UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO DE CIÊNCIAS DA EDUCAÇÃO DA UNIVERSIDADE FEDERAL DE SANTA CATARINA – CED/UFSC
PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO (PGCIN)

Roberto de Paiva Soares Júnior

Propostas para melhorias na Gestão da Informação dos processos de contestação de fraudes bancárias pela Internet baseadas no “Projeto Tentáculos” da Polícia Federal

Florianópolis
2021

Roberto de Paiva Soares Júnior

Propostas para melhorias na Gestão da Informação dos processos de contestação de fraudes bancárias pela Internet baseadas no "Projeto Tentáculos" da Polícia Federal

Dissertação, apresentado ao Programa de Pós-Graduação em Ciência da Informação (PGCIN), do Centro de Ciências da Educação da Universidade Federal de Santa Catarina - CED/UFSC, para obtenção do título de Mestre em Ciência da Informação como parte dos requisitos necessários à obtenção do título de mestrado.
Orientador: Dr. William Barbosa Vianna

Florianópolis
2021

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

Soares, Roberto de Paiva
Propostas para melhorias na Gestão da Informação dos processos de contestação de fraudes bancárias pela Internet baseadas no "Projeto Tentáculos" da Polícia Federal / Roberto de Paiva Soares ; orientador, William Barbosa Vianna, 2021.
154 p.

Dissertação (mestrado) - Universidade Federal de Santa Catarina, Centro de Ciências da Educação, Programa de Pós Graduação em Ciência da Informação, Florianópolis, 2021.

Inclui referências.

1. Ciência da Informação. 2. Fraude Bancária. 3. Crime Cibernético. 4. Internet Banking. 5. Gestão da informação. I. Barbosa Vianna, William. II. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Ciência da Informação. III. Título.

Roberto de Paiva Soares Júnior

Propostas para melhorias na Gestão da Informação dos processos de contestação de fraudes bancárias pela Internet baseadas no "Projeto Tentáculos" da Polícia Federal

O presente trabalho em nível de Mestrado foi avaliado e aprovado por banca examinadora composta pelos seguintes membros:

Prof. (a) Convidado 1, Dr. Edilson Giffhorn
Adjunto da Universidade Tecnológica Federal do Paraná - Campus Ponta Grossa - (Departamento de Engenharia de Produção)

Prof. (a) Convidado 2, Dr. Rafael Pereira Ocampo Moré
Programa de Pós-graduação em Administração Universitária – PPGAU da Universidade Federal de Santa Catarina - UFSC

Prof. (a) Convidado 3, Dr. Alexandre Marino Costa
Programa de Pós-graduação em Administração da Universidade Federal de Santa Catarina – UFSC

Certificamos que esta é a **versão original e final** do trabalho de conclusão que foi julgado adequado para obtenção do título de Mestre em Ciência da Informação.

Documento assinado digitalmente
Edgar Bisset Alvarez
Data: 22/09/2021 09:25:37-0300
CPF: 236.516.228-27
Verifique as assinaturas em https://v.ufsc.br

Coordenação do Programa de Pós-Graduação

Documento assinado digitalmente
William Barbosa Vianna
Data: 22/09/2021 08:50:20-0300
CPF: 456.660.911-15
Verifique as assinaturas em https://v.ufsc.br

Prof. (a) William Barbosa Vianna, Dr.
Orientador

Florianópolis
2021

“Consagre ao Senhor tudo o que você faz, e os seus planos serão bem-sucedidos”. (Provérbios 16:3).

Dedico este trabalho ao senhor meu Deus, por me agraciar e permitir a oportunidade dessa conquista, por me encorajar e manter firme encarando os desafios e dificuldades enfrentados.

À meu querido pai, Roberto de Paiva Soares “*in memorian”,* que quando em vida afirmava na realização do sonho de trabalhar arduamente e batalhar para a formação de seus filhos.

Às três pessoas mais importante em minha vida, minha amada mãe, Maria Jacinta Torres de Paiva e meus filhos, Pedro Roberto Justo Soares e João Pedro Justo Soares.

Ao meu grande amigo de trabalho DPF RICARDO MATIAS por quem considero como um grande profissional, homem de muita fé e um ser humano admirável.

Ao pesquisador e Agente de Polícia Federal, Alex Moreira do Patrocínio “*in memorian”* que muito contribuiu com suas pesquisas para o sucesso desse trabalho.

À minha família e amigos que sempre me apoiaram e acompanharam a trajetória desse sonho realizado.

AGRADECIMENTOS

Agradeço à Polícia Federal, honrosa instituição a qual muito me orgulho de pertencer.

À Universidade Federal de Santa Catarina a qual juntamente com a Polícia Federal celebraram esse convênio que propiciou aos servidores da Polícia Federal a oportunidade de adquirir novos conhecimentos que outrora não vislumbrava.

Aos meus colegas de GRCC/DRCOR/SR/PF/CE, que adquiri grande aprendizado e conhecimento em fraudes bancárias, além de terem aceitado o convite e muito contribuírem como participantes da pesquisa. Neste ponto, um especial agradecimento ao APF OZETE e APF MESSIAS que muitos contribuíram com suas ideias e críticas ao projeto.

Aos meus colegas de trabalho e turma de mestrado da UFSC, todos extremamente motivadores e parceiros, os quais construímos amizades verdadeiras. Estão todos no meu coração.

Um agradecimento ESPECIAL ao meu orientador, professor Dr. William Barbosa Vianna, por ter me recebido como orientando e por me fazer crescer e aprender com a construção dessa dissertação. Concedeu ampla liberdade para trabalhar e demonstrou infinita paciência com os percalços e dificuldades enfrentadas. Ensinou-me muito mais do que aquilo que está escrito nessa pesquisa. Seu profissionalismo e conhecimento irão comigo para a vida pessoal e profissional, principalmente com sua abordagem para solução de problemas, mostrando sempre como a partir de detalhamentos podemos superar cada fase problemática.

Aos professores da UFSC que além do grande conhecimento transmitido, se envolveram com toda a turma indo além das fronteiras da sala de aula e na medida do possível se congregando e confraternizando ao final de cada ciclo de aulas.

Aos meus chefes, Wellington Santiago da Silva, Juliana de Sá Pereira Gonçalves Pacheco e Paulo Henrique Oliveira Rocha, que sempre me apoiaram, incentivaram para encarar e concluir esse trabalho.

À Katharina Justo que sempre me ajudou durante a realização do trabalho com sua experiência acadêmica, me auxiliando e tirando dúvidas na construção da dissertação.

RESUMO

Nos últimos anos, o "Projeto Tentáculos" da Polícia Federal trouxe um marco na melhoria da qualidade da informação sobre fraude bancária com vistas a combater crimes de fraudes bancárias pela internet. O “Projeto Tentáculos”, termo de cooperação idealizado como um modelo para gestão da informação entre a Polícia Federal e a Caixa Econômica Federal possibilitou a centralização de informações referentes à fraudes bancárias eletrônicas em um banco de dados nacional, denominado Base Nacional de Fraudes Bancárias Eletrônicas (BNFBE), representando grande avanço no modelo investigativo. O sucesso do projeto resultou no estabelecimento de outros termos e acordos de cooperação com diversas instituições financeiras vinculadas à Federação Brasileira de Bancos (FEBRABAN). Entretanto, embora a ocorrência dessas parcerias tenha demonstrado melhoria nos resultados investigativos, ainda são verificados pela Polícia Federal problemas na qualidade na gestão das informações sobre fraude bancária, o que acarreta prejuízo, demora e dificuldade nos procedimentos investigativos. Nessa conjuntura, o problema que conduziu o desenvolvimento dessa pesquisa foi: Como melhorar a Gestão das Informações sobre fraudes bancárias inseridas na BNFBE? Diante disso, o objetivo primordial foi propor melhorias na Gestão das Informações sobre fraudes bancárias inseridas na BNFBE, descrevendo o estágio atual desse processo de comunicação e correlacionado com a proposta de um novo fluxo. A pesquisa é de natureza qualitativa e documental, do tipo descritiva e exploratória. Foram utilizados como instrumento de pesquisa, entrevistas em grupo focal com os Policiais Federais, especialistas em fraudes bancárias eletrônicas lotados no Estado do Ceará. A aplicação da Soft Systems Methodology (SSM), ao processo de comunicação das fraudes eletrônicas, comparando o fluxo de informação atual com o modelo sugerido pelo autor da pesquisa, apresentou-se como ferramenta de suporte para identificar e detalhar outros elementos para se construir um modelo geral aplicável de apoio decisional de maneira viável e possível. Dentre os resultados encontrados a partir das análises das entrevistas em grupo focal após aplicação do SSM, foi possível observar a necessidade de se sugerir melhorias no fluxo de informação para melhoria da gestão das informações inseridas na BNFBE e consequente maior efetividade no combate aos grupos criminosos que cometem fraudes bancárias.

Palavras-chave: Fraude Bancária; Crime Cibernético; Internet Banking; Gestão da informação; Ciência da Informação; Ciência Policial.

ABSTRACT

It deals with proposals for improvements in the Information Management of Internet banking fraud contestation processes based on the Federal Police's “Tentáculos Project”. The “Tentacles Project”, a cooperation term idealized as a model for information management between the Federal Police and Caixa Econômica Federal, made it possible to centralize information regarding electronic bank fraud in a national database, called the National Electronic Bank Fraud Base - BNFBE, represented a great advance in the investigative model. The project's success resulted in the establishment of other terms and training studies with institutions linked to FEBRABAN. However, although the occurrence of these partnerships has disappeared from the investigative results, problems are still being verified by the Federal Police in terms of quality in the management of information about bank fraud, which leads to losses, delays and difficulties in investigative procedures. In this context, the problem that led to the development of this research was: How to improve the Management of Information on bank frauds inserted in the BNFBE? Therefore, the main objective was to propose improvements in the Management of Information on bank frauds inserted in the BNFBE, describing the current stage of this communication process and correlated with a proposal for a new flow. The research is qualitative and documentary, descriptive and exploratory. They were used as a research instrument, classification in a focus group with the Federal Police, specialists in electronic banking frauds located in the State of Ceará. The application of Soft Systems Methodology (SSM), to the electronic fraud communication process, comparing the current information flow with the model suggested by the research author, presented as a support tool to identify and other elements to build a model general framework of decision support in a viable and possible way. Among the results found from the analysis of the interviews in a focus group after the application of the SSM, it was possible to observe the need to suggest improvements in the information flow to improve the management of information inserted in the BNFBE and consequent greater effectiveness in combating criminal groups. who commit bank fraud.

Keywords: Bank Fraud; Cyber Crime; Internet Banking; Information Management; Information Science; Police Science.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE SIGLAS E ABREVIATURAS

PC	Computador Pessoal
PF	Polícia Federal
CEF	Caixa Econômica Federal
BNFBE	Base Nacional de Fraude Bancária Eletrônica
FEBRABAN	Federação Brasileira de Bancos
SSM	Soft System Methodology
MPF	Ministério Público Federal
BDTD/IBICT	Biblioteca Digital Brasileira de Teses e Dissertações
PNAD	Pesquisa Nacional por Amostra de Domicílios Contínua
CI	Ciência da Informação

SUMÁRIO

1 INTRODUÇÃO

Nos últimos anos, o advento da globalização e dos avanços tecnológicos resultaram na popularização e massificação da internet *banking* com uso de computadores e smartphones. *Internet banking* refere-se à prestação de serviços bancários eletrônicos, geralmente através de um computador pessoal (PC) ou outros dispositivos de acesso com recursos de Internet (GKOUTZINIS, 2006).

A velocidade e o progresso na prestação de serviços bancários por meio da internet permitiram a migração do acesso via *internet banking*, para o acesso via *mobile banking*, que consiste primordialmente na prestação de serviços bancários por meio de dispositivos móveis, tais como celulares, smartphones e tablets (LIN, 2011; YU, 2014).

Atualmente, o aumento de fraudes bancárias eletrônicas contra as instituições financeiras, decorre do crescimento expressivo de transações bancárias realizadas por meio da internet banking e mobile banking (PATROCINIO, 2016).

O poder público, por meio de suas forças de segurança pública, deve estar sempre atento à evolução e diversificação das ações criminosas, acompanhando e se aperfeiçoando conforme se dinamizam o modo de agir dos agentes com comportamentos inadequáveis à conduta social; encarando deste modo, os desafios que a tecnologia propicia, o volume de informações e a crescente popularização dos serviços prestados aos usuários do sistema bancário por meio da internet.

Desta forma, o estabelecimento de parcerias por meio de termos e acordos de cooperação entre o poder público e entes de natureza privada propiciam um ambiente para gestão da Informação de maneira colaborativa que beneficia tanto o poder público e as instituições financeiras, assim como a sociedade. Tais parcerias têm como objetivo integrar conhecimento e interesses comuns com a troca de experiências visando combater de forma eficiente o volume devastador desse tipo de fraude.

Ao redor desse mundo moderno globalizado, organizações governamentais estão lutando para manter seu papel e posição na sociedade. A necessidade de inovação pública pode ser definida como a busca de novas ideias e conceitos, tecnologias, técnicas e métodos, formas, sistemas e procedimentos para criar interações significativas entre o governo e a sociedade, a fim de lidar com uma série de desafios sociais. O poder público para ser inovador, precisa possuir além dos valores de eficiência e eficácia, precisa também garantir sua confiança e capacidade de resposta para restaurar as conexões perdidas entre governo e sociedade. (BEKKERS; EDELENBOS; STEIJN, 2011).

Neste sentido, a Polícia Federal (PF) atuando como órgão permanente de Estado para a segurança pública, tem estabelecido parcerias por meio de termos e acordos de cooperação com diversas instituições financeiras, no combate às organizações criminosas que realizam fraudes bancárias pela internet e com uso de cartões bancários.

O "Projeto Tentáculos" idealizado como um modelo para gestão da informação entre a PF e a CAIXA ECONÔMICA FEDERAL (CEF), formalizado através de um Termo de Cooperação Técnica firmado em 29/10/2008 entre ambos. Dentre as ações de gestão da informação, houve a troca de ideias e experiências, buscando o aperfeiçoamento tecnológico em benefício dos entes envolvidos. Foi implementada a centralização de informações referentes às fraudes bancárias em um banco de dados nacional, denominado Base Nacional de Fraudes Bancárias Eletrônicas (BNFBE). Tal medida tornou o trabalho investigativo mais eficiente, visando de fato alcançar grandes organizações criminosas especializadas em fraudes bancárias na internet (BRASIL, 2009).

De acordo com Siqueira (2014), a experiência investigativa comprovou a necessidade do estabelecimento da parceria entre as instituições. Assim, o "Projeto Tentáculos" definiu, dentre outras coisas, o padrão da troca de informações, com os campos mínimos para que possibilitasse um melhor resultado nas investigações. Além dos tipos de dados, estabeleceu-se um canal seguro de comunicação e o uso de criptografia assimétrica, o que garantiu a segurança na troca de informações. O estabelecimento dessa parceria entre Polícia Federal e CEF com objetivos em comum foi fundamental para o sucesso do projeto.

Entretanto, o mesmo não ocorreu com as trocas de informações e centralização das informações referentes às fraudes bancárias entre outras instituições financeiras que também firmaram os mesmos termos e acordos de cooperação, além de existir atraso na troca de informações até mesmo com a CEF nas contestações que alimentam a BNFBE, perdendo assim, o princípio da oportunidade em investigar essas fraudes. Precisava, deste modo, ampliar os horizontes da experiência investigativa para identificar porque as demais instituições financeiras não obtiveram êxito em padronizar e centralizar as informações sobre fraudes bancárias. Necessitava ainda reunir estudos e modelos conceituais, comparando-os com a realidade para melhorar a Gestão das Informações repassadas pelas demais instituições financeiras, além de sugerir mudanças para se verificar a viabilidade de participação efetiva da vítima de fraude bancária dentro do processo de Gestão da Informação.

Conhecer e reconhecer o sucesso já alcançado pelos termos e acordos de cooperação firmado entre a Polícia Federal e a Caixa Econômica Federal, torna-se bastante interessante, uma vez que traça um modelo de sucesso a ser seguido e proposto a outras instituições

financeiras vinculadas à Federação Brasileira de Bancos (FEBRABAN) que também firmaram os mesmos acordos de cooperação. Mostra-se, assim, a necessidade de se propor com a participação dos atores envolvidos um modelo possível e aceitável de padronização na comunicação dos processos de contestação de fraude bancária para alimentar de forma rápida, efetiva e eficiente a BNFBE, para, desta maneira, se produzir informações estratégicas e relatórios de inteligência capazes de combater organizações criminosas que agem contra todas as instituições financeiras do Brasil ao mesmo tempo, além de coibir a transmissão de dados sobre fraudes bancárias sem a qualidade da informação desejada.

Feita esta contextualização, a formulação do problema, que vem a ser a razão da própria pesquisa e para a qual se busca resposta, nesse sentido pergunta-se: **Como melhorar a Gestão das Informações sobre fraudes bancárias inseridas na BNFBE?**

A seguir, passa-se ao detalhamento do problema de pesquisa. Com o intuito de conhecer e entender a formulação do problema da presente pesquisa, utilizou-se as condições inter-relacionadas de eventos marcantes sugeridas por Landry (1995). O autor considera que o dinamismo e constantes mudanças nas atividades de gestão acarretam diariamente problemas para serem enfrentados por seus gestores (LANDRY, 1995).

1.1 PROBLEMÁTICA DETALHADA

Para Landry (1995), esse conjunto de condições que servem como marco para sinalização da presença de problemas na gestão de organizações, assim denominados como pontos de referências (LMs), sem uma ordem fixa de ocorrência, elencados da seguinte forma:

LM 1 - Um passado, presente ou futuro julgado como negativo.

LM 2 - Decisão prévia sobre a capacidade de intervir.

LM 3 - Expressão de interesse em fazer algo e comprometer recursos.

LM 4 - Incerteza quanto a ação apropriada e sua implementação.

A descrição da metodologia aplicada por Landry (1995) demonstrando os Pontos de Referências para sinalização de problemas em organizações e correlacionando com o contexto do problema de pesquisa em desenvolvimento, está representado na Figura 1 a seguir.

Figura 1 - Com a demonstração dos Pontos de Referências – Landmark sugeridos por Landry (1995) correlacionado com o intuito de conhecer e entender o problema de pesquisa.

Fonte: Elaborado pelo autor (2020) adaptado de Landry (1995).

Com essa representação (Figura 1), visando conhecer e entender de forma expressa a situação problemática relacionada aos processos de contestação de fraude bancárias eletrônicas, pode ser enfatizado.

LM1 – Embora inicialmente a experiência investigativa tenha comprovado o sucesso na troca de informações de maneira padronizada entre a PF e a CEF, o mesmo não ocorreu com as trocas de informações e centralização das informações referentes às fraudes bancárias entre outras instituições financeiras vinculadas à FEBRABAN que também firmaram os mesmos termos e acordos de cooperação. A falta de padronização, o atraso na alimentação e a incompletude de dados demonstram problemas na gestão das informações com essas instituições e até mesmo com a CEF.

Diante da constante mudança e aperfeiçoamento do *modus operandi* de grupos criminosos, fica evidente a situação de risco que precisa ser melhorada para acompanhar o crescimento dos ataques de fraudes bancárias eletrônicas e combater com meios investigativos viáveis.

LM2 - Os donos do problema (Gestores) envolvidos na situação problemática e que possuem decisão prévia sobre a capacidade de intervir, devem agir propondo boas práticas de mudança. Devem ter o controle do que pode ser feito procurando melhorias na gestão das informações sobre fraudes bancária eletrônica inseridos na BNFBE.

Deve ainda haver articulação dos Gestores com os atores envolvidos (Instituições Financeiras) na gestão dessas informações por serem interessados diretos, tendo em vista o dispêndio de capital humano e dificuldade investigativa enfrentada pela PF, assim como os prejuízos arcados com o volume de fraudes bancárias suportadas pelas Instituições Financeiras.

LM3- Propor com a participação dos atores envolvidos uma melhoria na gestão das Informações inseridas na BNFBE como forma de criar um modelo possível e viável de padronização na comunicação dos processos de contestação de fraude bancária, transmitidos e alimentados de forma rápida e completa.

O Comprometimento de recursos tais como: aumento de capital humano de equipes de segurança das Instituições Financeiras e de Policiais envolvidos na produção de inteligência a partir dos dados inseridos da BNFBE; Criação de ferramentas de inteligência geradoras de informações estratégicas e relatórios de inteligência capazes de combater organizações criminosas que agem contra todas as instituições financeiras do Brasil ao mesmo tempo causando percas enormes de valores com o volume de fraudes bancárias sofridas.

O emprego desses recursos reveste-se em repreensão aos constantes aumentos de grupos criminosos que aplicam fraudes bancárias.

LM4- A falta de recursos, conhecimento, investimento e treinamento não tem acompanhado as crescentes mudanças no *modus operandi* de grupos criminosos que realizam ataques e fraudes cibernéticas. A tecnologia a cada dia se inova e evolui, criminosos exploram novas maneiras de cometer crimes cibernéticos. A lei e organizações envolvidas na persecução penal devem reagir e manter o ritmo de conhecimento, habilidades, parcerias e cooperação para responder a alturas as ameaças que se tornam tarefas complexas e desafiadoras para as forças policiais (HUNTON, 2011).

A atualização profissional das equipes de segurança das Instituições Financeiras e de Policiais envolvidos na produção de inteligência a partir dos dados inseridos da BNFBE; Maior comprometimento das instituições financeiras; Modernização da legislação de combate aos crimes cibernéticos, revertem-se no conhecimento necessário para acompanhar a evolução desses crimes cibernéticos.

É necessário a produção de conhecimento que possibilite a transmissão e alimentação dos processos de contestação sobre fraude bancária inseridos na BNFBE com a qualidade desejada, com vista a enfrentar e acompanhar as crescentes mudanças no *modus operandi* de grupos criminosos que realizam ataques e fraudes bancárias eletrônicas.

Aplicada as condições inter-relacionadas de eventos marcantes sugeridas por Landry (1995), observa-se a necessidade de estudos orientados para identificar o que é relevante para o processo de padronização e agilidade na comunicação das informações sobre fraude bancária eletrônica. Colher suas percepções e disseminar boas práticas entre os Gestores e atores envolvidos na comunicação, transmissão e em especial na alimentação dos processos de contestação, de forma que sua identificação possa contribuir para o gerenciamento e melhoria do desempenho organizacional do "Projeto Tentáculos" da PF, bem como ir além e ainda propor condições de inovação em que a vítima de fraude bancária possa contribuir nos processos investigativos sobre fraude bancária eletrônica.

1.2 OBJETIVOS

Geral:

Propor melhorias na Gestão das Informações sobre fraudes bancárias inseridas na BNFBE.

Específicos:

a- Sistemografar o atual processo de comunicação das contestações de operações de fraudes bancárias;

b- Relacionar o processo de comunicação, inserção e registro das contestações de fraudes bancárias eletrônicas na BNFBE com os fundamentos da Ciência da Informação (CI);
c- Selecionar da literatura os elementos que se relacionam com a sistemática de comunicação dos processos de contestação sobre fraude bancária eletrônica;
d- Sistemografar uma proposta de fluxo da informação para melhoria na comunicação dos processos de contestação sobre fraudes bancárias inseridas na BNFBE.

1.3 JUSTIFICATIVA

O documento principal na produção de informação é a "informação documentada". Um estudo completo do processo de preparação do documento físico, seja qualquer nome que possua o papel produzido. Neste estudo se nomeou a informação física produzida como Informação Estratégica e Relatórios de inteligência. Assim, colocará em evidência, de forma concreta, os princípios básicos de sua produção e contribuirá para compreensão do ponto de vista de informações (PLATT, 1974).

Uma vez cumprido os objetivos propostos no presente projeto, busca-se de forma efetiva, viável e possível, a alimentação da BNFBE de maneira ágil e padronizada, produzindo-se, a partir disso, relatórios de inteligência e informações estratégicas, seguindo o modelo de fluxo informacional proposto.

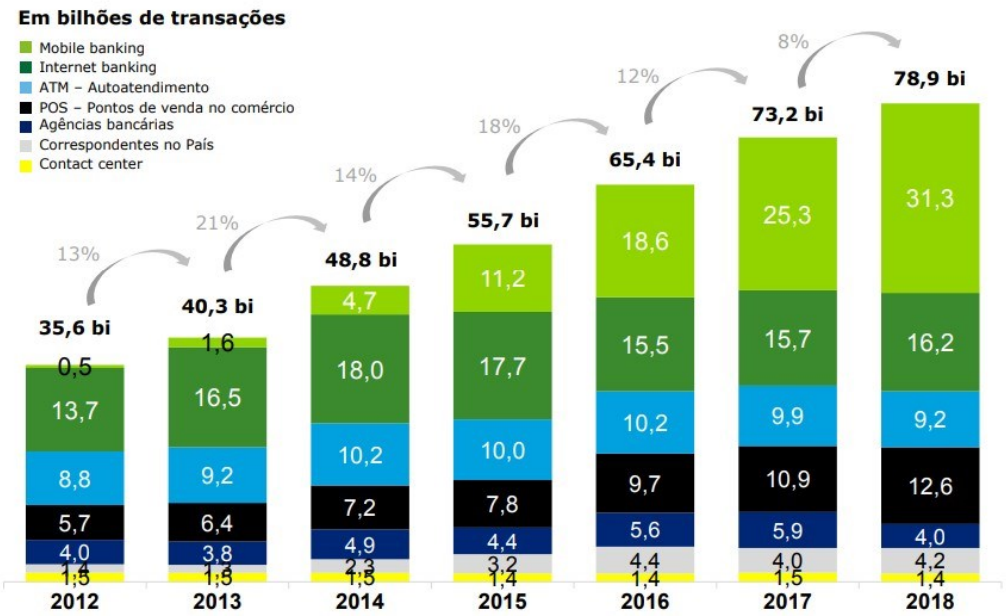
O início de investigações ocorre quando uma autoridade policial toma ciência de maneira provocada ou espontânea da notícia de infração penal, por intermédio da *notitia criminis* ou notícia crime (TOURINHO FILHO, 2008).

A Constituição Federal atribui à PF a apuração de infrações penais praticadas em detrimento de bens, serviços ou interesses da União ou de suas empresas públicas. Assim, a CEF, empresa pública federal, comunicava, por meio de suas agências espalhadas por todo o país, todas as fraudes ocorridas em contas de seus correntistas, na modalidade clonagem de cartões e *internet banking*, diretamente à unidade da Polícia Federal mais próxima (SIQUEIRA, 2014).

Com a evolução dos equipamentos e plataformas de acesso à internet, a BNFBE passou a receber também dados de informações sobre fraudes bancárias eletrônicas na modalidade *mobile banking*, sendo as duas modalidades de fraudes bancárias via *internet banking* e *mobile banking,* consideradas para fins de alimentação na BNFBE subtipos do termo fraude bancária eletrônica.

Para Mompean (2016), o número de fraudes bancárias na modalidade *mobile banking* aumentou 16 vezes no período de 2011 a 2015. A Pesquisa FEBRABAN de Teconologia Bancária de 2019, representada na Figura 2, contando com a participação de 20 bancos e amostra representando 91 % do setor bancário brasileiro, demonstra que o volume de transações bancárias cresceu 8% e que na modalidade *mobile banking* apresentou um crescimento de 24%, tornando-se cada vez mais um canal propício ao aumento de fraudes bancárias eletrônicas.

Figura 2 - Pesquisa FEBRABAN de Tecnologia Bancária de 2019



Fonte: FEBRANBAN (2019).

Das atividades desenvolvidas por investigadores da PF no combate às fraudes bancárias eletrônicas, surge a necessidade do uso de informações que fundamentam e justificam o presente estudo.

Assolini (2015) publicou artigo pela Kaspersky Lab, empresa russa com destaque na produção de softwares e soluções em segurança para internet, nesse artigo considerou que, diante dos números de ataques e fraudes realizadas na internet, o submundo criminoso brasileiro foi classificado como um dos mais ativos e criativos perpetradores de *cibercrimes* do mundo, ao lado da China e Rússia. Naquele cenário de 2014, no caso específico para ataques financeiros e para ataques via *phishing,* o Brasil foi classificado como o país mais perigoso do mundo (ASSOLINI, 2015).

Com a evolução desses ataques e o aumento substancial da quantidade de fraudes cometidas criou-se a necessidade de desenvolvimento de novas técnicas investigativas, o que

resultou na assinatura de um termo de cooperação técnica entre a Polícia Federal e a Caixa Econômica Federal em 2008. Assim foi criada a denominada Base Nacional de Fraudes Bancárias Eletrônicas (BNFBE), pertencente ao Projeto "Tentáculos" da Polícia Federal, no qual são inseridas todas as informações de fraudes bancárias eletrônicas nas modalidades *internet banking* e clonagem de cartões bancários, que implicaram prejuízo para a instituição financeira (SIQUEIRA, 2014).

Em 2009 a PF assina também acordos de cooperação com outras instituições financeiras com o objetivo de fortalecer o combate a fraudes bancárias. Ocorre que o cumprimento dos termos e metas para os acordos não avançaram. Somente em 26/02/2018 a PF, a Federação Brasileira de Bancos – FEBRABAN e mais 14 bancos renovaram aquele acordo de cooperação. Entre os termos firmados dessa vez, regulamenta os procedimentos que todos bancos terão que realizar para comunicar suspeitas ou confirmação de práticas de ilícitos penais. Segundo o acordo, acredita-se que a comunicação entre as instituições possibilitará o compartilhamento de informações e tecnologias recentes (BRASIL, 2018).

Siqueira (2014) afirma que para o sucesso do Projeto Tentáculos, deveria existir, dentre outras coisas, o padrão da troca de informações, com os campos mínimos para que possibilitasse um melhor resultado nas investigações. Além dos tipos e dados, precisava de se estabelecer um canal seguro de comunicação e o uso de criptografia assimétrica para garantir a proteção dos dados na troca de informações.

Entretanto a falta de padronização na formalização das comunicações de fraudes bancárias tem sido recorrente, implicando desde o atraso nas comunicações de notícias crimes (processos de contestações), passando por processos de contestações incompletos ou com campos faltantes, até o preenchimento dos campos dos formulários digitais de comunicação sem um modelo padrão e formato predeterminado.

A necessidade de se propor melhorias na Gestão das Informações sobre fraudes bancárias inseridas na BNFBE entre as instituições financeiras e a Polícia Federal visa melhorar o padrão de comunicação de seus processos de contestação, bem como procurar agilizar essa comunicação, evitando o atraso excessivo, no intuito de obter melhores resultados nos processos de investigação de fraude bancária.

O atraso nessas comunicações de fraudes bancárias por parte das instituições financeiras e a falta de um padrão na comunicação acarretam prejuízos para as investigações, dispêndio de capital humano na formatação dos dados antes da inserção na BNFBE, gerando perda de tempo nas adequações necessárias.

Uma vez inseridas as informações sobre fraudes bancárias eletrônicas na BNFBE, cabe ao Policial Federal especialista em crimes cibernéticos desempenhar suas funções para produzir relatórios de inteligência e informações estratégicas capazes de subsidiar grandes investigações, muitas resultando em operações que desarticulam grupos criminosos que agem em todo o território nacional e algumas vezes em outros países.

Justifica-se, especificamente para a Polícia Federal, pela possibilidade de melhoria na alimentação dos processos de contestação provenientes das notícias crimes informados por todas instituições financeiras vinculadas a FEBRABAN que firmaram acordos de cooperação.

Estas condições justificam o tema escolhido e demonstram a relevância do estudo e a necessidade de se propor melhorias na gestão das informações sobre fraudes bancárias eletrônicas a ser implantado pela PF e demais instituições financeiras vinculadas à FEBRABAN, para maior eficiência e melhores resultados para a investigação.

2 PROCEDIMENTOS METODOLÓGICOS

Nesta seção são apresentados os procedimentos metodológicos relacionados a esta pesquisa, especificando sua caracterização e os procedimentos adotados para sua execução.

2.1 CARACTERIZAÇÃO DA PESQUISA

A presente pesquisa se caracteriza como estudo bibliográfico, exploratório descritivo com abordagem qualitativa.

O estudo bibliográfico se baseia no levantamento de literatura já existente como livros e artigos científicos, dentre outros. Estudos realizado com fundamentação bibliográfica procura contextualizar uma situação a partir de referências teóricas já publicadas em outros documentos científicos (SANTOS, 2012; MICHEL, 2005).

O estudo também é classificado como exploratório descritivo, pois é desenvolvido no sentido de proporcionar uma visão geral de determinado fato. Possui o objetivo de descrever com a utilização de técnicas padronizadas de coleta de dados as características de determinada situação, estabelecendo relações entre suas variáveis (GIL, 1999).

A pesquisa com abordagem qualitativa atua em razão de ações humanas objetivas e portadoras de significado. Possui uma aproximação fundamental e de intimidade entre sujeito e objeto, considerando ambos da mesma natureza. A pesquisa qualitativa volta seus interesses aos motivos, às intenções, aos projetos dos atores, a partir dos quais as ações, as estruturas e as relações tornam-se significativas (MINAYO, 2006; 1993).

Para Serapioni (2000), a abordagem qualitativa aplicada em estudos relacionados aos fenômenos sociais é considerada a mais adequada por sua capacidade de fazer emergir aspectos novos, de ir ao fundo do significado e de estar na perspectiva do sujeito. Em consequência disso, possibilita a descoberta de novos nexos e explicações de significados, tornando-se apta a apreender os aspectos subjetivos, raramente aparentes na realidade.

A seguir discrimina-se de forma detalhada como se deu a delimitação do universo de entrevistados na abordagem qualitativa com a aplicação de entrevistas em grupo focal, quais instrumentos de coleta e o campo de estudo visando atender os objetivos da pesquisa.

2.2 DELIMITAÇÃO DO UNIVERSO

A PF possui em todo território nacional área técnica especializada na investigação de fraudes bancárias eletrônicas assim denominados Grupo de Repreensão à Crimes Cibernéticos

– GRCC, grupos especializados em fraudes bancárias responsáveis e com atribuições para investigar organizações criminosas sediadas em seus estados, mas que cometem crimes eletrônicos em todo território nacional e no exterior. Formalmente existem 15 (quinze) GRCC's estruturados nos estados do Amazonas, Mato Grosso, Pernambuco, Rio Grande do Norte, São Paulo, Minas Gerais, Paraná, Rio Grande do Sul, Rio de Janeiro, Bahia, Pará, Maranhão, Goiás, Ceará e no Distrito Federal. Nas demais Unidades da Federação possuem corpo de Policiais Federais especializados em fraudes bancárias lotados em outras delegacias, mas que atuam diretamente com fraudes bancárias eletrônicas.

Possui ainda como já informado anteriormente o Grupo Permanente de Análise – GPA como divisão especial do SRCC que por delegação cumpre as funções de coordenar, administrar e operar a BNFBE.

Segundo dados apontados pelo SRCC existem hoje na PF 250 Policiais Federais treinados, certificados e especializados em fraudes bancárias eletrônicas com acesso à BNFBE, muito embora especificamente o efetivo de policias lotados nos GRCCs e/ou que trabalham com fraude bancária por estados e no Distrito Federal sejam os descritos na tabela 3, podendo alguns destes policiais ainda não possuírem o curso em fraude bancária eletrônicas em razão de movimentações recentes naturais entre setores da PF, conforme dados apontados nos pedidos de informações de quantitativos aos GRCCs dos Estados e do Distrito Federal (ANEXO E).

Tabela 1 - Policiais Federais lotados no GRCC por Estado da Federação

Sigla do Estado	Policiais Federais lotados no GRCC
AC	02
AL	04
AM	04
BA	08
CE	09
DF	06
ES	03
GO	05
MA	02
MG	04
MS	-

MT	02
PA	04
PB	02
PE	05
PI	02
PR	02
RJ	04
RN	02
RO	-
RR	02
RS	02
SC	04
SE	-
SP	06
TO	02
TOTAL	86

Fonte: Elaborado pelo autor (2019).

Alcançar universo de todos Policiais Federais lotados nos GRCC dos estados e do Distrito Federal seria inviável para que todos participassem das entrevistas em razão da distribuição pelas Unidades da Federação. Incialmente se definiu como delimitação do universo alcançar os 08 (oito) Policiais Federais lotados no GPA em razão da responsabilidade pela administração e coordenação do Projeto Tentáculos, bem como seu suporte as demais regiões do país acerca da operacionalização da BNFBE.

O GPA conta atualmente com um Coordenador responsável, um corpo permanente de 08 (oito) Policiais Federais e um corpo variável de Policiais especialistas em fraudes bancárias eletrônicas de missão que essencialmente auxiliam nas investigações e suporte da BNFBE.O autor da pesquisa se encontrava com Ordem de Missão expedida e passagens para Brasília/DF emitidas para coleta das entrevistas conforme cronograma inicial de entrevistas, mas que em razão da declaração pela Organização Mundial da Saúde, em 11 de março de 2020, de pandemia de COVID-19, doença causada pelo novo coronavírus (Sars-Cov-2); da declaração de Emergência em Saúde Pública de Importância Nacional (ESPIN) em decorrência da Infecção

Humana pelo novo coronavírus (Sars-Cov-2), nos termos da Portaria nº 188/2020, do Ministério da Saúde; e dos inúmeros decretos Estatuais e do Distrito Federal decretando a situação de emergência em saúde de nível nacional, proibindo o deslocamento e circulação de pessoas, o autor da pesquisa ficou impedido de realizar o deslocamento para Brasília/DF. Considerando o estado de emergência ocasionado pelo novo coronavírus (Sars-Cov-2) o autor da pesquisa redefiniu como delimitação do universo alcançar os Policiais Federais lotados no GRCC do Estado do Ceará e/ou que se encontravam lotados nesse GRCC durante a investigação que deflagrou a Operação Valentina.

A escolha dos participantes de um grupo focal deve se basear na reunião de um pequeno grupo relativamente homogêneo de pessoas com conhecimento e experiências vivenciadas na organização. A formação do grupo focal deve ser identificada apenas por etiquetas com os nomes de PARTICIPANTE 1, 2 e assim por diante, bem como por características gerais de cada indivíduo participante, preservando sua identidade e função (ALMEIDA, 2005).

Os participantes foram escolhidos por terem profundo conhecimento em operações policiais sobre fraudes bancárias deflagradas no Estado do Ceará, em especial quase em sua totalidade terem de alguma forma se envolvido durante a investigação da Operação Valentina.

2.3 INSTRUMENTO DE COLETA E APLICAÇÃO DO MÉTODO DE GRUPO FOCAL

Além da análise do material da busca para revisão de literatura e do referencial teórico, para se atingir o objetivo geral e específicos foi realizada também a análise das respostas das entrevistas propostas aos sujeitos envolvidos na pesquisa, feita com entrevistas semiestruturadas em grupos focais, com o intuito de revelar as percepções destes policiais a partir dos processos de contestações provenientes das instituições financeiras visando fornecer ao pesquisador, informações acerca das circunstâncias no atraso na comunicação dos processos de constatação de fraudes bancárias e sua incompletude de dados na comunicação entre as instituições financeiras e a PF.

Entrevista em grupo focal consiste na formação de um grupo de discussão informal composto de 7 a 12 pessoas, com o propósito de obter informações de caráter qualitativo em profundidade de maneira rápida e com baixo custo. Os participantes devem possuir características em comum de interesse da pesquisa, podendo ser de um mesmo setor. As entrevistas devem preferencialmente ser dirigidas por duas pessoas, sendo um moderador que conversa com os entrevistados levantando assuntos identificados num roteiro de discussão e um

auxiliar que realiza a gravação da entrevista, faz as anotações escritas completas visando refletir o conteúdo da discussão e o comportamento dos participantes (GOMES; BARBOSA, 1999).

