desenvolvimento de especialistas.

Como sugestão para trabalhos futuros indica-se a utilização da técnica de grupo focal voltado para identificar requisitos para o serviço de análise de malwares, uma vez verificado que tal serviço é uma atividade bastante complexa para as instituições financeiras e tende a contribuir na prevenção fraudes eletrônicas.

Referências

ALFURAIH, S. Using Trusted Email to Prevent Credit Card Frauds in Multimedia Products. **World wide web**, v.5, n. 3 p. 245 -256. 2002.

ALESKEROV, E., FREISLEBEN, B., Rao, B. CARDWATCH: A neural network based database mining system for credit card fraud detection. **IEEE/IAFE 1997 computational intelligence for financial engineering (CIFEr)** p. 220–226. 1997

ARVIDSON, M.; CARLBARK, M.; Intrusion detection systems – technologies, weaknesses and trends. **Department of Electrical Engineering, Linko ping University**. 2003.

BACEN – BANCO CENTRAL DO BRASIL. **Resolução Nº 3380.** Disponível em: http://www.bcb.gov.br/pre/normativos/res/2006/pdf/res_3380_v2_P.pdf Acessada em: 20/01/2014.

BELLA, M.A.; ELOFF, J.H.P.; OLIVER, M.S.; A fraud management system architecture for next-generation networks. **Forensic science international**. v. 185 n. 1 – 3 p. 51 – 58. 2008.

BENAROCH, M. Pricing e-service quality risk in financial services. **Electronic commerce research and applications** v.10 n. 5 p. 534 -544. 2011

BOUKERCHE, A.; NOTARE, M. S. M. A. Neural fraud detection in mobile phone operations. **Lecture Notes in Computer Science**, p. 636–644. 2000

BRAUSE, R.; LANGSDORF, T.; & HEPP, M. Neural data mining for credit card fraud detection. **11th IEEE international conference on tools with artificial intelligence** p. 103–106. 1999

BURGE, P.; SHAWE-TAYLOR, J.; COOKE, C.; MOREAU, Y., PRENEEL, B.; STOERMANN, C. Fraud detection and management in mobile telecommunications networks. **European conference on security and detection, ECOS 97** p. 91–96. 1997

BORGES, C.D.; SANTOS, M.A.; Aplicações metodológicas da técnica de grupo focal: fundamentos metodológicos, potencialidades e limites. **Rev.SPAGESP**, v.6, n.1, 2005.

CALISIR, F. Internet banking versus other banking channels: Young consumers' view. **International journal of information management** v.28 p. 215 -221. 2008

CAMPELLO, M. L. C.; COSTA NETO, P. L. O. A tecnoclogia como fator de competitividade dos bancos no Brasil. XXIV Encontro Nac. de Eng. de Produção – Florianópolis. 2004

ENSSILIN, L. Processo de Investigação e Análise Bibliométrica: Avaliação da Qualidade dos Serviços Bancários. RAC, Rio de Janeiro, v. 17, n. 3, pp. 325-349. 2013

FEBRABAN – Federação Brasileira de Bancos. – **FEBRABAN dá Dicas de Segurança Eletrônica**. Disponível em: http://www.febraban.org.br/Noticias1.asp?id_texto=1886&id_pagina=60&palavra= Acesso em: 22/01/2012

FEBRABAN – Federação Brasileira de Bancos. – **Pesquisa FEBRABAN de Tecnologia Bancária**. Disponível em: http://www.febraban.org.br/7Rof7SWg6qmyvwJcFwF7I0aSDf9jyV/sitefebraban/Pesquisa%20FEBRABAN%20de%20Tecnologia%20Banc%E1ria%202013.pdf Acesso em: 20/02/2014

GHOSH, M. Telecoms Fraud. **Computer fraud and security** v. 2010 n. 7 p. 14 -17. 2010.

