ENCCLA 2025

Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro

AÇÃO 01/2025

PRODUTO I

DIAGNÓSTICO DETALHADO SOBRE OS GOLPES VIA FALSA CENTRAL E CONDUTAS CONEXAS.

PRODUTO I

DIAGNÓSTICO DETALHADO SOBRE OS GOLPES VIA FALSA CENTRAL E CONDUTAS CONEXAS

EIXO I - SISTEMA FINANCEIRO E FRAUDES ELETRÔNICAS

Ação 01/2025: Mapear e definir mecanismos de prevenção e combate a fraudes bancárias eletrônicas por meio de falsas centrais de atendimento.

Coordenadores: FEBRABAN, PF

Colaboradores: AGU, AJUFE, BB, BCB, CAIXA, CGU, CNMP, CVM, DRCI, MPGO, MPPB, MPPE, MPPR, MPRJ, MPS, MPSE, PCDF, PCMA, PCRJ, PCRS, PCSP, PREVIC, REDE-LAB, RFB, SAL/MJSP, SENASP/MJSP.

Convidado: ANATEL.

SUMÁRIO EXECUTIVO

Este documento apresenta um diagnóstico detalhado sobre o Golpe da Falsa Central. São abordadas suas principais tipologias, tecnologias empregadas pelos criminosos, medidas de controle existentes e lacunas identificadas no sistema atual. O estudo, além de destacar a importância da conscientização da população, propõe soluções integradas entre instituições financeiras, empresas de telecomunicações, autoridades públicas e *big techs*, com propostas de medidas operacionais e normativas apresentadas no Produto 2 desta Ação.

PRINCIPAIS ACHADOS:

- 50,7% dos brasileiros foram vítimas de fraudes em 2024[1].
- 54,2% das vítimas tiveram perdas financeiras efetivas[2].
- 4 golpes por minuto[3].
- Evolução tecnológica dos criminosos supera velocidade de resposta institucional.
- Dispersão de informações e fragmentação de competências dificulta resposta coordenada.

1. INTRODUÇÃO

Nas últimas décadas, com a incorporação da Internet e de novas tecnologias em praticamente todas as esferas da vida cotidiana, a sociedade tem vivenciado um processo acelerado de digitalização. Contudo, esse avanço não veio acompanhado, de forma proporcional, por uma maturidade digital da população. A falta de conhecimento técnico e de práticas de segurança torna os cidadãos cada vez mais vulneráveis a golpes eletrônicos.

O crescimento desenfreado das fraudes bancárias e golpes digitais reflete não apenas a evolução das estratégias criminosas, mas também um desequilíbrio entre a rapidez da transformação digital e a capacidade de adaptação segura da sociedade.

Entre os diversos tipos de golpes eletrônicos, destaca-se do Golpe da Falsa Central, modalidade em que criminosos se passam por atendentes de instituições financeiras e outras empresas, utilizando técnicas sofisticadas de engenharia social para manipular vítimas e obter dados confidenciais ou autorizações de transações. Esses golpes não apenas prejudicam as vítimas financeiramente, mas também causam danos emocionais e psicológicos significativos.

Em pesquisa realizada pela Serasa Experian com consumidores, 50,7% dos brasileiros foram vítimas de fraudes em 2, aumento de 9 pontos percentuais em relação a 2023. Desse total, 54,2% das vítimas afirmaram ter perdido dinheiro.[4]

---

[1] [2] [3] Tentativas de fraudes bancárias cresceram 10,4% em 2024 e poderiam gerar prejuízo de até R$ 51,6 bilhões, revela Serasa Experian. Sala de Imprensa da Serasa Experian, 11 de mar. 2025. Disponível em < https://www.serasaexperian.com.br/sala-de-imprensa/prevencao-a-fraude/tentativas-de-fraudes-bancarias-cresceram-104-em-2024-e-poderiam-gerar-prejuizo-de-ate-r-516-bilhoes-revela-serasa-experian/>

[4] Tentativas de fraudes bancárias cresceram 10,4% em 2024 e poderiam gerar prejuízo de até R$ 51,6 bilhões, revela Serasa Experian. Sala de Imprensa da Serasa Experian, 11 de mar. 2025. Disponível em < https://www.serasaexperian.com.br/sala-de-imprensa/prevencao-a-fraude/tentativas-de-fraudes-

Na mesma esteira, o recente anuário Brasileiro de Segurança Pública 2025 indica, com dados de 2024, o registro de 04 golpes por minuto no Brasil.

O presente diagnóstico visa abordar o Golpe da Falsa Central em suas principais modalidades, elucidar tecnologias e engenharias empregadas pelos golpistas e, em parceria com entes públicos e privados, avaliar medidas de prevenção e repressão.