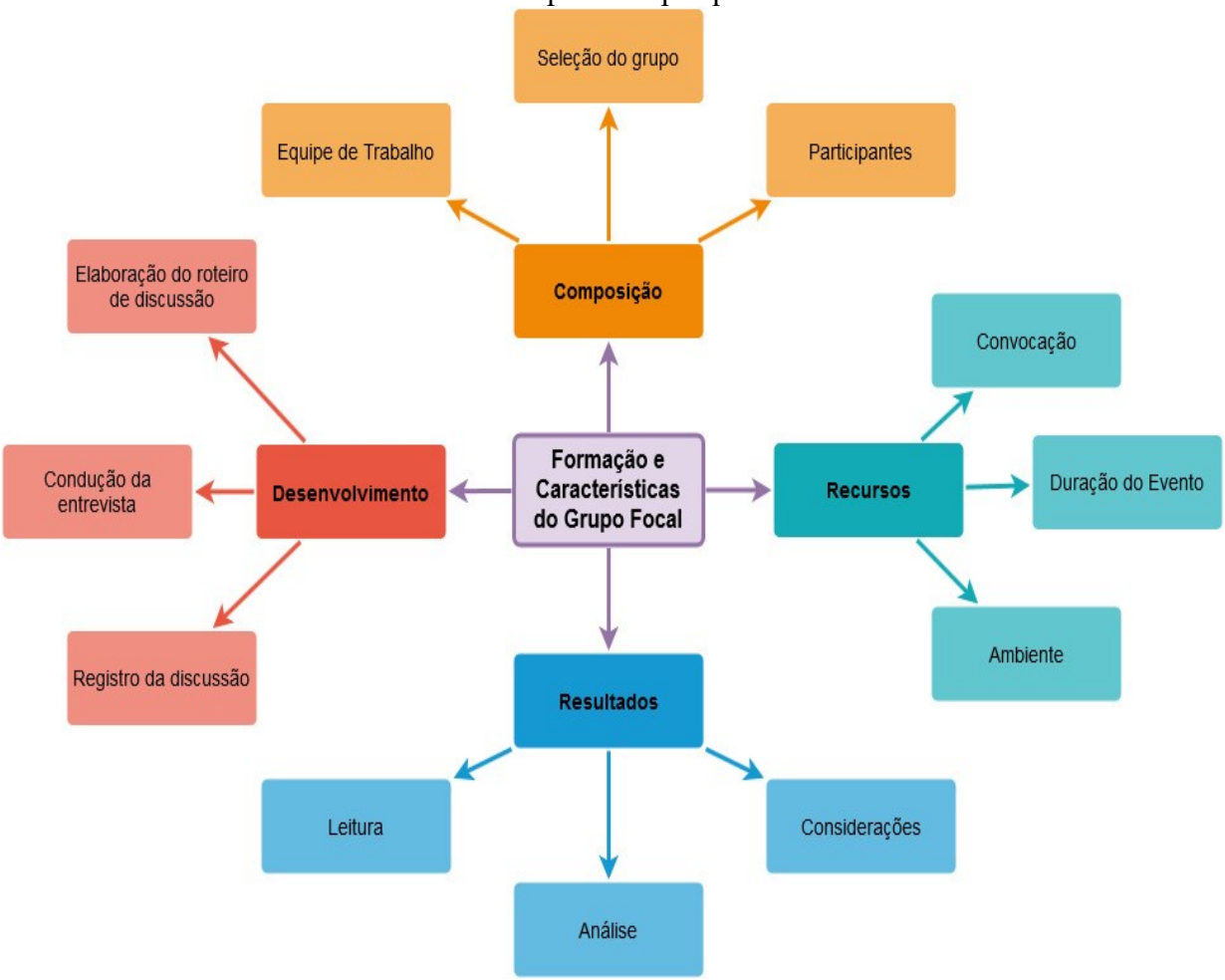
A entrevista em grupo focal consistirá em apresentar o atual fluxo das informações dos processos de contestação sobre fraude bancária eletrônica com o intuito de verificar e expor as percepções dos entrevistados quanto aos problemas observados na inserção de dados na BNFBE.

Por meio de entrevista em grupo focal, pretende-se obter os dados quanto a frequência e intensidade de problemas de qualidade da informação na comunicação dos processos de contestação de fraudes bancárias eletrônicas, ou seja, as circunstancias que causam atraso no envio dos processos de contestação, a incompletude de dados essenciais para a investigação e sua relação com as instituições bancárias envolvidas.

Entrevistas em grupos focais têm sido sugeridas como um método adequado para estudos exploratórios. A força das entrevistas com grupos focais está na dinâmica de grupo e interação, visando fornecer aos pesquisadores perspectivas elaboradas sobre o tema em discussão. Grupos focais refletem o processo através do qual o significado é construído na vida cotidiana. A escolha e seleção de grupos é especialmente importante visando uma maior viabilidade e realidade para a pesquisa (MALLAT, 2007).

A Figura 3 apresenta a representação gráfica da formação e características do uso da técnica de grupo focal na presente pesquisa.

Figura 3 - Representação gráfica da formação e características do uso da técnica de grupo focal na presente pesquisa



Fonte: Elaborado pelo autor adaptado de TRAD (2009).

Dentre as múltiplas finalidades dos grupos focais, pode-se dizer o estabelecimento de um propósito para a pesquisa é considerado um dos passos mais importantes para se planejar e um grupo focal (TRAD, 2009). No caso da presente pesquisa, o Quadro 1 na sequência descreve como ocorreu a utilização da técnica de grupo focal.

Quadro 1 - Descrição da Formação e Características de aplicação da técnica de grupo focal

Formação e Características do Grupo Focal	
Composição	**Seleção do Grupo:** Para seleção do grupo, o critério primordial foi Policiais Federais que atuam diretamente com fraudes bancárias eletrônicas, permitindo, assim, a troca de experiências entre os participantes e a equipe de trabalho. **Participantes:** A escolha dos participantes ocorreu em razão da intenção de se obter as informações e percepções sobre os problemas de qualidade das informações na comunicação dos processos de contestações inseridos na BNFBE. Foi escolhido os Policiais Federais lotados no GRCC do Estado do Ceará e/ou que se encontravam lotados nesse GRCC durante a investigação que deflagrou a Operação Valentina. O grupo é homogêneo, são Policiais que trabalham ou que já trabalharam em fraude bancária eletrônica, possuindo assim, características em comum à temática da presente pesquisa. **Equipe de Trabalho**: A equipe de trabalho do estudo é composta por um coordenador ou moderador e por um apoio técnico observador. Neste caso o autor da presente pesquisa possui a função de atuar como moderador, cabendo-lhe conduzir o grupo adequadamente, facilitando a interação e trocas de experiências acerca do problema debatido. O moderador deverá oferecer previamente aos participantes o termo de consentimento livre e esclarecido (TCLE), constante do APENDICE III. Esse termo deve, dentre outras circunstâncias, fazer referência ao uso de filmagem para gravação das entrevistas, garantir o anonimato e a voluntariedade. O apoio técnico observador possui a função de relator para documentar de forma escrita as conversas em paralelo as gravações. As anotações feitas pelo apoio técnico observador devem ser completas e refletir o conteúdo da discussão daquilo que for relevante sobre o problema de pesquisa.
Recursos	**Convocação**: O sucesso da presença dos participantes decorre do fato do autor da pesquisa se encontrar lotado fisicamente no GRCC do Estado do Ceará e ter trabalhado diretamente com todos os participantes do grupo focal escolhido. **Duração do Evento:** Serão realizadas duas rodadas de entrevistas com no máximo duas horas de discussão, sendo disponibilizado tempo cinco minutos para cada participante. A segunda rodada de entrevista terá o interstício de dois dias para compilação das ideias da primeira rodada. **Ambiente:** O local de realização das entrevistas será realizado na sala de análise do GRCC do Estado do Ceará às portas fechadas com gravação audiovisual.
Desenvolvimento	**Elaboração do roteiro de discussão**: O foco principal e assunto a serem discutidos giram em torno de se obter dados quanto a frequência e intensidade de problemas de qualidade da informação na comunicação dos processos de contestação de fraudes bancárias eletrônicas, ou seja, as circunstancias que causam atraso no envio dos processos de

	contestação, a incompletude de dados essenciais para a investigação e sua relação com as instituições bancárias envolvidas. O roteiro de entrevista segue no APENDICE I e direcionados aos Policiais Federais participantes. **Condução da entrevista:** O moderador/autor da pesquisa conhece todos os participantes da entrevista, tendo inclusive trabalhado diretamente com todos os entrevistados. As discussões devem girar essencialmente na pergunta de pesquisa "Como melhorar a Gestão das Informações sobre fraudes bancárias inseridas na BNFBE?", podendo serem repetidas as perguntas do roteiro de discussão, ressaltando sempre o intuito da pesquisa em tentar observar meios de melhoria da qualidade das informações sobre fraude bancária eletrônica. **Registro da discussão:** O registro das discussões será feito em gravações audiovisuais por meio de web câmeras e armazenadas em HD externo, sendo feita em paralelo a anotações escritas pelo apoio técnico observador.
Resultados	**Leitura:** Ao final de cada rodada de entrevistas o moderador deverá resumir o resultado das reuniões e suas impressões acerca dos objetivos da entrevista. **Análise**: Coletar as opiniões dos Policiais Federais entrevistados, visa medir as percepções dos mesmos quanto a qualidade das informações repassadas pelas instituições financeiras nos processos de contestações. Com base nas percepções dos participantes e suas opiniões expressas tem o objetivo de identificar as tendências e os padrões nas respostas dos entrevistados acerca dos problemas de pesquisa, apontar soluções e propor recomendações. **Resultados:** O propósito do grupo focal deverá resultar na confecção de quadros temáticos com análises das entrevistas que considere a pergunta de pesquisa "Como melhorar a Gestão das Informações sobre fraudes bancárias inseridas na BNFBE"? e reúna informações necessárias para a tomada de decisão e melhoria qualidade das informações inseridas na BNFBE, cujo resultado deverá constar de uma lista de recomendações, apontamentos de inconsistências e incompletudes na alimentação da BNFBE, bem como sistemografar uma proposta de fluxo da informação para melhoria na comunicação dos processos de contestação sobre fraudes bancárias inseridas na BNFBE, visando ao final produzir informações estratégicas e relatórios de inteligência eficientes.

Fonte: Elaborado pelo autor adaptado de TRAD (2009).

Antes do início das duas rodadas de discussões do grupo focal, foi realizada uma reunião de planejamento no dia 05 de novembro de 2020 com parte da equipe de entrevistados (03 participantes), juntamente com o Chefe Coordenador do GRCC-CE, também participante das rodadas de entrevista e com o componente de apoio técnico observador para discutir a disposição dos participantes na sala de análise do GRCC-CE, teste dos equipamentos de gravação áudio visual e de vídeo apresentação. Ao final da reunião foi realizado um sorteio para definir a ordem de identificação dos participantes.

As duas rodadas de discussões do grupo focal foram realizadas na sala de análise do GRCC-CE, localizado no 3º andar da Sede da Caixa Econômica Federal em Fortaleza/CE, situada à Rua Sena Madureira, nº 800, Bairro Centro. Cada rodada de discussão se iniciou com uma breve explanação sobre o tema específico e o roteiro a ser seguido.

A primeira rodada de discussão ocorreu no dia 06 de novembro de 2020, iniciando às 10 horas e 10 minutos e terminando às 11 horas e 47 minutos. Reuniu 10 participantes convidados, o moderador autor da pesquisa e um participante como apoio técnico observador para registro. Pela característica da atividade policial ainda no início da rodada de discussão o PARTICIPANTE 09 solicitou permissão para se retirar em razão de acionamento policial, não participando efetivamente da rodada de discussão.

A segunda rodada de discussão ocorreu no dia 09 de novembro de 2020, iniciando às 10 horas e 30 minutos e terminando às 11 horas e 15 minutos. Reuniu 08 participantes, o moderador autor da pesquisa e um participante como apoio técnico observador para registro. Novamente pela característica da atividade policial os PARTICIPANTES 03 e 09 convidados não puderam comparecer em virtude de acionamento para viagem e missão policial.

As duas rodadas de discussões se iniciaram com 25 minutos de explanação na primeira rodada e 12 minutos de explanação na segunda rodada, ambos gravados em áudio e vídeo. A primeira rodada de discussão teve o tempo de duração de 01 hora e 37 minutos de gravação de áudio e vídeo. A segunda rodada teve o tempo de duração de 45 minutos de gravação de áudio e vídeo, sendo ao final realizado os registros de agradecimento pela colaboração com a pesquisa.

2.4 O CAMPO DO ESTUDO

O levantamento de dados sobre fraude bancária para o campo de estudo foi realizado por meio de pedidos de autorização para acessar e quantificar o volume de fraudes bancárias à Chefe do Serviço de Repreensão à Crimes Cibernéticos da PF (SRCC), sediado em Brasília/DF, que lhe compete especificamente realizar operacionalização, alimentação, tratamento, coordenação e execução da análise de dados disponíveis na BNFBE (ANEXOS A e C) e ao Excelentíssimo Senhor Juiz Titular da 32ª Vara Federal por onde correu o processo judicial relacionado à Operação Valentina (ANEXOS B e D).

2.4.1 A Base Nacional de Fraudes Bancárias Eletrônicas (BNFBE)

Um dos maiores desafios das instituições policiais é a determinação de autoria e materialidade de um crime. A especialização dos grupos criminosos dedicados à prática de fraudes pela internet propõe um desafio ainda maior para as forças policiais (SIQUEIRA, 2014).

Com a evolução dos ataques, especialização e o aumento substancial da quantidade de fraudes cometidas criou-se a necessidade de desenvolvimento de novas técnicas investigativas, o que resultou na criação da BNFBE, pertencente ao Projeto Tentáculos da Polícia Federal.

A BNFBE, desenvolvida e gerida pela PF, é fruto de termos e acordos de cooperação entre a PF, MPF e diversas instituições financeiras a partir da implementação do Projeto Tentáculos detalhado na seção 3.5.2 A operacionalização da BNFBE propiciou celeridade e efetividade no desenvolvimento de investigações de crimes sobre fraudes bancárias. A centralização dos processos de contestação sobre fraude bancária e o fluxo da informação, com sua origem na vítima, usuário do serviço bancário fraudado até o processamento a partir das análises de vínculos geradas na BNFBE, possui estreita relação com a CI, visto que a aplicação de modelos de gestão da informação possibilita a produção de relatórios e informações estratégicas de inteligência que servem de instrumento de combate às fraudes bancárias.

Embora tratados com o mesmo princípio, mas com enfoques em diferentes atores envolvidos no sistema geral de fluxo informacional relacionado à fraude bancária eletrônica, os autores fazem um apanhado sobre a definição de processo consistindo na transformação de uma série lógica de dados alimentados como entrada, que após ordenados de forma específica, fornecem determinados resultados como saída com a finalidade de atender um objetivo ou fornecer serviços e produtos aos clientes (KINTSCHNER; BRESCIANI FILHO, 2005).

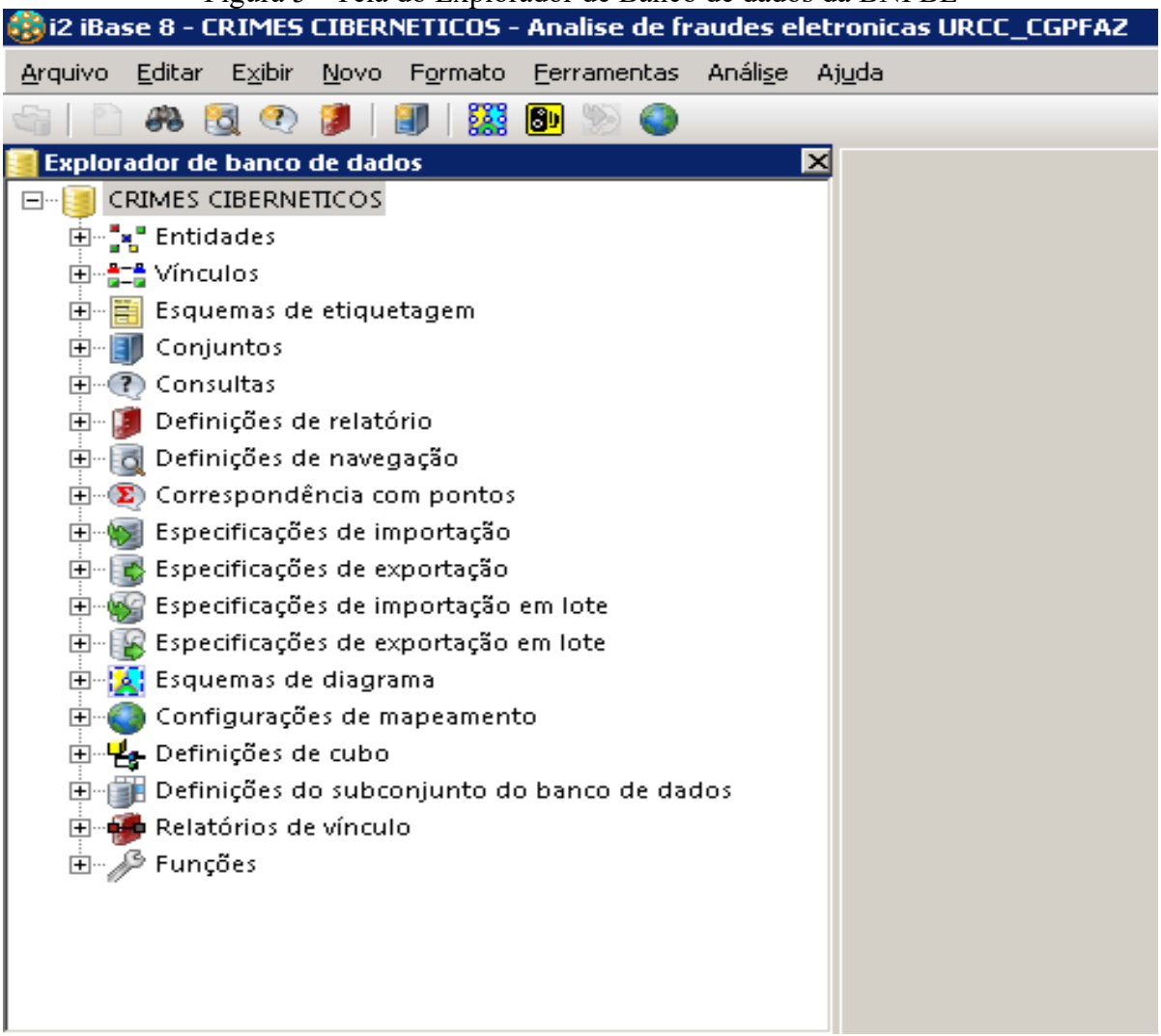
A Figura 4 mostra o panorama geral do modelo investigativo criminal sobre fraude bancária eletrônica de atribuição da PF. Consiste na formação de três processos distintos de fluxo informacional, compondo do processo de contestação de fraude bancária eletrônica do cliente usuário do sistema bancário à instituição financeira, processo de comunicação dos processos de contestação de fraude bancária eletrônica pelas vítima instituições financeira à PF e processo de inserção dos processos de contestação de fraude bancária eletrônica na BNFBE.

Figura 4 - Representação gráfica do fluxo informacional sobre fraude bancária

Fonte: Elaborado pelo autor (2019).

Para efeitos do interesse para a investigação criminal, a origem da informação sobre fraude bancária eletrônica se inicia com a inserção dos processos de contestação na BNFBE. A base de dados foi modelada, no software I2-IBM IBASE 8. A interface da BNFBE no software I2-IBM IBASE 8, mostrada na Figura 5, possibilita explorar, por meios da realização de consultas e pesquisas, os dados alimentados e, a partir das análises de vínculos, produzir informações estratégicas e relatórios de inteligência.

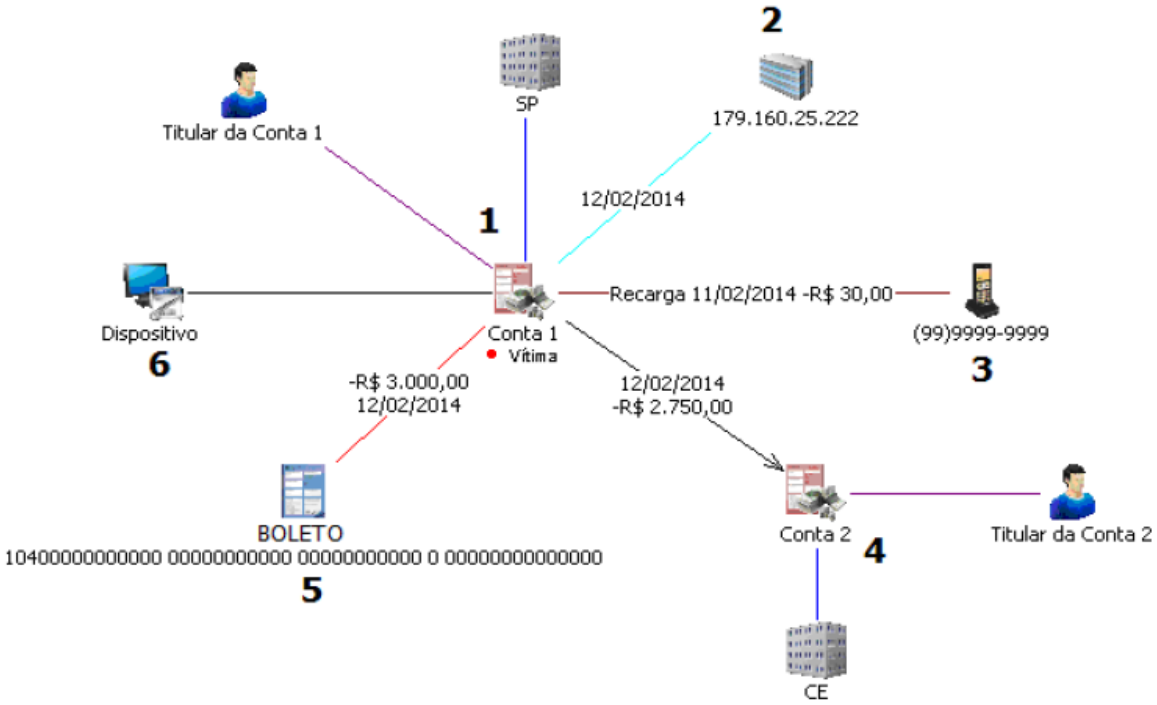
Figura 5 - Tela do Explorador de Banco de dados da BNFBE



Fonte: Elaborado pelo autor (2019) adaptado da interface do software I2-IBM IBASE 8.

A representação gráfica dos dados alimentados é gerada a partir do software Analyst's Notebook 8 por meio de associação a vínculos relacionais. A Figura 6 mostra a representação gráfica gerada de determinada conta fraudada após o policial especializado em fraudes bancária eletrônica realizar a varredura em busca de vínculos (diretos e indiretos) associados à conta fraudada, na figura é possível visualizar dados informados no processo de contestação tais como: titulares da conta vítima e conta beneficiária de valores, número telefônico beneficiários de recarga, número de boleto pago, número IP e dispositivo de origem da fraude, dentre outros dados (SIQUEIRA, 2014).

Figura 6 - Representação gráfica de vínculos do processo de contestação apresentado



Fonte: Siqueira (2014).

Quase que a totalidade das informações inseridas na BNFBE provem dos dados fornecidos pelas instituições financeiras por meio dos processos de contestações. Muitas informações que o cliente vítima de fraude bancária detém não fazem parte dos dados para alimentação da BNFBE. O cliente vítima de fraude bancária quase nunca possui contato com o policial especialista em fraude bancária.

2.4.2 A Experiência investigativa da Operação Valentina

A Operação Valentina investigou um esquema de fraudes, que furtou pelo menos R$ 7,5 milhões de contas bancárias do Banco do Brasil, Caixa Econômica Federal e Itaú e fez mais de mil vítimas em todo o País. A “Operação Valentina”, deflagrada pela Polícia Federal (PF), prendeu 13 pessoas, a maior parte delas no Ceará, onde se concentrava a quadrilha que atuava em todo território nacional e no exterior. No Ceará estavam os quatro líderes da organização criminosa; outro integrante foi detido no Estado de São Paulo (FENAPEF, 2017).

O inquérito policial que deu origem a Operação Valentina foi instaurado em 30 de junho de 2016, tendo a referida operação sido deflagrada em 11 de abril de 2017 com a conclusão do inquérito em 09 de junho de 2017. Os investigados foram denunciados em 16 de

maio de 2017 e condenados em 20 de junho de 2018 a penas que somadas somam mais de 85 anos de prisão pela Justiça Federal da 32ª Vafa Federal do Ceará (BORGES, 2018).

Embora a investigação que resultou na deflagração da Operação Valentina tenha se originado a partir de relatórios e informações produzidas na BNFBE, quase a totalidade das fraudes investigadas na operação não se encontravam na base, tendo em vista o lapso temporal de inserção das informações sobre fraudes bancárias na BNFBE, no entanto, a experiência investigativa e sucesso da operação demonstrou a importância da cooperação de troca de informações entre a PF e as Instituições Financeiras Vítimas das fraudes, assim como o total apoio e comprometimento em fornecer recursos humanos, tecnológicos e de inteligência pelo SRCC administrador da BNFBE.

2.4.2.1 Modus operandi investigado na Operação Valentina

O grupo criminoso especializado em fraudes bancárias eletrônicas investigado na Operação Valentina cometia os mais diversos *modus operandi* de ilícito e fraudes bancárias eletrônicas, no entanto, o *modus operandi* de quase a totalidade das fraudes investigadas na operação se dividia basicamente em três etapas conforme descrito no Quadro 2:

Quadro 2 - Etapas do Modus operandi investigado na Operação Valentina

ETAPAS	DESCRIÇÃO DA ATUAÇÃO DO *MODUS OPERANDI*
ETAPA 1	Envio de phishing maliciosos por aplicativos instantâneo de mensagens, SMS's, e-mails e redes sociais para computadores e celulares com o objetivo de capturar os dados bancários dos clientes. Após isso, realizavam consultas das contas que tiveram os dados capturados com o intuito de verificar valores, empréstimos e investimentos financeiros;
ETAPA 2	Transferências ilícitas de recursos encontrados, mediante desvios dos CHIP's SIMCARD das vítimas, para contas de beneficiários "laranjas" previamente selecionados ou pagamentos de boletos de forma fraudulenta;
ETAPA 3	Saque dos valores adquiridos indevidamente e/ou utilização da conta "laranja" para compras fraudulentas em estabelecimentos comerciais (Ex. postos de combustíveis e sites de compras eletrônicas) na opção débito.

Fonte: Elaborado pelo autor (2019).

ETAPA 1

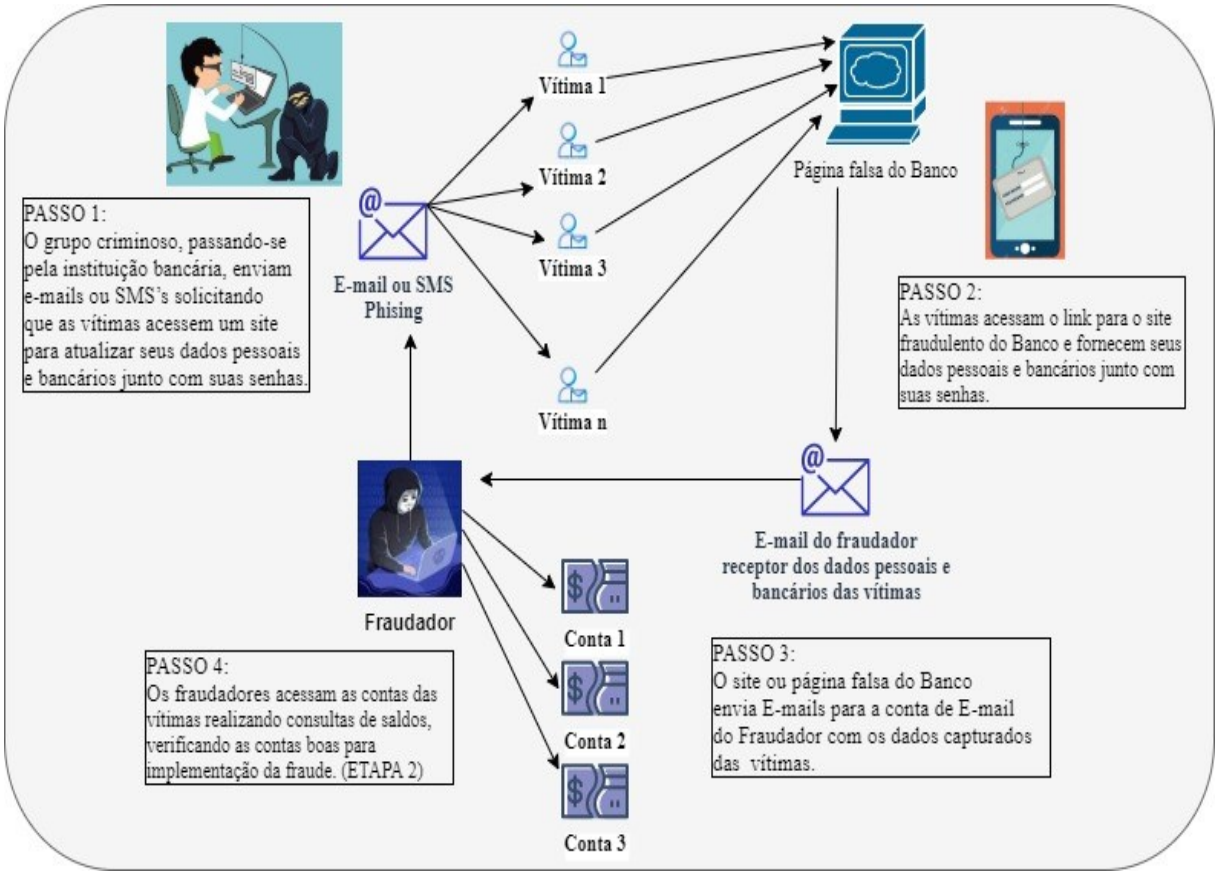
É a etapa mais importante do ciclo criminoso dos fraudadores. Nessa etapa, a organização criminosa cria caixas de e-mails que são utilizadas principalmente como destino de mensagens contendo dados pessoais de proprietários de contas, com suas respectivas senhas, capturados por meio de *phishing*.

Esse tipo de fraude funciona com o fraudador atraindo a vítima de alguma forma e induzindo-a, por meio de engenharia social, a fornecer dados pessoais e bancários (PASSO 1).

Uma das formas dessa engenharia social de aplicar o golpe utilizada pelo grupo criminoso é enviando mensagens chamativas para uma lista de e-mails, mensagens telefônicas (SMS), para aplicativos de mensagens instantâneas (Whatsapp, Telegram, etc.…) ou redes sociais solicitando atualizações de dados de suas contas bancárias e os ameaçando de bloqueio da conta ou de outras penalidades caso não siga o procedimento recomendado (PASSO 2).

Ao ler a mensagem, a vítima é induzida a acessar um link para uma página falsa de seu banco e a fornecer seus dados pessoais e os dados de sua conta juntamente com as respectivas senhas (PASSO 3). Após a vítima preencher um formulário eletrônico com tais dados, a página falsa envia um e-mail para o fraudador com essas informações (PASSO 4). A Figura 7 representa todo esse ciclo percorrido (PASSOS) nessa primeira etapa da fraude bancária.

Figura 7 - Representação gráfica da 1ª etapa do Modus operandi investigado na Operação Valentina



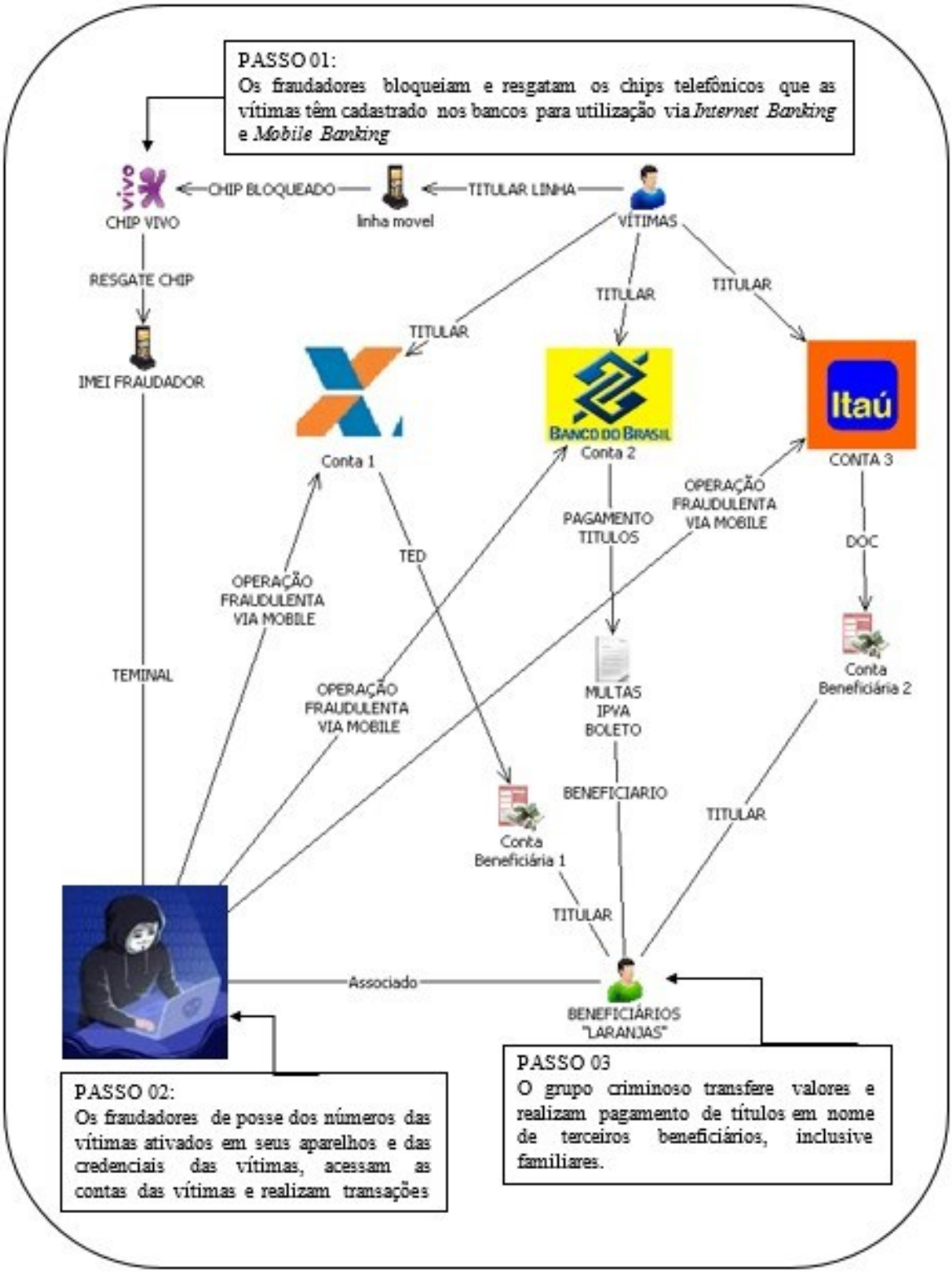
Fonte: Elaborado pelo autor (2019).

ETAPA 2

Nessa etapa o grupo criminoso realiza o desvio dos SIMCARD das vítimas com o aliciamento e auxílio de funcionários das operadoras de telefonia que realizam o bloqueio da linha da vítima da fraude e reativam em um novo SIMCARD que se encontra na posse do fraudador (PASSO 1).

A partir dessa reativação do SIMCARD da vítima (PASSO 2) em poder do fraudador o recebimento de SMS "token" com os códigos autorizadores de operações, o acesso à conta da vítima, via *Internet Banking* e *Mobile Banking*, se dá de forma ilimitada (PASSO 3). A Figura 8 representa os passos percorridos nessa segunda etapa.

Figura 8 - Representação gráfica da 2ª etapa do Modus operandi investigado na Operação Valentina



Fonte: Elaborado pelo autor (2019).

ETAPA 3

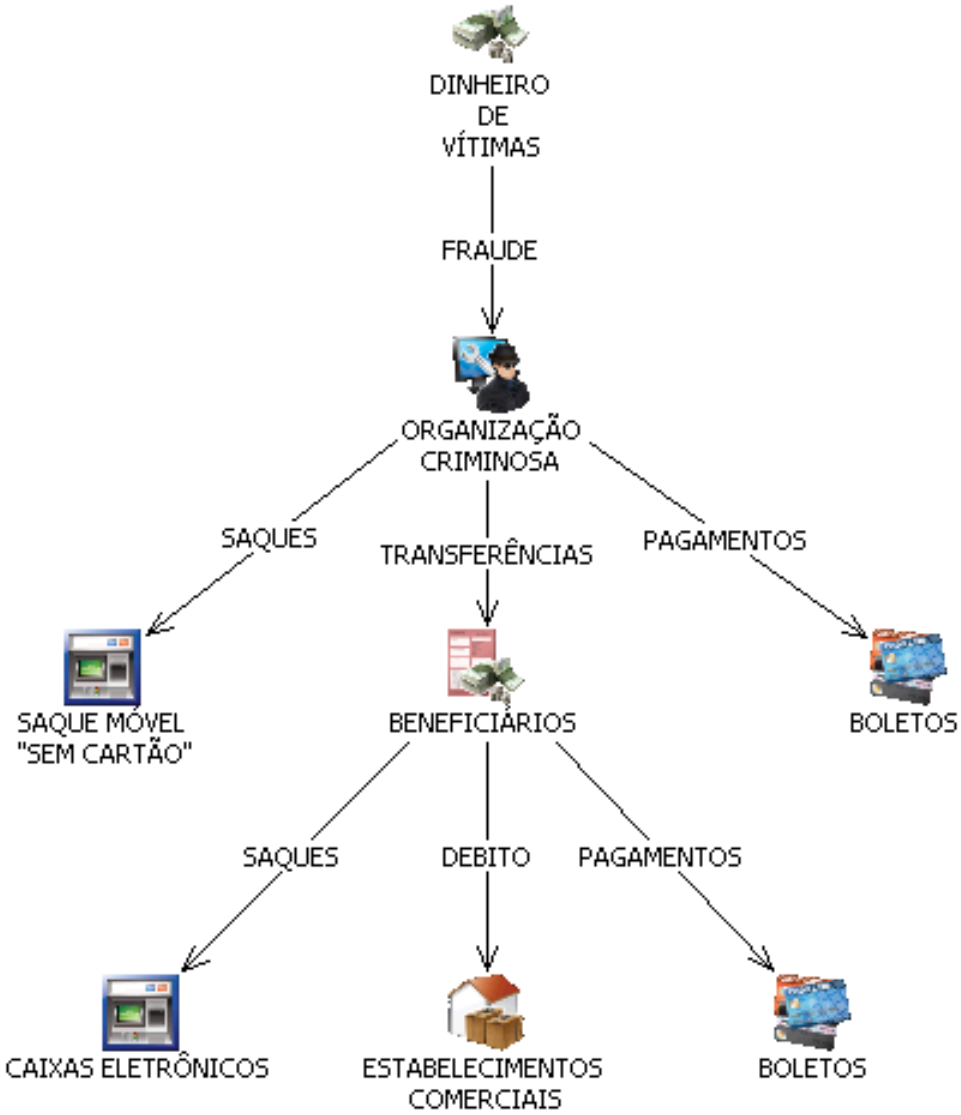
A terceira e última etapa do *modus operandi* dos grupos de fraudadores da Operação Valentina funciona como uma espécie de saturação da etapa 2 e disseminação dos valores obtidos fraudulentamente. O grupo age no intuito de evitar o bloqueio e recuperação dos valores pelos setores de segurança de operações fraudulentas das instituições financeiras. Depois de cumprida a etapa 2, os fraudadores tentam todos os artifícios para realizar no menor espaço de tempo possível a retirada dos valores fraudados.

De forma articulada, minutos após as transferências, um integrante do grupo criminoso se posiciona na porta de bancos e caixas eletrônicos para "sacar" as quantias provenientes das fraudes antes que os setores de prevenção dos bancos detectem a fraude e realizem as tentativas de confirmar a transação e bloquear os valores fraudados.

Por questões de segurança contra fraude as instituições financeiras estipulam limites diários de saques em caixas eletrônicos. Para driblar essa situação os fraudadores arregimentam estabelecimentos comerciais com o objetivo subtrair mais valores das contas das vítimas.

Nesses estabelecimentos os fraudadores deixam os cartões de débitos dos beneficiários "laranjas" para que sejam feitas movimentações financeiras na opção "débito" driblando assim o limite diário de saques em contas correntes. A Figura 9 representa os passos percorridos nessa última etapa.

Figura 9 - Representação gráfica da 3ª etapa do Modus operandi investigado na Operação Valentina



Fonte: Elaborado pelo autor (2019).

2.4.2.2 Resultados Operacionais da Operação Valentina

O grupo criminoso com seus principais membros domiciliados no Ceará, especializado no cometimento de fraudes bancárias eletrônicas em todo o país foi condenado a penas que juntas somam mais de 85 anos de prisão. A investigação policial juntou provas por meio de informações estratégicas e relatórios de inteligência que apontam um prejuízo de R$ 7,5 milhões de reais e feito mais de mil vítimas, embora não tenha sido possível dimensionar o total dos valores fraudados pelos cibercriminosos e o seu número total de vítimas (BORGES, 2018).

A investigação teve como responsáveis dois policiais federais especialistas em crimes cibernéticos, conhecedores de infraestruturas tecnológicas, engenharia de softwares e de sistemas integrados de segurança. Pela complexidade da fraude bancária investigada, além dos responsáveis, a investigação contou ainda com a participação de vários policiais especializados em crimes cibernéticos (FENAPEF, 2017).

Participaram da investigação 09 Policiais Federais especialistas em fraudes bancárias eletrônicas lotados no Grupo de Repressão a Crimes Cibernéticos da PF no Ceará – GRCC/DRCOR/SR/PF/CE; 06 Policiais Federais especialistas em fraudes bancárias eletrônicas enviados de missão para apoio durante a investigação; 04 Policiais Federais para apoio durante a investigação; 03 Delegados de Polícia Federal como Autoridades Policiais que conduziram o Inquérito Policial da investigação;

Segundo dados apontados ao final do Inquérito Policial nº 737/2016 – SR/PF/CE da PF e no Processo nº 0000291-75.2017.4.05.8100 da 32ª Vara Federal do Ceará que originaram a deflagração da Operação Valentina resultaram nos seguintes levantamentos de dados:

a) Produzidas 08 Informações Estratégicas de Inteligência em fraude bancária, sendo que 04 Informações Estratégicas de Inteligência produzidas a partir de consultas na BNFBE;
b) Confeccionados 07 Autos Circunstanciados de Interceptação Telefônica com período de renovação de 15 dias, com registro de 24.116 ligações telefônicas e destas o total de 421 ligações degravadas resultando no volume de dados de 3.26 GB;
c) Confeccionados 06 Autos Circunstanciados de Interceptação Telemática de dados com 16 E-mails investigados com período de renovação de 15 dias;
d) Produzido 01 Relatório Final de Inteligência e análise de alvos com 452 páginas;
e) 30 Ofícios com pedido de informações sobre fraudes bancárias eletrônicas às instituições financeiras vítimas das fraudes investigadas;

Além dos dados acima apresentados foi ainda realizado a quebra judicial de sigilo bancário dos investigados, realizadas inúmeras diligências de campo e identificado o volume de vítimas de fraudes bancárias conforme descrito na próxima seção.

