Josiane Klettenberg

SEGURANÇA DA INFORMAÇÃO:
Um estudo sobre o uso da engenharia social para obter informações sigilosas de usuários de Instituições Bancárias

Dissertação de mestrado apresentada à Banca Examinadora do Programa de Pós-Graduação em Ciência da Informação do Centro de Ciências da Educação da Universidade Federal de Santa Catarina, como requisito parcial para obtenção do título de Mestre em Ciência da Informação, na área de concentração Gestão da Informação, linha de pesquisa Informação, Gestão e Tecnologia.

Orientação: Professor Doutor Angel Freddy Godoy Viera.

Florianópolis
2016

Ficha de identificação da obra elaborada pelo autor, através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Klettenberg, Josiane

K63s SEGURANÇA DA INFORMAÇÃO: Um estudo sobre o uso da engenharia social para obter informações sigilosas de usuários de Instituições Bancárias / Josiane Klettenberg; orientador, Angel Freddy Godoy Viera - Florianópolis, SC, 2016. 181 p.

Dissertação (mestrado) - Universidade Federal de Santa Catarina, Centro de Ciências da Educação. Programa de Pós-Graduação em Ciência da Informação.

Inclui referências

1. Ciência da Informação. 2. Segurança da Informação. 3. Informação. 4. Engenharia social. 5. Usuários. I. Godoy Viera, Angel Freddy. II. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Ciência da Informação.
III. Título.

FOLHA DE APROVAÇÃO – COLOCAR A VERSÃO ASSINADA PÓS IMPRESSÃO

Dedico aos meus pais, Waldir Klettenberg e Teresinha Ventura Klettenberg, a minha irmã, Gislene Klettenberg, ao meu noivo, Mauro César Blum e ao meu cunhado, Andrey Starke Sardo, pelo apoio incondicional.

AGRADECIMENTO

Agradeço à Deus por iluminar a minha trajetória de vida;

À Universidade Federal de Santa Catarina (UFSC) e ao Programa de Pós-Gradução em Ciência da Informação (PGCIN), pela transparência no processo seletivo, orientação pedagógica, oportunidade e incentivo;

Ao orientador, professor Dr. Angel Freddy Godoy Viera, pela orientação no desenvolvimento da pesquisa;

Aos professores da banca que se dispuseram em avaliar e tecer suas contribuições de grande valia para o resultado final da pesquisa;

Ao corpo docente do PGCIN, representados pelos professores, Dra. Edna Lúcia da Silva, Dr. Vinícius Medina Kern, Dra. Rosângela Schwarz Rodrigues, Dr. Adilson Luiz Pinto e Dra. Clarice Fortkamp Caldin, por terem compartilhado seus conhecimentos de forma generosa e apresentado uma visão de mundo que até então era desconhecida por mim;

À secretaria do PGCIN, representada por Sabrina de Conto, que fez parte de todo o processo, desde a minha inscrição no programa até a conclusão da pesquisa.

À Instituição Bancária por ter depositado confiança e autorizado a realização da pesquisa;

À minha equipe de trabalho, principalmente aos meus colegas, Eduardo Antônio Pereira e Renato Borba de Miranda, que incentivaram a realização da pesquisa e não se opuseram quando da necessidade de eventuais ausências, sendo compreensivos;

Aos meus amigos e amigas, Thais Carrier Mendonça, Sirlei Uhlig, Jessyca Fronza, Miriam Mattos, Evandro Jair Duarte, Aline Oliveira, Alexandre Lucas, Charles Rodrigues, pelo encorajamento e trocas de experiências;

A turma 2013/1 do Programa de Pós-Graduação em Ciência da Informação pelo acolhimento, paciência e orientações;

Aos meus pais Waldir Klettenberg e Teresinha Ventura Klettenberg, pelo incentivo para a conclusão de cada fase do processo de desenvolvimento da pesquisa, por nunca terem duvidado da minha capacidade, pelo amor, exemplo de vida e por serem o meu alicerce;

À minha irmã, Gislene Klettenberg e ao meu cunhado, Andrey Starke Sardo, pela força, paciência e colaboração na vida pessoal e profissional;

Ao meu noivo, Mauro César Blum, pelo amor, estímulo e companheirismo, se fazendo presente durante todo o processo.

À minha avó, Maria Ventura, e a minha tia que veio a falecer durante o processo de pesquisa, Maria de Lourdes Ventura, pela compreensão nas minhas ausências em períodos de desenvolvimento da pesquisa;

A todos aqueles que de alguma forma, direta ou indiretamente, emanaram energia positiva para conclusão dessa etapa de vida.

Muito obrigada!

“A melhor maneira de ficar em segurança é nunca se sentir seguro."
Benjamin Franklin

RESUMO

A segurança da informação e a engenharia social fazem parte do processo da ciência que estuda o comportamento, as características do indivíduo e a sua relação com a informação e a geração do conhecimento. Esta pesquisa tem como objetivo geral analisar a segurança da informação de usuários de Instituições Bancárias a partir da perspectiva da engenharia social. O estudo de caso foi composto por uma amostra com 132 correntistas de uma instituição bancária, vítimas de fraudes eletrônicas. Como resultado, foi constatado que a fraude eletrônica está concentrada no canal internet banking. A invasão de sistemas e a disseminação de programas espúrios são as atividades de maior relevância dos engenheiros sociais. Estes se beneficiam de informações sigilosas e a sua presença no ciberespaço impulsiona o desenvolvimento de instrumentos tecnológicos que venham a neutralizar a sua ameaça, fazendo parte também do dinamismo da rede. O conhecimento pelos usuários da Internet dos subterfúgios utilizados pelos engenheiros sociais, nas suas práticas criminosas, é essencial para auxiliá-los na proteção contra as ameaças presentes na rede. Assim, a segurança da informação é um processo dinâmico e complexo, cuja efetividade está alicerçada na sistematização da comunicação, das pessoas e da informação comunicada.

Palavras-chave: Informação Sigilosa. Segurança da Informação. Engenharia Social. Usuários - Instituições Bancárias. Fraude Bancária.

ABSTRACT

The information security and social engineering are part of the process of science that studies the behavior of the individual characteristics and their relationship with information and knowledge generation. This research has as main objective to analyze the safety of Banking Institutions user information from the perspective of social engineering. The case study consisted of a sample of 132 account holders of a bank, victims of electronic fraud. As a result, it was found that electronic fraud is concentrated in the internet banking channel. The invasion of systems and the spread of spurious programs are the most relevant social engineers activities. These benefit from confidential information and its presence in cyberspace drives the development of technological tools that will neutralize their threat, also part of the network's dynamism. Knowledge by Internet users of the subterfuges used by social engineers in their criminal practices, it is essential to help them protect against the threats on the network. Thus, information security is a dynamic and complex process whose effectiveness is based on the systematization of communication, people and the report.

KEYWORDS: Sensitive Information. Information Security. Social Engineering. Users - Banking Institutions. Banking Fraud.

.

LISTA DE ILUSTRAÇÕES

LISTA DE TABELAS

LISTA DE QUADROS

LISTA DE GRÁFICOS

LISTA DE ABREVIATURAS E SIGLAS

ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS.

BACEN - BANCO CENTRAL DO BRASIL.

BB - BANCO DO BRASIL

BRAPCI - BASE DE DADOS REFERENCIAL DE ARTIGOS DE PERIÓDICOS EM CIÊNCIA DA INFORMAÇÃO.

CAPES - COORDENAÇÃO DE APERFEIÇOAMENTO DE PESSOAL DE NÍVEL SUPERIOR.

CEF - CAIXA ECONÔMICA FEDERAL

CERT.BR - CENTRO DE ESTUDOS, RESPOSTAS E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL

FEBRABAN - FEDERAÇÃO BRASILEIRA DE BANCOS

FECAM - ASSOCIAÇÃO DOS MUNICÍPIOS DA GRANDE FLORIANÓPOLIS

IBGE - INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA.

ISO - INTERNATIONAL STANDARDIZATION ORGANIZATION.

SAC - SERVIÇO DE ATENDIMENTO AO CLIENTE

SFN - SISTEMA FINANCEIRO NACIONAL

SMS - SHORT MESSAGE SERVICE

SSL - SECURE SOCKET LAYER

UFSC - UNIVERSIDADE FEDERAL DE SANTA CATARINA.

SUMÁRIO

1 INTRODUÇÃO

A Internet é uma ferramenta de comunicação que revolucionou a forma dos indivíduos interagirem e se socializarem. Esse formato de interação e socialização é conhecido como sociedade em rede ou sociedade da informação (CASTELLS, 2003; MATTELART, 2002).

O aumento dos estoques de informações e a liberdade são características do ambiente digital suficientes para comprometer a segurança das informações dos usuários. A proteção aos estoques informacionais é uma necessidade presente na sociedade da informação e o principal desafio da segurança da informação.

A segurança da informação está alicerçada em três pilares básicos, a confidencialidade, a integridade e a disponibilidade. O comprometimento de qualquer um desses pilares representa um risco à segurança informacional. A invasão de *sites* do governo, *sites* de empresas, a captura de códigos dos cartões de créditos e senhas, informações particulares expostas em redes sociais e exploradas para prática de extorsão, o uso ilegal de hardware, software ou dados, são alguns exemplos do comprometimento da segurança da informação.

Entende-se por engenharia social a ciência que estuda o conhecimento do comportamento humano e das suas características, com intuito de induzir um indivíduo a atuar conforme o desejo de quem a pratica. O autor da engenharia social explora a confiança do usuário para organizar e comprometer a segurança da informação (PEIXOTO, 2006). Quando aplicada contra usuários de Instituições Bancárias, nesse caso, o infrator utiliza de canais como a internet e cartões de crédito e débito para obter sucesso. A visão sistêmica da rede por seus usuários, com intuito de identificar as possíveis ameaças e os riscos que norteiam uma informação, circundam a efetividade da segurança da informação. A tecnologia, associada aos usuários comprometidos em salvaguardar suas informações contra os mal-intencionados, é imprescindível para a sociedade em rede protegida.

Nesse contexto, a comunicação científica pode cooperar para o desenvolvimento da visão sistêmica dos usuários, publicando trabalhos científicos relacionados ao tema. Paradoxalmente, a produção científica sobre o tema segurança da informação, tendo como escopo o usuário, é pouco explorada na área da Ciência da Informação. A partir do

mapeamento do fluxo e a identificação dos riscos relacionados à exposição das informações sigilosas, será possível conhecer os subterfúgios utilizados pelos engenheiros sociais para comprometer a segurança da informação.

O intuito da presente pesquisa é contribuir para as áreas do Direito, Sociologia, Administração, Tecnologia e em especial, a Ciência da Informação, no que se refere à exploração dos temas segurança da informação, engenharia social e análise das características dos usuários de Instituições Bancárias, quando vítimas de fraudes eletrônicas, considerando a escassa produção científica pela área, inclusive cooperando com perspectivas para novas pesquisas científicas. Visa-se também, produzir informações e que as mesmas sejam convertidas em conhecimento, no que se refere aos usuários de Instituições Bancárias, quando promoverem a junção da teoria com as suas experiências de vida, em ambientes situacionais. Além de tais prerrogativas, se pretende contribuir para avaliação da Instituição Bancária em relação à percepção de seus usuários no que tange à segurança da informação, bem como estabelecer programas de melhorias e aperfeiçoamento no processo de implementação de uma cultura de segurança.

1.1 DELIMITAÇÃO DA PESQUISA

A globalização socioeconômica e o uso massificado da internet fazem com que a sociedade contemporânea esteja em constante transformação. Esta transformação, aliada a problemas sociais como a má distribuição de renda, os crimes cibernéticos e as fraudes, de uma forma geral, denotam um sentimento de insegurança.

A ausência de regulamentação da publicação de informações na internet (CASTELLS, 2005) propicia ao indivíduo trocas informacionais livres de barreiras temporais, espaciais e de censura. Neste contexto, as informações podem fluir de forma desordenada, o que implica em um ambiente propício para corromper a privacidade, comprometer a segurança das informações dos usuários, explorando a sua confiança para obtenção de vantagens.

Este processo de exploração da confiança dos usuários visando a obtenção de vantagem é conhecido como engenharia social e corresponde a uma técnica empregada para ludibriar pessoas, subtraindo

informações valoradas de indivíduos ou organizações, comprometendo a segurança da informação (PEIXOTO, 2006).

A engenharia social é um dos instrumentos utilizados para comprometer a segurança das informações dos usuários de Instituições Bancárias, cujo autor se utiliza da boa-fé e das informações da vítima para organizar e efetivar as fraudes.

A característica preponderante da engenharia social é a criação de uma falsa sensação de segurança. Esta falsa sensação induz as vítimas a divulgarem informações de foro íntimo, indisponíveis e valoradas, sem que percebam a exposição, comprometendo a confidencialidade, integridade e disponibilidade.

A definição de fraude eletrônica está associada a um golpe, abuso, beneficiamento financeiro. Para Lau (2006), fraude eletrônica está relacionada ao emprego de qualquer tipo de golpe, por intermédio de serviços disponíveis na internet, mediante a persuasão de potenciais vítimas, com intuito de realizar transações fraudulentas em benefício de um indivíduo ou grupo de pessoas. Uma visão análoga é de Kovach (2011), que a define como qualquer acesso ou transação não autorizados, realizados em conta corrente, cujo canal é a internet.

A partir de tais definições, serão consideradas como fraude eletrônica, para efeitos da nossa pesquisa, toda ação ou omissão que permita a realização de um golpe, por meio de ataques diretos ou por canais alternativos, como a internet - *Internet Banking*, caixas eletrônicos e centrais de atendimento das Instituições Bancárias, com emprego da engenharia social.

A presente pesquisa apresenta em seu escopo, a delimitação das características comuns dos usuários de Instituições Bancárias, que tiveram as suas informações sigilosas comprometidas, mediante o uso da engenharia social e as técnicas utilizadas para tal comprometimento.

1.2 HIPÓTESE

Foi levanta a seguinte hipótese relacionada aos objetivos da pesquisa:

I. A engenharia social compromete a segurança da informação dos usuários de Instituições Bancárias.

1.3 OBJETIVOS

Para nortear este trabalho, foram definidos os objetivos geral e específicos que serão descritos a seguir.

1.3.1 Objetivo geral

A presente pesquisa tem como objetivo geral analisar a segurança da informação de usuários de Instituições Bancárias a partir da perspectiva da engenharia social.

1.3.2 Objetivos específicos

a) Identificar e entender as técnicas da engenharia social às quais os usuários de Instituições Bancárias estão suscetíveis;
b) Identificar as informações disponibilizadas em *sites* de Instituições Bancárias relacionadas com a segurança da informação de seus usuários.
c) Identificar o perfil dos usuários fraudados eletronicamente na Instituição Bancária estudada;

1.4 JUSTIFICATIVA

Nesta subseção são apresentadas as justificativas pessoal, científica, econômica e social, motivadoras para a realização da pesquisa.

1.4.1 Justificativa Pessoal

Desde 2001 a condução dos processos de contestação de fraudes de usuários da Instituição Bancária na qual a autora trabalha, passou a integrar as suas atividades e despertou seu interesse sobre a área. A

partir de 2007, a condução e a análise dos processos de fraude passaram a compor, exclusivamente, as suas atividades laborais.

Neste contexto, algumas inquietações afloraram: diante do investimento de recursos alocados pelas Instituições Bancárias para os processos relacionados à segurança das informações sigilosas dos usuários, por que as fraudes crescem? Os usuários conhecem a política de segurança da sua instituição bancária e os canais de comunicação utilizados por esta para a divulgação de sua política de segurança? Os usuários conseguem identificar as ameaças relacionadas à segurança de suas informações sigilosas?

Durante as especializações da autora sobre o assunto, identificou a necessidade de desenvolver um trabalho científico que responda a estas inquietações. Assim, a identificação das características comuns dos usuários de Instituições Bancárias, cujas informações sigilosas foram comprometidas surgiu como proposta desafiadora para responder aos seus anseios e que a partir de tal delimitação, novos estudos possam ser propostos com objetivo de atenuar as fraudes contra usuários de Instituições Bancárias, aperfeiçoar o processo de comunicação das Instituições Bancárias sobre as suas políticas de segurança e desenvolver a cultura de segurança dos usuários.

1.4.2 Justificativa Científica

A Ciência da Informação estuda o comportamento, as características do indivíduo, a sua relação com a informação e a geração do conhecimento. A proteção e a segurança da informação fazem parte deste contexto. Porém, há poucos referenciais teóricos na área da Ciência da Informação relacionados ao tema segurança da informação. A grande maioria dos trabalhos científicos sobre a segurança da informação apresenta um enfoque direcionado para Ciência da Computação e Tecnologia da Informação, escapando da temática a que se propõe esta pesquisa.

A constatação de referenciais teóricos sobre o tema foi observada a partir da coleta de dados no portal de periódicos da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - CAPES, acessado durante o mês de junho de 2014, pela rede da Universidade Federal de Santa Catarina – UFSC. Foi utilizado o termo exato “segurança da

informação" no campo destinado à busca por assunto, presente nos títulos dos trabalhos científicos, dos últimos dez anos, ou seja, de 2003 à 2013. Foram recuperados apenas 12 trabalhos, indexados em todas as bases de dados que incorporam o portal da CAPES. A pesquisa foi repetida utilizando o termo exato em inglês "*Information Security*", sendo recuperados 372 resultados. Em ambas as pesquisas, o resultado recuperado demonstrou a predominância do assunto na área de tecnologia.

A pesquisa bibliográfica foi realizada também na Base de Dados Referencial de Artigos de Periódicos em Ciência da Informação – BRAPCI, com a mesma metodologia de pesquisa realizada no portal de periódicos da CAPES e igual período, tendo como resultado a recuperação de 08 artigos científicos com o termo exato em português e apenas dois artigos com o termo em inglês.

1.4.3 Justificativa Econômica e Social

A última pesquisa realizada pela FEBRABAN, sobre a perda dos bancos brasileiros com fraudes eletrônicas foi divulgada em 2012 e demonstrou que os mesmos perdem, por ano, o equivalente a R$ 1,4 bilhão. As perdas estão relacionadas, em sua grande maioria, com a exploração do comportamento e das características do indivíduo na internet pelos fraudadores. A FEBRABAN estimou na pesquisa que a cada dezesseis segundos há uma tentativa de fraude contra usuários de Instituições Bancárias.

Tais instituições investem grande parte de seus recursos em aparatos tecnológicos para protegerem suas informações e de seus usuários. De acordo com a FEBRABAN, os bancos que operam no Brasil gastaram cerca de R$ 21,56 bilhões em tecnologia em 2014, correspondendo a um volume que equivale a 17% dos gastos em tecnologia da informação no Brasil, sendo o setor bancário o maior investidor em tecnologia quando comparado com todas as indústrias instaladas no país. No entanto, as fraudes aumentam exponencialmente, crescendo em média 35% ao ano. Este crescimento tem como impacto, nos indivíduos vítimas, a perda da confiabilidade do canal utilizado na fraude e na própria instituição bancária.

Para Laudon (2010), é difícil mensurar os prejuízos econômicos advindos dos crimes de informática, devido a quantidade de sistemas

invadidos, as pessoas envolvidas e também, porque as empresas, como as instituições bancárias, resistem em divulgar tais informações, com o propósito de preservação da sua imagem e reputação.

Não se pode deixar de mencionar o destino dos valores oriundos das fraudes eletrônicas, pois é de saber notório que tais valores representam um dos braços financeiros do crime organizado, que se retroalimenta à medida que as fraudes acontecem. Isto é, os delitos são organizados por quadrilhas especializadas em crimes eletrônicos, responsáveis por recrutarem profissionais, e estas são financiadas por organizações criminosas de alcance internacional.

Espera-se que esta pesquisa possa contribuir para o entendimento do fluxo das informações sigilosas dos usuários de Instituições Bancárias, cuja segurança informacional foi comprometida. Acredita-se que a partir do mapeamento do fluxo e a identificação dos riscos relacionados com a exposição das informações sigilosas, será possível conhecer os subterfúgios utilizados para comprometer a segurança da informação, na perspectiva de propor uma maior atenção ao tema, com intuito de preservar as informações de natureza sigilosa.

1.5 ESTRUTURA DO TRABALHO

Esta dissertação está estruturada em 6 capítulos para melhor abordagem do objeto de estudo. Os elementos introdutórios estão no capítulo 1. No capítulo 2, é apresentado o referencial teórico que norteia os estudos sobre o impacto da internet na organização dos sistemas informacionais, os avanços da Ciência da Informação e a necessária segurança, bem como as ameaças que surgiram aos ativos informacionais, expressas na engenharia social, entendida como conjunto de práticas utilizadas para se obter informações sigilosas ou importantes de empresas, pessoas e sistemas de informações.

No capítulo 3, são abordadas as orientações das instituições bancárias para seus usuários no que tange à segurança da informação, considerando as regras, diretrizes e parâmetros normatizados pela FEBRABAN, relacionadas ao fluxo informacional, transações financeiras e incidentes de segurança.

No capítulo 4 estão descritos os métodos aplicados na coleta e tratamento dos dados obtidos com a pesquisa realizada relativamente ao

tema na região da Grande Florianópolis. O capítulo 5 é dedicado à observação dos resultados e repercussões do estudo relativo ao fluxo informacional desenvolvido pela engenharia social e das iniciativas das instituições bancárias para combater as fraudes contra seus usuários e fortalecer sua política de segurança. Em seguida, apresentadas as considerações finais acerca do estudo desenvolvido. E por fim, as referências consultadas no desenvolvimento desta dissertação.

2 REFERENCIAL TEÓRICO

Para um melhor ordenamento do referencial teórico que sustenta esta dissertação, apresentamo-lo em três eixos de abordagem: Segurança da Informação; A Segurança da Informação no Contexto da Ciência da Informação; e Engenharia Social.

No primeiro eixo aborda-se aspectos conceituais e as ameaças à Segurança da Informação. No segundo, observa-se o escopo da Ciência da Informação, a segurança da informação no contexto do ciberespaço e normas e padrões nacionais e internacionais sobre o tema. Já no terceiro eixo, nos atemos na abordagem conceitual da Engenharia social, seu perfil e atuação, suas ferramentas e fluxo, as técnicas da engenharia social e seus aspectos comuns.

2.1 SEGURANÇA DA INFORMAÇÃO

A automatização dos sistemas de informação e as redes de comunicação de dados constituem o espaço cibernético digital e a segurança desse espaço envolve não só os computadores, como os seus usuários. Os aspectos conceituais relacionados à segurança da informação e as ameaças gerais às informações, serão abordadas nas sessões 2.1.1 e 2.1.2.

2.1.1 Segurança da Informação – aspectos conceituais

A internet revolucionou a forma da organização dos sistemas informacionais, com a intensificação das interações entre o usuário e a tecnologia, tendo o imediatismo como característica determinante do processo. A arquitetura de tais sistemas pode ser equiparada à arquitetura das edificações, iniciando o processo com a escolha do público ao qual se destina, o seu escopo e os procedimentos necessários para atuarem de forma segura, eficiente e eficaz (VIDOTTI; SANCHES, 2004). Assim como a arquitetura informacional, as edificações apresentam propósitos singulares, constituídos por elementos que as individualizam, como *design* e localização (VIDOTTI; SANCHES, 2004). Porém, se projetados ou utilizados de forma inadequada, poderão ser corrompidos.

As informações, "cimento" dos sistemas informacionais, podem ser igualadas a um produto e, para tanto, traz para o seu cerne as vulnerabilidades e ameaças, visto que um produto ou um sistema é considerado seguro, quando não utilizado (WOOD, 2005). O diferencial da segurança informacional para os demais produtos é que não há perda de valor ou destruição com o uso da informação e, em determinadas situações, quanto mais utilizada, maior valor lhe será agregado (SILVA, 2011). A informação pode ser conceituada como uma articulação de dados que, após trabalhados ou processados, apresentam um significado sobre determinado assunto, conceito este elaborado pelos autores Coelho, Rasma, Morales (2013), utilizando referenciais do latim, cuja palavra *informationem*, corresponde a "delinear", "conceder uma ideia", bem como referenciais bibliográficos, como de Rezende e Abreu (2000), que descrevem a informação como um dado dotado de interpretação do usuário, sendo esta lógica ou natural.

Sêmola (2014, p. 69) define informação como:

> [...] conjunto de dados utilizados para a transferência de uma mensagem entre indivíduos e/ou máquinas em processos comunicativos ou transacionais. [...] A informação pode estar presente ou ser manipulada por inúmeros elementos deste processo, chamados ativos, os quais são alvos de proteção da segurança da informação.

As informações e o seu intercâmbio impulsionam a sociedade da informação, cujas distâncias foram diminuídas. Com os avanços tecnológicos e com a internet, o seu transporte é imediato. Ao mesmo tempo em que os avanços tecnológicos foram criados e desenvolvidos, surgiram as ameaças aos ativos informacionais, seja através de equipamentos, sistemas ou pessoas.

Em análise da literatura sobre conceitos de segurança da informação, depara-se com amarras relacionadas ao seu campo de atuação, a sua função e objetivo e não ao conceito propriamente dito.

Pemble (2004) buscou parametrizar e compreender a segurança da informação, considerando a atuação dos seus profissionais, e vislumbrou três esferas conceituais. A primeira é a esfera operacional, pela qual a segurança da informação está relacionada aos incidentes e as suas consequências no âmbito operacional da organização. A relação entre os incidentes e os seus impactos sob o valor da marca e valor

acionário, representam a segunda esfera, denominada de esfera da reputação, enquanto que a terceira é a esfera financeira e envolve os custos advindos de eventuais incidentes.

A segurança da informação é embasada por Anderson (2003) como sendo um sentimento bem fundamentado da garantia de que os controles de riscos da informação estão bem equilibrados, trazendo os desdobramentos de tal conceito e as principais ameaças informacionais.

Considerando o estudo ontológico da segurança da informação, Peixoto (2006) descreve seis principais atributos ou princípios. O primeiro atributo ou princípio, diz respeito à confidencialidade, cujas ferramentas tecnológicas de segurança atuam no sentido de proteger o sigilo, limitando o acesso à informação. Este princípio garante que apenas as pessoas que devam ter conhecimento da informação possam acessá-la. Para Sêmola (2014), a confidencialidade está relacionada à acessibilidade da informação aos agentes autorizados e inacessibilidade aos agentes não autorizados.

O segundo princípio, da integridade da informação, visa garantir a manutenção das características originais da informação, estabelecidas pelo autor, ou seja, inviabiliza as alterações do documento de origem. No mesmo sentido que Peixoto (2006), Sêmola (2014) relaciona a integridade com a possibilidade de que a informação somente pode ser alterada por agentes autorizados e os não autorizados estão impedidos de comprometê-las.

O terceiro princípio se refere à disponibilidade, ou seja, a informação poderá ser acessada por qualquer pessoa e a qualquer tempo, assim, refere-se ao acesso da informação somente por agentes autorizados e a qualquer momento (PEIXOTO, 2006; SÊMOLA, 2014).

Na tentativa de se estabelecer um conceito mais abrangente, Marciano e Marques (2010) consideram a segurança da informação como um fenômeno social cujos usuários dos sistemas de informação - sejam eles os gestores ou os usuários comuns - detém conhecimento coerente das suas regras de uso. Os autores, ao desdobrarem este conceito, delimitaram os requisitos formadores da segurança da informação, sendo eles: os atores do processo, o ambiente no qual estão inseridos - sistemas computacionais e tecnológicos - além da sociedade, por ser esta, o alcance final da atuação da segurança da informação.

As ontologias que permeiam a segurança da informação, isto é, a categorização do que é essencial para a segurança da informação, o seu

objeto ou o seu processo, foram elaboradas pelos autores Almeida, Souza e Coelho (2010), a partir de uma revisão de literatura, dos quais foram destacados: organização, atributo de segurança, ativo, controle, ameaças e vulnerabilidades, visto que os conceitos individualizados foram assim expostos:

Quadro 1: Principais definições da ontologia de segurança.

Organização	Uma organização é uma entidade social composta por recursos materiais e humanos, a qual possui objetivos comuns, procedimentos sistemáticos para controle de seu desempenho e limites definidos que a separam do ambiente. Pode ser uma instituição pública ou privada.
Atributo de segurança	Um atributo de segurança é uma propriedade atribuída a um ativo, a qual diz respeito a requisitos de segurança. Pode ser um atributo de confidencialidade, de integridade e de disponibilidade
Ativo	Um ativo é um bem de propriedade da organização, utilizado para alcançar seus objetivos sociais. Pode ser um equipamento, estoque, imóvel, dentre outros.
Controle	Um controle é um procedimento padrão sistemático implementado para atenuar vulnerabilidades, bem como para proteger ativos através de medidas preventivas e corretivas.

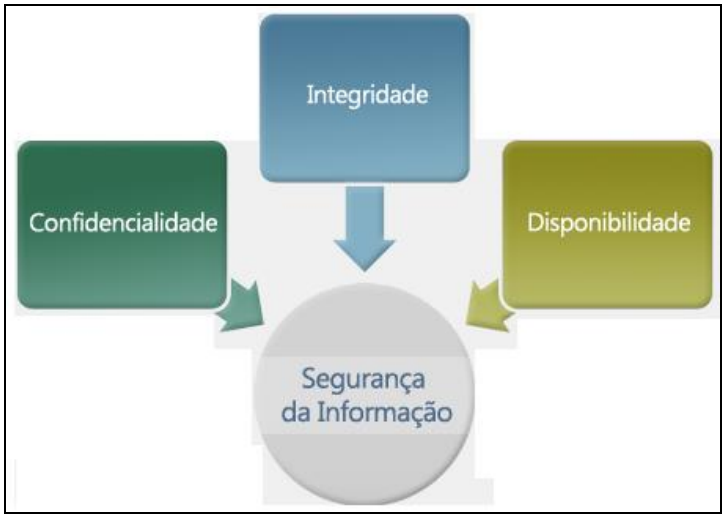
Ameaça	Uma ameaça é uma possibilidade de dano aos ativos da organização, que afeta os atributos de segurança específicos e explora vulnerabilidades da organização. Pode ser de origem humana ou natural e ter como fonte um evento acidental ou uma ação deliberada.
Vulnerabilidade	Vulnerabilidade é uma situação caracterizada pela falta de medidas de proteção adequadas. Uma vulnerabilidade possui um grau de severidade associado (por exemplo, crítico, moderada ou baixo). Pode ser uma vulnerabilidade de origem administrativa, técnica ou física.

Fonte: Coelho (2010, p 161)

Entenda-se então, com base nos conceitos e nas ontologias supracitadas, que a segurança da informação é formada pela simbiose dos sistemas informacionais e tecnológicos, aliada ao comportamento e características do usuário, envolvendo aspectos de natureza física, política e cultural. O desafio da segurança da informação é equilibrar tal relação e afastar as ameaças e vulnerabilidades que circundam as informações sistematizadas.

Na ilustração 1 destaca-se os princípios que regem a segurança da informação.

Ilustração 1: Princípios da Segurança da Informação.



Fonte: Maia (2013)

Assim, integridade, confidencialidade e disponibilidade são considerados princípios fundamentais para garantir a segurança da informação bancária, além de, afastar possíveis ameaças e vulnerabilidades que possam comprometer os sistemas informacionais.

O ritmo da evolução da humanidade está interligado ao aumento dos estoques informacionais. Tanto a disponibilidade, quanto a confidencialidade e integridade da informação podem ser comprometidas quando esta é manipulada por pessoas não autorizadas.

As práticas criminosas exploram a tríade da segurança da informação, comprometendo-a. As atividades em rede, que podem comprometer a segurança da informação envolvem: a invasão de *sites* de governos, de empresas e contas bancárias, com captura de códigos dos cartões e senhas, a exploração de informações particulares disponibilizadas em redes sociais usadas para a prática de extorsão contra os usuários, que serão analisadas posteriormente.

> Neste sentido cabe dizer que a preocupação tanto com o conteúdo quanto com o tipo de uso, e a respectiva segurança da rede, crescem em igual medida aos desenvolvimentos tecnológicos e ao

> número de usuários, observados ao longo dos últimos anos (CANONGIA, 2009, p. 24).

A segurança e a privacidade são valores que fazem parte dos sistemas de informação. A organização da sociedade da informação circunda tais valores, os quais precisam ser protegidos contra os crimes cibernéticos que envolvem o uso ilegal de hardware, software ou de dados (LAUDON; LAUDON, 2010).

A segurança da informação é aplicada para tudo aquilo que possui um valor, seja para o indivíduo ou para uma organização, que é denominado de ativo (RAMOS, 2006). Para Campos (2014), ativo é um bem patrimonial em razão do seu valor, seja para a empresa ou para o indivíduo, como, por exemplo, a informação, os seus suportes e os seus canais de utilização, sendo estes denominados de ativos de informação. De uma forma geral, os ativos podem ser classificados como tangíveis exemplificados por informações impressas e escritas, e intangíveis, como a imagem, confiabilidade e a marca.

Salvaguardar os sistemas de informação contra acessos não autorizados, alterações, furtos informacionais e danos físicos é premissa da segurança da informação. Neste sentido, Laudon (2010) destaca que as ferramentas computacionais são utilizadas por usuários mal-intencionados para cometer *cibercrimes*, que são aqueles cometidos no ambiente virtual, cujo agente ativo (criminoso), aguarda o *click* do agente passivo (vítima) para obter a informação desejada. O *cibercrime* vem sendo intensificado face aos baixos custos, visto que o comprometimento da segurança da informação mediante a exploração das vulnerabilidades humanas tem como instrumental um computador com acesso à internet. O engenheiro social que aplica técnicas, muitas vezes simples, para obter a informação valorada, para Mitnick e Simon (2003), são profissionais especializados na "arte de enganar".

