CRIMES E FRAUDES ELETRÔNICOS: PERSPECTIVAS DE AÇÕES EMPRESARIAIS ADOTADAS POR INSTITUIÇÕES FINANCEIRAS

Ana Cristina Azevedo Pontes de Carvalho

Coordena a Especialização em Computação Forense da Universidade Presbiteriana Mackenzie. E-mail: anacristina.carvalho@mackenzie.br.

Raquel Cymrot

Professora da Universidade Presbiteriana Mackenzie.
E-mail: raquelc@mackenzie.br.

Eduardo Pozze

Analista de prevenção a fraudes e atos ilícitos. E-mail: du_pozze@hotmail.com.

Roque Theophilo Junior

Professor da Faculdade de Direito da Universidade Presbiteriana Mackenzie.
E-mail: roque.theophilo@mackenzie.br.

RESUMO

O presente artigo discorre sobre crimes eletrônicos que envolvem as instituições financeiras bancárias, abordando alguns métodos que os criminosos utilizam para fraudar essas instituições. O objetivo deste trabalho é analisar estatisticamente os crimes e fraudes eletrônicos dessa espécie ocorridos em 2009 na cidade de São Paulo, estudando suas características e fazendo a relação espacial, temporal e preditiva desse tipo de crime nas instituições financeiras bancárias, tendo em vista relacionar as características das fraudes e o modo como afetam, principalmente, essas instituições. A metodologia baseia-se em uma pesquisa de caráter qualitativo e exploratório, precedida de uma pesquisa documental para o levantamento de conceitos que embasaram a revisão bibliográfica. Os resultados identificaram a influência das variáveis: região, mês e faixa horária nas condutas pesquisadas, estabelecendo-se a relação espacial e temporal com base nos testes de independência, e geraram um modelo estatístico de previsão para os crimes de fraudes eletrônicas bancárias, o qual se mostrou adequado para a previsão de ocorrência. Conhecendo-se a região, o mês e a faixa horária, poderá se estimar com maior probabilidade de acerto se ocorrerão crimes de fraude eletrônica ou não. Concluiu-se pela existência de relação entre algumas variáveis e os crimes de fraude eletrônica, a qual demonstra ser possível a adoção de métodos preventivos, podendo embasar projetos de lei junto à Câmara dos Deputados, assim como levar essas instituições a agir de maneira preventiva e coerente com relação aos crimes de fraudes eletrônicas, a fim de inibir este tipo de criminalidade dentro das instituições financeiras bancárias.

PALAVRAS-CHAVE: *Fraudes eletrônicas. Melhoria de processo. Predição. Variáveis socioeconômicas.*

ABSTRACT

The present paper discusses on electronic crimes that involve the financial banking institutions, approaching methods which criminals are used to commit frauds against those institutions. Its objective is to analyze statistically the crimes regarding electronic frauds committed in Sao Paulo in 2009, studying their characteristics and making the spatial, temporal and predictive relations of those crimes in the financial banking institutions, aiming to relate the frauds' characteristics and the mode that they mainly affect these institutions. The methodology was based on a qualitative and exploratory research, preceded by a documental research in order to get concepts to compose the bibliographic revision. The results identified the influence of the variables: region, month and time in the researched procedures, making the spacial and temporal relation based on independence tests. These results also originated a statistical prediction model to the crimes regarding electronic frauds, which is able to predict their occurrences. Electronic fraud crimes will be estimated with a higher probability of success if we know the region, the month and the time period. A established relation between some variables and the crimes regarding electronic frauds was the conclusion of this research, which demonstrates that it is possible to adopt preventive methods and to back up law projects at the Congress and can also lead the institutions to act in a preventive and coherent way when relating to electronic fraud crimes, aiming to restrain this kind of criminality inside the financial banking institutions.

KEYWORDS: *Electronic fraud. Process improvement. Prediction. Socioeconomic variables.*

RESUMEN

El presente artículo trata sobre crímenes electrónicos que envuelven a las instituciones financieras banqueras, abordando algunos métodos que los criminales utilizan para defraudar esas instituciones. El objetivo es analizar estadísticamente los delitos de fraudes electrónicos ocurridos en 2009 en San Pablo, sus características y hacer la relación espacial, temporal y predictiva de este tipo de delito en las instituciones financieras, teniendo en vista relacionar las características de los fraudes y el modo cómo afectan, principalmente, a esas instituciones. La metodología se basa en una investigación cualitativa y exploratoria, precedido por una investigación documental para estudiar conceptos que apoyaron la revisión de la literatura. Los resultados mostraron la influencia de las variables región, mes y ranura de tiempo de las conductas investigadas, el establecimiento de la relación espacial y temporal basada en test chi-cuadrados y generaran un pronóstico modelo estadístico para los delitos de fraudes electrónicos adecuado para predecir eventos. Conociendo la región, el mes y el período de tiempo, se puede estimar con mayor probabilidad de éxito si

se pueden ocurrir delitos de fraude electrónico o no. Se concluyó que existe alguna relación entre las variables y los delitos de fraudes electrónicos, lo que demuestra que es posible adoptar métodos preventivos, pudiendo implicar propuestas de ley junto à la Cámara de los Diputados, así como pueden llevar esas instituciones financieras a actuar de manera preventiva y coherente con relación a los crímenes de fraudes electrónicos, con el objetivo de reducir este tipo de criminalidad dentro de las instituciones financieras banqueras.
PALABRAS CLAVE: *Fraudes electrónicos. Mejora de procesos. Predicción. Variables socioeconómicas.*

INTRODUÇÃO

Devido ao crescimento populacional, demográfico, financeiro e socioeconômico da população mundial encontram-se atualmente, no mundo todo, grandes centros urbanos organizados, nos quais há governos que aplicam políticas de melhoria de vida de acordo com suas necessidades como, por exemplo, educacional, de saúde, segurança e econômico.

Dentro desses centros urbanos encontram-se diversos fatores e indicadores de crescimento. Um desses fatores de desenvolvimento é a segurança pública e privada que está de certa forma, relacionada com a criminalidade, cujo aumento seria um fator negativo de tais locais. Junto ao crescimento econômico social e cultural têm-se variáveis negativas que também são indicadores como, por exemplo, a desigualdade socioeconômica, desemprego populacional, falta de estrutura de governo perante a sociedade e falta de oportunidade de desenvolvimento de toda a população.

A criminalidade faz parte de toda e qualquer sociedade. Tendo os crimes organizados concentrados, em geral, nos centros urbanos, consegue-se ter apenas mapas de criminalidade com foco na análise sazonal e temporal para obtenção de dados sobre ações criminalísticas.

Com o aparecimento das novas tecnologias surgiram também alguns problemas legais associados. A rápida evolução destas novas tecnologias levou à existência de "vazios legais" e à difícil definição de crime informático (BRANCO, 2004, p. 01).

Com o avanço e desenvolvimento de uma sociedade, em conjunto vem o avanço e desenvolvimento tecnológico com a inclusão digital e a facilidade em transmitir dados com aparelhos eletrônicos. O aparecimento da *Internet* é um facilitador para a população, de um modo geral, devido à

sua flexibilidade de sistema de rede e sua facilidade de pesquisa, atualização e entretenimento.

Contudo, indivíduos infaustos têm se utilizado desses meios de telecomunicações para se aproveitar da falta de conhecimento e descuido da população (PINHEIRO, 2007). São exemplos desses delitos a invasão de sistemas computacionais para fraudar contas bancárias eletronicamente, enganar indivíduos para prejudicá-los moralmente e ludibriar instituições financeiramente, expondo instituições e indivíduos de forma errônea, ferindo a integridade e idoneidade.

As instituições financeiras são um dos alvos dos fraudadores para suas ações. Para que esse tipo de instituição tenha uma política de segurança corporativa competente, é necessário um modelo de previsão de ações que vão de encontro aos crimes de fraudes eletrônicas, com intuito de auxiliar na ação preditiva, estudando como são feitas essas ações, em que época, onde e qual a sua tempestividade, para nortear a tomada de decisões e melhorar a implementação de processo de segurança.

Escolheu-se, assim, o tema em questão para a pesquisa que originou o trabalho de conclusão de curso apresentado à Escola de Engenharia da Universidade Presbiteriana Mackenzie em 2010, do qual resulta o presente artigo, cujo objetivo geral é analisar estatisticamente os crimes de fraudes eletrônicas praticados contra instituições financeiras bancárias na cidade de São Paulo no ano de 2009, a fim de buscar a relação espacial e temporal dessas ações e por meio de um plano com meios estratégicos preditivos e preventivos, obter ações empresariais coerentes para tomada de ações efetivas pelas instituições financeiras bancárias.

Os objetivos específicos são:

a) Levantar dados de instituições financeiras bancárias com relação a crimes de fraudes eletrônicas na cidade de São Paulo.

b) Fazer a relação espacial e temporal quantitativamente desses crimes por meio de métodos estatísticos.

c) Apresentar uma abordagem com planos de melhoria no processo de tomada de decisão, de maneira a prevenir as instituições financeiras bancárias desse tipo de crimes.