2.4.3 Processos de Contestações e Notícias Crimes sobre fraude bancária analisadas

Com o intuito de demonstrar o atraso na inserção de informações na BNFBE, buscou-se quantificar o número de processos de contestação inseridos na BNFBE no período dos dois anos que transcorreram as investigações da Operação Valentina, visando ilustrar de maneira

mais clara a situação real durante uma investigação acerca dos dados inseridos na BNFBE e os relatórios e informações estratégicas produzidos.

Os processos de contestações inseridos na BNFBE nos anos de 2016 e 2017 correspondem aos listados na Tabela 2 a seguir:

Tabela 2 - Processos de contestação sobre fraude bancária inseridos na BNFBE

Ano	Quantidade de Processos de contestação
2016	35.530
2017	52.869

Fonte: Elaborado pelo autor (2019).

A Tabela 3, mostra os dados quantitativos de informações sobre fraude bancária investigados na operação, mas que em razão do lapso temporal de inserção das informações sobre bancárias na BNFBE não se encontravam na base.

Tabela 3 - Vítimas de fraude bancária relacionadas à Operação Valentina

Ano	Quantidade de informes sobre fraude bancária não inseridos na BNFBE
2016	954
2017	456

Fonte: Elaborado pelo autor (2019).

Embora seja evidente o enorme volume de processos de contestação sobre fraudes bancárias inseridos na BNFBE, o quantitativo de fraude bancárias investigadas na Operação Valentina serviu para uma análise descritiva sobre a perda de oportunidade de se investigar fraudes bancárias sem atraso na comunicação dos processos de contestação ou com informações mais completas que somente o cliente vítima de fraude bancária possui, necessitando assim de uma completude de dados atualizados conforme se dinamiza o modo de agir de grupos criminosos. A título de exemplo sobre a completude de dados que poderiam ser inseridos na BNFBE observados na Operação Valentina sendo considerado informações importantes para a investigação criminal que somente o cliente vítima usuário do sistema bancário detém, tais como número do terminal, link e endereço que encaminhou a mensagem

ou informação maliciosa, dentre outros. As Figuras 10 e 11 mostram a forma que grupos criminosos encaminham mensagens de texto via SMS com os links maliciosos de páginas bancárias falsas.

Figura 10 - Tela dos celulares de vítimas de fraudes bancárias com o recebimento das mensagens de texto via

Elaborado pelo autor (2019).

Figura 11 - Tela dos celulares de vítimas de fraudes bancárias com o recebimento das mensagens de texto via SMS com os links maliciosos de páginas bancárias falsas

Elaborado pelo autor (2019).

Nas Figuras 10 e 11 podemos observar os números telefônicos que enviaram as mensagens de texto via SMS com os links maliciosos de páginas bancárias falsas, o endereço

eletrônico em que as páginas maliciosas ficam hospedadas, bem como a hora e data exata que ocorreu a disseminação das mensagens maliciosas.

3 REFERENCIAL TEÓRICO

O referencial teórico tem como objetivo prover um embasamento e contextualização ao problema de pesquisa, mostrando inicialmente como o tema se adere aos fundamentos dos campos da Ciência da Informação e Ciência Policial. Após isto, expõe-se as considerações sobre cada trabalho relacionada e reportado como relevante dentre os selecionados na busca para revisão de literatura. Por conseguinte, destaca-se seções sobre fraudes bancárias na internet, o papel da vítima de fraude bancária, por fim, tenta-se comentar sobre um modelo de tomada de decisão com a produção de informação estratégica no combate às fraudes bancárias eletrônicas para alimentar a BNFBE do "Projeto Tentáculos" da Polícia Federal.

3.1 RELAÇÃO DO TEMA DE PESQUISA COM A CIÊNCIA DA INFORMAÇÃO E A CIÊNCIA POLICIAL

A Ciência de Informação e a Ciência Policial se aderem à pesquisa sob o contexto das seguintes características que convergem para o objeto de estudo desta pesquisa: a interdisciplinaridade de ambas; a visão da informação como objeto físico central da pesquisa e seus desafios com o advento da internet, assim como o interesse e função social desempenhado pelas duas ciências.

Este trabalho está inserido no contexto dos estudos em abordagens interdisciplinares sobre o gerenciamento de dados e informações sobre fraude bancária eletrônica, desenvolvido no âmbito do eixo de pesquisa Gestão da Informação e do conhecimento do Programa de Pós-Graduação em Ciência da Informação na Universidade Federal de Santa Catarina (UFSC). Trata-se primordialmente de um estudo que tem o intuito de propor melhorias na gestão de informações relacionadas às fraudes bancárias na internet.

A interdisciplinaridade como características das ciências da Informação e Policial se relaciona com a pesquisa pelo interesse por outras áreas dos conhecimentos, tendo a informação sobre fraude bancária como objeto físico que interliga suas relações.

Para Cardoso (1996), a interdisciplinaridade da CI, está relacionada aos problemas enfrentados pela nossa sociedade atual, exigindo soluções inovativas e plurais por todos. Neste sentido, a CI vem se consolidando, então, a partir de elementos emprestados de qualquer ciência que possa contribuir para sua fundamentação e aplicabilidade (CARDOSO, 1996).

Efetividade, comunicação humana, conhecimento, registro do conhecimento, informação, necessidade de informação, usos da informação, contexto social, contexto

institucional, contexto individual e tecnologia da informação são fronteiras da Ciência da Informação que revestem seu caráter interdisciplinar (SARACEVIC, 1996).

Para Saracevic (1996) a variedade de formação de pessoas que se ocupavam com as questões de fronteira descritas acima, em seus mais diversos problemas, caracterizava seus enfoques interdisciplinares e soluções multidisciplinares, mostrando relação com a Ciência da Informação (SARACEVIC, 1996).

Deste modo, observamos o interesse da CI com o campo da Ciência Policial. Suas fronteiras se interligam, revestindo suas características interdisciplinares e multidisciplinares. Nesta pesquisa o documento físico na forma de processo de contestação sobre fraude bancária de interesse para a Ciência Policial serve de fronteira que interliga a Ciência da Informação.

Para Santos Junior; Santos; Silva (2013) a Ciência Policial está composta num amálgama de diversidade, multidisciplinaridade e transdisciplinaridade, requisitando um arcabouço metodológico multidimensional usualmente constituído nas demais ciências. A Ciência Policial se consagra como sendo uma ciência do Estado e da sociedade, suas regras estão definidas no direito constitucional e administrativo, integrando um campo maior do direito público, bem como as demais ciências, mormente, as ciências sociais aplicadas.

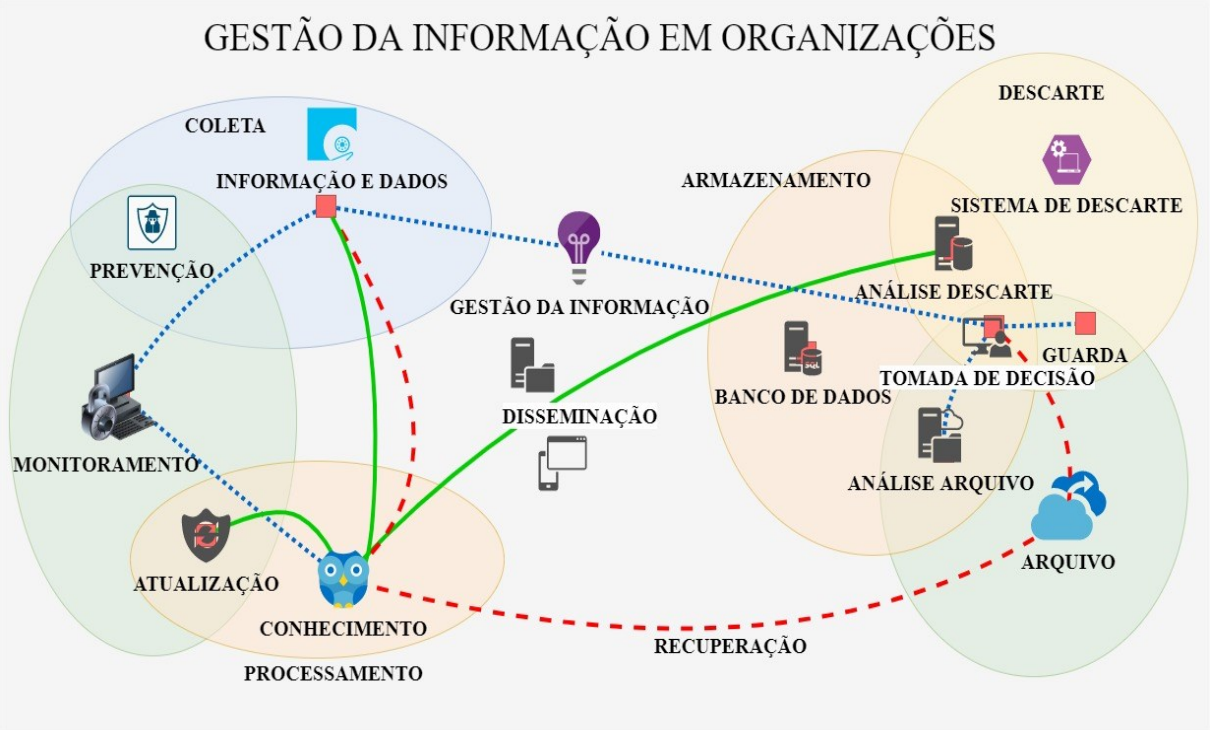
Em outro contexto de visão da Ciência Policial, Ferro Junior (2008) alerta que a comunidade científica policial deve voltar seus olhares de inteligência policial de maneira multidisciplinar de modo a enxergar o aumento crescente da criminalidade em todos seus aspectos. A Ciência Policial deve trilhar seu caminho olhando para o futuro que contemple um ambiente de criminalidade selvagem, violento, sofisticada, organizada e globalizada.

Nessa correlação entre a Ciência da Informação e a Ciência Policial, a informação, como objeto físico central da pesquisa e seus desafios com o advento da internet, surge como elemento essencial de um processo investigativo para operadores da Ciência Policial, na busca de melhorias na gestão das informações no combate às fraudes bancárias pela internet.

Para Valentim (2004), gestão da informação em ambientes organizacionais consiste na reunião de um conjunto de atividades visando obter um processo analítico das necessidades informacionais; adquirir e representar os fluxos de informação a partir de um ou mais setores da organização, ou seja, compreende todo um ciclo de atividade composto de coleta, processamento, monitoramento, disseminação, arquivamento ou descarte, objetivando apoiar o desenvolvimento das ações cotidianas e o processo decisório nesses ambientes. Davenport e Prusak (1998) resume gestão da informação em ambientes organizacionais no modo como as organizações obtêm, distribuem e usam a informação e o conhecimento por meio de um ciclo estruturado de atividades.

A Figura 12 ilustra o ciclo de atividade no ambiente de gestão da informação em organizações propostos por Valentim (2004) e Davenport e Prusak (1998).

Figura 12 - Representação gráfica resumida de gestão da informação em ambientes organizacionais.



Fonte: Elaborado pelo autor (2020) adaptado de Valentim (2004) e Davenport e Prusak (1998).

O tema e a pergunta da presente pesquisa, bem como o objetivo geral, se relacionam na medida que trata de descrever o conjunto de atividades realizadas com as informações sobre fraude bancária coletadas, a sua inserção, armazenamento e disseminação, bem como propõe o desenvolvimento de melhorias nesse processo de alimentação da BNFBE.

A Pesquisa Nacional por Amostra de Domicílios Contínua - PNAD Contínua, indicam que em 2016 mais de 116 milhões de brasileiros fazem uso de algum modo da internet (BRASIL, 2016). A popularização da rede mundial de computadores trouxe a potencialização de condutas delituosas já praticadas anteriormente, só que agora por meio de um novo canal e *modus operandi*, como é o caso das fraudes bancárias. Esta potencialização resultou em um aumento substancial da quantidade de fraudes cometidas com o advento da internet (SIQUEIRA, 2014).

Uma vez ocorrendo fraude bancária pela internet, a vítima de fraude bancária precisa externalizar na forma de notícia crime a forma como ocorreu a fraude. Aquele conhecimento

sobre a fraude sofrida precisa ser materializado na forma de informação para contribuir para a persecução penal.

Informação é um fenômeno que envolve indivíduos transmitindo e recebendo mensagens no contexto de suas ações possíveis (CAPURRO; HJÖRLAND, 2007).

Buckland (1991), ao conceituar informação-como-coisa, reintroduz o conceito de documento e processo podendo como informação-como-coisa, ressalta a natureza subjetiva da informação como qualquer coisa que possa ser informativa e tratada por sistemas de informação (BUCKLAND, 1991).

A ciência da informação (CI) como ciência social, em seus estudos Araujo (2003), considera a ciência da informação em sua natureza de ciência social quanto de ciência pós-moderna. Procura contextualizar a CI de maneira teórica numa realidade social de uma perspectiva estatística e quantitativa, com apropriação dos princípios filosóficos da dialética. De maneira prática entende a CI como algo construído socialmente e não com uma existência em si mesma, independentemente dos sujeitos que conhecem. Em seu apanhado, a informação não seria somente um dado, uma coisa que teria um significado ou uma importância em si, mas um processo percebido e compreendido de variadas formas de acordo com os sujeitos que estão envolvidos (ARAUJO, 2003).

Segundo Wersig (1993), a CI seria estabelecida como um protótipo de um novo ou uma ciência pós-moderna. A ciência pós-moderna não é como a ciência clássica, impulsionada pela busca de uma compreensão completa de como o mundo funciona, mas pela necessidade de desenvolver estratégias para resolver em particular, os problemas que foram causados pelas ciências e tecnologias.

Feito este apanhado, observamos que os conceitos de ciência da informação, ciência policial, informação e suas características relacionadas, possuem fronteiras com o objeto de estudo desta pesquisa, dando assim suporte para continuidade pelo referencial teórico que adiante se segue.

3.2 BUSCA PARA REVISÃO DE LITERATURA

A busca para a revisão de literatura teve o intuito de selecionar os principais autores e obras já produzidos acerca de assuntos ligados aos termos fraudes bancárias pela internet e ao tema da pesquisa. Neste aspecto, a pesquisa se desenvolveu essencialmente em relação aos termos relacionados à fraude bancária pela internet. Para composição da pesquisa foram

elencados artigos científicos, monografias, teses, dissertações, livros, dentre outros trabalhos com publicação nacional e internacional.

A metodologia utilizada para elaboração desta busca tem por base o exemplo seguido por Sampaio e Mancini (2007) sugerindo como método os critérios de:

1) definir a pergunta de pesquisa;
2) buscar evidências;
3) revisar e selecionar os estudos;
4) analisar a qualidade dos estudos;
5) apresentar os resultados da pesquisa.

Vale ressaltar que o método de pesquisa utilizado por Sampaio e Mancini (2007) segue as diretrizes proposta no campo da medicina. Por outro lado, embora os estudos nessa área buscam reunir o somatório de provas relativos aos tratamentos médicos e a busca sistemática serve para identificar evidências de pesquisas anteriores. Outrossim, as diretrizes de revisões de literatura em outras áreas de estudo, fora da medicina, como nas ciências sociais, muitas vezes não conseguem reconhecer esta limitação e, portanto, são mal interpretadas como oferecendo uma abordagem geral para a realização de revisões de literatura, enfatizando mais no rigor, detalhamento no processo de pesquisa e qualidade no processo de identificação da literatura (BOELL E CECEZ-KECMANOVIC, 2014).

Para Boell e Cecez-Kecmanovic (2014) o uso de terminologias alternativas e a falta de precisão dos termos de pesquisa representa um problema frequente na recuperação da informação. Do mesmo modo, a indeterminação da linguagem e as interpretações diferentes reportam resultados incertos para de diferentes expressões usadas para descrever um termo de pesquisa.

Com isso, além da revisão adquirida em livros e artigos obtidos por meio físico em bibliotecas e livrarias, foram realizadas buscas em fontes consideradas de referência na área de Ciência da Informação, listadas no Portal de Periódicos da Capes, em especial, na Biblioteca Digital Brasileira de Teses e Dissertações – BDTD/IBICT, assim como na base de dados internacionais, *Web of Science*.

Inicialmente tentou-se utilizar os termos “fraude bancária na internet” em português e ‘*fraud internet banking*” em inglês, de forma fechada por completo, sendo reportado um número de produção cientifica muito pequeno. Deste modo, com o intuito de obter resultados mais abrangentes, optou-se por utilizar a seguinte metodologia de pesquisa: fraude and bancária and internet em português e internet and *banking* and *fraud* em inglês.

Neste sentido, observamos que o tema relacionado às fraudes bancárias pela internet, embora pareça ser recorrente e comum, não demonstra grande volume de produção científica proporcional ao crescente número e diversidades de fraudes bancárias que ocorrem por meio da internet em todo mundo.

Quanto aos aspectos da criminalidade, o tema causa enorme prejuízos às instituições financeiras e grande dispêndio de capital humano e tecnológico por parte de órgãos governamentais no combate a este tipo de fraude, embora ainda o volume de produção científica não represente o tamanho dos danos causados com esse tipo de crime.

Adiante é demonstrado o resultado das buscas realizadas no Portal de Periódicos da Capes, em especial, na Biblioteca Digital Brasileira de Teses e Dissertações – BDTD/IBICT, assim como na base de dados internacionais, *Web of Science*.

3.2.1 Consulta Literária sobre Fraude Bancária na Internet na Biblioteca Digital Brasileira de Teses e Dissertações – BDTD/IBICT

A revisão de literatura de produções científicas produzidas com a busca na base de dados da Biblioteca Digital Brasileira de Teses e Dissertações – BDTD/IBICT demonstrou a produção de artigos de grande relevância quanto ao conteúdo produzido por partes dos autores, sendo conteúdo primordial para enriquecimento do presente trabalho, no entanto, mostrou que ainda são poucos os trabalhos acadêmicos produzidos relacionados à Fraude Bancária, e menor ainda quando refinadas em especial aos aspectos quando ocorridas pela internet.

A busca na base de dados da Biblioteca Digital Brasileira de Teses e Dissertações – BDTD ocorreu com as seguintes etapas:

a) Busca alternada com os termos da expressão “Fraude Bancária na internet”, em diferentes composições, tendo como estratégia de busca a seleção por “Todos os campos”;
b) A recuperação de dados da busca retornou como resultado as produções cientificas relacionadas aos termos pesquisados;
c) Os resultados foram dispostos por tipo de documento;
d) Os dados disponibilizados para a pesquisa que demonstrou maior interesse, foram exportados no formato em Excel com a exportação definida no formato Export CSV, sendo gravado o conteúdo nesse formato;

O Quadro 3 a seguir resume o resultado da busca pelos diferentes tipos de combinações do termo “Fraude Bancária na Internet”, apresentando as produções cientificas reportadas com as expressões de busca utilizadas pelo número de trabalhos produzidos e o número de trabalhos relacionados a pesquisa.

Quadro 3 - Levantamento de trabalhos reportados na pesquisa - BDTD/IBICT

Expressão de Busca	Nº Trabalhos produzidos X Expressão de busca utilizada	Nº Trabalhos relacionados à pesquisa X Expressão de busca utilizada
Fraude AND Bancária AND Internet	141	7
“Fraude Bancária” AND Internet	133	7
Fraude AND “*Internet Banking*”	7	7
"Fraude bancaria" AND “*Internet Banking*”	2	2

Fonte: Elaborado pelo autor (2019).

Com os resultados dos trabalhos recuperados, com a leitura dos títulos e resumos dos trabalhos, foi possível observar que os (07) sete trabalhos reportados com a expressão de busca (Fraude AND “Internet Banking”) possuíam grande relevância para a pesquisa, sendo realizada a leitura por completa dos trabalhos selecionados com a expressão de busca (Fraude AND “Internet Banking”), estando discorridos cada um na seção trabalhos relacionados.

Deste resultado, foi possível listar os trabalhos relevantes e relacionados à pesquisa conforme descritos no Quadro 4, ordenados por relevância decrescente de pesquisa, pelo nome do(s) autor (es), o título do trabalho e o ano de produção.

Quadro 4 - Descrição da Formação e Características

Ordem de Relevância de citação com o tema	Autor	Título	Ano
01	Marcelo Lau	Análise das fraudes aplicadas sobre o ambiente Internet Banking	2006
02	André Luis Damiano	As fraudes no Internet Banking e sua evolução para o Social Banking	2013
03	Patrocínio, Álex Moreira do	Técnicas baseadas em grafos para priorização de investigações policiais de fraudes bancárias eletrônicas	2016
04	Stephan Kovach	Detecção de fraudes em transações financeiras via Internet em tempo real	2011
05	Klettenberg, Josiane	Segurança da informação	2016
06	Arthur Wongtschowski	Segurança em aplicações transacionais na internet: o elo mais fraco	2006
07	ARCOVERDE, Henrique Ferraz	Malwares brasileiros: técnicas, alvos e tendências	2013

Fonte: Elaborado pelo autor (2019).

3.2.2 Consulta Bibliográfica sobre Fraude Bancária na Internet Contida na Base Web Of Science

Para a revisão de literatura de produções científicas internacionais, foi realizado buscas no repositório da base de dados da *Web of Science*, sendo reportado como resultados das pesquisas, produções científicas importantes e de grande relevância quanto ao conteúdo produzido por partes dos autores, sendo, assim, como a pesquisa na base de dados da Biblioteca Digital Brasileira de Teses e Dissertações – BDTD, conteúdo de suma importância para enriquecimento do presente trabalho. A pesquisa, mesmo ampla, mostrou também a pequena quantidade de artigos e de outras produções científicas produzidas relacionados aos termos Fraude Bancária na Internet em inglês "Fraud Internet Banking", mas que, embora sendo pouco os resultados, o conteúdo das produções bastante relevantes para a pesquisa.

A busca na base de dados internacional da *Web of Science* ocorreu com as seguintes etapas:

a) Busca alternada com os termos da expressão "Fraud Internet Banking", em diferentes composições, tendo como estratégia de busca a seleção por "Tópico";

b) A recuperação de dados da busca retornou como resultado as produções cientificas relacionadas aos termos pesquisados;

c) Os resultados foram refinados com a habilitação dos "Tipos de documento" para "Article";

d) Os dados disponibilizados para a pesquisa que demonstrou maior interesse foram exportados no formato em Excel com a exportação definida no formato salvar em outros formatos de arquivo; gravado o conteúdo como Registros completo e Referências citadas, e o formato de arquivo por Separação por tabulação (Win).

O Quadro 5 a seguir resume o resultado da busca pelos diferentes tipos de combinações do termo "Fraud Internet Banking", apresentando as produções cientificas reportadas, dentre elas Proceedings Paper, Articles e Editorial Material, com as expressões de busca utilizadas pelo número de artigos científicos produzidos e o número de artigos científicos produzidos relacionados a pesquisa.

Quadro 5 - Levantamento de trabalhos reportados na pesquisa – *Web of Science*

Expressão de Busca		Nº Produções Científicas produzidas X Expressão de busca utilizada		Nº Artigos Científicos produzidos X Expressão de busca utilizada	Nº Artigos Científicos produzidos relacionados à pesquisa X Expressão de busca utilizada
Fraud AND Internet AND Banking		94		35	6
Fraud AND "Internet Banking"		25		7	6
"Internet Banking Fraud"		5		0	0

Fonte: Elaborado pelo autor (2019).

Com os resultados dos trabalhos recuperados, com a leitura dos títulos e resumos dos trabalhos, foi possível observar que os (06) seis artigos científicos reportados com a expressão de busca (Fraude AND Internet AND Banking"), possuíam relevância para a pesquisa, englobando também os mesmos artigos científicos reportados com a expressão de busca (Fraude AND "Internet Banking"), sendo realizada a leitura por completa dos trabalhos selecionados.

Deste resultado, foi possível listar os artigos científicos relevantes e relacionados à pesquisa conforme descritos no Quadro 6, ordenados por relevância decrescente de pesquisa, pelo nome do(s) autor (es), o título do trabalho e o ano de produção.

Quadro 6 - Lista dos trabalhos considerados relevantes à pesquisa após a busca na base de dados internacional da *Web of Science*

Ordem de Relevância de citação	Autor	Título	Ano
01	Carminati, M; Caron, R; Maggi, F; Epifani, I; Zanero, S	BANKSEALER: A decision support system for online banking fraud analysis and investigation	2015
02	Hartmann-Wendels, T; Mahlmann, T; Versen, T	Determinants of banks' risk exposure to new account fraud - Evidence from Germany	2009
03	Shanmugam, M; Wang, YY; Bugshan, H; Hajli, N	Understanding customer perceptions of internet banking: the case of the UK	2015
04	Jansen, J; van Schaik, P	Testing a model of precautionary online behaviour: The case of online banking	2018
05	Kiljan, S; Simoens, K; De Cock, D; Van Eekelen, M; Vranken, H	A Survey of Authentication and Communications Security in Online Banking	2017
06	Guijarro, EGL; Silva, LCA	The risks of Internet banking transactions	2017

Fonte: Elaborado pelo autor (2019).

Na seção a seguir com o título Trabalho Relacionados, foram tratados as discussões e comentários sobre os trabalhos reportados nesta busca para revisão de literatura em relação aos estudos propostos nessa pesquisa.

3.3 TRABALHOS RELACIONADOS À FRAUDES BANCÁRIAS PELA INTERNET

Entre os trabalhos científicos relacionados ao tema sobre fraude bancária na internet, alguns foram de primordial importância para a composição da fundamentação teórica desta pesquisa. Importante destacar que os trabalhos explanados nesta seção são decorrentes do resultado das consultas da subseção 3.2.1 e 3.2.2 sobre busca para revisão de literatura.

Adiante estão contextualizados os trabalhos relacionados reportados na consulta a Biblioteca Digital Brasileira de Teses e Dissertações – BDTD/IBICT.

O trabalho com título "Análise das fraudes aplicadas sobre o ambiente Internet Banking", apresentado por Marcelo Lau em 2006 à Escola Politécnica da Universidade de São Paulo para obtenção do título de Mestre em Engenharia. É uma das primeiras produções científicas no brasil que contextualizam fraudes bancárias com o início do oferecimento dos serviços de *internet banking* pelo sistema bancário.. O trabalho serviu de primordial importância para a pesquisa no sentido de contextualizar a evolução das fraudes bancárias pela internet e definir os atores envolvidos no processo de comunicação das contestações de fraude bancária na Polícia Federal (LAU, 2016).

Do mesmo modo, a pesquisa realizada por André Luis Damiano em 2013 para conclusão de seu mestrado em Engenharia de Produção na Escola de Engenharia de São Carlos da Universidade de São Paulo, com o título "As fraudes no *Internet Banking* e sua evolução para o *Social Banking*", faz um apanhado das principais questões e desafios referentes às fraudes bancárias eletrônicas e suas ameaças, além de descrever as tendências das fraudes no ambiente de *Internet Banking* e sua evolução para o *Social Banking*. Neste aspecto relaciona-se com a presente pesquisa no sentido de contextualizar o papel das vítimas de fraude bancárias e sua importância para contribuição dos processos investigativos e dificuldades advindas com uso cada vez mais recorrente de novas tecnologias oferecidas pelo sistema bancário (DAMIANO, 2013).

A dissertação com o título "Técnicas baseadas em grafos para priorização de investigações policiais de fraudes bancárias eletrônicas", defendida por Álex Moreira do Patrocínio em 2016 para obter o título de mestre em Engenharia Elétrica pela Universidade de Brasília, surge pela primeira vez como uma dissertação de mestrado em que discorre sobre o papel da Polícia Federal do Brasil (PF) em concentrar esforços para elucidar crimes de fraudes bancárias praticados contra a empresa pública e instituição financeira da Caixa Econômica Federal (CAIXA). O trabalho propõe aprimorar a experiência investigativa por meio de técnicas com o uso de grafos e análise de vínculos, denominada Kraken, tendo como base as informações

inseridas na Base Nacional de Fraudes Bancárias Eletrônicas (BNFBE), sendo essas informações transformadas em grafos conexos, que representem os atores e seus relacionamentos (vínculos) na ação delitiva desse tipo de fraude, servindo assim a ferramenta como uma interface gráfica. Importante registrar nessa pesquisa, a contribuição prestada na fundamentação teórica do mencionado trabalho acerca da produção científica apresentada por Siqueira, E. P. em 2014 como o título "O Projeto Tentáculos da Polícia Federal: Da concepção à Proposta de Modelo Aplicável na Segurança Pública Brasileira como requisito do título de Especialização em Gestão da Segurança da Informação e Comunicações pela Universidade de Brasília. Nesse trabalho, o autor e um dos idealizadores do Projeto Tentáculos faz um apanhado do modelo investigativo desde sua concepção até a proposta de modelo nacional de centralização das informações sobre fraudes bancárias eletrônica, sendo este trabalho base fundamental para contextualização da fundamentação teórica da presente pesquisa (SIQUEIRA, 2014).

A tese de doutorado de Stephan Kovach (2011), com o título "Detecção de fraudes em transações financeiras via Internet em tempo real" apresenta o desenho de proposta de uma arquitetura de um sistema de detecção de fraudes em tempo real em transações bancárias via Internet, baseando-se em observações do comportamento local e global de usuários. O trabalho inovador merece destaque em relação ao tema da pesquisa quanto aos atributos e características locais de uma transação bancária que descrevem as atividades de uma transação bancária em contas correntes de usuários do sistema bancário, assim como outras questões relacionadas aos atributos que compõem uma fraude bancária. Possui deste modo relevância com a pesquisa em relação a proposta de um modelo de layout padrão para uniformização das comunicações de fraudes bancárias por todas instituições financeiras que realizaram acordos de cooperação com a Polícia Federal.

Outro trabalho de interesse para a pesquisa foi a dissertação de mestrado com o título "Segurança da informação", defendida por Josiane Klettenberg em 2016 para obtenção do título de mestre pela Universidade Federal de Santa Catarina. A pesquisa tinha 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 por meio da internet banking. O trabalho também serviu como embasamento para compor o referencial teórico da pesquisa quanto à segurança da informação, engenharia social sobre a vítima de fraude bancária e contextualização dos relatos de fraudes bancárias obtidos com o estudo (KLETTENBERG, 2016).

A produção científica com título “Segurança em aplicações transacionais na internet: o elo mais fraco” proposta por Arthur Wongtschowski (2006), como requisito ao mestrado em Engenharia pela Escola Politécnica da Universidade de São Paulo tem sua relevância como contribuição para a pesquisa na composição do referencial teórico quanto a evolução dos tipos e métodos de ataques sofridos por usuários de serviços pela internet.

O trabalho proposto por Henrique Ferraz Arcoverde (2013) com o título “Malwares brasileiros: técnicas, alvos e tendências” como requisito a obtenção do mestrado em Ciência da Computação pela Universidade Federal de Pernambuco, faz uma análise minuciosa dos artefatos maliciosos brasileiros que causam ataques cibernéticos. Do mesmo modo do trabalho acima mencionado, tem importância para a pesquisa na composição do referencial teórico quanto a evolução das tecnologias, tipos e métodos de engenharia social utilizada nos ataques aos usuários serviços pela internet, em especial os serviços bancários.

A seguir discorre-se sobre os trabalhos relacionados reportados na consulta à base de dados internacionais, *Web of Science*, cabendo destacar a diversidade de países que a pesquisa retornou, dentre eles Estados Unidos, Alemanha, Reino Unido, Holanda e Equador, todos com assuntos relacionados às fraudes bancárias pela internet de algum modo, seja pelos estudos de casos práticos, seja por estudo de referencial teórico.

O artigo de Carminati *et al.* (2015) com o título “BANKSEALER: A decision support system for online banking fraud analysis and investigation” tem como objetivo desenhar um sistema de suporte a tomada de decisões sobre fraudes bancárias. Possui semelhança com os objetivos propostos na tese de doutorado de Stephan Kovach (2011), com o título “Detecção de fraudes em transações financeiras via Internet em tempo real” já mencionado acima. Nesse artigo, Carminati *et al.* (2015) desenha modelos para quantificar anomalias em transações bancárias pelo perfil do usuário em relações a padrões previamente estabelecidos, criando cenários de fraudes e comparando com ataques típicos e reais. Neste sentido possui relevância com a pesquisa em relação à proposta de um modelo de layout padrão para uniformização das comunicações de fraudes bancárias por todas instituições financeiras que realizaram acordos de cooperação com a Polícia Federal, podendo ter como referencial teórico os perfis de ataques e fraudes sofridas que o artigo científico discorre em seus ensaios.

Os autores Hartmann-Wendel; Mählmann; Versen (2009) publicam artigo com o título “Determinants of banks' risk exposure to new account fraud - Evidence from Germany”, logo na introdução do artigo discorre que naquele tempo em evidências na Alemanha, fraudes bancárias com uso de uma identidade falsa, inventada ou roubada, para abrir uma nova conta, normalmente para obter um cartão de crédito ou empréstimo, está se tornando uma séria

preocupação na economia baseada em informações. Discorre ainda que segundo estatísticas oficiais do Departamento Federal de Polícia Criminal da Alemanha, os custos totais para bancos de fraudes com novas contas aumentaram de 13 milhões de euros em 1999 para mais de 35 milhões de euros em 2006. Deste modo o artigo possui relevância para a pesquisa quanto ao apanhado histórico e evolução das modalidades de fraudes bancárias como contextualização do referencial teórico da presente pesquisa.

Já os autores Hajli; Shanmugam; Wang; Bugshan, (2015), publicam no Reino Unido artigo científico com o título "Understanding customer perceptions of internet banking: the case of the UK" relatando sobre um estudo de caso sobre as percepções dos clientes de serviços bancários pela internet. No estudo de caso é detalhada as percepções dos clientes usuários de serviços bancários por meio do Internet banking. O estudo visou primordialmente aumentar a confiabilidade, tendo a segurança como fator mais importante na prestação dos serviços bancários pela internet naquele país. Assim, o referido trabalho científico possui interesse para a pesquisa tendo em vista se relacionar às percepções das vítimas de fraudes bancárias, sob o ponto de vista como cliente usuário dos serviços bancários por meio de internet banking.

O trabalho de Jansen; Van Schaik (2018) com título "Testing a model of precautionary online behaviour: The case of online banking" possui foco na proteção no acesso indevido realizado por terceiros às contas bancárias por meio da internet a usuários do sistema bancário. O artigo mostra um estudo de caso realizado na Holanda. Centra-se na segurança dos serviços bancários via internet banking. O trabalho se propõe a disseminar metodologias e rotinas para melhorar a educação de segurança, campanhas de treinamento e conscientização direcionadas aos usuários dos serviços bancários pela internet, possuindo assim relação com o problema de pesquisa deste trabalho.

A Survey of Authentication and Communications Security in Online Banking foi um artigo recentemente publicado por Kiljan; Simoens; Cock; Eekelen; Vranken (2017). Na pesquisa, Kiljan et al faz um apanhado histórico da aplicação do internet banking, ressaltando as diferenças de uniformidade entre segurança das comunicações e autenticação do usuário diante das mudanças tecnológicas e sociais com o advento da internet, descrevendo métodos de autenticação de usuário via mobile banking, tendo assim relação com a pesquisa em virtude das condições de diferença de padronização de prestação de serviços bancários, assim como na despadronização da comunicação das notícias crime de fraudes bancárias no sistema bancário brasileiro. Deste modo servido como referencial teórico para a pesquisa.

Guijarro e Silva (2017) da mesma forma, publicam também artigo recentemente em 2017 no Equador com o título "Los riesgos de las transacciones bancarias por Internet" em que

faz uma análise documental de referencial teórico, conceituando os diferentes tipos de fraudes mais comuns na Internet. O autor faz uma contextualização da problemática atual sobre fraudes bancárias no Equador, ressaltando que o aumento de transações bancárias pela internet fez surgir a necessidade de novas medidas de segurança tendo em vista a incidência do aumento de fraudes maior que o esperado. O trabalho possui relevância para a pesquisa por discorrer sobre os tipos de fraudes bancárias pela internet, bem como do apanhado histórico sobre fraudes bancárias antes do advento da internet.

Antes de adentrar nos aspectos sobre fraude bancária eletrônica, na seção a seguir busca expor de uma forma mais ampla os aspectos relacionados ao anonimato, vigilância e privacidade relacionados à vítima de fraude bancária e os cibercriminosos que cometem esse tipo de fraude.

3.4 ANONIMATO, VIGILÂNCIA E PRIVACIDADE DOS ATORES ENVOLVIDOS EM FRAUDE BANCÁRIA NA INTERNET

O espectro deste trabalho será o ambiente de fraude bancária pela internet por meio do *internet banking* ou *mobile banking*, considerado, assim, uma modalidade de fraude eletrônica que resulta muitas vezes em crimes das mais diversas formas de ataques, assim entendidos também como um tipo de crime cibernético ou cibercrime.

Crime cibernético de maneira prática é definido como a conduta facilitada pela tecnologia da informação ou comunicação como veículo ou ferramenta no intuito de cometer o mal, prejuízo ou dano corpóreo ou incorpóreo contra uma pessoa ou organização, sendo a fraude bancária eletrônica uma modalidade deste delito criminoso (BROWN, 2015).

Para Brown (2015), a informação como meio de prova está cada vez mais sendo armazenada, transmitida ou processada em formato eletrônico. A tecnologia se tornou o símbolo, sujeito (local), ferramenta (instrumento) e objeto (alvo) de crime, sendo comum o crime cibernético ser transnacional em termos de localização física das vítimas, perpetradores e evidência.

Brown (2015) afirma ainda que a interconectividade da economia global permite que criminosos operem e cometam crimes em qualquer lugar e sobre qualquer jurisdição, com elementos discretos de seus crimes espalhados amplamente em todo o mundo em tempo e espaço. Seu acompanhamento se torna algumas vezes ineficaz, tendo em vista que um suspeito criminoso pode ser apreendido em uma jurisdição, mas prova digital necessária para avançar uma investigação podem residir em outro país.

A contemporaneidade, com o surgimento da internet, trouxe avanços tecnológicos que deram aos indivíduos um grande desejo por informação e seus consumos. Neste sentido, termos como privacidade, vigilância e anonimato relacionados ao indivíduo ganham novas reflexões na medida que a globalização por meio da internet passa a registrar e deter tais dados e informações. O indivíduo passa a ser vigiado de forma invisível, muitas vezes sem seu conhecimento, em especial em relação aos indivíduos envolvidos no processo de fraude bancária por meio da internet.

Para Lyon (2010), os dados e informações trafegam com mais fluidez na visão das pessoas e assim como Bauman, a fragilidade dos laços sociais remetem a uma ideia de vigilância líquida, onde a modernidade trouxe uma relação de desconfiança entre os indivíduos de uma sociedade. Lyon cita como exemplos diante das necessidades de consumo, que as pessoas se tornam vulneráveis e que todos estão sujeitos aos perigos existentes a partir das relações de confiança, sendo cada indivíduo um ser estranho e perigoso, podendo ser um pedófilo, terrorista, dentre outros indivíduos não merecedores de confiança.

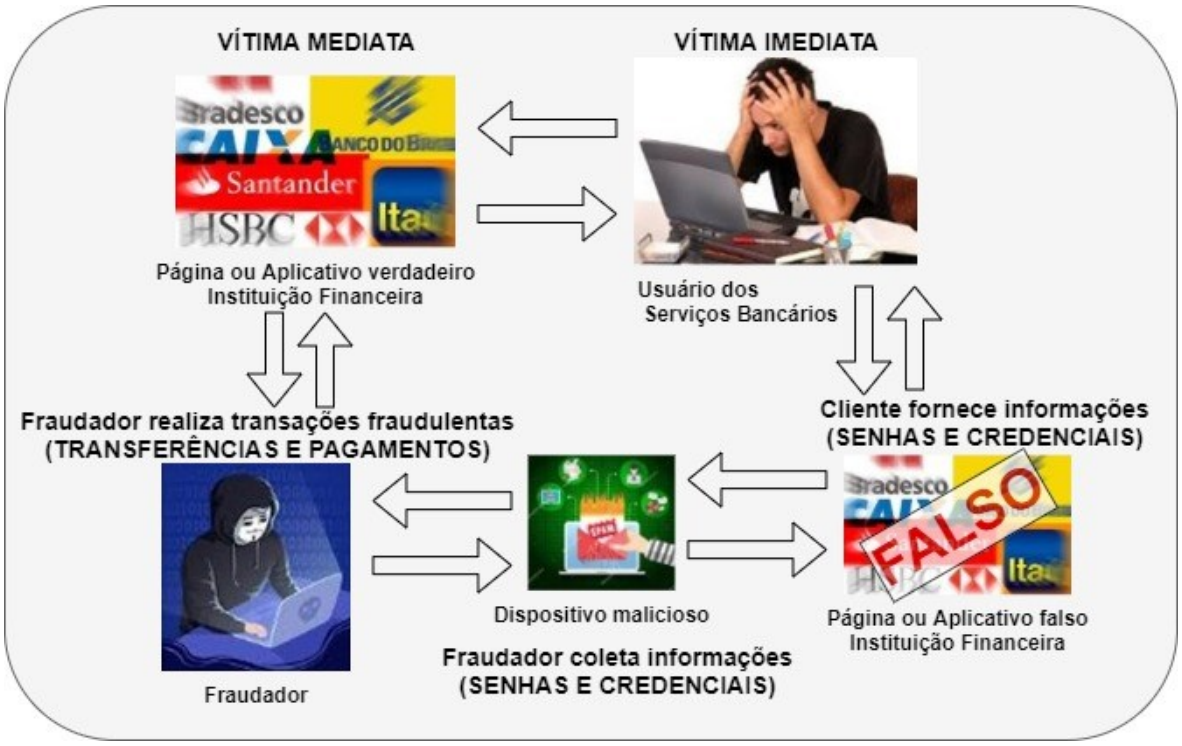
Neste contexto, não poderia ser diferente em relação aos sujeitos ligados às fraudes bancárias por meio da internet, em especial a vítima de fraude bancária e aqueles que se beneficiam das fraudes. A primeira quando necessita da internet para realização de transações bancárias, se torna vulnerável aos ataques; o segundo, que no aparente anonimato, vigiando invisivelmente a primeira, logra muitas vezes êxitos no cometimento da fraude diante do conjunto de informações que detém da vítima atacada.