A ação conjunta entre diversos setores impactará diretamente a segurança e a confiança dos clientes em relação aos serviços bancários, de telefonia e segurança pública.

2. TIPOLOGIAS E TECNOLOGIAS EMPREGADAS

O Golpe da Falsa Central é a principal modalidade de golpe bancário atualmente, explorando vulnerabilidades humanas e tecnológicas para enganar vítimas por meio de ligações telefônicas. Durante os trabalhos da Ação, destacamos as seguintes modalidades:

i) **Falso Gerente do Banco:** o criminoso se apresenta como gerente da agência em que a vítima possui conta. Com dados pessoais obtidos por vazamentos ou compra ilegal e utilização de *Spoofing*, mascarando a bina com o telefone da agência/funcionário, ele informa sobre uma suposta invasão ou movimentação suspeita. Para "proteger" a conta ou "contestar" transações não reconhecidas, orienta a vítima a realizar operações financeiras, sem que perceba que está caindo em um golpe.

ii) **Falso Advogado:** neste cenário, o golpista se passa por advogado envolvido em um processo judicial da vítima. Utiliza linguagem jurídica sofisticada e envia documentos falsificados por e-mail ou WhatsApp. Alega que há valores a serem liberados mediante pagamento de custas ou taxas, induzindo a vítima a realizar transferências via PIX.

iii) **Falsa Investigação:** o golpista afirma ser policial, agente da justiça ou funcionário da área de segurança do banco, alegando que a agência bancária da vítima está sob investigação por envolvimento em fraudes. Para "proteger" os valores ou auxiliar nas investigações, orienta a transferência imediata para contas "monitoradas" ou solicita dados bancários sob o pretexto de bloqueio preventivo. Além do tom ser autoritário e urgente, intimidando a vítima, a convencem de que, para não comprometer o andamento das investigações, ela somente deve confiar em único funcionário.

iv) **Falso Técnico de TI:** o criminoso se apresenta como técnico de segurança digital do banco. Alega que há uma falha no sistema ou tentativa de invasão e orienta a instalação de um aplicativo de acesso remoto como *AnyDesk* ou *RustDesk*. Após obter controle do celular, realiza transações bancárias, altera senhas e apaga rastros da fraude.

v) **Outras Modalidades Identificadas:**

a. **Falso Presente:** Entrega com cobrança via máquina de cartão alterada.

---

bancarias-cresceram-104-em-2024-e-poderiam-gerar-prejuizo-de-ate-r-516-bilhoes-revela-serasa-experian/>

b. **Falso Sequestro:** Simulação de sequestro, com uso de informações obtidas por meio de redes sociais.
c. **Golpe do WhatsApp:** Clonagem de contas para solicitação de valores a contatos.
d. **Falso Motoboy:** Coleta de cartões sob pretexto de perícia técnica.

3. TECNOLOGIAS EMPREGADAS PELOS CRIMINOSOS

3.1 TECNOLOGIAS DE COMUNICAÇÃO

***VoIP* (*Voice over IP*):** Permite que chamadas sejam feitas pela internet, facilitando a falsificação de números e a ocultação da origem real da ligação. Representa 85% das fraudes identificadas.

Spoofing: Técnica que mascara o número de origem, fazendo parecer que a chamada vem de fonte confiável, como o banco da vítima. Permite exibição de números oficiais das instituições.

Vishing (*Voice Phishing*): Variante do *phishing* que utiliza chamadas de voz para enganar a vítima e obter informações sensíveis ou induzi-la a realizar ações prejudiciais.

3.2 EVOLUÇÃO TECNOLÓGICA IDENTIFICADA (2024-2025)

Ascensão do Acesso Remoto Legítimo: Milhares de casos registrados desde 2024, utilizando software legítimo (*TeamViewer, AnyDesk, Chrome Remote Desktop*).

Uso de Inteligência Artificial: Implementação de *deepfakes* para clonagem de voz de atendentes bancários, tornando as ligações indistinguíveis das originais.

3.2 ESTRUTURA OPERACIONAL DOS CRIMINOSOS (BÁSICA)

Nível 1 - Liderança: Coordenação geral, gestão financeira.

Nível 2 - Operacional: Execução das fraudes, movimentação financeira.

Nível 3 - Suporte: Fornecimento de dados, recrutamento de "laranjas", abertura de contas, saque de valores, suporte técnico.

4. ESTRUTURAS EXISTENTES

4.1 PLATAFORMA TENTÁCULOS (POLÍCIA FEDERAL)

A Plataforma Tentáculos da Polícia Federal representa um dos principais instrumentos de combate às fraudes bancárias eletrônicas no país, tendo registrado mais de 570 operações realizadas e 1.200 mandados de busca e apreensão executados desde sua criação. No entanto, sua efetividade pode ser significativamente ampliada através da expansão operacional planejada.