GHOSH, S.; REILLY, D. L. Credit card fraud detection with a neural-network. **Twenty seventh Hawaii international conference on system science** v. 3 p. 621–630). 1994

GIL, A. C.. Como elaborar projetos de pesquisa. São Paulo. **Atlas**. 1991

LIN, H. An empirical investigation of mobile banking adoption: The effect of innovation attributes and knowledge-based trust. **International journal of information management** v.31 p.252 -260. 2011

ICT Statistics Newslog - **Report Predicts 894 Million Mobile Banking Users by 2015. News Related to ITU Telecommunication/ICT Statistics** . Disponível em: http://www.itu.int/ITU-D/ict/newslog/Report+Predicts+894+Million+Mobile+Banking+Users+By+2015.aspx Acesso em: 15/02/2014

IBBETT, G. Top Telco Frauds and How to Stop them. **Billing World and OSS Today Magazine**, Disponível em: http://www.billingworld.com/secondary.cfm?page=detail&archiveId=7824 Acessado em: 22/01/2014

JACOBS, R. **Telecommunications Fraud, Dimension Data White Paper**. Disponível em: http://www.didata.com/services/white_papers/Fraud_White_Paper. pdf Acessado em: 15/01/2014

KOU, Y.; LU, C.-T.; SIRWONGWATTANA, S.; HUANG, Y. Survey of fraud detection techniques. **In 2004 IEEE international conference on networking, sensing and control**, V. 2 p. 749–754). 2004

LEVESQUE, T; McDOUGALL, G. H. G. Determinants of customer satisfaction in retail banking. **International Journal of Bank Marketing**, v. 14, n. 7, p. 12-20, 1996.

MAHMOOD, T.; SHAIKH, G. M.; Adaptive Automated Teller Machines. **Expert systems with applications** v. 40 n. 4 p.1152 -1169. 2013

MAES, S.; TUYLS, K., VANSCHOENWINKEL, B.; MANDERICK, B.: Credit card fraud detection using bayesian and neural networks. **NF 2002**. p. 16-19 2002

MILLS, J E Cybercrimes against Consumers: Could Biometric Technology Be the Solution? **Internet Computing** v. 10 n. 4 p. 64 -71. 2006.

MOORI, R. G., MARCONDES, R. C., & ÁVILA, R. T.. A análise de agrupamentos como instrumento de apoio à melhoria da qualidade dos serviços aos clientes. **Revista de Administração Contemporânea**, p. 63-84. 2002.

MOREAU, Y.; PRENEEL, B.; BURGE, P.;SHAWE-TAYLOR, J.; STOERMANN, C.; COOKE, C.; Novel techniques for fraud detection in mobile telecommunication networks. **ACTS (Advanced Communications Technologies and Services)**. 1996.

MOREAU, Y.; VANDERWALLE, J. Detection of mobile phone fraud using supervised neural networks: A first prototype. **International Conference on Artificial Neural Networks** – p. 1065–1070. 1997

PAIVA, J. C. N., BARBOSA F. V., & RIBEIRO, A. H. P. Proposta de escala para mensurar o valor percebido no varejo bancário brasileiro. **Revista de Administração Contemporânea**, p. 310-327. 2009.

PROVOST, F. Statistical fraud detection: A review Statistical Science. **Statistical science** v. 17 n. 3. p. 235–255. 2002.

RESSEL, L. B.; BECK, C. L. C.; GUALDA, D. M. R.; HOFFMANN, I. C.; SILVA, R. M.;SEHEM, G. D.; O uso do grupo focal em pesquisa qualitativa. **Texto Contexto Enferm**, v.17, n.4, p. 779-86, 2008.

RIBEIRO, J. L. D.. Determinantes da satisfação e atributos da qualidade em serviços bancários. **Gest. Prod.**, São Carlos, v. 17, n. 4, p. 775-790, 2010

RIBEIRO, J. L. D.; MILAN, Gabriel Sperandio. Entrevistas Individuais: teoria e aplicações. Porto Alegre: FEENG/UFRGS, 2004.

SCHIEHLL, E., & MORISSETTE, R. Motivation, measurement and rewards from a performance evaluation perspective. **Revista de Administração Contemporânea**, p. 7-24. 2000

SOUZA NETO, A. F.; FONSECA, F. R. B.; OLIVEIRA, P. A. S. Dimenções do relacionamento e variáveis demográficas: uma investigação com base nas opiniões dos clientes de um grande banco brasileiro. **AENCONTRO NACI0ONAL DA ASSOCIAÇÃO NACIONAL DOS PROGRAMA DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO**. 2005

Yin, R.. **Case study research: Design and methods** (2nd ed.). Beverly Hills, CA: Sage Publishing, 1994.