A característica relativamente anônima e sem rosto do crime cibernético complica questões associadas aos relatórios de vitimologia e cibercrime. Existe equívoco generalizado entre as comunidades sobre a natureza do crime cibernético e capacidade de aplicação da lei para apreender os infratores. A falta de consciência sobre os mecanismos de comunicação para identificar vítimas e perpetradores de crimes cibernéticos e a relutância das vítimas prejudica a capacidade da polícia para responder aos avanços dos crimes cibernéticos (BROWN, 2015).

No contexto da presente pesquisa, podem ser diferenciados dois tipos de vítimas de uma mesma fraude bancária perpetrada. O cliente usuário do sistema bancário que teve sua conta fraudada e valores de sua conta desviados poderia se caracterizar como a vítima de fraude bancária imediata. A instituição financeira que diante da legislação de proteção e defesa dos usuários dos serviços bancários disponibilizados a seus clientes e das falhas nas regras de segurança desses produtos tendo que ressarcir os valores fraudados arcando quase que todas vezes com os prejuízos das fraudes cibernéticas, assim consideradas como vítimas mediatas dessas fraudes.

A vítima imediata, cliente usuário dos produtos e serviços disponibilizados pela instituição que ativa e diretamente forneceu por meio de engenharia social suas senhas e credenciais possibilitando a perpetração da fraude. A vítima mediata, instituição financeira que indiretamente com a participação involuntária da vítima imediata teve sua página ou aplicativo de serviços bancários acessados de forma fraudulenta. A Figura 13 mostra a representação gráfica resumida do *modus operandi* da fraude bancária.

Figura 13 - Representação gráfica resumida do modus operandi da fraude bancária considerando as vítimas imediata e mediata.



Fonte: Elaborado pelo autor (2019).

Para a vítima de fraude bancária, a necessidade de se informar e as facilidades dos usos de meios tecnológicos práticos que se modernizam rotineiramente tornam-se cada vez mais presente e inseguro em seu cotidiano. Bauman (2013, p. 7) propõe o termo “Vigilância líquida” como a maneira de encarar o que a modernidade trouxe e que perturbam uma sociedade consumista em que informações que o indivíduo pensa em fornecer para uma finalidade, de fato visa atender outro fim.

Quanto aos criminosos que se beneficiam com o cometimento de fraudes bancárias por meio da internet, do mesmo modo que a modernidade facilitou o dia a dia dos cidadãos, inseriu num aparente anonimato indivíduos que se utilizam de dados pessoais de outras pessoas, obtidos de forma invisível ou sem o conhecimento destes para obter sucesso nos ataques.

3.4.1 Do Aparente Anonimato Criminoso a Vigilância da Vítima de Fraude Bancária na Internet

É sabido que a permanente necessidade do uso de tecnologias de informação e comunicação, que facilitam os desejos de consumos dos indivíduos, faz com que estes se tornem vulneráveis e expostos de suas informações pessoais. No momento em que indivíduos se utilizam de meios tecnológicos para se informar e comunicar, abre margem para serem monitorados. Muitas vezes, indivíduos utilizando de meios tecnológicos agem em aparente anonimato, fazendo com que pessoas sejam vigiadas e repassem informações de forma inconsciente ou despercebida, agindo quase que invisível.

Embora Bauman (2013, p. 20) em diálogos com Lyon exponha reflexões de outros pensadores sobre os avanços tecnológicos, no qual a internet se tornou o ambiente de "morte do anonimato", em que os próprios indivíduos abrem mão de seus direitos de privacidade, em troca dos benefícios oferecidos pela modernidade como preço razoável pelas maravilhas oferecidas em troca.

Muitas vezes, vítimas de fraudes bancárias na internet, no intuito de usufruir dos benefícios tecnológicos de ter as operações bancárias ao toque de um clique de computador ou celular, tornam-se vulneráveis aos ataques invisíveis, sendo vigiadas permanentemente.

O autor indica ainda como justificativa da insegurança e erosão dos anonimatos, a mudança na visão das pessoas do que deve ser público e o que deve ser privado:

> Essa erosão do anonimato é produto dos difundidos serviços da mídia social, de câmeras em celulares baratos, sites grátis de armazenamento de fotos e vídeos e, talvez o mais importante, de uma mudança na visão das pessoas sobre que deve ser público e o que deve ser privado (BAUMAN, 2013, p. 20).

A vítima de fraude bancária na internet, além de não saber que é vigiada, muitas vezes é induzida a realizar ações de forma inconsciente e manipulada por fraudadores invisíveis. Neste sentido, o autor ressalta uma ideia atual sobre vigilância:

> Creio que o aspecto mais notável da edição contemporânea da vigilância é que ela conseguiu, de alguma maneira, forçar e persuadir opositores a trabalhar em uníssono e fazê-los funcionar de comum acordo, a serviço de uma mesma realidade. Por um lado, o velho estratagema pan-óptico ("Você nunca vai saber quando é observado em carne e osso, portanto, nunca imagine que não está sendo espionado") é implementado aos poucos, mas de modo consistente e aparentemente inevitável, em escala quase universal. Por outro, com o velho pesadelo pan-óptico ("Nunca estou sozinho") agora transformado na esperança de "Nunca mais vou ficar sozinho" (abandonado, ignorado e desprezado, banido e excluído), o medo da exposição foi abafado pela alegria de ser notado (BAUMAN, 2013, p. 21).

Por outro lado, no aparente anonimato, fraudadores obtém sucesso no cometimento de fraudes bancárias com informações pessoais das próprias vítimas, contudo, é sabido que o aparente anonimato do fraudador é passível de rastreamento.

Neste sentido Bauman, (2013, p. 20) cita o exemplo do fotógrafo Rich Lam, que documentou os distúrbios de rua em Vancouver e conseguiu em dois dias rastrear e identificar pessoas fotografadas sem intenção e assim ele finaliza:

> Tudo o que é privado agora é feito potencialmente em público – e está potencialmente disponível para consumo público; e continua sempre disponível, até o fim dos tempos, já que a internet "não pode ser forçada a esquecer" nada registrado em algum de seus inumeráveis servidores (BAUMAN, 2013, p. 20).

Operadores da Ciência Policial devem evoluir, aperfeiçoar e combinar competências digitais para atender aos rigores e dificuldades para se combater e enfrentar criminosos cibernéticos (BROWN, 2015).

Brown (2015) demonstra no Quadro 7 a seguir o conjunto de habilidades e competências no meio digital e tecnológico que investigadores policiais devem possuir para produzir inteligência capaz de enfrentar e encarar as dificuldades de investigar os crimes cibernéticos.

Quadro 7 - Conjunto de habilidades e competências no meio digital e tecnológico que investigadores policiais devem possuir para produzir inteligência capaz de enfrentar e encarar as dificuldades de investigar os crimes cibernéticos

Habilidade no meio digital	**Competência**
Pesquisa	Recuperação rápida de informações de domínio público e material de referência armazenados em rede corporativa. Capacidade para obter *insights* por triangulação informações dispersas de fontes que são inacessíveis através de motores de busca públicos.
Consciência	Vigilância em manter a consciência dos desenvolvimentos no campo da segurança da informação. Aplicado conhecimento das melhores práticas da indústria para a realização de investigações forenses digitais.
Continuidade Evidence	Estrita conformidade com os processos estabelecidos para demonstrar cadeia de custódia ao manusear informação armazenada eletronicamente.
Imagem forense	Conhecimento aplicado de técnicas de conservação de dados, que utilizam tanto métodos físicos e lógicos para garantir que fontes de informação estão devidamente estruturadas. Está relacionado a autenticidade do dado preservado.
Arquitetura de Networking	Compreensão prática do modelo OSI (Open System Interconnection) e da função de tecnologias de comunicação no armazenamento e transmissão de dados, tais como protocolos de rede, endereços de controle de acesso à mídia (MAC), firewalls, roteadores, servidores proxy, data centers, aplicativos, serviços em nuvem, aplicativos baseados em host, matriz redundante de discos independentes (RAID), clusters, servidores virtuais e modos de autenticação multifator.
Hardware	Conhecimento aplicado de componentes e periféricos conectados aos sistemas de informação, incluindo discos rígidos, drives de estado sólido (SSDs), memória de acesso aleatório (RAM), o insumo básico sistema de saída (BIOS), placas de interface de rede (NIC), chips, e armazenamento flash.
Sistemas de Arquivos	conhecimento aplicado de sistema de arquivos diversos atributos como FAT, FAT32, exFAT, NTFS, HFS +, XFS, ext2, ext3, ext4, e UFS.
Análise de dados estruturados	Recuperação e interpretação de informações formatadas universalmente, como entradas de campo fixas dentro de registros, bem como informações incorporadas associadas a sistemas operacionais, bancos de dados, planilhas, registros, histórico da Internet, logs de segurança e de sistema e arquivos criptografados sistemas.

Análise de dados não estruturados	Interpretação de valores associados a arquivos desanexados armazenados em vários sistemas de arquivos, como fotos digitais, imagens gráficas, vídeos, dados de streaming, páginas da Web, arquivos PDF, PowerPoint apresentações, dados de e-mail, entradas de blog, wikis e documentos de processamento de texto.
Análise de dados Semi-estruturados	Extração de etiquetas, metadados ou outros tipos de marcadores de identidade que subsistem em arquivos desanexados, incluindo informações indicativas de autoria, número de revisão, criador, remetente, destinatário, tempo e detalhes de data, coordenadas de GPS, palavras-chave e versão de firmware. Esta atividade também se estende à análise de dados relacionais em arquivos associados a arquivos desanexados, como XML e outras linguagens de marcação.
Engenharia reversa	Compreensão funcional dos mecanismos de desenvolvimento de software, administração remota e proliferação de malware.
Programação e Scripting	Conhecimento de codificação usando linguagens como C, C ++, C #, Perl, Delphi, Html, .NET, ASP, Python, Java, JavaScript, Ruby, Bash Scripting, VBScript, PowerShell, Unix / Linux, enscript.
Virtualização	Conhecimento aplicado da construção, configuração e implantação de máquinas virtuais.
Relatório técnico	Experiência na produção de relatórios altamente granulares detalhando o funcionamento interno de informações tecnologias de comunicação, integridade de arquivos, a autenticidade da informação e circulação de dados.

Fonte: Brown (2015).

Assim, fica claro que embora exista grande dificuldade em encontrar e rastrear aqueles que comentem fraude bancária, com as informações certas repassada pelas vítimas das fraudes, meios tecnológicos de processamentos das informações, o aparente anonimato dos fraudadores pode ser rastreado e ficam registrados na rede.

3.4.2 A Privacidade da Vítima de Fraude Bancária na Internet

Uma vez ocorrida a fraude bancária na internet sobre uma vítima, esta teve sua intimidade, sua privacidade e seu sigilo invadido sem o seu consentimento por terceiros.

Ocorre que uma vez confirmado essa prática como fraude bancária na internet por meio de contestação da própria vítima, esta terá que mais uma vez abrir mão de sua privacidade para o Estado poder investigar, rastrear e procurar identificar aqueles que cometeram a fraude.

O dicionário Aurélio define privacidade como a habilidade de uma pessoa em controlar a exposição e a disponibilidade de informações acerca de si. Relaciona-se com a capacidade de existir na sociedade de forma anônima.

Segundo Bauman (2013, p. 24) entende que o sigilo é a fronteira da privacidade, sendo o domínio e o território da pessoa, equiparando a um segredo, senão vejamos:

> Um segredo, tal como outras categorias de propriedades pessoais, é por definição a parte do conhecimento cujo compartilhamento com outros é recusada, proibida e/ou estritamente controlada. O sigilo traça e assinala, por assim dizer, a fronteira da privacidade; esta é o espaço daquilo que é do domínio da própria pessoa, o território de sua soberania total, no qual se tem o poder abrangente e indivisível de decidir "o que e quem eu sou", e do qual se pode lançar e relançar a campanha para ter e manter suas decisões reconhecidas e respeitadas. Mas, numa surpreendente guinada de 180 graus em relação aos hábitos de nossos ancestrais, perdemos a coragem, a energia e, acima de tudo, a disposição de persistir na defesa desses direitos, esses tijolos insubstituíveis da autonomia individual.

Embora considere-se que a privacidade e o sigilo dos dados pessoais da vítima de fraude bancária sejam propriedades pessoais de segredo da própria pessoa, uma vez existindo a fraude bancária, nos processos de contestação sobre fraude bancária, a vítima abre mão de privacidade daqueles dados pessoais seus fraudados, no intuito de rastrear e identificar os responsáveis pelo cometimento da fraude.

3.5 FRAUDE BANCÁRIA PELA INTERNET E O PAPEL DA VÍTIMA DE FRAUDE BANCÁRIA

Diante do desejo irresistível de ter uma existência "cibernética" como parte cotidiana do mundo moderno globalizado, com facilidades de acesso e liberdades discretas entre uma vasta comunidade global, a Internet também forneceu ao cibercriminoso a oportunidade e meios para cometer atos criminosos e comportamentos virtuais indesejáveis (HUNTON, 2011).

Neste sentido, dentre as constantes mudanças de condutas delituosas, os crimes cibernéticos, em especial, os crimes de fraudes bancárias sofreram grandes inovações tecnológicas, saindo da engenharia social física para a engenharia social tecnológica, sendo os usuários do sistema bancário seu principal ator facilitador da ação delituosa.

Segundo Brown (2015) cibercriminosos possuem, além de aptidões técnicas avançadas e recursos tecnológicos, habilidades em linguística e psicologia, que eles combinam para executar engenharia social sobre suas vítimas, manipular processos de tomada de decisão e distorcer percepções, dificultando, assim, a investigação criminal (BROWN, 2015).

O desenvolvimento de novas regras e condições de segurança aplicadas por instituições financeiras, mudanças na legislação ou o aprimoramento da capacidade

investigativa policial não têm acompanhado o volume devastador de fraudes bancárias com o advento da internet.

Na medida que a tecnologia continua a evoluir, criminosos exploram novas maneiras de cometer cibercrime, se agravando ainda mais quando os modelos tradicionais de investigação são frequentemente argumentados como ineficazes ou não acompanham o ritmo dos criminosos (HUNTON, 2011).

As forças de segurança pública devem estar sempre atentas à evolução e modificações das ações criminosas, acompanhando e se aperfeiçoando conforme evoluem e se dinamizam o modo de agir dos agentes com comportamentos inadequáveis à conduta social. Para Levy (2007), o oceano de informações em que estamos imersos nos projeta a evoluir não somente no desenvolvimento de atividades benéficas à sociedade, mas desenvolver também atividades não compatíveis com a conduta social ou criminosas (LEVY, 2007).

Deste modo, operadores da Ciência Policial possuem não só o desafio de enfrentar o modo de agir atual daqueles que praticam os crimes de fraudes bancárias, como também de evoluir conforme se inova o modo delituoso dos fraudadores. Para Brown (2015), o modelo de investigação tradicional precisa evoluir com respostas estratégicas e táticas diferenciadoras por parte daqueles que promovem a persecução penal desses criminosos (BROWN, 2015).

Sabe-se que o ideal seria prever e identificar com antecedência, evitando assim o prejuízo e desvio da conduta social delituosa, no entanto, a velocidade de inovações informacionais e tecnológicas absorvidas por grupos criminosos, fazem da prevenção apenas um paliativo na diminuição do volume de fraudes.

Neste aspecto, a vítima de fraude bancária sempre serviu como fonte de informação essencial, seja como fornecedora involuntária de informação para prática delituosa, seja de forma voluntária contribuindo com informações que identifiquem ou facilitem a persecução criminal. A vítima como detentora de informação deve externalizar e documentar de maneira física essa informação, transformando-a em conhecimento para a Ciência Policial.

A Ciência Policial por sua vez precisa fazer gestão do conhecimento gerado pelas informações comunicadas pela vítima de fraude bancária. Borko (1968) discorre em essência que a Ciência da Informação investiga as propriedades e o comportamento da informação, o uso e a transmissão da informação, e o processamento da informação, visando uma armazenagem e uma recuperação ideal.

Usuários do sistema bancário e potenciais vítimas de fraudes bancárias são constantemente alertados sobre medidas de prevenção, no entanto, tais medidas não acompanham os avanços tecnológicos e de engenharia social. Fraudes bancárias eletrônicas

ocorrem com o comprometimento de informações e senhas obtidas, seja de forma inconsciente pelo cliente do sistema bancário, seja por meio de software, ou por ambos em conjunto (VAN GOOL, 2011).

Para Alexandria (2009) “engenharia social ocorre quando alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter acesso não autorizado a computadores ou informações sigilosas”.

Do mesmo modo, Parodi (2005) define que a Engenharia Social consiste em um “conjunto de métodos e técnicas que têm como objetivo obter informações sigilosas e importantes através da exploração da confiança das pessoas, de técnicas investigativas, de técnicas psicológicas, de enganação, etc.”.

Neste contexto, a engenharia social para obter informações sobre a vítima ocorre de maneira tecnológica. A vítima muitas vezes repassa informações ao fraudador de forma inconsciente ou despercebida com o uso de tecnologias, muitas vezes a fraude ocorre com a combinação de dispositivos maliciosos (softwares) e com a ação direta ou indireta da vítima. Uma vez estes dispositivos instalados, podem permanecer por longo tempo nos equipamentos eletrônicos de seus usuários com intuito de roubar informações com características bancárias (VAN GOOL, 2011).

Para Damiano (2013), a engenharia social aplicada aos programas maliciosos visa buscar e explorar o psicológico das pessoas a fim de executar suas tarefas, deste modo, deve existir também controles sociais para se evitar o uso ou instalação indevida destes ardis maliciosos.

Van Gool (2011) classifica a ação da fraude sobre o Internet Banking sob os seguintes pontos de vista:

> **Fraudes através da combinação de hardware e software:** os ataques são realizados sem ação direta do usuário. Esta classificação não exclui ataques que foram possíveis pela ação humana indireta. Um dos exemplos das ações humanas que indiretamente causam fraudes eletrônicas é a instalação acidental e/ou por desconhecimento do usuário de softwares maliciosos que, uma vez acionados, executam o ataque.
> **Fraudes através da combinação de hardware, software e usuário:** estes são os métodos que fazem uso de hardware e software para executar seus ataques, mas também exigem ação direta do usuário. Um exemplo é o phishing, o qual o usuário é induzido a inserir manualmente as informações de sua conta em uma página falsa do banco (VAN GOOL, 2011, p. 1).

Nessa mesma perspectiva, Thornburgh (2004) afirma que com o uso da engenharia social, o fraudador convence a vítima que naquele momento o fraudador é a instituição que a vítima é cliente, a qual repassa voluntariamente informações vitais como senhas, credenciais, dados pessoais.

Como contraponto, a vítima de fraude bancária por meio da internet, pode contribuir de maneira relevante para o operador da Ciência Policial. As tecnologias mudam constantemente, as informações se abstraem se não houver mecanismos que a preservem. Deve existir uma profunda proximidade entre a vítima de fraude bancária e o operador da Ciência Policial para compartilhamento dos registros informacionais.

Neste liame, a comunicação humana entre a vítima da fraude bancária e o operador da Ciência Policial serve não só como meio de preservação do conhecimento, mas como forma de registrar informações importantes acerca do modo e uso de tecnologia aplicada pelo fraudador. Saracevic propõe um seguinte conceito sobre CI:

> A CIÊNCIA DA INFORMAÇÃO é um campo dedicado às questões científicas e à prática profissional voltadas para os problemas da efetiva comunicação do conhecimento e de seus registros entre os seres humanos, no contexto social, institucional ou individual do uso e das necessidades de informação. No tratamento destas questões são consideradas de grande interesse as vantagens das modernas tecnologias informacionais (SARACEVIC, 1996, p. 1).

Deste modo, entende-se como é importante a necessidade da vítima de fraude bancária, participar fornecendo informações essenciais sobre essas fraudes que lhe foram aplicadas, tais como: reportando as instituições financeiras e órgão de investigação, o tipo de fraude ocorrida, metodologia tecnológica que foi vítima, fornecimento de metadados e identificação das máquinas utilizadas na fraude.

Neste ponto, pode ser julgado o quanto é importante a informação que a vítima imediata de fraude bancária detém, no entanto, como materializar aquela informação de modo que contribua para investigação e auxilie a investigação policial? O conteúdo da mente da vítima imediata jamais será agregado como informação viável para investigação se não houver maneiras de externalizar o que a vítima sabe sobre a fraude sofrida.

Isso corrobora com o defendido por Robredo (2007) em sua obra de 2003. Nela ele tenta aprofundar as seguintes reflexões sobre o conceito de informação:

> A 'informação' pode ser: registrada, duplicada, transmitida, armazenada, organizada, processada, recuperada. Sim, mas somente quando extraída da mente e codificada pela linguagem natural (falada ou escrita), seguindo normas e padrões (gramática, sintaxe) próprios de cada língua, ou de outras linguagens criadas pelo homem (linguagens de programação, que também têm suas gramáticas e sintaxes). Há, de fato, um processo de transformação do conhecimento (dentro da mente) em 'informação' fora da mente. [...] Então, 'informação' seria o conhecimento 'externalizado', mediante algum tipo de codificação [...] (ROBREDO, 2007, p. 7-8).

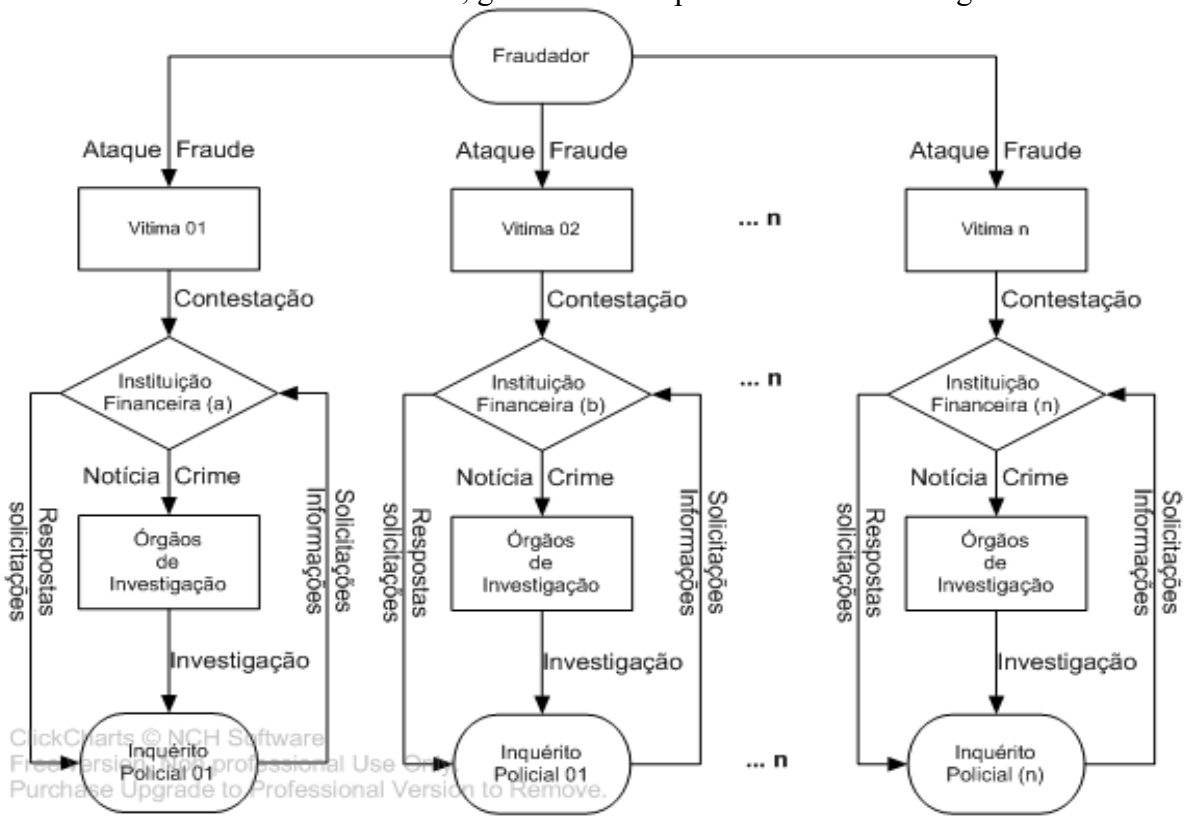
Robredo (2007) aponta ainda que a informação não é uma entidade física, não é um objeto tangível, visível, audível. O que se toca, se vê ou se ouve é o documento escrito, gravado, etc., contendo conhecimento registrado, em geral, mediante um código de representação.

A vítima de fraude bancária por meio da internet possui informação própria em sua mente humana que deve ser não só documentada, mas ser trabalhada de forma eficiente para que seja comunicada de forma rápida e segura, assim como diante dos avanços de tecnologias, devem existir meios tecnológicos capazes de centralizar e criar bases de dados inteligentes que contribuam com o papel investigativo da Ciência Policial.

Por outro lado, Buckland (1991), quando conceitua informação como coisa, define informação como algo tangível que possa ser expresso, descrito ou representado de alguma maneira física, capaz de informar algo por meio do processamento de sistemas de informação.

Com o advento da internet, o modelo investigativo tradicional se manteve por um bom tempo na razão de um procedimento policial (inquérito policial) para cada ataque/fraude ocorrida. Um mesmo fraudador poderia realizar inúmeras fraudes em diversos locais. O fluxo do processo de comunicação da fraude bancária representado na Figura 14, procura demonstrar como ocorria o processo investigativo tradicional sobre fraudes bancárias pela internet.

Figura 14 - Representação de fluxograma de diversos ataques/fraudes de um mesmo fraudador a várias vítimas, gerando vários procedimentos investigativos.



Fonte: Elaborado pelo autor (2019).

O modelo investigativo tradicional adotado pela PF, baseado na instauração de um inquérito policial para cada notícia crime enviada pela CEF de cliente vítima de fraude bancária eletrônica, mostrava-se totalmente improducente. Um mesmo grupo criminoso fraudava vítimas de diversos estados da federação e de diversas instituições financeiras. Diante disso, nasceu a necessidade de centralizar as informações de fraudes bancárias para se chegar aos grupos criminosos por meios da análise de vínculos coincidentes na investigação (SIQUEIRA 2014).

Baseado nessas dificuldades investigativas surgiu como modelo de centralização de informações sobre fraude bancária pela internet o “Projeto Tentáculos” da Polícia Federal.

Entretanto, embora imensuráveis os benefícios investigativos advindos da idealização do “Projeto Tentáculos”, o modelo foi idealizado e baseado no processo de centralização das informações repassadas pelas instituições financeiras, ocorrendo atrasos na comunicação dos processos de contestações, não se observando ainda a importância de participação da vítima nesse processo de centralização.

3.5.1 A Produção de Informação Estratégica

Na percepção de Capurro (2007) sobre informação, considera que a distinção mais importante é aquela entre informação como coisa (documento físico) e informação como signo (como algo subjetivo de depende de interpretação). O autor ressalta a facilidade de se contar um número de palavras em um documento físico ou descrevê-lo de outras formas, visto assim a importância da informação como um objeto ou uma coisa; argumenta ainda, por outro lado, ser muito mais difíceis questões de interpretações do significado do documento, ou como tentar descobrir para quem aquele documento tem relevância, ou ainda quais as perguntas que ele pode responder, quando a informação necessita ser interpretada.

De maneira mais estrita, Platt (1974) considera Informações como um termo específico e significativo, derivado da informação, informe, fato ou dado que foi selecionado, avaliado, interpretado e, finalmente, expresso de forma tal que evidencie sua importância para determinado problema de política nacional corrente.

Já inteligência estratégica é uma atividade especializada, permanentemente exercida, com o objetivo de produzir "informação acionável" – Inteligência – de interesse de determinada organização, além da salvaguarda dessa informação contra ações adversas de qualquer natureza (MARCIAL, 2005, p. 243).

O produto Inteligência é resultante de um processo metodológico próprio, que tem por finalidade prover um determinado usuário de um conhecimento diferenciado, auxiliando no processo decisório (FERNANDES, 2006).

Assim, "Informação" é a matéria-prima para a produção de "Inteligência". Relaciona-se com fatos presentes ou passados e deve expressar o estado de certeza. É utilizada em apoio ao processo de tomada de decisão, particularmente em decisões pontuais ou de nível tático-operacional (FERNANDES, 2006).

Inteligência busca o significado, o sentido do fato em que todo planejamento estratégico visa traçar circunstâncias futuras baseadas em conhecimento (PLATT, 1974).

Com base nesses conceitos de produção de informação estratégica com inteligência, a são apresentados os princípios propostos por Platt (1974), para produção sistemática de informação estratégica com inteligência, originalmente voltados ao contexto militar, descritos como "princípios da guerra", mas que, no entanto, segundo o próprio autor, as mesmas técnicas utilizadas no contexto militar para conquistas de territórios podem contribuir em diversos contextos de outras organizações para melhoria no ambiente competitivo:

I. **Finalidade** - O Princípio da Finalidade permeia cada aspecto de cada projeto de informações. A forma de atacar um projeto de informações sofre

influência do uso a fazer dele. Esse uso comanda o calendário, a extensão da cobertura, a linguagem e a forma do tratamento do assunto. A finalidade imediata de um documento é resolver o que comumente se chama "O Problema".

II. **Definições** - O princípio das definições claras é essencial na produção de informações. A experiência mostra a grande importância de tornar claro, pela definição ou de outra forma, a exata significação de cada palavra ou ideia. Concentram o esforço no que é realmente desejado, evitando mal-entendidos. Definições são particularmente necessárias em Informações Estratégicas.

III. **Explorações das Fontes** - O Princípio da Exploração das Fontes requer o perfeito acionamento de todas as fontes que possam jogar alguma luz sobre fatos e Informações. Quais são as possibilidade e limitações prováveis de cada fonte? Até que ponto confirma-se ou se contradizem? Quanto mais variadas as fontes, maior a possibilidade de efetivas verificações cruzadas. Fontes variadas ampliam as bases do documento, aprofundam a perspectiva e diminuem a possibilidade de erros sérios.

IV. **Significado** - O Princípio do Significado recomenda que se dê significação aos simples fatos. A busca da significação deve promover-se com vigor. Evidenciar sempre o significado dos fatos e das afirmações. Isso se faz, frequentemente, comparando-se o fato com um correspondente à mesma data no ano anterior, ou com fato similar em nosso próprio país. Apontar-lhe o significado aumenta muito a utilidade de um fato. Os fatos raramente falam por si mesmos.

V. **Causa e Efeito** - Este princípio leva o analista a procurar a relação de causa e efeito em qualquer problema de informações. Seguir o rastro da causa e efeito é um meio excelente para entender o funcionamento de qualquer situação, evitando mal-entendidos. Esse exame, muitas vezes, ajuda descobrir o fator-chave. Apontar as causas facilita, também, a utilização da Informação no nível da política.

VI. **Espírito do Povo** - Uma apreciação deve levar em conta a influência fundamental do espírito do povo. Este princípio recomenda que o espírito seja considerado aspecto de importância vital. O pano de fundo é a cultura do grupo, incluindo religião, folclore nacional e todas aquelas ideias que seus membros aprendem de criança. O princípio faz distinção entre um grupo vigoroso, agressivo, otimista, com espírito de progresso, de um lado, comparado com um grupo cansado, desiludido, pessimista, de outro.

VII. **Tendências** - O Princípio das Tendências baseia-se na mutação e nos padrões dos assuntos humanos. Este princípio requer uma estimativa da provável direção de mudança. As tendências estão intimamente ligadas à Previsão, parte importante da produção de informações. O estudo das Tendências busca penetrar o Nevoeiro do Futuro.

VIII. **Grau de Certeza** - O Princípio do Grau de Certeza considera a idoneidade das afirmações sobre um fato; a precisão dos dados quantitativos; e a probabilidade das estimativas e conclusões. Uma das responsabilidades essenciais do produtor de informações é determinar, através de um estudo crítico, o grau de confiança, precisão e probabilidade, conforme o caso, de cada elemento importante de seu documento, e fazer, então, com que fiquem claros para o leitor. Esse procedimento aumenta de muito a utilidade de qualquer Informação.

IX. **Conclusões** - As conclusões são essenciais para a completa utilidade de um grande número de informações. O Princípio das Conclusões é um corolário do Princípio da Finalidade. As conclusões exigem uma resposta à questão: E daí? Em muitos documentos somente as conclusões são lidas e relembradas. É necessário o maior cuidado para que as conclusões tragam os pontos principais clara e concisamente; mas não causem enganos devido à brevidade. As conclusões exigem o máximo de um oficial de informações (PLATT, 1974, p. 20).

Figura 15 - Representação dos noves princípios da produção de informação estratégica propostos por Platt (1974).

Fonte: Adaptado de Platt (1974).

Platt (1974) descreve ainda que a pesquisa para produção de informação estratégica parte da premissa que fatos isolados possuem pouca relevância, mas que na medida que se relacionam com outros fatos ou postos em destaquem, podem formar a base para produção de conhecimento.

Neste sentido, Platt (1974) elenca as principais fases para produção de informações estratégicas, no qual inova aos modelos científicos propostos de produção de informação, tecendo críticas acerca da importância de se realizar o levantamento geral e plano global do problema, assim como na extrema relevância das retroalimentação e feedbacks entre os percursos que a produção de informação estratégica percorre até sua apresentação.

O Quadro 8 a seguir apresenta as setes fases que Platt (1974) considera que melhor se adapta a pesquisa para produção de informações estratégica em qualquer nível organizacional:

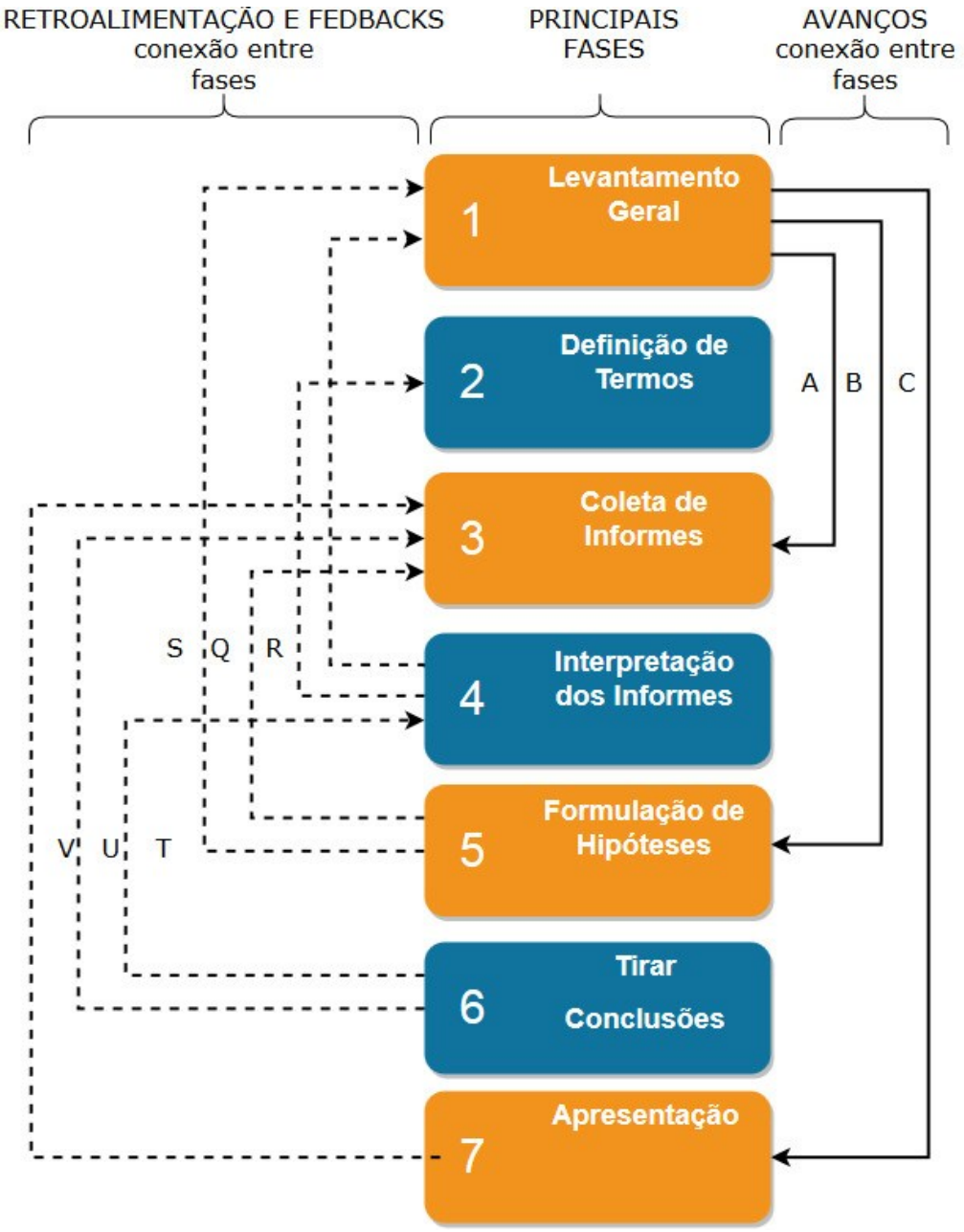
Quadro 8 - Descrição das setes fases para produção de informações estratégica proposta por PLATT (1974).

FASE	DESCRIÇÃO
1ª Fase Levantamento Geral	Plano geral para a condução do trabalho com indicação de prazo, pessoal a ser envolvido e principais fontes de informação disponíveis.
2ª Fase Definição de Termos	Definição do que se quer dizer claramente com cada termo e conceito para os analistas, revisores e clientes.
3ª Fase Coleta de Informes	Estabelecimento de um *modus operandi* ou fluxo de processo para a ação de coleta de dados disponíveis e não disponíveis.
4ª Fase Interpretação dos Informes	Avaliação, classificação, análise e interpretação de informes. A avaliação pode ser considerada parte da interpretação.
5ª Fase Formulação de Hipóteses	A partir da interpretação dos informes são formuladas as hipóteses que apoiam a compreensão do contexto e fornecem elementos para as conclusões.
6ª Fase Tirar Conclusões	Fase destinada a provar ou reprovar a hipótese de trabalho. Forma o chamado cerne do trabalho de produção de informações.
6ª Fase Apresentação	Na apresentação o redator deve ter ideias claras e expressá-las com clareza. O grau de certeza que merece cada afirmação importante deve ser indicado.

Fonte: Elaborado pelo autor (2020) adaptado de Platt (1974).

A Figura 16 representa de forma sintética a descrição das fases de pesquisa para produção de informação estratégica propostos por Platt (1974), apontando os relacionamentos de avanços, realimentações e feedbacks.

Figura 16 - Descrição das fases de pesquisa para produção de informação estratégica propostos por Platt (1974), apontando os relacionamentos de avanços, realimentações e feedbacks



Fonte: Elaborado pelo autor (2020) adaptado de Platt (1974).

Realizado este esboço de aplicação de métodos propostos por Platt (1974) para produção de informação estratégica com inteligência, na seção a seguir será descrito o atual modelo de produção de informações sobre fraudes bancárias eletrônicas no Âmbito da Polícia Federal.

3.5.2 O Modelo atual de Produção de Informação relacionada à Fraude Bancária Eletrônica na Polícia Federal

A partir da formalização da notícia crime, o operador da ciência policial, por meio da experiência investigativa, reúne outros elementos e evidências de prova para produzir informação capaz de subsidiar os procedimentos investigativos.

O conjunto de massa de dados e informes é transformado em informação conclusiva sobre determinado assunto na medida que agentes executam um plano de ação olhando aquela massa de dados e informes em toda sua amplitude, procurando rever se preciso for os limites expostos e os termos de referência (PLATT, 1974).