Atualmente, as Polícias Civis do DF, GO, MG e PI estão integradas à plataforma, situação que precisa ser rapidamente ampliada. A meta estabelecida prevê a integração com 100% das polícias civis estaduais para uso da Plataforma Tentáculos. Esta ampliação permitirá cobertura

nacional completa e acesso a um espectro mais amplo de informações relevantes para as investigações.

Criada em 2007 para investigar crimes de fraudes bancárias eletrônicas, a plataforma evoluiu significativamente:

2018: Ampliação com bancos da FEBRABAN.

2023: Integração com a ZETTA e ABRANET.

2024: Expansão para polícias civis estaduais.

2025: Integração com ABECS, ACREFI e ABBC.

2025+: Integração com ABRACAM e outras.

A plataforma baseia-se na premissa de que o combate efetivo às fraudes exige ruptura com o modelo tradicional de investigação isolada. Os grupos criminosos operam coordenadamente entre múltiplas instituições, exigindo resposta sistêmica que transcende fronteiras institucionais tradicionais.

4.1.1 Resultados Alcançados

(i) Mais de 570 operações realizadas desde a criação.
(ii) Desarticulação de organizações criminosas complexas multiestados.
(iii) Desenvolvimento de metodologias de análise de vínculos.

4.1.2 Conquistas Identificadas

(i) Estabelecimento de cultura de cooperação sistemática entre setores.
(ii) Padronização de procedimentos investigativos especializados.
(iii) Desenvolvimento de linguagem técnica comum para diferentes atores.

4.2 ALIANÇA NACIONAL DE COMBATE A FRAUDES (MJSP & FEBRABAN)

A Aliança Nacional representa iniciativa pioneira na articulação estruturada entre Ministério da Justiça e setor bancário privado para enfrentamento coordenado das fraudes digitais. Estruturada em três eixos estratégicos, constitui modelo inovador de cooperação que transcende fronteiras tradicionais entre setores público e privado.

Eixo de boas práticas: tem foco na padronização de protocolos antifraude em todas as instituições do sistema financeiro nacional, com ênfase no emprego unificado das tipologias. Esta padronização facilitará o compartilhamento de informações e a coordenação de respostas entre diferentes instituições.

Eixo de compartilhamento de dados: prevê significativa ampliação das bases atualmente disponíveis. A integração com dados de telecomunicações permitirá correlações mais precisas entre chamadas suspeitas e transações fraudulentas. O compartilhamento com fintechs, meios de pagamento e corretoras de criptoativos garantirá cobertura completa do ecossistema financeiro digital. A ampliação do uso da Plataforma Tentáculos representará instrumento fundamental para a prevenção e repressão das condutas ilícitas.

Eixo de atendimento às vítimas: será fortalecido através da implementação de protocolo de atendimento padronizado que garanta tratamento uniforme e eficaz em todo o território nacional, complementado por campanhas educativas direcionadas aos grupos mais vulneráveis.

O desenvolvimento da aliança surge do reconhecimento de que a sofisticação das fraudes contemporâneas exige cooperação sistemática que supere a fragmentação institucional tradicionalmente observada.

4.2.1 Conquistas Identificadas

(i) Protocolos de compartilhamento entre setores.
(ii) Campanhas educativas coordenadas.
(iii) Capacitação de agentes e consumidores.

4.2.2 Limitações Observadas

(i) Alcance limitado a participantes voluntários.
(ii) Concentração no setor bancário tradicional, excluindo fintechs emergentes.
(iii) Integração limitada com outros setores afetados (telecomunicações, *big techs*).
(iv) Cobertura insuficiente de outros players do ecossistema financeiro digital.

4.3 RESOLUÇÃO Nº 142 (BANCO CENTRAL)

Estabelece diretrizes e mecanismos de controle voltados à prevenção de fraudes nos serviços de pagamento, que devem ser implementados por instituições financeiras, entidades autorizadas pelo Banco Central do Brasil e instituições de pagamento que fazem parte do Sistema de Pagamentos Brasileiro (SPB).

4.4 RESOLUÇÃO CONJUNTA Nº 6 (BANCO CENTRAL)

A Resolução Conjunta nº 6, publicada em maio de 2023, estabelece marco regulatório para compartilhamento sistemático de dados sobre fraudes entre instituições financeiras supervisionadas pelo BCB. Representa mudança paradigmática na abordagem regulatória, passando de modelo baseado em ações isoladas para sistema coordenado de inteligência antifraude.

4.4.1 Características Principais

Sistema: Base eletrônica integrada para consulta de CPF/CNPJ com denúncias;

Governança: Protocolos para qualidade e integração de dados.