> Uma vez que os dados são coletados em forma digital, todos os itens de informação contidos no banco de dados podem ser agregados, desagregados, combinados e identificados de acordo com o objetivo e o poder legal. Por vezes, trata-se simplesmente de fazer perfis agregados, em pesquisa de mercado, seja para comércio ou para a política. Em outros casos trata-se de visar

> indivíduos, já que uma pessoa pode ser caracterizada por um grande corpo de informação contido em seus registros eletrônicos, de pagamentos por cartão de crédito a visitas a web *sites*, correio eletrônico e chamadas telefônicas (CASTELLS, 2003, p. 142).

A simbiose entre o controle de acesso e a sua eficiência são um dos escopos da segurança da informação e:

> É relevante destacar que não adianta as instituições apenas elaborarem regras se estas não forem devidamente registradas e conhecidas pelas pessoas que trabalham com o tratamento da informação e, também, por aqueles que possuem o direito de acesso a ela (SFREDDO; FLORES, 2012, p. 175-176).

Quanto maior o controle e a quantidade de restrições para acessar uma informação, segundo Silva (2011), maior será o grau de desconforto do usuário, pois tal sentimento é diretamente proporcional ao grau de segurança, podendo alcançar o seu comprometimento dependendo das reações dos usuários e das medidas implementadas pelas organizações. Nesse sentido, Mitnick e Simon (2003) ressaltam que a segurança não é problematizada pela tecnologia, mas sim pelas pessoas, consideradas o elo mais fraco da segurança.

2.1.2 Ameaças gerais às informações

Os colaboradores e usuários são, para Mitnick e Simon (2003), as maiores ameaças à segurança da informação, seja por negligência ou por falta de conhecimento. Assim, as estratégias de segurança precisam considerar o fator humano como integrante do processo, ambos ativos, afastando os riscos mediante duas dimensões interconectadas, o conhecimento e o comportamento (NIEKERK, SOLMS, 2010).

O desenvolvimento tecnológico impulsionou as diversas formas de ameaças à informação, sejam elas físicas ou virtuais e em consequência a segurança da informação está suscetível de ser comprometida. Para Santos (2011), o ser humano é a principal ameaça a qualquer tipo de informação, visto que o seu processamento se inicia e finaliza no usuário do sistema informacional.

A estrutura da internet e a sua característica liberal pode ser equiparada a abertura de um cofre, onde todos os dados e informações, em princípio, estão acessíveis e disponíveis aos usuários (LAUDON, 2010).

A dificuldade de proteção da informação na rede está intrínseca à falta de uma cultura de segurança, pois os sentimentos de ameaça e risco são imperceptíveis para certos usuários. A esse respeito, Canongia (2009) converge no sentido de que é necessária a conscientização do usuário dos riscos que norteiam as tecnologias, reportando inclusive, que todos os que estão inseridos na rede são responsáveis pela segurança cibernética, como se observa a seguir:

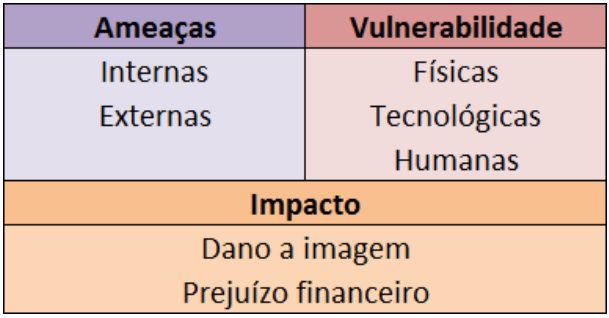
> Pois, de nada vale a melhor capacitação técnica senão se conscientizar o usuário, o profissional, o cidadão, destas tecnologias, e de que a segurança da informação e, consequentemente, a segurança cibernética, é um problema de todos. Assim sendo, esta conscientização deve ser iniciada desde o ensino fundamental, criando uma cultura orientada a esta abordagem, pois é inegável que a cada dia a iniciação digital se dá em idades mais precoces. (CANONGIA, 2009, p. 43).

Os riscos que envolvem a segurança da informação, conforme descreve Sêmola (2014), estão relacionados a vários fatores, entre os quais podemos destacar as ameaças internas em uma organização, como por exemplo, desastres naturais (inundações, incêndios), ações voluntárias de funcionários insatisfeitos e desconhecedores das normas e políticas de segurança, e ainda, as ameaças externas, com ações de engenharia social. As políticas de segurança da informação são normas de conduta destinadas aos usuários de sistemas computacionais durante o processo de interação entre o homem e a máquina (MARCIANO, MARQUES, 2006, p. 90). Para Laudon (2010), as políticas de segurança da informação têm como premissa a proteção aos ativos de uma empresa, na qual estabelece hierarquia aos riscos de informação, identifica metas de segurança e níveis de acesso.

Um segundo fator, segundo Sêmola (2006) são as vulnerabilidades físicas, exemplificadas pela autora pela ausência de barreiras de controle de acesso, além das vulnerabilidades tecnológicas, advindas de configuração inadequada de *firewall* e, por fim, as

vulnerabilidades humanas, marcadas pela ausência de conscientização através de treinamentos que difundam as políticas de segurança. Os impactos, também são destacados pelo autor, como fatores de riscos para segurança da informação, sendo estas consequências do pós-incidente, como o dano à imagem e o prejuízo financeiro.

Ilustração 2: Diagrama – Fatores de riscos da segurança da informação.



Fonte: elaborado pela autora com base texto de Sêmola (2006)

As ameaças mais recorrentes na rede envolvem os usuários de boa fé e aqueles mal-intencionados, que têm objetivo de adquirir algo valioso, seja um dado, uma informação ou mesmo uma vantagem pecuniária, explorando as vulnerabilidades dos sistemas, a confiança e o comportamento do usuário.

2.2 A SEGURANÇA DA INFORMAÇÃO NO CONTEXTO DA CIÊNCIA DA INFORMAÇÃO

Será apresentada a seguir a relação entre a Ciência da Informação e a Segurança da Informação, bem como as normas nacionais e internacionais voltadas para a segurança da informação.

2.2.1 O escopo da Ciência da Informação

Os aspectos culturais, políticos e econômicos da sociedade estão relacionados diretamente ao trato e a valoração da informação. Há muito tempo as pessoas apresentaram uma necessidade instintiva de se

comunicar e transmitir informações, e para tanto desenvolveram códigos. Tais códigos, com a evolução da humanidade, permitiram o desenvolvimento de vantagens informacionais, seja para fins comerciais, pessoais ou empresariais e influenciaram a alteração de comportamentos dos indivíduos, cuja relação homem e informação passou a ser estudada por várias áreas do conhecimento humano, como a Ciência da Informação.

A década de 1960 foi marcada pelos primeiros conceitos de Ciência da Informação, cujo escopo, ainda presente, está voltado para a produção, a organização, o armazenamento, a disseminação e o uso da informação. Este uso, seja para produção do conhecimento ou para prática de espionagem, se transforma e acompanha o desenvolvimento da sociedade. A Ciência da Informação promoveu, desde a sua concepção, uma reflexão afeita à informação e, com o advento das tecnologias, estuda a mediação entre a informação e a geração do conhecimento para o indivíduo (BARRETO, 2002).

A Ciência da Informação, ao final da década de 1970, iniciou o desenvolvimento de estudos científicos voltados aos usuários. O principal marco foi a Conferência de Copenhagen, em 1977, com a apresentação de trabalhos científicos focados nos padrões de comportamento informacional e características dos usuários (ARAÚJO, 2009). A partir desse período a Ciência da Informação enfatiza a informação como ferramenta norteadora dos padrões de comportamento e características dos indivíduos, de natureza cumulativa e responsável pela formação de um mapa mental. Assim, o indivíduo, suas percepções e interações com o meio no qual está inserido passam a ser analisados.

Os usuários são estudados enquanto seres dotados de determinado "universo" de informações em suas mentes, utilizando essas informações para pautar e dirigir suas atividades cotidianas, "[...] tal perspectiva permite compreender a informação inclusive numa lógica cumulativa, à medida que novas informações se somam às anteriores no mapa mental dos indivíduos" (ARAÚJO, 2009, p. 200).

Uma das características da Ciência da Informação é ser interdisciplinar, pois suas pesquisas estão relacionadas a campos derivativos da Matemática, Lógica, Linguística, Psicologia, Ciência da Computação, Engenharia da Produção, Artes Gráficas, Comunicação, Biblioteconomia, Administração, entre outros. Pode ser considerada uma ciência pura quando investiga seu objeto sem considerar sua

aplicação ou ciência aplicada, quando desenvolve serviços e produtos (BORKO, 1968).

Para Borko (1968), a meta da Ciência da Informação é fornecer *corpus* teórico sobre informação que poderá aperfeiçoar os procedimentos relacionados à acumulação e transmissão do conhecimento.

Portanto, o fluxo da informação é estudado pela Ciência da Informação, que investiga desde o comportamento da informação, o seu uso, a sua transmissão, o seu processamento, com objetivo de armazená-la permitindo uma recuperação eficaz.

Para Burke (2003), o processamento e a sistematização da informação são aspectos fundamentais para a conceituação do conhecimento e a partir do surgimento da prensa móvel, disponibilizando documentos e textos na forma impressa, a publicidade e difusão do conhecimento foram impulsionados. Contudo, se alavancou também as práticas de espionagem de documentos oficiais e sigilosos, sendo copiados e comercializados até mesmo com incentivos governamentais, na busca de informações confidenciais, comprometendo a segurança informacional.

O estudo do indivíduo em relação as suas informações sigilosas ou confidenciais pela Ciência da Informação, pode revelar um processo de construção de conhecimento e afastar riscos inerentes à exposição de tais informações, pois a tecnologia da informação por si só não é suficiente para afastar ameaças físicas ou virtuais advindas da exploração informacional (MARCIANO, MARQUES, 2006). A construção do conhecimento permite gerenciar os riscos e propicia um fluxo informacional seguro, partindo da criação de significados, considerando as informações encontradas, transformando um cenário de incertezas para um ambiente de confiança (CHOO, 2006).

Para Marciano e Marques (2006), a Ciência da Informação e a sua natureza multidisciplinar permitem analisar a segurança da informação sob o escopo da teoria das ciências sociais, visto que:

> [...] a informação é gerada, armazenada, tratada e transmitida com o fim de ser comunicada, e a comunicação é eminentemente um processo grupal, seja ela interna ou externa às fronteiras da organização (MARCIANO, MARQUES, 2006, p. 90).

Os autores complementam o assunto, descrevendo que a padronização das regras de conduta da sociedade da informação, sedimentadas por políticas da informação governamentais ou organizacionais, formatadas em linguagem natural, estão suscetíveis a compreensões ambíguas, situação esta, que pode contribuir para o comprometimento das informações pessoais, presentes nos acervos informacionais. Para tanto,

> Cumpre observar que os sistemas de informação, mormente aqueles digitais, em ampla voga no contexto da sociedade da informação, encontram-se, naturalmente, envoltos por completo em agentes do mundo real, estando sujeitos a várias formas de ações afeitas à sua segurança, tais como negações de serviços, fraudes, roubos, tentativa de invasão, corrupção e outras atividades hostis (MARCIANO, MARQUES, 2006, p. 93).

Contudo, a segurança da informação tem como premissa resguardar a origem, o uso, o processamento e o descarte da informação, estabelecendo um fluxo informacional padronizado e certificado (SÊMOLA, 2014).

2.2.2 A Sociedade da Informação: ciberespaço e segurança da informação

Para Toffler (1985), o processo de evolução da sociedade foi definido em três passagens históricas distintas. A primeira onda de mudança foi determinada pela revolução agrícola, cuja posse da terra era um dos interesses do indivíduo a ser protegido. A segunda onda, caracterizada pela revolução industrial, na qual surge a necessidade de assegurar os meios de produção. E a terceira onda ficou conhecida como a sociedade das novas tecnologias, tendo como figura central a informação.

O conceito de sociedade pós-industrial ou sociedade da informação, para muitos sociólogos como Hugh Gaitskell, Richard Crossmann, Daniel Bell, Seymour Martin Lipset e economistas como Fredrich A. Von Havek, citados por Mattelart (2002), passou a ser desenvolvido a partir de 1960, com a declaração do fim das ideologias e

as primeiras concepções de "sociedade livre", na tentativa de construção de uma sociedade ideal. Por volta de 1970, a expressão sociedade da informação surgiu no meio científico, que atrelada aos avanços tecnológicos ampliou os estoques informacionais em virtude do trabalho em rede dos atores sociais (MATTELART, 2002). Atualmente a sociedade da informação está alicerçada nos avanços tecnológicos, nesse sentido:

> A convergência tecnológica reforça os efeitos da sinergia decorrente da penetrabilidade das tecnologias na sociedade da informação. Daí é fácil compreender a fascinação (e o temor) como uma utópica sociedade informatizada em que não apenas o desenvolvimento tecnológico parece não ter limites nem desacelerar e, dessa forma, alterar continuamente todos os processos que afetam a vida individual e coletiva (WERTHEIN, 2000, p. 74).

Com o desenvolvimento tecnológico, a partir da década de 1970 e as novas concepções da Ciência da Informação, surgiu a sociedade em rede, denominação dada por Castells (1997). Neste contexto, foi desenhada uma nova estrutura organizacional do conhecimento, onde cada indivíduo faz parte de uma cadeia de interações caracterizadas pelas diferenças, com papéis que se transmutam no ambiente informacional e comunicativo, ora o indivíduo atua como produtor e ora atua como receptor do conhecimento, sendo que "[...]o uso cada vez mais disseminado de sistemas informatizados por meio de redes é um fato determinante da sociedade da informação". (MARCIANO; MARQUES, 2006, p. 89).

Esta liberalidade e descontrole presentes também nas relações empíricas dos usuários com a internet, foram determinantes para os avanços tecnológicos e para as transformações da rede. À medida que as necessidades e os comportamentos dos usuários eram mapeados, surgiam novas tecnologias para suprir tais necessidades e esse trânsito foi fundamental para a expansão universal da internet:

> Quer dizer, é um instrumento de comunicação livre, criado de forma múltipla por pessoas, setores e inovadores que queriam que fosse um instrumento de comunicação livre. Nesse sentido, creio que há que ter em mente que as tecnologias

> são produzidas por seu processo histórico de constituição e não simplesmente por desenhos originais de tecnologia (CASTELLS, 2003, p. 262).

O pensar corresponde à libertação do indivíduo de um conhecimento já programado, único e verdadeiro, possibilitando a adaptação de tais conhecimentos às suas necessidades, gerando novos conhecimentos, "[...] mudam-se os tempos, mudam-se as sentenças" (D'AMARAL, 2003, p. 39). Este é o paradigma central da sociedade da informação, a natureza mutável do conhecimento do indivíduo interligada a um processo cíclico que se retroalimenta, inserido em um sistema de rede globalizado.

O processo de transição de uma sociedade industrial, impulsionado pela Revolução Industrial, centralizado na mecanização dos processos de produção e na relação entre a oferta e a procura, para uma sociedade pós-industrial ou sociedade da informação, ou sociedade em rede, reunida no saber e nas inovações tecnológicas, foi marcado pela ruptura de paradigmas significativos.

Um dos precursores desta quebra de paradigmas foi o filósofo Gottfried Wilhelm Leibniz (1646-1716), destacado por Mattelart (2002), que associou a racionalização do pensamento com combinações da matemática, iniciando o processo de automação do pensamento aos moldes da computação moderna. Outro grande filósofo desta área foi Renê Descartes (1596-1650), que sustentava a fundamentação científica dos seus estudos na razão humana livre como capaz de mudar o mundo. Ambos convergiam no sentido da racionalização do pensamento humano, contrariando os dogmas religiosos predominantes até meados do século XVII.

A racionalização dos processos informacionais a partir do século XVII culminou na união das forças industriais e científicas. Neste processo, o Estado, "encarregado pelo negócio", perdeu forças para uma classe elitizada da sociedade e, consequentemente, as funções foram hierarquizadas. O cerne relacional foi o determinismo técnico repercutindo nas primeiras concepções de trabalho em rede, com objetivo de organizar e catalogar o conhecimento (MATTELART, 2002). Diante de tal concepção, Mattelart (2002), na sua análise histórica dos fenômenos sociais, relacionou o surgimento da sociedade da informação aos avanços tecnológicos e à informatização dos

processos, impulsionados após a segunda Guerra Mundial.

A partir da industrialização e do incremento da competitividade das organizações empresariais, a sociedade da informação passou a considerar a informação como o núcleo para o desenvolvimento de estratégias com foco na inteligência competitiva. Desta forma, a internet passou a representar o principal instrumento para realizar negócios. Com a incidência cada vez mais aflorada do fluxo informacional nas relações, a criação, manuseio, armazenamento, transporte e descarte da informação, repercutiu em uma maior vulnerabilidade do processo, que está cada vez mais propenso a incidentes que venham a causar prejuízos (SILVA; ARAÚJO; AZEVEDO, 2013). Uma visão simplista da organização da sociedade da informação, ou sociedade em rede, leva a crer que há uma força dominante e ditadora de regras de comportamento do indivíduo, partindo do alto das classes sociais em direção à base, que o escritor de ciência norte-americano Steven Johnson (2003) denomina de processo *top-down*.

Contrariamente a esta afirmação, Johnson (2003) afirma que a organização social é inversa, há uma força maior, que permeia os grupos sociais para que se organizem a partir de experiências e padrões de comportamento locais, premissa essa também caracterizadora da sociedade em rede. O autor defende a sistematização das organizações sociais, com a interação dinâmica de diversas formas, seguindo ordenamentos locais e sem influência de níveis mais altos, estabelecendo um macro comportamento.

O resultado desse macro comportamento é comparado por Johnson (2003) à organização das colônias de formigas, cuja observação inicial indica que há uma rainha ditadora de regras para manter a colônia em funcionamento, porém experiências demonstraram que há um sistema emergente de auto-organização. O papel da rainha nas colônias de formigas é colocar ovos para a perpetuação da espécie, enquanto que o das operárias é proteger a rainha, alimentando-a e protegendo-a, mas sem nenhum comando direto da rainha. Esta conduta se relaciona diretamente à evolução da espécie, sendo que:

> As colônias estudadas por Gordon mostram um dos mais impressionantes comportamentos descentralizados da natureza: inteligência, personalidade e aprendizado emergem de baixo para cima, *botton-up* (JOHNSON, 2003, p. 23).

Assim, os padrões de comportamentos e características individuais desordenados e repetitivos influenciam os padrões globais, sem uma liderança pré-estabelecida. Esta afirmação é apoiada por Johnson (2003), que descreve a cidade como uma máquina de ampliar padrões.

As ampliações destes padrões estabelecendo uma ordem global partem das interações entre os indivíduos, emitindo e recebendo *feedback*. Para Johnson (2003), uma das formas de representar esse cenário é o processo de aprendizagem, onde há um reconhecimento e uma resposta às mudanças de padrões, com intuito de aperfeiçoar os processos, adaptando-os aos objetivos.

Os sistemas emergentes, baseados em *feedback* e interações, são propulsores do aprendizado especializado. Nas organizações das cidades, o autor exemplifica esses sistemas, comparando-os aos vizinhos que se fixam em determinados locais e trocam experiências mudando padrões comportamentais e aprendendo a partir de observações.

Partindo da asserção de que os padrões individuais influenciam as interações globais, a sociedade em rede também é um exemplo de formação de um sistema de conhecimento *botton-up*. Porém, para Johnson (2003), quanto mais informações fluem no ambiente *web*, mais difícil é o processo de recuperação da informação, em virtude da sua desorganização. O autor defende que a *web* depende de *feedbacks* de seus usuários para ser efetiva, cuja instrumentalização se fundamenta em *softwares* que acompanham o usuário e mapeiam os seus padrões de comportamento e características, como na organização de uma cidade, com a observação de padrões entre vizinhos.

Neste mesmo sentido, a *web* e a sua capacidade de mobilidade e transformação, descritas por Bauman (2001), correspondem a uma das características da Sociedade da Informação, ou seja:

> Associamos “leveza” ou “ausência de peso” à mobilidade e à inconstância: sabemos pela prática que quanto mais leves viajamos, com maior facilidade e rapidez nos movemos. Essas são razões para considerar “fluidez” ou “liquidez” como metáforas adequadas quando queremos captar a natureza da presente fase, nova de muitas maneiras, na história da modernidade (BAUMAN, 2001, p. 12).

Convergindo com Johnson (2003), para Castells (2003), a trajetória da internet desde os seus primórdios foi marcada pela liberalidade e descontrole, com intuito de estabelecer uma comunicação livre entre os indivíduos.

Para tanto, a Sociedade em Rede, ou Sociedade da Informação, é o resultado de um pensamento complexo, influenciado pelos avanços tecnológicos e impulsionador do trabalho em rede. Este trabalho possibilitou a massificação, a evolução e o intercâmbio de técnicas, informações e conhecimento. Acompanhando esta assertiva, Lemos (2010) expõe:

> O que constitui essa nova "comunicação pessoal" é o controle individual e a partilha coletiva da informação em mobilidade com o alcance planetário. Esses novos formatos midiáticos podem criar práticas políticas reais que "comecem a agir sobre a grande mídia, a controlar as informações, a desmenti-las e até mesmo a produzi-las" (LEMOS, 2010, p. 71)

Nesse sentido, o sociólogo Manuel Castells defende que o trabalho em rede é determinante da sociedade da informação, sendo que:

> Redes constituem a nova morfologia social de nossas sociedades, e a difusão da lógica de redes modifica de forma substancial a operação e os resultados dos processos produtivos e de experiência, poder e cultura (CASTELLS, 2000, p. 497).

O computador conectado em rede representa a forma de comunicação bilateral da sociedade da informação. Neste ciberespaço os indivíduos trocam informações, atuando ora como emissor, ora como receptor, e a palavra-chave desse processo é interatividade, assim destacada:

> Na Internet, não há limites para a informação. Milhões de computadores em todo o mundo estão interligados em sintonia com o nascimento de uma sociedade da informação. Neste universo, também há lugar para o comércio. Afinal, a Internet saiu dos circuitos universitários, e hoje atinge um grande público consumidor (MEDEIROS, 2002, p. 15).

Conforme descrito por Lévy (1999, 2003) na década de noventa, do século passado, atuando como visionário para o período das tendências da evolução do pensamento complexo, com a internet, o conhecimento teria abrangência coletiva, globalizada e em tempo real, cuja informação seria o centro das interações, estabelecendo um espaço antropológico.

O ciberespaço surge, neste contexto, na Sociedade da Informação, formado por estruturas físicas, como cabos, computadores e pelo indivíduo, que exerce papel fundamental e transformador quando interage com tal ambiente, onde as pessoas poderiam promover encontros, estabelecer fronteiras econômicas e culturais, bem como digladiar. No ciberespaço há a presença de uma cibercultura, concebida por cenário digital, dotada de práticas, atitudes, ideias e valores, naturalmente universais, que é "[...] a presença (virtual) da humanidade em si mesma" (LÉVY, 1999, p. 121).

A informação em formato digital, disponível no ciberespaço, estabelecendo ciberculturas e universalmente disponível, sobrecarrega o sistema informacional e, para Paiva (2014, p. 3), "[...] tratar de um elemento como a informação torna-se uma missão árdua, haja vista que diversos conceitos são dotados para esse substantivo de natureza irregular". Com base nesta assertiva:

> O ciberespaço (o espaço cibernético) é considerado como a metáfora que descreve o espaço não físico criado por redes de computador, notadamente a Internet, onde as pessoas podem se comunicarem de diferentes maneiras, como mensagens eletrônicas, salas de bate-papo, grupos de discussão, dentre outros (CANONGIA, 2009, p. 25).

A Internet no ciberespaço é considerada por Gonzalez de Gomes (2006) uma metatecnologia, pois:

> [...] aumenta o grau de liberdade com que os homens podem atuar nos mundos social e material. Permitem executar largas cadeias de processamento, a partir de diversos *inputs* e obtendo um número indefinido de produtos. Sendo sociais em sua produção, permite que desde um único ponto se possa intervir em uma vasta

> rede com múltiplas consequências no mundo social e material (GONZALEZ DE GOMES, 2006, p. 52).

A metatecnologia e o universo interativo e conectado em rede, para Callon (2010), é uma tendência da sociedade atual, saindo de um ambiente de passividade e emergindo para um ambiente de interações, promovendo escolhas individuais e, consequentemente, influenciando o coletivo, estabelecendo padrões e incentivando inovações. Para Callon (2010) e Parente (2010), este processo é mediado pela conexão do passado com o presente, transformando o futuro.

Segundo Lévy (2001), este sistema corresponde a um rizoma, sem início, meio e fim, constituído por nós interconectados, estabelecendo uma via de mão dupla sob o escopo informacional. As relações sociais se desenvolvem neste espaço democrático, sendo que:

> Hoje, a *world wide web* – literalmente a teia mundial – já realizaria, conforme alguns, um "planeta relacional", uma sociedade transparente, consensual e democrática. A técnica desempenharia o papel de prótese multiforme: as redes de informação ocupariam lugar de novo vínculo social e de ferramentas para uma nova "democracia eletrônica", direta, interativa e instantânea. (MUSSO, 2010, p. 35)

Contudo, o gerenciamento do crescente volume informacional é um desafio para os profissionais da informação, cientistas, Estado e indivíduos. Para delimitar qual informação pode ser considerada relevante ou não para o indivíduo ou para um grupo e estabelecer qual a ferramenta mais adequada para disponibilizá-la e protegê-la, é preciso considerar o cenário heterogêneo e despadronizado da Sociedade da Informação. Assim,

> [...] para se construir um comportamento de segurança da informação em uma organização, será preciso interagir os elementos pertinentes à Ciência da Informação, e que esses elementos alimentam uma trajetória que se inicia com a necessidade de informação, passa pela busca informacional e termina com o comportamento informacional (ALMEIDA; CARNEIRO, 2013, p. 181).

As inovações tecnológicas repercutiram, além das trocas informacionais de conhecimentos e ideias na Internet, na comercialização eletrônica de bens e serviços e ainda na transmissão de dados sensíveis. E nesse escopo surge a necessidade de um ciberespaço seguro. Os usuários se expõem ao ambiente da internet e, para Castells (2003), significa que ao estar conectado, não existe privacidade.

Considerando a assertividade de Castells (2003), foi realizado um estudo, por Silva, Araújo e Azevedo (2013), no qual identificaram que as informações pessoais estão cada dia mais presentes na Internet, principalmente com a ascensão das redes sociais, e ultrapassam a esfera da organização. Na pesquisa, se considerou como informação pessoal, aquela "[...]relacionada à pessoa natural identificada ou identificável, relativa à intimidade, vida privada, honra e imagem", definição disponível no Decreto nº 7.724, de 16 de maio de 2012 (BRASIL, 2012). As variáveis aplicadas foram o número da carteira de identidade e Cadastro de Pessoa Física – CPF, gostos e preferências, data de aniversário, informações familiares, lugares frequentados, relacionamentos, endereços, e-mail pessoal e profissional, telefones, profissão, local de trabalho e educação. Os resultados da pesquisa demonstraram que 70% da amostra apresentou um grau de exposição das informações pessoais na Internet alto, 20% extremamente alto e nenhum indivíduo apresentou grau de exposição zero. Desta forma, a visão holística do uso da informação em segurança é fundamentada por processos inerentes ao indivíduo - criar significado, construir conhecimento e a tomada de decisões - processos estes interconectados, produzindo os fluxos de informação (CHOO, 2006). Nessa mesma perspectiva, o autor descreve que:

> O valor da informação, reside no relacionamento que o usuário constrói entre si mesmo e determinada informação. Assim, a informação só é útil quando o usuário infunde-lhe significados e a mesma informação objetiva pode receber diferentes significados subjetivos de diferentes indivíduos (CHOO, 2006, p. 70).

O autor ressalta, ainda, que as reações emocionais dos indivíduos, os orientam na busca da informação. O processo se inicia com a necessidade de informações, aflorando sentimentos de insegurança e

apreensão. As interações sociais fazem parte do processo da formação do conhecimento e a partir deste fluxo, conforme as informações são identificadas, o sentimento de insegurança é substituído por otimismo. Assim, o indivíduo é incentivado a buscar maiores informações sobre o tema, ficando mais bem informado e orientado. Para tanto, a segurança da informação está relacionada diretamente ao conhecimento e à cooperação humana (CHOO, 2006).

O fluxo das informações é estudado considerando o indivíduo e as suas interações com o ambiente no qual está inserido. Os objetivos de tais estudos podem ser diversificados, como o desenvolvimento e aperfeiçoamento de produtos e serviços. Podem, inclusive, ser utilizados como ferramentas para a prática de espionagem, tornando pública uma informação particular, ou ainda obter alguma vantagem que não é devida.

Assim, considerando a continuidade da garantia da liberdade da rede, o máximo que se consegue desenvolver são ferramentas de vigilância e monitoramento para coibir o cibercrime contra os Estados e os cidadãos.

A implementação de tais ferramentas pode transformar o ciberespaço em um ambiente regulado pelo Estado e há uma linha tênue entre o controle estatal com intuito da proteção da soberania e dos cidadãos e o cerceamento à liberdade do indivíduo. Diante disso:

> Se esse sistema de vigilância e controle da Internet se desenvolver plenamente, não poderemos fazer o que nos agrada. Talvez não tenhamos nenhuma liberdade, e nenhum lugar onde nos esconder. [...] O ataque global à privacidade para restaurar o controle num padrão de soberania compartilhada assegura direitos de propriedade sobre a informação à custa do uso público dessa informação. Para fazer valer seus interesses, o comércio e os governos ameaçam conjuntamente a liberdade ao violar a privacidade em nome da segurança (CASTELLS, 2003. p. 149 e 150).

Para se manterem ativas no mercado globalizado, as organizações empresariais precisam investir uma parcela representativa de seus ganhos em segurança, tratando todo o fluxo informacional de seus produtos e serviços, ou seja, desde a criação até o seu descarte,

potencializando as oportunidades e afastando as ameaças. Para tanto, o sistema informacional das organizações empresariais não é uniforme, porém o fluxo tem como premissa agregar valor.

> O fluxo da informação em uma organização é um processo de agregação de valor, e o sistema de informação pode ser considerado como uma cadeia de valor, por ser o suporte para produção e transferência da informação (MORESI, 2000, p. 23).

Assim, a informação valorada é um ativo que requer proteção. Porém, a mutabilidade e a mobilidade da Internet propiciam aos indivíduos trocas informacionais, eliminando barreiras temporais e espaciais. Neste contexto, as informações fluem livremente, criando também um ambiente propício para corromper a privacidade e alavancar ameaças à segurança de empresas, governos e usuários, mediante a exploração da confiança dos usuários.

Este processo de exploração da confiança dos usuários para obter informações sigilosas ou importantes é conhecido como engenharia social.

Silva (2011) destaca que as organizações possuem informações que geram conhecimento, representando ativos que constituem um diferencial competitivo, assim, dependem de recursos tecnológicos para alavancarem os seus negócios e precisam de um sistema de gerenciamento e apoio nas tomadas de decisões, considerando as informações estratégicas e a necessidade de proteção. O que nos leva a refletir: como uma empresa pode proteger as informações? O usuário faz parte deste processo? Tais temas serão abordados a seguir.

2.2.3 Segurança da Informação – normas e padrões nacionais e internacionais

O desenvolvimento tecnológico afastou a possibilidade de se proteger as informações com o fechamento de armários com cadeados, trancas nas portas, utilização de crachás e instalação de câmeras e alarmes. O uso da tecnologia pode ser desvirtuado e permitir a invasão de organizações por criminosos localizados a milhares de quilômetros de distância.

Com intuito de controlar os riscos relacionados à segurança da informação das informações das empresas, a *International Standardization Organizatios* – ISO, é responsável por desenvolver e publicar normas internacionais.

Silva (2011) ressalta que os incidentes de segurança podem repercutir em consequências negativas para as organizações no que se refere aos seus produtos, imagens ou clientes, quando as vulnerabilidades são exploradas pelos criminosos. Assim, identificar tais vulnerabilidades, sejam elas: físicas (relacionadas à infraestrutura organizacional), técnicas (voltadas aos equipamentos), processuais, (condizentes com as normas, definições e configurações), ou humanas, (fundamentalmente comportamental), e implementar normas e políticas de segurança de natureza preventivas ou corretivas, são balizadores de uma organização conectada e com visão multirreferencial.

As normas internacionais de segurança são aplicadas e adaptadas ao cenário nacional pela a Associação Brasileira de Normas Técnicas – ABNT, que trabalha de acordo com a ISO com intuito de proteger as informações pessoais e sigilosas das pessoas e organizações.

> Por outro lado, compreendem que as normais ISO e ABNT são o resultado de um esforço internacional que consumiu anos de pesquisa e desenvolvimento para se obter um modelo de segurança eficiente e universal. [...] O objetivo fundamental da ISO e da norma brasileira, nela baseada, é assegurar a continuidade e minimizar o dano empresarial prevenido e minimizando o impacto de segurança (CASANAS, MACHADO, 2000).

A ISO 27.001 de 2013 é uma norma internacional e apresenta estratégias gerenciais para assegurar as informações de uma organização. A primeira versão da norma foi publicada em 2005, a partir da norma Britânica BS 7799-2. Esta norma internacional tem como objetivo proteger a confidencialidade, integridade e disponibilidade da informação de uma organização, com intuito de identificar os riscos e tratá-los de forma sistêmica.

A virtualização da informação é, sem dúvida, um processo que modificou a forma da sociedade da informação se organizar, socializar, produzir e desfrutar de serviços ao alcance das pontas dos dedos. Mas,

atrelados às facilitações advindas com o processo de virtualização, vieram os crimes cibernéticos e os furtos ou vazamento de informações sigilosas.