Diante dos avanços tecnológicos dos últimos anos, na medida em que as operações bancárias passaram do modelo tradicional, com uso de cartões bancários, para o meio tecnológico, por meio do *Internet Banking*, o volume de fraudes bancárias eletrônicas cresceram de forma avassaladora. Grupos criminosos se especializaram e migraram daquele modelo de fraude bancária tradicional para o uso do *Internet Banking.*

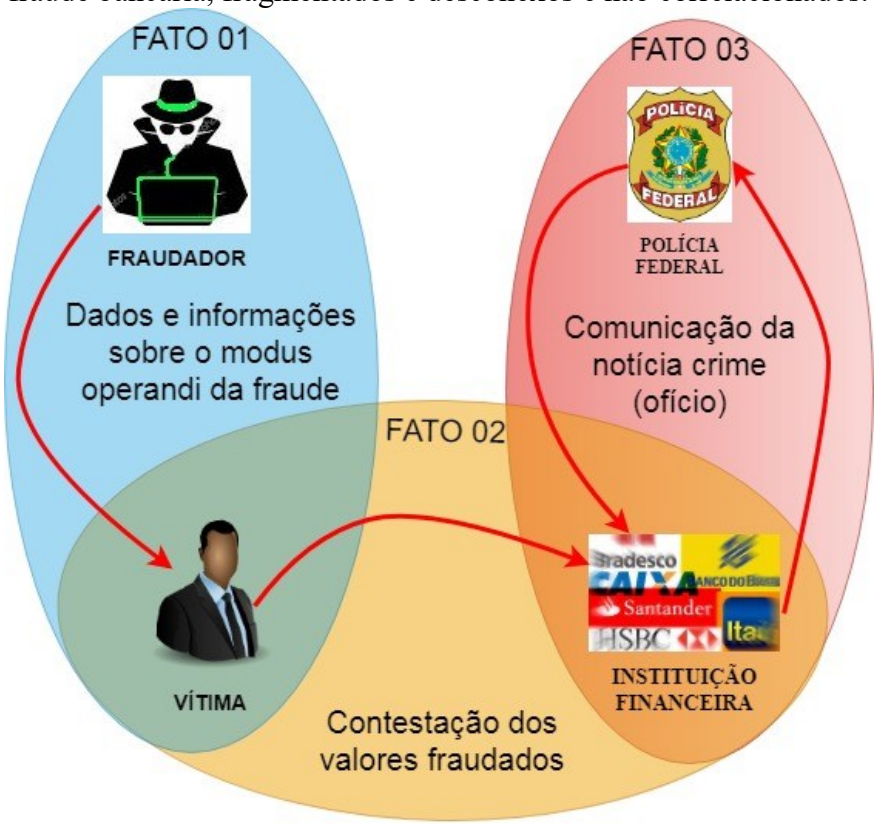
A produção inicial de informação sobre fraudes bancárias eletrônicas na PF basicamente decorre da comunicação da contestação de valores fraudados das contas de usuários do sistema bancário.

Originalmente, usuários do sistema bancário, quando vítima de fraude, se dirigiam a sua agência para fins de contestação das transações fraudulentas. A partir daí era aberto um processo de contestação para verificação da reclamação do cliente. O banco, por sua vez, comunicava por meio de ofício aquela notícia crime de fraude bancária a unidade da Polícia Federal mais próxima da agência da vítima fraudada. Com base nesta notícia crime, a Polícia Federal instaurava um Inquérito Policial (IPL) para cada conta vitimada (SIQUEIRA, 2014).

Siqueira (2014) ressalta ainda que fatos isolados relacionados ao mesmo fraudador não se comunicavam ou se inter-relacionavam. Toda a cadeia de produção de informação, desde a contestação, passando pela comunicação da notícia crime pela instituição financeira até a produção de informação pelos agentes de investigação se mantinha de forma isolada ou desconexa, ou seja, sem vínculos.

A Figura 17 representa os fatos geradores de informação, as etapas de coleta e difusão da informação sobre fraude bancária, fragmentados e desconexos e não correlacionados.

Figura 17 - Fatos geradores de informação, as etapas de coleta e difusão da informação sobre fraude bancária, fragmentados e desconexos e não correlacionados.



Fonte: Elaborado pelo autor (2019).

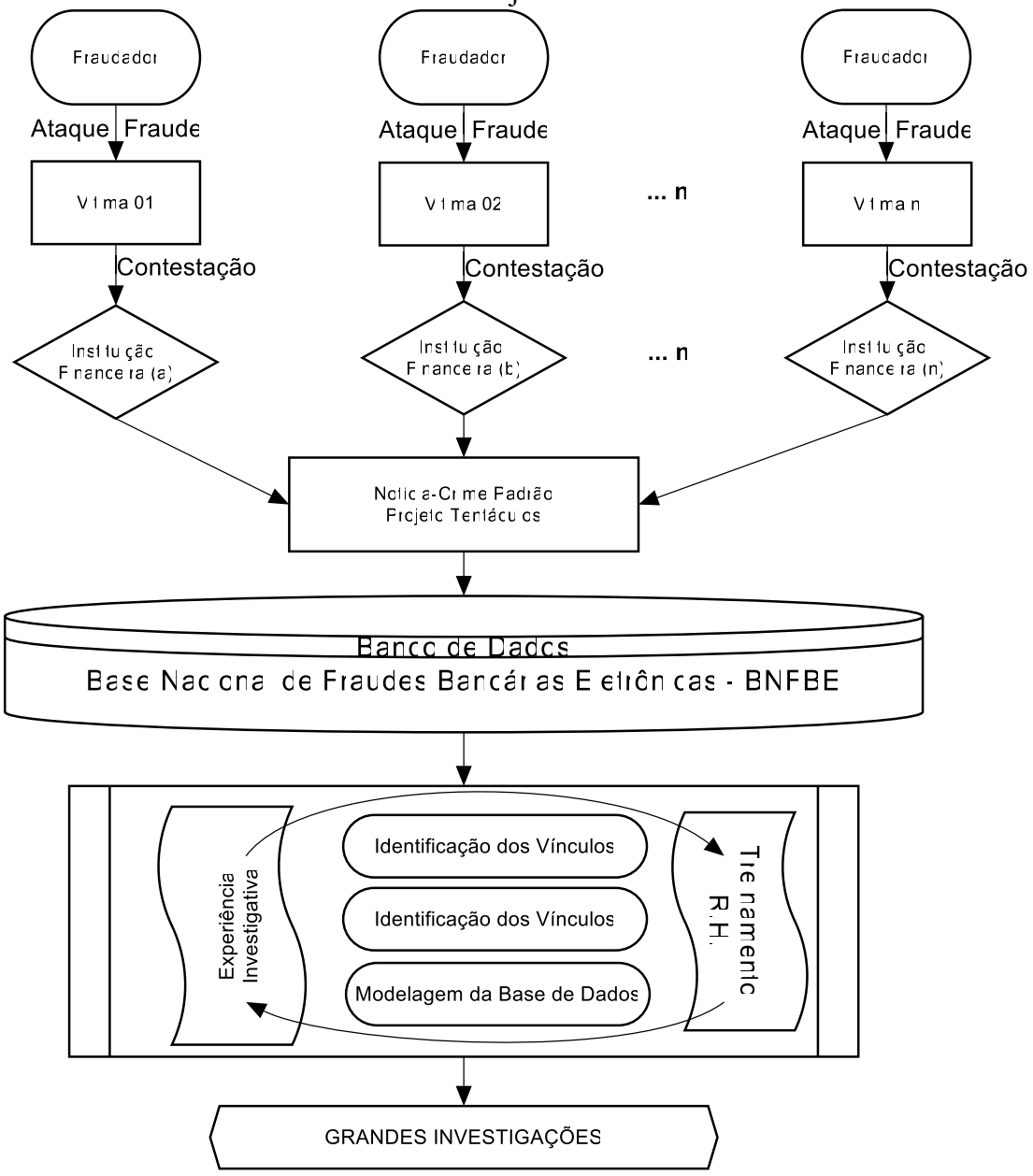
Conforme pode ser observado, o desenvolver da fraude bancária originalmente ocorria com o *modus operandi* do fraudador aplicado sobre a vítima (FATO 01) que muitas vezes a vítima sequer passava os dados e informações sobre a fraude bancária sofrida para a instituição financeira. Na medida em que a vítima de fraude bancária contestava os valores fraudados para a instituição financeira (FATO 02), esta não coletava qualquer dado ou informação sobre o tipo de fraude bancária sofrida pela vítima. Do mesmo modo, a comunicação de notícia crime pela instituição financeira para a Polícia Federal ocorria de maneira extremamente formal (por meio de ofícios), também sem qualquer dado ou informação sobre o tipo de fraude bancária (FATO 03). A Investigação ocorria de forma inócua e muitas vezes sem os resultados desejáveis.

A consideração de que um fato isolado significa muito pouco, a não ser relacionado com outros fatos, ou posto em destaque o seu significado, porém a grande dificuldade desse relacionamento de fatos, baseia-se pelo maior volume de trabalho e melhor compreensão pelo analista produtor de informação (PLATT, 1974).

O Projeto Tentáculos propiciou um modelo de centralização das informações no combate às fraudes bancárias eletrônicas. A Figura 18 demonstra o fluxo do processo de comunicação da fraude bancária, possibilitando uma melhor contextualização de como as

fraudes ocorrem, muito embora ainda não dispondo de um canal de comunicação direta da vítima da fraude bancária com a investigação, ou seja, fatos, dados e informações relacionados às informações sobre a fraude bancária ocorrida que somente a vítima da fraude detém, ainda não se relacionam com os fatos e produção de conhecimento realizados pelos agentes de investigação que realizam o combate à fraude bancária.

Figura 18 - Representação de fluxo da informação de fraude bancária eletrônica centralizada na BNFBE do Projeto Tentáculos.



Fonte: Elaborado pelo autor (2020) adaptado de Siqueira (2014).

Segundo Siqueira (2014), o modelo acima implementado com a idealização do Projeto Tentáculos possibilitou a padronização das notícias-crime sobre fraudes bancárias eletrônicas

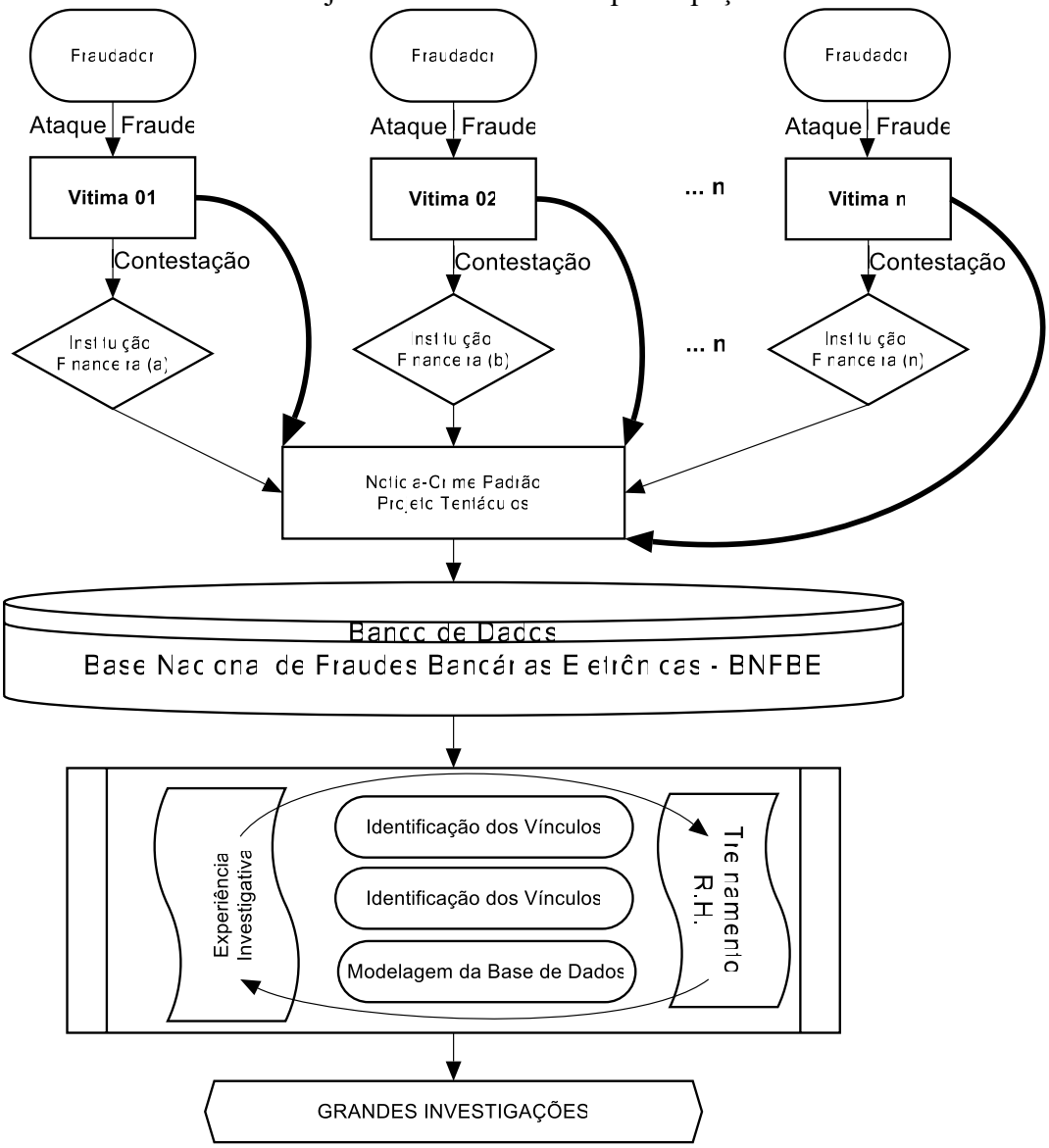
oriundas da CEF. A criação de um banco de dados único sobre fraudes eletrônicas padronizado, análise de vínculos baseados na experiência Investigativa, *modus operandi* da conduta criminosa, Identificação dos Atores, estabelecimento dos vínculos, modelagem da base de dados, treinamento dos recursos humanos e por fim, na seletividade investigativa indicando o melhor local para o início do procedimento investigatório (SIQUEIRA, 2014).

Por se tratar de um modelo em constante evolução, imperioso se faz, com base no conhecimento empírico adquirido por meio da experiência investigativa, uma reanálise e reavaliação constante para verificação da necessidade de mudanças (SIQUEIRA, 2014).

Neste sentimento de constante evolução, observa-se a importância da contribuição que a vítima da fraude bancária pode exercer fornecendo dados e informações úteis para o modelo atual existente. É preciso que os fatos relacionados às fraudes bancárias sejam levantados de forma ampla e geral. Deve existir um aproveitamento das informações que só a vítima da fraude bancária detém e que não são abarcadas pelos agentes de investigação.

Deste modo, acreditando na busca de melhorias contínuas, a Figura 19 destina a mostrar uma proposta de complementação ao modelo existente no Projeto Tentáculos em que diante dos avanços tecnológicos, possibilitassem a vítima da fraude bancária eletrônica interagir, complementando, realimentando, informando, ratificando e retificando os dados constantes na notícia crime de forma a enriquecer ainda o processo investigativo.

Figura 19 - Representação de fluxo da informação de fraude bancária eletrônica centralizada na BNFBE do Projeto Tentáculos com a participação da vítima.



Fonte: Adaptado de Siqueira (2014).

Uma vez existindo a fraude bancária, a informação encontra-se presente nas mais diversas formas. A informação sempre é documentada pela instituição financeira lesada na medida em que ocorre uma fraude bancária, no entanto, a informação que a vítima de fraude bancária tem em sua mente, se não documentada, não servirá como conhecimento humano útil para contribuir com o processo investigativo contra a fraude bancária.

Na seção a seguir, das análises de dados e resultados, será aplicada a metodologia Soft System Methodology (SSM) de Checkland (1985) para sistemografar o fluxo atual da informação sobre fraude bancária, colhemos as percepções dos entrevistados no grupo focal e ao final, a partir das recomendações dos entrevistados, propor o traçado de um paralelo entre as fases de produção de informação estratégica de Platt (1974) e uma proposta de um modelo

possível e viável de produção de informação estratégica para enfrentamento aos crimes de fraudes bancárias eletrônicas na Polícia Federal.

4 ANÁLISE DE DADOS E RESULTADOS

Os resultados a seguir apresentados decorrem da produção textual literária da pesquisa em si, dados coletados inerentes ao perfil dos entrevistados, como também em especial a colheita das percepções observadas nas entrevistas em grupo focal, suas avaliações sobre as dificuldades, soluções e recomendações de melhorias aos temas propostos.

Com a análise das discussões comentadas pelos participantes aos temas propostos, verificou-se a necessidade de criação de uma codificação de categorias. Para Barbour (2009) e Moraes (2003), organizar o conteúdo de transcrições e descrever a análise textual qualitativa a partir de categorias construídas ao longo da análise, pode consistir em uma lista de temas gerais apresentados em categoria e subcategorias, visando mostrar as relações retiradas dos textos e os códigos de categorias criados.

Para a análise da pesquisa, foram determinadas três categorias codificadas como base nas três últimas etapas de aplicação da SSM no processo de comunicação dos processos de contestação sobre fraude bancária, assim descritas como: dificuldades, soluções e recomendações, retiradas das discussões do grupo focal.

Diferentemente de outras técnicas, as discussões em grupo focal não decorrem apenas das transcrições literais do texto degravados entre os participantes, mas sim das observações relevantes de convergência e de não consenso. Para tanto, foi necessária a transcrição em forma de texto das interações registradas nas gravações áudio visual, representando literalmente o total de 11 folhas em transcrições, somadas a 04 folhas obtidas a partir dos apontamentos realizados pelo apoio técnico observador.

A partir das análises de todas transcrições e sua categorização foi possível obter resultados relacionados aos objetivos propostos na pesquisa mediante a transcrição dos instrumentos utilizados nos encontros de grupo focal conforme quadro abaixo:

Quadro 9 - Instrumentos de análise utilizados nas duas reuniões de Grupo Focal

Instrumento	Quantidade/Tempo	Transcrições
VÍDEO AUDIO	2h e 02 min – 1ª reunião 57 min – 2ª reunião	07 folhas 03 folhas
APOIO	1 apoio - 1ª reunião 1 apoio – 2ª reunião	02 folhas 02 folhas

Fonte: Elaborado pelo autor (2020).

Orlandi (2002 e 2004) afirma que diferente do esquema básico de construção da mensagem, tratado apenas como algo linear, sendo uma forma de transferência de informação; a análise do discurso busca os efeitos de sentido que se pode aprender mediante interpretação. A análise do discurso traz a ideia de sujeito, história e produção de sentidos.

Neste prisma vale ressaltar a grande contribuição realizada pelo apoio técnico observador que não apenas transcreveu as interações, mas apontou em sua visão os momentos de intervenção, as "reações" e "sentimentos" dos participantes durantes os discursos e debates realizados nas duas reuniões.

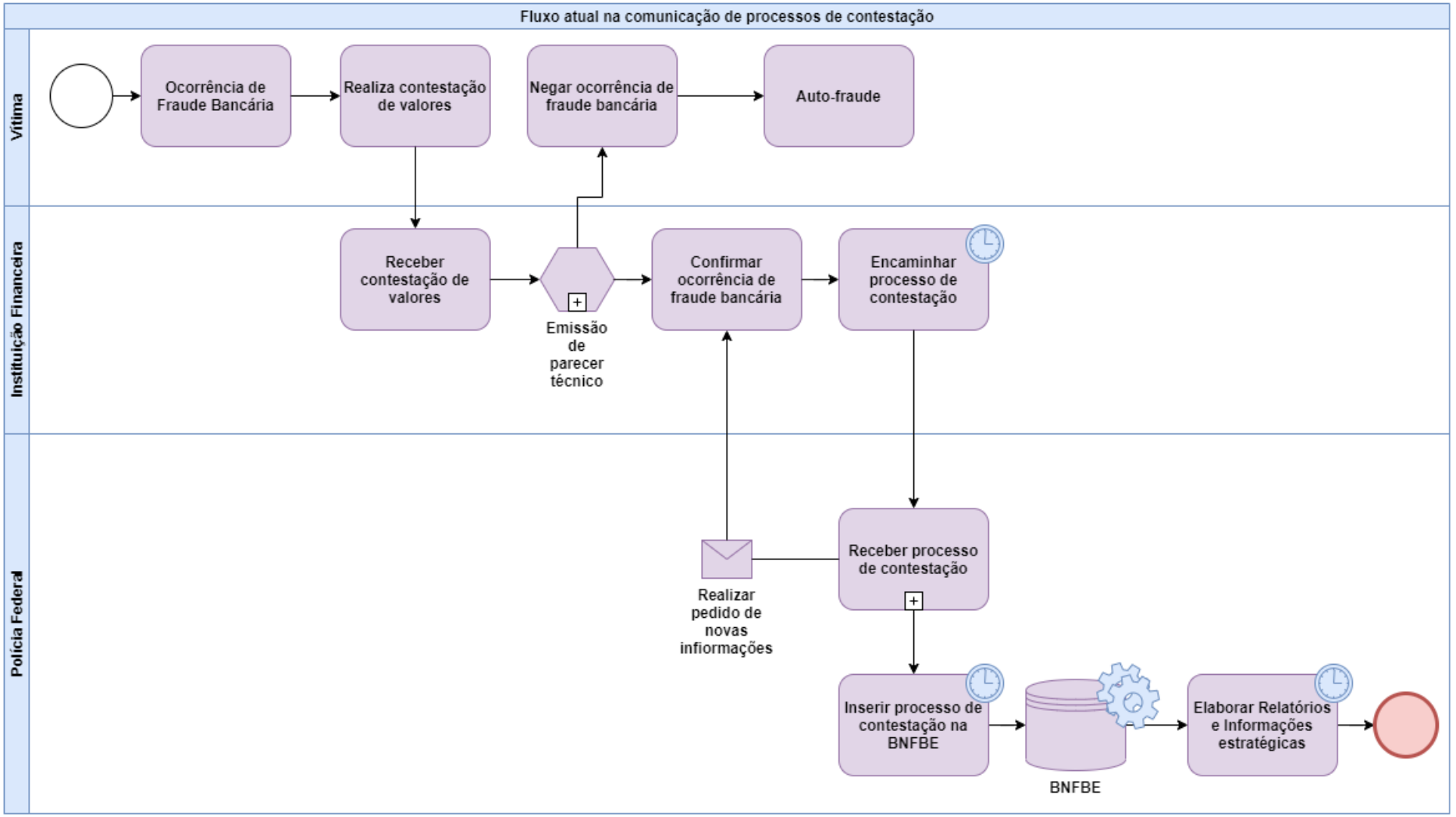
4.1 FLUXO DA INFORMAÇÃO ATUAL NA COMUNICAÇÃO DOS PROCESSOS DE CONTESTAÇÃO SOBRE FRAUDE BANCÁRIA

A definição, a representação gráfica da BNFBE e mapeamento do fluxo de informação na comunicação dos processos de contestação serviu para sistemografar o processo de alimentação da BNFBE, visto que tal mapeamento não existe atualmente na PF. Para demonstração do fluxo da informação atual na comunicação dos processos de contestação de fraude bancária, o presente estudo utilizou a ferramenta de desenho vetorial, ilustração e mapeamento por meio de fluxogramas, <https://app.diagrams.net/> (draw.io), que a partir de sua plataforma on line foram construídos esquemas e arquiteturas informacionais a serem apresentados na estrutura desta pesquisa.

Para criação do fluxo de informação atual de comunicação dos Processos de Contestação sobre Fraude Bancária foram utilizadas os normativos que traçam a metodologia para inclusão de notícias crimes para cadastramento dos dados dos processos de contestação na BNFBE. A Orientação n.º 002/2009 – CGPFAZ/DIREX traça o passo a passo do fluxo das informações sobre fraudes bancárias inseridas na BNFBE.

O mapeamento a seguir exposto na Figura 20 será apresentado aos Policiais Federais entrevistados no grupo focal como fluxo atual comunicação dos Processos de Contestação e servirá de parâmetro inicial para análise das percepções e discussões dos entrevistados.

Figura 20 - Representação gráfica do fluxo da informação atual na comunicação dos processos de contestação sobre fraude bancária eletrônica



Fonte: Elaborado pelo autor (2019).

Uma vez apresentado o fluxo da informação atual na comunicação dos processos de contestação de fraude bancária e colhido as opiniões e percepções dos Policiais Federais consultados envolvidos no grupo focal a partir da análise dos dados, buscou-se apresentar por meio da aplicação da Soft Systems Methodology (SSM) de Checkland (1985), o diagnóstico e proposta de representação gráfica que possa melhorar a gestão da informação dos dados inseridos na BNFBE.

4.2 DONOS DO PROBLEMA

Definida a formulação do problema de pesquisa em "**Como melhorar a Gestão das Informações sobre fraudes bancárias inseridas na BNFBE?**", indo além, reunindo pesquisas e opiniões dos atores envolvidos visando evitar a alimentação da BNFBE sem a qualidade desejada, verificando ainda a possibilidade e viabilidade de participação efetiva de vítima de fraude bancária nos processos sobre fraude bancárias eletrônicas. Optou-se pela aplicação da metodologia Soft System Methodology (SSM), para comparar o fluxo de informação atual com o modelo sugerido pelo autor da pesquisa. A aplicação da SSM visa identificar e detalhar outros elementos para se construir um modelo geral aplicável que possa servir de constructor de apoio decisional para se resolver o problema de maneira viável e possível.

Para isso, foi aplicada a metodologia SSM para representação gráfica da realidade do fluxo de informação dos processos de contestação de fraudes bancárias eletrônicas. A aplicação da SSM buscou representar de forma gráfica todos os atores envolvidos (donos do problema, clientes e população da amostra), suas fontes formais e informais de informação, o processamento de entrada e saída de informações na Base Nacional de Fraudes Bancárias Eletrônicas – BNFBE, comparando o modelo atual com um modelo conceitual como solução da situação problemática expressada e como pode ser proposto seu funcionamento.

Checkland (1985), propõe dentro da Teoria Geral dos Sistemas um melhor suporte para a expressão formal de cenários problemáticos, assim como da concepção mental das pessoas sobre o ambiente em que operam e em um paralelo da realidade prática. Deste modo, de maneira prática, os observadores devem-se abstrair dos arreios da experiência investigativa, ampliando horizontes de forma isenta, para se questionar uma maneira de padronizar uma boa prática de inserção das informações sobre as comunicações dos processos de contestação de fraudes bancária eletrônica. Demonstra assim, a gênese da exploração de uma situação que carece de gestão inovadora.

A tomada de decisão exige aplicação hábil de métodos e processos científicos e não científicos pelos quais os indivíduos interpretam dados ou informações para produzir resultados de inteligência perspicazes e recomendações viáveis (FLEISHER; BENSOUSSAN, 2007).

Dentro do campo da ciência da informação, a sistemografia serve como ferramenta útil para construir graficamente sistemas complexos para idealizar um modelo viável por meio de signos, propondo um sistema ágil, racional e flexível (BRESCIANI FILHO, 2001; LE MOIGNE, 1977; LE MOIGNE, 1990).

A sistemografia procura desenhar e compreender o comportamento de sistemas de informação complexos em relação às circunstâncias problemáticas de sua realidade, tendo como objetivo a tentativa de uma modelagem ideal (SCHODERBEK, 1990).

A SSM favorece o pensamento sistêmico e organiza um cenário para se discutir problemas e soluções como forma de beneficiar o entendimento acerca das fraquezas organizacionais, abstraindo-se de soluções tecnológicas ou modismo, como também exigindo a participação e o debate aberto de todos os atores envolvidos com o intuito de conhecer e entender a situação problemática (BELLINI; RECH; BORENSTEIN, 2004).

Para isso, a abordagem sistêmica utilizada neste projeto para representar os donos do problema decorre pela possibilidade de aplicação da metodologia Soft Systems Methodology (SSM), em situações tanto de maneira restrita, como ampla nos setores públicos e privados. Uma vez aplicada em um contexto decisional, permite a exploração de como as pessoas criam para si o significado de seu mundo, para poder agir intencionalmente de forma objetiva (CHECKLAND, 2000).

A aplicação da SSM é notável, tanto em termos do tamanho da organização envolvida, como também em termos de seu modo de utilização, a metodologia funciona de dentro para fora com seus participantes atuando na estruturação do sistema para solução do problema e não simplesmente a partir do exterior por alguém de fora da organização (MINGERS; ROSENHEAD, 2004).

Inicialmente proposta como metodologia aplicável no campo da engenharia de sistemas, aplicada de maneira rígida, logo se verificou que seria possível para resolver problemas sistêmicos que envolviam a complexidade dos assuntos humanos, focados em procurar resolver um problema por meio de um desenho sistêmico mais leve e maleável (CHECKLAND, 2000).

Neste sentido, Checkland (2000) propôs um desenho sistêmico em que suas fases ou estágios não possuíam uma sequência ou hierarquia, mas uma interação de ida e volta entre suas fases. Suas partes seriam separadas apenas por dimensões conceituais e reais, possuindo

assim apenas uma sequência não estanque baseada na análise dos seguintes elementos: definição raiz de sistemas relevantes, contextualização, comparação e definição de mudanças de implementação, projeto de mudança e implementação. Chckland (2000) denominou esses elementos ainda como setes estágios ou passos de um processo de aprendizagem circular.

Vianna e Ensslin (2008) consideram que resolver um problema inicialmente consiste no processamento de diversos tipos de dados com alguns sendo incorporados e outros sendo descartados ao logo do tempo, acarretando na mudança de concepção em circunstâncias originalmente propostas, alterando as fronteiras de interação entre objeto, sujeito e ambiente, gerando, assim, novos contextos viáveis e possíveis.

A incapacidade de sistemas de engenharia em lidar com todas as complexidades de problemas de gestão fez surgir a necessidade de se construir um sistema de atividade humana com aprendizagem cíclica para solução de situações problemas (CHECKLAND, 1985).

A partir dos conceitos já definidos nesta pesquisa sobre sistemografia, Iarozinski Neto e Leite (2010) apresentam como proposta as seguintes etapas:

1) identificar o fenômeno;

2) desenvolver o modelo geral;

3) observar a realidade;

4) desenvolver modelos da realidade;

5) Agir sobre a realidade.

Na representação da Figura 12, Checkland (1985) apresenta a metodologia Soft System Methodology (SSM) consistindo basicamente em sete estágios para aplicação:

1) explorar uma situação problemática não estruturada;

2) expressar a situação problemática;

3) construir definições sucintas de sistemas relevantes;

4) elaborar modelos conceituais desses sistemas;

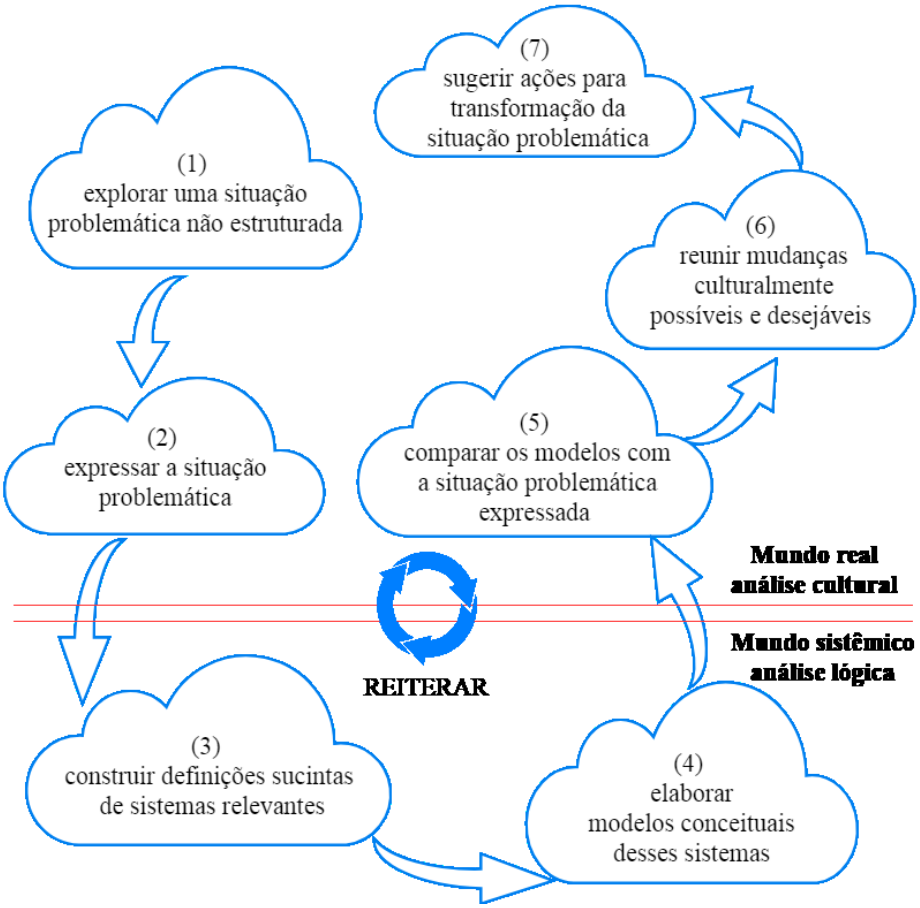
5) comparar os modelos com a situação problemática expressada;

6) reunir mudanças culturalmente possíveis e desejáveis;

7) sugerir ações para transformação da situação problemática.

A partir das etapas proposta por Neto e Leite (2010) e dos sete estágios para aplicação da metodologia Soft System Methodology (SSM), apresenta-se uma representação sistemográfica geral da etapa 1 (identificar o fenômeno) idealizada por Neto e Leite (2010), bem como representação gráfica geral dos sete estágios de Checkland (1985) para visualização e contextualização dos donos do problema de pesquisa, vítimas e beneficiários do sistema, dos atores envolvidos, transformações do processo, visão do mundo.

Figura 21 - Estágios da Soft Systems Methodology



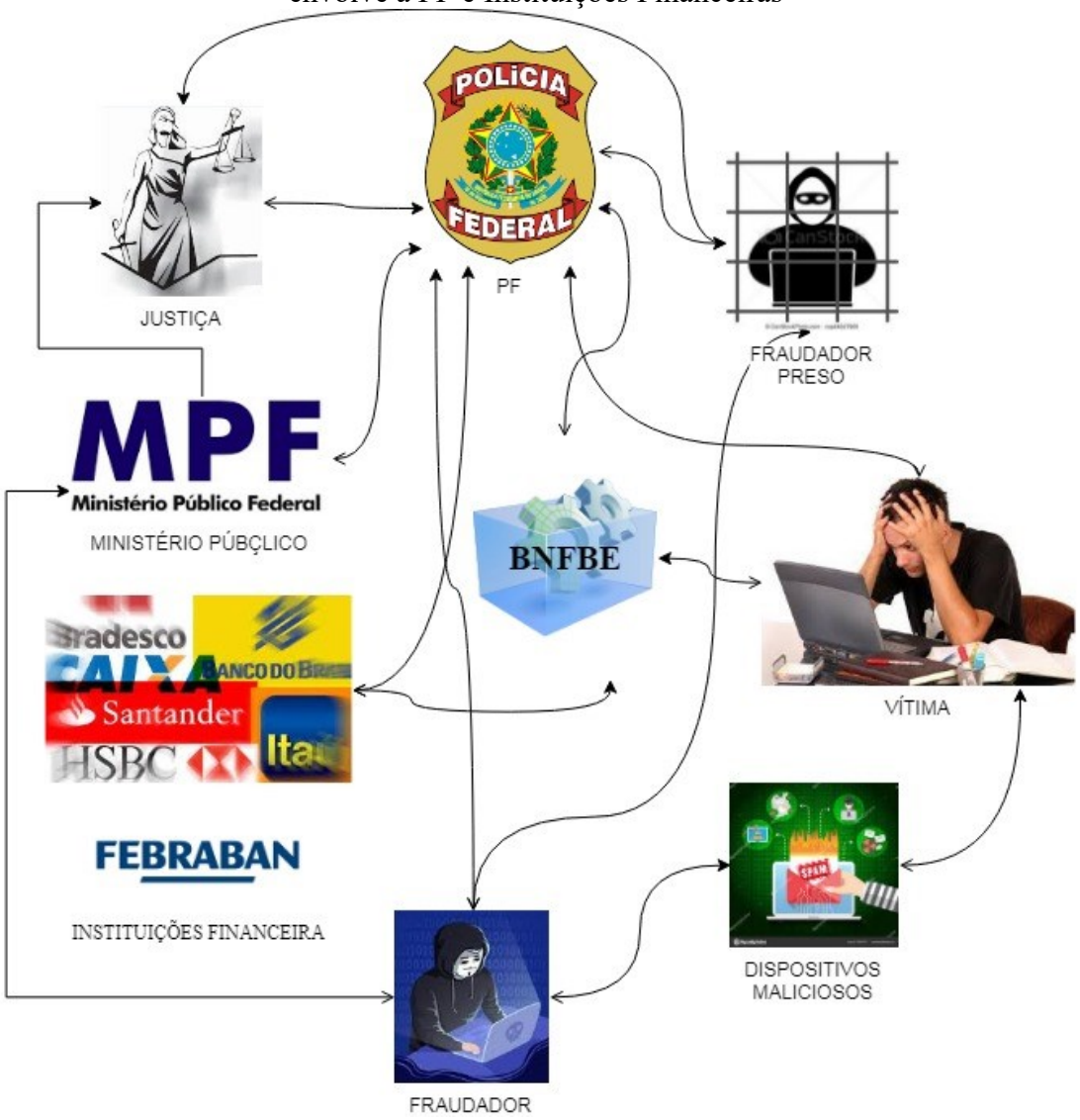
Fonte: Checkland (1985).

Desta forma, para aplicação prática da metodologia Soft System Methodology (SSM), visando expressar a realidade percebida e responder a pergunta de "**Como melhorar a Gestão das Informações sobre fraudes bancárias inseridas na BNFBE?",** optou-se a seguir a descrição detalhada do estudo de caso acerca do desenho sistêmico sobre a comunicação dos processos de contestação de fraudes bancária eletrônica.

Os estágios 1 e 2 de aplicação da SSM proposta por Checkland (1985) consiste em realizar um mapeamento da situação problemática com uso de gráficos elaborados de maneira neutra e ampla, representados por meio de figuras ricas, conforme Figura 20. Checkland (1985) enfatiza, ainda, que a construção de figuras ricas tem como função expressar por meio representações gráficas livres que origine um sistema relevante que se espera que aconteça para de fato expressar a situação problemática.

A Figura 22 consiste na representação gráfica por meio da figura rica proposta por Checkland (1985), do mapeamento livre e amplo do processo de contestação de fraude bancária eletrônica que envolve a PF e Instituições Financeiras.

Figura 22 - Representação gráfica por meio da figura rica proposta por Checkland (1985), do mapeamento livre e amplo do processo de contestação de fraude bancária eletrônica que envolve a PF e Instituições Financeiras



Fonte: Elaborado pelo autor (2020) adaptado de Checkland (1985).

Da figura rica representada na Figura 22, destaca-se o contexto da necessidade de padronização na comunicação dos processos de contestações de fraude bancárias e sobre o funcionamento dos fluxos de informações sobre fraudes bancárias entre a PF e as instituições financeiras. Vislumbrou-se ir além e verificar sobre a viabilidade e possibilidade de participação efetiva da vítima de fraude bancária na alimentação direta à BNFBE com vista a propiciar maior eficiência acerca da fraude bancária sofrida, o que não ocorre atualmente.

Expressada a situação problemática de maneira ampla acerca do processo de contestação de fraude bancária eletrônica, aplicou-se o **estágio 3 da SSM de Checkland (1985)**, com a proposta de construção de perguntas e definições possíveis de sistemas relevantes, chegando a propor e estruturar os seguintes questionamentos: **I.** O primeiro

questionamento relevante visava questionar a frequência e intensidade de problemas de qualidade da informação repassados por todas instituições financeiras na comunicação dos processos de contestação de fraude bancária eletrônica; **II.** O segundo como proposta futura se considerado relevante pela amostra entrevistada seria a viabilidade de inserção e efetiva participação da vítima de fraude bancária na comunicação de forma padronizada de todas comunicações de processos de contestação sobre fraude bancária.

Ressalta-se que Checkland (1985) enfatiza que o sistema relevante proposto deve possuir definição detalhada. Os problemas verificados na qualidade e padronização das informações fornecidas pelas instituições financeiras devem constar no detalhamento do sistema relevante de base para solução aceitável e viável da situação problemática e deve conter os seguintes elementos essenciais:

Clientes (C): Os observadores Polícia Federal, MPF (que vão se beneficiar inicialmente na solução do problema, com a maior efetividade nas investigações e persecução penal). A JUSTIÇA FEDERAL em decorrência dos melhores resultados da experiência investigativa e maior conjunto de provas para decidir as ações penais originadas a partir de notícias crimes oriundas dos processos de contestações bancárias de fraudes eletrônicas, agindo assim como beneficiários do sistema;

Atores (A): Instituições Financeiras vinculadas à FEBRABAN (2019) (vítimas mediatas) e os usuários dos serviços bancários eletrônicos (vítimas imediatas), ambos agindo como protagonistas das atividades de fornecer dados e informações sobre fraudes bancárias;

Transformação (T): Padronização, completude de informações e rapidez na comunicação dos processos de contestação de fraudes bancárias eletrônicas;

Visão de mundo (V): melhoria da qualidade e completude das informações na comunicação dos processos de contestação de fraudes bancárias eletrônicas, visando possibilitar maior agilidade na identificação de grupos criminosos que comentem fraudes bancárias eletrônicas.