Com o crescimento de compra, venda e troca de produtos, serviços e informações por meio do comércio eletrônico e com o pagamento dessas transações sendo realizado, em sua maioria, por cartões de crédito, tem ocorrido um aumento de crimes de fraudes eletrônicas relacionadas com a *Internet* e seus meios de propagação (INÁCIO, 2009). A partir dessas análises de crimes de fraudes eletrônicas o presente trabalho poderá auxiliar na tomada de decisão de ação preventiva e preditiva nas instituições financeiras bancárias envolvendo crimes de fraudes eletrônicas. Com isto, poderá haver um ganho para a população que estará menos sujeita a esses tipos de crimes e um ganho econômico para as instituições financeiras que muitas vezes tem de arcar com o prejuízo de seu cliente. Muitos trabalhos de investigação e ressarcimento poderão ser evitados, bem como, poderá haver até mesmo uma economia de equipamentos, energia etc., devido às ações administrativas que seriam desnecessárias.

A metodologia baseia-se em uma pesquisa de caráter qualitativo e exploratório, precedida de uma pesquisa documental para o levantamento de conceitos que embasaram a revisão bibliográfica, baseada principalmente na doutrina de autores como Barros, Branco, Cramer, Farhat, Febraban, Inácio, Lordello, Parodi, Pinheiro e Montgomery e Runger. A seguir foram coletados dados quantitativos de crimes de fraudes eletrônicas em instituições financeiras bancárias na cidade de São Paulo. Os dados coletados durante este trabalho foram obtidos pelos autores diretamente das pessoas responsáveis pelo setor de fraudes eletrônicas das instituições financeiras bancárias públicas e privadas, após a contabilização dos números sobre crimes de fraude eletrônica, por isso os referidos dados são tratados de maneira confidencial. A proposta detalhada para coleta dos dados foi submetida e aprovada pela Comissão de Ética em Pesquisa da Escola de Engenharia da Universidade Presbiteriana Mackenzie, e foram devidamente assinados o Termo de Consentimento Livre e Esclarecido e a Carta de Informação à Instituição.

A partir desses dados foi realizada uma análise descritiva e realizados testes de independência entre haver ou não fraude e variáveis de interesse. Por meio de um teste de aderência, variáveis relacionadas com o perfil dos indivíduos que sofreram fraude foram comparadas às da população em geral (SIEGEL; CASTELLAN JR, 2008).

Foi então construído um modelo de previsão de fraudes baseado em regressão logística (MONTGOMERY; RUNGER, 2009). Para todos os testes de hipótese foram calculados seus respectivos níveis descritivos sendo esses comparados com o nível de significância de 5%. As análises foram realizadas utilizando-se o programa Minitab® (MINITAB, 2015).

REVISÃO DA LITERATURA

Fraudes na Internet

A fraude na *Internet* é um conceito inovador que precisa ser muito bem analisado e compreendido. Devido ao fato deste tipo de criminalidade ser um conceito novo suas denúncias não são muito comuns, mas, acontecem em grande quantidade. Há um despreparo da polícia e perícia investigativa com relação à fraude na *internet* no Brasil, por exemplo, não temos muitas equipes preparadas para tal acontecimento (PINHEIRO, 2007).

O combate a esses crimes torna-se extremamente difícil por dois motivos: a) a falta de conhecimento do usuário, que dessa forma, não passa às autoridades informações relevantes e precisas; e b) a falta de recursos em geral das autoridades policiais (PINHEIRO, 2007, p. 255).

Ou seja, com a disseminação da *Internet* pode-se dizer que o crime informático ainda é um crime sem fronteiras e, segundo Pinheiro (2007) podem ocorrer crimes a quilômetros de distância do local onde foi efetuado. Tal fator gera dificuldade em se ter a localização e os verdadeiros fraudadores, isto servindo então como um facilitador para o criminoso, a utilização deste tipo de crime devido ao anonimato proporcionado.

Quem realiza esse tipo de crimes eletrônicos são indivíduos chamados *hackers* ou, também chamados de piratas informáticos (PINHEIRO, 2007), que conseguem acesso não autorizado a determinado sistema ligado a uma rede de computadores. Com o conhecimento que têm desses sistemas computacionais, fazem a interceptação de dados sigilosos provocando danos às pessoas, instituições públicas e privadas que acabam sendo fraudadas por meio de redes de serviços. Ainda segundo Pinheiro (2007), há duas categorias de *hackers*, o *White Hats* e o *Black Hats*. Estes primeiros são criminosos que cometem crimes eletrônicos invadindo o sistema de rede de instituições e depois que a invasão a este sistema é bem-sucedida, revelam ao presidente ou dono da instituição e ao gerente de sistemas de rede computacional quais são as falhas que este possui, podendo até consertá-las e com isto ganhar algum benefício por este tipo de informação fornecida à instituição. Os *Black Hats* são *hackers* profissionais, seus estudos para invasão de sistema são, na maioria das vezes, financiados por governos para espionagem e extravio de informações secretas, trabalho esse que era muito utilizado em épocas passadas, como por exemplo, na Guerra Fria, para que um país pudesse invadir um sistema computacional de redes de um outro país confrontante, podendo conseguir informações confidenciais e sigilosas (PINHEIRO, 2007).

De acordo com Barros (2006), têm-se mais duas categorias de indivíduos com conhecimento e aprimoramento de técnicas de computadores para invasão de sistemas em redes, a saber: os *crackers* e os *lamers*. Os *crackers* são indivíduos com técnicas aprofundadas em informática, conhecimento e aprimoramento de computadores. São indivíduos com o mesmo conhecimento de um *hacker. A* diferença está quando ocorre a invasão de um sistema computacional em rede: os *crackers* têm a finalidade de destruir banco de dados, apagar ou copiar programas e quaisquer códigos operacionais. Já os *lamers* também são indivíduos com um conhecimento muito grande de informática. Eles conseguem criar programas maliciosos que propagam vírus para um sistema de redes de computadores, denegrindo e afetando seu funcionamento (BARROS, 2006).

De acordo com Pinheiro (2007), os crimes eletrônicos ou informáticos são atribuídos em sua maioria, aos próprios usuários do sistema computacional, devido à falta de conhecimento e também, à falta de interesse nas informações sobre segurança destes próprios sistemas. Sendo assim, os usuários são os alvos mais visados pelas instituições públicas e privadas para uma mudança de atitude, no que se diz respeito à segurança da informação como, por exemplo, colocar senhas de acesso de difícil decifração.

Primeiramente, um código malicioso é enviado por *e-mail* para as vítimas, as quais, não analisando a veracidade do conteúdo nem o remetente da mensagem, acessam a informação, executam o arquivo e, consequentemente, o computador do usuário é infectado, comprometendo suas informações confidenciais, tais como, senhas, dados pessoais etc. Essas informações são transmitidas para o fraudador, que as utiliza para acessar, por exemplo, o *Internet Banking* da vítima e desviar dinheiro para outra conta (PINHEIRO, 2007, p. 265).

Para Pinheiro (2007, p. 180), "a evidência de digital é toda a informação/intervenção humana ou não, que pode ser extraído de um computador ou de dentro de outro dispositivo eletrônico". Ainda segundo a autora, essas evidências, muitas vezes, estão no formato de entendimento humano. Toda informação importante tem que se utilizar de uma ferramenta ou técnica de busca, tratamento de evidências na investigação de crimes eletrônicos, requerendo competências específicas, análise de dados e tratamentos de evidências.

A *Internet* é um meio de propagação de informações, dados e aplicativos que, por sua vez, abrange um sistema em rede de computadores. Com a evolução desse tipo de tecnologia e a facilidade de obter algumas vantagens com relação à velocidade da informação e transferências de dados,

muitas pessoas estão utilizando este sistema em rede para transferência de informações, sendo estas, por exemplo, de cunho confidencial, pagamento de contas, compra de produtos e até mesmo, o uso do *e-mail* para comunicação e recados (CERT.BR, 2006).

Ainda, o CERT.br discorre que os criminosos, sabendo das vulnerabilidades das pessoas, têm usado a *Internet* para cometerem crimes que, em sua maioria, tentam induzir o usuário do sistema a fornecer seus dados pessoais e financeiros ou, até mesmo, instalar algum programa que contenha código malicioso para extração de material com dados sigilosos pessoais, senhas de *e-mail* e também de cartões magnéticos, podendo se utilizar destes, futuramente de maneira fraudulenta. Os usuários da *Internet* têm que ter alguns cuidados relacionados à segurança da informação contido em seus computadores, para que não ocorra a apropriação de seus dados confidenciais pessoais por criminosos, principalmente quando se trata de um serviço de comércio eletrônico.

O CERT.br fez uma cartilha sobre Segurança para *Internet* que inclui, em parte desta cartilha, as fraudes na *Internet*. Os tópicos a seguir, apresentarão o conteúdo relacionado a quatro tipos de fraudes com uso da *Internet* contido nesta cartilha, decorrido nos pontos a seguir.

Scam

Denomina-se *scam* ou golpe, todo e qualquer ato fraudulento mediante uso da *Internet* que tem por objetivo a vantagem financeira.