Para criar amarras e controlar as práticas ilícitas, foi promulgado no Brasil, em 14 de julho de 2000, a Lei nº 9.983, para proteção às informações sigilosas do governo, sendo introduzido no Código Penal do Brasil o artigo 313-A, que trata de inserção de dados falsos em sistema de informações, e o 313-B, que dispõe sobre a modificação ou alteração não autorizada de sistemas de informações, tipificando o crime e estabelecendo sanções penais, conforme a seguir:

> Art. 313-A. Inserir ou facilitar, o funcionário autorizado, a inserção de dados falsos, alterar ou excluir indevidamente dados corretos nos sistemas informatizados ou bancos de dados da Administração Pública com o fim de obter vantagem indevida para si ou para outrem ou para causar dano: (Incluído pela Lei nº 9.983, de 2000).
>
> Pena - reclusão, de 2 (dois) a 12 (doze) anos, e multa.
>
> Art. 313-B. Modificar ou alterar, o funcionário, sistema de informações ou programa de informática sem autorização ou solicitação de autoridade competente: (Incluído pela Lei nº 9.983, de 2000).
>
> Pena - detenção, de 3 (três) meses a 2 (dois) anos, e multa (BRASIL, 2000b).

Utilizando da pesquisa realizada por Araújo (2012), sobre as Leis, Decretos e Normas relacionadas a gestão da segurança da Informação nos órgãos da Administração Pública Federal, foram destacados alguns ordenamentos jurídicos nacionais sobre o assunto. Em 28 de junho de 2001, foi homologada a Medida Provisória nº 2.200, com objetivo de instituir a Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil. O Decreto nº 3.505, de 13 de junho de 2000, "institui a Polícia de Segurança da Informação nos órgãos e entidades da Administração Pública". O Decreto nº 4.553, de 27 de dezembro de 2002, "dispõe em salvaguardar dados, informações e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da

Administração Pública Federal", entre outras disposições. O autor descreve que os conteúdos listados em tais ordenamentos jurídicos devem ser observados por todos os órgãos da gestão pública federal.

Para auxiliar ainda mais o processo de proteção à informação, foram organizadas, na esfera nacional brasileira, normas técnicas e padrões voltados às organizações, seguindo disposições internacionais, como por exemplo:

> Atualmente existem algumas metodologias e melhores práticas em segurança da informação e governança para o ambiente de tecnologia, que são reconhecidas mundialmente e largamente utilizadas como, por exemplo, a NBR ISO/IEC 17799:2005 e o CobiT. (FERREIRA; ARAUJO, 2006, p. 27).

A ISO 17799 se refere à segurança da informação como sendo a proteção de informações a partir de uma vasta gama de ameaças, a fim de assegurar a continuidade dos negócios, minimizar os riscos de negócios e maximizar o retorno de investimentos e oportunidades de negócios. Envolve mais de 100 controles voltados a garantia da segurança da informação das empresas, que quando observados pelas mesmas, são certificadas pela ISO, demonstrando à sociedade a preocupação com a segurança da informação, representando um marketing positivo da sua imagem (CASSANAS; MACHADO, 2000).

A Associação Brasileira de Normas Técnicas – ABNT, fundada em 1940, é o órgão responsável pela normalização técnica no país. A norma técnica brasileira relacionada à proteção da informação das organizações, segue as recomendações da ISO e Comissão Eletrotécnica Internacional – IEC - e foi publicada em 2000, sob o número ABNT NBR ISO/IEC 17799. Tal norma foi atualizada em 2005 e em 2007 sofreu atualização da numeração, passando para NBR ISO/IEC 27002. Em 2013 ela foi substituída pela NBR ISO/IEC 27002:2013, que prevê orientações para implementação dos controles listados na ISO 27001.

A NBR ISO/IEC 27002 de 2013 tem como objetivo estabelecer diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização, prevendo diretrizes gerais sobre as metas geralmente aceitas para a gestão de segurança da informação.

As ameaças ou incidentes de segurança no tocante à segurança da informação, segundo a NBR ISO/IEC 27002:2013, incluem as fraudes

eletrônicas, espionagem, sabotagem, vandalismo, incêndio e inundação.

A definição de fraude eletrônica está associada a um golpe, abuso, beneficiamento financeiro. Para Lau (2006), fraude eletrônica está relacionada ao emprego de qualquer tipo de golpe, por intermédio de serviços disponíveis na internet, mediante a persuasão de potenciais vítimas, com intuito de realizar transações fraudulentas em benefício de um indivíduo ou grupo de pessoas. Uma visão análoga é de Kovach (2011), que a define como qualquer acesso ou transação não autorizados, realizados em conta-corrente, cujo canal é a internet.

A partir de tais definições, serão consideradas como fraude eletrônica, para efeitos dessa pesquisa, toda ação ou omissão que permita a realização de um golpe, por meio de ataque direto ou por canais alternativos, como a internet - *Internet Banking*, caixas eletrônicos e centrais de atendimento das Instituições Bancárias.

Como medida educativa, o Comitê Gestor da Internet no Brasil – CGI.br, desenvolve serviços e orientações à sociedade em geral, relacionados à segurança da informação e disponibiliza em seu portal uma cartilha de segurança, que enumera os riscos presentes na internet.

Em resposta a resistência social ao AI-5 Digital, denominação esta, dada ao projeto de lei de cibercrimes, de autoria do Deputado Federal, Eduardo Azeredo, se iniciaram as primeiras discussões sobre o projeto do Marco Civil da Internet, com intuito de garantir a neutralidade e a função social da rede, a privacidade, além, da garantia de liberdade de expressão e transmissão do conhecimento, impondo direitos e obrigações aos provedores e usuários. Os internautas equipararam a Lei Azeredo ao AI-5, fazendo uma alusão ao ato que reduziu as liberdades individuais na ditadura militar. Foi organizado pelos internautas um abaixo assinado com 350 mil assinaturas repudiando a proposta, considerada uma ameaça aos direitos e liberdade na internet, por propor a guarda de dados de conexão dos usuários pelos provedores e criminalizar a obtenção, transferência ou fornecimento não autorizado de dado ou informação, dentre outros.

Em 23 de abril de 2014 foi aprovada no Brasil, a Lei n. 12.965, que descreve sobre o Marco Civil da Internet, estabelecendo princípios, garantias, direitos e deveres para internautas e provedores de internet, garantindo a cidadania. Tal iniciativa, destacou o Brasil na governança global da internet, por ter sido a primeira proposta no mundo, uma espécie de “constituição da internet”.

> [...] com a aprovação do texto do Marco Civil, o Brasil consolida a sua reputação como líder da democracia e ajuda a inaugurar uma nova era, na qual os direitos dos cidadãos do mundo serão protegidos por Constituições digitais. (LIMA, 2014).

Em fevereiro de 2016, segundo site "Portal Brasil" oficial do Governo, foi encerrada a consulta pública para discussão da minuta do decreto para regulamentação do Marco Civil da Internet. Tal documento foi dividido em quatro capítulos e disponibilizada na página <www.marcocivil.mj.gov.br> para que, qualquer interessado, pudesse contribuir na elaboração da redação e do conteúdo (PORTAL BRASIL, 2016).

Em 11 de maio de 2016, foi publicado pela presidenta do Brasil, Dilma Rousseff o Decreto 8.771, com intuito de regulamentar o Marco Civil da Internet:

> Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações.

A Comissão Parlamentar de Inquérito - CPI dos Crimes Cibernéticos, segundo o site da Câmara de Deputados Federal, foi criada por ato da presidência da Câmara dos Deputados Federais, em 17 de julho de 2015, com a premissa de investigar a prática de crimes cibernéticos e seus efeitos nocivos à economia e a sociedade brasileira, considerando os números alarmantes envolvendo fraudes na Internet divulgados pelo Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil.

Em 04 de maio de 2016, após nove meses de discussão com a realização de mais de 50 audiências públicas, a CPI dos Crimes Cibernéticos aprovou o relatório final do projeto de lei que autoriza os magistrados determinarem o bloqueio de *sites* e aplicativos, hospedados

fora do País ou sem representação nacional, votados à prática criminosa, puníveis com pena mínima de dois anos de reclusão, exceto os crimes contra honra, no qual fica proibido o bloqueio. A pirataria, ou seja, os crimes contra os direitos autorais, tráfico e pornografia infantil são exemplos de tais práticas criminosas sujeitas ao bloqueio. Porém, tal medida poderá repercutir na violação da neutralidade da rede prevista no Marco Civil da Internet, que estabelece a transmissão de qualquer conteúdo enviado pela internet com igual velocidade e condições técnicas.

Como resultado do relatório final da CPI dos Crimes Cibernéticos foram propostos mais cinco projetos de lei relacionados ao assunto. Um dos projetos prevê a criminalização da invasão de qualquer sistema informatizado, com ou sem vantagem pessoal. No atual cenário jurídico nacional, o Código Penal, criminaliza tal prática somente se for comprovado o objetivo de obter, adulterar ou destruir dado ou informações sem autorização do dono do dispositivo.

Um outro projeto visa modificar o Marco Civil da Internet, obrigando quaisquer serviços de internet a retirar em até 48 horas, sem uma nova decisão judicial, imagens, vídeos e quaisquer conteúdos iguais ou semelhantes àqueles que já tiveram a exclusão determinada pela Justiça.

Há uma proposta distinta, que tem como premissa, alterar a Lei nº 12.737, de 2012, conhecida como "Lei Carolina Dieckmann", punindo aquele que invada computadores com a intenção de obter dados particulares, ampliando e transformando em crime o acesso não permitido a qualquer sistema informatizado ou aparelho eletrônico que cause prejuízo econômico, alteração de dados, instalação de vulnerabilidades, obtenção de conteúdo ou o controle remoto da plataforma ou aparelho em questão. A lei atual descreve de forma genérica os atos puníveis.

Foi sugerido também, proposta da criação de lei que destine 10% dos recursos do Fundo de Fiscalização das Telecomunicações – Fistel, advindos de taxas de fiscalização cobradas pela Agência Nacional de Telecomunicações – ANATEL, de parte de valores pagos por empresas que desejam operar no Brasil e de multas aplicadas pela agência. Tais recursos estariam voltados ao aparelhamento do judiciário para combater o crime cibernético.

Como resultado final da CPI dos Crimes Cibernéticos os deputados sugeriram que a Polícia Federal seria a entidade competente para conduzir os processos de investigação dos crimes praticados por meio de um computador, assim, aqueles que se utilizem de senha de outro para acesso às redes sociais, seriam investigados pela Polícia Federal.

A inclusão de multa culminada com prisão para aqueles que cometem crimes cibernéticos também foi proposta, permitindo que o Estado confisque os seus valores e bens.

Tais projetos de lei serão submetidos à análise e parecer do Senado e Câmara Federal.

Porém, a regulamentação do ciberespaço provoca uma série de discursos entre os diversos atores políticos, por envolver aspectos relacionados a garantia das liberdades individuais e coletivas, a privacidade e a possibilidade de controle.

Para Wolton (2003), não há liberdade de comunicação sem regulamentação, no sentido de estabelecer mecanismos de proteção de tal liberdade. A ausência de regulamentação para o uso da internet sustenta a lógica do mercado e das relações econômicas, o que poderá acarretar em censura.

No âmbito da segurança da informação, a regulamentação por si só, não é suficiente para sua garantia. Para a efetividade da gestão da segurança da informação é necessária a interação entre as organizações, as pessoas, os processos e as tecnologias. O comportamento do indivíduo passa a ter uma relação direta com a segurança da informação, pois este é detentor de grande parte dos ativos valorados. O gerenciamento de um cenário de risco depende do saber agir do indivíduo, ou seja, da sua proatividade face ao cenário de risco apresentado.

2.3 ENGENHARIA SOCIAL

Será apresentado a seguir o conceito de engenharia social, o perfil de quem a pratica, as ferramentas, o fluxo e as técnicas relacionadas à engenharia social.

2.3.1 Engenharia social – abordagem conceitual

A engenharia social é utilizada para ameaçar a integridade informacional e precede aos cibercrimes. Corresponde às práticas utilizadas para se obter informações sigilosas ou importantes de empresas, pessoas e sistemas de informações, explorando o comportamento e a confiança dos indivíduos.

> Engenharia social é a ciência que estuda como o conhecimento do comportamento humano pode ser utilizado para induzir uma pessoa a atuar segundo seu desejo. Não se trata de hipnose ou controle da mente, as técnicas de engenharia social são amplamente utilizadas por detetives (para obter informação) e magistrados (para comprovar se um declarante fala a verdade). Também é utilizada para lograr todo o tipo de fraudes, inclusive invasão de sistemas eletrônicos (PEIXOTO, 2006, p. 4).

A disjunção dos termos "engenharia social" nos leva a um conceito literal, no qual, o termo "engenharia" aparece no sentido de construção e "social" por envolver pessoas, forças externas ao indivíduo situado em um determinado ambiente. A construção está interligada ao desenvolvimento de táticas que permitam o acesso à informação não disponível naturalmente, mediante a exploração de vulnerabilidades das pessoas, relacionadas as suas características comportamentais (BRAGA, 2011). Portanto, a engenharia social não corresponde diretamente a uma ação ou omissão que envolva somente o meio digital, o seu cerne está na exploração direta do comportamento do indivíduo.

Silva (2011) compilou, através de uma revisão de literatura dos artigos presentes na internet, algumas definições relacionadas ao termo engenharia social:

Quadro 2: Definições Engenharia Social

ENGENHARIA SOCIAL
Arte de fazer com que outras pessoas concordem com você e atendam aos seus pedidos ou desejos, mesmo que você não tenha autoridade para tal;
Termo utilizado para se obter informações importantes de uma empresa, por intermédio de seus usuários e colaboradores;
Aquisição de informações ou privilégio de acesso por “alguém de fora”, baseado em uma relação de confiança estabelecida, inapropriadamente, com “alguém de dentro”;
Técnicas utilizadas para tirar proveito de falhas que as pessoas cometem ou que sejam levadas a cometer com relação às informações da área de tecnologia da informação;
Técnica de influenciar as pessoas pelo poder da persuasão com objetivo de conseguir que elas façam alguma coisa ou forneçam determinada informação a pedido de alguém não autorizado;
Método de ataque virtual no qual é aproveitada a confiança ou a ingenuidade do usuário para obter informações que permitem invadir um micro;
Habilidade de um hacker manipular a tendência natural de confiança com o objetivo de obter informações por meio de um acesso válido em um sistema não autorizado;
Arte e ciência de persuadir as pessoas a atenderem aos seus desejos; e
Garimpagem das informações.

Fonte: elaborado pela autora com base em Silva (2011).

A engenharia social é composta por ações que venham a ameaçar comunidades virtuais e atacar os sistemas de informação, aproveitando da diminuição da interação pessoal, considerando a utilização massificada de ferramentas computacionais para comunicação pessoal e

profissional, como por exemplo, e-mail, *Twitter*, *Facebook*, sem dar importância a segurança e privacidade (KROMBHOLZ, et al. 2014).

> Engenharia social é a arte de levar os usuários a comprometer os sistemas de informação. Em vez de utilizar técnicas sobre os sistemas, os alvos dos engenheiros sociais são os humanos com o acesso a informação, manipulando-os para divulgar informações confidenciais ou até mesmo realizar ataques maliciosos sob sua influência e persuasão. (KROMBHOLZ, et al, 2014, **tradução nossa**)

Tais conceitos foram resumidos pelo Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil (CERT, 2012, p. 115), como sendo "[...] uma técnica por meio da qual uma pessoa procura persuadir outra a executar determinadas ações", sejam elas no sentido de proteger a informação ou explorá-las, identificando as vulnerabilidades, ameaças e impactos, de sistemas informacionais de organizações empresariais ou informações particulares.

A engenharia social é definida como o uso de técnicas sociais de disfarces, manobras culturais e truques psicológicos para obter dos usuários de computadores ajuda na invasão ilegal ou uso de sistemas de computadores e redes sem autorização (ERBSCHLOE, 2004). É uma técnica antiga de se obter vantagens e informações para cometimento de ilícitos, que faz com que o indivíduo concorde em atender aos anseios de um terceiro, mesmo este não tendo autoridade para tal. A primeira prática da engenharia social na história da humanidade foi na passagem bíblica que descreveu Adão e Eva sendo persuadidos pela serpente para provarem o fruto proibido. Nesta passagem histórica, a serpente faz o papel do engenheiro social (PEIXOTO, 2006, p. 3).

Os conceitos ora relacionados estão alicerçados no princípio da investigação informacional, com intuito de obter acesso negado naturalmente, através da especulação da ingenuidade, confiança ou sinceridade das pessoas, visto que:

> A engenharia social atua sobre a inclinação natural das pessoas de confiar umas nas outras e de querer ajudar. Nem sempre a intenção precisa ser de ajuda ou de confiança; pelo contrário, pode ser por senso de curiosidade, desafio, vingança,

> insatisfação, diversão, descuido, destruição, entre outros. [...] Há ainda um grupo de pessoas ao qual é necessário dispensar uma atenção especial, porque não entra no contato físico com a empresa, mas por meio de telefone, fax ou correio eletrônico (KLEIN, 2004, p. 9).

Um estudo conjectural da engenharia social nos leva a observar que está diretamente relacionada às ciências humanas e sociais, das quais podemos citar a filosofia, psicologia, economia, por estarem intimamente relacionadas com as teorias do comportamento das pessoas e dos seus reflexos para sociedade. Neste contexto, Hadnagy (2014), complementa que a engenharia social é técnica direcionada a manipular as pessoas para as induzirem a realizar atos que no seu cotidiano não realizariam, explorando a vulnerabilidade humana, conceito este inserido no contexto de estudo das Ciências Humanas.

2.3.2 Engenheiro social – perfil e atuação

Segundo Rosa et. al. (2011), para que seja praticada a engenharia social, são necessários conhecimentos empíricos e científicos socialmente aceitáveis e agradáveis, considerando as necessidades humanas para obter uma informação, seja ela um dado pessoal ou de contas bancárias, por exemplo. Desta forma, pode-se observar que:

> A engenharia social passa muitas vezes despercebida por muitas pessoas, pois as vítimas adquirem confiança pelo "agressor" e assim se tornam alvo fácil de ser manipulado e enganado por ele. O "agressor" finge ser funcionário motivado e amigo que estuda a empresa e pessoas percebendo onde estas não estão realmente capacitadas e que possam a lhe fornecer informações importantes causando-lhes danos financeiros (ROSA, et al., 2011, p. 31)

O engenheiro social mais famoso dos últimos tempos, Kevin Mitnick, foi o hacker responsável pela popularização do termo engenharia social na década de noventa do século passado. Aos dezessete anos de idade, Mitnick se transformou em "celebridade" após invadir o sistema do Comando de Defesa Aérea dos Estados Unidos.

Depois de ser preso pela *Federal Bureau of Investigation* – FBI, em 1993, e ficar oito anos sob custódia dos Estados Unidos, o hacker fundou uma empresa de consultoria relacionada à segurança da informação e foi autor do livro "A Arte de Enganar e a Arte de Invadir", no qual, descreve as formas de abordagem de um engenheiro social frente à sua vítima (MITNICK, 2003).

Conforme Mitnick (2003), o perfil de um engenheiro social é formado pela tendência da personalidade de enganar as pessoas, popularmente conhecido como "mal caráter", aliados a fatores como influência e convencimento, visto que nem mesmo a tecnologia é suficiente para detê-los.

Desta forma, o engenheiro social não está atrelado a uma formação específica, pois as suas ações são dotadas de características que podem ser desenvolvidas por qualquer pessoa, dependendo apenas do *animus furandi*, do latim vontade de roubar.

Os engenheiros sociais atuam na sociedade da informação, fazendo parte dos atores sociais, e se utilizam dos avanços tecnológicos para mapear os padrões de comportamento dos usuários com dois objetivos específicos e distintos. O primeiro objetivo está voltado para o desenvolvimento e aperfeiçoamento de sistemas e produtos que auxiliem os usuários no processo de recuperação da informação, melhorando o desempenho dos sistemas tecnológicos e informacionais. Neste caso, os engenheiros sociais são conhecidos como *hackers*. O segundo objetivo tem como premissa recuperar informações sigilosas e importantes de empresas, usuários e corporações para a execução de atividades ilícitas. Sob este escopo, os engenheiros sociais são denominados de *crackers*.

Segundo Levy (1994) há três gerações de *hackers*. A primeira nasceu em Massachusetts, na década de 1950, cujo principal legado foi o aprimoramento de programas de computadores. A sociedade neste período ainda não estava conectada em rede de forma massificada e tais aprimoramentos foram fundamentais para a criação do ciberespaço, com a premissa básica de que toda informação devesse ser livre.

Na década de 1970, marcada pela democratização da informática e a crítica do monopólio da IBM, surgiu a segunda geração de *hackers* que levantam a bandeira do acesso universal à informática de forma gratuita e democrática. A terceira geração de *hackers* apareceu em meados da década de 1980, formada por programadores responsáveis

pelo desenvolvimento de jogos para computador. Neste período, o termo *cracker* passa a ser utilizado para designar alguém que utiliza os seus conhecimentos tecnológicos para a prática de atividades criminosas. (LEVY, 1994).

Silva (2011, p.20) elucida que os engenheiros sociais, embora sejam classificados como criminosos eletrônicos, podem apresentar-se somente como captores e receptores da informação, cuja infração se resume em repassar a informação restrita de acesso. O autor descreve uma classificação dos *hackers*, considerando o grau do dano provocado a vítima, assim sendo:

> - Os *Hackers* ou "*White hat*" – aqueles que após detectarem uma falha na segurança e invadirem uma organização deixam um alerta para que a incorreção seja eliminada. Praticamente fazem a invasão pela satisfação de vencer o desafio de superar as barreiras existentes.
>
> - Os *Crackers* ou "*Black hat*" – aqueles que possuem praticamente o mesmo nível de conhecimento do tipo anterior, mas diferem dele pelos objetivos realmente criminosos, causando qualquer espécie de prejuízo ao invadido e, se possível, obtendo lucro pessoal.
>
> - Os *Phreakers* – aqueles que, essencialmente, manipulam equipamentos e sistemas de telecomunicações para conseguirem as informações desejadas (SILVA, 2011, p.20)

A engenharia social, portanto, pode ser aplicada pelos *hackers* (pessoas que invadem os sistemas de computadores sem interesses financeiros), como pelos *crackers* (indivíduos que invadem os sistemas para destruir, roubar dinheiro, senhas ou informações), mediante a identificação prévia das vulnerabilidades relacionadas às pessoas e ao ambiente que irá atuar (SILVA; ARAÚJO; AZEVEDO, 2013).

Para Mitnick (2003), os engenheiros sociais exploram o comportamento do indivíduo, cujos principais fatores de vulnerabilidades e de manipulação são: a vontade de se tornar útil, a busca por amizades, a divisão de responsabilidades e a persuasão que é caracterizada pela capacidade de convencer, buscando assim a resposta auferida. A atuação dos engenheiros sociais pode ser de forma direta ou

indireta. Na atuação de forma direta há um contato com a vítima, utilizando o telefone ou contato pessoal. Esta técnica exige um maior preparo do engenheiro, pois é necessário planejamento detalhado da forma de abordagem. A abordagem indireta é realizada através de recursos tecnológicos, com a invasão de computadores por meio de softwares espúrios.

O sucesso da engenharia social está associado diretamente ao comportamento do indivíduo, sendo este o autor ou a vítima. O autor no sentido de convencer a vítima em lhe entregar as informações que deseja e a vítima no sentido de se deixar ser induzida (MENDES, 2004).

2.3.3 Engenharia social – ferramentas e fluxo

O ferramental de um engenheiro social inclui telefonemas, internet, e-mail, *chat*, correspondências, *spyware*, observação pessoal, procura no lixo e intervenção pessoal direta (SILVA, 2011). Para tanto, o que se percebe é que a engenharia social pode ser utilizada na informática, mas basicamente explora as falhas humanas, pois, para Artigonal (2010), as informações não documentadas, aquelas de foro íntimo, estão amparadas em características comportamentais e psicológicas, que quando atreladas às técnicas como a leitura e linguagem corporal, podem ser exploradas e desvendadas.

Desta forma, a engenharia social se utiliza de ferramentas para explorar as falhas, sejam das organizações, como das pessoas, portanto, pode ser utilizada em diversas áreas. De posse das informações relevantes, os engenheiros sociais,

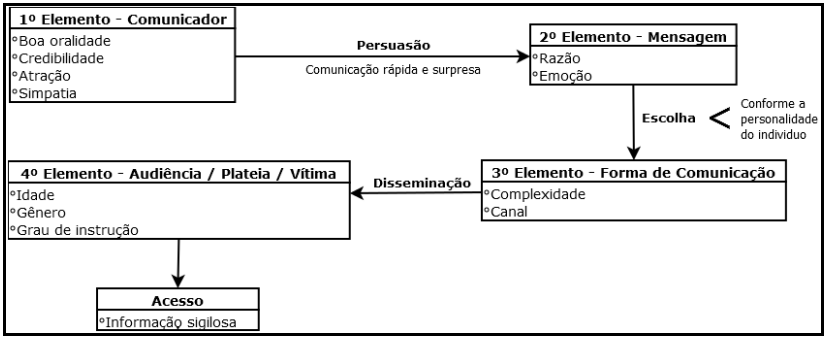
> [...] interagem com partes ou todo o sistema, seja ele físico ou virtual [...] e apesar da lei brasileira ainda ser imatura no aspecto tecnológico e da Ciência da Informação, um ataque de engenharia social, dependendo da motivação ou objetivo, pode ser tipificado no artigo 171 do código Penal Brasileiro, que diz que "Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento", incide em crime de estelionato, prevendo como pena, reclusão, de um a cinco

> anos, e multa (ROSA; SILVA; SILVA, 2012, p. 10).

A interação entre as partes somada a evolução da humanidade estão interligadas diretamente ao aumento da disponibilidade da informação que, manipulada por pessoas não autorizadas, denominadas de engenheiros sociais, compromete a sua confidencialidade, integridade e disponibilidade.

Nesse contexto, a manipulação ou persuasão são constituídas por quatro elementos responsáveis pela formação do fluxo na obtenção de uma informação sigilosa. O comunicador é o primeiro elemento, constituído por uma boa oralidade, transmitindo credibilidade em virtude de uma formação especializada e fidedigna, aliadas da atratividade e simpatia. A comunicação rápida e surpresa são instrumentos auxiliadores da persuasão. A mensagem representa o segundo elemento, que está relacionada com a razão e a emoção do persuadido, cuja predominância de um ou de outro vai depender das características pessoais. Em seguida, o terceiro elemento, a forma de comunicação interligada diretamente à combinação da complexidade e o canal escolhido para disseminá-la. Para encerrar, o quarto elemento é a audiência, formada pela idade, gênero e inteligência (SILVA, 2011).

Ilustração 3: Diagrama – Elementos da captura da informação sigilosa



Fonte: elaborado pela autora com base em Silva (2011).

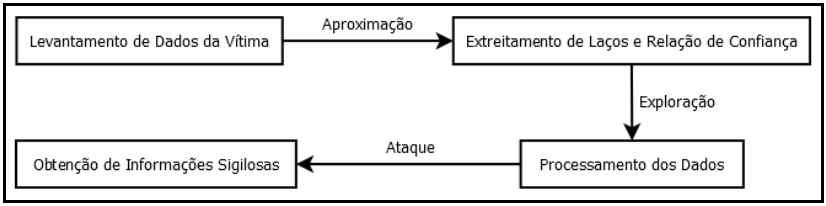
Os aspectos motivadores para se utilizar da engenharia social são ganhos financeiros, vantagens competitivas e a vingança. O primeiro deles, os ganhos financeiros, serão mais explorados pela presente pesquisa, com foco na manipulação do indivíduo, detentor de conta

corrente em uma Instituição Bancária, cuja ação praticada pelo engenheiro social lhe traz prejuízos financeiros. Já as vantagens competitivas e a vingança são subterfúgios vinculados, na maioria das vezes, às organizações empresariais e seus profissionais, não fazendo parte do escopo deste trabalho.

O engenheiro social manipula sentimentos, emoções e aspirações das pessoas para obter as informações desejadas, que em procedimentos normais, se perguntado diretamente ao detentor da informação, este não a revelaria, o que pode ser constatado como uma falha de interpretação do próprio cérebro humano. O sucesso da engenharia social e da persuasão está relacionado à forma de comunicação e de convencimento, que na maioria das vezes seguem técnicas relacionadas ao processo de comunicação, balizadas pelo uso de elogios, parcerias, argumentos bem fundamentados, determinação (PHUN, 2005). O emprego de tais técnicas leva a interpretações errôneas e o comprometimento da segurança da informação.

O fluxo de atuação dos engenheiros sociais, conforme Lennert e Oliveira (2011), pode ser resumido em quatro etapas distintas. A primeira consiste em reunir os dados sobre as vítimas, perfis e vulnerabilidades relacionadas a elas e ao ambiente no qual estão inseridas. Na segunda etapa, o engenheiro social se aproxima da vítima para estreitar laços, aflorando um sentimento de confiança. Em seguida, os dados obtidos sobre a vítima e o canal de atuação passam a ser explorados e por fim, na quarta etapa, o ataque é executado e as informações sigilosas são obtidas.

Ilustração 4: Diagrama - Etapas para se obter informação sigilosa



Fonte: elaborado pela autora com base em Lennert e Oliveira (2011)

Um exemplo da violação de dados sigilosos foi divulgado pela empresa de segurança *Check Point*, em 2011, que realizou entrevista com 850 profissionais da área de tecnologia da informação, dos quais

48% foram vítimas de engenharia social, com um prejuízo de 25.000 à 100.000 dólares por incidente. Conforme o relatório da pesquisa, as vítimas da engenharia social são as pessoas que detêm um conhecimento implícito ou possuem acesso às informações sigilosas. A pesquisa demonstrou que a violação das informações sigilosas está fundamentada basicamente em duas técnicas utilizadas pela engenharia social, os e-mails de *phishing*, representando 47% dos incidentes, e as redes sociais, que alcançaram 39% (GOODCHILD, 2012).

2.3.4 As técnicas da engenharia social

Os ataques com a utilização da engenharia social envolvem várias facetas que incluem aspectos físicos, sociais e técnicos, utilizados nas diferentes fases do ataque propriamente dito.

Na abordagem física, o engenheiro social, realiza uma ação, com intuito de obter informações pessoais e profissionais sobre a vítima, procurando por exemplo, nos lixos domésticos e da empresa, para prática de furto ou extorsão.

A abordagem social é utilizada pelo engenheiro social como forma de persuasão para manipular a vítima, cujos métodos podem envolver o uso de uma suposta autoridade, a curiosidade e a confiança, também conhecido como ataque direto.

As abordagens físicas e sociais requerem uma ação direta do engenheiro social, na busca de informação, enquanto que a abordagem técnica, a ação do engenheiro social está voltada ao uso da internet, reunindo informações a partir de diferentes recursos da *Web*. (KROMBHOLZ, 2014).

A engenharia social pode ser processada em três categorias: canal, operador e tipo (KROMBHOLZ, 2014). O canal engloba, o e-mail e aplicativos de mensagens, além do telefonemas e redes sociais para entrega de informações sensíveis. A categoria operador é representada pelo humano - limitando o número de alvo; se o ataque está voltado para uma única pessoa – software – permite a automação do ataque. A categoria tipo está relacionada a forma de atuação do engenheiro social, seja por meio de envio de mensagens falsas, pela busca de informações no lixo doméstico ou ainda pela observação e abordagem direta da vítima.

Ampliando as formas de obtenção de informações sigilosas, as principais técnicas utilizadas pela engenharia social são: o furto de identidade, a antecipação de recursos, códigos maliciosos, *phishing*, golpes do comércio eletrônico, boatos, análise do lixo, contato telefônico e abordagem pessoal, cujas características serão reportadas em seguida (LAUDON, 2010).

2.3.4.1 Furto de Identidade

O furto de identidade, ocorre quando engenheiro social se passa por outra pessoa, atribuindo-lhe falsa identidade com intuito de obter vantagens indevidas (SÊMOLA, 2014). O furto pode ser de documento físico de identificação da pessoa ou de dados presentes em redes sociais. No primeiro caso, o engenheiro social, de posse do documento furtado, pode realizar vários golpes, como a abertura de uma conta corrente em uma Instituição Bancária. Já no segundo evento, o engenheiro social pode criar perfil falso em redes sociais utilizando os dados disponíveis na rede (LAU, 2006).

2.3.4.2 Fraude de antecipação de recursos

Nessa técnica, o indivíduo é induzido pelo engenheiro social a fornecer informações confidenciais ou realizar um pagamento adiantado, com a promessa de recebimento futuro de algum benefício. A fraude pode ocorrer por recebimento de mensagens eletrônicas e/ou acesso a *sites* fraudulentos. A fraude de antecipação de recursos apresenta uma série de variações, das quais se destacam o golpe do bilhete premiado, cujo valor total de uma loteria somente será repassado mediante depósito de um valor bem menor do sorteado, ou *e-mail's* solicitando informações de dados pessoais e bancários para liberar o recurso (CHAWKI, 2009).

2.3.4.3 Códigos maliciosos *(Malware)*

Os códigos maliciosos são programas desenvolvidos para danificar o computador ou permitir atividades maliciosas com intuito de obter vantagens financeiras, coletar informações confidenciais, se autopromover ou cometer vandalismo (LAUDON, 2010). O *e-mail* é a

forma mais popular usada pelos engenheiros sociais para enganar os usuários, levando-os a violar a política da segurança da informação ao acessarem *links* contendo os códigos maliciosos. São instalados de forma automatizada no computador do usuário, que é atraído pela curiosidade (ABRAHAM; SMITH, 2010, p. 3). Além do *e-mail*, os códigos maliciosos podem ser instalados nos computadores com o emprego da engenharia social por intermédio de mídias removíveis (CD, DVD, *pen-drives*), recebidas pelos usuários que, curiosos, os executam nos computadores. A instalação de um *malware* pela engenharia social depende de uma facilitação do usuário que, de alguma forma, os instala em seu computador.