Proprietários (P): MPF e PF com poderes para avaliar continuamente, modificar conforme evoluem o *modus operandi* de grupos criminosos que comentem fraudes bancárias eletrônicas, ou até mesmo parar o sistema se não obtiver os resultados esperados para efetiva persecução penal. Possuem ainda o poder de criar grupos de trabalhos para avaliar e decidir sobre as diretrizes a serem tomadas para melhorar os métodos investigativos de combates as fraudes bancárias eletrônicas;

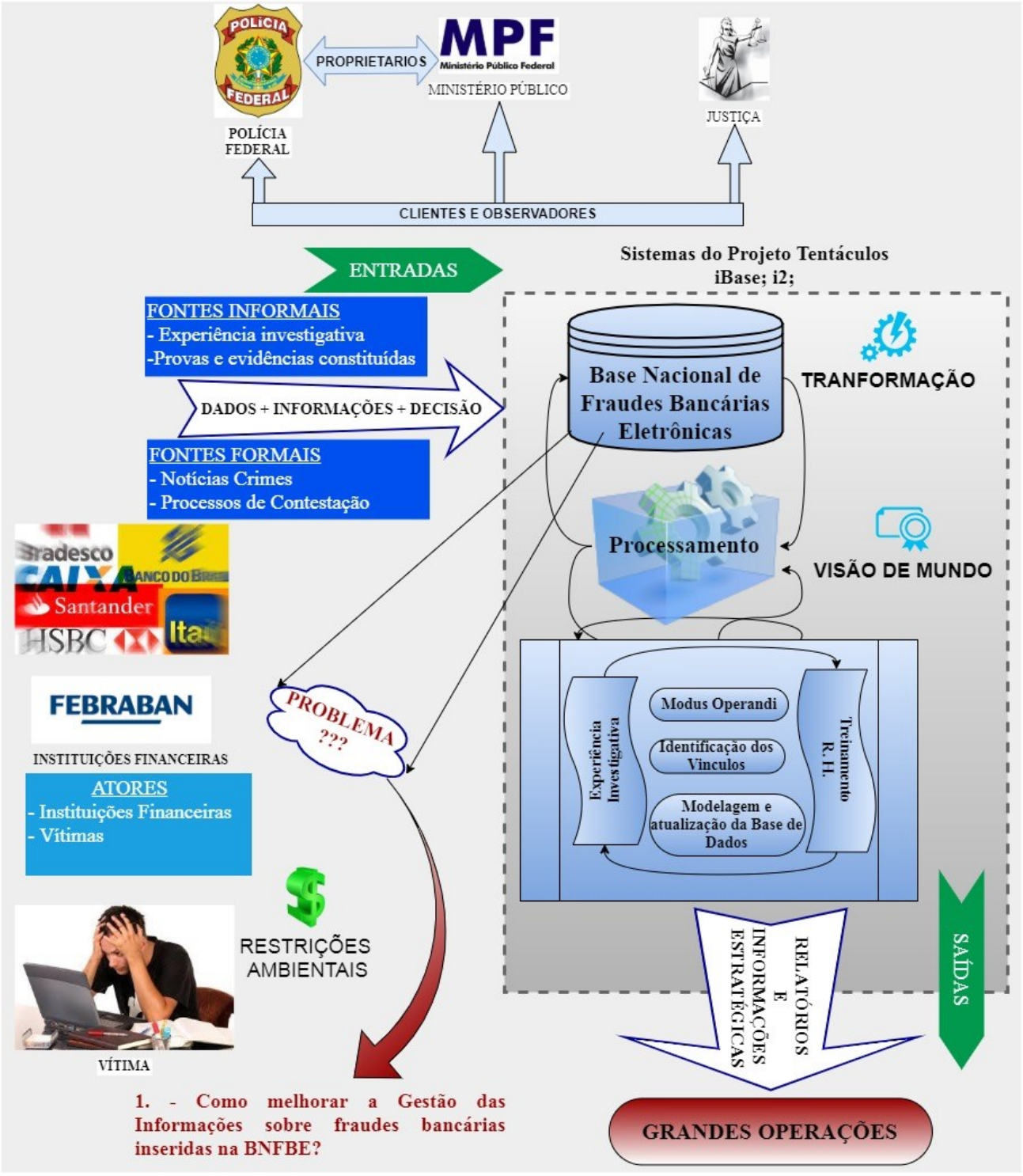
Restrições Ambientais (A): Interesse da vítima de fraude bancária em comunicar a fraude bancária;

A definição sucinta, depois de representado o sistema relevante, consiste ainda na descrição de um conjunto de atividades humanas significativas, concebidas como um processo de transformação, no entanto, ressalta-se a cautela na formulação de um modelo conceitual, o qual não se deve levar em conta a concepção do sistema conceitual como uma descrição dos sistemas de atividades da realidade presente no mundo real, pois isso foge a proposta de se fazer uma profunda reflexão da situação problemática (CHECKLAND, 1981).

Neste sentido, na aplicação do **estágio 4 da SSM de Checkland (1981)**, procura-se propor um sistema conceitual que deve contemplar e estar de acordo com as definições sucintas do sistema relevante. Na aplicação prática, propõe-se identificar a frequência e intensidade de problemas de qualidade da informação repassadas por todas instituições financeiras na comunicação dos processos de contestação de fraude bancária eletrônica.

O Projeto Tentáculos propiciou um modelo de centralização das informações no combate às fraudes bancárias eletrônicas. A Figura 23, procura-se demonstrar a modelagem preliminar do modelo conceitual relevante com o fluxo do processo de comunicação da fraude bancária, possibilitando uma melhor contextualização como ocorre a comunicação e o processamento das informações sobre fraudes bancárias eletrônicas, muito embora ainda não dispondo de um canal de comunicação direta da vítima da fraude bancária com a investigação atualmente, sendo apenas uma proposta conceitual a ser comparada com a realidade.

Figura 23 - Representação gráfica do modelo conceitual expressando a situação problemática do processo de contestação de fraudes bancárias eletrônicas.



Fonte: Elaborado pelo autor (2020) adaptado de Siqueira (2014).

O estágio 5 de Checkland (1981) é denominado como "comparação do modelo conceitual com a realidade", em decorrência de que partes da situação problemática analisada no estágio 2 são examinadas ao longo dos modelos conceituais.

Deste modo, de maneira prática, uma vez representado o modelo conceitual, consistindo em buscar identificar os problemas de qualidade das informações dos processos de contestação de fraude bancária eletrônica, deve-se comparar esse constructo com o modelo real anterior, discutindo, apontando **soluções** e verificando melhorias.

Checkland (1981) enfatiza ainda que a proposta do estágio 5 de comparação tem o intuito de gerar o debate sobre as mudanças possíveis e desejáveis que podem ser levadas além de situação problemática detectada, ou seja, trabalhos futuros.

Assim, finaliza-se os dois últimos **estágios 6 e 7 proposto por Checkland (1981),** consistindo na elaboração de **recomendações** de mudança, enfatizando que a principal característica da Metodologia SSM é a aprendizagem, ou seja, não bastando apenas desenhar um modelo ideal, mas fazer uma reflexão sobre a realidade, sobre uma situação problemática, buscando alternativas para a resolução destas, de forma cíclica e reiterada (CHECKLAND, 1981).

Por fim, de forma prática, uma vez identificada a frequência e intensidade de problemas de qualidade das informações inseridas na BNFBE, será discutido e apontado melhorias/recomendações a partir das percepções dos entrevistados, idealizando alternativas, assim como outras inovações. Neste sentido, avalia-se continuamente e reúne propostas de estudos futuros para se verificar a viabilidade da participação efetiva de vítima de fraude bancária nos processos de comunicação de fraudes bancárias pela internet.

De forma sintetizada, a visualização sistemográfica da Figura 24 consiste na representação gráfica dos sete estágios da metodologia SSM para representar de forma prática os elementos gerais do contexto que envolve a comunicação dos processos de contestação de fraude bancárias eletrônicas entre as instituições financeiras e a Polícia Federal.

Figura 24 - Representação gráfica dos sete estágios da metodologia SSM para representar de forma prática os elementos gerais do contexto que envolve a comunicação dos processos de contestação de fraude bancárias eletrônicas entre as instituições financeiras e PF

Fonte: Elaborado pelo autor (2020) adaptado de Checkland (1985).

4.3 ANÁLISE DOS DADOS E A SSM NA ALIMENTAÇÃO DA BNFBE

A análise dos dados se baseou consoante a técnica de análise por método sistemático proposta por Oliveira et al (2007) visando assegurar que as informações coletadas nas entrevistas de grupo focal sejam confiáveis e verdadeiras (OLIVEIR; LEITE FILHO; RODRIGUES, 2007).

Coletar as opiniões desses policiais visa medir a percepção do fluxo de informação na comunicação dos processos de contestação sobre fraude bancária e suas opiniões quanto a qualidade da informação repassada pelas instituições financeiras.

Como ideias centrais do roteiro de entrevista foram tratadas o fluxo da informação dos processos de contestação com base no modelo representado pelo autor e as percepções dos entrevistados, observando as seguintes características:

a) Tempo médio na comunicação dos processos de contestação;
b) Completude dos dados informados essenciais para alimentação da BNFBE ou de dados ainda não suportados para inserção na BNFBE;
c) Necessidade, capacidade e efetividade nos pedidos de informações complementares;
d) Melhorias e inovações sugeridas na visão dos entrevistados, em espacial sobre a viabilidade de participação da vítima de fraude bancária na inserção de informações.

Considerando o princípio da oportunidade para eficácia investigativa contra grupos criminosos em atuação o tempo médio razoável para se alimentar a BNFBE se considera 01 (um) mês desde o processo de comunicação da contestação de valores fraudados pelo cliente vítima, análise da contestação pela instituição financeira, processo de comunicação da contestação pela instituição financeira à PF e a consequente inserção na BNFBE.

Ocorre que nem sempre esse tempo médio razoável ocorre, seja em razão de atrasos na comunicação das contestações pelas instituições financeiras, seja pelo atraso na alimentação da BNFBE devido à falta de capital humano para análise, adequação e inserção dos dados ou pela incompletude de informações.

Quanto a completude de dados muitas vezes as instituições financeiras encaminham os dados referentes aos processos de contestações incompletos ou inseridos incorretamente, dentre os mais comuns, data e hora exata da fraude, dados de identificação da conta do cliente fraudado, dados de identificação dos valores fraudados, tais como contas beneficiárias e tipos de transações realizadas.

A metodologia de discussão nas entrevistas terá o intuito de apontar melhorias quantos aos dados atualmente inseridos na base, bem como melhorias em relação aos dados

considerados importantes para investigação que atualmente não são inseridos, em especial aqueles que a vítima de fraude bancária detém e não é alimentada na BNFBE, tais como método da fraude aplicada, números telefônicos de envio das mensagens de SMS com os endereços das páginas bancárias falsas e a identificação do identificador de usuário do dispositivo de acesso a da vítima em casos de fraudes realizadas via *mobile bank*.

O relatório final com a coleta das opiniões dos Policiais federais que atuam diretamente na BNFBE visa medir a percepção sobre os dados inseridos na BNFBE. Com base na aplicação da metodologia Soft System Methodology (SSM), visando expressar a realidade percebida e responder a pergunta de "**Como melhorar a Gestão das Informações sobre fraudes bancárias inseridas na BNFBE?",** após a compilação dos dados obtidos com o grupo focal, será apresentado a representação gráfica geral de um sistema ideal, bem como a comparação atual da inserção de dados na BNFBE com uma proposta futura de produção de relatórios de inteligência e informações estratégicas sobre Fraude Bancária Eletrônica na Polícia Federal.

4.4 PERFIL DOS ENTREVISTADOS

Considerando a delimitação do universo de participantes, a seguir são apresentados os dados colhidos inerentes ao perfil dos 10 Policiais Federais convidados a participar das entrevistas em grupo focal, muito embora como já relatado anteriormente os PARTICIPANTES 03 e 09 por motivos já apontados não puderam efetivamente participar das discussões.

Para Almeida (2005), encontro em Grupo Focal consiste na reunião de um pequeno grupo de pessoas que compartilhem conhecimentos, vivências, experiências, rotinas semelhantes de trabalho ou características. Os Policiais Federais que participaram das entrevistas foram identificados com etiquetas com os nomes PARTICIPANTE 1, 2 e assim por diante, escolhidos e determinados mediante sorteio de forma a ordenar a participação e preservar suas identidades.

Como critério de inclusão foram convidados a participar Policiais Federais lotados ou que já foram lotados no GRCC-CE e possuem conhecimentos em fraude bancária eletrônica, em especial aqueles que de alguma forma trabalharam na Operação Valentina. Tal critério de inclusão serviu para selecionar Policiais Federais que perceberam problemas na gestão das informações que deveriam ser inseridas da BNFBE e que não se encontravam naquela base durante a investigação que desencadeou a referida operação, conforme modelo de ficha de qualificação do perfil dos entrevistados constante no APENDICE II.

Quadro 10 - Caracterização do perfil dos participantes do estudo em relação aos conhecimentos sobre fraude bancária eletrônica na PF

Codificação	Tempo de PF	Tempo de GRCC	Quantidade de operações sobre fraude bancária	Trabalhou na Operação Valentina
PARTICIPANTE 01	16 anos	6 anos	5 Operações	Sim
PARTICIPANTE 02	16 anos	3 anos	2 Operações	Sim
PARTICIPANTE 03	21 anos	2 anos	2 Operações	Sim
PARTICIPANTE 04	21 anos	10 anos	8 Operações	Sim
PARTICIPANTE 05	16 anos	11 anos	8 Operações	Sim
PARTICIPANTE 06	15 anos	2 anos	3 Operações	Sim
PARTICIPANTE 07	16 anos	2 anos	2 Operações	Sim
PARTICIPANTE 08	15 anos	10 anos	8 Operações	Sim
PARTICIPANTE 09	16 anos	1 ano	1 Operação	Sim
PARTICIPANTE 10	21 anos	2 anos	2 Operação	Sim

Fonte: Elaborado pelo autor (2020).

4.5 APLICAÇÃO DAS SETE ETAPAS DA METODOLOGIA *SOFT SYSTEM METHODOLOGY* (SSM) NO PROCESSO DE COMUNICAÇÃO DOS PROCESSO DE CONTESTAÇÃO SOBRE FRAUDE BANCÁRIA

Tendo por base a Figura 18 da subseção 4.1, nela foi correlacionada a produção da presente pesquisa com as sete etapas da SSM podendo ser melhor sintetizado conforme Quadro 11 a seguir:

Quadro 11 - Caracterização da aplicação das setes etapas da metodologia SSM e sua representação no estudo.

Estágio da SSM	Aplicação no Processo de Comunicação de Fraudes Bancárias Eletrônicas na PF
1. Explorar uma situação problemática existente	Foi realizado o detalhamento da situação problemática na subseção 1.1 com a demonstração dos Pontos de Referências – *Landmark* sugeridos por Landry (1995) no intuito de conhecer e entender o problema de pesquisa. Realizado ainda a representação gráfica da situação problemática no processo de comunicação de Fraudes

	Bancárias Eletrônicas na PF representados nas Figuras 19, 20 e 21 da subseção 4.2 observando problemas na qualidade da gestão das informações sobre fraude bancária eletrônica.
2. Expressar a situação problemática	Além da Representação gráfica expressa na Figura 21 da subseção 4.2, foi expressa a formulação do problema, que vem a ser a razão da própria pesquisa e para a qual se busca resposta, nesse sentido pergunta-se: **Como melhorar a Gestão das Informações sobre fraudes bancárias inseridas na BNFBE?**
3. Construir definições sucintas de sistemas relevantes	Além de apresentados os questionamentos para construção das definições sucintas de sistemas relevantes, nas páginas 85 e 86 mostraram-se os elementos essenciais para definição do sistema relevante viável e aceitável para solução da situação problemática.
4. Elaborar modelos conceituais de sistemas relevantes	Uma vez apresentado a Figura 18 da subseção 4.1 com o Fluxo da Informação atual na comunicação dos Processos de Contestação sobre Fraude Bancária, juntamente com os resultados sugeridos de ajuste no fluxo inicialmente apresentado, foram elencadas propostas de melhorias no fluxo de informação, visando criar um novo modelo de sistema relevante que resultaram em parte nas sugestões do autor, bem como novas recomendações de inserção de informações e alteração do fluxo inicialmente representado.
5. Compara os modelos com a situação problemática	A partir da avaliação das percepções dos entrevistados no grupo focal e comparação do fluxo atual real, foram elencadas as **Dificuldades** encontradas no atual fluxo de informação a partir das convergências de ideias apresentadas nos encontros.
6. Reunir mudanças culturalmente possíveis e desejáveis	Analisadas as entrevistas de grupo focal, foram elencadas as **Soluções** geradas com o debate sobre as mudanças possíveis e desejáveis que podem ser levadas além de situação problemática detectada.
7. Sugerir ações para transformação da situação problemática	As **Recomendações** surgiram como ações de melhorias e transformação. Como principais ações de transformação ficou evidenciado o problema de pesquisa do autor com uma forma de melhorar a gestão das informações em verificar a viabilidade da participação efetiva de vítima de fraude bancária nos processos de comunicação de fraudes bancárias pela internet, bem como surgiu uma nova ideia de envolvimento das instituições financeiras em efetivamente alimentar a BNFBE, passando a responsabilidade para cada instituição financeira. No decorrer das entrevistas surgiram ainda ideias de trabalhos futuros que podem ser sintetizados na proposta final de produção de informação estratégica.

Fonte: Elaborado pelo autor (2020) adaptado de Checkland (1985).

4.6 PERCEPÇÕES E ANÁLISES OBSERVADAS NA APLICAÇÃO DO GRUPO FOCAL

A seguir seguem os resultados das sínteses relevantes das entrevistas e os quadros de análise dos temas propostos com suas categorias analisadas a partir das reuniões realizadas do grupo focal, visando analisar e interpretar de forma clara os temas discutidos com o fim de atender os objetivos da pesquisa aqui estudada. Os quadros foram divididos conforme os temas debatidos.

4.6.1 Percepções quanto ao Fluxo da Informação atual na comunicação dos Processos de Contestação sobre Fraude Bancária

Iniciada a discussão do primeiro tema "Atraso na comunicação e na alimentação das informações dos processos de contestação sobre fraude bancárias eletrônica e incompletude de dados", com a pergunta direcionada ao grupo focal "Como melhorar a gestão das informações sobre fraude bancária eletrônica na BNFBE evitando atraso na comunicação e na alimentação das informações dos processos de contestação sobre fraude bancárias eletrônica e incompletude de dados?" Considerando-se que o grupo de PARTICIPANTES foi formado por policiais com vasta experiência e especialistas em investigações que envolve fraudes bancárias eletrônicas na PF.

No primeiro momento e diante do conhecimento que os PARTICIPANTES detinham, tornou-se desafiador para o moderador manter o foco acerca do tema em discussão, quase sempre os PARTICIPANTES norteavam suas percepções para o segundo tema da pesquisa, precisando algumas vezes enfatizar o interesse em manter o foco em discussão, muito embora se tornasse claro que as circunstâncias acerca do segundo tema era consequência direta dos problemas abordados na primeira discussão.

Para Hughes e Dumont (1993), o moderador/pesquisador deve mediar as discussões a partir do conhecimento cultural e da forma de falar dos participantes. Ele deve intervir o mínimo possível visando direcionar as discussões, mantendo o foco e assegurando o envolvimento de todos os participantes no tema de pesquisa discutido (GREENBAUM, 1998).

Todos os PARTICIPANTES declararam de alguma forma problemas para a investigação relacionados ao "tempo" no fluxo de informação atual. Relataram que o fluxo completo na comunicação de fraude bancária desde a vítima de fraude até o início de uma investigação depois das informações inseridas na BNFBE possui problemas na comunicação, no tempo de inserção das informações, na completude de dados e inter-relacionamento entre os atores envolvidos.

Apenas o PARTICIPANTE 6, após apresentado o fluxo atual da informação, relatou que o modelo atual é viável e que no papel como mostrado não visualiza nenhum problema aparente no fluxo, mas observa que o que precisa melhorar é a questão de resposta de todas as instituições financeiras para que elas possibilitem que as informações sobre fraude bancárias cheguem na BNFBE o mais rápido possível.

Neste sentido, os PARTICIPANTES do encontro sinalizaram problemas relacionados a tempo que a informação percorre no fluxo atual, conforme se verifica nas falas a seguir ocorridas pela ordem que os participantes interviam:

"[...] a informação quando ela chega na polícia, ela chega de forma a fracionada [...]".

"[...] fracionada porque eu num primeiro momento o banco informa a fraude e após a instauração do inquérito policial esse dado inicial ele se mostra muito pouco para o bom andamento da investigação [...]".

"[...] daí são feitas diversas solicitações ao banco de informações que muitas vezes a própria instituição bancária já tem [...]".

"[...] isso faz com que a investigação demore e com o passar do tempo a probabilidade de sucesso dessa investigação ela diminui [...]" (PARTICIPANTE 4)

"[...] o fluxo de informação ele não é tão simples então ele acaba demandando por mais sério que sejam os envolvidos em tornar isso rápido, acaba demandando um tempo razoável que não seria o tempo ideal para uma investigação. O ideal para investigação seria praticamente um tempo imediato ou então 1, 2 ou 3 dias no máximo, no entanto a gente vê que é inviável [...]" (PARTICIPANTE 5).

"[...] a gente trabalha hoje com *deley* temporal muito alto, muito longo e a partir da nossa experiência com investigações anteriores nós percebemos que as quadrilhas estão se organizando cada vez mais e acho que as que são só um pouquinho mais organizadas elas já trabalham com troca de equipamento semanal é o que dificulta muito a investigação [...]" (PARTICIPANTE 5).

"[...] O que demora e que estamos desde o começo falando, é para essa informação ficar disponível para ser pesquisada pelo investigador, isso é que é a demora e onde se processa e muito essa demora é na carga de alimentação da BNFBE [...]"

"[...] o ideal seria a disponibilização da informação praticamente em tempo real [...]" (PARTICIPANTE 4).

“[...] também temos o problema que algumas informações que são importantes para os dados em investigação que nesse modelo a vítima não consegue fornecer [...]” (PARTICIPANTE 4).

“[...] se você tem uma informação paralela ao processo de contestação direto à espera de ser validado essa informação ainda que incompleta ela pode alimentar pontos de convergência que já estão sendo explorados na investigação [...]”(PARTICIPANTE 7).

“[...] As instituições financeiras deveriam ser as mais interessadas nessa rapidez de troca de informações [...]”

“[...] As instituições financeiras deveriam se antecipar na alimentação dos dados para tornar o processo de comunicação mais ágil porque o prejuízo recai sobre ele, assim liberaria mais policiais para trabalhar diretamente com as investigações em si [...]” (PARTICIPANTE 3).

“[...] pra complementar com os colegas que já falaram eu acho que inicialmente os bancos eles precisam investir um pouco no aumento das equipes e no treinamento das equipes de alimentação e transmissão de dados de forma que essa alimentação seja o mais completa possível mais correta possível para evitar retrabalho, o que reduz a incompletude de dados e ganha agilidade também [...]” (PARTICIPANTE 10).

“[...] Necessita que o banco gerasse essa informação que pudesse mandar pra polícia federal o mais rápido possível; então o gargalo todo aqui está na instituição bancária [...]” (PARTICIPANTE 6).

“[...] com relação a incompletude de dados as instituições financeiras poderiam inovar tendo em vista que cada operação é feita por meio eletrônico, automaticamente elas vão ter coordenadas do ponto onde foram efetivadas e esses dados que podem indicar de onde partiu a fraude, serve de grande importância para a polícia e em tempo real melhor ainda, pois se conseguiria com o cruzamento de fluxo de dados a possível localização de grupo criminoso [...]” (PARTICIPANTE 1).

Evidencia-se, portanto, que todos os participantes de alguma forma apontaram que uma das grandes dificuldades para o bom andamento de investigações está relacionada ao

tempo de inserção das informações na BNFBE, seja pelo atraso, quando tardia, seja pela completude de informações inseridas que também gera atraso nas investigações com os novos pedidos de informações por falta de dados completos.

Já nesse primeiro encontro vale ressaltar a análise das transcrições e percepções prestadas pelo apoio técnico observador. Foi de grande relevância as observações apontadas quanto às intervenções dos participantes e debate entre um e outro participante sobre o tema em questão, conforme podemos verificar a seguir:

"[...] os PARTICIPANTES 2 e 5 se anteciparam acerca dos convênios atuais de acesso à BNFBE e se as polícias civis estaduais estariam tendo o compartilhamento da base [...]" (Apoio Técnico).

"[...] O Moderador/pesquisador interviu: Os bancos pedem ajuda da PF mas não compartilham informações suficientes, mas tão somente aquilo que os interessa [...] (Apoio Técnico).

"[...] os PARTICIPANTES 4 e 8 debateram sobre... exigência que as instituições financeiras exigem o boletim de ocorrência, que são totalmente divergentes quanto ao formato, mas que formulário único, padrão, facilitaria a investigação [...]" (Apoio Técnico).

"[...] os PARTICIPANTES 4, 5 e o Moderador/pesquisador debateram o tempo de inserção dos dados na BNFBE desde o cometimento da fraude. O PARTICIPANTE 5 pela experiência investigativa informa que antigamente a margem de segurança era de seis meses para inserção completa da fraude. O Moderador/pesquisador apontou que o normal é de dois a três meses o tempo de inserção. Já o PARTICIPANTE 4 complementou com a experiência investigativa na Operação Las Vegas, foi aberto contato com o pessoal do cartão de crédito da CEF. Relatou que o colega da PF afirmou que recebe as informações, mas não tem como alimentar pela falta de pessoal. Por isso se faz o pedido diretamente à CEF. As informações não são padronizadas [...]" (Apoio Técnico).

Deste modo é possível identificar como resultado do encontro do primeiro tema discutido que a alimentação tardia causa dificuldades para o bom andamento de investigações, que o melhor momento de combate ao crime é logo após o seu cometimento. Os policiais estão sempre atrás de um flagrante e essa demora na alimentação da BNFBE dificulta demais a ocorrência de flagrantes.

A vítima sofre uma fraude e já nesse momento, ela demora a contestar no banco. O banco por sua vez também demora em repassar as informações para a Polícia. E a Própria PF demora em de fato alimentar a base. Ainda tem a demora para o Policial fazer uma análise devida desses dados para gerar a informação ou relatórios para combater o crime. Como resultado do debate e pela experiência investigativa entendeu-se que todo o processo de inserção dos dados sobre determinada fraude bancária demora de um a quatro meses no mínimo, perdendo assim, o princípio da oportunidade em investigar grandes grupos criminosos, quando o ideal deveria ser no máximo um mês.

O Quadro 12 mostra o resultado da análise do Tema 1 do Grupo Focal acerca do atraso na comunicação e na alimentação das informações dos processos de contestação sobre fraude bancárias eletrônica e incompletude de dados.

Quadro 12 - Análise do Tema 1 do Grupo Focal

TEMA I	CATEGORIA	ANÁLISE DO GRUPO FOCAL
ATRASO NA COMUNICAÇÃO E NA ALIMENTAÇÃO DAS INFORMAÇÕES DOS PROCESSOS DE CONTESTAÇÃO SOBRE FRAUDE BANCÁRIAS ELETRÔNICA E INCOMPLETUDE DE DADOS.	DIFICULDADES	Alimentação tardia da BNFBE.
		Bancos Privados resistem em repassar as informações sobre fraudes bancárias.
		Pouco capital humano para inserir os dados. Retrabalho com o recebimento dos dados antes de inserção na BNFBE.
		Fraudes ainda não inseridas na BNFBE durante investigações.
		Arquivos com muitos erros nos dados sobre as contestações e/ou desatualizados.
		Maior integração entre Instituições Financeiras e Polícia
		Falta de comprometimento das Instituições financeiras
		Facilidade nos descartes de dispositivos que realizaram as fraudes
		Legislação muito fraca de combate aos crimes cibernéticos.
	SOLUÇÕES	Maior envolvimento e comprometimento das Instituições Financeiras
		Validação automática pelo banco para não ocorrer demora.
		Criação de máscaras para não ocorrer erro na inserção dos dados.

		Criação de um sistema complexo e robusto que possibilite a interação entre instituição financeira e PF em tempo real
	RECOMENDAÇÕES	Criar ferramentas de inteligências geradoras de informações estratégicas e relatórios de inteligências.
		Aumentar efetivo das equipes de segurança das Instituições Financeiras e de Policiais envolvidos na manutenção da BNFBE
		Criar Canal de comunicação direta da vítima de fraude com a BNFBE com a participação efetiva das instituições financeiras e da PF em tempo real para validar essas informações sobre fraude.

Fonte: Elaborado pelo autor (2020).

4.6.2 Percepções quanto à viabilidade e meios de se propor a participação efetiva da vítima imediata na comunicação dos processos de contestação de fraude bancária

Antes de iniciar a segunda rodada de entrevistas em grupo focal, o pesquisador resumiu o resultado da primeira reunião, com as primeiras citações e informações relevantes apontadas pelos PARTICIPANTES acerca dos objetivos da primeira rodada. Ressaltou que a ideia central é poder compilar as opiniões de cada PARTICIPANTE para, a partir dos problemas e sugestões apontadas, obter recomendações sobre o segundo tema a ser debatido e, com o resultado dos dois encontros, se o grupo entender, recomendar um novo fluxo e sistemografia do modelo a ser proposto para melhoria na gestão das informações inseridas na BNFBE.

Iniciada a discussão do segundo tema sobre "Quais informações importantes que a vítima de fraude bancária eletrônica detém que podem ser relevantes para as investigações sobre fraude bancária" com a pergunta sugerida pelo autor da pesquisa "De que forma poderia ocorrer com maior efetividade a participação da vítima de fraude bancária eletrônica?". Os PARTICIPANTES iniciaram os debates do segundo encontro sobre problemas e sugestões para obter maior efetividade à participação da vítima de fraude bancária eletrônica, conforme se verifica nas discussões a seguir:

"[...] Tinha que ser um formulário digital totalmente padronizado com a Base, que ele tivesse a capacidade de criticar qualquer informação que não tivesse dentro dos padrões e um campo livre de informações adicionais acho que esse seria o primeiro passo, pra já começar a criação do procedimento modelado [...] seja através do banco, seja através da vítima [...] esse sentido do fluxo deveria se discutir com os bancos[...] mas seria obrigatório... o sentido se vai

da vítima pro banco, do banco pra base ou se vai direto da vítima uma plataforma que alimentaria a base... eu acho que a gente tem que realmente amadureci a participação da vítima nesse processo de alimentação [...]" (PARTICIPANTE 5).

"[...] Essa viabilidabe de participação da vítima como o PARTICIPANTE 5 falou com certeza ganharia velocidade... Essas informações entrariam direto na base e ficariam submetido a homologação por parte da CAIXA; então a iria ter informações para trabalhar com dados homologados e não homologados [...] que a CAIXA iria demorar 2 ou 3 meses para homologar, mas o policial já teria informações que determinada conta, determinadas transações são objeto de contestação; Então quem está operando a base já veria logo isso aí com 1 ou 2 dias... os policiais que já tinha conhecimento quase que de imediato de determinadas contestações [...]" (PARTICIPANTE 1)

"[...] o banco tem o tempo pra fazer o processo de contestação dele...nada impediria que no momento que a fraude fosse cadastrada numa plataforma gerenciada pelo banco, ele fornecesse as informações por meio digital dessa plataforma dele e corresse o processo de contestação dele [...]" (PARTICIPANTE 5).

"[...] poderia-se então ficar a cargo da FEBRABAN e não só dos bancos individualmente, pois pelos acordos de cooperação existentes, a FEBRABAN é o meio de unir todos os bancos [...]" (MODERADOR).

"[...] Mas nenhum banco abra mão de analisar sua própria contestação...cada banco tem o seu formato, suas exigências, suas medidas, suas políticas, por tudo isso fica difícil centralizar os processos de contestação na FEBRABAN [...]" (PARTICIPANTE 5).

"[...] Mas a FEBRABAN poderia sugerir o mesmo formulários para todos os bancos do acordo de cooperação...só o poder decisório ficaria a cargo de cada instituição financeira. As instituições financeiras poderiam ficar com a responsabilidade de inserção dos dados em uma basenacional de fraude bancária inificada para todos os bancos [...]" (PARTICIPANTE 10)

"[...] seria interessante a ideia do preenchimento de um formulário que já caísse direto na base e na base de dados ter um campo lá, um "flag" informando se a fraude já foi validada

ou não... a questão primordial aqui é dinamizar o processo...porque mandar pro banco e o banco ficar analisando lá e só deus vais saber quando vai chegar na base para se iniciar a investigar...então uma coisa interessante seria você já ter o dado na base e o passo seguinte seria procurar saber se aquela contestação foi validada ou não...o policial envolvido na investigação já teria como fazer levantamentos, fazer estudo de caso... então acho que deveria um formulário único para todos os banco, esse formulário único deveria ser pré-requisito do processo de contestação, senão os bancos não iriam fazer... e que esses dados fossem diretamente inseridos na BNFBE [...] essa ideia de fomentar de algum modo a participação da vítima não seria apenas viável no modelo atual, mas necessária [...]" (PARTICIPANTE 8).

"[...] É importante para a gente também (PF) ter as informações sobre as auto-fraudes, não deixa de ser um informação que agrega a investigação [...] outra circunstância relevantes é que a BNFBE só recebe determinados dados brutos, alguns detalhes adicionais que os clientes vítimas informam no processo de contestação que não são alimentados na BNFBE, isso não chega ao investigador. No momento que você reforça a participação da vítima nesse processo de alimentação, teríamos além dos dados que o bancos fornece, teríamos a descrição da vítima e outros dados que não chegam para a investigação [...]"(PARTICIPANTE 5).

"[...] A vítima alimentando a base e isso estando para a gente em tempo real você vai ver as fraudes acontecer em tempo real, então assim, você vai ter ali três mil contestações acontecendo num curto espaço de tempo de determinado tipo de fraude, isso dá o poder a polícia de dizer, olha tá ocorrendo a atuação de uma organização criminosa aqui, até mesmo geograficamente e focar e descobrir qual o tipo de fraude [...] e como é feito hoje, vai entrando as contestações, elas vão entrando em momentos diferentes na base e quando a gente vai ver que aquilo é a atuação de uma organização criminosa já se passou um tempo que a organização já se moveu ou mudou a forma de atuar [...]" (PARTICIPANTE 10).

"[...] aquela parte de inserção de dados que está exclusivamente com a parte policial e iria traze-la bem precocemente, iria deslocar ela para a vítima, isso traria a vantagem que esse mesmo formulários, na realidade quando a vítima preenche como sendo pre-requisito para a contestação, eu entendo ela indo para dois caminhos, cai na base e no sistema de segurança do banco. Daí eu vejo dois processos correndo em paralelo. Aquelas informações que só a vítima tem, já está disponível pra polícia e aquelas informações que o banco vai inserir em paralelo, o

banco pode ir inserindo em tempo real dentro da base e caso haja uma auto-fraude, isso fica visível pra gente [...]" (PARTICIPANTE 7).

"[...] É um cenário simples para a vítima entender, é como se fosse a declaração de imposto de renda da Receita Federal, que a própria pessoa declara e automaticamente cai na base da receita, fica lá em análise e quem quiser já está trabalhando com os números tudo ali em tempo real. Pode copiar o mesmo modelo da declaração de imposto de renda [...]" (PARTICIPANTE 1).

"[...] outro exemplo interessante em que a participação da vítima ocorre com a inserção de dados em a base de dados do ALERTA da Polícia Rodoviária Federal sobre notícia de furto e roubo de veículos, a vítima alimenta os dados do carro roubado e responde nas medidas dos dados falsos inseridos e naquele momento é disparado alertas em tempo real na tentativa de recuperar esse veículo roubado [...]" (MODERADOR).

"[...] Para mim a viabilidade não é clara num primeiro momento, mas acho a ideia boa e válida, vale a pena o estudo. Seria uma mudança de formato que para a polícia seria maravilhoso, agora assim, tudo isso envolve segurança, porque o usuário que vai enviar esses dados ele vai precisar está seguro para fazer isso, como que a polícia implementaria isso. São dados importantes, ele vai digitar CPF, vai digitar número de conta. Então assim a ideia é interessante, mas para implementar isso tem um custo computacional e de segurança alto. E assim, eu acredito que hoje você já tem as informações que são direcionadas ao banco; então como falei da outra vez, eu acho que o ideal para mim seria melhorar essa qualidade, essa velocidade da informação [...]" (PARTICIPANTE 6).

"[...] o grande problema e grande entrave é justamente a legislação. Não há ainda uma legislação que de certa forma obrigue ou então que nos dê acesso a tais informações. Nós sempre estamos dependendo ou da instituição bancária ou da própria vítima. Eu acho que a mudança principal seria uma legislação que nos desse pleno acesso a essas informações sobre fraude bancária sem ter que tá pedindo ao banco. Hoje o banco nos dar o que ele quer e da maneira que ele quer, no tempo dele e isso atrapalha investigação policial [...]" (PARTICIPANTE 4).

“[...] da maneira que é feito hoje o material humano que nós temos no GPA ele é insuficiente, para quantidade de dados brutos que temos que alimentar, pra quantidades de dados brutos que vão ter que ser informado, aquele pessoal não vai ter condições de gerenciar, de tratar esses dados. Eu creio que ou se aumenta a quantidade de policiais para fazer o tratamento desses dados ou seria esses dados já virem tratados num formato próprio da base, desde a instituição bancária até o GPA. Existisse um acordo para que os dados já viessem pronto para serem inseridos na base. Já diminuíram muito da carga humana, mas da forma que está hoje seria impossível pela quantidade absurda de dados [...]” (PARTICIPANTE 4).

Do mesmo modo do primeiro, encontro o apoio técnico observador realizou anotações ocorridas durante o debate e que não ficaram muito claras nas gravações áudio-visuais, conforme podemos verificar a seguir:

“[...] o MODERADOR e o PARTICIPANTE 5 discutiram sobre as circunstâncias se a FEBRABAN não poderia administrar os processos de contestação. Tendo o PARTICIPANTE 5 respondido que era muito difícil ocorrer isso por conta da diversidade de formas de contestação dos bancos [...]” (Apoio Técnico).

“[...] O PARTICIPANTE 10 relata que a vítima alimentando a BNFB, em tempo real, dá-se o cruzamento de informações. Atualmente existe na BNFB um processo de migração na produção de relatórios vinculantes [...]” (Apoio Técnico).

“[...] O PARTICIPANTE 7 faz a observação que o processo de inserção: vítima e banco seria mais célere. Na medida que as informações fossem incluídas, a investigação seria eficiente [...]” (Apoio Técnico).

“[...] O PARTICIPANTE 6 faz a objeção que a implementação dessa forma se requer um custo muito alto. O ideal era melhorar a informação dos bancos em relação a polícia [...]” (Apoio Técnico).

“[...] por fim o PARTICIPANTE 4 opina que a ideia do formulário é interessante, mas a legislação é um entrave. Pois, a polícia sempre vai depender de pedidos aos bancos. Os bancos por sua vez, somente dão as informações que eles querem. As informações chegam incompletas atrapalhando em muito a investigação. Da forma que a estrutura é composta atualmente não é

viável dado a quantidade volumosa de informações e os recursos humanos serem aquém daquilo que se necessitaria para fluir a investigação [...]" (Apoio Técnico).

Com resultado e análise de todos os debates foi possível observar que quase todos PARTICIPANTES relataram que para a rapidez e o sucesso na produção de relatórios e informações de inteligência, resultando em uma boa investigação, é viável a participação efetiva da vítima de fraude bancária na inserção dos dados na BNFBE, conforme sugestão do tema proposto pelo autor.

O PARTICIPANTE 10 destacou que além da participação da vítima de fraude bancária na inserção dos dados na BNFBE, poder-se-ia verificar a viabilidade de participação das instituições financeiras na inserção dos dados na BNFBE.

O PARTICIPANTE 6 por outro lado, embora considerando a ideia válida e interessante, não concordou com a proposta de melhoria sugerida pelo autor da pesquisa, tendo em vista que considerou que a implementação poderia requerer um custo muito alto, que a base já se encontra modelada, implementada e em utilização. Considerou ainda que o ideal seria melhorar a informação que os bancos repassam para a polícia.