São páginas da *Internet* montadas por criminosos que oferecem serviços de venda de produtos com uma situação atrativa de compra, com preços relativamente muito abaixo dos praticados no mercado comum. Após efetivar a compra do produto pelo *site* fraudulento o indivíduo, muito provavelmente, não receberá o bem ou, receberá um produto que não condiz com o que estava sendo mostrado na *Internet* e isso não significa que o produto está com defeitos, significa dizer que não é o mesmo. Além de o consumidor ser desfavorecido com o serviço prestado pelo *site* em relação à obtenção do produto pago, os criminosos, por sua vez, usarão os dados pessoais e financeiros concedidos pela vítima na compra do bem, podendo até, obter a senha do cartão magnético da vítima, mediante o uso desse mecanismo na compra do produto pelo *site*.

Um tipo comum de s*cam* é através do recebimento de *e-mail*s. O mais conhecido é o *Advanced Fee Fraud* (Fraude de Antecipação de Pagamentos). Esse tipo de golpe é realizado em nome de alguma instituição governamental, geralmente da Nigéria (FBI, 2015). Consiste no recebimento do

e-mail pelo usuário com assunto de cunho confidencial sobre transferência de milhões de dólares ou euros de fundos internacionais, sendo a vítima um intermediário que terá direito a uma participação dos lucros da transferência, em porcentagem, do valor mencionado na mensagem. Para a vítima ter essa participação terá que pagar antecipadamente uma taxa que, geralmente tem o valor elevado, para arcar com as transferências do fundo. Após a vítima se submeter a pagar essa taxa, estará enviando seu dinheiro para o criminoso que enviou este *e-mail* e a vítima, não terá a porcentagem do valor mencionado na mensagem como prometido.

A situação apresentada no exemplo acima é um dos *scams* mais utilizados pelos criminosos, podendo surgir novas formas de fraude com intuito de tirar vantagem financeira da vítima.

Phishing

Este tipo de fraude consiste no envio de mensagens de e-mail para alguns usuários em nome de uma determinada instituição financeira, visando à indução do usuário para acesso do *site* da instituição utilizado no *e-mail* fraudulento (FBI, 2013). Depois que a vítima acessar o *site*, os criminosos são capazes de obter os dados pessoais e financeiros destas, a fim de ter o privilégio dessas informações confidenciais.

Neste tipo de fraude são usadas mensagens de *e-mail* para que as vítimas instalem programas de teor fraudulento ou, preencham formulários com requisitos pessoais e financeiros. Tendo, estes dois tipos de características de fraudes, o objetivo de capturar os dados pessoais dispostos pelas vítimas na rede de computadores e utilizá-los de forma fraudulenta.

No Brasil, são amplamente conhecidas, pelo menos, quatro situações que vêm sendo utilizadas por criminosos, exemplificando o caso do *phishing*.

a) O primeiro modo de atuação dos criminosos é quando o usuário do *e-mail* recebe uma mensagem abordando um assunto para atrair sua atenção. Sendo, provavelmente, o assunto tratado para que a vítima obtenha vantagem financeira ao realizar algum negócio ou transação e, também pode conter o assunto de que, a vítima poderá ter o cancelamento da sua conta bancária ou seu nome colocado em protesto se não proceder de maneira correta ao executar o *e-mail*.

   De acordo com o teor dessa mensagem, a vítima clica no *link* do *e-mail* ou executa algum programa com teor corrompido. Após a vítima clicar nesse *link* e executar o programa corrompido,

aparecerá uma mensagem de orientação para salvar o programa em sua máquina. Esse programa, após ser instalado, tem a finalidade de furtar os dados pessoais, financeiros e senhas de cartões de banco. O programa pode recuperar movimentos de teclas e posições do cursor em telas acessadas pelo usuário, mapeando assim, a máquina da vítima. Depois do mapeamento da máquina, o programa envia mensagens de *e-mail* para o fraudador com todos os resultados das pesquisas realizadas para o criminoso poder utilizar os dados da vítima para a fraude.

b) O segundo modo de atuação dos fraudadores na utilização do *phishing* é um processo parecido com o anterior. O usuário do *e-mail* recebe uma mensagem com assunto de alguma promoção para atrair sua atenção e, desta maneira, será necessária a confirmação de alguns dados pessoais para participar da promoção. Mas, ao contrário do exemplo anterior, neste tipo de *phishing* o usuário clica diretamente no endereço de um *site* que será direcionado para uma página de *Internet* falsificada. Neste ambiente é solicitado à vítima que preencha algum tipo de formulário com seus dados pessoais e financeiros como, por exemplo, número e senha de seu cartão de crédito. Após o preenchimento dessas informações pela vítima e seu respectivo envio, os dados estarão dispostos para os criminosos, criadores da página de *Internet* falsificada. Com os dados pessoais e financeiros da vítima, os criminosos irão utilizar os dados da vítima para a fraude.

c) O terceiro modo de atuação dos fraudadores por intermédio do *phishing* é o acesso do usuário a uma página de comércio eletrônico ou acesso à *Internet* de uma instituição bancária, sendo direcionado para uma página falsificada. Esse tipo de redirecionamento do usuário para *sites* fraudulentos, mesmo o usuário digitando o endereço do site corretamente no *browser*, é chamado de *pharming*. O *pharming* tem por finalidade comprometer, de maneira eficaz, o serviço de resolução dos nomes dos *sites*, corrompendo o DNS (Domain Name System). O DNS é um sistema de gerenciamento de nomes e distribuição de operações, ou seja, permite a localização de todos os computadores que estão ligados a uma determinada rede e em um determinado domínio. Depois que é realizado todo este processo para um *site* fraudulento, a

vítima não perceberá que está em um domínio de *site* fraudulento e preencherá campos de dados pessoais e financeiros nas páginas falsificadas. Portanto, as informações serão transmitidas para os fraudadores que irão realizar as operações fraudulentas utilizando os dados da vítima.

d) O quarto modo de atuação dos criminosos com relação ao uso do *phishing* é a obtenção do acesso ao *site* de uma instituição bancária por intermédio de computadores de terceiros, por exemplo, em uma *Lan House*. Os aparelhos de terceiros são utilizados por diversas pessoas e, é capaz de ter sido instalado algum programa malicioso na máquina. Ao realizar algum tipo de transação bancária na máquina infectada, o usuário, através de um *site* terá suas ações totalmente monitoradas por programas maliciosos. Após o uso da máquina pela vítima, o fraudador pode usar a mesma máquina e retirar as informações necessárias para realizar suas operações com objetivo de vantagem financeira, lesando os usuários das máquinas.

Boatos

Tipo de fraude que tem por base os assuntos que são provenientes do uso da *Internet*. São *e-mails* com conteúdos falsos que têm como remetente uma instituição financeira bancária ou uma empresa renomada. Com a promessa de algum ganho financeiro, com a realização da ação proposta no *e-mail* ou consequências graves para o leitor do *e-mail*, caso esse não realize a tarefa do conteúdo. O *e-mail* solicita o encaminhamento da mensagem recebida para o maior número de usuários possíveis, como um exemplo de boatos podemos citar as correntes. Esse tipo de mensagem tem a finalidade de espalhar a desinformação sobre um determinado assunto ou criar certa situação de confronto entre pessoas ou instituições privadas e públicas, tendo o fraudador objetivo de maximizar o tempo que esse tipo de *e-mail* fraudulento permanece na *Internet* e sua consequente propagação. Esta transferência de *e-mails* é devido ao receptor da mensagem ter uma certeza de que o conteúdo do *e-mail* é verdadeiro, de fato, conhecendo a instituição que o enviou, por isso, encaminham para outros usuários tendo a certeza de que estão fazendo o correto. A maioria das vezes não é uma fraude efetiva porque só ocupa espaço na caixa de *e-mail* dos usuários que a recebem e não tem por objetivo espalhar vírus.

Existem ainda alguns casos de *e-mail* contendo boatos comoventes, que podem fazer com que os usuários, ao lê-los, acabem por fornecer informações pessoais e financeiras.

E-mail falso

O objetivo e a característica mais marcantes de um fraudador para se utilizar de um *e-mail* falso é assustar o usuário do sistema para depois buscar o êxito na fraude (SECRETARIA DA RECEITA FEDERAL DO BRASIL, 2005). Neste caso é utilizado um sistema pelo fraudador que tem como recurso identificar endereços de instituições financeiras públicas e privadas como fonte de envio do *e-mail* falso. Dessa forma, pode-se ter o campo de remetente do *e-mail* preenchido com o nome de instituições bancárias públicas e privadas conhecidas. Um exemplo disso é o *e-mail* contendo notificações dessas instituições com conteúdo de mensagens relacionadas ao cancelamento do Cadastro de Pessoa Física (CPF) ou pendente regularização de documento, inclusive, um encaminhamento do nome do usuário ao Serviço de Proteção ao Crédito (SPC), podendo levar o usuário a crer que o *e-mail* é realmente verdadeiro.