Fazem parte dos códigos maliciosos diversas formas de ameaças, tais como (LAUDON, 2010):

- Vírus: é um programa de software espúrio, que se anexa a outros programas ou arquivos de dados, com intuito de ser executado, sem o conhecimento ou permissão do usuário. O vírus é utilizado para destruir programas ou dados, entupir a memória do computador, reformatar o disco rígido ou fazer com que programas funcionem de maneira imprópria;

- *WORM*: é um programa que se propaga pela execução direta de suas cópias, enviando cópias de si mesmo de um computador para o outro, de forma automática, diferentemente dos vírus, podem funcionar isoladamente, sem a necessidade de anexar a outros arquivos de programas. São utilizados para destruir dados ou programas e ainda, interromper o funcionamento de redes de computadores;

- *BOT e Botnet*: é um código que permite estabelecer uma comunicação entre computadores, sendo que um deles é controlado a distância, cuja propagação é similar aos *worm*. *Botnet* é uma rede formada por milhares de computadores zumbis e que potencializa as ações danosas dos *bots*;

- *Spyware*: é um *malware* que monitora as atividades de um sistema e envia as informações coletadas para terceiros e pode ser utilizado de forma legítima ou maliciosa. Neste último caso pode comprometer a privacidade do usuário e a segurança do computador;

- Cavalo de Troia *(Trojan)*: é um programa que executa funções legítimas e maliciosas, neste caso, sem consentimento do usuário, atuando como intermediador entre outro *malware*. O Cavalo de Troia contamina os computadores através do uso de disfarces de programas legítimos, atuando como uma armadilha, abrindo as portas para

instalação de outro *malware*.com objetivo de invadir sistemas ou furtar senhas dos usuários.

2.3.4.4 *Phishing*

A engenharia social utiliza o *phishing* para obter informações sigilosas, pelo o envio de mensagens através de correio eletrônico, conhecidos como *spam*, similares aos das Instituições Bancárias. Os correntistas são condicionados a repassar dados confidenciais, como número de cartões, documentos e senhas. O correntista confiante de que se tratava de um ambiente virtual seguro, não percebe a manipulação por ter estabelecido previamente, uma relação de confiança com o canal escolhido para realizar as suas transações financeiras (LAUDON, 2010).

Essa mesma concepção é descrita por Lennert e Oliveira (2011), que descrevem o *phishing* como uma das principais técnicas utilizadas pelos engenheiros sociais, na qual combina engenharia social com recursos tecnológicos. Esse processo permite a instalação de códigos maliciosos projetados para coletar informações sensíveis do computador do usuário.

> *Phishing* é uma ameaça amplamente espalhada na internet e consiste na tentativa do atacante atrair as vítimas e entregar informações sensíveis como senhas ou número de cartões de crédito em um site falsificado que é controlado pelo atacante. (KROMBHOLZ et al., 2014, **tradução nossa**).

Em suma, é um golpe *on-line* caracterizado pela falsificação, cujos criadores são especializados em tecnologia com objetivo de furtar informações, se passando por clones de empresas renomadas, bancos, entre outros (ROSA, et al., 2011).

A disponibilidade de informação pessoal em *sites* de redes sociais, como *Facebook*, *MySpace* e *Linkedin*, aumenta a vulnerabilidade das vítimas e da taxa de sucesso de *phishing* (ABRAHAM; SMITH, 2010).

2.3.4.5 Golpes de comércio eletrônico

Nesta técnica o engenheiro social explora a relação de confiança entre as partes envolvidas em uma transação comercial, mediante a

criação de um site fraudulento para compras coletivas, leilão e venda de produtos, muitas vezes com valores inferiores ao praticado pelo mercado, e o indivíduo ao realizar a compra não recebe a mercadoria (LAU, 2006 e LAUDON, 2010).

2.3.4.6 Boato

O boato é uma mensagem composta por um conteúdo alarmante ou falso que remete a autoria a uma pessoa ou instituição renomada, podendo conter códigos maliciosos, espalha desinformação pela internet, compromete a credibilidade e a reputação de uma pessoa ou instituição (LAU, 2006).

2.3.4.7 Análise do lixo

Segundo a Sêmola (2014), o lixo pode ser uma fonte de informação rica para os engenheiros sociais, para obterem nome de funcionários, telefones, e-mail, senhas, contatos de clientes, fornecedores e transações realizadas.

2.3.4.8 Contato telefônico

O contato telefônico ocorre após a obtenção de informações originadas da análise do lixo, da internet ou redes sociais. Assim, o engenheiro social possui o ferramental necessário para realizar uma abordagem via telefonema, com intuito de obter acesso não autorizado, se passando por um funcionário de empresa, fornecedores ou terceiros, estabelecendo um vínculo de confiança com a vítima (LAU, 2006).

2.3.4.9 Abordagem pessoal

Mediante contato direto e utilizando da persuasão, os engenheiros sociais conseguem convencer a vítima a entregar a informação valorada. Nas Instituições Bancárias, os correntistas são vítimas dos engenheiros sociais em várias modalidades de golpes, como a troca de cartão, precedida de observação de senha, retenção de cartão e indicação de central de atendimento falsa para obter a senha, falso sequestro de familiar mediante solicitação de resgate, entre outros, que serão

abordados com mais detalhes posteriormente (SILVA; ARAÚJO; AZEVEDO, 2013).

2.3.5 Aspectos comuns às técnicas da engenharia social

A característica peculiar das ameaças à segurança da informação pela engenharia social é uma ação prévia do usuário. Os engenheiros sociais, de posse do padrão de comportamento dos usuários e suas características, as exploram para obterem vantagens que não lhes são devidas, visto que,

> As pessoas são consideradas um elo frágil nos sistemas de segurança da informação, seja ele físico ou virtual, sendo necessário a valorização de políticas de segurança da informação e treinamentos nos ambientes intraorganizacional e domésticos para sensibilização e conscientização das vulnerabilidades e ameaças existentes por meio da atuação da engenharia social [...] (SILVA; ARAÚJO; AZEVEDO, 2013, p. 45).

A engenharia social funciona através da manipulação de emoções tais como medo, curiosidade, entusiasmo, empatia e ganância, ou através da exploração dos vieses cognitivos, táticas estas de persuasão elencadas por Abraham e Smith (2010, p.5). A primeira etapa da engenharia social é convencer um usuário a ativar *malwares* acessando *e-mails* maliciosos ou *links*, utilizando das táticas de persuasão. Em seguida entra em ação a tecnologia, com a instalação de programas maliciosos destinados a captura de informações negadas naturalmente.

As pessoas, na sua grande maioria, não distinguem o valor das informações por elas divulgadas e o embate caso sejam utilizadas de forma lasciva. E há ainda, aquelas que acreditam reconhecerem e inibirem a ação de um engenheiro social, porém, cabe destacar, que este é manipulador, cuja abordagem explora a vulnerabilidade humana, como o afeto, sobrecargas, reciprocidade, difusão de responsabilidade, dever moral, integridade, autoridade e relações enganosas (MOUTON, 2015).

A engenharia social está intimamente relacionada à interferência humana com o emprego de técnicas para obter informações controladas e essenciais. A simulação de uma relação de amizade entre o engenheiro

e a vítima facilita a obtenção de informações, cuja simulação é de difícil percepção, pois não é da condição humana suspeitar de pessoas vistas como amigas ou que tenham previamente estabelecido uma relação de confiança.

3 AS INSTITUIÇÕES BANCÁRIAS E ORIENTAÇÕES GERAIS AOS USUÁRIOS RELACIONADAS À SEGURANÇA DA INFORMAÇÃO

Neste capítulo é descrito sobre o fluxo informacional nas Instituições Bancárias, as transações financeiras e os incidentes de segurança.

3.1 AS INSTITUIÇÕES BANCÁRIAS E O FLUXO INFORMACIONAL

O Sistema Financeiro Nacional é composto por um conjunto de órgãos regulamentadores, fiscalizadores e executores das operações necessárias à circulação da moeda e do crédito na economia brasileira. As instituições bancárias estão classificadas como órgãos operadores do Sistema Financeiro Nacional, cuja atuação está voltada para operacionalização das transferências de recursos envolvendo os fornecedores de fundos e os chamados tomadores de recursos, considerando as regras, diretrizes e parâmetros normatizados (FEBRABAN, 2013).

As Instituições Bancárias, acompanhando a tendência de informatização dos serviços, investem em canais alternativos de atendimento aos seus correntistas, proporcionando-lhes comodidade, praticidade, redução dos custos e segurança. Exemplo desta tendência são as salas de autoatendimento, dotadas de terminais, *internet banking*, centrais de atendimento, aplicativos para *smartphones*, que permitem a execução de várias transações financeiras sem a intervenção de terceiros.

> Hoje, a maioria dos bancos tradicionais usam a tecnologia da internet para oferecer serviços bancários aos seus clientes. Como resultado, os consumidores podem acessar suas contas, realizar transferências, visualizar declarações, pagar contas, e realizar outras transações bancárias eletronicamente através do site do banco a qualquer hora e em qualquer lugar (YOON, STEEGE, 2013, p. 1133, **tradução nossa**).

No entanto, a disponibilização de canais alternativos, tendo como pressupostos a tecnologia, repercute no aumento de ameaças e os riscos envoltos à informação, que transmutam do mundo real para o virtual.

O ciberespaço está sofrendo com a atuação acirrada dos *crackers* e o Brasil está entre os principais países alvos de ataques, ocupando o quarto lugar, conforme última pesquisa realizada pela FEBRABAN em 2013.

A FEBRABAN, fundada em 1967, é a principal entidade representativa do setor bancário brasileiro, cuja sede está localidade na cidade de São Paulo. É uma associação sem fins lucrativos que tem o compromisso de fortalecer o sistema financeiro e suas relações com a sociedade e contribuir para o desenvolvimento econômico, social e sustentável do País (FEBRABAN, 2014).

A obtenção de informações, ultrapassa os ataques contra os recursos tecnológicos. Fazem-se presentes nas atividades rotineiras das pessoas, como acessar a sua Instituição Bancária, seja de forma virtual ou pessoal, com o furto de informações, ou ainda, um simples atendimento telefônico, de chamadas iniciadas de presídios, simulando situações de risco para família, como o golpe do falso sequestro. Em ambos os exemplos, o efeito surpresa, a manipulação e a persuasão são característicos, fragilizam as pessoas e, em consequência, podem levar a exposição de informações. Nesse escopo: “Declara-se que o 'elo mais frágil', entretanto, da segurança de dados e informações confidenciais, não está no sistema, e sim na pessoa que interage com este sistema” (ROSA et al., 2012, p. 30).

Os sistemas informacionais, conforme Marciano e Marques (2006, p. 95), representam a junção do sistema social, pelo qual o sistema informacional está inserido, formado pelos usuários e as suas interações com o sistema, além do complexo tecnológico, responsáveis pela sustentabilidade das interações. Neste contexto, o mundo real transcende o virtual, formando um sistema informacional complexo, dotado de avanços e interações inimagináveis entre a tecnologia e o usuário, visto que “[...] o usuário de um sistema de informação é o indivíduo para o qual se concretiza o fenômeno do conhecimento mediante as informações providas por aquele sistema” (MARCIANO; MARQUES, 2006, p. 95).

O fluxo da formação das informações sigilosas dos correntistas de uma Instituição Bancária inicia no ato da abertura de uma conta, que segundo a FEBRABAN (2014), é um contrato celebrado entre o banco e

o cliente, por livre consentimento de ambas as partes, que estabelecem direitos e obrigações. O alerta a segurança no procedimento de abertura de conta corrente envolve as duas partes. Como por exemplo, para se evitar a utilização e aceitação de documentos fraudados, é necessária a apresentação de documentos originais pelo cliente e a sua análise minuciosa por funcionário do banco, sendo que este deve manter em seus arquivos cópias validadas.

Para realizar os serviços e operações bancárias disponibilizadas pelas Instituições Bancárias é necessário o cadastramento de uma senha bancária, que funciona, conforme a FEBRABAN (2014), como uma chave que abre a porta de acesso à sua conta bancária através dos diversos canais de atendimento disponibilizados pelos bancos, podendo ser utilizada com o cartão magnético nos caixas eletrônicos ou sem o cartão, para o *Internet Banking*.

Os principais serviços oferecidos por uma instituição bancária são as contas-correntes, poupanças, cartões de crédito, cartões de débito e empréstimos.

A ativação de uma conta corrente-corrente ocorre a partir do primeiro depósito em dinheiro, no qual, o mesmo permanece custodiado, ao contrário da conta poupança, que além de permanecer custodiado, oferece também uma rentabilidade.

Os cartões de crédito são o instrumento de pagamento que possibilita a aquisição de bens e serviços em estabelecimentos comerciais credenciados, cujo pagamento é realizado pelo cliente, por intermédio de fatura. Já os cartões de débito são um instrumento de pagamento com vínculo em uma conta bancária que permite realizar saques em dinheiro e pagar bens e serviços (FEBRABAN, 2014).

Os empréstimos são disponibilizados para aqueles que precisam de um montante superior ao disponível, para aquisição de bem ou serviço, sendo estipulado um prazo maior de pagamento em relação aos cartões de crédito (BUENO, 201; FEBRABAN, 2014).

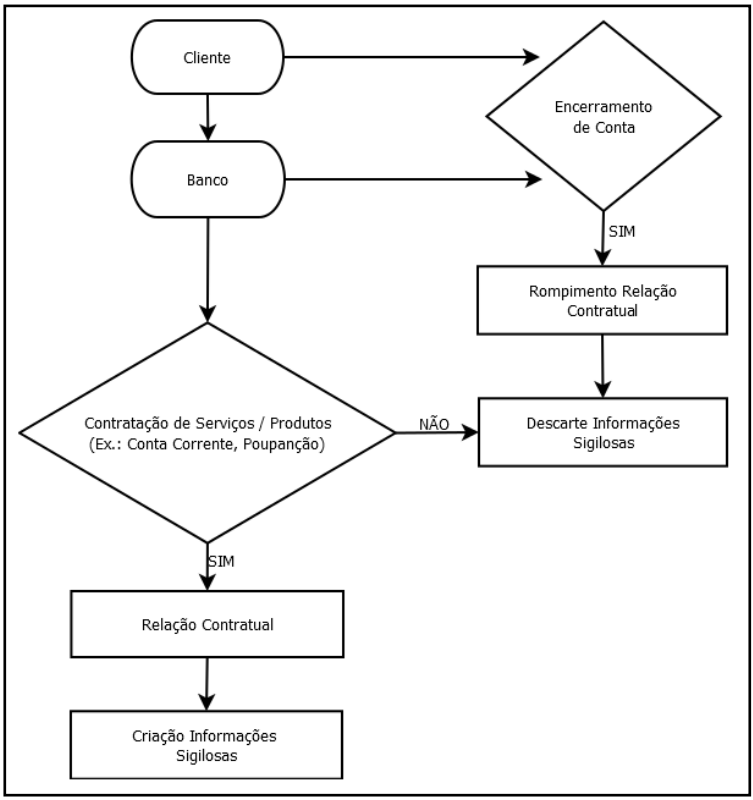
A FEBRABAN (2014) descreve ainda que o acesso aos serviços bancários requer senhas distintas para canais específicos, como senhas para cartões, senhas para acesso ao site da Instituição Bancária e centrais de atendimento telefônico, etc, para preservar o acesso à informação. As Instituições Bancárias são responsáveis, por preservar a tríade balizadora da segurança das informações sigilosas de seus clientes e das suas respectivas transações, formada pela integridade, legitimidade

e confiabilidade (FEBRABAN 2014). Portanto, para se evitar as fraudes eletrônicas, além das medidas de segurança de responsabilidade do banco, há um rol de recomendações de segurança relacionadas principalmente com o comportamento seguro dos clientes, com destaque para:

> - Acompanhar lançamento na conta corrente;
> - Ter em mãos o telefone da agência e da central de atendimento do banco;
> - Contatar o banco ao constatar qualquer débito ou crédito estranho, furto, extravio de cheques e cartões, tentativas indevidas de se obter informações sobre a conta;
> - Em relação às senhas e aos cartões, o cliente é orientado a jamais fornecê-las a terceiros, não anotá-las, escolher senhas formadas por números imprevisíveis, não informar a senha por telefone, não emprestar os cartões da conta, realizar saques durante o horário comercial, não utilizar celulares de terceiros para se comunicar com o banco, não aceitar ou solicitar auxílio de terceiros;
> - Sobre a Internet, a FEBRABAN orienta os clientes que os bancos não enviam *e-mails* com *links* para acesso aos seus respectivos *sites*, solicitando atualização cadastral ou informações relacionadas a senhas e contas, da necessidade de manter instalados no computador programas antivírus, trocar as senhas de acesso periodicamente, não executar ou abrir arquivos de origem desconhecida, manter atualizados os programas de navegação *(browser*), etc (FEBRABAN, 2014; BACEN, 2015).

O contrato de abertura de conta e o acesso aos serviços bancários poderá ser desfeito ou cancelado, por iniciativa formal do cliente e do banco, encerrando, assim, o fluxo das informações sigilosas. (FEBRABAN, 2014).

Ilustração 5: Diagrama - Composição das Informações Sigilosas em Instituição Bancária.



Fonte: elaborado pela autora com base FEBRABAN (2014) e BACEN (2015).

As informações sigilosas de usuários de Instituições Bancárias poderão ser comprometidas desde a origem de tais informações até a finalização do seu processo de descarte, por intermédio de incidentes de segurança.

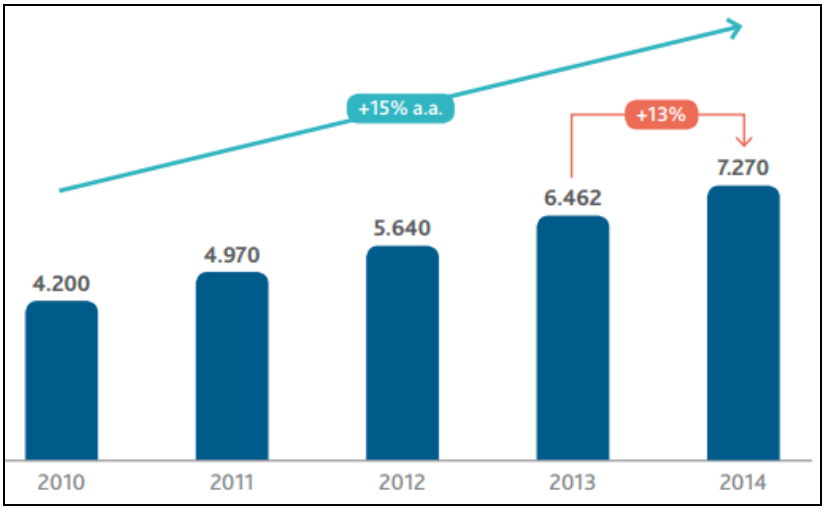
3.2 TRANSAÇÕES FINANCEIRAS E INCIDENTES DE SEGURANÇA

A FEBRABAN realiza anualmente pesquisa relacionada a tecnologia do sistema bancário, com objetivo de demonstrar a evolução

da indústria bancária nacional, mediante a análise de indicadores específicos. Segundo a última pesquisa realizada em 2014, a FEBRABAN, consultou as 20 maiores Instituições Bancárias do País, representando 95% do mercado em termos de números de agências e 90% em termos de ativos totais do setor financeiro.

Nos últimos anos, segundo a pesquisa, houve uma ampliação dos índices de bancarização da população economicamente ativa, consequência esta, relacionada a estabilidade macroeconômica e monetária, aliada ao crescimento da renda e ascensão social. Neste contexto, analisando a pesquisa, pode-se identificar a continuidade do desenvolvimento do setor financeiro.

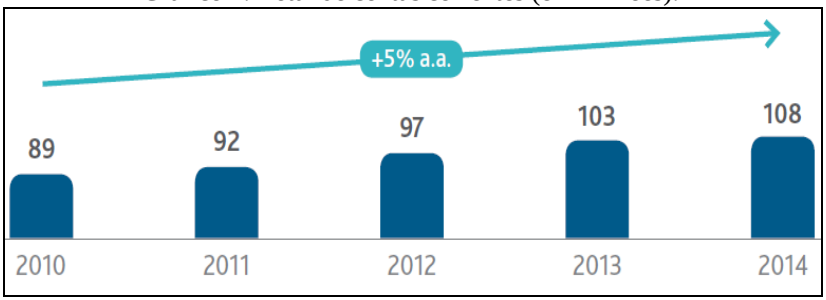
Gráfico 1: Total de Ativos do Setor Bancário 2010-2014 (em bilhões).



Fonte: FEBRABAN, (2014).

Em 2010 havia no setor bancário nacional, 89 milhões de contas correntes abertas e em 2014 este número alcançou 108 milhões, colaborando para a expansão do setor, conforme os dados a seguir.

Gráfico 2: Total de contas correntes (em milhões).



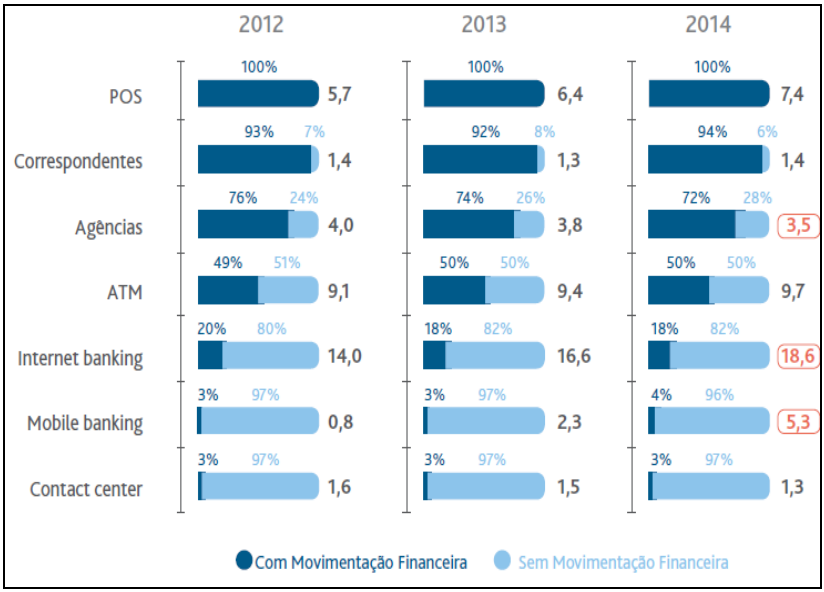
Fonte: FEBRABAN (2014)

O Brasil apresenta uma taxa de bancarização de 60%, equiparando-o com outras nações emergentes como a Turquia (58%) e a Índia (55%), segundo a pesquisa da FEBRABAN (2014). Igualmente ao crescimento do setor bancário, o volume de transações bancárias acompanha tal crescimento, que segundo a pesquisa, foi alavancado pelo uso da Internet e *Mobile Banking*, além de transações que não envolvem movimentações financeiras, como as de consultas. Esta estatística corrobora com a associação de que a automação bancária transforma o dinheiro em informação, conduzindo as Instituições Bancárias para estarem à frente da tecnologia da informação (DINIZ, 2004)

Ao se analisar a origem das transações bancárias em 2014, sejam elas envolvendo movimentação financeira ou apenas consultas, verifica-se que o canal de maior representatividade é a Internet, com 39% da concentração do número das transações, seguida de 21% dos *Automatic Teller Machine* – ATM, conhecidos também como caixa automático, caixa eletrônico, ou terminal de autoatendimento. A seguir aparecem, com 16%, os *Point of Sale* ou *Point of Service* – POS, que são dispositivos eletrônicos utilizados para realizar transações com cartões de crédito e débito. Nos 24% restantes se concentram as transações realizadas diretamente nas agências bancárias, *Contact Center* – Centrais de Atendimento, *Mobile Banking* – Banco Móvel (*smartphones* e *tablet*) e correspondentes bancários. Ao se separar as transações com movimentação financeira daquelas sem movimentação financeira, aplicando o filtro por canal, se conclui, segundo a pesquisa da FEBRABAN (2014), que o uso da *internet* e *Mobile Banking*, apresenta uma menor representação de transações envolvendo movimentação

financeira, quando comparado com atendimento via canais com contato pessoal, como os POS, correspondentes bancários, agências e ATM, sendo estes ainda os mais utilizados pelos clientes, face a segurança e a confiabilidade, conforme no gráfico a seguir:

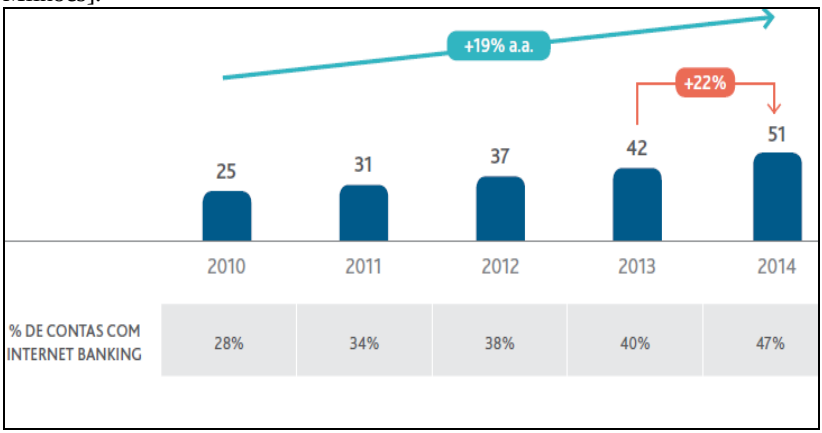
Gráfico 3: Canal por tipo de transação (canal por tipo de transação - % do total de transações por canal e total de transações – em bilhões)



Fonte: Febraban (2014)

A sociedade brasileira apresenta um comportamento predominantemente digital. Quando observado isoladamente, o uso da *internet banking* vem crescendo continuamente a taxa de dois dígitos desde 2010, com cada vez mais contas correntes com acesso a esse canal. No final de 2014, quase 50% de todas as contas correntes estavam habilitadas a utilizar o canal, representando um crescimento de 22% de contas vinculadas ao Internet Banking no último ano (FEBRABAN, 2014).

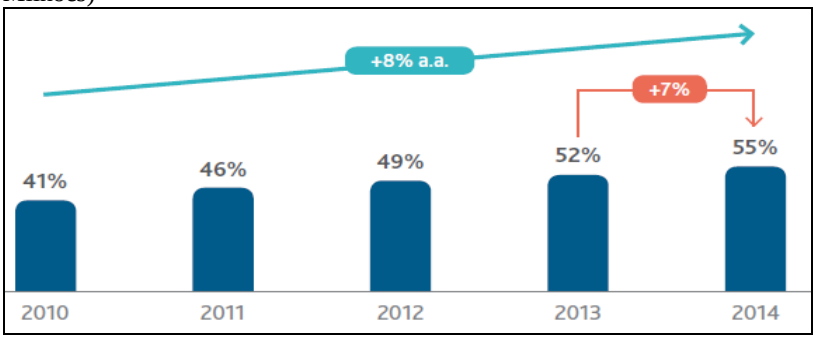
Gráfico 4: Contas correntes habilitadas para acesso via internet banking [Em Milhões].



Fonte: Febraban (2014)

Comparando o resultado do último ano, nota-se que ainda houve uma expansão maior de contas correntes com *internet banking* (22%), comparado ao aumento da população com acesso à *internet banking* (7%), que alcançou em 2014, um crescimento de 7% a faixa dos 105 milhões.

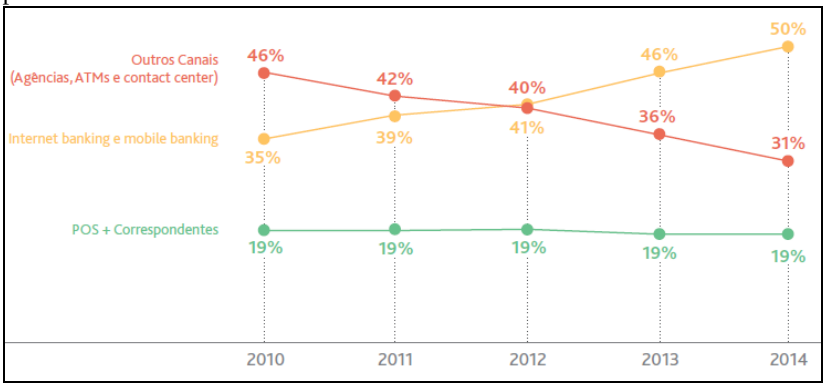
Gráfico 5: População com acesso à internet banking (2010 – 2014) (Em Milhões)



Fonte: Febraban (2014)

Porém, a pesquisa demonstra, certo receio dos clientes em utilizar a *internet banking* e *mobile banking* para realizar transações com movimentação financeira, receios estes atribuídos a três variáveis: 1) questões culturais de uso e geração de clientes; 2) a percepção de falta de segurança do software, com roubo de informações e hardware, com roubo do aparelho; 3) o crescimento de transações sem movimentação financeira oriundo da comodidade e rapidez do canal (FEBRABAN, 2014).

Gráfico 6: Comportamento do usuário (% da soma de volumes de transações por canais.



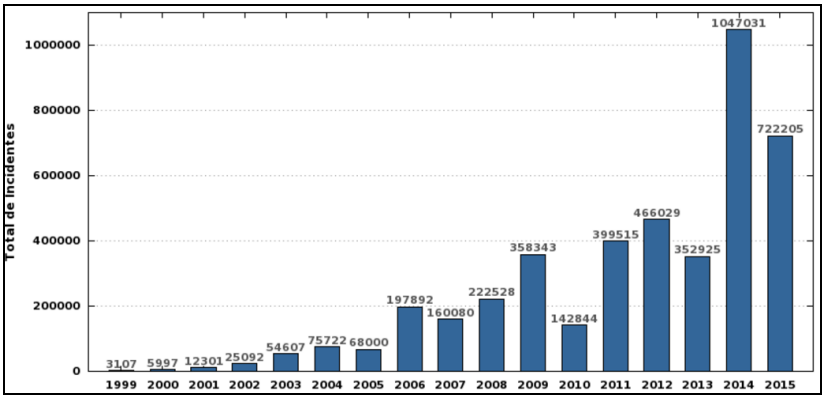
Fonte: FEBRABAN, (2014).

Acompanhando a tendência de utilização de canais eletrônicos pelos correntistas de Instituições Bancárias, os incidentes de segurança são moldados e adaptados aos respectivos canais.

Um incidente de segurança é "[...] qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores", segundo a Norma Complementar n. 05/IN01/DSIC/GSIPR, que disciplina a criação de equipes de tratamento e respostas a incidentes em segurança e o conceitua. Os exemplos característicos de tais incidentes são: as tentativas de ganhar acesso não autorizado a sistemas ou dados; ataques de negação de serviço; uso ou acesso não autorizado a um sistema; modificações em um sistema sem o conhecimento, instruções ou consentimento prévio de seu dono; desrespeito à política de segurança ou à política de uso aceitável de uma empresa ou provedor de acesso. CERT.br (2015, sem paginação).

Os incidentes de segurança ocorridos na rede no Brasil, são computados a partir de notificações voluntárias dos indivíduos e das organizações, cuja quantidade acumulada em 2015, alcançou 722.205 incidentes, 31% menor que em 2014. CERT.br (2015), conforme o gráfico:

Gráfico 7: Total de incidentes reportados ao CERT.br.



Fonte: CERT.br (2015).

A seguir serão descritos os incidentes de segurança notificados à CERT.br segundo relatório com as informações compiladas de 2015. Os incidentes são categorizados pela CERT.br em 06 categorias:

- Ataques aos servidores *web*;
- Ataques de negação de serviço;
- Tentativas de fraude;
- Varreduras e propagação de códigos maliciosos;
- Computadores comprometidos;
- Outros incidentes reportados.

Para os ataques aos servidores *web*, no ano de 2015 houve um aumento de 128% em relação a 2014, totalizando 65.647 notificações. Os atacantes exploraram as vulnerabilidades em aplicações *web* para, então, hospedar nesses *sites* páginas falsas de Instituições Bancárias, Cavalos de Troia, ferramentas utilizadas em ataques a outros servidores *Web* e *scripts* para envio de *spam* ou *scam* (CERT, 2015).

No ano de 2015, a CERT.br, recebeu 25.360 notificações sobre computadores que participaram de ataques de negação de serviço (DoS). Este número foi 89% menor que o número de notificações recebidas em 2014. O principal objetivo de tais ataques é tornar os serviços oferecidos pelas vítimas inacessíveis aos usuários legítimos, comprometendo a tríade balizados da segurança da informação. Para tanto, nenhum dado é furtado, alterado, há simplesmente, uma interrupção dos serviços prestados, considerando a sobrecarga da estrutura da rede pelo grande tráfego, oriundo da quantidade de requisições de acesso por supostos usuários, ou seja, o computador fica sobrecarregado e nega o serviço (MIRKOVIC et al., 2004).