O Quadro 13 mostra o resultado da análise do Tema 2 do Grupo Focal sobre "Quais informações importantes que a vítima de fraude bancária eletrônica detém que podem ser relevantes para as investigações sobre fraude bancária:

Quadro 13 - Análise do Tema 2 do Grupo Focal

TEMA I	CATEGORIA	ANÁLISE DO GRUPO FOCAL
QUAIS INFORMAÇÕES IMPORTANTES QUE A VÍTIMA DE FRAUDE BANCÁRIA ELETRÔNICA DETÉM QUE PODEM SER	DIFICULDADES	Atualmente não existe meios de saber qual porta a vítima de fraude abriu para inserção do artefato malicioso
		Não existe formulário padrão digitalizado para todas instituições.
		Cada banco possui seus módulos de segurança, seu próprio formulário de contestação e a polícia não sabe os meios e mecanismos de bloqueio e de proteção dos clientes.
		As instituições financeiras não abrem mão de analisar seu próprio processo de contestação.
		A polícia quase nunca possui acesso aos módulos de segurança do banco fraudado.
		Os bancos orientam as vítimas a formatar os computadores. Melhor fonte de investigação é um computador ou celular

		infectado de uma vítima. Engenharia reversa. Classificar o artefato malicioso. Vincular ao fraudador.
		Custo computacional e de segurança alto para mudar o modelo atual existente
	SOLUÇÕES	Acesso aos módulos de segurança dos bancos após a ocorrência de fraudes.
		Inserção dos dados sobre fraudes a cargo da instituição financeira ou da vítima.
		Melhorar a troca de informações das instituições financeiras com a polícia
		FEBRABAN padronizar um formulário digital padrão de contestação
		Aumentar o capital humano nas instituições financeiras e na polícia que tratam sobre os dados brutos sobre fraude bancária
	RECOMENDAÇÕES	Criar um meio de inserção na BNFBE ficando a cargo da vítima ou da instituição financeira de modo que essas informações entrariam direto na base e ficariam submetido a homologação por parte da instituição financeira fraudada, possibilitando o policial ter tais informações para trabalhar com dados homologados e não homologados visando aproveitar o princípio da oportunidade para ocorrências de fraudes bancárias o mais próximos de seu cometimento.
		Como trabalhos futuros, estudos sobre a viabilidade de criação de uma plataforma web por meio de convênios que possibilite inserção de informações sobre fraudes bancárias diretamente pelas vítimas e validadas pelas instituições financeiras com acesso e integração entre todas forças de segurança pública.

Fonte: Elaborado pelo autor (2020).

4.6.3 Propostas de novo fluxo da informação na comunicação dos processos de contestação sobre fraude bancária

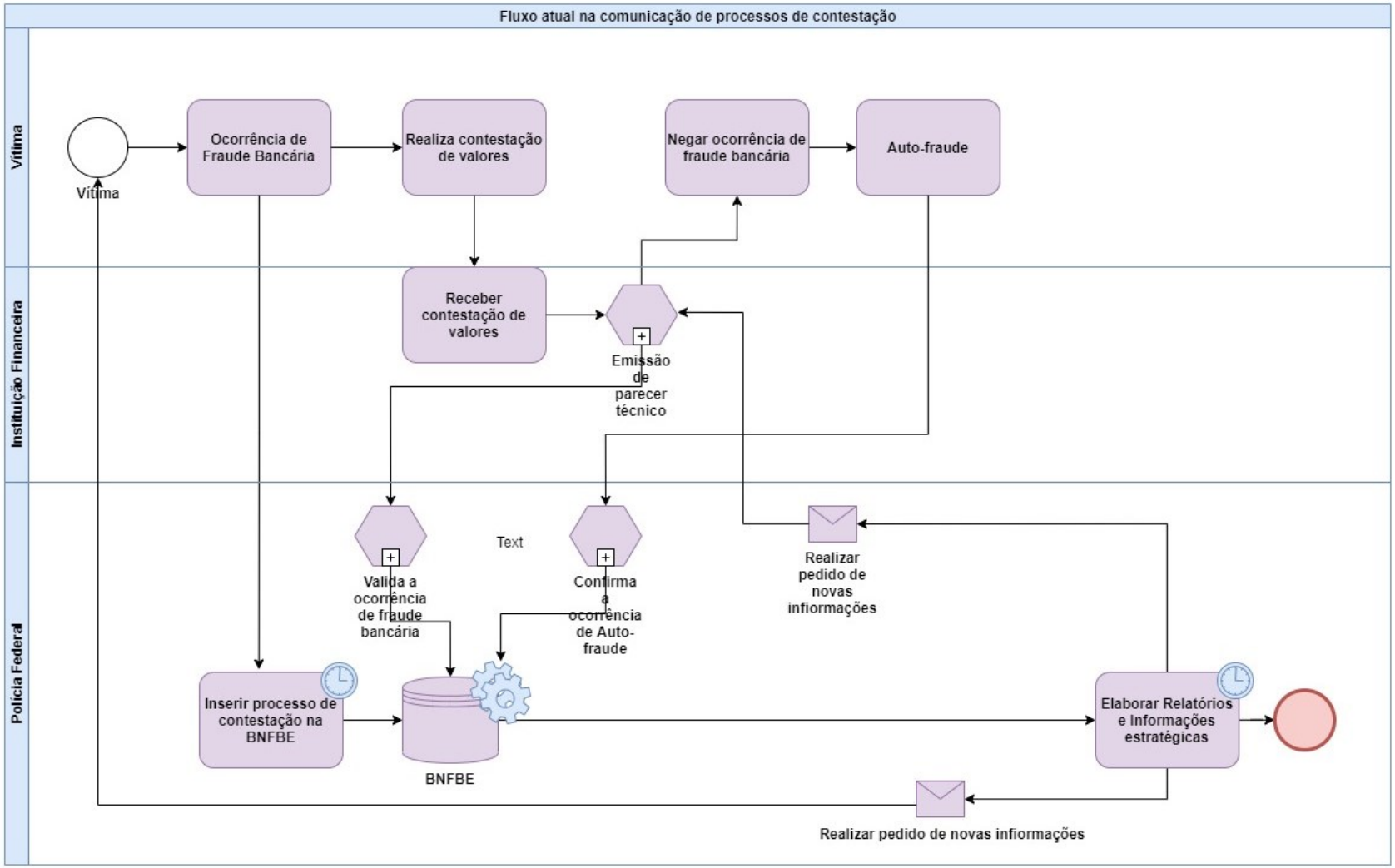
Ao final das entrevistas de grupo focal, apresentado e debatido a atual representação gráfica do fluxo da informação da BNFBE e o mapeamento do fluxo de informação na comunicação dos processos de contestação, foram debatidos durantes os encontros esboços e duas propostas de melhorias de fluxo da informação dos processos de contestação na alimentação da BNFBE.

Segundo Simon (1999), a falha mais comum após realizada a análise científica e criteriosa dos dados coletados é que a informação gerada não é efetivamente utilizada. Para que isso não ocorra, deve-se definir uma maneira de transformar os resultados em ações concretas.

Das duas propostas de melhorias que surgiram como recomendações, uma resultou de forma muito semelhante ao pretendido e proposto como sugestão do autor em que consiste numa forma que a vítima imediata da fraude bancária possa inserir as informações sobre fraude bancária, sendo validado pela instituição financeira posteriormente, mas que a PF já pudesse ter acesso a esses dados inseridos pela vítima.

A partir do modelo de fluxo da informação atual na comunicação dos processos de contestação sobre fraude bancária eletrônica (Figura 20), a Figura 25 foi elaborada como uma proposta de melhoria de um novo fluxo da informação na comunicação dos processos de contestação sobre fraude bancária eletrônica, de acordo com as sugestões e recomendações pertinentes ocorridas nos encontros de grupo focal realizados.

Figura 25 - Representação gráfica de novo fluxo da informação na comunicação dos processos de contestação sobre fraude bancária eletrônica com a participação efetiva da vítima de fraude bancária na inserção das informações



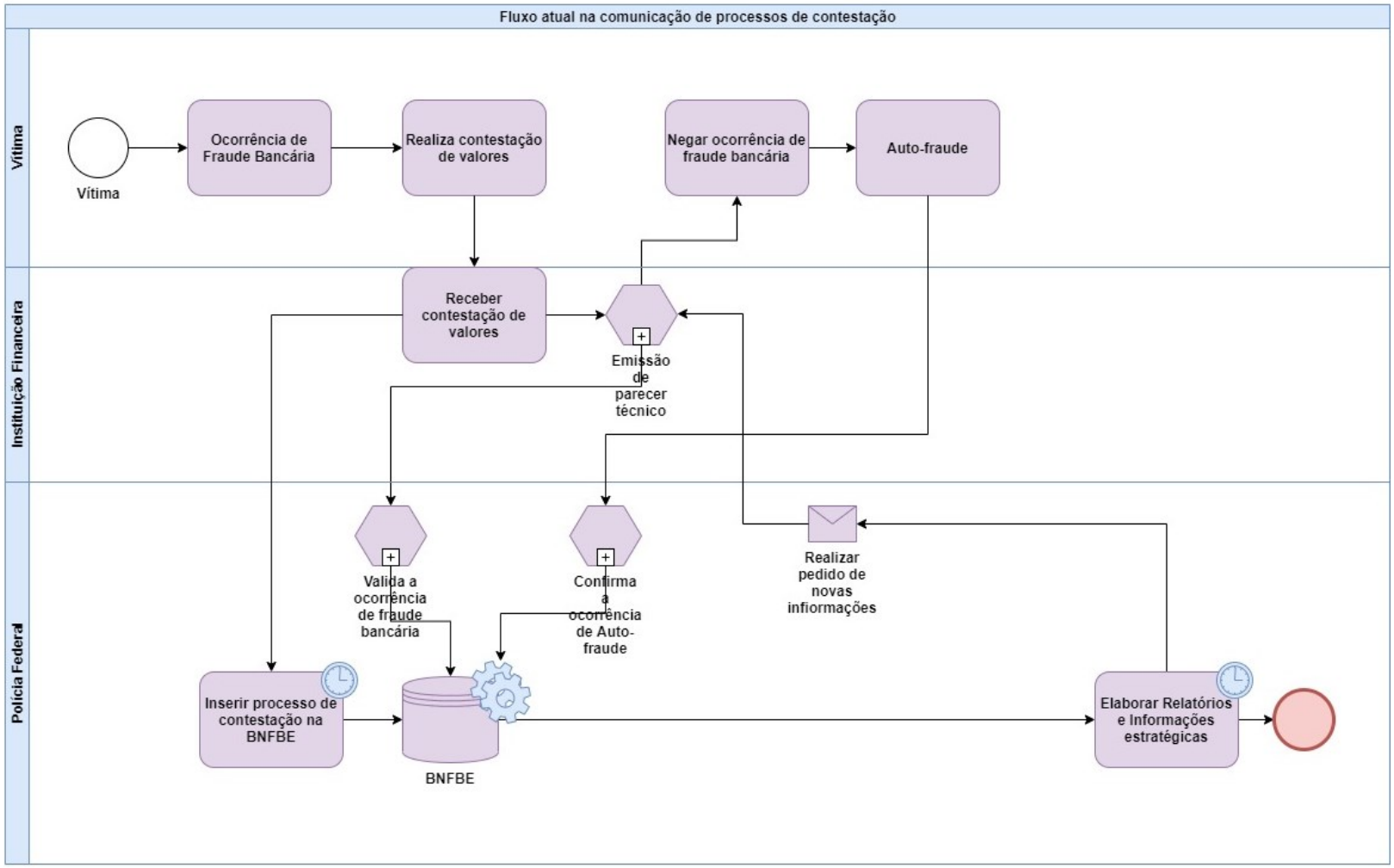
Fonte: Elaborado pelo autor (2020).

O fluxo representado na Figura 25 foi apresentado a partir das melhorias propostas pela maioria dos participantes do grupo focal, enfatizando em especial melhorar os problemas e dificuldades na alimentação tardia e/ou fraudes ainda não existentes na BNFBE.

Outro ponto destacado no encontro consistiu no encaminhamento de informações com muitos erros nos dados sobre as contestações e/ou desatualizados, ou seja, dados incompletos, o que pode se confirmar que, embora existam formalmente criados os acordos de cooperação, ainda carecem de maior integração entre Instituições Financeiras e a Polícia Federal.

Com exceção dos PARTICIPANTES 6 e 10, todos PARTICIPANTES foram unanimes em afirmar a necessidade de envolver a participação da vítima de fraude bancária na inserção de dados nos processos de contestação, concordando como viável e possível uma proposta de melhoria em que a vítima de fraude bancária possa inserir na BNFBE as informações sobre a fraude bancária sofrida. Os PARTICIPANTES do grupo focal realizaram ainda um esboço de representação gráfica de fluxo da informação na comunicação dos processos de contestação sobre fraude bancária eletrônica a partir da sugestão e percepção do PARTICIPANTE 10, resultando no mapeamento representado na Figura 26 em que a inserção de dados na BNFBE ficasse a cargo de cada instituição financeira.

Figura 26 - Representação gráfica de novo fluxo da informação na comunicação dos processos de contestação sobre fraude bancária eletrônica com a participação efetiva da vítima de fraude bancária com a inserção das informações pelas instituições financeiras.



Fonte: Elaborado pelo autor (2020).

Atualmente, a Polícia Federal encabeça o desenvolvimento de um novo projeto que tem como objetivo a migração de todos os dados sobre fraudes bancárias da atual BNFBE para um novo conceito de banco de dados não relacional denominado de grafos. Este tipo de armazenamento facilita o encontro de vínculos entre as fraudes. Além da migração dos dados para esta nova plataforma e do encontro de fraudes relacionadas, o projeto também pretende buscar dados dos alvos da investigação em outros bancos de dados e indicar o melhor local para a atuação da persecução penal.

O surto de pandemia de COVID-19 ocasionado pelo novo Coronavírus (Sars-Cov-2) fez surgir uma nova modalidade de fraude bancária consistindo em saques fraudulentos do Auxílio Emergencial. A metodologia investigativa é baseada nos mesmos moldes do Projeto Tentáculos. As fraudes são relacionadas à concessão e ao pagamento do benefício do Auxílio Emergencial concedido pelo Governo Federal e destinado aos trabalhadores informais, microempreendedores individuais (MEI), autônomos e desempregados, com o objetivo de fornecer proteção emergencial no período de enfrentamento à crise causada pela pandemia.

Para tanto foi firmado novos acordos de cooperação entre a PF e a CEF para criação e desenvolvimento da Base Nacional de Fraudes ao Auxílio Emergencial (BNFAE) visando combater esse novo tipo de fraude relacionadas ao pagamento fraudulento desses benefícios.

A qualidade das informações reunidas irá depender da forma que o pesquisador planeja e conduz as entrevistas. Vencidas essas etapas, realizadas com método e rigor científico, uma análise criteriosa irá gerar as conclusões atinentes ao trabalho de pesquisa, as quais poderão direcionar alguma tomada de decisão (RIBEIRO; MILAN, 2004, p. 21-22).

A importância da presente pesquisa como um estudo não generalizado, mas direcionado e realizado com os dois encontros em grupo focal com Policiais Federais especialistas em fraude bancária serviu para lançar luzes não só para outros Policiais Federais que trabalham com investigações sobre fraudes bancárias, mas também para outros sujeitos envolvidos tais como Membros do Ministério Público, Governo Federal, titulares das ações penais e em especial as instituições financeiras que possuem o interesse direto em razão dos enormes prejuízos que sofrem com tais fraudes, podendo o estudo ser expandido como trabalhos futuros.

4.6.4 Proposta de Produção de Informação Estratégica sobre Fraude Bancária Eletrônica na Polícia Federal aplicando as sete fases de Washington Platt

Considerando as recomendações e melhorias propostas pelos participantes do grupo focal, correlacionado com os conceitos dos princípios e fases de Washington Platt (1974), explanados neste trabalho e o modelo atual de produção de informação sobre fraude bancária eletrônica na Polícia Federal, os participantes do grupo focal elencaram proposta de aplicação de melhorias na gestão da informações sobre fraude bancária conforme descrito no Quadro 14, que possibilitem um modelo possível e viável de produção de informação estratégica.

Quadro 14 - Produção de informação estratégica proposta por Platt (1974) adaptado pelo autor da pesquisa a partir das percepções dos PARTICIPANTES do Grupo Focal

FASE	DESCRIÇÃO
1ª Fase - Levantamento Geral **MÉTODO**: Plano geral para a condução do trabalho com indicação de prazo, pessoal a ser envolvido e principais fontes de informação disponíveis.	**PROPOSTA DE APLICAÇÃO:** As informações e relatórios estratégicos originados a partir das informações inseridas na BNFBE devem evidenciar os sujeitos (vítima; instituição financeira; agentes de investigação) envolvidos em todo o contexto da fraude bancária eletrônica, assim como os meios de se colher auxílios e manter permanente relacionamento e comunicação com vista a obter novos informes julgados importantes. No planejamento geral deve existir os canais de comunicação e troca de informações, reais, ágeis e eficientes, entre os atores envolvidos no enfrentamento das fraudes bancárias.
2ª Fase - Definição de Termos **MÉTODO**: Definição do que se quer dizer claramente com cada termo e conceito para os analistas, revisores e clientes.	**PROPOSTA DE APLICAÇÃO:** A padronização na comunicação dos processos de contestação de fraudes bancárias eletrônicas é essencial para uma eficiente alimentação da BNFBE. A definição correta de termos associada a uma boa padronização na alimentação da BNFBE propicia estabelecer o que realmente deve ou não ser inserido na BNFBE, facilitando tanto a comunicação entre os atores envolvidos, como a produção de informações e relatórios precisos e claros pelos agentes de investigação. Convênios e acordos de cooperação podem lançar luzes para implementação de uma BNFBE com rotinas de Inteligência Artificial – IA que facilitem os trabalhos investigativos.

3ª Fase - Coleta de Informes **MÉTODO:** Estabelecimento de um *modus operandi* ou fluxo de processo para a ação de coleta de dados disponíveis e não disponíveis.	**PROPOSTA DE APLICAÇÃO: -** A produção de informações e relatórios estratégicos de fraudes bancárias eletrônicas são gerados pelos dados inseridos na BNFBE, no entanto, podem ser complementados com diversos outros dados e informações não disponíveis na BNFBE**.** É nessa fase de coleta de outros informes que se enfatiza a importância da participação da vítima de fraude bancária no fornecimento de informes úteis sobre a fraude bancária sofrida, assim como um meio de comunicação viável entre o agente de investigação e a vítima. A PF utiliza ainda outros meios de investigação para complementar os dados contidos na BNFBE, como informações levantadas por meio da vigilância policial em determinados locais, dados fornecidos por informantes, provas coletadas no cumprimento de mandados de busca e apreensão, depoimentos de vítimas, quebra de sigilos bancários, telemáticos, telefônicos autorizados judicialmente, dentre outros (PATROCINIO, 2016).
4ª Fase - Interpretação dos Informes **MÉTODO**: Avaliação, classificação, análise e interpretação de informes. A avaliação pode ser considerada parte da interpretação.	**PROPOSTA DE APLICAÇÃO:** A Produção de informações e relatórios estratégicos de fraudes bancárias eletrônicas são criados pelos agentes de investigação por meio de análises investigativa dos dados constantes na BNFBE, com o uso de técnicas, software e ferramentas, não uma análise em si de toda da situação investigativa, cabendo aos agentes de investigação definir os rumos e métodos da investigação de forma ampla para confirmar e ratificar os dados analisados a partir da BNFBE. - A BNFBE utiliza ferramentas de análise de vínculos, com modelagem própria, que buscam identificar relações existentes entre fraudes bancárias do mesmo tipo a fim de gerar informações e relatórios estratégicos únicos, que reúnam todas as vítimas de um mesmo criminoso ou organização criminosa (SIQUEIRA, 2014).
5ª Fase - Formulação de Hipóteses **MÉTODO:** A partir da interpretação dos informes são formuladas as hipóteses que apóiam	**PROPOSTA DE APLICAÇÃO: -** Produzida as informações e relatórios estratégicos sobre fraudes bancárias eletrônicas, os agentes de investigação podem ajustar a experiência investigativa, bem como outras grandes investigações em curso com *modus*

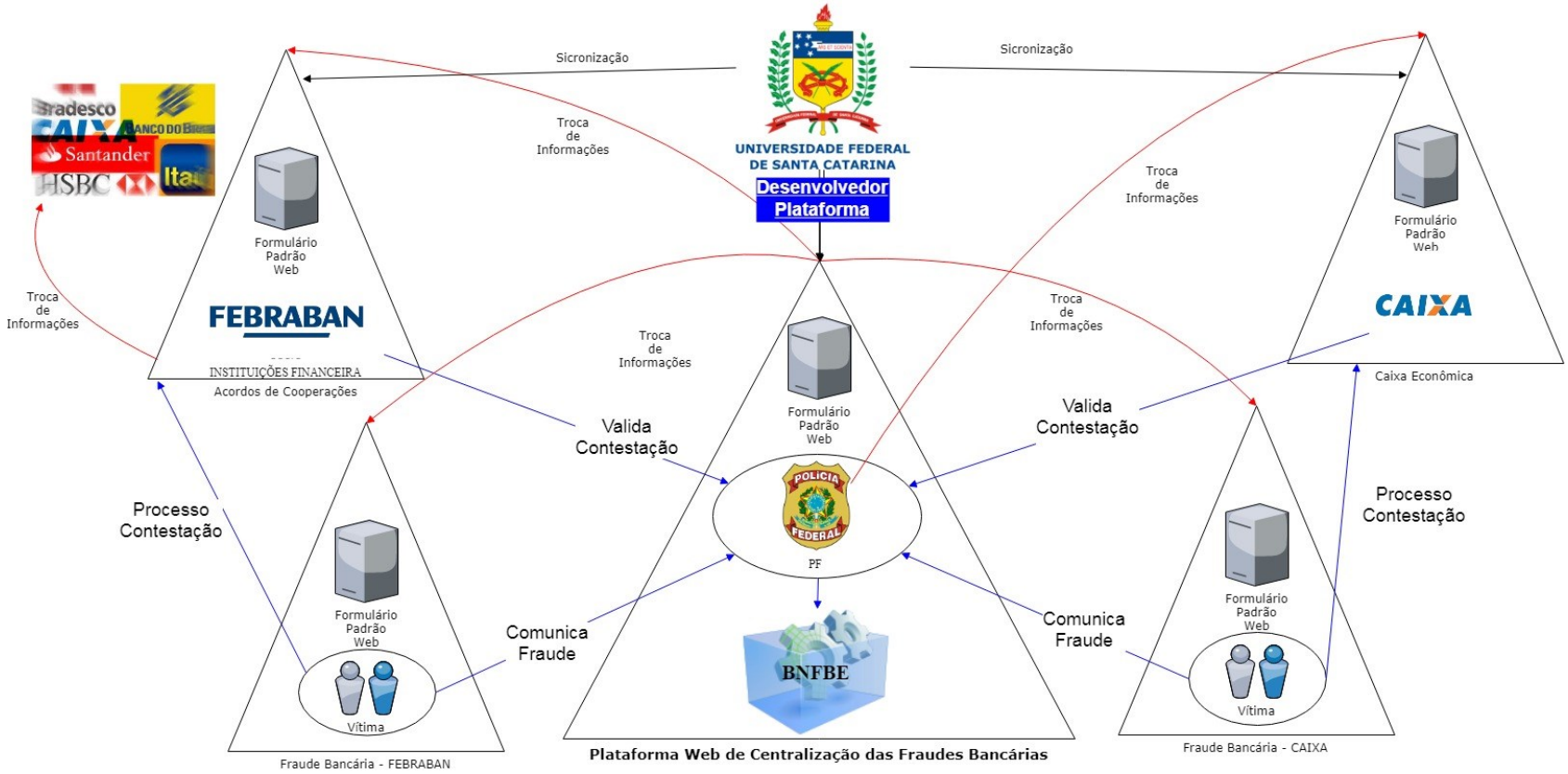
a compreensão do contexto e fornecem elementos para as conclusões.	*operandi* semelhante para definir sobre a continuidade dos métodos investigativos aplicados ou reavaliação e mudança do modo investigativo. A constante inovação tecnológica e a permanente mudança dos *modus operandi* de grupos fraudadores, fazem com que os meios investigativos sejam constantemente avaliados e modificados a partir da formulação das hipóteses experimentais. - O modelo proposto pelo Projeto Tentáculos de alimentação da BNFBE é cíclico, tendo a contínua necessidade de reavaliação com consequente proposição de alterações. O Projeto Tentáculos ao longo dos últimos anos tem sido constantemente aperfeiçoado com base nas novas formas de ação das quadrilhas especializadas em fraudes bancárias pela internet (SIQUEIRA, 2014).
6ª Fase -Tirar Conclusões **MÉTODO:** Fase destinada a provar ou reprovar a hipótese de trabalho. Forma o chamado cerne do trabalho de produção de informações.	**PROPOSTA DE APLICAÇÃO: -** Uma vez implementado a participação efetiva da vítima de fraude bancária eletrônica em todo o processo de produção das informações estratégicas, existindo o relacionamento e troca de informes entre o agente de investigação e a vítima de fraude, o agente de investigação deve ser capaz apontar, de forma clara e precisa, respostas coerentes e proveitosas às análises originadas a partir dos dados inseridos na BNFBE. Nesta proposta, temos dois objetivos: 1) Ressaltar a real importância na padronização aplicável a todas instituições financeiras na produção de informação para subsidiar o combate às fraudes bancárias de maneira estratégica, visto que, embora existam termos e acordos de cooperação para padronização, essa padronização não tem ocorrido e/ou quando ocorrem, a alimentação da BNFBE é feita de forma tardia, prejudicando o desenvolvimento de grandes investigações; 2) Inovar propondo a criação de uma plataforma web, em que a vítima de fraude bancária possa participar de forma efetiva com o fornecimento de dados e informações que possam subsidiar a produção de informação estratégica para combate às fraudes bancárias eletrônicas.
7ª Fase - Apresentação **MÉTODO:** Na apresentação o redator	**PROPOSTA DE APLICAÇÃO:** - Um bom relatório de informações estratégicas é, sem dúvida, um exemplo do Pensamento

deve ter ideias claras e expressá-las com clareza. O grau de certeza que merece cada afirmação importante deve ser indicado.	Criador. Sua redação deve considerar mais as ideias a serem exposta do que a beleza do estilo. (PLATT, 1974). Agentes de investigação da Polícia Federal, que trabalham com relatórios produzidos a partir da BNFBE, são treinados com técnicas de análise de vínculos das entidades relacionadas às fraudes bancárias (PATROCINIO, 2016). - É com base na produção de informações e relatórios estratégicos que agentes de investigação produzem conhecimento capaz de enfrentar grupos criminosos e possam provar seus envolvimentos nas fraudes para a devida persecução penal.

Fonte: Elaborado pelo autor (2020) adaptado de Platt (1974).

A expressão gráfica da Figura 27 a seguir representa o modelo proposto de maneira possível e viável da produção de informação estratégica que possa agilizar e padronizar a comunicação da informação dos processos de contestação de fraudes bancárias eletrônicas.

Figura 27 - Representação gráfica de uma proposta futura possível e viável da produção de informação estratégica



Fonte: Elaborado pelo autor (2019).

A produção de informação estratégica sobre fraudes bancárias eletrônicas pela Polícia Federal é uma forma de produção de conhecimento de inteligência policial, que se beneficia do uso de tecnologias e experiência investigativa, para obter oportunidades para o enfrentamento de organizações criminosas que cometem fraudes bancárias pela internet.

Para Sianes (2005), inteligência são informações processadas por um conjunto de estratégias, implementadas de forma eficaz, em decisões e ações necessárias. A produção de inteligência visa o alcance de objetivos preestabelecidos, como uma síntese de conhecimentos que se utiliza, inclusive, do julgamento e da intuição, antecipar e prever cenários futuros.

Muitas pessoas passam a vida toda num setor de atividades, sem tentar compreendê-la, explorar suas possibilidades ou procurar solucionar seus problemas reais de forma possível e viável. Aquele que não pensa em solucionar os problemas de seu próprio setor ou organização, desperdiça o prazer de se satisfazer com o sucesso dessas realizações (PLATT, 1974).

É com esse espírito que se tem como o objetivo de propor melhorias contínuas, possíveis e viáveis para inovação constantes no modelo de padronização, celeridade na alimentação da BNFBE e uma futura e possível participação efetiva da vítima de fraude bancária eletrônica em todo o processo de produção de informações estratégicas que contribuíam para o enfretamento daqueles que comentem fraudes bancárias pela internet.

5 CONSIDERAÇÕES FINAIS

A gestão da informação em ambientes organizacionais consiste no conjunto de atividades que visam obter um diagnóstico das necessidades informacionais; mapear fluxos de informação em seus diferentes setores; prospectar, coletar, processar, filtrar, armazenar, difundir e disseminar conhecimento com o objetivo de melhorias na tomada de decisão para o pleno desenvolvimento de suas atividades/tarefas cotidianas no ambiente corporativo (VALENTIM, 2004).

5.1 ATENDIMENTOS AOS OBJETIVOS QUE NORTEARAM A PESQUISA

O trabalho aqui demonstrado esclarece como responder a pergunta de pesquisa "**Como melhorar a Gestão das Informações sobre fraudes bancárias inseridas na BNFBE?**" sendo conduzida e detalhada a resposta com o cumprimento e atendimento ao objetivo geral e objetivos específicos da seguinte forma:

Em síntese para atingir o Objetivo Geral de **Propor melhorias na Gestão das Informações sobre fraudes bancárias inseridas na BNFBE** na seção 4.6.3 foi construído duas propostas de novos fluxo da informação na comunicação dos processos de contestação sobre fraude bancária aplicando os e ainda proposto um novo modelo de produção de informação estratégica sobre fraude bancária aplicando as sete fases de Wasshigton Platt.

O Objetivo Geral só foi possível ser alcançado após o cumprir os Objetivos Específicos que se deram com a apresentação atual do fluxo da informação na comunicação dos processos de contestação sobre fraude bancária definido como Objetivo Específico "a".

Para atendimento ao Objetivo Específico "b" foi demonstrado como é idealizada a Base Nacional de Fraude Bancária Eletrônica, como ocorre todo o processo de contestação sobre fraude bancária pela internet, a metodologia dos crimes praticados na Operação Valentina, relacionando ainda com os fundamentos da Ciência da Informação como Campo de Estudo.

A seção do Referencial Teórico desta pesquisa serviu para cumprimento do Objetivo Específico "c" ao selecionar da literatura produções já existentes que serviram para esclarecer ao leitor mais sobre elementos relacionados aos processos de contestação sobre fraude bancária, seus atores envolvidos, modus operandi das fraudes e relação do tema de pesquisa com a Ciência da Informação e Ciência Policial.

Por fim o Objetivo Específico “d” que vem a ser a essencial e resultado final esperado para completar o Objetivo Geral foi sistemografar a partir das duas entrevistas dos grupos de focais uma proposta de fluxo da informação para melhoria na comunicação dos processos de contestação sobre fraudes bancárias inseridas na BNFBE na qual resultou em duas propostas de novos fluxos.

O Quadro 15 elenca as seções que atenderam os objetivos que nortearam a presente pesquisa.

Quadro 15 - Atendimento aos objetivos que nortearam a pesquisa

OBJETIVOS	DESCRIÇÃO	SEÇÃO DE ATENDIMENTO
Geral	**Propor melhorias na Gestão das Informações sobre fraudes bancárias inseridas na BNFBE**.	4.6.3 e 4.6.4
Específico “a”	Sistemografar o atual processo de comunicação das contestações de operações de fraude bancárias;	4.1
Específico “b”	Relacionar o processo de comunicação, inserção e registro das contestações de fraudes bancárias eletrônicas na BNFBE com os fundamentos da Ciência da Informação;	2.4 e 3.1
Específico “c”	Selecionar da literatura os elementos que se relacionam com a sistemática de comunicação dos processos de contestação sobre fraude bancária eletrônica;	3
Específico “d”	Sistemografar uma proposta de fluxo da informação para melhoria na comunicação dos processos de contestação sobre fraudes bancárias inseridas na BNFBE;	4.6.3

Fonte: Elaborado pelo autor (2020).

5.2 RESULTADOS ESPERADOS

Como resultados esperados, deseja-se que esse trabalho possa contribuir como melhoria na gestão da informações trocadas entre as entidades mencionadas (Polícia Federal, Instituições Bancárias vinculadas à FEBRABAN), no sentido de aprofundar conhecimentos e instigar mudanças no modo de troca e repasse de informações sobre fraudes bancárias, bem como propor melhorias no atual sistema de comunicação dos processos de contestação, possibilitando reflexões e estudos futuros para que a vítima de fraude bancária voluntariamente

forneça as informações necessárias da ação delituosa, formando-se um grande estoque de informação de inúmeras vítimas para que possa ser preservado e recuperado oportunamente por operadores da Ciência Policial em processos investigativos e na produção de conhecimento.

Os acordos de cooperação já firmado entre a PF e a FEBRABAN são imprescindíveis para o alcance cada vez maior de melhores resultados. É preciso que cada instituição assuma sua responsabilidade e sensibilidade quanto às dificuldades de se investigar fraudes bancárias na internet, tendo discernimento quanto à dialética da constante de mudança do *modus operandi* de organizações criminosas que cometem fraudes bancárias na internet.

A busca de melhoria constante na qualidade de informações inseridas sobre fraudes bancárias na BNFBE serve de contribuição essencial e inovadora da Gestão da Informação. Espera-se ainda que a presente pesquisa contribua com boas ideias para o atual desenvolvimento do novo projeto e migração dos dados da BNFBE para um novo conceito de banco de dados não relacional denominado de grafos.

Para Ismail; Zainab (2013), a informação e seus sistemas de informação são como edifícios que necessitam de manutenção constante para evitar sua degradação devido a evolução e interações com o meio ambiente. Por sua vez, Choo (2006) afirma que a busca por significado, a criação de conhecimento e a tomada de decisões se apresentam integradas para garantir a constante inovação e as mudanças necessárias à perpetuação da organização frente ao dinamismo do ambiente. Informações geradas no âmbito da organização possuem universo limitado, se comparado ao volume de informações gerado fora da organização.

Sob a ótica dos fundamentos da CI, espera-se que o presente trabalho também possa contribuir para a comunidade científica mediante a comparação de modelos conceituais que propiciem efetivamente uma disseminação de boas práticas na comunicação e gestão da informação com a qualidade desejada, melhorando o método investigativo de combate às fraudes bancárias pela internet.

Diante do exposto, espera-se que as instituições envolvidas no combate às fraudes bancárias mantenham-se aprimorando a gestão de suas informações sobre fraudes bancárias e constamente inovem seus modelos investigativos visando acompanhar as modificações dos *modus operandi* de grupos criminosos que a cada dia criam novos métodos de cometimento de fraudes bancárias.

5.3 LIMITAÇÕES DA PESQUISA, VIABILIDADE DE IMPLANTAÇÃO DAS RECOMENDAÇÕES E PROPOSTA DE TRABALHOS FUTUROS

A presente pesquisa sofreu limitações de ordem profissional, na segurança e sigilo das informações e em especial de evento de força maior inesperado de ordem mundial.

As limitações de ordem profissional se deram em razão da resistência das instituições financeiras em fornecer em sua totalidade todas informações necessárias para a devida alimentação da BNFBE mesmo já firmado diversos acordos de cooperação. As instituições financeiras em razão da economia de mercado e concorrência não enxergam como interessante expor suas falhas de segurança preferindo suportar os prejuízos causados por grandes organizações criminosas, ou seja, preferem arcar com os prejuízos causados que correr o risco de perder grandes clientes.

As limitações em decorrência da segurança e sigilo das informações como já informado no discorrer desta pesquisa nas seção 2.2 e 2.2.3 se deram com relação a BNFBE devido aos termos de compromisso de confidencialidade sobre o volume de fraudes bancárias individualizada por instituições financeiras (ANEXO C) e em relação a Operação Valentina em razão de levantamento de dados quantitativos e sigilo em relação aos investigados (ANEXO D).

Quantos as limitações em razão do estado de emergência ocasionado pelo novo coronavírus (Sars-Cov-2) conforme já mostrado no final da subseção 4.2.1 decorreu em razão da impossibilidade da realização dos encontros em grupo focal inicialmente idealizado com aqueles Policiais Federais lotados em Brasília que realizam a coordenação, execução, manutenção e inserção de dados sobre fraudes bancárias eletrônicas na PF, no entanto, as entrevistas em grupo focal realizadas com os Policiais Federais lotados no Ceará teve melhor proveito em razão do envolvimento direto com a deflagração da Operação Valentina.

A viabilidade de implantação das recomendações propostas nos dois encontros de grupo focal decorre de aspectos técnicos, operacionais e financeiros. O Quadro 16 mostra o modo possível e viável de implantação das recomendações.

Quadro 16 - Viabilidade de implantação das recomendações

ASPECTO	VIABILIDADE DE IMPLANTAÇÃO
Técnico	A Polícia Federal possui atualmente uma Diretoria específica de Tecnologia da Informação e Inovação que pode integrar conhecimentos com as áreas de Segurança e Tecnologia da Informação das instituições financeiras que firmaram acordos de cooperação dispor de tecnologias que possam: • Criar ferramentas de inteligências geradoras de informações estratégicas e relatórios de inteligências.; • Criar Canal de comunicação direta da vítima de fraude com a BNFBE com a participação efetiva das instituições financeiras e da PF em tempo real para validar essas informações sobre fraude; • Realizar estudos sobre a viabilidade de criação de uma plataforma web por meio de convênios que possibilite inserção de informações sobre fraudes bancárias diretamente pelas vítimas e validadas pelas instituições financeiras com acesso e integração entre todas forças de segurança pública;
Operacional	O volume e diversidade de fraudes bancárias pela internet aumenta e surge rotineiramente. As instituições financeiras e o Estado precisam concentrar esforços para combater os crimes de fraudes bancárias pela internet, em especial no aumento de efetivo das equipes de Segurança das Instituições Financeiras e de Policiais envolvidos na manutenção da BNFBE;
Financeiro	As instituições Financeiras que sofrem ataques de fraudes bancárias das mais diversas modalidades são interessadas diretas em disponibilizar recursos financeiros para: • Criar Canal de comunicação direta da vítima de fraude com a BNFBE com a participação efetiva das instituições financeiras e da PF em tempo real para validar essas informações sobre fraude; • Realizar estudos sobre a viabilidade de criação de uma plataforma web por meio de convênios que possibilite inserção de informações sobre fraudes bancárias diretamente pelas vítimas e validadas pelas instituições financeiras com acesso e integração entre todas forças de segurança pública; A Polícia Federal juntamente com as instituições financeiras que firmaram acordos de cooperação no combate a fraudes bancárias poderiam propor parcerias com Universidades Públicas para produção de conhecimento e inovação

	tecnológica em uma Hélice Tríplice de promoção de desenvolvimento de modelos atuais de investigação.

Fonte: Elaborado pelo autor (2020).

Para aprofundamento dessa pesquisa como proposta de estudos futuros, sugerimos ainda, o estudo dos dois temas abordados na pesquisa na visão dos donos do problema, em especial dos Membros do Ministério Público, titulares das ações penais e principalmente com os Gerentes de Segurança em fraude bancária das instituições financeiras, para obter suas percepções acerca dos temas abordados, apontar melhorias na produção de relatórios e informações estratégicas eficientes que efetivamente possam combater grandes organizações criminosas especializadas em fraude bancária eletrônica.

REFERÊNCIAS

ALEXANDRIA, J. C. S. **Gestão da segurança da informação**: uma proposta para potencializar a efetividade da segurança da informação em ambiente de pesquisa científica. 2009. (Tese Instituto de Pesquisas Energéticas e Nucleares**)** - Universidade de São Paulo, São Paulo, 2009.

ALMEIDA, M.C.B. **Planejamento de bibliotecas e serviços de informação**. 2. ed. Brasília, DF: Brinquet de Lemos, 2005.

ARAÚJO, C. A. A. A ciência da Informação como ciência social. **Ciência da Informação,** Brasília, v. 32, n. 3, p. 21-27, set./dez. 2003.

ARCOVERDE, Henrique Ferraz. **Malwares brasileiros**: técnicas, alvos e tendências. Recife, 2013. Dissertação (Mestrado) - UFPE, Centro de Informática, Programa de Pós-graduação em Ciência da Computação, 2013. Disponível em: https://repositorio.ufpe.br/handle/123456789/11832. Acesso em: 19 jul. 2021.

ASSOLINI, Fabio. Beaches, carnivals and cybercrime: a look inside the Brazilian underground. **Kaspersky, Lab**, nov. 2015. Disponível em: https://securelist.com/beaches-carnivals-and-cybercrime-a-look-inside-the-brazilian-underground/72652/. Acesso em: 19 jul. 2021.

BAUMAN, Z. **Vigilância líquida**. Rio de Janeiro: Zahar, 2013.

BARBOU, R. **Grupos Focais**. Porto Alegre: Artmed, 2009.

BEKKERS, V. J. J. M.; EDELENBOS, J.; STEIJN, B. Linking innovation to the public sector: Contexts, concepts and challenges. *In*: Innovation in the public sector. Linking capacity and leadership. **Governance and Public Management**, v. 6, p. 3–34, 2011. Houndsmills: Plagrave McMillan.

BELLINI, Carlo Gabriel Porto; RECH, Ionara; BORENSTEIN, Denis. Soft Systems Methodology: uma aplicação no "pão dos pobres" de Porto Alegre. **RAE Eletrônica**, v. 3, 2004.

BORKO, H. Information Science: What is it? **American Documentation**, v. 19, n. 1, p. 3-5, jan. 1968.

FENAPEF. **Operação Valentina**: Policiais Federais desmontam esquema de fraudes Bancárias. [Brasília], abr. 2017. Disponível em: http://www.fenapef.org.br/operacao-valentina-policiais-federais-desmontam-esquema-de-fraudes-bancarias/. Acesso em: 19 jul. 2021.

BRASIL. Policia Federal (PF). **PF e Febraban renovam acordo de cooperação técnica**. Brasília, fev., 2018. Disponível em: http://www.pf.gov.br/agencia/noticias/2018/02/pf-e-febraban-renovam-acordo-de-cooperacao-tecnica. Acesso em: setembro de 2018.