Fraude em cartão magnético

Para Nascimento e Pereira (2005) as fraudes eletrônicas estão relacionadas com o universo das fraudes contábeis e financeiras sendo definidas as fraudes contábeis em "[...] aquelas que ocorrem no registro contábil dos fatos ocorridos nas empresas e, por sua natureza, agridem o ambiente interno e externo do negócio" (NASCIMENTO; PEREIRA, 2005, p. 58) e, definidas as fraudes financeiras como "[...] são aquelas que agridem diretamente as operações que envolvem valores monetários no ambiente interno das empresas" (NASCIMENTO; PEREIRA, 2005, p. 61). Portanto, observa-se que com a definição dada por Nascimento e Pereira (2005) para fraudes contábeis e financeiras é, de fato, possível englobar a fraude eletrônica nesse contexto, com a possibilidade de ocorrer um registro contábil de um caso, por exemplo, que ocorreu em um ambiente amplo para exploração e análise, podendo até mencionar o ambiente externo da fraude, que seria da pessoa fraudada e, o ambiente interno, que seria o ambiente da invasão do sistema operacional da rede de computadores da instituição financeira bancária. O tipo financeiro mencionado por Nascimento e Pereira (2005) é definido pelo montante extraído da conta na transação fraudulenta, no qual se tem a perda de dinheiro da pessoa fraudada, tornando essa pessoa e a instituição financeira as maiores lesadas pela fraude.

De acordo com Pinheiro (2007), fraudes eletrônicas podem ser de origem interna e externa. A fraude eletrônica interna é quando o indivíduo fraudador tem algum tipo de vínculo empregatício com a instituição, alvo da fraude como, por exemplo, um funcionário realizando a fraude no local de trabalho através do conhecimento adquirido no sistema operacional da rede institucional. Por sua vez, a fraude eletrônica externa, que ocorre quando o fraudador não tem nenhuma relação interna ou vínculo empregatício com a instituição ou indivíduo, que é alvo da fraude.

Para Parodi (2008), a fraude com cartão de crédito também é um ato comum de indivíduos que agem de má índole para prejudicar pessoas e instituições a fim de se favorecer desse ato. Sendo que, esses tipos de fraudes envolvem pequenas quantias e acarretam grandes problemas para as pessoas fraudadas e instituições financeiras.

Observa-se que para a maioria dos *modus operandi* deste tipo de fraude são necessários um cartão clonado e alguns dados sobre a pessoa fraudada. Após o fraudador ter o cartão clonado e alguns dados dessas pessoas em mãos, ele fará algumas compras e usará a conta da vítima para debitar as compras ou transações. Neste caso sempre vai se utilizar de máquinas para executar a clonagem dos cartões de crédito, técnica muito usada nos dias de hoje (PARODI, 2008).

Outra técnica ressaltada por Parodi (2008) é a utilização pelos fraudadores de ligações para algum número telefônico nos quais se identificam como sendo funcionário da empresa de cartão de crédito, perguntando dados pessoais e se aproveitando da boa vontade das pessoas para se beneficiar e encontrar a senha ou assinatura eletrônica do cartão a fim de que essa seja utilizada em aquisições posteriores.

Segundo Pinheiro (2007), a partir do momento que é entendido que com a chegada de novas tecnologias, há necessidade de aperfeiçoamento de ferramentas que transmitam segurança, está claro também a necessidade de se obter leis que possam garantir seu uso. Exemplos disso são as *International Organization for Standardization* (ISO), ISO's 17799, 18044 e 27001 que, segundo Pinheiro (2007), são baseadas e relacionadas com a segurança da informação. A norma ISO/IEC 17799:2005 corresponde a proteger todo e qualquer tipo de informação de natureza nociva para que não aconteça o rompimento de negócios, não oferecendo riscos ao mesmo. Para dar continuidade ao ciclo de negociações e, para a sua implementação é preciso ter ciência da segurança do projeto idealizado e ter o conhecimento que se deve acompanhar os processos, descobrir as vulnerabilidades desses e classificar informações de total valia para

desenvolvimento e criação do Comitê de Segurança (PINHEIRO, 2007). De acordo com Pinheiro (2007), a ISO/IEC 27001:2005 diz respeito à gestão de segurança da informação e a ISO/IEC 18044 trata sobre a gestão de incidentes de segurança da informação.

Golpe de troca de cartões magnéticos

O golpe de troca de cartões magnéticos, segundo Lordello (2002), tem o foco de ser aplicado em pessoas idosas devido às dificuldades apresentadas por elas ao operar os terminais eletrônicos das instituições bancárias. O acontecimento do golpe se dá pelo fato do fraudador aguardar dentro dos estabelecimentos bancários as vítimas, se passando por funcionário da instituição bancária à procura de alguma pessoa que necessite de ajuda para manusear o terminal eletrônico.

Após o criminoso realizar algum contato com a vítima, ele apresentará várias atitudes e ações para manusear o terminal eletrônico junto da vítima a fim de que, de maneira oportuna, venha obter a senha do cartão magnético. Quando o criminoso está de posse do cartão magnético da vítima e com sua senha memorizada, trocará esse cartão por outro qualquer sem que ela perceba. O criminoso ficará então com o cartão magnético da vítima e sua senha para realizar operações fraudulentas (LORDELLO, 2002).

Cartão magnético retido em caixa eletrônico

Segundo Lordello (2002) existem duas formas de retenção de cartão magnético em um terminal eletrônico que, são expostas nas seguintes situações:

a) O primeiro modo é quando o cartão magnético é travado no terminal eletrônico da instituição bancária. Neste caso, os criminosos implantam um mecanismo para travar o cartão magnético no leitor do cartão e, sendo assim, a pessoa tenta utilizar o telefone da própria cabine para entrar em contato com a central de atendimento da instituição, não conseguindo o contato porque o telefone está mudo. O indivíduo não conseguirá o contato com a central de atendimento porque os criminosos danificaram o aparelho telefônico também.
   O criminoso, falando ao celular, se aproxima da vítima que está com o cartão travado no terminal e diz estar com o mesmo problema e que conseguiu entrar em contato com a central de atendimento da instituição financeira. Então, o criminoso oferece à vítima seu aparelho celular. A vítima usa o aparelho celular cedido

pelo criminoso para falar com o suposto atendente da instituição financeira que, no caso, é outro criminoso e que pede para a vítima digitar no aparelho celular o número da senha do cartão magnético que está preso no terminal. Ao realizar este procedimento a vítima deixa o cartão retido no terminal com a promessa de que o cartão magnético está cancelado e que receberá novo cartão em sua residência e vai embora, com o parecer de que seu problema está solucionado. Em seguida, o cartão magnético da vítima é retirado pelo criminoso que, destrava o mecanismo implantado no leitor de cartão e, fica de posse do cartão magnético da vítima e sua respectiva senha.

b) O segundo modo é quando o cartão fica travado na máquina aparecendo uma mensagem no visor do terminal que o equipamento está violado. Os criminosos utilizam papéis plastificados com o logotipo da instituição bancária, com os dizeres para ligarem para um determinado número se houver algum tipo de problema no terminal. A vítima, ao ligar para o número do papel, é atendida por um criminoso que está do lado de fora da instituição bancária, observando todo o movimento dentro desta. Em seguida, pede os dados cadastrais e a senha do cartão magnético da vítima, prometendo solucionar o problema do cartão retido no terminal. Depois da obtenção de todos os dados da vítima o criminoso diz que o cartão está bloqueado e que a vítima receberá um novo cartão em sua residência. Com isso, o cliente sai do local deixando o cartão dentro do terminal e, o criminoso, sabendo qual foi o terminal utilizado pela vítima, destrava o leitor de cartão e extrai o cartão magnético da vítima. Tendo o criminoso os dados cadastrais da vítima, seu cartão magnético e a senha, pode fazer qualquer tipo de transferência ou transação para utilizar indevidamente a conta bancária da mesma (LORDELLO, 2002).

Instituições financeiras

Um dos crimes mais comuns nas instituições financeiras são invasões remotas de sistemas empresariais que arcam prejuízos reais ou denigrem a imagem da empresa publicamente (PINHEIRO, 2007).

Tenha-se presente que na linha de ataques aos sistemas de informação, as vítimas mais visadas são os operadores de redes de comunicação eletrônicas, os fornecedores de serviços e as empresas de comércio eletrônico. Outros setores da economia também podem ser apontados como alvo

fixo desses ataques, tais como bancos e instituições financeiras, indústrias, organismos do setor público, incluindo neste conjunto até os hospitais (BARROS, 2006, p. 280).

De acordo com Barros (2006), as instituições financeiras vêm agindo preventivamente para evitar e coibir fraudes cibernéticas e eletrônicas, bem como têm utilizado a aplicação de técnicas e modelos de análise para uma ação preditiva a fim de que a troca de informações dentro da *Internet* seja a mais segura possível, tomando assim todas as medidas de modo a identificar e penalizar os infratores, aumentando a segurança de seus clientes, usuários de cartões de crédito ou débito e clientes que fazem suas operações via *Internet Banking*.

Outra forma que as instituições financeiras têm usado para identificar fraudadores por meio de informações confiáveis é usando um banco de dados dos clientes com contas ativas e inativas na instituição, com uma fotografia ou imagem digital (biometria), facilitando identificar movimentações financeiras fraudulentas por meio de emissão de dados da fatura mensal detalhadas das instituições (PARODI, 2008).

As instituições financeiras têm realizado grandes investimentos relacionados à segurança corporativa, principalmente na área de tecnologia da informação. São itens que têm a necessidade de atualização periódica e que têm um custo elevado devido à quantidade de informações cedidas, requerendo competências específicas.