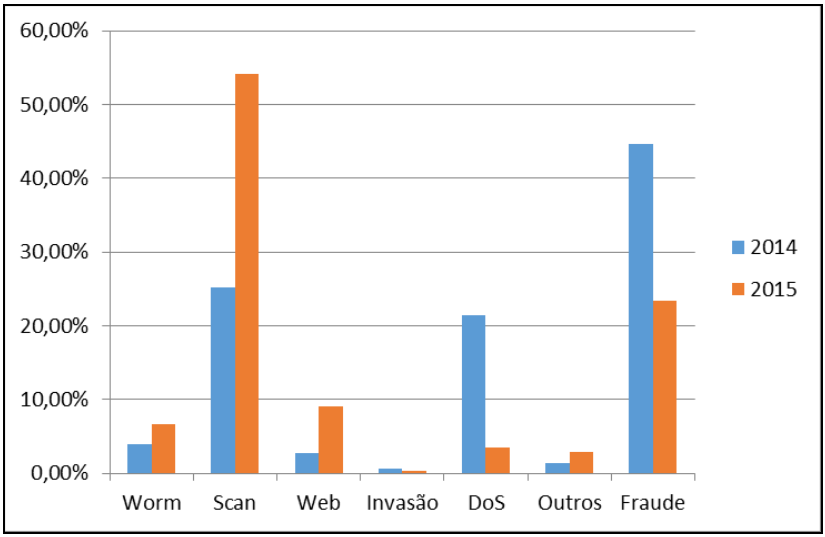
As notificações de tentativas de fraude, em 2015, totalizaram 168.775, correspondendo à uma queda de 64% em relação à 2014. As notificações de casos de páginas falsas de bancos e *sites* de comércio eletrônico (*phishing* clássico) em 2015 diminuíram 32% em relação a 2014. As notificações sobre Cavalos de Troia, utilizados para furtar informações e credenciais, tiveram uma queda de 59% em relação ao ano de 2014. Como resultado da pesquisa, nota-se que em 2015 o número de notificações de casos de páginas falsas que não envolvem bancos e *sites* de comércio eletrônico teve um aumento de 19% em relação a 2014. Nesses casos estão incluídos os serviços de *webmail* e redes sociais, por exemplo. Em 2015, a CERT.br, recebeu 86.619 notificações relacionadas a eventuais quebras de direitos autorais, este número foi 75% menor que o do ano de 2014.

As notificações referentes a varreduras chegaram a 391.223 em 2015, representando um aumento de 48% em comparação ao ano de 2014. As notificações de atividades relacionadas com a propagação de *worms* e *bots* (categoria *worm*) totalizaram 47.722 em 2015, aumentando 13% em comparação com 2014.

A quinta categoria de incidentes da Cert.br (2015), relaciona-se aos computadores comprometidos, que alcançou 2.457 notificações. Este total foi 62% menor do que o número de notificações recebidas em 2014.

Para os outros incidentes reportados à CERT.br (2015), foi recebido 21.021 notificações que se enquadram na categoria "outros", correspondendo a um número 47% maior que o total de 2014.

Gráfico 5: Incidentes reportados: tipos de ataques – 2014/2015.



Fonte: CERT.br (2015)

Com base no gráfico 5, quando analisados os incidentes reportados relativos ao ano de 2014, observa-se que 44,66% referiram-se às fraudes e 25% a notificações de varreduras em redes de computadores, que compuseram a grande maioria. Já em 2015, percebe-se a desaceleração de incidentes relacionados às fraudes, mas um aumento exponencial de mais que o dobro (54,17%) de incidentes reportados à notificações de varreduras em redes de computadores (*Scan*).

O volume de transações bancárias no Brasil e os incidentes de segurança crescem proporcionalmente, quando comparamos os dados estatísticos de 2012 e 2013, segundo dados da CERT e do Banco Central do Brasil – BACEN (2015).

O BACEN, foi criado em dezembro de 1964, com a promulgação da Lei nº 4.595, com natureza administrativa de autarquia federal integrante do Sistema Financeiro Nacional – SFN - e tem como missão assegurar a estabilidade do poder de compra da moeda e um sistema financeiro sólido e eficiente. Em junho de 2014, o BACEN divulgou a relação dos 50 maiores bancos do Sistema Financeiro Nacional - SFN,

tendo como referencial classificatório os ativos totais das Instituições Bancárias. Os ativos de uma empresa são formados por todos os bens e direitos que a constituem. Em suma, é tudo aquilo que possui valor para uma organização e, portanto, requer proteção (RAMOS, 2006) A sinergia dos ativos de uma organização é fundamental para salvaguardá-los e a falta de conhecimento pode comprometê-los, pois o agir correto depende do saber agir (ALMEIDA, CARNEIRO, 2013).

Considerando a classificação publicada pelo BACEN (2015) e o conceito de ativos de uma empresa, foram selecionados os três maiores bancos que consolidam o SFN: Banco do Brasil S.A. - BB, Itaú S.A e Caixa Econômica Federal. O objetivo da seleção é identificar se as mesmas divulgam em seus *sites*, orientações aos usuários sobre o tema segurança da informação.

Tabela 1: Classificação dos três maiores bancos do Brasil conforme os seus ativos.

Instituição	Ativo Total
Banco do Brasil	R$ 1.438.964.956,00
Itaú	R$ 1.285.393.163,00
Caixa Econômica Federal	R$ 1.203.756.044,00

Fonte: Elaborado pela autora com base site do BACEN (2015).

Posteriormente, serão analisadas as informações acerca a segurança da informação elencadas nos *sites* dos três maiores Bancos do SFN, sendo este o canal de comunicação selecionado para subsidiar a pesquisa.

4 METODOLOGIA

Esta seção destina-se a demonstrar os métodos aplicados na coleta e tratamento dos dados obtidos, com intuito de alcançar resultados e as suas respectivas repercussões.

4.1 ABORDAGEM E METODOLOGIA DE PESQUISA

Os objetivos da pesquisa serão desenvolvidos a partir de uma metodologia quali-quantitativa, com substrato em dados obtidos no ambiente da pesquisa, que serão descritos e quantificados.

Considerando as diretrizes retratadas pelos autores Gil (2002) e Moreira (2005), a metodologia utilizada para o desenvolvimento do estudo, é classificada como exploratória e descritiva. Na análise exploratória, para Gil (2007), o objetivo é ampliar o conhecimento sobre um determinado assunto tratado, com intuito de promover modelos, enquanto que na pesquisa descritiva, se procura descrever as características determinantes de uma população ou fenômeno, ou ainda, correlacionar variáveis.

Tais conceitos foram utilizados como alicerces para o desenvolvimento de uma pesquisa bibliográfica, com intuito de identificar nas produções científicas os conceitos e cenários norteadores, principalmente, da segurança da informação, engenharia social e suas técnicas, os riscos e ameaças informacionais, relacionando-os com a área da Ciência da Informação.

Optou-se por desenvolver a pesquisa em três fases distintas.

A primeira fase engloba a análise dos *sites* das três maiores Instituições Bancárias do Brasil, comparando os anos 2014 e 2016. O intuito é demonstrar quais informações sobre segurança estão disponíveis aos usuários e correntistas.

A segunda fase é uma abordagem qualitativa que considera como fonte direta dos dados o ambiente natural e tem o pesquisador como o principal instrumento, cujos dados uma vez coletados são descritos pelo pesquisador (BODGAN; BIKLEN, 1994). Os dados quantitativos foram obtidos através de uma pesquisa documental, realizada em uma Instituição Bancária, com objetivo de se coletar uma amostra de

indivíduos, cujas informações sigilosas foram comprometidas. A Instituição Bancária estudada não permite a divulgação do seu nome em produções científicas, por ser uma das suas diretrizes da política de segurança de informação.

Após a seleção da amostra, se inicia a terceira fase. Com objetivo de analisar as principais características dos indivíduos que foram vítimas da engenharia social. Seguindo os ditames de Marciano e Marques (2006, p. 91), se optou pelo desenvolvimento, aplicação e análise do instrumento da pesquisa no formato de entrevistas, com intuito de formular conceitos pelos quais se pretende medir, a sua extensão.

A entrevista foi realizada no período de 01/11/2014 a 15/11/2014, por meio de ligação telefônica e transcrição dos relatos dos entrevistados. No contato inicial foi descrito o propósito da pesquisa científica, os seus conceitos-chave, e em seguida foi aplicado o roteiro da entrevista, após a concordância em participar da pesquisa.

Segundo os autores Nogueira (1968), Triviños (1987) e Creswell (2007), a entrevista pode estar relacionada a um método, ou instrumento de pesquisa ou uma técnica, utilizada em procedimento de coleta de dados de pesquisa científica em ciências humanas. Para Creswell (2007), as entrevistas semiestruturadas combinam perguntas abertas e fechadas, onde o informante tem a possibilidade de discorrer sobre o tema proposto. Assim, optou-se por este procedimento para coleta de dados, permitindo aos entrevistados expressar livremente os seus sentimentos quando vítimas das fraudes eletrônicas.

Neste contexto, como uma amostragem representativa da população poderá resultar em um referencial fidedigno? Em resposta a esta indagação temos a seguinte consideração:

> A chave para decifrar este enigma é a representatividade. A amostra representa a população se a distribuição de algum critério é idêntica tanto na população quanto na amostra. Os parâmetros de uma população são calculados através das estimativas observadas na amostra. (BAUER; AARTS, 2002, p. 41).

No geral, a pesquisa está estruturada, conforme o quadro a seguir:

Quadro 3: Estrutura da pesquisa

Pesquisa	1º Fase	2º Fase	3º Fase
Atividade	Analisar os *sites* das três maiores Instituições Bancárias	Pesquisa documental: - Banco de dados da Instituição Bancária Estudada	Análise do Instrumento de Pesquisa: - Entrevista
Objetivo	Demonstrar quais informações sobre segurança da informação estão disponíveis nos *sites*	Coletar amostra dos correntistas, cujas informações sigilosas foram comprometidas	Analisar as principais características dos correntistas vítimas da engenharia social

Fonte: Elaborado pela autora com base na metodologia da pesquisa

As entrevistas foram descritas integralmente, porém, para o que se pretendia com este trabalho foram consideradas algumas passagens relevantes para se atingir os objetivos da pesquisa. Optou-se por não anexar a transcrição integral das entrevistas pela quantidade de páginas resultantes.

Para compor a tabulação dos dados obtidos com as entrevistas, foi utilizado como ferramenta o programa Excel, permitindo a constituição dos gráficos e tabelas.

Apesar da entrevista ser composta de questões abertas, as respostas foram similares, permitindo compilar os dados.

4.2 POPULAÇÃO E AMOSTRA

A população da presente pesquisa é composta por correntistas de Instituições Bancárias, com domicílio bancário na Grande Florianópolis. O domicílio bancário é o local onde o correntista mantém ativa a sua conta corrente (BACEN, 2015).

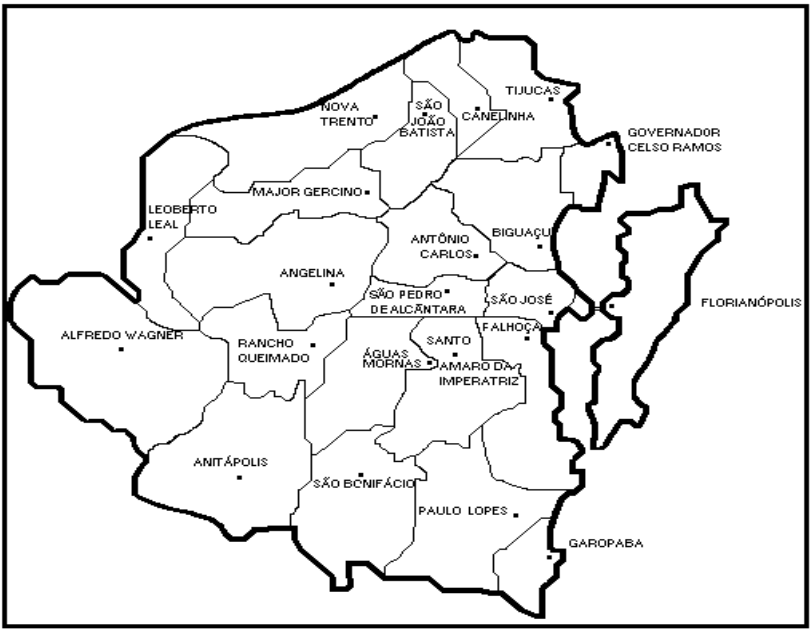
Segundo definição do Instituto Brasileiro de Geografia e Estatística - IBGE, a Grande Florianópolis é composta por 22 municípios, compreendendo: Águas Mornas, Alfredo Wagner, Angelina, Anitápolis, Antônio Carlos, Biguaçu, Canelinha,

Florianópolis, Garopaba, Governador Celso Ramos, Leoberto Leal, Major Gercino, Nova Trento, Palhoça, Paulo Lopes, Rancho Queimado, Santo Amaro da Imperatriz, São Bonifácio, São João Batista, São José, São Pedro de Alcântara e Tijucas[1] assim ilustrada:

Ilustração 6: Mapa da divisão geográfica dos municípios da Grande Florianópolis.

Fonte: FECAM (2014)

[1] (http://www.granfpolis.org.br/ municipios/index.php),



Fonte: FECAM (2014)

A amostra da pesquisa foi obtida da Instituição Bancária que aceitou disponibilizar informações dos correntistas vítimas da engenharia social, sendo esta, uma das três maiores Instituições Bancárias do Brasil, em relação ao seu número de ativos. Foram selecionados os correntistas vítimas de fraudes pela internet e por cartão de crédito e débito, no período de 1º de janeiro de 2014 à 31 de junho de 2014.

4.3 PROCEDIMENTOS DA COLETA DE DADOS

Os dados da amostra foram obtidos através da base de dados própria da Instituição Bancária pesquisada, mediante os registros de processos de contestação de débitos de seus correntistas, tendo como

instrumento de coleta a tabulação das informações, considerando as seguintes variáveis qualitativas:

Em relação à fraude: local (cidade da Grande Florianópolis); tipos de fraudes eletrônicas (internet e cartões de débito e crédito); modalidades de fraude considerando os tipos (auxílio de terceiro, token, central de atendimento e internet - *internet banking*), o canal explorado pelo fraudador para realizar a fraude (internet, *smatphones* ou caixas eletrônicos); tipo de transação fraudulenta (pagamento de boletos, transferências eletrônicas, saques ou compras) e a forma como ocorreu a fraude (ação indireta do engenheiro social com envio de *malwares*, *phising*, ou ação direta do engenheiro social, como a troca de cartão ou a retenção do cartão);

Em relação ao correntista fraudado: profissão; renda média; grau de escolaridade; data de nascimento e gênero.

O ensaio documental de dados alcançados na Instituição Bancária procurou compor a totalidade de correntistas vítimas de fraudes eletrônicas, seja pelo uso da internet ou de cartões na Grande Florianópolis, com intuito de identificar características comuns dos correntistas.

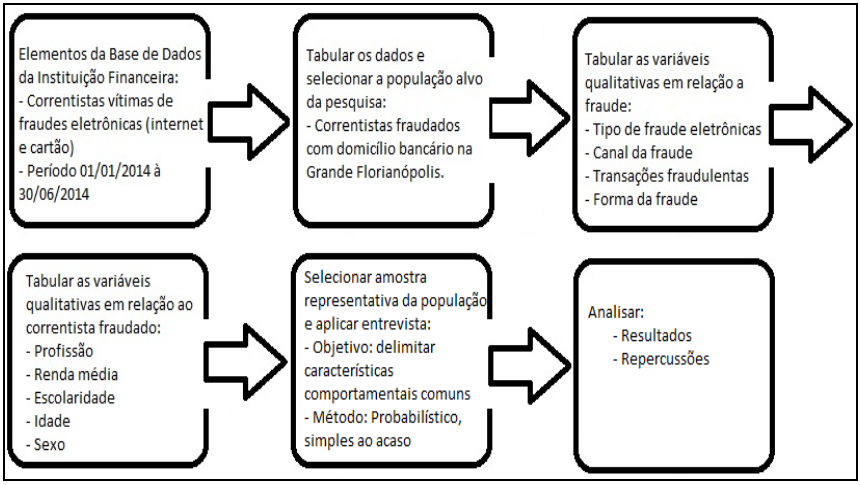
Na primeira etapa da recuperação dos dados foi identificado um total de 132 correntistas vítimas de fraudes eletrônicas na Grande Florianópolis, na modalidade de internet e cartão de crédito e débito, cujas características serão apresentadas nos resultados da pesquisa.

Em seguida se delimitou uma amostra representativa da população para aplicação da entrevista e com objetivo de identificar as características dos usuários de Instituições Bancárias, que foram exploradas pela engenheira social e, por consequência, levaram ao comprometimento da segurança das informações.

A forma de seleção desta amostra foi pelo método probabilístico simples ao acaso, mediante sorteio aleatório. Neste método, para os autores Bauer e Aarts (2002), todas as unidades da população apresentam a mesma probabilidade de serem selecionadas. Para garantir a proporcionalidade, optou-se por selecionar 20% do total de correntistas vítimas de fraude via internet. O mesmo percentual foi utilizado para os correntistas vítimas de fraude via cartão de débito e crédito.

A ilustração 7 a seguir representa a coleta de dados, as suas respectivas fontes e trajetória.

Ilustração: 7: Base de Dados.



Fonte: da autora - dados da pesquisa 2015.

A entrevista foi composta por questões abertas e semi-dirigidas, ajustadas considerando o pré-teste realizado com cinco pessoas selecionadas do curso de Pós-Graduação em Ciência da Informação, da UFSC, aplicado em outubro de 2013. Foi aplicada a técnica de incidente crítico que envolve um conjunto de procedimentos aplicados para coletar observações de comportamento humano, com intuito de solucionar problemas voltados as necessidades de um sistema (FLANAGAN, 1954).

Após a aplicação do roteiro da entrevista (APÊNDICE A), os dados coletados foram compilados para se atingir os objetivos da pesquisa.

5 ANÁLISE DOS DADOS, RESULTADOS E REPERCUSSÕES

A seguir serão apresentadas as análises e repercussões de cada fase da pesquisa, com intuito de alcançar os objetivos traçados.

5.1 ANÁLISE DOS *SITES* DAS TRÊS MAIORES INSTITUIÇÕES BANCÁRIAS DO BRASIL

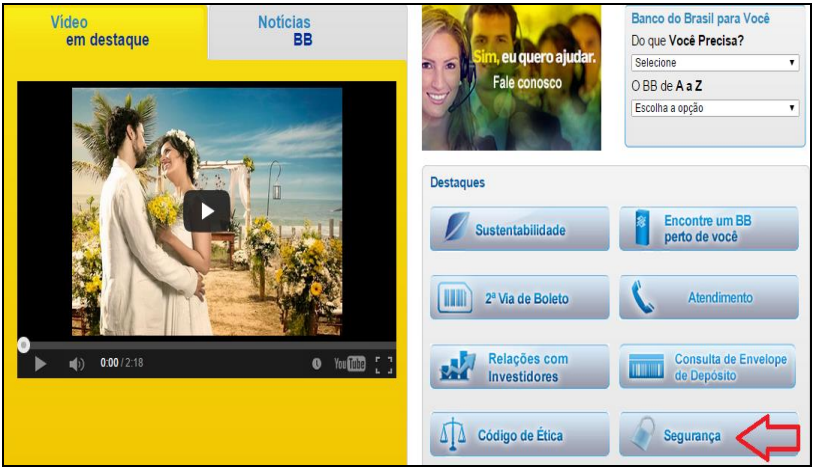
O objeto da análise dos *sites* das três maiores Instituições Bancárias do Brasil, Banco do Brasil, Itaú e Caixa Econômica Federal, é demonstrar quais informações sobre segurança estão disponíveis aos usuários e correntistas, comparando-as entre os anos 2014 e 2016.

5.1.1 Site Banco do Brasil

Em consulta ao site do Banco do Brasil[2], em 2014, o tema segurança estava disposto em um ícone específico localizado no canto inferior direito, após rolagem de tela, conforme demonstrado na Ilustração 8.

[2] http://www.bb.com.br

Ilustração 8: Home Page Banco do Brasil – Ícone Segurança.



Fonte: Banco do Brasil (2014).

Caso o usuário optasse em acessar diretamente os dados da sua conta corrente, o ícone segurança não estava visível no primeiro acesso, sendo necessária a rolagem da página. Após o acesso à conta corrente, o acesso ao tema não aparecia de forma automática, sendo necessária a busca pelo termo, no campo específico, por iniciativa do usuário.

Ao acessar o ícone segurança, em 2014, apenas como visitante da página, sem acessá-la como correntista da instituição, eram disponibilizadas as seguintes opções de informações relacionadas à segurança em seus canais de atendimento: internet, caixas eletrônicos, *smartphones*, central de atendimento BB, dicas de segurança e prevenção a combate à lavagem de dinheiro. No canto esquerdo, ao final da página, havia informações sobre como tornar as transações mais seguras na internet, nos caixas eletrônicos e no celular, como demonstrado na Ilustração 9.

Ilustração 9: Home Page Banco do Brasil – Ícone Segurança.

Fonte: Banco do Brasil (2014).

A aba segurança na Internet descrevia os produtos e serviços disponibilizados pelo banco aos seus clientes e informações sobre segurança. Ofertava-se produtos aos clientes pessoas físicas e jurídicas, voltados à proteção das informações sigilosas, em formato de perguntas mais frequentes.

A aba "segurança caixas eletrônicos" descrevia a rede de atendimento do banco, que era composta por mais de 40.000 terminais, com cerca de 250 transações voltadas para pessoas físicas, jurídicas, não correntistas e governo, elencando orientações sobre o comportamento seguro.

O Banco do Brasil reservou o item segurança em *smartphones*, para orientar os seus correntistas quando da utilização de seus aparelhos celulares na realização de transações financeiras, sendo totalmente eletrônico.

A aba Central de Atendimento BB – CABB, era um canal de negócios destinado aos correntistas para realizar transações financeiras como consultas a saldo e extrato, pagamentos, resgates de aplicações financeiras, transferências, demais transações bancárias, elogios e sugestões, atendendo pelos telefones específicos. O acesso a este canal somente poderia ser realizado com a informação da senha de seis dígitos e a de quatro dígitos, para confirmar as transações, ambas pré-cadastradas na agência do correntista ou pela internet. O alerta de segurança descrevia que tais senhas somente deveriam ser informadas caso a ligação fosse iniciada pelo correntista.

O item dicas de segurança, ilustração 10, era composto por oito subitens: engenharia social, comportamento seguro nas salas de autoatendimento e agências, segurança pessoal, cheques, boletos bancários, senhas, *e-mail* e cartões-conforme segue:

Ilustração 10: Home Page Banco do Brasil – Ícone Segurança – Dicas de Segurança.

Fonte: Banco do Brasil (2014).

A engenharia social era conceituada pelo *site*, em 2014, como sendo uma técnica de convencimento e enganação para se obter informações sigilosas, credenciais de acesso a ambientes ou sistemas, com objetivo de aplicar golpes e obter vantagens ilícitas, como por exemplo, acesso a contas bancárias. Era descrito, ainda, que qualquer pessoa poderia ser alvo do engenheiro social, cujo sucesso da investida estava relacionado à ganância, vaidade, ingenuidade, carência, desejo de ajudar, curiosidade, insatisfação profissional, entre outros.

As orientações na *home page* do Banco do Brasil, em 2014, relacionadas a senhas, iniciava com alerta informando que o Banco não realizava ligações aos clientes solicitando informações, desbloqueio ou cadastramento de senhas e que as mesmas somente deveriam ser digitadas quando a ligação fosse iniciada pelo correntista. Apontava que a senha representa uma assinatura eletrônica e não deveria ser divulgada à terceiros.

O subitem *e-mail*, divulgava que o Banco do Brasil não enviava *e-mails* sem autorização de seus clientes, com objetivo de proteger os

seus correntistas de fraudadores que utilizavam os *e-mails* para instalar no computador programas espiões, para furtar senhas, dados bancários, números de cartões de crédito e outras informações. O correntista, ao receber um *e-mail* encaminhado supostamente pelo Banco do Brasil, poderia enviá-lo para análise, via *e-mail* "abuse@bb.com.br" e em seguida apagá-lo da sua caixa de entrada.

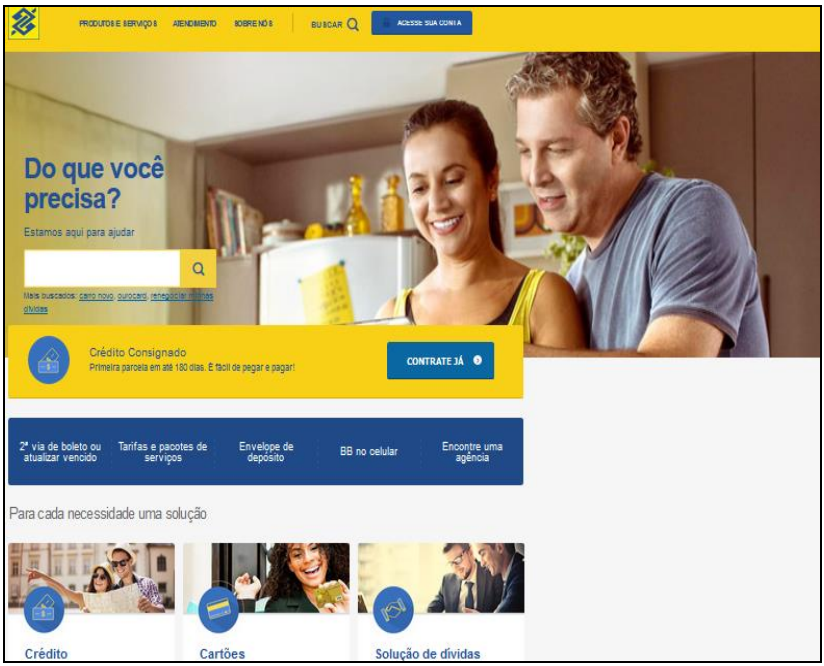
As dicas de segurança associadas aos cartões, disponível no *site* do Banco do Brasil em 2014, orientava o correntista a colocar sua assinatura no verso dos seus cartões. Por armazenarem informações, os cartões deveriam ser mantidos em poder do portador, não o emprestando ou permitindo que terceiros o examinassem, pois poderia haver na ocasião, o golpe da troca de cartões.

Ao realizar compras via internet, o site orientava, que o correntista analisasse as informações que estavam sendo digitadas em área segura do *site*, contendo um pequeno cadeado fechado na tela do programa de navegação e se o endereço do *site* iniciava com as letras "*https*".

O usuário comum da internet ou o correntista do Banco do Brasil, caso buscassem informações sobre segurança bancária no *site*, precisavam acessar o ícone segurança para obter as informações, pois as mesmas não estavam disponibilizadas de forma automática.

Ao acessar o site do Banco do Brasil em maio de 2016, como visitante da página, não há referência sobre o tema segurança no acesso inicial, sendo necessário rolar a página para acessar *link* específico sobre segurança, conforme a ilustração a seguir:

Ilustração 11: Home Page Banco do Brasil – 2016



Fonte: Banco do Brasil (2016).

No rodapé da página há um ícone específico sobre segurança, cujo acesso traz informações interativas sobre o tema, em formato de história com animações, com slogan "em casa é muito seguro".

Ilustração 12: Home Page Banco do Brasil – 2016

Fonte: Banco do Brasil (2016).

Neste espaço são abordados temas referentes a proteção das senhas, internet, BB Mobile, canais de atendimento, segurança no site do BB.

Ilustração 13: Home Page Banco do Brasil – 2016.

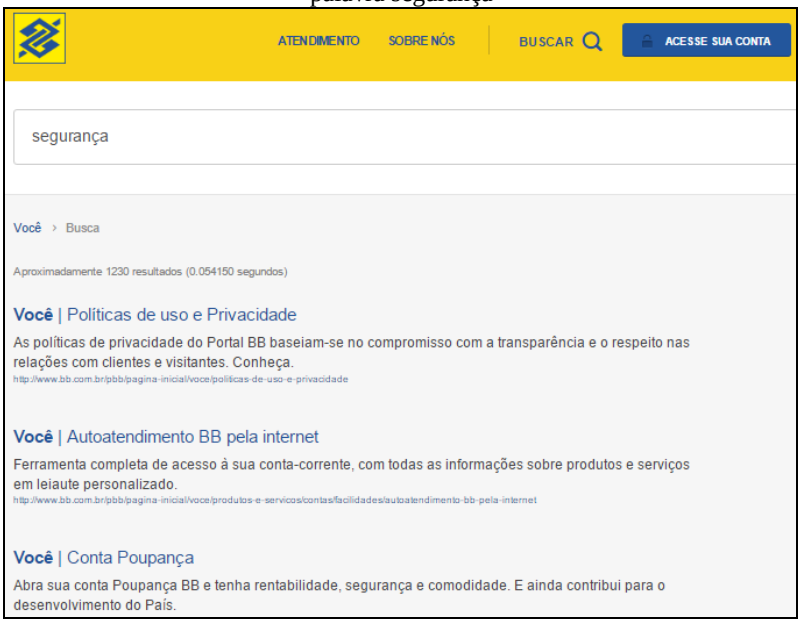
Fonte: Banco do Brasil (2016).

No mesmo ambiente, há um teste de segurança voltado para correntistas e não correntista, com a apresentação, vantagens e as instruções para o uso das soluções de segurança que o BB oferece, em formato de perguntas e respostas. Após o teste, há um ícone que reúne todas as soluções de segurança disponíveis ao correntista para proteger as suas informações e utilizar os canais de atendimento com segurança.

O último ícone sobre o assunto "mais informações", reúne dicas de segurança, com as mesmas informações apresentadas em 2014, contendo alertas sobre golpes envolvendo boletos, engenharia social, salas de autoatendimento, segurança em redes sociais, entre outras.

No ícone "Do que você precisa", na página principal, ao se digitar a palavra segurança, são recuperados 1.230 resultados, porém os assuntos estão dispersos não se observa orientações aos clientes sobre a segurança de suas informações, conforme ilustração 14.

Ilustração 14: Home Page Banco do Brasil – 2016 – resultado da busca pela palavra segurança



Fonte: Banco do Brasil (2016).

O acesso ao site como correntista em maio de 2016, traz um ícone específico sobre segurança, porém com informações diferentes das expostas em 2014. Tais informações estão voltadas para o oferecimento de serviços, incluindo, a liberação de computadores via mensagem de celular, para se realizar transações via internet, BB Code, certificados digitais, autorização e bloqueio de transações, senhas (alteração, cadastramento e desbloqueio), cadastro (atualização e autorização para recebimento de *e-mails*).

Ao se comparar as informações contidas no site do Banco do Brasil em 2014 e 2016, se observa além da alteração do leiaute, uma abordagem sobre o tema segurança mais interativa, com figuras e textos, em formato de histórias, contendo explicações sobre o tema.

5.1.2 Site do Banco Itaú

O *site* do Banco Itaú S.A[3], dispunha em sua página em 2014, ícones que poderiam ser acessados por qualquer usuário, com os seguintes temas: o que você procura, produtos, seus objetivos, atendimento, a campanha publicitária, acesso agência e conta, este último somente para correntista, todos dispostos no topo da página.

O acesso ao ícone "o que você procura", com a digitação da palavra "segurança", foram recuperados 297 resultados da pesquisa, com os mais diversificados assuntos, com notícias, produtos, dicas de segurança, etc. Ao acessar o ícone específico "mais segurança" (rodapé da página), são apresentados quatro subitens, relacionados à segurança bancária, segurança pessoal, segurança digital e saiba mais.

Ilustração 15: Home Page Itaú – Página inicial.

Fonte: Banco Itaú (2014).

Havia um alerta sobre *e-mails* suspeitos, com destaque no centro da página. O acesso ao tópico "Segurança Bancária – internet", permitia a consulta em mais sete subtópicos: o Itaú na Internet, com orientações para proteção da segurança das informações digitadas no site; dicas como manter o computador protegido; descrevia o que era uma fraude na Internet, destacando que a característica principal era quando uma

[3] https://www.itau.com.br

pessoa se passa por outra, utilizando as informações de identificação, como usuário e senha.

O subtópico da "segurança bancária", apresentava o tema "soluções de segurança", que descrevia os produtos e serviços voltados à proteção da segurança das informações como, ferramentas de segurança, criptografia dos dados, senha eletrônica, teclado virtual variável, cartão de segurança Itaú, *iToken*, guardião 30 horas, entre outros.

O subitem "segurança bancária para sua empresa", era formado por um vídeo sobre segurança na internet, um guia rápido sobre cuidados com sua empresa e como prevenir fraudes bancárias.

O "guia rápido: cuidado com sua empresa", apresenta um *menu* com informações básicas sobre fraude na internet, forma de identificação e proteção.

Ilustração 16: Home Page Itaú – Mais Segurança.

Fonte: Banco Itaú (2014).

A abordagem do tema seguia com exemplos de fraudes via internet, destacando o envio de *e-mails* falsos identificados pelo Banco Itaú, conforme se observa na ilustração 17.

Ilustração 17: Home Page do Banco Itaú – Internet – Exemplos de fraude.

Fonte: Banco Itaú (2014).

A segurança bancária ao telefone da ilustração 18, elencava três tópicos sobre o assunto: ao falar com o Itaú; como as fraudes acontecem; atualização do Certificado Digital.

O alerta "como as fraudes acontecem" descrevia que o fraudador necessitava ter acesso ao cartão e senhas do correntista para cometer fraudes. Para tanto, se utilizava de esbarrões para tentar realizar a troca do cartão, após ter observado a digitação pelo correntista da senha previamente nos caixas eletrônicos, ou ainda, se oferecia para auxiliar o correntista e trocava o cartão sem que a ação fosse percebida. Assim, cometia o golpe conhecido como troca de cartão.

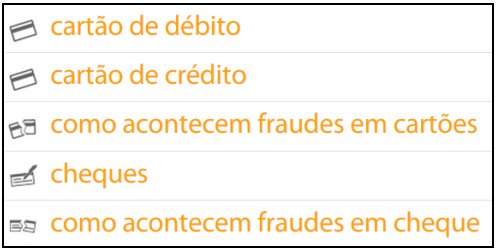
Ilustração 18: Home Page Itaú – Mais Segurança – Segurança Bancária.

Fonte: Banco Itaú (2014).

O tema segurança bancária em cartões e cheques da ilustração 19 é subdividido no *site* do Itaú em cinco tópicos que incluíam, cartão de débito, cartão de crédito, como acontecem as fraudes com o uso de cartões, cheques e como aconteciam as fraudes com o uso de cheques.