IV CONCLUSÕES

Este trabalho teve como objetivo identificar requisitos para um processo de prevenção a fraudes eletrônicas em instituições financeiras. Para tanto, foram realizados estudos utilizando diferentes métodos e em diferentes períodos, trazendo resultados que possuem semelhanças e diferenças complementando-se um ao outro. Os estudos realizados: **(1)** estudo de requisitos da qualidade no processo de prevenção a fraudes eletrônicas em uma instituição financeira e **(2)** a utilização de métodos qualitativos para identificação de requisitos em um processo de prevenção a fraudes eletrônicas: estudo de caso envolvendo especialistas de uma instituição financeira, permitiram identificar requisitos para um processo de prevenção a fraudes eletrônicas de maneira a corroborar com o aumento da eficiência do serviço bancário e mitigar os riscos de ocorrência de fraudes nos canais eletrônicos.

Cada um dos estudos apresentados resultou em achados com grande quantidade de similaridades dos quais ratificaram parte dos requisitos encontrados em ambas as pesquisas. Porém, alguns dos resultados apontados não foram identificados nas duas pesquisas, o que oferece margem para discussões e análises dos resultados. Com relação as similaridades encontradas nos estudos, no que refere a **indicadores,** ambas as pesquisas apontaram para a identificação das transações fraudulentas pelo monitoramento, recuperação de valores fraudados e número global de fraudes, contudo, as pesquisas se complementam com relação aos indicadores de percentual de falsos negativos, percentual de falsos positivos, tempo de tratamento da fraude e primeira transação fraudulenta. No que diz respeito a **serviços** que corroboram com os objetivos de um processo de prevenção a fraudes eletrônicas, ambos os estudos convergiram na maioria dos serviços a serem prestados. A diferença ficou por conta do último estudo realizado que identificou a análise de *malwares* e monitoramento de páginas falsas (*phishing*) como serviços que devem ser executados por uma área de prevenção a fraudes eletrônicas. Cabe salientar que esta diferença pode estar na evolução do processo de prevenção a fraudes eletrônicas, uma vez que a diferença dos estudos é de cerca de um ano, logo, a evolução dos ataques aos usuários de *internet banking* aumentou o esforço das equipes de prevenção a fraudes eletrônicas que perceberam a adoção de subterfúgios para mitigar os riscos de fraudes eletrônicas.

Quanto aos **recursos** apontados por cada estudo como necessários para o estabelecimento de um processo de prevenção a fraudes, as diferenças limitaram-se a equipamentos de tecnologia da informação e ambiente controlado. O primeiro suporta os

recursos de *software* de monitoramento e o especialista em prevenção a fraudes para a análise de cenários de fraudes eletrônicas, o segundo, é um artifício para controlar as informações geradas na área de prevenção a fraudes de maneira que não venha a ser de domínio público informações sensíveis de ataques

		Estudo 1	**Estudo 2**
Indicadores	Percentual de fraudes identificadas pelo monitoramento	X	X
	Percentual de falsos negativos	X	
	Percentual de falsos positivos	X	
	Tempo de tratamento da fraude	X	
	Recuperação de valores fraudados	X	X
	Número global de fraudes	X	X
	Primeira transação fraudulenta		X
Serviços	Análise de *Malware*		X
	Monitoramento de páginas falsas (*phishing*)		X
	Contato com o cliente	X	X
	Tratamento de eventos de fraudes	X	X
	Geração/atualização de regras de monitoramento	X	X
	Análise preventiva de canais e produtos financeiros	X	X
Recursos	*Software* de monitoramento	X	X
	Especialistas em prevenção a fraudes eletrônicas	X	X
	Linha telefônica	X	X
	Equipamentos de Tecnologia da Informação	X	
	Desenvolvimento de competências	X	X
	Sala controlada	X	

Figura 8 - Visão geral

Fonte: Elaborado pelos autores

É possível perceber analisando a Figura 8 que os requisitos identificados para estabelecimento de um processo de prevenção a fraudes eletrônicas em cada estudo se complementam promovendo uma sinergia de apoio ao combate a fraudes. Os dois estudos, juntos, reuniram dezenove requisitos que direcionam o processo de prevenção a fraudes eletrônicas de maneira a otimizar recursos e esforço para reduzir o impacto financeiro causado pelas fraudes.