Todos os colaboradores são responsáveis por cumprir a Política de Segurança da Informação da empresa, e para tanto é necessário haver ciência formal do documento, seja com assinatura física seja eletrônica; além disso, a etapa da divulgação e conscientização dela é fundamental, tanto para prevenção de incidentes como para proteção da empresa no sentido de que capacitou seus profissionais no correto uso da tecnologia (PINHEIRO, 2007, p.135).

Nas instituições financeiras bancárias são as políticas de segurança corporativa que mantêm diretrizes para estabelecer os controles de segurança, sendo que essas políticas de segurança podem agregar valor financeiro para a instituição e ter relação direta com o processo de melhoria contínua de negociação. As diretrizes exigem estrita relação com procedimentos e conduta ética com indivíduos envolvidos nos processos e atividades.

A segurança corporativa bancária vem passando por significativa evolução no que diz respeito à sua forma de atuação com inovação de processos, produtos e serviços. Agora, tem-se a implementação de tecnologias inteligentes de segurança, com processo de biometria, analisando

e correlacionando dados, proporcionando maior capacidade e reação da instituição e otimizando as estratégias corporativas de prevenção a fraude.

Alguns desafios que as instituições financeiras têm são com relação à cultura das organizações, para ter estrutura de dados consolidados, disseminando cultura de prevenção e segurança contra os crimes de fraude eletrônica e outros tipos de crimes e implementando normas de melhores práticas, aperfeiçoando ferramentas já utilizadas para análise e conciliação com a evolução tecnológica, requerendo a pró-atividade de seus colaboradores, fazendo autoavaliação de risco e controle, conscientização e apregoando valores fundamentais que são importantes para a sustentação no processo e estrutura de segurança corporativa, minimizando atos irregulares.

ESTUDO DE CASO

A pesquisa e seus instrumentos utilizados servem de forma a dar prosseguimento aos objetivos expostos no presente trabalho, no qual foram coletados dados públicos e privados de instituições financeiras bancárias sobre fraude eletrônica no decorrer do ano de 2009 na cidade de São Paulo. Saliente-se que os dados mais recentes divulgados no Relatório Anual de 2013 da Febraban (2014, p. 54), apontam um investimento anual dos bancos de R$ 2 bilhões em tecnologia para segurança da informação, bem como o registro de 77.646 invasões, das quais 56.192 foram em contas de pessoas físicas e 21.454 em contas jurídicas, totalizando perdas no valor de R$ 270,3 milhões. No entanto, a Federação Brasileira de Bancos (Febraban) não divulga números detalhados como aqueles obtidos em 2009 pelos autores em nenhum dos seus relatórios, como se pode observar no Relatório Anual de 2009 (Febraban, 2010), motivo pelo qual a presente análise não há de perder sua importância, mormente o fato de que, em 30 de novembro de 2012, foi promulgada a "Lei Carolina Dieckmann" (Lei nº 12.737). Dessa forma, uma nova análise estatística dos crimes de fraudes bancárias pode utilizar os dados de 2009 como parâmetro de comparação, a fim de verificar se a tipificação do delito de invasão de dispositivo informático promoveu alterações substanciais nos índices ora utilizados.

A análise estatística visou verificar quais são as características mais significativas dos criminosos no ato da fraude e como eles estão agindo com relação a essas instituições. Tais informações trarão subsídios para delimitar algumas características que podem ser levadas em consideração no tratamento do planejamento estratégico e preditivo buscando uma redução da criminalidade sobre a responsabilidade das instituições bancárias.

A partir dos dados coletados foram consideradas as variáveis: haver ou não fraude, mês, dia da semana, dias do mês, região da cidade de São Paulo e horário no dia.

Foi realizada uma análise descritiva desses dados coletados e realizados testes de independência entre pares de variáveis que são descritas acima, bem como construídos intervalos de confiança de 95%. Foram calculados, para todos os testes, seus níveis descritivos e as conclusões foram obtidas utilizando-se um nível de significância de 5%. Nos testes realizados, quando ocorre a rejeição da hipótese de variável independente, ou seja, uma dependência das variáveis analisadas, encontra-se por meio da comparação entre os valores observados e esperados subsídios para conclusão de uma possível relação de dependência entre as variáveis analisadas (MONTGOMERY; RUNGER, 2009).

Depois de selecionadas as variáveis com maior relação de dependência com a variável resposta (haver ou não fraude), foram testados vários modelos de previsão baseados em regressão logística. Para isto utilizou-se 10% dos dados, sorteados aleatoriamente, uma vez que a amostra na sua totalidade tinha algumas milhares de unidades, prejudicando a utilização da técnica de previsão baseados em regressão logística. Foi escolhido o modelo que teve melhor aderência e maior capacidade de predição da variável resposta, a saber, região na cidade de São Paulo, mês e faixa horária, no período do ano de 2009.

Os dados foram analisados com o auxílio do programa Minitab®.

Testes de independência

O método de análise escolhido foi o teste de independência porque, segundo Montgomery e Runger (2009) quando se deseja saber se dois métodos de classificação são estatisticamente independentes deve-se comparar as frequências esperadas sob a hipótese de independência entre as duas variáveis aleatórias consideradas, E_{ij}, com as frequências observadas, O_{ij}, (número de efetiva ocorrência) para todos os níveis i da primeira variável, com $1 \leq i \leq r$, e todos os níveis j da segunda variável , com $1 \leq j \leq c$. Este procedimento requer uma amostra aleatória provindo de população com distribuição de probabilidades desconhecida, que no caso, são os dados analisados das instituições financeiras bancárias com relação à fraude eletrônica, na cidade de São Paulo, no período do ano de 2009. As duas variáveis no caso são a existência ou não de fraudes e uma das variáveis selecionadas, a saber: dia do mês, dia da semana, horário, mês ou região da cidade de São Paulo.

A seguir é apresentada a fórmula para o cálculo do teste de independência (MONTGOMERY; RUNGER, 2009):

$$c_o^2 = \sum_{i=1}^{r}\sum_{j=1}^{c}\frac{(O_j - E_j)^2}{E_j} = \sum_{i=1}^{r}\sum_{j=1}^{c}\frac{O_j^2}{E_j} - n \qquad (1)$$

No caso da análise realizada, os dados observados são todos os que são considerados fraudes e não fraudes em cada categoria. Os dados esperados são estimados através da tabela de teste de independência, obtidos com o auxílio do programa Minitab®, com conclusões obtidas utilizando-se de um nível de significância de 5%.

As duas variáveis serão consideradas dependentes se seus valores observados e esperados diferirem muito, isto é se o valor calculado em (1) exceder um valor tabelado da distribuição quiquadrado com (r – 1)(c – 1) graus de liberdade e nível de significância igual a 5%.

A seguir são apresentadas algumas tabelas utilizadas para o teste de independência das variáveis analisadas, baseado na distribuição quiquadrado. As Tabelas 1, 2, 3, 4 e 5 apresentam, respectivamente, as porcentagens de ocorrência e as porcentagens esperadas de fraude e não fraude para cada uma das variáveis: dia do mês, dia da semana, horário, mês e região da cidade de São Paulo.

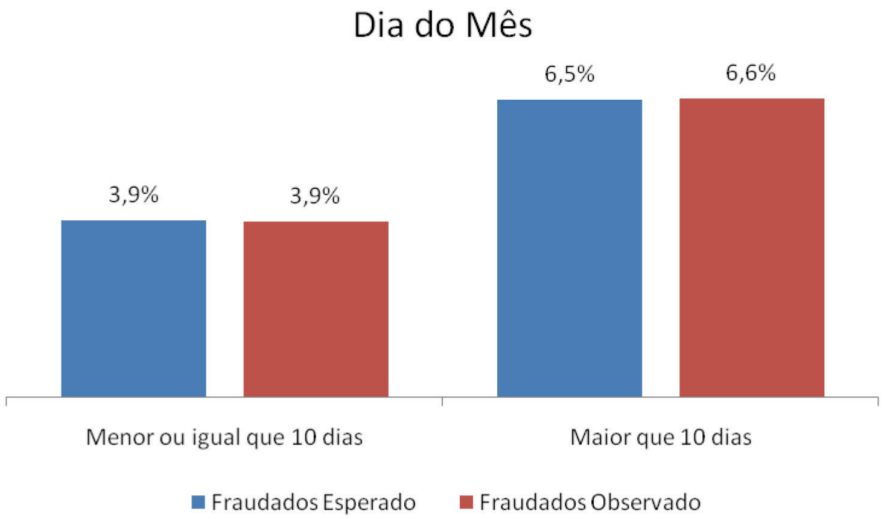
Tabela 1 – Porcentagens de ocorrência e esperada de fraude por dia do mês

Ocorrência de fraude	*Dia do Mês*	*Esperado*	*Observado*	*Total*
Não	<= 10 dias	33,4%	33,4%	89,6%
	> 10 dias	56,2%	56,1%	
Sim	<= 10 dias	3,9%	3,9%	10,4%
	> 10 dias	6,5%	6,6%	

FONTE: Elaboração própria, 2010.