Sobre cartão de débito, o *site* enfatizava que os cartões eram pessoais, intransferíveis e armazenavam as informações individualizadas dos clientes e orientava a necessidade de apor a assinatura no verso do cartão, não devendo o mesmo ser emprestado para terceiros

Ilustração 19: Home Page do Banco Itaú – Mais Segurança – Segurança Bancária – Cartões/Cheques.



Fonte: Banco Itaú (2014).

As fraudes com cartões de crédito seguiam a mesma linha das fraudes com cartão de débito, cujas informações eram obtidas pela observação da digitação da senha, das informações que constavam no cartão e pela troca do cartão, seja por meio de esbarrões ou por fraudadores se passando por falso atendente.

O *site* seguia alertando sobre a segurança bancária em *e-mail* e *Short Message Service - SMS*, conforme demonstrado na ilustração 20, transcrevendo dicas de segurança relacionadas a estes dois canais.

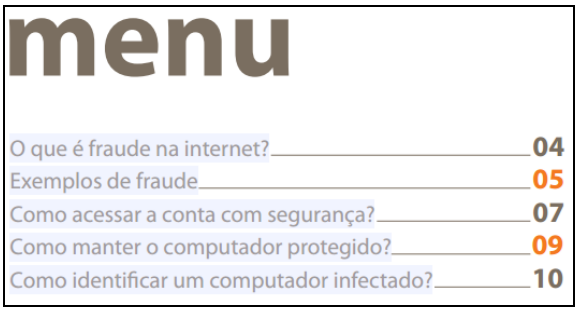
O tópico "*e-mails* suspeitos" alertava o correntista que tais *e-mails* podem infectar o computador e/ou roubar as informações pessoais e bancárias. O Banco Itaú dispunha de *e-mail* próprio para analisar *e-mails* recebidos pelos correntistas com suspeita de fraude, o "emailsuspeito@itau-unibanco.com.br". Enfatizava que o Banco não solicita dados pessoais, senhas ou informações sigilosas *por e-mail* ou por qualquer outro canal.

Ilustração 20: Home Page do Banco Itaú – Mais Segurança – Segurança Bancária – *Email/SMS*.

Fonte: Banco Itaú (2014).

O furto de identidade, segundo o *site* do Itaú em 2014, acontecia quando um terceiro utiliza sem permissão informações ou dados pessoais para cometer crimes ou fraudes e estava ligado a golpes *online* resultantes de práticas como *phishing*, *spywares* e *malwares*. No cuidado com a segurança digital, o *site* do Banco Itaú se preocupava com dois principais temas: a segurança digital na internet e no computador pessoal. Neste sentido, em relação à internet, reportava para dicas gerais, mídias sociais e compras *online*.

Ilustração 21: Home Page Itaú – Mais Segurança – Segurança Bancária – Para sua empresa – Guia rápido: cuidados com a sua empresa.



Fonte: Banco Itaú (2014).

Os perigos *online*, da Ilustração 22, eram discriminados no item "segurança digital", reportando a conceitos relacionados aos golpes por *e-mail*, *phishing*, *spyware*, *malware* e como evitá-los. O *site* conceituava *phishing* como sendo um golpe cometido por fraudadores que enviam *spam* ou mensagens *pop-up*. O *malware*, é uma abreviação de *malicious software*, ou seja, *software* malicioso, englobando vírus (programas que

se reproduzem sem o conhecimento do usuário) ou *spyware* (programas utilizados para monitorar e controlar o computador), cuja instalação é feita pelo próprio usuário, ao realizar *downloads* de programas, histórias, entre outros. O objetivo do *malware* é roubar informações pessoais, enviar *spam* e cometer fraude.

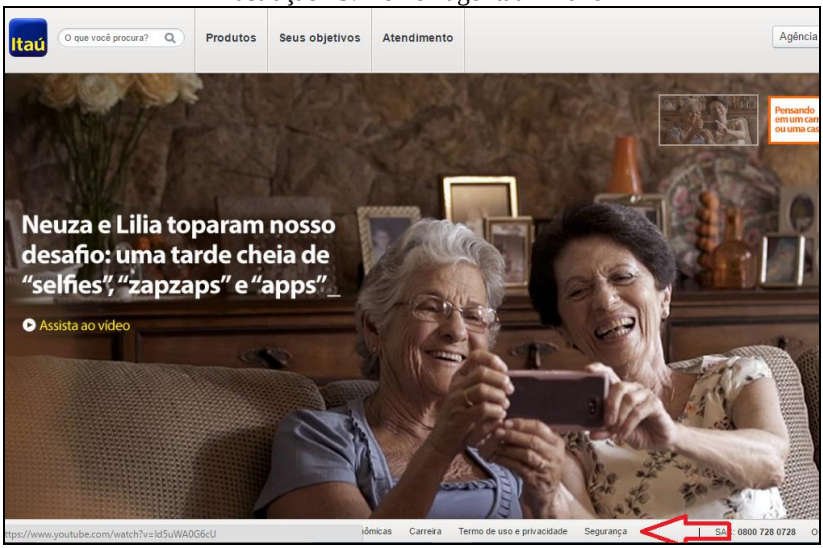
Ilustração 22: Home Page Itaú – Mais Segurança – Segurança Digital – Perigos Online.

Fonte: Banco Itaú (2014).

Todas as informações descritas no *site* do Itaú, aos usuários da internet, também poderiam ser obtidas pelos correntistas do Banco Itaú ao acessarem a sua conta corrente, em ícone específico, ou seja, as informações afetas à segurança somente serão acessadas nos dois ambientes, caso o usuário ou o correntista as procurassem.

A consulta ao site do Banco Itaú em 2016 traz as mesmas informações de 2014, porém, com um leiaute reformulado.

Ilustração 23: Home Page Itaú – 2016



Fonte: Banco Itaú (2016).

Aqueles que venham acessar o site do Banco Itaú para obterem informações sobre segurança, precisarão acessar um ícone específico sobre o assunto, ou seja, a iniciativa de se obter informações e orientações sobre o assunto, dependerá do interesse do usuário, assim como em 2014.

5.1.3 Site do Banco Caixa Econômica Federal – CEF

A Caixa Econômica Federal – CEF, disponibiliza informações aos usuários da internet e correntistas, pessoas físicas ou jurídicas, relacionadas a produtos e serviços, no *site* www.caixa.gov.br.

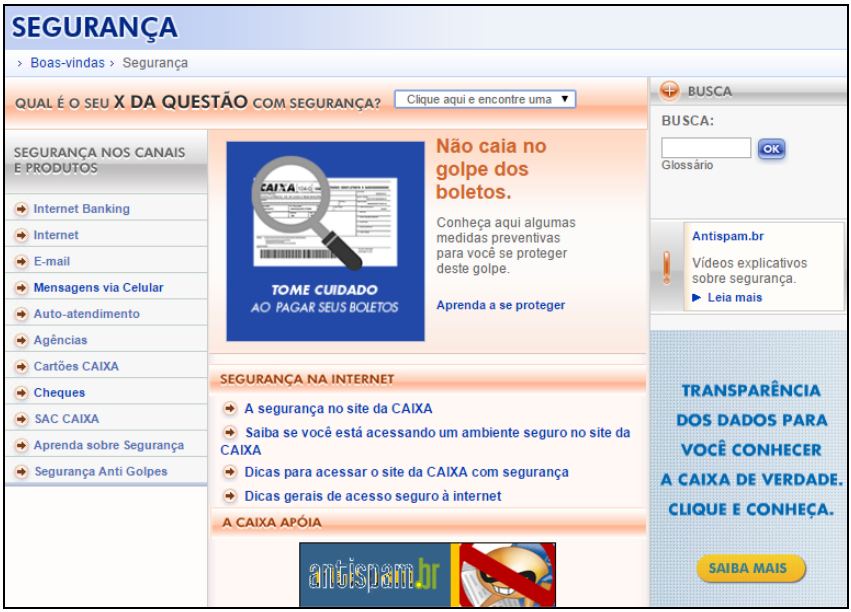
Em 2014 a sua página inicial, apresentava quatro abas com as denominações "Você", "Empresa", "Governo" e "Judiciário". Ao acessar a aba "Você", os usuários poderiam acessar diversas informações sobre produtos e serviços e a abordagem do tema segurança aparecia no rodapé da página, de forma discreta, conforme demonstrado na ilustração a seguir.

Ilustração 24: Home Page da CEF.

Fonte: CEF (2014).

Sobre as informações disponíveis na imagem da ilustração 24, ao clicar no item segurança, o usuário poderia acessar sem restrições o conteúdo da página relacionada a segurança nos canais e produtos, abordando os seguintes tópicos: internet *banking*, internet, *e-mail*, mensagens via celular, autoatendimento, agências, cartões Caixa, cheques, Serviço de Atendimento ao Cliente – SAC da Caixa, aprenda sobre segurança, segurança antigolpes. Tais tópicos estão dispostos na ilustração 25.

Ilustração 25: Home Page CEF – Segurança.



Fonte: CEF (2014).

O usuário ao clicar em "Segurança no *Internet Banking* Caixa", recebia orientações sobre a proteção ao acesso. A senha da internet disponibilizava ao correntista o acesso à *Internet Banking* da Caixa, porém a mesma não permitia transações bancárias, dependiam da assinatura eletrônica. O item encerrava com orientações de como utilizar o *Internet Banking* da Caixa com segurança.

A segurança na internet era demonstrada no *site* da CEF e a equiparava com o mundo físico, pelo qual o computador era a casa e precisava ser protegida com muros, grades, cadeados e alarme, enquanto no mundo virtual tais proteções eram as soluções tecnológicas de segurança, como *firewall*, antivírus, *anti-spyware*, *anti-spybot*, etc. Recomendava ao usuário que se informasse sobre o assunto.

Apresentava ainda, orientações de segurança voltadas a *e-mails* que eram utilizados para infectar o computador ou levar o usuário a informar dados em *sites* falsos, através de mensagens contendo promoções, desastres, fofocas, ou simulando ser o próprio *site* do banco. Assim, caso o correntista recebesse e-mail de origem desconhecida ou

mensagens com links, era recomendado que fossem ignoradas ou que se realizasse uma varredura do arquivo pelo antivírus. Tais informações estavam no *site* de igual modo como o representado na ilustração 26.

Ilustração 26: Home Page CEF – Segurança – Segurança na Internet – E-mails.

Fonte: CEF (2014).

Sobre as redes sociais, Facebook, MSN, Twitter, dentre outras, eram demonstradas no *site* como também sendo um canal utilizado por criminosos para clonarem perfis para envio de mensagens a amigos contendo *links* que direcionavam à *sites* para instalação de programas maliciosos, no formato de vídeos ou fotos. As orientações sobre o comportamento nas redes sociais estavam dispostas no site da CEF em 2014 conforme demonstra a ilustração 27.

Ilustração 27: Home Page CEF – Segurança – Segurança na Internet – Redes Sociais.

Fonte: CEF (2014)

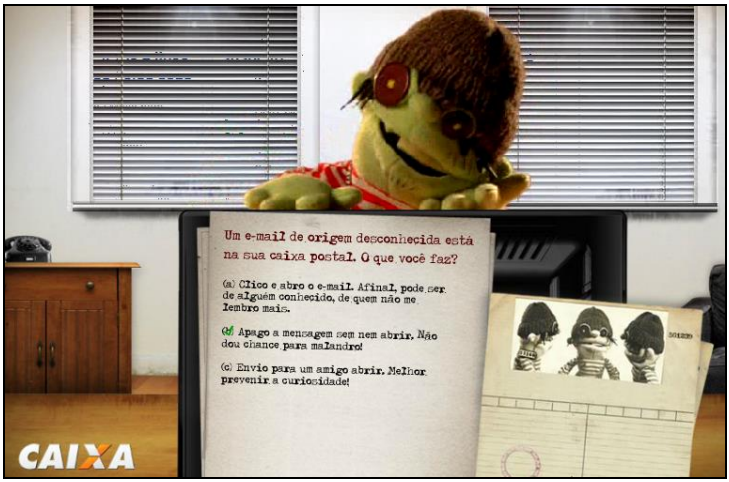
A CEF oferecia aos seus clientes o serviço de mensagens via celular, mediante prévio cadastro, contendo informações sobre as transações de débitos e compras aprovadas, canceladas e negadas, inclusive as realizadas em conta corrente e conta poupança.

O tópico sobre a segurança nos terminais de autoatendimento informava aos usuários e correntistas que todas as salas de autoatendimento eram dotadas de circuito fechado de televisão, que registra as imagens do ambiente e orientava a não aceitar e nem pedir ajuda de estranhos.

Sobre os cartões de débito e crédito haviam uma série de recomendações, como assinar o cartão ao recebê-lo, utilizar senhas de difícil dedução, entre outras.

Havia a demonstração de um vídeo "aprenda sobre segurança", voltado para orientações de segurança na internet e uso do caixa eletrônico, composto por caixas de diálogos contendo perguntas sobre o assunto, interagindo com o usuário, como destaca a ilustração 28.

Ilustração 28: Home Page CEF – Segurança – Aprenda sobre Segurança.



Fonte: CEF (2014)

O último tópico voltado à segurança elencava informações relacionadas aos golpes mais comuns e ações para proteção, além de disponibilizar o telefone da Ouvidoria da Caixa para receber denúncias.

Um dos golpes mais comuns descritos no *site* da CEF era o falso mecânico, pelo qual o golpista, se fazia passar por membro da família, contatava a vítima e relatava que estava com o carro quebrado e para realizar os reparos era preciso realizar um depósito na conta do suposto parente. Na mesma linha, havia o falso sequestro e as falsas premiações ou sorteios, exigindo um depósito para liberação do prêmio.

O *site* da CEF direcionava o usuário para o *site* Antispam.br, com vídeos explicativos sobre segurança na internet.

O usuário poderia acessar no *site* da CEF todas as informações acima descritas, digitando a palavra no campo "digite o que você procura", assim como o correntista após estar no ambiente da sua conta corrente. Porém, as informações não apareciam de forma automática, precisavam ser procuradas, clicando no ícone correspondente ao tema ou digitando a palavra segurança.

Ilustração 29: Home Page CEF – 2016

Fonte: CEF (2014)

Em consulta ao site da CEF em maio de 2016 se observa um novo leiaute, porém com as mesmas informações e orientações aos usuários e correntistas.

5.1.4 Resultados e repercussões – *sites* das três maiores Instituições Bancárias do Brasil

A correlação das informações sobre o tema segurança dispostas nos *sites* das três maiores Instituições Bancárias do Brasil, demonstra que em 2014, estas eram semelhantes. Enquanto, que em 2016, ao contrário do Banco Itaú e da CEF, que mantiveram as orientações, porém com reformulação de leiaute, o Banco do Brasil inovou. Este, por sua vez, manteve as informações relacionadas a sua política de segurança, optando por disponibilizá-las de forma interativa e didática, utilizando histórias e personagens para introdução do tema.

Percebe-se que a política de segurança está apresentada, com orientações claras, objetivas e preventivas aos usuários, independentemente de serem ou não correntistas da instituição. Entretanto, o acesso à política de segurança está sujeito a uma ação do usuário, que não é instigado de forma automatizada a acessá-las.

Ilustração 30: Comparativo dos *sites* das três maiores Instituições Bancárias

	BB		ITAÚ		CEF	
	2014	2016	2014	2016	2014	2016
Acesso direto pelo site principal	SIM	SIM	SIM	SIM	NÃO	NÃO
Disposição do link segurança	Rodapé	Rodapé	Rodapé	Rodapé	Rodapé	Rodapé
Interatividade	NÃO	SIM	NÃO	NÃO	SIM	SIM
Fraude internet orientação	SIM	SIM	SIM	SIM	SIM	SIM
Fraude cartões orientação	SIM	SIM	SIM	SIM	SIM	SIM
Fraude SAA orientação	SIM	SIM	SIM	SIM	SIM	SIM
Engenharia social orientação	SIM	SIM	SIM	SIM	SIM	SIM
Demais Produtos– cheque, boleto, senhas	SIM	SIM	SIM	SIM	SIM	SIM
Análise e-mail suspeito	SIM	SIM	SIM	SIM	NÃO	NÃO

Fonte: elaborado pela autora com base nas informações dos *sites* das três maiores Instituições Bancárias (2016)

A interatividade que permeia a internet não se faz presente nos *sites* da FEBRABAN, BACEN, ou nos bancos estudados. Quando o assunto é segurança, todos dependem de um clique em um *link* pelo usuário. Outro aspecto observado é a posição do *link*, que na maioria dos *sites* se apresenta no rodapé da página, no qual podem passar despercebidos por usuários mais afoitos.

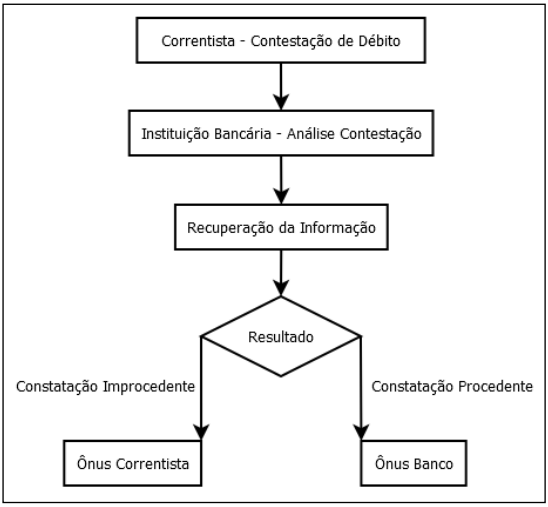
Neste cenário, considerando o imediatismo do ambiente da internet, a divulgação de políticas de segurança de forma mais ativa e provocativa poderá ser uma estratégia a ser adotada, com intuito de informar e esclarecer aos usuários sobre as vulnerabilidades e ameaças que circundam o ciberespaço.

5.2 ANÁLISE DO BANCO DE DADOS DA INSTITUIÇÃO BANCÁRIA ANALISADA

Os dados recuperados da Instituição Bancária analisada relacionados às fraudes eletrônicas, são registrados pela instituição a partir de contestação de débito de seus correntistas, mediante a apresentação de boletim de ocorrência registrado em órgão da segurança pública local.

Após o registro da contestação de débito, a instituição realiza a análise das informações elencadas pelo correntista, confrontando-as com os dados da transação contestada, histórico das transações reconhecidas pelo correntista, para identificar o seu padrão de comportamento e características, além das imagens das câmeras instaladas nas agências e nos caixas eletrônicos. Em seguida, as contestações são processadas como "procedentes", com ônus para a Instituição Bancária, quando é confirmada a fraude eletrônica, ou "improcedentes", com ônus para o correntista, quando as informações recuperadas descartam a fraude, conforme ilustração a seguir:

Ilustração 31: Processo de Contestação de débito.



Fonte: elaborado pela autora - dados recuperados da Instituição Bancária

Para efeitos dessa pesquisa foram trabalhadas com as contestações de fraude eletrônica, registradas no canal da internet e uso de cartão, consideradas procedentes, na qual, o correntista foi vítima e, portanto, foi ressarcido pela Instituição Bancária estudada, no período de 01/01/2014 a 30/06/2014.

Em relação à fraude foram analisadas as seguintes variáveis: local da fraude (cidades da Grande Florianópolis), o tipo de fraude (internet ou cartão), modalidade de fraude conforme o tipo (auxílio de terceiro, token, central de atendimento, internet), canal da fraude (senha da internet, *smatphone*, caixas eletrônicos), tipo de transações (pagamento de boletos, transferências, saques ou compras) e a forma como ocorreu a fraude (ação direta ou indireta do engenheiro social). Para uma melhor seleção dos dados, as fraudes via internet ou cartão foram assim classificadas:

- Auxílio de terceiro: nessa modalidade de fraude via cartão de débito ou de crédito, a engenharia social é utilizada de forma direta, onde o engenheiro social se utiliza de identidade falsa, se passando, na maioria das vezes, por funcionário da Instituição Bancária ou por alguém cortês e prestativo, nas salas de autoatendimento. O objetivo é conquistar a confiança do correntista, realizando golpes como a troca de cartão e visualização da senha digitada nos caixas eletrônicos, retirada de valores do caixa eletrônico, ou oferecimento de vantagem ou fraude de antecipação de recursos, como o bilhete premiado;

- *Token*: o correntista, previamente à utilização do *token* para autenticar as transações financeiras na internet, é vítima da engenharia social de forma indireta, que geralmente se concretiza com o recebimento de *e-mail* falso ou *malwares*, permitindo a captura de suas senhas e dados pessoais;

- Central de atendimento por telefone: neste tipo de fraude, o engenheiro social liga para o correntista ou o aborda nas salas de autoatendimento, se passa por funcionário da Instituição Bancária e o direciona para uma central de atendimento falsa. Ao contatar a central, o correntista é persuadido a entregar os seus dados sigilosos como número do cartão, senhas bancárias, número do CPF, identidade, data de nascimento, entre outros;

- Internet - *internet banking*: para este tipo de fraude, a atuação do engenheiro social é a mesma do *token*, ou seja, com o uso da internet

para obtenção da senha, por *e-mail* falso ou *malwares*, permitindo o acesso aos dados sigilosos do correntista;

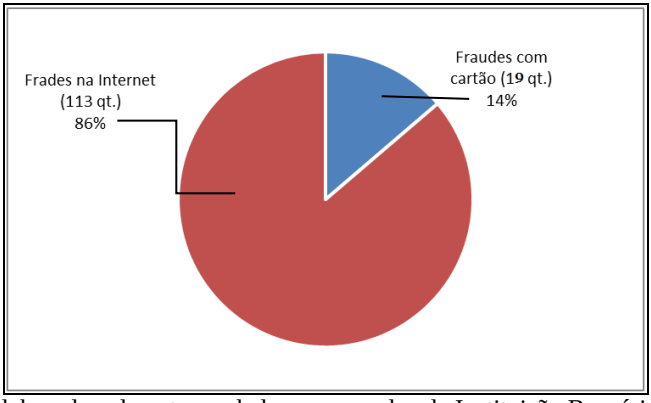
- Gerenciador financeiro, canal alternativo, de autoatendimento, presente no *site* da Instituição Bancária, utilizado pelos correntistas pessoas jurídicas para realização de transações financeiras exclusivas de suas empresas, cooperativas, entidades, entre outras, cujo comprometimento corresponde ao da internet e do *token*, no qual, através de um *malware*, as informações sigilosas da empresa são capturadas e exploradas pelos engenheiros sociais.

A seguir serão demonstrados os resultados obtidos após a análise e processamento das informações do banco de dados da Instituição Financeira estudada.

5.2.1 Informações relacionadas à fraude – resultados e repercussões

As informações recuperadas no banco de dados da Instituição Bancária revelaram que, para o período de 01/01/2014 a 30/06/2014, houve 113 fraudes eletrônicas na *internet banking* e 19 fraudes de cartão, totalizando 132 processos de contestações de débito procedentes na região da Grande Florianópolis, considerando pessoas físicas e pessoas jurídicas, conforme exposto no Gráfico 6.

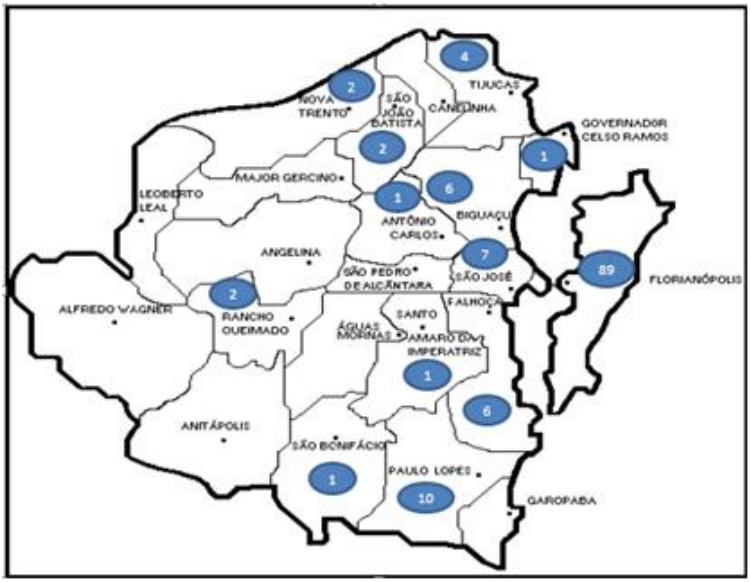
Gráfico 6: Quantidade fraudes de internet e de cartão.



Fonte: elaborado pela autora - dados recuperados da Instituição Bancária (2014)

As fraudes eletrônicas, internet e cartão, estão distribuídas nas cidades que compõem a Grande Florianópolis, conforme a ilustração 32, tendo uma maior concentração na cidade de Florianópolis, com um total de 89 fraudes, enquanto que as 42 fraudes restantes estão distribuídas nas demais cidades.

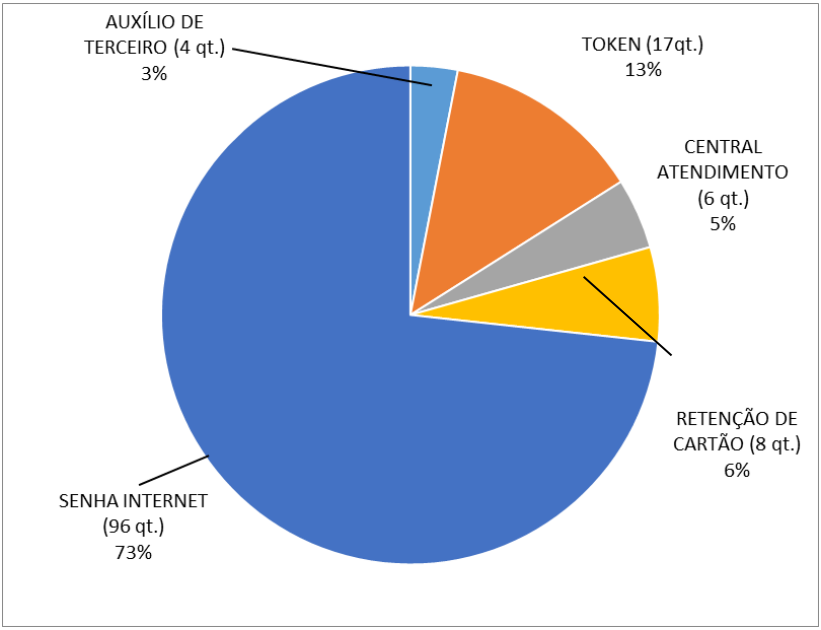
Ilustração 32: Fraudes por município da Grande Florianópolis.



Fonte: GRANFPOLIS (2014) e elaborado pela autora - dados recuperados da Instituição Bancária (2014)

Das 132 fraudes eletrônicas, 96 foram na modalidade via internet – *internet banking*, representando 73%, seguidas do *token* com 17 fraudes, ou seja, 13%, oito fraudes do tipo retenção de cartão, correspondendo a 6%, sete delas foram via central de atendimento, significando 5%, e 4 quatro fraudes com auxílio de terceiros, sendo 3%, desta forma representada no Gráfico 7.

Gráfico 7: Quantidade de fraudes por modalidade.

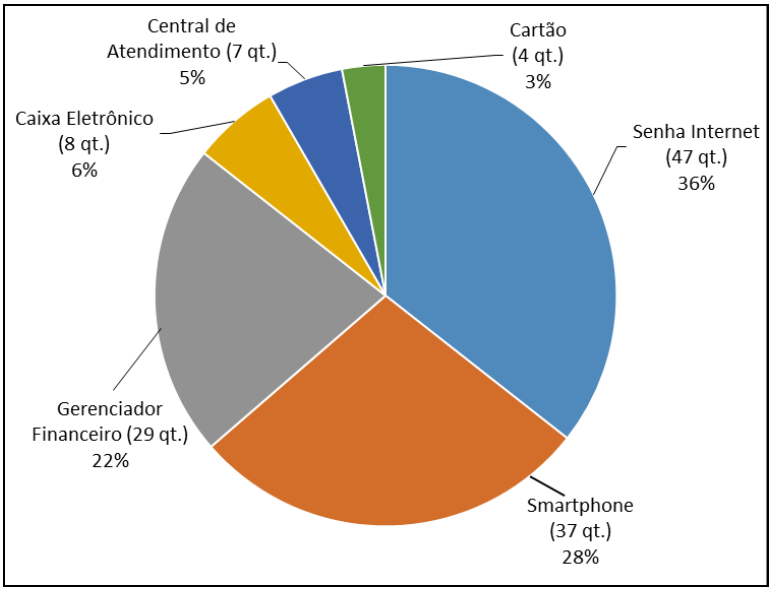


Fonte: elaborado pela autora - dados recuperados da Instituição Bancária (2014)

As fraudes eletrônicas estão concentradas na internet - *internet banking* – como se observa no gráfico 7, o que implica dizer que a internet é o canal de maior concentração de fraudes financeiras. Portanto, nela o risco está, quando comparado com os demais meios, considerando a população da pesquisa. A constância entre os indivíduos, as tecnologias e os processos informacionais fazem parte da gestão da segurança da informação (SVEEN, TORRES E SARIEGI, 2009). Porém, tal constância é discutível quando a tecnologia e os processos informacionais são ameaçados.

Considerando a variável canal, ou seja, onde a fraude ocorre, aquele que apresentou maior representatividade foi a internet, seguida dos *smartphones* e por gerenciador financeiro (ambiente da internet destinado às transações financeiras de pessoas jurídicas). No Gráfico 8, está demonstrado os canais utilizados para as fraudes eletrônicas.

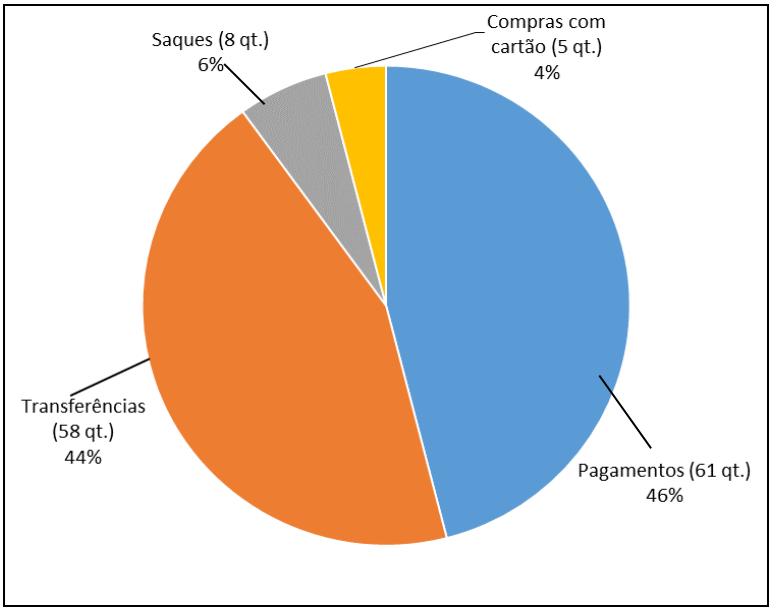
Gráfico 8: Canais das fraudes eletrônicas.



Fonte: elaborado pela autora - dados recuperados da Instituição Bancária (2014)

Os tipos de transações realizadas pelos engenheiros sociais após obterem as informações sigilosas dos correntistas da Instituição Bancária foram: pagamento de boletos, com um total de 61 transações fraudulentas, seguidas de 58 transferências, logo após aparecem os saques, no total de oito, e as compras com cartão, com cinco registros. Tais dados assim se apresentam no Gráfico 9

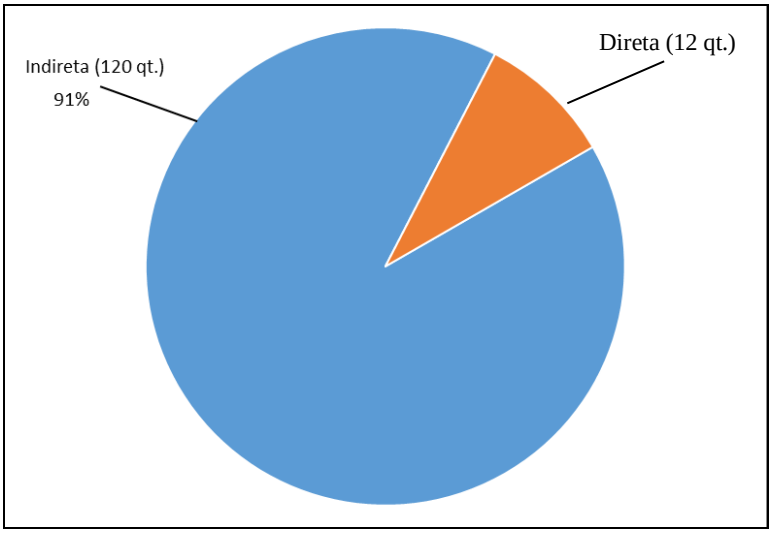
Gráfico 9: Tipos de transações financeiras fraudadas.



Fonte: elaborado pela autora - dados recuperados da Instituição Bancária (2014)

Ao se analisar a forma de atuação do engenheiro social para obter as informações sigilosas dos correntistas da Instituição Bancária identificou-se que a ação indireta é determinante para o sucesso da fraude; utilizando os recursos tecnológicos para persuadir os correntistas a instalarem programas maliciosos em seus computadores, permitindo assim, o acesso às informações. Tal ação não requer uma atuação mais sofisticada, pois depende apenas de um click do correntista em um *link* falso para contaminar o computador ou o *smartphone*. Já a ação direta requer uma maior preparação do engenheiro social, pois a forma da abordagem e a persuasão são articuladas previamente e projetadas conforme as características da vítima, possibilitando a opção por uma ação mais emocional ou racional. Portanto, considerando a variável de atuação do engenheiro social, sendo de forma indireta ou direta, se obteve-se o seguinte resultado:

Gráfico 10: Forma de atuação do engenheiro social.