O resultado dos estudos demonstrou que um processo de prevenção a fraudes eletrônicas deve ser continuamente avaliado de maneira a identificar potenciais focos de ataques dos fraudadores. Esse esforço de identificar as fragilidades nos canais eletrônicos é

continuamente colocado a prova pelo avanço tecnológico. Os meios de contato do cliente com as instituições financeiras, bem como os meios eletrônicos de pagamento e movimentação financeira, são ampliados de tempos em tempos, o que implica em novos riscos de fraudes eletrônicas.

Esta orientação a avaliação continua dos canais eletrônicos não garante a total segurança dos mesmos, contudo, agrega valor ao minimizar as chances de ocorrência de ataques, e, torna-se um diferencial neste mercado onde a segurança e a confiabilidade são aspectos chave para avançar no mercado. As fraudes, de maneira geral, trazem perdas significativas a imagem e aos resultados da instituição ameaçando a saúde financeira das organizações.

Vale salientar que a influência social que as instituições financeiras promovem na sociedade vão além do desenvolvimento econômico. O trabalho em conjunto com outras instituições financeiras e com departamentos policiais de repressão a lavagem de dinheiro e crimes cibernéticos contribuem para que a sociedade avance na luta contra a corrupção e do financiamento ao crime organizado.

Referências

ABREU, F. S.; QFD - desdobramento da função qualidade - estruturando a satisfação do cliente. **Revista de administração de empresas [online],** 1997, vol.37, n.2, pp. 47-55. ISSN 0034-7590.

AKAO, Y.;**Quality function deployment: integrating costumer requirements in product design**. New York: Productivy Press, 1990.

ALFURAIH, S. Using Trusted Email to Prevent Credit Card Frauds in Multimedia Products.**World wide web**, v.5, n. 3 p. 245 -256. 2002.

ALESKEROV, E., FREISLEBEN, B., Rao, B. CARDWATCH: A neural network based database mining system for credit card fraud detection.**IEEE/IAFE 1997 computational intelligence for financial engineering (CIFEr)** p.220–226, 1997.

ARVIDSON, M.; CARLBARK, M.; Intrusion detection systems – technologies, weaknesses and trends.**Department of Electrical Engineering,Linko ping University**. 2003.

BACEN – BANCO CENTRAL DO BRASIL. **Resolução nº 3380.** Disponível em:<http://www.bcb.gov.br/pre/normativos/res/2006/pdf/res_3380_v2_P.pdf> Acesso em: 20 jan. 2014.

BELLA, M.A.;ELOFF, J.H.P.;OLIVER, M.S.; A fraud management system architecture for next-generation networks. **Forensic science international**. v. 185, n. 1-3, p. 51-58, 2008.

BENAROCH, M. Pricing e-service quality risk in financial services. **Electronic commerce research and applications,** v.10,n. 5, p. 534 -544, 2011.

BHATLA, T. P., VIKRAM, P., & DUA, A. Understanding Credit Card Frauds.**Cards Business Review1,**2003.

BOUKERCHE, A.; NOTARE, M. S. M. A. Neural fraud detection in mobile phone operations.**Lecture Notes in Computer Science**, p. 636–644, 2000.

BRAUSE, R.; LANGSDORF, T.;& HEPP, M. Neural data mining for credit card fraud detection. **11th IEEE international conference on tools with artificial intelligence**p. 103–106, 1999.

BURGE, P.; SHAWE-TAYLOR, J.; COOKE, C.; MOREAU, Y., PRENEEL, B.; STOERMANN, C. Fraud detection and management in mobile telecommunications networks. **Europeanconferenceonsecurityanddetection, ECOS 97,** p. 91–96, 1997.

COELHO, L. S.; RAITTZ, R. T.; TREZUB, M. FControl®:sistema inteligente inovador para detecção de fraudes em operações de comércio eletrônico.**Gestão e Produção[online]**. vol.13, n.1, p. 129-139, 2006.

DONG, W. et al. A feature extraction method for fraud detection in mobile communication networks. **Fifth world congress on intelligent control and automation,** p. 1853–1856, 2004.