O teste quiquadrado apresentou um nível descritivo P = 0,755 > 0,05, logo ao nível de significância de 5% não se rejeita a hipótese de independência entre existência de fraude e dia do mês. Tal resultado fica claro, ao se analisar o gráfico 1, uma vez que a variação entre as porcentagens observadas e esperadas, tanto dos dias menores ou iguais a dez e maiores do que dez são semelhantes. Não existe, portanto, relação de dependência entre o período do mês e a ocorrência de fraudes.

Gráfico 1 – Dia do mês e porcentagem



FONTE: Elaboração própria, 2010.

Tabela 2 – Porcentagens de ocorrência e esperada de fraude por dia da semana

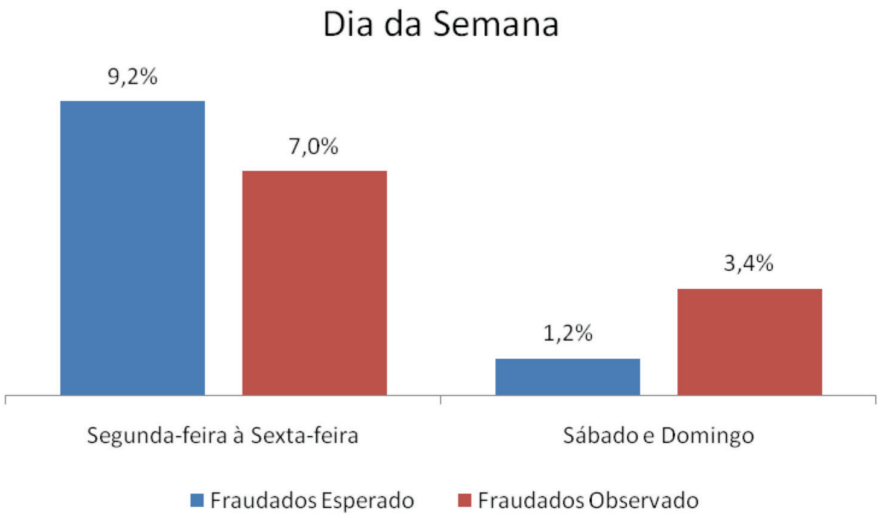
Ocorrência de fraude	*Dia da Semana*	*Esperado*	*Observado*	*Total*
Não	Segunda-feira a Sexta-feira	79,5%	81,7%	89,6%
	Sábado e Domingo	10,1%	7,9%	
Sim	Segunda-feira a Sexta-feira	9,2%	7,0%	10,4%
	Sábado e Domingo	1,2%	3,4%	

FONTE: Elaboração própria, 2010.

O teste quiquadrado apresentou um nível descritivo P = 0,000 < 0,05, logo ao nível de significância de 5% rejeita-se a hipótese de independência entre existência de fraude e dia da semana. Ao se analisar o gráfico 2, conclui-se que a maior discrepância ocorreu ao se comparar as porcentagens observadas e esperadas de sábado e domingo. Conclui-se, ao nível de significância de 5%, que há dependência entre as variáveis aleatórias na ocorrência de fraude e dia da semana, sendo que entre sábado e domingo, proporcionalmente, ocorreram mais fraudes.

O teste quiquadrado apresentou um nível descritivo P = 0,000 < 0,05, logo ao nível de significância de 5% rejeita-se a hipótese de independência entre existência de fraude e horário. Ao se analisar o gráfico 3, conclui-se que proporcionalmente há mais fraudes que o esperado entre 6 e 12 horas e menos fraudes entre 12 e 18 horas.

Gráfico 2 – Dia da semana e porcentagem



FONTE: Elaboração própria, 2010.

Tabela 3 – Porcentagens de ocorrência e esperada de fraude por horário

Ocorrência de fraude	*Horário*	*Esperado*	*Observado*	*Total*
Não	6 horas até 12 horas	30,5%	27,5%	89,6%
	12 horas até 18 horas	44,1%	46,4%	
	18 horas até 6 horas	15,0%	15,7%	
Sim	6 horas até 12 horas	3,5%	6,6%	10,4%
	12 horas até 18 horas	5,1%	2,8%	
	18 horas até 6 horas	1,7%	1,1%	

FONTE: Elaboração própria, 2010.

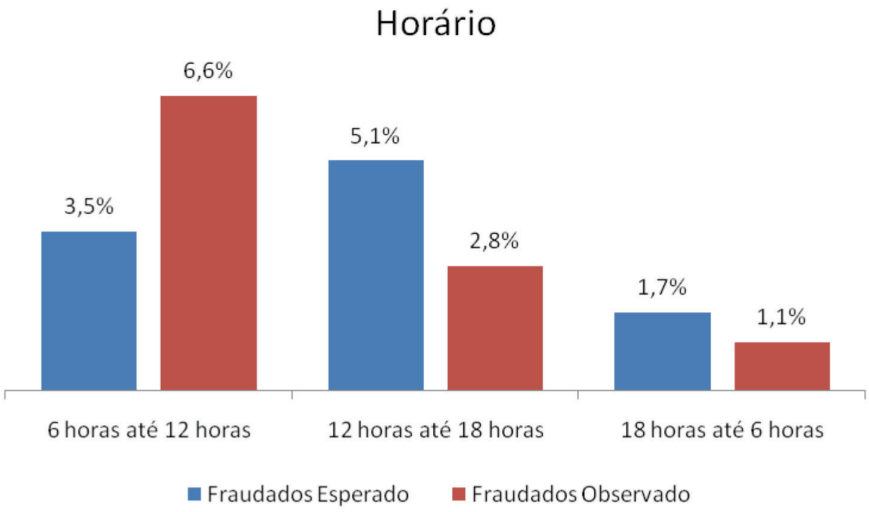
A análise mais detalhada, com o horário das 6 às 12 horas subdivididas de duas em duas horas, mostrou que proporcionalmente as fraudes ocorrem em maior proporção principalmente entre 8h e 10h da manhã.

O teste quiquadrado apresentou um nível descritivo P = 0,000 < 0,05, logo ao nível de significância de 5% rejeita-se a hipótese de independência entre existência de fraude e trimestre. Ao se analisar o gráfico 4, conclui-se que proporcionalmente há mais fraudes que o esperado no segundo trimestre e menos fraudes no quarto trimestre.

Uma análise mais detalhada realizada mês a mês também rejeitou a hipótese de independência entre existência de fraude e mês (P = 0,000), concluindo-se ao nível de significância de 5% que de março a junho,

proporcionalmente, ocorreram mais fraudes, principalmente nos meses de março e junho e que em dezembro, proporcionalmente, ocorreram menos fraudes.

Gráfico 3 – Horário e porcentagem



FONTE: Elaboração própria, 2010.

Tabela 4 – Porcentagens de ocorrência e esperada de fraude por trimestre

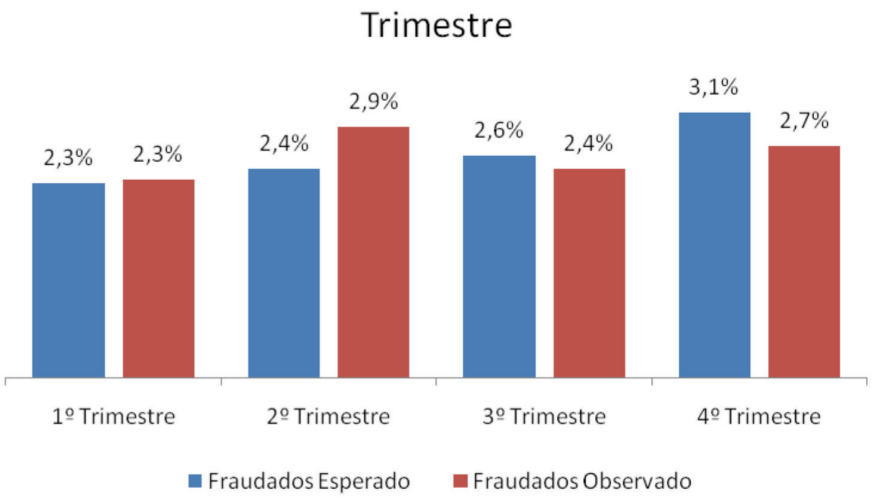
Ocorrência de fraude	*Trimestre*	*Esperado*	*Observado*	*Total*
Não	1º Trimestre	19,5%	19,5%	89,6%
	2º Trimestre	21,0%	20,5%	
	3º Trimestre	22,4%	22,5%	
	4º Trimestre	26,7%	27,1%	
Sim	1º Trimestre	2,3%	2,3%	10,4%
	2º Trimestre	2,4%	2,9%	
	3º Trimestre	2,6%	2,4%	
	4º Trimestre	3,1%	2,7%	

FONTE: Elaboração própria, 2010.

O teste quiquadrado apresentou um nível descritivo P = 0,000 < 0,05, logo ao nível de significância de 5% rejeita-se a hipótese de independência entre existência de fraude e região da cidade de São Paulo. Observando o gráfico 5, nota-se que no que se diz respeito à região da cidade de São Paulo, pode-se analisar que a região que engloba a zona leste, centro da cidade e ABCD (Região de Santo André, São Bernardo do Campo, São

Caetano do Sul e Diadema) e a região que engloba a zona norte e região metropolitana tem, em porcentagem de ocorrência de fraude, um valor observado maior do que o esperado. Já se observando a região que engloba a zona sul e zona oeste, pode-se verificar que em relação à porcentagem de ocorrência de fraude observada, esta é menor do que a ocorrência de fraude esperada nessa região.