Fonte: elaborado pela autora - dados recuperados da Instituição Bancária (2014)

A ação direta, como nos casos de troca de cartão do correntista nas salas de autoatendimento, requer uma maior cautela e preparação do engenheiro social, que escolhe a sua vítima considerando as suas características e vulnerabilidades, que serão abordadas na próxima subseção.

Para identificar a forma e qual tipo de programa malicioso foi instalado no equipamento do correntista, seria necessário a Instituição Bancária realizar perícia no equipamento. Porém, considerando a quantidade de fraudes em todo território nacional, a instituição não realiza este tipo de procedimento. Desta forma, adota programas de computadores e parâmetros próprios para identificar a fraude e a classifica como sendo fraude de internet ou de cartão.

5.2.2 Informações sobre as características comuns dos correntistas fraudados – resultados e repercussões

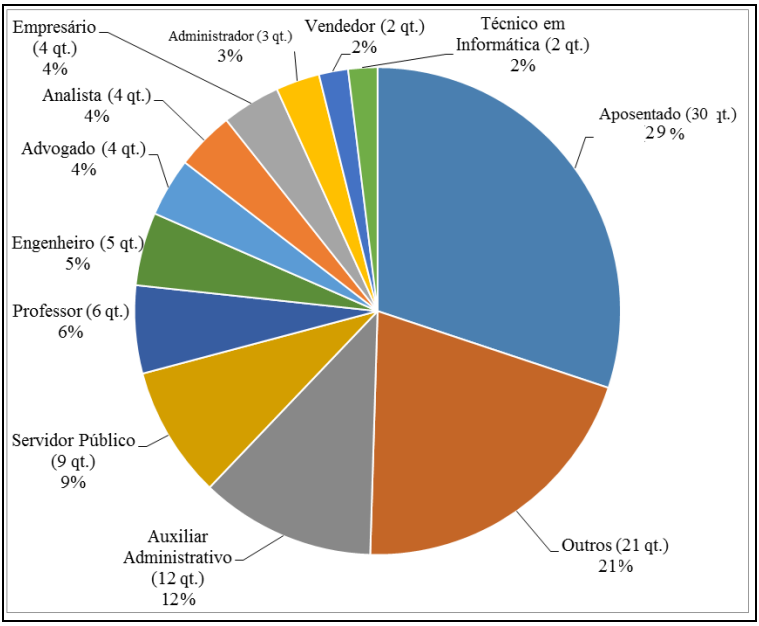
As variáveis estudadas com objetivo de identificar as principais características dos correntistas vítimas da engenharia social, implicando

em fraudes eletrônicas foram: a profissão, renda, grau de escolaridade, faixa etária e gênero.

Do total das fraudes eletrônicas, 102 ocorreram com pessoas físicas e 30 com pessoas jurídicas. Para um levantamento mais fidedigno das características dos correntistas fraudados, considerando as variáveis que serão estudadas, os dados a seguir estão relacionados às pessoas físicas.

Para a variável profissão foram considerados os dados cadastrados no sistema da Instituição Bancária estudada, dos quais constatou-se que as pessoas com maior comprometimento das suas informações sigilosas são os aposentados, com 31 ocorrências, o que equivale a 23% dos casos, em segundo lugar aparece a profissão de auxiliar administrativo (12 casos, 15% do total) e em terceiro a profissão de servidor público (nove casos, equivalendo a 9% do total), como se observa no Gráfico 11.

Gráfico 11: Correntistas fraudados – profissão.



Fonte: elaborado pela autora - dados recuperados da Instituição Bancária (2014)

Considerando a variável "renda" da pesquisa, utilizou-se os parâmetros seguidos pelo IBGE, que divide suas amostras para efeito de pesquisa em cinco faixas de renda ou classes sociais, conforme a TABELA 2, válida para o ano de 2014, considerando o salário mínimo de R$ 725,00 (setecentos e vinte e cinco reais).

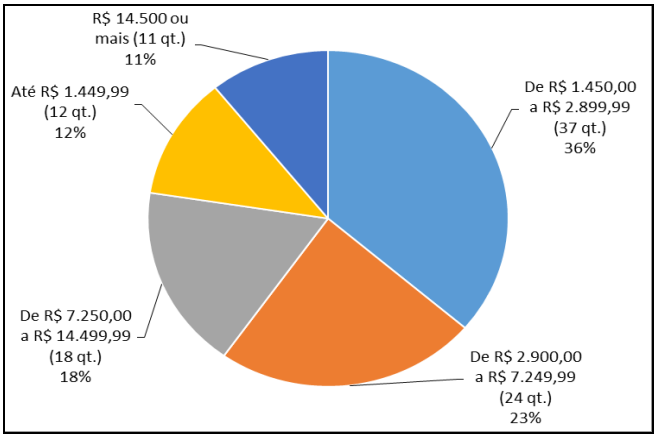
Tabela 2: Critério do IBGE para definição de classes sociais.

CLASSE	SALÁRIOS MÍNIMOS (SM)	RENDA FAMILIAR (R$)
A	Acima 20 SM	R$ 14.500 ou mais
B	10 a 20 SM	De R$ 7.250,00 a R$ 14.499,99
C	4 a 10 SM	De R$ 2.900,00 a R$ 7.249,99
D	2 a 4 SM	De R$ 1.450,00 a R$ 2.899,99
E	Até 2 SM	Até R$ 1.449,99

Fonte: elaborado pela autora - IBGE, 2014

Tendo como parâmetro o critério de definição do IBGE para a variável renda, a pesquisa revelou que a classe D é aquela que apresenta a maior concentração de fraude eletrônica, representada pelos correntistas da Instituição Bancária com renda mensal entre 02 a 04 salários mínimos, seguida das classes C, B, E e A, como podemos observar:

Gráfico 12: Correntistas fraudados – renda.

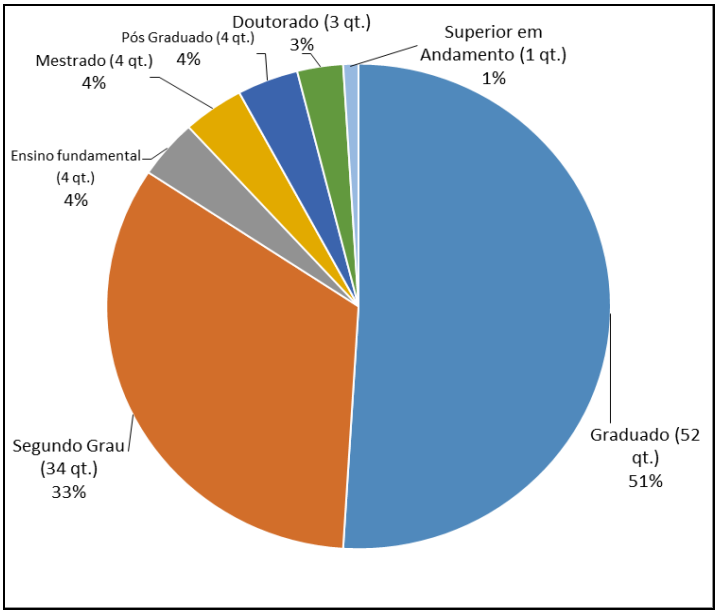


Fonte: elaborado pela autora - dados recuperados da Instituição Bancária (2014)

O grau de escolaridade dos correntistas fraudados é a terceira variável explorada na presente pesquisa, cujos parâmetros do IBGE foram seguidos: ensino fundamental, ensino médio, superior completo, acrescidos dos dados da Instituição Bancária, os pós-graduados, mestres (mestrado concluído) e doutores (doutorado concluído).

Os resultados colhidos demonstraram que 52 correntistas vítimas de fraudes eletrônicas, são graduados, representando 51%, em segundo lugar aparecem os correntistas com o segundo grau completo, no total de 34 pessoas (33%) e em terceiro lugar aparecem os que cursaram o ensino fundamental, os mestres e doutores, no total de quatro vítimas, o que corresponde a 4%.

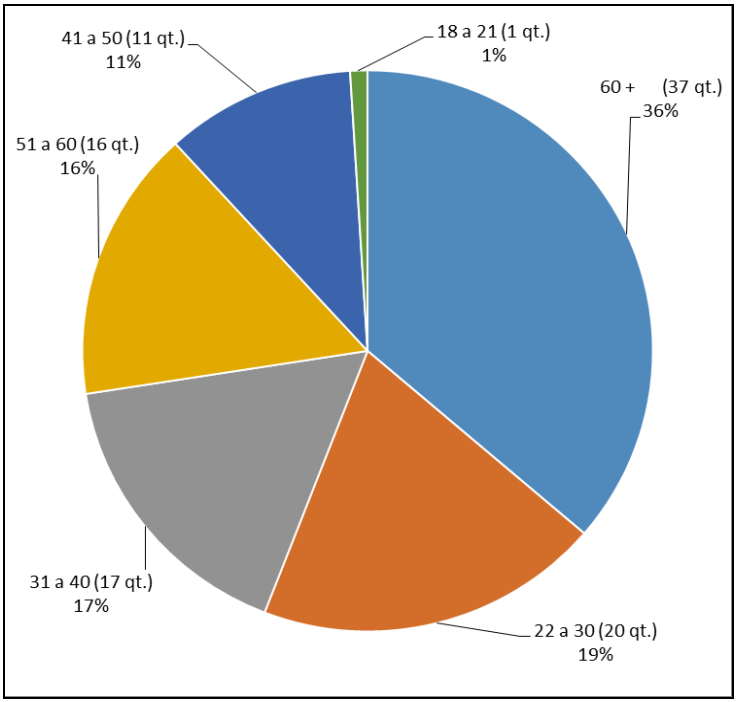
Gráfico 13: Correntistas fraudados – grau de escolaridade.



Fonte: elaborado pela autora - dados recuperados da Instituição Bancária (2014)

Para a variável "faixa etária", 37 pessoas físicas com mais de 60 anos foram vítimas de fraude, representando 36%, seguidas dos classificados entre 22 a 30 anos, com 20 pessoas, ou seja, 20%, cujos detalhes podem ser observados no gráfico 14.

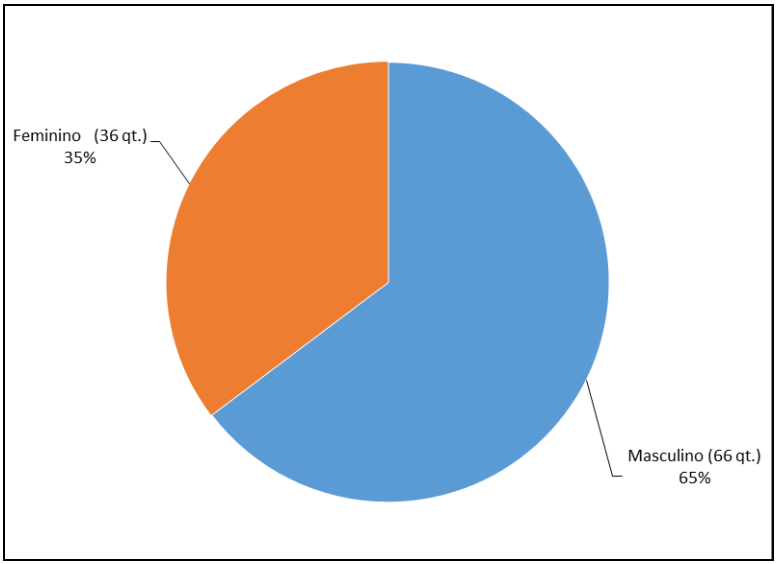
Gráfico 14: Faixa etária dos correntistas fraudados.



Fonte: elaborado pela autora - dados recuperados da Instituição Bancária (2014)

As fraudes eletrônicas se concentraram no gênero masculino com 66 correntistas fraudados, representando 65%. Em contrapartida, 36 mulheres foram fraudadas nos seis primeiros meses do ano de 2014 na região da Grande Florianópolis, correspondendo a 35% do total das fraudes, como segue:

Gráfico 15: Correntistas fraudados – gênero.



Fonte: elaborado pela autora - dados recuperados da Instituição Bancária (2014)

Ao se compilar as informações obtidas após a análise dos elementos em relação a fraude e as características do correntista, conclui-se que as fraudes eletrônicas estão concentradas no *site* da instituição financeira, mediante a obtenção dos dados para acesso à conta corrente, com o número da agência, da conta e a respectiva senha, através da ação indireta do engenheiro social persuadindo o correntista a acessar *links* falsos, permitindo a instalação de *trojans*, ao passo que as ações diretas se apresentam de forma mais tímida.

5.3 PESQUISA EXPLORATÓRIA - ENTREVISTA

Com objetivo de identificar a relação entre os correntistas vítimas das fraudes eletrônicas e as suas informações sigilosas, optou-se por adotar como instrumento de pesquisa a entrevista, cuja amostra foi selecionada a partir do banco de dados disponibilizado pela Instituição Bancária estudada.

Foram selecionados de forma aleatória 20% de cada tipo de fraude para compor o público alvo da pesquisa. Portanto, foram entrevistados 23 correntistas vítimas de fraude via internet e quatro com o uso do cartão. Foi elaborado um roteiro de entrevista, de antemão convencionado, aplicado aos correntistas vítimas de fraudes eletrônicas, seguindo os 20% para cada modalidade de fraude.

A seguir serão expostos os aspectos observados e as respectivas apreciações dos dados da pesquisa.

5.3.1 Entrevista – resultados e repercussões

O objetivo da interpretação dos dados tabulados é analisar o processo informacional dos correntistas das Instituições Bancárias, cujos dados sigilosos foram comprometidos. Portanto, para garantir o sigilo das informações disponibilizadas pela Instituição Bancária pesquisada, sobre os dados de seus correntistas, e ainda considerando os princípios éticos que circundam a entrevista como ferramenta de pesquisa, não serão revelados os nomes dos entrevistados, sendo estes diferenciados por números cardinais.

Para a primeira pergunta da entrevista, quais das informações pessoais relacionadas à Instituição Bancária, são consideradas como sigilosas, dos 23 correntistas vítimas de fraude via internet, 21 deles consideram que todas as informações registradas no sistema da Instituição Bancária são sigilosas, por envolver informações pessoais, como o número da identidade, do CPF, endereços, telefones, filiação, cargo, renda e principalmente as senhas de acesso aos canais de atendimento, sendo assim respondidas pelos correntistas vítimas de fraude pela internet: “considero todas as informações sobre mim registradas pela instituição como sigilosas, principalmente após a fraude” (entrevistados 1, 2, 3, 4, 5, 7, 8, 10, 11, 12, 13, 14, 16, 18, 19, 20 e 21); “considero as senhas como informações sigilosas” (entrevistado 6, 9, 15, 17 e 22), “para mim as senhas e os números dos cartões são informações sigilosas” (entrevistados 6, 15 e 23).

Constatação congênere verificou-se para as fraudes com uso de cartão, sendo que todos os quatro entrevistados consideram todas as informações registradas pela Instituição Bancária como sigilosas, desta forma representada:

Tabela 3: Correntistas fraudados (internet e cartão) – tipos de informações consideradas sigilosas.

1. Quais são as suas informações pessoais relacionadas à instituição financeira que você considera como sigilosas?	
Todas	21
Senhas	3
Senhas e Número do Cartão	2
Senhas e Cartões	1
Total	27

Fonte: elaborado pela autora – resultado da entrevista (2014)

Para o processo organizacional do fluxo da informação, se procurou levantar como os correntistas, cujas informações sigilosas foram comprometidas, procuravam se manter informados sobre a segurança das suas informações. Para tanto, foi feito o seguinte questionamento: quais são os meios ou canais que você utiliza para se manter informado sobre as formas de proteção das informações financeiras sigilosas?

Como resultado foi identificado que nove deles procuram o funcionário da Instituição Bancária, cinco dos entrevistados procuram se manter informados buscando funcionários ou o site da instituição e quatro deles não procuram informações sobre o assunto. A compilação dos dados demonstra o seguinte cenário:

Tabela 4: Correntistas fraudados (internet e cartão) – canais de informação.

2. Quais são os canais que você utiliza para se manter informado sobre as formas de proteção das suas informações sigilosas?	
Funcionário da Instituição Bancária	9
Funcionário e site da Instituição Bancária	5
Nenhum	4
Funcionário Insituição Bancária e Internet	2
Televisão	2
Site da Insituição Bancária e Internet	2
Site da Insituição Bancária	1
Internet	1
Site G1 Tecnologia	1
Total	27

Fonte: elaborado pela autora – resultado da entrevista (2014)

O mapeamento das tipologias dos canais de informação utilizados, sendo estes internos ou externos à Instituição Bancária, é essencial para se identificar quais os canais mais utilizados pelos correntistas, podendo inclusive ser alicerce para futuras pesquisas voltadas ao desenvolvimento da melhoria de tais meios. Sobre este aspecto, a questão formulada foi assim descrita: "a Instituição Bancária lhe orientou sobre o cuidado com informações sigilosas, como as senhas? Se sim, quem?".

Identificou-se que os correntistas fraudados não foram orientados sobre o cuidado com as suas informações sigilosas e, quando recebidas as informações, foram repassadas superficialmente, sem o devido esclarecimento sobre a forma como o comprometimento das informações poderia ocorrer. Seguem alguns relatos dos correntistas vítimas de fraudes eletrônicas: "não recebi nenhuma orientação" (entrevistados 1, 2, 5, 8, 9, 11, 13, 17, 18, 19, 21 e 23); "recebi orientação superficial do funcionário da instituição" (entrevistados 3 ,4 ,6 ,7 ,10, 12, 14, 15, 16 20 e 22).

Assinalou-se que, dos entrevistados, 13 foram orientados de forma superficial e 14 não receberam qualquer esclarecimento sobre o assunto. Elementos estes que implicam na necessidade de melhoria por

parte da Instituição Bancária nos canais de comunicação sobre a informação, envolvendo todo o corpo funcional e os canais destinados à divulgação de orientações sobre o trato da informação sigilosa, agregando valor à informação sigilosa. Segue o resultado:

Tabela 5: Correntistas fraudados (internet e cartão) – orientações sobre o cuidado com as informações sigilosas.

3. A Instituição Financeira lhe orientou sobre o cuidado com informações sigilosas, como as senhas? Se sim, quem?	
Não	14
Sim - Funcionário da Instituição Bancária	13
Total	27

Fonte: elaborado pela autora – resultado da entrevista (2014)

Com a intenção de identificar se o correntista vítima de fraude eletrônica estaria suscetível novamente a ser fraudado, foi elaborada a questão: atualmente você estaria suscetível a ser vítima de uma nova fraude com as mesmas características e abordagens? Uma fração significativa dos entrevistados, ou seja, 10 deles, relataram que não estariam suscetíveis a cair novamente no engodo da engenharia social, enquanto que sete deles declararam que não seriam novamente vítimas por não utilizarem mais o canal explorado pelo engenheiro social, por perda da confiança e credibilidade, assim mencionados: "não caio mais no golpe, pois perdi a confiança no canal e não o utilizo mais" (entrevistados 1, 13, 16, 17, 21 e 23). No entanto, três responderam que poderiam ser vítimas sim de nova engenharia social e com isso terem prejuízos financeiros.

Tabela 6: Correntistas fraudados (internet e cartão) – vítimas de novas fraudes.

4. Atualmente você estaria suscetível de vítima de uma nova fraude com as mesmas características e abordagens?	
Não	10
Não - não utiliza mais o canal fraudado	7
Talvez	3
Sim	3
Não sabe	2
Sim - o hacker consegue fraudar e tenho medo	1
Não - instalei antivírus	1
Total	27

Fonte: da autora - dados da pesquisa.

Para os casos de atuação do engenheiro social de forma direta ou indireta contra o correntista, os entrevistados foram indagados por que decidiram fornecer as suas informações sigilosas à terceiros e a entrevista revelou que a confiança foi o principal sentimento explorado para persuasão. Porém, 23 entrevistados (85,19%) não identificaram a atuação do engenheiro social, inclusive descreveram que não sabem como as suas informações sigilosas foram comprometidas.

Tabela 7: Correntistas fraudados (internet e cartão) – repasse de informações sigilosas.

5. Por que você decidiu fornecer as suas informações sigilosas para o engenheiro social?	
Não decidi fornecer as informações, inclusive não sei como tiveram acesso aos meus dados para cometer a fraude.	23
Confiança na pessoa que me abordou, pois se passou por funcionário da instituição bancária.	3
Confiança na pessoa que me abordou, parecia gente do bem.	1
Total	27

Fonte: elaborado pela autora – resultado da entrevista (2014)

Em alguns casos, a vítima foi enganada pelo engenheiro social, que se passou por funcionário da instituição, por demonstrar conhecimento, simpatia, gentileza no momento do auxílio na sala de autoatendimento. Os relatos dos correntistas revelaram tais sentimentos:

> A pessoa se passou por funcionário, disse que iria me ajudar a bloquear o cartão para que não houvesse problemas, pareceu ser honesto e na hora não desconfiei de nada, pois achei que estava em boas mãos (ENTREVISTADO 1).

> Fui abordado na sala de autoatendimento por um homem bem vestido, com boa intenção e me auxiliou a ligar para a central de atendimento do banco, assim, poderia bloquear o cartão que ficou trancado no terminal e aproveitar para pedir outro. Achei que era funcionário, mas me enganei e estou indignado por não ter notado que se tratava de golpe (ENTREVISTADO 4).

Um dos principais construtos da sustentação de qualquer negócio, é a confiança, assim, a perda de confiança no canal pode vir a restringir o crescimento da Instituição Bancária, podendo causar a diminuição de seus ativos. A segurança corresponde a uma percepção, uma sensação. Dessa forma, caso as pessoas não venham a se sentir seguras, dificilmente virão a mudar esta percepção, fato este confirmado pela pesquisa.

Para avaliar o grau de satisfação dos entrevistados em relação às orientações recebidas da Instituição Bancária sobre as fraudes as quais estariam sujeitos, os entrevistados revelaram que as orientações recebidas são ruins e precisam melhorar, para tanto, assim se manifestaram: “ruim, a instituição deveria cuidar melhor sobre a segurança das informações e comunicar sobre os tipos de fraudes existentes”(entrevistado 6); “ruim, é necessário melhorar as informações repassadas aos correntistas e o sistema da instituição” (entrevistado 7); “ruim, a instituição deveria instruir melhor os correntistas sobre os tipos de golpes” (entrevistado 8); “ruim, falta informação sobre o assunto” (entrevistado 9); “ruim, os funcionários deveriam conversar e explicar melhor sobre as fraudes, pois não adianta ligar depois que a fraude aconteceu e hoje estou inseguro” (entrevistado 25); “ruim, falta um folder com exemplos de fraudes, como o utilizado em postos de saúde para alertar sobre doenças, assim, as pessoas preveniriam riscos futuros” (entrevistado 27). Na tabela 8 será apresentado o resultado geral das respostas.

Tabela 8: Correntistas fraudados (internet e cartão) – informações recebidas da Instituição Bancária.

6. Como você avalia a orientação da Instituição Bancária em relação as fraudes que você estaria suscetível? Há algum ponto a ser melhorado?	
Ruim	11
Boa	8
Regular	8
Total	27

Fonte: elaborado pela autora – resultado da entrevista (2014)

Para ampliar a liberalidade da entrevista, foi solicitado aos entrevistados se teriam interesse em abordar algum tópico sobre a segurança da informação e engenharia social, não elencados nas questões anteriores. Aqueles que se manifestaram arrolaram a necessidade de a Instituição Bancária promover de forma mais eficaz o tema sobre segurança das informações sigilosas, principalmente com exemplos práticos, seja no processo de abertura de conta corrente, durante o acesso ao *site* e mensagens esporádicas, via SMS, em falas assim descritas:

Tabela 9: Correntistas fraudados (internet e cartão) – demais manifestações.

7. Você gostaria de abordar algum tópico que não foi contemplado na entrevista, mas considera relevante para esta pesquisa?	
A Instituição Bancária deveria divulgar mais informações sobre as fraudes.	9
Não respondeu.	6
A Instituição Bancária deveria divulgar mais informações sobre as fraudes e melhorar o sistema.	5
Perdi a confiança na Instituição Bancária.	3
Não utilizo mais o canal por não confiar.	1
A Instituição Bancária deveria explicar melhor sobre os limites de transações na Internet.	1
É difícil acompanhar as informações sobre o assunto pela velocidade da tecnologia usada para o mal.	1
A fraude pode acontecer com qualquer pessoa.	1
Total	27

Fonte: elaborado pela autora – resultado da entrevista (2014)

A perda de confiança na Instituição também foi elencada. Consequentemente alguns dos entrevistados descreveram que optaram por outra instituição para realizar as suas transações financeiras, “perdi a confiança e retiro o dinheiro e o uso em outro lugar” (entrevistado 1).

Relataram, também, a dificuldade em se manter atualizados sobre o assunto, considerando a velocidade como novos golpes surgem explorando os avanços da tecnologia: “hoje em dia é muito difícil acompanhar as informações, pois elas são muito velozes. Todos os dias são criadas novas ferramentas para um bom ou mau uso” (entrevistado 26).

Conforme constatado, a engenharia social está presente no cotidiano dos correntistas de instituições bancárias. Em certas formas de atuação não são notados ou são confundidos com pessoas de confiança, o que repercute no rompimento da proteção da informação. A informação passa a ser exposta e utilizada, causando prejuízos financeiros, descrédito dos canais e da própria Instituição Bancária, colocando em risco a sua imagem. A reversão deste cenário depende da divulgação de informações sobre o assunto de forma proativa e interativa com os usuários e correntistas de Instituições Bancárias.

6 CONCLUSÕES E PERSPECTIVA PARA NOVAS PESQUISAS CIENTÍFICAS

Para a finalização da pesquisa serão descritas a seguir as considerações finais, sistematizadas segundo os objetivos estabelecidos na pesquisa. Com o propósito de contribuir para novas pesquisas científicas serão elencadas algumas propostas de estudos relacionadas ao assunto aqui abordado.

6.1 CONCLUSÕES

O silogismo da pesquisa está relacionado diretamente ao objetivo geral proposto, isto é, analisar a segurança da informação de usuários de Instituições Bancárias a partir da perspectiva da engenharia social.

A análise do estudo apresentou como universo da pesquisa correntistas de Instituições Bancárias, vítimas da engenharia social, e a sua analogia com as informações sigilosas, considerando as orientações recebidas da Instituição Bancária e de outras fontes, como *sites* da internet. Em consequência da análise preliminar, foi constatada a necessidade de um trabalho científico composto por tais variáveis, acrescentando inovações sobre o assunto.

Conforme o resultado da pesquisa, conclui-se que a principal vulnerabilidade da segurança da informação são as pessoas, pois não há recursos tecnológicos suficientes para garantir a segurança da informação mediante usuários que as desconhecem ou as utilizam de forma inadequada. Tal assertiva corrobora com os autores Kevin Mitnick e Mario Peixoto quando conceituam a engenharia social.

As técnicas de engenharia social de maior efetividade em relação ao comprometimento da segurança da informação foi o envio de *phising* aos usuários de Instituições Bancárias, na qual o engenheiro social, mediante uma ação indireta, induz o usuário a acessar *sites* falsos como verdadeiros, permitindo em tal ambiente a captura das suas informações sigilosas. Fato este confirmado pela pesquisa, quando foi identificada a internet como o canal de maior destaque no comprometimento das informações sigilosas de usuários de Instituições Bancárias, bem como, quando os entrevistados revelaram que desconheciam a forma como as suas informações sigilosas foram violadas.

Considerando os pilares da segurança da informação, a confidencialidade, a integridade e a disponibilidade é necessário atrelar os recursos tecnológicos e a conscientização de pessoas em relação aos subterfúgios utilizados pelos engenheiros sociais para garantir a tríade balizadora da segurança da informação.

A educação voltada para a gestão da a segurança da informação nas organizações e de seus usuários, como correntistas de Instituições Bancárias é um importante aliado ao enfrentamento desta ameaça social, a engenharia social.

O desconhecimento das normas de política de segurança pelos usuários de Instituições Bancárias, também é observado na presente pesquisa, considerando a forma como são divulgadas pelas Instituições Bancárias, na qual, o usuário precisa ir em busca da informação, não havendo interatividade. Esta vulnerabilidade é classificada como vulnerabilidade humana da segurança da informação, explorada pela engenharia social.

Como melhoria da segurança da informação as Instituições Bancárias poderiam dispor em seus *sites* as informações já existentes sobre a política de segurança da informação, porém, de forma mais interativa, não dependendo da ação única e exclusiva dos usuários, através de alertas de segurança antes de realizarem uma transação financeira, além de concordância com tais políticas no primeiro acesso realizado pelo usuário.

A seguir, demonstra-se as variáveis estudadas em relação à fraude e ao correntista vítima da engenharia social, considerando como referência somente aqueles que concentraram a maior percentagem.

Nas condicionantes estudadas em relação à fraude eletrônica, os engenheiros sociais concentraram a sua atuação na cidade de Florianópolis, com 89 eventos de sucesso, apontando para a captura dos dados do correntista para acesso à conta bancária com auxílio da internet. Isto posto, a abordagem de destaque do engenheiro foi a forma indireta, persuadindo os correntistas a acessarem *links* espúrios e a instalarem *malwares* em seus computadores e *smartphones*. A fraude eletrônica foi concretizada, após o acesso à conta corrente dos correntistas e pagamento de boletos não reconhecidos, ensejando na abertura de processo de contestação de débito em face à Instituição Bancária.

Vislumbrando as variáveis dos correntistas fraudados, as principais vítimas da engenharia social foram homens, aposentados,

com mais de 60 anos, da classe social D, que recebem em média de 2 a 4 salários mínimos.

Os correntistas estudados consideram que todas as informações disponibilizadas à Instituição Bancária são de natureza sigilosa, portanto, procuram se manter informados sobre a segurança de tais informações acessando o *site* da própria instituição ou *sites* correlatos. Revelaram, ainda, que não receberam orientações precisas da Instituição Bancária referentes à proteção das suas informações sigilosas, bem como a forma que poderiam ser acometidas.

Os correntistas que foram vítimas de forma direta da ação dos engenheiros sociais para obtenção das informações valoradas ressaltaram que foram ludibriados, devido à atuação do engenheiro social ter sido convincente, transmitindo confiança, conhecimento, simpatia e gentileza.

Tais conclusões corroboraram com o referencial teórico estudado, no qual, as ameaças advindas da tecnologia, aliadas à mobilidade e compartilhamento social, estão associadas diretamente ao comprometimento das informações.

Para a hipótese levantada foi possível chegar à conclusão que a engenharia social compromete a segurança da informação dos usuários de Instituições Bancárias. A segurança da informação é uma preocupação dos usuários de Instituições Bancárias e estas divulgam em seus *sites* orientações relacionadas ao assunto.

O tópico inicial da pesquisa demonstrou os conceitos norteadores do tema e a sua interação com a Ciência da Informação, relacionando-os e evidenciando o desafio da segurança da informação em proteger informações valoradas disponíveis nas Instituições Bancárias.

Isto posto, ao referendar o estudo com o embasamento bibliográfico, conclui-se que a segurança das informações sigilosas dos correntistas de uma Instituição Bancária é de responsabilidade de tais organizações, independente do canal escolhido para obtenção de serviço. Porém, as pessoas detentoras de tais informações fazem parte do processo de proteção e, para tanto, precisam ser orientadas.

Para Coelho, Rasma, Morales (2013), a concessão de ideias para um determinado dado pelo usuário de forma natural ou lógica é o que corresponde à informação, sendo esta valorada quando representa um ativo informacional, cuja forma de manejo poderá repercutir em algum prejuízo, seja ele financeiro ou de natureza subjetiva, como a imagem.

Em consonância, Sêmola (2014), destaca que a informação acrescida de elementos de valor corresponde a um ativo, objeto de proteção da segurança da informação.

A segurança da informação está relacionada diretamente à Ciência da Informação, esta de natureza multidisciplinar e que dispõe de uma vertente interligada ao estudo do usuário, suas características e seu comportamento, considerando os sistemas informacionais.

Para tanto, a segurança da informação está ameaçada no ciberespaço pelos *cibercrime*s, bem como em locais de interação direta entre correntistas e Instituição Bancária, como nas salas de autoatendimento, tendo a engenharia social como balizadora de práticas ilícitas e comprometimento das informações valoradas. Os subterfúgios utilizados pelos engenheiros sociais estão voltados para a manipulação de suas vítimas, explorando vulnerabilidades comportamentais e sentimentos de confiança.

Conclui-se, também, que as Instituições Bancárias promovem em seus *sites* a divulgação de alertas voltados à segurança da informação, atingindo assim, o segundo objetivo específico da pesquisa. Porém, o acesso à tais informações dependem da iniciativa do correntista em procurar a informação. Não foi identificada interatividade instigadora do tema em tais ambientes.

Os correntistas das Instituições Bancárias, de posse de orientações superficiais sobre o tema, oriundas de funcionários, *sites* e internet, ou em determinadas casos, sem qualquer orientação, se aventuram pelos diversos canais disponibilizados para realizarem as suas transações financeiras, estando vulneráveis ao ambiente e suscetíveis de serem vítimas da engenharia social. Ao identificar tais vulnerabilidades, o engenheiro social explora o comportamento dos correntistas e, de posse das informações sigilosas, realiza as fraudes eletrônicas, ludibriando a vítima que se rende às suas técnicas de persuasão.

A sensibilidade das pessoas ao reconhecerem a importância de protegerem as suas informações sigilosas da atuação dos engenheiros sociais, tendo ciência do subterfúgio utilizado, dependem da sua conscientização. A educação voltada para a gestão da segurança da informação nas organizações e de seus usuários, como correntistas de Instituições Bancárias, é um importante aliado ao enfrentamento dessa ameaça social, a engenharia social.

Pode-se observar a presença de um círculo vicioso quando se analisa a simbiose entre tecnologia e segurança, visto que na medida em que os recursos tecnológicos são incrementados e utilizados pelos indivíduos da sociedade da informação, identifica-se o aumento de ameaças que introduzem vulnerabilidades nos ambientes digitais, sendo necessário o desenvolvimento de novas ferramentas tecnológicas para controlá-las.