FEBRABAN – FederaçãoBrasileira de Bancos. – **FEBRABAN dá Dicas de Segurança Eletrônica**. Disponível em: <http://www.febraban.org.br/Noticias1.asp?id_texto=1886&id_pagina=60&palavra=> Acesso em: 22 jan 2012.

FEBRABAN – Federação Brasileira de Bancos. – **Pesquisa FEBRABAN de Tecnologia Bancária**. Disponível em: <http://www.febraban.org.br/7Rof7SWg6qmyvwJcFwF7I0aSDf9jyV/sitefebraban/Pesquisa%20FEBRABAN%20de%20Tecnologia%20Banc%E1ria%202013.pdf> Acesso em: 20 fev. 2014.

GHOSH, M. Telecoms Fraud.**Computer fraud and security,** v. 2010,n. 7, p. 14 -17, 2010.

GHOSH, S.; REILLY, D. L. Credit card fraud detection with a neural-network. **Twenty seventh Hawaii international conference on system science** v. 3 p. 621–630, 1994.

GIL, A. C. **Como elaborar projetos de pesquisa**. São Paulo: Atlas. 1991.

ICT Statistics Newslog - **Report Predicts 894 Million Mobile Banking Users by 2015. News Related to ITU Telecommunication/ICT Statistics**. Disponívelem: <http://www.itu.int/ITU-D/ict/newslog/Report+Predicts+894+Million+Mobile+Banking+Users+By+2015.aspx>.Acessoem: 15fev. 2014.

IBBETT, G. Top Telco Frauds and How to Stop them. **Billing World and OSS Today Magazine.**Disponível em: <http://www.billingworld.com/secondary.cfm?page=detail&archiveId=7824> Acesso em: 22 jan 2014.

JACOBS, R.**Telecommunications Fraud, Dimension Data White Paper**. Disponível em: <http://www.didata.com/services/white_papers/Fraud_White_Paper. pdf> Acesso em: 15 jan 2014.

KOU, Y.; LU, C.-T.; SIRWONGWATTANA, S.; HUANG, Y. Survey of fraud detection techniques. **In 2004 IEEE international conference on networking, sensing and control**, v. 2, p. 749–754, 2004.

MAHMOOD, T.; SHAIKH, G. M.; Adaptive Automated Teller Machines. **Expert systems with applications,** v. 40,n. 4, p.1152 -1169, 2013.

MAES, S.; TUYLS, K., VANSCHOENWINKEL, B.; MANDERICK, B.: Credit card fraud detection using bayesian and neural networks. **NF 2002,** p. 16-19,2002.

MILLS, J E Cybercrimes against Consumers: Could Biometric Technology Be the Solution?**Internet Computing,** v. 10,n. 4, p. 64 -71, 2006.

MOREAU, Y.; PRENEEL, B.; BURGE, P.;SHAWE-TAYLOR, J.; STOERMANN, C.; COOKE, C.; Novel techniques for fraud detection in mobile telecommunication networks. **ACTS (Advanced Communications Technologies and Services)**. 1996.

MOREAU, Y.; VANDERWALLE, J. Detection of mobile phone fraud using supervised neural networks: A first prototype. **International Conference on Artificial Neural Networks,** p. 1065–1070, 1997.

PROVOST, F. Statistical fraud detection: A review Statistical Science.**StatisticalScience.** v. 17, n. 3, p. 235–255, 2002.

RIBEIRO, J. L. D.**A utilização do QFD na otimização de produtos, processos e serviços.**FEENG/UFRGS – Fundação Empresa Escola de Engenharia da Universidade federal do Rio Grande do Sul. 2001

SÁNCHEZ, D. Association rules applied to credit card fraud detection. **Expert systems with applications,** v.36,n.2, p. 3630 -3640, 2009.

TASSABEHJI, R.; KAMALA, M. A. Evaluating biometrics for online banking: The case for usability. **International journal of information management,** v.32,n.5, p.489 - 494, 2012.

VIANE, S.; DEDENE, G.; DERRIG, R. Auto claim fraud detection using Bayesian learning neural networks. **Expert Systems with Applications: An International Journal**, p. 653–666, 2005

Yin, R. **Case study research: Design and methods** (2nd ed.). Beverly Hills, CA: Sage Publishing, 1994.