BRASIL. MINISTÉRIO PÚBLICO FEDERAL. **Ata da 475ª Sessão**. 2ª Câmara de Coordenação e Revisão em Matéria Criminal e Controle Externo da Atividade Policial.

Brasília, 2009. Disponível em: http://www.mpf.mp.br/atuacao-tematica/ccr2/coordenacao/comissoes-e-grupos-de-trabalho/grupos-de-trabalho-com-atividades-encerradas-ou-transferidas/projeto tentaculos/temporario/ata_475_2009.pdf/at_download/file. Acesso em: 11 set. 2018.

BRASIL. **Pesquisa Nacional por Amostra de Domicílios Contínua PNAD Contínua**. Brasília, 2016. Disponível em https://agenciadenoticias.ibge.gov.br/media/com_mediaibge/arquivos/49bcf11e47179d434bda979434770b0b.pdf. Acesso em: nov. 2018.

BRESCIANI FILHO, E. Métodos de estudo de sistema: sistemografia. **Revista Eletrônica de Informática**, Campinas, v. 1, n. 1, 2001. Disponível em: http://www.puccampinas.edu.br/centros/ceatec/revista_eletronica/primeira_edicao.html. Acesso em: 28 dez. 2014.

BROWN, C. S. Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice. **International Journal of Cyber Criminology,** v. 9, n. 1, p. 55-73, 2015.

BUCKLAND, M. K. Information as thing. **Journal of the American Society for Information Science**, v. 45, n. 5, p. 351-360, 1991.

BORGES, Messias. Quadrilha que furtou R$ 7,5 milhões é condenada a 85 anos. **Diário do Nordeste**, [Ceará], 20 jul. 2018. Segurança, p. 1. Disponível em: https://diariodonordeste.verdesmares.com.br/seguranca/quadrilha-que-furtou-r-7-5-milhoes-e-condenada-a-85-anos-1.1972628. Acesso em: 17 set. 2021.

BOELL, Sebastian K.; CECEZ-KECMANOVIC, Dubravka. A hermeneutic approach for conducting literature reviews and literature searches. **Communications of the Association for information Systems**, v. 34, n. 1, p. 12, 2014.

CAPURRO, R.; HJÖRLAND, B. O conceito de informação. **Perspectivas em Ciências da Informação**, v. 12, n. 1, p. 148-207, 2007.

CARDOSO, Ana Maria Pereira. Pós-Modernidade e informação: conceitos complementares? **Perspectivas em Ciência da Informação**, Belo Horizonte, v. 1, n. 1, p. 63-79, jan./jul. 1996.

CARMINATI, M. *et al*. **Banksealer**: A decision support system for online banking fraud analysis and investigation, Computers & Security, 2015.

CHECKLAND, P. Systems thinking, systems practice. **Chichester**: John Wiley & Sons, 1981.

CHECKLAND, P. Achieving 'desirable and feasible' change: an application of soft systems methodology. **Journal of the Operational Research Society**, v. 36, n. 9. p. 821-831, 1985.

CHECKLAND P. Soft Systems Methodology: A Thirty Year Retrospective. **Systems Research and Behavioral Science** 17:s11–s58, 2000.

CHOO, C. W. **A organização do conhecimento**: como as organizações usam a informação para criar significado, construir conhecimento e tomar decisões. São Paulo: SENAC, 2006.

DAMIANO, A. L. As Fraudes no Internet Banking e sua evolução para o Social Banking. **Dissertação (Mestrado em Engenharia de Produção)** Escola de Engenharia de São Carlos - Universidade de São Paulo, São Paulo, 2013. Disponível em: http://www.teses.usp.br/teses/disponiveis/18/18157/tde-12092013 094137/publico/AndreDamianoDEFINITIVO.pdf. Acesso em: 19 jul. 2021.

DAVENPORT, T. H.; PRUSAK, L. **Conhecimento empresarial: como as organizações gerenciam o seu capital intelectual**. Rio de Janeiro: Campus, 1998.

FEBRABAN, Federação Brasileira de Bancos. **Pesquisa FEBRABAN de Teconologia Bancária**. Brasília, 2019. Disponível em: https://cmsportal.febraban.org.br/Arquivos/documentos/PDF/Apresenta%C3%A7%C3%A3o%20Febraban%202019_Pesquisa%20de%20Tecnologia%20Banc%C3%A1ria.pdf. Acesso em: 16 jul. 2021.

FERRO JÚNIOR, Celso Moreira. **A inteligência e a gestão da informação policial**: conceitos, técnicas e tecnologias definidos pela experiência profissional e acadêmica. Fortium, 2008.

FERNANDES, F.C. Inteligência ou informações? **Revista Brasileira de Inteligência**. Brasília: Abin, v. 2, n. 3, set. 2006.

FLEISHER, C. S.; BENSOUSSAN, B. **Business and competitive analysis**: effective application of new and classic methods. New Jersey: Pearson Education, 2007.

GREENBAUM, T.L. **The handbook for focus group research**. 2. Ed. Thousand Oaks: Sage, 1998.

GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social**. 5. Ed. São Paulo: Atlas, 1999.

GKOUTZINIS, A. A. **Internet banking and the law in Europe**. Cambridge: University Press, 2006.

GOMES, M. E. S. BARBOSA, E. F. A Técnica de Grupos Focais para Obtenção de Dados Qualitativos. **Instituto de Pesquisas e Inovações Educacionais,** 1–7 p. (1999).

GUIJARRO, Elva Gioconda Lara; SILVA, Luis Camilo Albán. Los riesgos de las transacciones bancarias por Internet. Revista Publicando, v. 4, n. 10 (1), p. 62-74, 3 may 2017.

HAJLI, N.; SHANMUGAM, M.; WANG,Y.; BUGSHAN, H. Understanding customer perceptions of internet banking: the case of the UK. **Journal of Enterprise Information Management**, v. 28, n. 5, p. 622–636, 2015.

HARTMANN-WENDELS, T.; MÄHLMANN, T.; VERSEN, T. Determinants of banks' risk exposure to new account fraud – Evidence from Germany. **Journal of Banking & Finance**, v. 33, n. 2, p. 347–357, 2009.

HUGHES, D.; DUMONT, K. Using focus groups to facilitate culturally anchored research. **American Journal of Community Psychology**, v. 21, n. 6, p. 775-806, 1993.

HUNTON, P. The stages of cybercrime investigations: Bridging the gap between technology examination and law enforcement investigation. **Computer Law & Security Review,** v. 27, p. 61-67, 2011.

IAROZINSKI NETO, A.; LEITE, M. S. A abordagem sistêmica na pesquisa em engenharia de produção. **Produção**, São Paulo, v. 20, n. 1, mar. 2010.

ISMAIL, R.; ZAINAB, A. N. Assessing the status of library information systems security. **Journal of Librarianship Science**, v. 45, n. 232, 2013. Disponível em http://lis.sagepub.com/content/45/3/232.abstract_ Acesso em: 13 dez. 2020.

JANSEN, J.; VAN SCHAIK, P. Testing a model of precautionary online behaviour: The case of online banking. **Computers in Human Behavior**, v. 87, p. 371–383, 2018.

KILJAN, S.; SIMOENS, K.; COCK, D. D.; EEKELEN, M. V.; VRANKEN, H. A Survey of Authentication and Communications Security in Online Banking. **ACM Computing Surveys**, v. 49, n. 4, p. 1–35, 2016.

KINTSCHNER, Fernando; BRESCIANI FILHO, E Ettore. Método de Mapeamento e Reorganização de Processos: sistemografia. **Revista Produção Online**, Florianopolis, v. 5, n. 1, jun. 2005. Disponível em: https://producaoonline.org.br/rpo/article/view/325/422. Acesso em: 19 jul. 2021.

KOVACH, Stephan. **Detecção de fraudes em transações financeiras via Internet em tempo real**. 2011. Tese (Doutorado em Sistemas Digitais) - Escola Politécnica, Universidade de São Paulo, São Paulo, 2011. Acesso em: 19 jul. 2021.

KLETTENBERG, Josiane. **Segurança da Informação**: um estudo sobre o uso da engenharia social para obter informações sigilosas de usuários de Instituições Bancárias. Dissertação (Mestrado em Ciência da Informação) - Universidade Federal de Santa Catarina, Centro de Ciências da Educação. Programa de Pós-Graduação em Ciência da Informação. Florianópolis, SC, 2016.

LANDRY, M. A note on the concept of problem. **Organization Studies**, Berlin, n. 16, p. 315-343, 1995.

LAU, Marcelo. **Análise das fraudes aplicadas sobre o ambiente Internet Banking**. 2006. Dissertação (Mestrado em Sistemas Eletrônicos) - Escola Politécnica, Universidade de São Paulo, São Paulo, 2006. Acesso em: 19 jul. 2021.

LE MOIGNE, J. L. **La modèlisation des systemes complexes**. Afcet systemes. Paris: Dunod, 1990.

LE MOIGNE, J. L.. **La théorie du système général, théorie dela modélisation**. Paris, 1977.

LÉVY, P. **A inteligência coletiva**: por uma antropologia do ciberespaço. São Paulo: Loyola, 2007.

LYON, D. **Liquid Surveillance**: the contribution of zygmunt bauman to surveillance studies. Cambridge: International Political Sociology, 2010.

LIN, Hsiu-Fen. An empirical investigation of mobile banking adoption: the effect of innovation attributes and knowledge-based trust. **International Journal of Informaion Management**, v. 31, n. 3, 252-260. 2011. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S026840121000099X. Acesso em: 16 jul. 2021.

MALLAT, N. Exploring consumer adoption of mobile payments: a qualitative study. **The Journal of Strategic Information Systems**, v.16, n. 4, p. 413–432, 2007.

MARCIAL, E. **O perfil do profissional de Inteligência competitiva**. *In*: Gestão estratégica da informação e inteligência competitiva. São Paulo: Saraiva, p. 242-254, 2005.

MICHEL, Maria Helena. **Metodologia e pesquisa científica em Ciências Sociais**: um guia prático para acompanhamento da disciplina e elaboração de trabalhos monográficos. São Paulo: Atlas, 2005.

MINAYO, Maria Cecilia de S.; SANCHES, Odécio. Quantitativo-qualitativo: oposição ou complementaridade? **Caderno de Saúde Pública**, Rio de Janeiro, v. 9, n. 3, p. 239-262, 1993.

MINAYO, Maria Cecilia de S. O desafio do conhecimento: pesquisa qualitativa em saúde. 9. ed. **Revista e aprimorada**. São Paulo: HUCITEC, 2006.

MINGERS, John; ROSENHEAD, Jonathan. Problem structuring methods in action. European journal of operational research, v. 152, n. 3, p. 530-554, 2004.

MORAES, R. Uma tempestade de luz: a compreensão possibilitada pela análise textual discursiva. **Ciência & Educação**, v. 9, n. 2, p. 191-211, 2003.

MOMPEAN, Adriana. Transações com mobile banking crescem 138% em um ano. **Ciab FEBRABAN**, São Paulo, v. 63, p. 17, 2016.

OLIVEIRA, Alysson André Régis de; LEITE FILHO, Carlos Alberto Pereira; RODRIGUES, Cláudia Medianeira Cruz. O Processo de Construção dos Grupos Focais na Pesquisa Qualitativa e suas Exigências Metodológicas. **XXXI Encontro da ANPAD1**, Rio de Janeiro, 22 a 25 set. 2007.

ORLANDI, E. R. **Análise de discurso**: princípios e procedimentos: Campinas, SP: Pontes, 2002.

ORLANDI, E. R. **Interpretação**: autoria, leitura e efeitos do trabalho simbólico. 4. Ed. Campinas, SP: Pontes, 2004.

PARODI, L. **Manual das fraudes**. Editora Brasport. 2005.

PATROCINIO, Álex Moreira do. **Técnicas Baseadas em Grafos para Priorização de Investigações Policias de Fraudes Bancárias Eletrônicas**. 2016. Dissertação (Mestrado

Engenharia Elétrica) - Universidade de Brasília, Faculdade de Tecnologia, Departamento de Engenharia Elétrica, 2016.

PLATT, W. **Produção de Informações estratégicas**. Rio de Janeiro: Biblioteca do Exército: Livraria Agir Editora, 1974.

RIBEIRO, José Luís Duarte; MILAN, Gabriel Sperandio. **Entrevistas Individuais**: teoria e aplicações. Porto Alegre: FEENG/UFRGS, 2004.

ROBREDO, J. "Ciência da informação e filosofia: reflexões". *In*: **Anais do VII ENANCIB**, Salvador, p. 28-31 out. 2007.

SAMPAIO, Rosana Ferreira; MANCINI, Marisa Cotta. Estudos de revisão sistemática: um guia para síntese criteriosa da evidência científica. **Brazilian Journal of Physical Therapy**, v. 11, p. 83-89, 2007.

SANTOS JR, Aldo Antonio; SANTOS, Aldo Antonio Hostins; SILVA, Adriano Ferreira Alves. A Ciência policial no Brasil. **Revista Eletrônica Direito e Política, Programa de Pós-Graduação Stricto Sensu em Ciência Jurídica da UNIVALI**, Itajaí, v. 8, n. 1, 1 quadrimestre de 2013. Disponível em: www.univali.br/direitoepolitica. Acesso em: 19 jul. 2021.

SANTOS, Izequias Estevam dos. **Manual de métodos e técnicas de pesquisa científica**. 9. ed. Niterói: Impetus, 2012.

SARACEVIC, Tefko. Ciência da Informação: origem, evolução e relações. **Perspectivas em Ciência da Informação,** v. 1, n. 1, p. 41-62, jan./jun. 1996.

SERAPIONI, Mauro. Métodos qualitativos e quantitativos na pesquisa social em saúde: algumas estratégias para a integração. **Ciênc. Saúde Coletiva,** Rio de Janeiro, v. 5, n. 1, p. 187-192, 2000.

SCHODERBEK, S. **Management System**: Conceptual Considerations. BPI IRWIN, 1990, p. 5-32.

SIANES, M. Compartilhar ou proteger conhecimentos? **Gestão estratégica da informação e inteligência competitiva**. São Paulo: Saraiva, 2005.

SIMON, J.S. **How to conduct focus group**. Nonprofit Word, Madison, v. 17, n. 5, 1999.

SIQUEIRA, E. P. **O Projeto Tentáculos da Polícia Federal: da concepção a proposta de modelo aplicável na segurança pública brasileira**. Monografia. **(**Especialização em Gestão da Segurança da Informação e Comunicações) — Universidade de Brasília, 2014.

THORNBURGH, T. Social engineering: the "Dark Art". *In*: Annual conference on information security curriculum development, Kennesaw, 2004. **Proceedings…** Kennesaw: ACM. p. 133-135, 2004.

TRAD, Leny Bomfim. Grupos focais: conceitos, procedimentos e reflexões baseadas em experiências com o uso da técnica em pesquisas de saúde. **Physis**, Rio de Janeiro, v. 19, n. 3, p. 777-796, mar., 2009.

TOUTINHO FILHO, F. C. **Prática de Processo Penal**. 13 ed. São Paulo: Saraiva, 2008.

VAN GOOL, L. M. W. Improving external control of online web based banking fraud in the Netherlands. Thesis (MsC.) – **Erasmus School of Economics**, 2011. Disponível em: https://thesis.eur.nl/pub/10421/MA007%20IENE-Gool_283517.pdf. Acesso em: 17 jan. 2019.

VALENTIM, Marta Ligia Pomim. Gestão da informação e gestão do conhecimento: especificidades e convergências. Londrina: **Infohome**, 2004. Disponível em: http://www.ofaj.com.br/colunas_conteudo.php?cod=88. Acesso em: 12 dez. 2020.

VIANNA, W. B.; ENSSLIN, L. O design na pesquisa quali-quantitativa em engenharia de produção: questões epistemológicas. **Revista Produção On-line**. Florianópolis, v. 8, n. 1, mar. 2008.

WERSIG, G. Information science: the study of postmodern knowledge usage. **Information Processing & Management**, v. 29, n. 2, p. 229-239, mar., 1993.

WONGTSCHOWSKI, Arthur. **Segurança em aplicações transacionais na internet**: o elo mais fraco. 2005. Dissertação (Mestrado em Sistemas Digitais) - Escola Politécnica, Universidade de São Paulo, São Paulo, 2006.

YU, Chian-Son. Consumer Switching Behavior from Online Banking to Mobile Banking. **International Journal of Cyber Society and Education**, v. 7, n. 1, 1-28. ATISR. 2014. Disponível em: http://academic-pub.org/ojs/index.php/IJCSE/article/view/1108. Acesso em: 16 jul. 2021.

APÊNDICE A - ROTEIRO PARA UTILIZAÇÃO DO GRUPO FOCAL AOS POLICIAIS FEDERAIS LOTADOS NO GRCC-CE

Mestrando: Roberto de Paiva Soares Júnior

ORIENTADOR: Prof. Dr. William Barbosa Vianna

Introdução:

Falar sobre o papel do moderador e sobre a pesquisa, informar que cabe ao moderador e autor da pesquisa a condução do grupo adequadamente, facilitando a interação e trocas de experiências acerca do problema debatido mantendo sempre o foco nos objetivos da pesquisa.

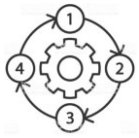
Ressaltar sobre o termo de consentimento livre e esclarecido (TCLE), em especial sobre o anonimato.

Explicar o roteiro a ser aplicado ao grupo focal, técnica de entrevista grupal, baseada em comunicação e interação. Falar do perfil homogêneo (todos especialistas em fraudes bancárias eletrônicas e usuários da BNFBE.

Tema1: Atraso na comunicação e na alimentação das informações dos processos de contestação sobre fraude bancárias eletrônica e incompletude de dados.

Pergunta1: Como melhorar a gestão das informações sobre fraude bancária eletrônica na BNFBE evitando atraso na comunicação e na alimentação das informações dos processos de constestação sobre fraude bancárias eletrônica e incompletude de dados?

1.1 - Qual a sua percepção a respeito do fluxo de informações?



a) Apresentar a imagem do modelo de fluxo de alimentação dos processos de contestação sobre fraude bancária

b) Falar sobre o modelo, fluxo e representações gráficas.

1.2- Você tem sugestões para o fluxo de alimentação dos processos de contestação sobre fraude bancária?

* Cada participante deverá ter a oportunidade de falar.

1.3- O que você pode falar sobre a qualidade da informação que recebemos das instituições financeiras para alimentação da BNFBE?

a) Tempo médio na comunicação dos processos de contestação;

b) Completude dos dados informados;

c) Necessidade de pedidos de informações complementares;

1.4- Quais Benefícios já observados na migração da BNFBE?

*Cada participante deverá ter a oportunidade de falar

Tema 2: Quais informações importantes que a vítima de fraude bancária eletrônica detém que podem ser relevantes para as investigações sobre fraude bancária

Pergunta2: De que forma poderia ocorrer com maior efetividade a participação da vítima de fraude bancária eletrônica?

2.1- Você pode sugerir melhorias e inovações, em espacial sobre a viabilidade de participação da vítima de fraude bancária na comunicação dos processos de contestação de fraudes bancárias?

* Cada participante deverá ter a oportunidade de falar

FINAL:

Agradecimentos a todos que participaram. Saibam que o ponto de vista de cada um de vocês é muito valioso para a pesquisa. Obrigado pelo tempo, participação e percepções. Caso queira receber uma cópia deste estudo assim que finalizado, favor me informar que será encaminhado via email.

APÊNDICE B - INSTRUMENTO DE COLETA DE DADOS - MODELO DE FICHA DE QUALIFICAÇÃO DO PERFIL DOS PARTICIPANTES E TRANSCRIÇÃO DAS OPINIÕES E PERCEPÇÕES DOS ENTREVISTADOS

Entrevista em grupo focal:

Data: ___/____/2020 Início: _____ Término: _____

1 PERFIL DO ENTREVISTADO: PARTICIPANTE ___

1.1. Tempo de Polícia Federal _____

1.2 Tempo de trabalho com fraude bancária eletrônica:_____

1.3 Quantas e Quais Operações sobre fraude bancária participou: _____

_____

1.4 Trabalhou na Operação Valentina ( ) Sim ( ) não.

2 QUESTÕES ORIENTADORAS

Tema 1: O atraso na comunicação e na alimentação das informações dos processos de contestação sobre fraude bancárias eletrônica e incompletude de dados, se dá....

Pergunta 1: Como melhorar a gestão das informações sobre fraude bancária eletrônica na BNFBE evitando atraso na comunicação e na alimentação das informações dos processos de constestação sobre fraude bancárias eletrônica e incompletude de dados?

Tema 2: Quais informações importantes que a vítima de fraude bancária eletrônica detém que podem ser relevantes para as investigações sobre fraude bancária

Pergunta 2: De que forma poderia ocorrer com maior efetividade a participação da vítima de fraude bancária eletrônica?

3 TRANSCRIÇÕES DAS OPINIÕES E PERCEPÇÕES DEGRAVADAS DOS REGISTROS AUDIO VISUAL

Tema 1:
Tema 2:

4 TRANSCRIÇÕES DAS PERCEPÇÕES OBSERVADAS PELO APOIO TÉCNICO OBSERVADOR

Tema 1:
Tema 2:

APÊNDICE C - TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO

UNIVERSIDADE FEDERAL DE SANTA CATARINA

CENTRO DE CIÊNCIAS DA EDUCAÇÃO DA UNIVERSIDADE FEDERAL DE SANTA CATARINA – CED/UFSC

PROGRAMA DE PÓS-GRADUAÇÃO EM CIÊNCIA DA INFORMAÇÃO (PGCIN)

Prezado(a) colaborador(a),

Esta pesquisa intitulada, "**Disseminação de Boas Práticas na Comunicação da Informação nos Processos de Contestação de Fraudes Bancárias pela Internet: O Projeto Tentáculos da Polícia Federal como Modelo"** é a proposta do trabalho de mestrado desenvolvido pelo pesquisador Roberto de Paiva Soares Júnior que utilizará como método de pesquisa, Entrevistas por Grupo Focal (método qualitativo), com o objetivo esclarecer e identificar os pontos críticos no fluxo de comunicação dos processos de contestações de fraudes bancárias eletrônicas na PF. Solicitamos a sua colaboração e autorização para apresentar os resultados deste estudo em eventos, bem como publicar em revista/livro científica na área da Ciência da Informação. Por ocasião de publicação dos resultados e em todo o processo restante, seu nome será mantido em sigilo, sendo identificado apenas como participante de grupo focal com a respectiva numeração. Vale mencionar a título de exemplo conforme consta na resolução da Comissão Nacional de Ética em Pesquisa - CONEP, Resolução 466/2012 – CONEP, toda pesquisa oferece risco imprevisível, contudo, informamos que essa pesquisa, não oferece riscos previsíveis. Esclarecemos que sua participação no estudo é voluntária e, portanto, o(a) Senhor(a) não é obrigado(a) a fornecer as informações e/ou colaborar com as atividades solicitadas pelo esquisador. Caso decida não participar do estudo, ou resolver a qualquer momento desistir do mesmo, não sofrerá nenhum dano. O pesquisador estará à sua disposição para qualquer esclarecimento que considere necessário em qualquer etapa da pesquisa, assim como o Comitê de Ética de Pesquisa do PGCIN. Contatos do pesquisador: roberto junior2706@gmail.com, (85) 9 8698-2001 / (85) 3392-4966 – Rua Manuel Teixeira de Melo, 788, casa 28, Bairro José de Alencar, Fortaleza/CE. Endereço do Programa de Pós-Graduação em Ciência da Informação (PGCIN) - Centro Ciências da Educação - Bloco B sala 105

Universidade Federal de Santa Catarina - UFSC - Campus Professor João David Ferreira Lima - Trindade - Florianópolis - Santa Catarina - Brasil - CEP 88.040-900 - e-mail: ppgcin@contato.ufsc.br - Fone secretaria: (48)3721-2234 - Fone coordenação: (48) 37212233.

Desde já, agradecemos sua colaboração.

Diante do exposto, declaro que fui devidamente esclarecido(a) e dou o meu consentimento para participar da pesquisa e publicação dos resultados.

_____

Assinatura do(a) Pesquisado(a)

_____

Assinatura do Pesquisador

Obs.: O sujeito da pesquisa ou seu representante e o pesquisador responsável deverão rubricar todas as folhas do TCLE apondo suas assinaturas na última página do referido Termo.

ANEXO A - PEDIDO DE AUTORIZAÇÃO DE ACESSO A À BASE NACIONAL DE FRAUDES BANCÁRIAS ELETRÔNICAS – BNFBE PARA COLETA DE DADOS ACERCA DO QUANTITATIVO DE PROCESSOS DE CONTESTAÇÕES INSERIDOS NA BNFBE

MINISTÉRIO DA JUSTIÇA
POLÍCIA FEDERAL
SUPERINTENDÊNCIA REGIONAL NO CEARÁ
DELEGACIA REGIONAL DE COMBATE AO CRIME ORGANIZADO

INFORMAÇÃO – Nº 1108-1206/2020 – SR/PF/CE

Fortaleza, 12 de junho de 2020.

Senhora Chefe do Serviço de Repreensão à Crimes Cibernéticos – SRCC/CGPFAZ/DICOR/PF,
CASSIANA SAAD DE CARVALHO
Delegada de Polícia Federal

Senhora Chefe,

1- Este signatário, aluno do Mestrado Acadêmico em Ciência da Informação da Universidade Federal de Santa Catarina - UFSC, originário de acordo pormenorizado no Plano de trabalho (doc. SEI 5420504) do Termo de Cooperação firmado entre a Polícia Federal - PF e UFSC, com objetivo, em especial, para de fomentar pesquisas que envolvam a produção, difusão e gestão do conhecimento e da informação para tomada de decisões estratégicas e resolução de problemas que envolvam a segurança pública e o manejo de recursos policiais na coleta e gestão e apresentação da informação.

2- A proposta do mestrado em geral, visa abordar a origem, a coleção, armazenamento, recuperação, interpretação, transmissão, transformação e utilização da informação, inclusive pesquisas sobre a representação da informação em sistemas, objetivando a transmissão eficiente da mensagem.

3- Feito a contextualização, foram propostos pelos alunos trabalhos interdisciplinares entre a Ciência da Informação e a Ciência Policial e submetidos à banca para avaliação quanto à qualificação. Este signatário tem seu trabalho de dissertação em andamento, já qualificado pela banca desde 27 de maio de 2019, conforme abaixo documento em anexo.

4- Atualmente, a dissertação em andamento " DISSEMINAÇÃO DE BOAS PRÁTICAS NA COMUNICAÇÃO DOS PROCESSOS DE CONTESTAÇÃO DE FRAUDES BANCÁRIAS PELA INTERNET PARA SEGURANÇA PÚBLICA" está em fase de coleta de dados e levantamentos para posterior análise e conclusões.

MINISTÉRIO DA JUSTIÇA
POLÍCIA FEDERAL
SUPERINTENDÊNCIA REGIONAL NO CEARÁ
DELEGACIA REGIONAL DE COMBATE AO CRIME ORGANIZADO

5. Considerando a importância do evento e da ação de capacitação fomentada pela PF, solicito a autorização e acesso à Base Nacional de Fraudes Bancárias Eletrônicas – BNFBE para coleta de dados acerca do quantitativo de processos de contestações inseridos na BNFBE. Para delimitação do período de análise documental, será observado os últimos 5 anos. **A autorização será para levantamento de dados apenas quantitativos, não passíveis de qualquer identificação de investigados**, servindo para mensurar o volume de informações sobre fraudes bancárias inseridas na BNFBE. Também poderão ser úteis dados quantitativos sobre fraudes bancárias por instituição financeira se assim for pertinente durante o transcorrer da pesquisa.

6. Conforme demonstrado no parágrafo inicial, a demanda é no sentido de demonstrar a relevância da aplicação do conhecimento acadêmico em caso concreto de gestão da informação pela PF.

É a informação.

ROBERTO DE PAIVA SOARES JUNIOR
Escrivão de Polícia Federal
Matrícula 18.356

ANEXO B - PEDIDO DE AUTORIZAÇÃO DE ACESSO PARA COLETA DE DADOS ACERCA DO QUANTITATIVO DE FRAUDES LEVANTADAS NO DECORRER DA INVESTIGAÇÃO DA OPERAÇÃO VALENTINA

MINISTÉRIO DA JUSTIÇA
POLÍCIA FEDERAL
SUPERINTENDÊNCIA REGIONAL NO CEARÁ
DELEGACIA REGIONAL DE COMBATE AO CRIME ORGANIZADO

INFORMAÇÃO – Nº 1109-1206/2020 – SR/PF/CE

Fortaleza, 12 de junho de 2020.

A Sua Excelência o Senhor
Francisco Luís Rios Alves
Juiz Federal Titular da 32ª Vara Federal – Seção Judiciária do Ceará
Rua João Carvalho, nº 485 - Aldeota
CEP: 60140-140
Fortaleza - CE
E-mail: dirvara32@jfce.jus.br

Senhor Juiz,

1- Este signatário, aluno do Mestrado Acadêmico em Ciência da Informação da Universidade Federal de Santa Catarina - UFSC, originário de acordo pormenorizado no Plano de trabalho do Termo de Cooperação firmado entre a Polícia Federal - PF e UFSC, com objetivo, em especial, para de fomentar pesquisas que envolvam a produção, difusão e gestão do conhecimento e da informação para tomada de decisões estratégicas e resolução de problemas que envolvam a segurança pública e o manejo de recursos policiais na coleta e gestão e apresentação da informação.

2- A proposta do mestrado em geral, visa abordar a origem, a coleção, armazenamento, recuperação, interpretação, transmissão, transformação e utilização da informação, inclusive pesquisas sobre a representação da informação em sistemas, objetivando a transmissão eficiente da mensagem.

3- Feito a contextualização, foram propostos pelos alunos trabalhos interdisciplinares entre a Ciência da Informação e a Ciência Policial e submetidos à banca para avaliação quanto à qualificação. Este signatário tem seu trabalho de dissertação em andamento, já qualificado pela banca desde 27 de maio de 2019, conforme abaixo documento em anexo.

4- Atualmente, a dissertação em andamento " DISSEMINAÇÃO DE BOAS PRÁTICAS NA COMUNICAÇÃO DOS PROCESSOS DE CONTESTAÇÃO DE FRAUDES BANCÁRIAS PELA INTERNET PARA SEGURANÇA PÚBLICA" está em fase de coleta de dados e levantamentos para posterior análise e conclusões.

5- Este signatário foi um dos Policiais Federais responsável pela confecção dos Autos Circunstanciados e do Relatório Final de análise de alvos nos Autos do Inquérito Policial nº 737/2016-SR/PF/CE – Processo 0003395-12.2016.4.05.8100 - 32ª VARA FEDERAL ├ SEÇÃO JUDICIÁRIA DO ESTADO DO CEARÁ que resultou na deflagração da denominada Operação Valentina.

6- Considerando a importância do evento e da ação de capacitação fomentada pela PF, solicito a autorização e acesso para coleta de dados acerca do quantitativo de fraudes levantadas no decorrer da investigação, bem como aquelas que deram início ao inquérito. Para delimitação do período de análise documental, será observado o período apenas da fase em sede inquérito policial até a deflagração da operação. **A autorização será para levantamento de dados apenas quantitativos, não passíveis de qualquer identificação de investigados**, servindo para mensurar o volume de informações sobre fraudes bancárias ocorrida durante a investigação.

6. Conforme demonstrado no parágrafo inicial, a demanda é no sentido de demonstrar a relevância da aplicação do conhecimento acadêmico em caso concreto de gestão da informação pela PF.

É a informação.

ROBERTO DE PAIVA SOARES JUNIOR
Escrivão de Polícia Federal
Matrícula 18.356
DELEFAZ/DRCOR/SR/PF/CE
Fones: (85) 98698-2001 / (85) 3621-4961

ANEXO C - AUTORIZAÇÃO DE ACESSO A À BASE NACIONAL DE FRAUDES BANCÁRIAS ELETRÔNICAS – BNFBE PARA COLETA DE DADOS ACERCA DO QUANTITATIVO DE PROCESSOS DE CONTESTAÇÕES INSERIDOS NA BNFBE

SERVIÇO PÚBLICO FEDERAL
MJSP - POLÍCIA FEDERAL
DIVISÃO DE REPRESSÃO A CRIMES CIBERNÉTICOS - DRCC/CGPFAZ/DICOR/PF

Assunto: **mestrado - pesquisa - solicita autorização e acesso à Base Nacional de Fraudes Bancárias Eletrônicas – BNFBE para coleta de dados acerca do quantitativo de processos de contestações inseridos na BNFBE.**

Destino: **EPF ROBERTO DE PAIVA SOARES JUNIOR - DELEFAZ/CE e GPA/DRCC**

Processo: **08270.005378/2020-83**

Interessado: **EPF ROBERTO DE PAIVA SOARES JUNIOR**

1. Ciente.

2. Ao EPF ROBERTO para ciência formal, em especial das observações quanto ao sigilo dos dados, e tratativas diretamente com o GPA/DRCC.

CASSIANA SAAD DE CARVALHO
Delegada de Polícia Federal
Chefe da DRCC/CGPFAZ/DICOR/PF

Documento assinado eletronicamente por **CASSIANA SAAD DE CARVALHO, Chefe de Serviço**, em 25/06/2020, às 09:42, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

SERVIÇO PÚBLICO FEDERAL
MJSP - POLÍCIA FEDERAL
DELEGACIA DE REPRESSÃO A CRIMES FAZENDÁRIOS - DELEFAZ/DRCOR/SR/PF/CE

CERTIFICO ciência do teor dos Despachos SEI 15140222 e 15143267, em especial das observações quanto ao sigilo dos dados, e que as tratativas serão realizadas diretamente com o GPA/DRCC inclusive com encontros em grupo focal coordenados e sob a supervisão do Chefe do GPA. O referido é verdade.

Documento assinado eletronicamente por **ROBERTO DE PAIVA SOARES JUNIOR, Escrivão(ã) de Polícia Federal**, em 25/06/2020, às 10:27, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.dpf.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **15144505** e o código CRC **9DE04D51**.

ANEXO D - AUTORIZAÇÃO DE ACESSO PARA COLETA DE DADOS ACERCA DO QUANTITATIVO DE FRAUDES LEVANTADAS NO DECORRER DA INVESTIGAÇÃO DA OPERAÇÃO VALENTINA

5- Este signatário foi um dos Policiais Federais responsável pela confecção dos Autos Circunstanciados e do Relatório Final de análise de alvos nos Autos do Inquérito Policial nº 737/2016-SR/PF/CE - Processo 0003395-12.2016.4.05.8100 - 32ª VARA FEDERAL - SEÇÃO JUDICIÁRIA DO ESTADO DO CEARÁ que resultou na deflagração da denominada Operação Valentina.

6- Considerando a importância do evento e da ação de capacitação fomentada pela PF, solicito a autorização e acesso para coleta de dados acerca do quantitativo de fraudes levantadas no decorrer da investigação, bem como aquelas que deram início ao inquérito. Para delimitação do período de análise documental, será observado o período apenas da fase em sede inquérito policial até a deflagração da operação. ***A autorização será para levantamento de dados apenas quantitativos, não passíveis de qualquer identificação de investigados*** *, servindo para mensurar o volume de informações sobre fraudes bancárias ocorrida durante a investigação.*

6. Conforme demonstrado no parágrafo inicial, a demanda é no sentido de demonstrar a relevância da aplicação do conhecimento acadêmico em caso concreto de gestão da informação pela PF.

Destinando-se, pois, o acesso aos autos à coleta apenas de dados quantitativos de fraudes, para fins exclusivamente acadêmicos, sem que isso implique em divulgação de informações sigilosas dos investigados e/ou de terceiros, que sequer serão identificados nos estudos, tenho como possível excepcionar o sigilo processual, desde que o pesquisador firme Compromisso, consignando os termos da utilização dos dados.

Registre-se, por oportuno, que não houve oposição nem do órgão ministerial nem da defesa dos acusados, pelo que se presume que não vislumbraram possibilidade de ofensa à intimidade.

Pelo exposto, autorizo o pretendido acesso aos autos ao requerente, para fins restritos de levantamento de dados apenas quantitativos de fraudes, sem identificação de investigados ou terceiros, destinado a trabalho acadêmico de mestrado na UFSC.

Comunique-se ao requerente, por telefone (números indicados no expediente dirigido a este juízo) ou por Ofício ao Departamento da Polícia Federal, dirigido ao escrivão de Polícia Federal ROBERTO DE

PAIVA SOARES JUNIOR, para que tome ciência desta decisão e firme um TERMO DE COMPROMISSO, consignando os termos da utilização dos dados, dando início, em seguida, aos seus trabalhos de pesquisa. Junto ao ofício, anexe cópia desta decisão.

Expedientes necessários.

SERVIÇO PÚBLICO FEDERAL
MJSP - POLÍCIA FEDERAL
DELEGACIA REGIONAL DE INVESTIGAÇÃO E COMBATE AO CRIME ORGANIZADO - DRCOR/SR/PF/CE

TERMO DE COMPROMISSO

Eu, ROBERTO DE PAIVA SOARES JÚNIOR, brasileiro, Escrivão de Polícia Federal, matrícula nº 18.356, inscrito no CPF sob o nº 768.669.473-91, RG nº 94017025360, lotado na Superintendência Regional de Polícia Federal no Ceará, localizada à Avenida Borges de Melo, 820, Bairro de Fátima, Fortaleza/CE, CEP 60.415-430, fone (85) 3392.4800, residente e domiciliado nesta capital, podendo ser contatado pelo telefone número (85) 9.8698-2001, aluno do Mestrado Acadêmico em Ciência da Informação da Universidade Federal de Santa Catarina - UFSC, originário de acordo pormenorizado no Plano de trabalho do Termo de Cooperação firmado entre a Polícia Federal - PF e UFSC, **pelo presente termo de compromisso e responsabilidade me comprometo** a cumprir integralmente os termos da Decisão proferida nos autos do Processo nº 0003395-12.2016.4.05.8100, expedido pelo Excelentíssimo Senhor FRANCISCO LUIS RIOS ALVES, Titular da 32ª VF/CE, Seção Judiciária de Fortaleza/CE, **em especial realizar de forma restrita o levantamento de dados apenas quantitativos de fraudes bancárias levantadaS no decorrer da investigação até a deflagração da operação valentina, sem identificação de investigados ou terceiros, destinados a subsidiar a pesquisa do trabalho acadêmico de mestrado na UFSC.** Firmo o presente termo.

Fortaleza/CE, 13 de agosto de 2020.

(assinado eletronicamente)
ROBERTO DE PAIVA SOARES JÚNIOR
CPF 768.669.473-91

Documento assinado eletronicamente por **ROBERTO DE PAIVA SOARES JUNIOR, Escrivão(ã) de Polícia Federal**, em 13/08/2020, às 07:23, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.dpf.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **15685534** e o código CRC **EEF6F26F**.

ANEXO E - PEDIDO DE INFORMAÇÃO QUANTO AO QUANTITATIVO DE POLICIAIS FEDERAIS LOTADOS NOS RESPECTIVOS GRCCS E SEUS RESPECTIVOS CARGOS NO BRASIL.

SERVIÇO PÚBLICO FEDERAL
MJSP - POLÍCIA FEDERAL
DELEGACIA DE REPRESSÃO A CRIMES FAZENDÁRIOS - DELEFAZ/DRCOR/SR/PF/CE

Informação nº 16950888/2020-DELEFAZ/DRCOR/SR/PF/CE

Aos Senhores Coordenadores dos GRCCs-PF e Chefes de DELEFAZ-PF

Senhor Coordenadores e Chefes de DELEFAZ-PF,

Este signatário, aluno do Mestrado Acadêmico em Ciência da Informação da Universidade Federal de Santa Catarina - UFSC, originário de acordo pormenorizado no Plano de trabalho do Termo de Cooperação firmado entre a Polícia Federal - PF e UFSC, com objetivo, em especial, para de fomentar pesquisas que envolvam a produção, difusão e gestão do conhecimento e da informação para tomada de decisões estratégicas e resolução de problemas que envolvam a segurança pública e o manejo de recursos policiais na coleta e gestão e apresentação da informação.

Atualmente, a dissertação em andamento " DISSEMINAÇÃO DE BOAS PRÁTICAS NA COMUNICAÇÃO DOS PROCESSOS DE CONTESTAÇÃO DE FRAUDES BANCÁRIAS PELA INTERNET PARA SEGURANÇA PÚBLICA" está em fase de análise dos dados coletados e demonstração dos resultados para posterior conclusão.

Considerando a importância do evento e da ação de capacitação fomentada pela PF, solicito:

Aos Senhores Coordenadores de GRCCs nas unidades da PF que dispõem de Grupos de Repreensão à Crimes Cibernéticos formado **informar o quantitativo de Policiais Federais lotados nos respectivos GRCCs e seus respectivos cargos.**

Aos Senhores Chefes de DELEFAZ na unidades PF que não dispõem de GRCC estruturado **informar o quantitativo de Policiais Federais lotados nas respectivas DELEFAZ que atuam com fraude bancária.**

Conforme demonstrado no parágrafo inicial, a demanda é no sentido de demonstrar a relevância da aplicação do conhecimento acadêmico em caso concreto de gestão da informação pela PF.

ROBERTO DE PAIVA SOARES JUNIOR
Escrivão de Polícia Federal
1ª Classe - Matrícula 18.356
DELEFAZ/DRCOR/SR/PF/CE