A sociedade da informação conectada em rede é uma forma de organização social instrumentalizada pela Internet, desenvolvida em um ciberespaço. As relações sociais se solidificam no ciberespaço através das interações dos indivíduos, que ultrapassam a passividade, promovem escolhas e influenciam o coletivo. A Internet, aliada aos avanços tecnológicos, possibilita a interação de conhecimento e de ideias de forma instantânea, pois as barreiras temporais e espaciais foram ultrapassadas pelo dinamismo estrutural do sistema, caracterizado pela liberdade e flexibilidade.

As experiências dos usuários da Internet e as suas interações com o ambiente são os balizadores para o mapeamento de características e padrões de comportamento estudados pela Ciência da Informação.

Na Internet o usuário se sente protegido contra ameaças físicas, porém a rede propicia uma ameaça silenciosa, colocando em risco a segurança da informação dos usuários. Este padrão de comportamento se transforma em uma vulnerabilidade no ciberespaço, explorada pelos engenheiros sociais.

As invasões de sistemas e a disseminação de programas espúrios são as atividades de maior relevância dos engenheiros sociais que ameaçam a segurança da sociedade da informação. Estes atores sociais se beneficiam de informações sigilosas e a sua presença no ciberespaço impulsiona o desenvolvimento de instrumentos tecnológicos que venham a neutralizar a sua ameaça, fazendo parte também do dinamismo da rede.

O conhecimento pelos usuários da Internet das ferramentas utilizadas pelos engenheiros sociais nas suas práticas criminosas é essencial para os auxiliarem na proteção contra as ameaças presentes na rede. Assim, a segurança da informação é um processo dinâmico e complexo, cuja efetividade está alicerçada na sistematização da comunicação, das pessoas e da informação comunicada.

Não se pode negar que a Internet inovou a forma de socialização dos indivíduos, exercendo um papel fundamental na sociedade da informação, permitindo um fluxo informacional sem barreiras físicas ou temporais. O computador aliado à internet é um complexo de interatividade, obscuro em relação aos reais objetivos dos usuários, considerando que estes podem ser mal-intencionados, como é o caso dos engenheiros sociais, cujas técnicas e armadilhas são desconhecidas.

Considerando que o comportamento do indivíduo e a sua interação estabelece padrões de comportamento e transportando esta premissa à rede, se inicia um processo de desenvolvimento de uma cultura de segurança.

Contudo, os problemas afetos à segurança da informação não poderão ser solucionados com implementação apenas de recursos tecnológicos, pois não se pode afastar o contexto social no qual está inserida.

Assim, a abordagem multifacetada das Instituições Bancárias brasileiras, promovendo a interação entre as políticas de segurança dotadas de tecnologia eficaz de segurança e correntistas motivados e conscientes da importância de tais recursos é um desafio a ser superado.

6.2 PERSPECTIVAS PARA NOVAS PESQUISAS CIENTÍFICAS

O tema abordado é caracterizado pela complexidade e pelo dinamismo tecnológico, portanto, ao se limitar o objeto da pesquisa, surgiram perspectivas para novas pesquisas científicas. Para tanto, considerando a multidisciplinaridade da Ciência da Informação e a sua relação direta com as demais áreas de conhecimento, seguem algumas propostas de estudos futuros:

- Identificar os canais de maior relevância para o correntista de uma Instituição Bancária no que se refere à segurança da informação, considerando o atendimento pessoal nas agências bancárias e os canais tecnológicos como *sites*, *folders*, caixas eletrônicos, centrais de atendimento, *smartphones*, entre outros;

- Analisar os sentimentos aflorados no correntista após serem vítimas de fraudes eletrônicas, considerando que os resultados da pesquisa identificaram sentimentos como o medo, insegurança, abandono e descrédito do canal utilizado e a perda da confiança na Instituição Bancária;

O assunto não se encerra neste ponto e a dinamicidade do processo e do conhecimento é determinante para a segurança da informação na sociedade da informação.

REFERÊNCIAS

ABNT NBR ISO/IEC 27001:2013 - **Tecnologia da Informação:** Técnicas de segurança - Código de práticas para a gestão da segurança da informação. Associação Brasileira de Normas Técnicas. Rio de Janeiro: ABNT, 2013. Disponível em: <http://www.abntcatalogo.com.br/norma.aspx?ID=306580> Acesso em: 15 maio 2014.

ABNT NBR ISO/IEC 27002:2005 - **Tecnologia da Informação:** Técnicas de segurança - Código de práticas para a gestão da segurança da informação. Associação Brasileira de Normas Técnicas. Rio de Janeiro: ABNT, 2005. Disponível em: <http://www.abntcatalogo.com.br/norma.aspx?ID=306582> Acesso em: 15, maio 2014.

ABNT NBR ISO/IEC 27002:2013 - **Tecnologia da Informação:** Técnicas de segurança - Código de práticas para a gestão da segurança da informação. Associação Brasileira de Normas Técnicas. Rio de Janeiro: ABNT, 2013. Disponível em: <http://www.abntcatalogo.com.br/norma.aspx?ID=306582> Acesso em: 15, maio 2014.

ABRAHAM, Sherly; SMITH, Indushobha Chengalur. An overview of social engineering malware: Trends, tactics, and implications. **Technology in Society**, Estados Unidos, v. 32, n. 3, p. 183-196, agos., 2010. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0160791X10000497 > Acesso em: 16, maio, 2014.

ALMEIDA, M. B. **Um modelo baseado em ontologias para representação da memória organizacional**.. Tese (Doutorado) Escola de Ciência da Informação, Universidade Federal de Minas Gerais, Belo Horizonte, 2006. 321p

_____.; SOUZA, Renato Rocha; COELHO, Kática Cardoso Coelho. Uma proposta de ontologia de domínio para segurança da informação em organizações: descrição do estágio terminológico. **Informação &**

Sociedade, João Pessoa, v. 20, n. 1, p. 155-168, jan./abr., 2010. Disponível em: <http://www.brapci.ufpr.br/download.php?dd0=11848> Acesso em: 23 nov. 2013.

_____.; CARNEIRO, Luciana Emirena Santos. Gestão da Informação e do Conhecimento no âmbito das práticas de Segurança da Informação: O fator humano nas organizações. **Encontros Bibli: revista eletrônica de biblioteconomia e ciência da informação**, Florianópolis, v. 18, n. 37, p. 175-202, mai./ago., 2013. Disponível em: <https://periodicos.ufsc.br/index.php/eb/article/view/1518-2924.2013v18n37p175.> Acesso em: 16 out. 2013.

ALVES, Cássio Bastos. **Segurança da informação vs engenharia social**: Como se proteger para não ser mais uma vítima. Brasília: UDF, 2010.

ANDERSON, James. M. Why we need a new definition of information security. **Computers & Security**, v. 22, n. 4, p. 308–313, May 2003. Disponível em:< http://www.sciencedirect.com/science/article/pii/S0167404803004073> Acesso em: 25 maio 2014.

ARTIGONAL. **Desvendando engenharia social**. 2010. Disponível em: <http://www.artigonal.com/tecnologias-artigos/desvendando-engenharia-social-3353724.html> Acesso em: 10 dez. 2014.

D' AMARAL, Márcio Tavares. Sobre "sociedade do conhecimento": um labirinto e uma saída. **Tempo Brasileiro:** Rio de Janeiro, n. 152, p. 33-42, jan./mar.2003.

ANDERSON, Ramos. **Guia Oficial para formação de gestores em segurança da informação**. Porto Alegre: Zouk, 2006.

ARAÚJO, Carlos Alberto Ávila. Correntes teóricas da ciência da informação. **Ciência da Informação**, v. 38, n. 3, p. 192-204, dez. 2009.

ARAÚJO, Wagner Junqueira. Leis, Decretos e Normas sobre Gestão da Segurança da Informação nos Órgãos da Administração Pública Federal.

Informação & Sociedade: Estudos, João Pessoa, v. 22, p. 13-24, número especial 2012. Disponível em: <http://www.ies.ufpb.br/ojs/index.php/ies/article/view/13675> Acesso em: 15 jul. 2013.

ASSOCIAÇÃO DOS MUNICÍPIOS DA REGIÃO DA GRANDE FLORIANÓPOLIS – GRANFPOLIS. Disponível em: <http://www.granfpolis.org.br/municipios/index.php> Acesso em: 01 mar. 2014.

BAUMAN, Zygmunt**. Modernidade líquida**. Rio de Janeiro: Jorge Zahar Ed., 2001.

BOGDAN, Robert; BIKLEN, Sari. **Investigação qualitativa em Educação**: fundamentos, métodos e técnicas. Portugal: Porto Editora, 1994.

BANCO CAIXA ECONÔMICA FEDERAL – CEF. Disponível em: <www.caixa.gov.br> Acesso em: 15, nov. 2014.

BANCO CENTRAL DO BRASIL – BACEN. Disponível em: <http://www4.bcb.gov.br/fis/TOP50/port/Top50P.asp> Acesso em: 28, out. 2014.

BANCO DO BRASIL. Disponível em: <http://www.bb.com.br> Acesso em: 01 nov. 2014.

BANCO ITAÚ S.A. Disponível em: <https://www.itau.com.br> Acesso em: 12, nov. 2014.

BARRETO, Aldo de Albuquerque. Os agregados de informação: memórias, esquecimento e estoques de informação. **DataGramaZero**: **revista de Ciência da Informação**, Rio de Janeiro, v.1, n.3, p.1-13, ago. 2000. Disponível em: <http://www.dgz.org.br/>. Acesso em: 13 jul. 2013.

_____. A condição da informação. **Perspectiva**, São Paulo, v. 16, n. 3, p. 67-74, jul./set. 2002. Disponível em:

<http://www.scielo.br/scielo.php?pid=S0102-88392002000300010&script=sci_arttext> Acesso em: 22 jan. 2013.

BAUER, Martin W.; AARTS, Bas. A construção do corpus: um princípio para a coleta de dados qualitativos. In: BAUER, Martin; GASKELL, George (Orgs.). **Pesquisa qualitativa com texto, imagem e som**. Petrópolis: Vozes, 2002.

BRAGA, Pedro Henrique da Costa. **Técnicas de engenharia social. Grupo de Resposta a Incidentes de Segurança**, Rio de Janeiro, 2011. Disponível em: <http://www.gris.dcc.ufrj.br/documentos/artigos/engenharia-social/view> Acesso em: 13 mar. 2014.

BRASIL. Norma complementar - criação de equipes de tratamento e resposta a incidentes em redes computacionais – etir. 05/IN01/DSIC/GSIPR. **Gabinete de segurança nacional**. Disponível em: <http://dsic.planalto.gov.br/documentos/nc_05_etir.pdf> Acesso em 17 maio 2016.

BRASIL, Presidência da República. Decreto nº 7.724, de 16 de maio de 2012. Regulamenta a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º, do inciso II do §3 do art. 37 e no §2 do art. 216 da Constituição. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/decreto/D7724.htm> Acesso em: 15 de ago. 2013.

_____. Lei 9.983, de 14 de julho de 2000. Altera o Decreto-Lei nº 2.248, de 7 de dezembro de 1940 – Código Penal e dá outras providências. Diário Oficial da República Federativa do Brasil, Brasília, DF, 17 de jul. 2000b. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L9983.htm> Acesso em: 15 de ago. 2013.

BRASIL, CAMARA DOS DEPUTADOS. Conheça as propostas do relatório final da cpiciber. Disponivel em:<http://www2.camara.leg.br/atividade-

legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-crimes-ciberneticos/noticias/conheca-as-propostas-do-relatorio-final-da-cpiciber>. Acesso em 03, mar. 2016

_____. Crimes cibernéticos – relatório final. Disponível em: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1447125>. Acesso em 03 mar. 2016.

BRASIL. Lei nº 12.735 de 30 de Novembro de 2012. Altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei no 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei no 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. 2012.

BORKO, H. Information science: what is it? **American Documentation**, v. 19, n. 1, p. 3-5, 1968. Disponível em: <http://www.marilia.unesp.br/Home/Instituicao/Docentes/EdbertoFerneda/k---artigo-01.pdf> Acesso em: 13 jan. 2014.

BUENO, R., AKEMI IKEDA, A. Segmentação de Consumidores de Produtos e Serviços Bancários: um Estudo Exploratório. **Revista Brasileira de Marketing**, n.12, aug. 2013. Disponível em: <http://www.revistabrasileiramarketing.org/ojs-2.2.4/index.php/remark/article/view/2333>. Acesso em: 27 Maio 2016.

BURKE, Peter. **Uma história social do conhecimento**: de Gutemberg a Diderot. Rio de Janeiro: Jorge Zahar, 2003. 241 p.

CALLON, Michel. O papel das redes sociotécnicas. In: PARENTE, André (Org.). **Tramas da rede**. Porto Alegre: Sulina, 2010. p. 17-38**.**
CAMPOS, André. **Sistema de segurança da informação**: controlando os riscos. 3. ed. Florianópolis: Visual Books, 2014.

CAMPOS, André. **Sistema de segurança da informação**: controlando os riscos. 3. ed. Florianópolis: Visual Books, 2014

CANONGIA, Claudia & MANDARINO, RAFAEL. Segurança Cibernética: o desafio da nova sociedade da informação. **Parcerias estratégicas,** Brasília, v.14, n.29, jul./dez. 2009, p.21-46.

CASTELLS, Manuel. **A sociedade em rede**: a era de informação: a economia, sociedade e cultura. 7 ed. São Paulo: Paz e Terra, 2003.

_____. Internet e Sociedade em Rede, In: MORAES, Dênis de (Org.). **Por Uma Outra Comunicação:** Mídia, mundialização cultural e poder, Rio de Janeiro: RECORD, 2003. p.255-287.

_____. **A Galáxia da Internet**: reflexões sobre a internet, os negócios e a sociedade. Rio de Janeiro: Jorge Zahar Ed., 2003.

CASANAS, Alex Delgado Gonçalves; MACHADO, Cesar de Souza. **O impacto da implementação da norma nbr iso/iec 17799:** código de prática para a gestão da segurança da informação - nas empresas. Disponível em:<file:///C:/Users/Usuario/Downloads/INCLUIR%20REFER%C3%8ANCIA%20-%20OK%20asti_ii_material_apoio_3_seguranca_informacaotexto_base1.pdf> Acesso em: 20 maio 2015.

CERT. Br - CENTRO DE ESTUDOS, RESPOSTAS E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. **Cartilha de segurança para internet**. Disponível em: <http://cartilha.cert.br/livro/cartilha-segurança-internet.pdf> Acesso em: 01, set., 2013.

_____. **FAQ**: Perguntas mais frequentes ao CERT.br. Disponível em: <http://www.cert.br/docs/certbr-faq.html> Acesso em: 01, set., 2013.

CHAWKI, Mohamed. Nigeria Tackles Advance Free Fraud. **Journal of Information, Law & Technology (JILT)**, 2009. Disponível em: <http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2009_1/chawki>Acesso em 27, dez. 2015.

CHOO, C. W. **A organização do conhecimento**. São Paulo: SENAC, 2006.

_____. **Estatística dos Incidentes Reportado ao CERT.br**. Disponível em: <http://www.cert.br/stats/incidentes/#2013> Acesso em: 02 fev. 2014.

COELHO, Cristiano Farias; RASMA, Eline Tourinho; MORALES, Gudelia. Engenharia social: uma ameaça à sociedade da informação. P**erspectivas online: exatas & engenharia:** Campos dos Goytacazes, v. 3, n. 5, p. 34-44, mar. 2013. Disponível em: <http://www.seer.perspectivasonline.com.br/index.php/exatas_e_engenharia/article/view/87/59> Acesso em: 17 nov. 2013.

CRESWELL, John W. **Projeto de pesquisa**: métodos qualitativo, quantitativo e misto. 2. ed. Porto Alegre: ARTMED, 2007. 248p.

DINIZ, Eduardo H. Cinco Décadas de automação. **Era Digital**: São Paulo, v. 3, n. 3, p. 55 – 60, ago./out. 2004.

DYSON, Esther. **Release 2.0**. Rio de Janeiro: Campus, 1998. 316p.

ERBSCHLOE, Michael. **Trojans, worms, and spyware**: a computer security professional's guide to malicious code. Elsevier Butterworth–Heinemann, 2004. 232p.

FEBRABAN - FEDERAÇÃO BRASILEIRA DE BANCOS. **Como se prevenir**. 2013. Disponível em: <http://www.febraban.org.br/Febraban.asp?id_pagina=121&idtexto=0&palavra=fraudes> Acesso em: 05 out. 2013.

_____.**Você e seu banco**. Um guia que vai facilitar seu relacionamento com os bancos. 2014. Disponível em: <http://www.febraban.org.br/7rof7swg6qmyvwjcfwf7i0asdf9jyv/sitefebraban/voce_e_seu_banco.pdf.> Acesso em: 27 ago. 2014.

_____. **Pesquisa FEBRABAN de Tecnologia Bancária 2013/2014**. Disponível em: <http://www.febraban.org.br/7Rof7SWg6qmyvwJcFwF7I0aSDf9jyV/sitefebraban/RPSP-60214%20FEBRABAN_Pesquisa%20Tecnologia%20Banc%E1ria_2013%207.5.2014_vf.pdf. Acesso em: 09 maio 2014.

FECAM - ASSOCIAÇÃO DOS MUNICÍPIOS DA GRANDE FLORIANÓPOLIS. **Granfpolis**. Disponível em: <http://www.fecam.org.br/associacoes/?cod_associacao=8> >Acesso em: 20 maio 2014.

FERREIRA, Fernando Nicolau Freitas; ARAÚJO, Márcio Tadeu de. **Política de Segurança da Informação:** guia prático e implementação. Rio de Janeiro: Ciência Moderna, 2006.

FLANAGAN, J. C. The critical incident technique. **Psychology Bulletin**, n. 51, v.4, p.327-358, 1954.

FREITAS, Henrique. et al. O método de pesquisa *survey*. **Revista de Administração**: São Paulo, v. 35, n. 3, p. 105-112, julho/setembro 2000.

GIL, Antônio Carlos. **Como elaborar projetos de pesquisa**. 4. ed. São Paulo: Atlas, 2002.

_____. Métodos e técnicas de pesquisa social. 5 ed. São Paulo: Atlas, 2007.

GONZÁLEZ DE GÓMEZ, Maria Nélida. Novos cenários políticos para a informação. **Ciência da Informação**: Brasília, v.31, n.1, p.27-41, jan./abr. 2002.

_____. As relações entre ciência, estado e sociedade: um domínio de visibilidade para as questões da informação. **Ciência da Informação**: Brasília, v.32, n.1, p.60-76, jan./abr.2003.

GOODCHILD, John. **Novos funcionários estão mais propensos a ataques de engenharia social**. 2012. Disponível em: <http://www.egov.ufsc.br/portal/conteudo/not%C3%ADcia-novos-funcion%C3%A1rios-est%C3%A3o-mais-propensos-ataques-de-engenharia-social> Acesso em: 11 jan. 2014.

HADNAGY, Chris. Social Engineering Defined. **Social engineering framework.** Disponível em: <http://www.social-engineer.org/framework/information-gathering/> Acesso em, 17, mar., 2014.

HAJ, L. **CPI dos crimes cibernéticos**: relatório final propõe excluir whatsapp de apps que podem ser bloqueados. Disponível em: <http://www.ebc.com.br/tecnologia/2016/05/cpi-dos-crimes-ciberneticos-relatorio-final-propoe-excluir-whatsapp-de-apps-que>. Acesso em 03, mar. 2016

IBGE – INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA. Disponível em: <http://www.ibge.gov.br>. Acesso em: 17 jun. 2014.

INGWERSEN, P. The Traditional IR Research Approach. In: INGWERSEN. **Information Retrieval Interaction**. London: Taylor Graham, 1992, p.72-78

ISO - INTERNATIONAL STANDARDS ORGANIZATION. **ISO/IEC 17.799 information technology security techniques**: code of practice for information security management. Geneva: ISO; 2005.

JOHNSON, Steven. **Emergência**: a dinâmica da rede em formigas, cérebros, cidades e softwares. Rio de Janeiro: Jorge Zahar Ed., 2003. 231 p.

KOVACH, Stephan. **Detecção de fraudes em transações financeiras via internet em tempo real**. 2011, 134p. Tese (Doutorado) – Escola Politécnica, Universidade de São Paulo, São Paulo. Disponível em: <http://www.teses.usp.br/teses/disponiveis/3/3141/tde-09082011-155153/publico/Tese_Stephan_Kovach.pdf> Acesso em: 25, out. 2013.

KLEIN, Soeli Claudete. **Engenharia social na Área da Tecnologia da Informação**. 2004. 63p., Monografia (trabalho de Ciências Exatas e Tecnológicas, Centro Universitário Feevale. Novo Hamburgo, RS. 2004

KROMBHOLZ, et al. Advanced social engineering attacks**. Journal of information security and applications,** n. 22, 2015. p.113 e122. Disponível em: <

<http://www.sciencedirect.com/science/article/pii/S2214212614001343 > Acesso em: 20 maio 2015.

LAU, Marcelo. **Análise das fraudes aplicadas sobre o ambiente Internet Banking.** 2006. 129 p. Dissertação (Mestrado) – Escola Politécnica, Universidade de São Paulo, São Paulo. Disponível em: <http://www.datasecurity.com.br/index.php/biblioteca-data-security> Acesso em: 15 ago. 2013.

LAUDON, Kenneth C., LAUDON, Jane P. **Sistemas de Informação**. Rio de Janeiro: Editora LTC – Livros Técnicos e Científicos, 9 ed., 2010. 389p.

LEMOS, André. LÉVY, Pierre. **O Futuro da Internet**: em direção a uma ciberdemocracia. São Paulo: Paulus, 2010. 258p.

LENNERT, Luiz S; OLIVEIRA, Marcos A. de. **Engenharia Social**: uma ameaça fraudulenta crescente. Revista Brasiliano, ed. 64, mar. 2011. Disponível em: < http://www.brasiliano.com.br/revistas/edicao_64.pdf?PHPSESSID=adfda77aeafbf51f2fc23ee 792f2a844 >. Acesso em: 15 maio 2012.

LÉVY, Pierre. **As tecnologias da inteligência**: o futuro do pensamento na era da informática. Rio de Janeiro: 34, 1993.

_____. **A conexão planetária**: o mercado, o ciberespaço, a consciência. São Paulo: Ed 34. 2001. 192p.

_____. **O que é o virtual?** São Paulo: Ed. 34, 1996.

_____. **Cibercultura**. São Paulo: Ed. 34, 1999.

_____. **A inteligência coletiva**: por uma antropologia do ciberespaço. 4. ed. São Paulo: Loyola, 2003.

_____. **Hackers**: Heroes of the Revolution Computer. New York: Nerraw Manijaime / Doubleday, 1984.

LIMA, Luiz. Dilma destaca defesa a Marco Civil feita por Berners-Lee. **Estadão Digital**. Disponível em: <http://politica.estadao.com.br/noticias/geral,dilma-destaca-defesa-a-marco-civil-feita-por-berners-lee,1148991>. Acesso em 15 maio 2015.

MAGANANI, Maria Cristina Brasil; PINHEIRO, Marta Macedo Kerr. Regime e informação: a aproximação de dois conceitos e suas aplicações na Ciência da Informação. **Liinc em Revista**, Rio de Janeiro, v.7, n.2, p.593-610, set. 2011.

MARCELO, Antônio; PEREIRA, Marcos. **A Arte de Hackear Pessoas**. Rio de Janeiro: Brasport, 2005.

MAIA, M. A. **o que é segurança da informação.** 2013. Disponível em: < http://segurancadainformacao.modulo.com.br/seguranca-da-informacao> Acesso em: 20 mar. 2015.

MARCIANO, João Luiz; MARQUES, Mamede Lima. O enfoque social da segurança da informação. **Ciência da Informação**, Brasília, v. 35, n. 3, p. 89-98, set./dez. 2006. Disponível em: <http://www.scielo.br/pdf/ci/v35n3/v35n3a09> Acesso em: 17, jun., 2013

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamentos da metodologia científica.** 6 ed. São Paulo: Atlas, 2005, p. 203.

MATTELART, Armand. **História da sociedade da informação**. São Paulo: Loyola, 2002.

MENDES, Antônio S. F. Entendendo e Evitando a engenharia Social: Protegendo Sistemas e Informações. **Revista Espaço Acadêmico**, n. 43, dez. 2004. Disponível em: <http://www.espacoacademico.com.br/043/43amsf.htm>. Acesso em: 13 maio 2012.

MEDEIROS, Assis. **Hackers**: Entre a Ética e a Criminalização – Uma análise sob a ótica da sociedade da informação. Florianópolis: Visual Books, 2002. 181p.

MITNICK, Kevin D.; SIMON, William L. **A arte de enganar**: Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação. São Paulo: Pearson Education, 2003.

MIRKOVIC et al. Internet Denial of Service: Attack and Defense Mechanisms. Prentice: Hall PTR,. 2004.

MOUTON, Francois et al. Necessity for ethics in social engineering research. **Computers & security**, n.55, 2015. p. 114–127. Disponível em:<http://www.sciencedirect.com/science/article/pii/S0167404815001224> Acesso em: 20 maio 2015.

MORESI, Eduardo Amadeu Dutra. Delineando o valor do sistema da informação em uma organização. **Ciência da Informação**, Brasília, v. 29, n.1, p. 14-24, jan/apr. 2000. Disponível em: <http://www.scielo.br/pdf/ci/v29n1/v29n1a2.pdf>. Acesso em 16, marc., 2014.

MUSSO, Pierre. A filosofia da rede. In: PARENTE, André (Org.). **Tramas da rede**. Porto Alegre: Sulina, 2010. p.17-38.

NIEKERK, Van J.F., SOLMS, Von R. Information security culture: A management perspective. **Cumputers & Security**, n. 29, p. 476-486, 2010. Disponível em:< http://www.sciencedirect.com/science/article/pii/S0167404809001126> Acesso, 15, out. 2014.

MOREIRA, S. V. Análise documental como método e como técnica. In: Jorge Duarte; Antônio Barros. (Org). **Métodos e técnicas de pesquisa em comunicação**. São Paulo: Atlas, 2005.

NOGUEIRA, O. **Pesquisa social**: introdução as suas técnicas. São Paulo: Ed. Nacional, 1968. p. 111-119.

PAIVA, Rodrigo Oliveira de. Um olhar para a arquitetura da informação no ciberespaço. **DataGramaZero**: revista de Ciência da Informação,

Rio de Janeiro, v. 15, n. 5, p. 1 – 13, 2014. Disponível em: <http://www.dgz.org.br/out14/Art_05.htm/>. Acesso em: 15 nov. 2014.

PARODI, Lorenzo. **Manual das fraudes**. Rio de Janeiro: Brasport, 2008.

PEIXOTO, Mário C. P. **Engenharia Social e Segurança da Informação na Gestão Corporativa.** Rio de Janeiro: Brasport, 2006.

PEMBLE, Matthew. What do we mean by "information security". **Computer fraud & scurtity**, v. 2004, n. 5, p. 17-19, may 2004. Disponível em:< http://www.sciencedirect.com/science/article/pii/S1361372304000673> Acesso em: 17, jun. 2014.

PHUN, Laurie. **A Mágica da Persuasão**. Rio de Janeiro: Brasport, 2005.

QUIVY, Raymond; CAMPENHOUDT, Luc Van. **Manual de investigação em Ciências Sociais.** Lisboa: Gradiva, 1992.

RAFAEL, Gustavo de Castro. **Engenharia Social**: as técnicas de ataques mais utilizadas. Profissionais TI. Disponível em: < http://www.profissionaisti.com.br/2013/10/engenharia-social-as-tecnicas-de-ataques-mais-utilizadas/> Acesso em: 30 out. 2013.

RAMOS, Anderson. **Security Officer**: Guia Oficial para Formação de Gestores em Segurança da Informação. Porto Alegre, RS: Zouk, 2006.

REZENDE, Denis Alcides; ABREU, Aline França de. **Tecnologia da informação aplicada a sistemas de informação empresariais**. 9 ed. Ver. São Paulo: Allas, 2013.

ROSA, Adriano C. M. et al. Engenharia Social: o elo mais frágil da segurança nas empresas**. Revisa Eletrônica do Alto Vale do Itajaí – REAVI**. Ibirama, v. 1, n. 2, dez. 2012. Disponível em: <http://www.revistas.udesc.br/index.php/reavi/article/view/2840> Acesso em: 17, maio, 2014.

ROSA, Adriano C.; Silva, Bruno D. da; Silva, Pedro L. da,. Análise de Redes Sociais Aplicada à Engenharia Social. In: SIMPÓSIO INTERNACIONAL DE GESTÃO DE PROJETOS 1. - I SINGEP (2012): Web. Disponível em: < http://www.singep.org.br/seer/index.php?conference=SINGEP&schedConf=SINGEP&page=paper&op=view&path%5B%5D=128&path%5B%5D=0> Acesso em: 15 maio 2014.

SANTOS, Luiz Arthur Feitosa. **Boas Práticas de Segurança da Informação**. 2011. Disponível em: <http://www.slideshare.net/luiz_arthur/palestra-mau-uso-datecnologia>. Acesso em: 18 set. 2013.

SVEEN, F. O.; TORRES, J. M.; SARRIEGI, J. M. Blind Information Security Strategy. **International Journal of Critical infrastructure Protection**, v.2, p.95-109, 2009.

SÊMOLA, Marcos. **Gestão da Segurança da Informação**: uma visão executiva da segurança da informação. Rio de Janeiro: Elsevier, 2014.

_____. Gestão da segurança da informação. In: STAREC, Cláudio; GOMES, Elisabeth; BEZERRA, Jorge (Org.). **Gestão estratégica da informação e inteligência competitiva**. São Paulo: Saraiva, 2006.

SFREDDO, Josiane A.; FLORES, Daniel. Segurança da informação arquivística: o controle de acesso em arquivos públicos estaduais. **Revista Perspectivas em Ciência da Informação**. Minas Gerais, v. 17, n.2, p. 158-178, abr./jun. 2012.

SHIMOMURA, Tsutomu & MARKOFF, John. **Contra-ataque**: a História da Captura do Pirata Cibernético Mais Procurado dos Estados Unidos. São Paulo: Companhia das Letras, 1996. 343p.

SILVA, Narjara B. X.; ARAÚJO, Wagner J. de; AZEVEDO, Patrícia M. de. Engenharia social nas redes online: um estudo de caso sobre a exposição de informações pessoais e a necessidade de estratégias de segurança da informação. **Revista Ibero-Americana de Ciência da Informação – RICI**. Brasília, v. 6, n. 2, p. 37-55, ago./dez. 2013.

TRIVIÑOS, A. N. S. **Introdução à pesquisa em ciências sociais**: a pesquisa qualitativa em educação. São Paulo: Atlas, 1987.

VIDOTTI, Silvana Aparecida Borsetti Gregorio; SANCHES, Silviane Aparecida. **Arquitetura da informação em websites**. 2004. Disponível em: <http://libdigi.unicamp.br/document/?view=8302> Acesso em: 26, nov., 2013.

OLIVEIRA E SILVA, Abner de. Engenharia social: o fator humano na segurança da informação. Coleção Meira Mattos - **Revista das Ciências Militares**. Rio de Janeiro, n. 23, nov. 2011. Disponível em: <http://www.eceme.ensino.eb.br/meiramattos/index.php/RMM/article/view/16/49>. Acesso em: 25 Nov. 2014.

TOFFLER, Alvin. **A Terceira Onda**. Rio de Janeiro: Record, 1980.
WERTHEIN, Jorge. A Sociedade da Informação e seus Desafios. **Ciência da Informação**, Brasília, v. 29, n. 2, p. 71-77, maio/ago. 2000.

WOOD, Charles Cresson. **Information scurity roles & responsibilities made easy**. Information Shield. 2 ed, Sugar Land: InformationShield, 2005.

WOLTON, Dominique. **Internet, e depois? Uma teoria crítica das novas mídias**. São Paulo: Sulinas, 2003.

YOON, Hyun Shik; STEEGE, Linsey M. Barker. Development of a quantitative model of the impact of customers' personality and perceptions on Internet banking use. **Elsevier [Computers in Human Behavior],** n. 29, 2013. p. 1133–1141. Disponível em: <http://www.sciencedirect.com/science/article/pii/S0747563212002737 > Acesso em: 20 maio 2015.

APÊNDICE – ROTEIRO DE ENTREVISTA

Pesquisa “SEGURANÇA DA INFORMAÇÃO: um estudo sobre o uso da engenharia Social para obter Informações Sigilosas de Usuários de Instituições Bancárias. O objetivo da coleta de dados é fundamentar o desenvolvimento da dissertação de Mestrado do Programa de Pós-Graduação em Ciência da Informação do Centro de Ciências da Educação da Universidade Federal de Santa Catarina. Os dados obtidos são de uso confidencial, sendo garantido o anonimato dos participantes da pesquisa, o sigilo bancário e o da informação.

1. Quais são as informações pessoais relacionadas com a instituição bancária que você considera como sigilosas?
2. Quais são os meios ou canais que você utiliza para se manter informado sobre as formas de proteção das informações financeiras sigilosas?
3. A Instituição bancária lhe orientou sobre o cuidado com informações sigilosas, como as senhas? Se sim, quem?
4. Por que você decidiu fornecer as suas informações sigilosas para o engenheiro social?
5. Atualmente você estaria suscetível a ser vítima de uma nova fraude com as mesmas características e abordagens?
6. Como você avalia a orientação da Instituição bancária em relação às fraudes que você estaria suscetível? Há algum ponto a ser melhorado?
7. Você gostaria de abordar algum tópico que não foi contemplado na entrevista, mas considera relevante para esta pesquisa?