Gráfico 4 – Trimestre e porcentagem



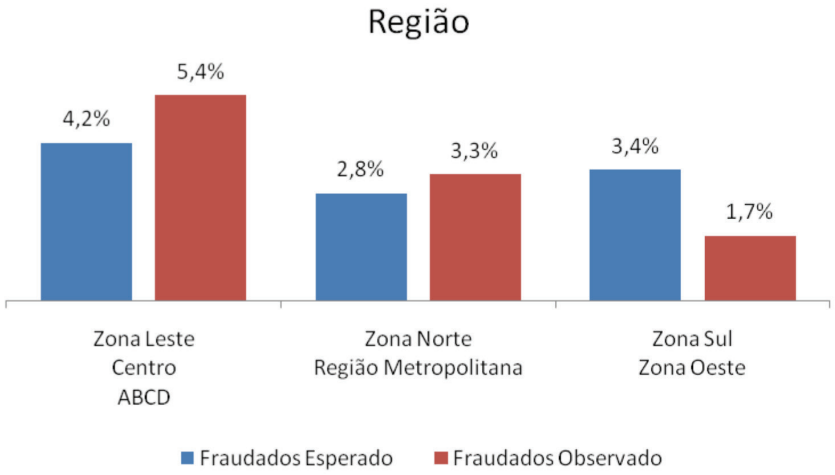
FONTE: Elaboração própria, 2010

Tabela 5 – Porcentagens de ocorrência e esperada de fraude por região da cidade de São Paulo

Ocorrência de fraude	*Região da cidade de São Paulo*	*Esperado*	*Observado*	*Total*
Não	Zona Leste / Centro / ABCD	35,8%	34,5%	89,6%
	Zona Norte / Região Metropolitana	24,3%	23,8%	
	Zona Sul / Zona Oeste	29,6%	31,3%	
Sim	Zona Leste / Centro / ABCD	4,2%	5,4%	10,4%
	Zona Norte / Região Metropolitana	2,8%	3,3%	
	Zona Sul / Zona Oeste	3,4%	1,7%	

FONTE: Elaboração própria, 2010.

Gráfico 5 – Região da cidade de São Paulo e porcentagem



FONTE: Elaboração própria, 2010.

Em uma análise mais detalhada, a zona leste foi a região em que proporcionalmente ocorreram mais fraudes e a zona sul foi a região em que proporcionalmente ocorreram menos fraudes.

Modelo de previsão

De acordo com Montgomery e Runger (2009), a análise de regressão é uma técnica utilizada para modelar determinado acontecimento (no caso a existência ou não de fraudes) em função de variáveis independentes (no caso mês, dia da semana, dias do mês, região da cidade de São Paulo e horário no dia).

O tipo de regressão utilizada neste trabalho é a regressão logística, na qual a variável resposta (dependente) pode assumir somente dois possíveis resultados (no caso ter ou não havido fraude). Segundo McCullagh e Nelder (1989), a variável de resposta (dependente) é binária, ou seja, aquela que aceita apenas dois tipos de respostas como, por exemplo, sim ou não. Na previsão, por meio da regressão logística, a decisão pela classificação em uma das duas categorias dependerá de uma série de atributos relacionados às variáveis independentes. Geralmente atribui-se o código 1 (um) ao resultado mais importante da resposta, neste caso quando ocorre a fraude, que representaria a presença de uma particular característica de interesse, e zero ao evento complementar que será a não fraude, denominado fracasso.

Com relação à regressão logística, é utilizado o método de máxima verossimilhança para estimar os parâmetros de um determinado modelo e restringir a relativa linearidade e a não linearidade dos testes de hipótese (CRAMER, 1986). Neste método é comum a estimação de alguns parâmetros, sendo já conhecidas as distribuições probabilísticas.

Partindo-se de uma amostra aleatória de um conjunto de dados com distribuição conhecida será obtida a máxima verossimilhança de β (valores dos parâmetros) dado a distribuição conhecida (CORDEIRO, 1992). Para que aconteça a estimação dos valores dos dados no método de máxima verossimilhança estes devem ser obtidos por métodos iterativos.

Portanto, o modelo de regressão logística ajusta-se a função g(x) e não a uma variável resposta. O processo para obtenção das estimativas de máxima verossimilhança dos parâmetros β's é feito através de procedimentos numéricos. Porém, um programa estatístico como o Minitab® permite o cálculo destas estimativas de maneira mais simples, auxiliando na obtenção do resultado desses parâmetros e facilitando o processo no que se diz respeito a tempo e precisão de dados.

Depois de realizada a regressão logística, determinado os valores das variáveis explicativas e estabelecido o modelo, deve-se testar a significância dos parâmetros bem como o ajuste do mesmo. O objetivo é determinar o modelo mais simples possível que tenha um bom ajuste, tornando possível a estimação da probabilidade de sucesso da variável resposta (FARHAT, 2003).

Aplicando o modelo de regressão logística adotado, utilizando os valores observados para uma nova observação é possível estimar a probabilidade de sucesso em uma nova análise. A resposta será de sucesso ou fracasso, dependendo do valor estimado da probabilidade. Em geral se essa probabilidade estimada for superior a 0,50 a observação será classificada como sucesso.

Se os erros de má classificação (classificar como sucesso um fracasso ou vice-versa) tiverem importâncias diferentes, outro valor limite para a probabilidade estimada de sucesso, diferente de 0,5, poderá ser usado (FARHAT, 2003).

Para a escolha do modelo de regressão logística a ser utilizado, optou-se por utilizar as 80% primeiras observações da amostra (2698 casos), guardando os 20% restantes (674 casos) para a validação do modelo. Valores longe de 1 (um) para a razão de chances indicam maior associação entre a ocorrência do fator e a ocorrência da variável resposta.

A probabilidade de ocorrer a fraude é dada por:

$$P(ocorrer\ \ fraude) = \frac{e^{Y}}{1+e^{Y}} \qquad (2)$$

Com Y função das variáveis independentes. Se esta probabilidade for superior a 0,50, terá uma provável ocorrência de fraude.

Baseado nos testes de independência de variáveis aleatórias e testando-se vários possíveis modelos, decidiu-se pelo modelo que incluiu as variáveis: região, mês e horário.

O modelo encontrado foi:

$$Y = 1{,}036 - 1{,}282\, X_{região1} - 0{,}038\, X_{região2} - 0{,}038\, X_{mês} - 0{,}896\, X_{horário1} - 1{,}054 X_{horário2}$$

Tem-se que:

$X_{região1}$ vale um caso seja da região da zona sul e zona oeste, caso contrário $X_{região1}$ vale zero.

$X_{região2}$ vale um caso seja da região metropolitana e zona norte, caso contrário

$X_{região2}$ vale zero.

$X_{mês}$ vale um caso seja janeiro, dois, caso seja fevereiro e assim sucessivamente.

$X_{horário1}$ vale um caso seja a faixa horária de 18 horas às 6 horas, caso contrário $X_{horário1}$ vale zero.

$X_{horário2}$ vale um caso seja a faixa horária de 12 horas às 18 horas, caso contrário $X_{horário2}$ vale zero.

Tabela 6 – Coeficientes, erro padrão, valor Z, nível descritivo P, razão de chances e intervalo com 95% de confiança

Preditor	*Coeficiente*	*Erro padrão do coeficiente*	*Z*	*P*	*Razão de chances*	*Intervalo com 95% de confiança*	
						Limite inferior	*Limite superior*
Constante	-1,03683	0,165501	-6,26	0,000			
Região 1	-1,34618	0,202860	-6,64	0,000	0,26	0,17	0,39
Região 2	-0,11829	0,147299	-0,80	0,422	0,89	0,67	1,19
Mês	-0,02310	0,019151	-1,21	0,228	0,98	0,94	1,01
Horário 1	-1,18539	0,228660	-5,18	0,000	0,31	0,2	0,48
Horário 2	-1,35439	0,149209	-9,08	0,000	0,26	0,19	0,35

FONTE: Elaboração própria, 2010.

O programa fornece uma estatística G = 165,833, na qual testa a hipótese de que todos os coeficientes são iguais a zero contra a hipótese de que pelo menos um dos coeficientes é diferente de zero. O nível descritivo P foi igual a 0,000, logo há evidências de que pelo menos um dos coeficientes é diferente de zero.

Foram realizados testes de ajuste do modelo por três métodos diferentes, a saber, o método de Pearson (P = 0,769), o método de *Deviance* (P = 0,522) e o método de *Hosmer- Lemeshow* (P = 0,775). Para os três métodos o modelo foi considerado bem ajustado uma vez que sua aderência não foi rejeitada, pois P foi sempre maior que 0,05.

Foram calculadas várias medidas de associação entre a variável resposta e as probabilidades de previsão.

Foram calculadas as estatísticas de *Somers*' D igual a 0,45, de Goodman-Kruskal Gamma igual a 0,46 e de Kendall's Tau-a igual a 0,08. Estas estatísticas resumem as tabelas de concordância e discordância dos pares de observações. Estas medidas devem estar entre 0 e 1 e valores altos indicam que o modelo tem uma boa capacidade de previsão.

Foi testado o modelo em algumas centenas de unidades e dados da amostra que não entraram na escolha do mesmo. Foi calculada a probabilidade de ocorrer fraude ou não. Como era conhecida a verdadeira situação quanto à ocorrência de fraude, pode-se calcular a porcentagem de acerto que foi igual a 61%, mostrando que o modelo está adequado.

É claro que esse modelo não explica totalmente a variável "ocorrência de fraude", porém sua eficiência foi significativa.

CONCLUSÃO

Os crimes e fraudes eletrônicas cometidos contra as instituições financeiras bancárias impactam diretamente na sua produtividade e nos seus índices de lucratividade. Os conceitos de crimes e fraudes eletrônicas foram explorados através de pesquisa bibliográfica, que forneceram embasamento técnico para um melhor conhecimento do funcionamento das fraudes eletrônicas e quais são seus malefícios para as respectivas pessoas lesadas por esse tipo de crime.

De acordo com esta pesquisa, pode-se concluir que a legislação é muito abrangente e imprecisa e, num breve futuro, é necessário apresentar planos de melhoria de redação e interpretação do texto. Através desse processo, é necessário que tenham tomadas de decisões consistentes e incisivas de maneira a prevenir as instituições financeiras bancárias contra esses tipos de crimes.

Foram coletados dados importantes e relevantes para a conclusão deste trabalho de pesquisa. Dados estes que são do ano de 2009, da cidade de São Paulo e sobre fraudes eletrônicas de instituições financeiras públicas e privadas. O principal objetivo foi realizar a análise estatística e verificar a relação temporal e espacial baseado nas características mais significativas dos criminosos para efetuação dos crimes eletrônicos. Para alcançar os objetivos propostos foram utilizados meios estatísticos que são testes de independência e modelo de previsão.

Fundamentado na metodologia deste trabalho pode-se concluir que o objetivo de analisar a relação espacial e temporal foi atingido utilizando-se os testes de independência através das variáveis, dia da semana, horário, trimestre e região, que de certa forma influenciam nas fraudes eletrônicas. Com relação ao modelo de previsão desenvolvido no trabalho pode-se concluir que as variáveis que influenciam na fraude eletrônica são região, mês e faixa horária. O modelo de previsão mostrou ser adequado para se prever ocorrências, conhecendo-se a região, o mês e a faixa horária, podendo estimar com maior probabilidade de acerto se ocorrerão crimes de fraude eletrônica ou não. Assim, a segunda parte da hipótese do trabalho conclui-se que existe relação entre algumas variáveis com os crimes de fraude eletrônica.

A promulgação da Lei nº 12.737, de 30 de novembro de 2012, popularmente chamada de "Lei Carolina Dieckmann", enseja nova análise estatística dos crimes de fraudes bancárias, a fim de verificar se a tipificação do delito de invasão de dispositivo informático promoveu alterações substanciais nos índices ora analisados, a qual fica sugerida como tema para trabalhos futuros.

REFERÊNCIAS

BARROS, M. A. (2006). **O Direito na Sociedade da Informação.** São Paulo: Atlas.

BEATO FILHO, C. C. (1998). Determinantes da criminalidade em Minas Gerais. **Revista Brasileira de Ciências Sociais.** v. 13, n. 37, jun. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0102=69091998000200004-&lang-pt>. Acesso em: 29 de setembro de 2009.

_____ (1999). **Políticas públicas de segurança e a questão policial**. São Paulo. São Paulo em Perspectiva. v. 13, n. 4, p. 13-27, out/dez. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0102-88391999000400003&lang=pt>. Acesso em: 29 de setembro de 2009.

BEATO FILHO, C. C.; SILVA, B. F. A.; TAVARES, R. (2008). Crimes e estratégias em espaços urbanos. **Revista de ciências sociais.** Rio de Janeiro, v. 51,

n. 3. Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0011-52582008000300005&lang=pt>. Acesso em: 18 de outubro de 2009.

BRANCO, C. M. F. (2003/2004). **Criminalidade Informática. Gestão de Empresas**. São Paulo. Disponível em: <http://student.dei.uc.pt/~cfilipe/portfolio_GE_files/GE%20-%20Trabalho2a.pdf>. Acesso em: 19 de outubro de 2009.

BRASIL. **Decreto-lei nº 2.848, de 07 de dezembro de 1940. Código Penal.** Diário Oficial da República Federativa do Brasil, Brasília, DF, 31 de dezembro de 1940. Disponível em: <https://www.planalto.gov.br/ccivil_03/Decreto-Lei/del2848.htm>. Acesso em: 05 de maio de 2010.

CERT.BR – CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL, *CERT.br.* São Paulo (2006). Disponível em: **<**http://cartilha.cert.br/fraudes/sec2.html#sec2>. Acesso em: 02 de fevereiro de 2010.

CENTRO DE TECNOLOGIA E SOCIEDADE DA ESCOLA DE DIREITO DO RIO DE JANEIRO DA FUNDAÇÃO GETÚLIO VARGAS, CTS-FGV. Rio de Janeiro. (2008). Disponível em: htttp://www.culturalivre.org.br/artigos/Proposta_e_Estudo_CTS-FGV_Cibercrimes.pdf>. Acesso em: 19 de maio de 2010.

CRAMER, J. S. (1986). **Econometric applications of Maximum Likelihood Methods**, Cambridge: Cambridge University Press.

CORDEIRO, G. (1992). Introdução à teoria de verossimilhança. Livro texto In: **10° SIMPÓSIO NACIONAL DE PROBABILIDADE E ESTATISTICA,** Rio de janeiro.

FARHAT, C. A. V. (2003). Análise de diagnóstico em regressão logística. 2003. **Dissertação** (**Mestrado em Estatística**) -Instituto de Matemática e Estatística da Universidade de São Paulo, São Paulo.

FEDERAL BUREAU OF INVESTIGATION – FBI (2013). **New E-scams & Warnings**. Disponível em: <http://www.fbi.gov/scams-safety/e-scams>. Acesso em: 22 de março de 2015.

_____ (2015). **Common Fraud Schemes**. Disponível em: <http://www.fbi.gov/scams-safety/fraud/fraud>. Acesso em: 22 de março de 2015.

FEBRABAN – FEDERAÇÃO BRASILEIRA DE BANCOS. (2010). **Relatório Anual 2009**. Disponível em: <http://www.febraban.org.br/7Rof7SWg6qmyvwJcFwF7I0aSDf9jyV/sitefebraban/Febraban_completo.pdf>. Acesso em: 22 de março de 2015.

_____ (2014). **Relatório Anual 2013**. Disponível em: <http://www.febraban.org.br/7Rof7SWg6qmyvwJcFwF7I0aSDf9jyV/sitefebraban/Relat%F3rio%20Anual%20FEBRABAN_2013.pdf >. Acesso em: 22 de março de 2015.

INÁCIO, Sandra Regina da Luz (2009). **As fraudes em cartões de crédito**. Atigologia. São Paulo, jan. Disponível em: <http://www.artigonal.com/tecnologia-artigos/as-fraudes-em-cartoes-de-credito-718455.html>. Acesso em: 10 de outubro de 2009.

LORDELLO, Jorge (2002). **Como Viver com Segurança: Dicas Práticas para sua Proteção**. 1ª ed. São Paulo: Tipo.

McCULLAGH, P.; NELDER, J. A. (1989). **Generalized Linear Models.** 2ª ed. Londres: Chapman and Hall.

MINITAB. **Minitab 17**. Disponível em: <http://www.minitab.com/pt-br/products/minitab/features/>. Acesso em: 22 de março de 2015.

MONTGOMERY, D. C.; RUNGER G. C. (2009). **Estatística Aplicada e Probabilidade para Engenheiros.** 4ª ed. Rio de Janeiro: LTC.

NASCIMENTO, Weslley S.; PEREIRA, Anísio C. (2005). Um estudo sobre a atuação da auditoria interna na detecção de fraudes nas empresas do setor privado no Estado de São Paulo. **Revista Brasileira de Gestão de Negócios. São Paulo,** SP, v. 7, n. 19, p. 46 – 56. Disponível em: <http://200.169.97.104/seer/index.php/RBGN/article/view/49/42>. Acesso em: 17 de setembro de 2009.

PARODI, Lorenzo (2008). **Manual das Fraudes.** 2ª ed. São Paulo, Brasport.

PINHEIRO, Patricia Peck (2007). **Direito Digital.** 2ª ed. São Paulo, Saraiva.

SECRETARIA DA RECEITA FEDERAL DO BRASIL. **Receita alerta para e-mail falso sobre regularização do CPF.** (2005). Disponível em: <http://www.receita.fazenda.gov.br/AutomaticoSRFsinot/2005/fevereiro/23022005a.htm>. Acesso em: 22 de março de 2015.

SIEGEL; S.; CASTELLAN JR, N. J. (2008). **Estatística não paramétrica para ciências do comportamento.** Métodos de Pesquisa. 2ª ed. Porto Alegra: Bookman.