A resolução surge da constatação de que fraudes contemporâneas transcendem limites institucionais individuais, caracterizando-se como fenômeno sistêmico que exige resposta coordenada.

4.4.2 Resultados Observados

(i) Base integrada para consulta de CPF/CNPJ com suspeitas de fraude.
(ii) Aplicável a todas as entidades financeiras reguladas pelo BCB, desde novembro/2023.
(iii) Redução no tempo de identificação de padrões fraudulentos.

4.4.3 Limitações Identificadas

(i) Escopo restrito às instituições supervisionadas pelo BCB.
(ii) Ausência de integração com setores de telecomunicações e tecnologia.
(iii) Dependência de adesão voluntária para compartilhamento com entidades não supervisionadas.
(iv) Necessidade de expansão para outros prestadores de serviços financeiros.

4.5 RESOLUÇÃO N° 501 (BANCO CENTRAL)

Modifica a Resolução nº 142 do Banco Central, datada de 23 de setembro de 2021, que estabelece diretrizes e mecanismos de controle voltados à prevenção de fraudes nos serviços de pagamento. Essas medidas devem ser adotadas por instituições financeiras, demais entidades autorizadas a operar pelo Banco Central do Brasil, bem como pelas instituições de pagamento que fazem parte do Sistema de Pagamentos Brasileiro (SPB).

4.5.1 Limitações Identificadas

(i) Ausência de definição de critérios, pelo regulador, sobre “fundada suspeita de envolvimento de fraude” a serem adotados pelas instituições financeiras.

5. INICIATIVAS DE TELECOMUNICAÇÕES

5.1 PROJETO "ORIGEM VERIFICADA" (ANATEL)

O projeto "Origem Verificada" implementa tecnologia internacional *Stir/Shaken* adaptada para a realidade brasileira, constituindo solução avançada para autenticação de chamadas telefônicas.

5.1.1 Funcionamento

(i) **Autenticação:** Verificação do número de origem.
(ii) **Assinatura Digital:** Token criptografado acompanha a chamada.
(iii) **Verificação:** Análise da legitimidade no destino.
(iv) **Exibição:** Nome, logotipo, motivo e selo de autenticidade na tela.

5.1.2 Situação Atual:

(i) Obrigatoriedade do uso do processo de autenticação de chamadas para contratantes de serviços de telefonia que realizem mais de 500 mil ligações por mês (publicado em agosto de 2025)[5].
(ii) 90 dias de prazo para adequação às novas regras[6].

[5] [6] Governo Federal aprova novas medidas para coibir práticas abusivas na realização de chamadas telefônicas em massa. Comunicações e Transparência Pública, Gov.br, 11/08/2025 14h59. Disponível em <https://www.gov.br/mcom/pt-br/noticias/2025/agosto/governo-federal-aprova-novas-medidas-para-coibir-praticas-abusivas-na-realizacao-de-chamadas-telefonicas-em-massa-1>

(iii) Crescimento consistente na adesão empresarial, com estimativa de conclusão em até 3 anos[7].

5.1.3 Resultados Esperados

(i) Redução substancial na efetividade do *spoofing* telefônico.
(ii) Aumento da confiança dos consumidores em chamadas empresariais.
(iii) Estabelecimento de padrão técnico nacional para autenticação.
(iv) Estímulo a investimentos privados em tecnologias complementares.

5.1.4 Limitações Identificadas

(i) Adesão ainda restrita a empresas de grande porte.
(ii) Dependência de adesão voluntária de operadoras menores.
(iii) Cobertura limitada para pequenas e médias empresas.
(iv) Ausência de cronograma para inclusão de redes móveis.

5.2 CONTROLES REGULATÓRIOS ATUAIS

Números 0800: Utilizados sistematicamente por criminosos devido à confiança tradicional dos consumidores. Controles atuais baseiam-se em verificação básica de documentação, processo que se mostrou insuficiente diante da criação de empresas de fachada para obtenção destes números.

Chips Pré-pagos: Regulamentados pelas Resoluções nº 477/2007 (identificação obrigatória) e nº 740/2020 (atualização cadastral), enfrentam problemas persistentes com documentos falsos, comercialização informal e ativações massivas suspeitas.

Serviços de SMS: Crescimento exponencial do *smishing* explora credibilidade das mensagens de texto, com sistemas de filtragem limitados e facilidade de utilização de gateways ilegais para disparos em massa.

6. ATUAÇÃO DAS *BIG TECHS*

A crescente influência das grandes empresas de tecnologia na economia digital brasileira criou paradigma no qual essas plataformas se tornaram vetores fundamentais para a disseminação dos golpes bancários por falsas centrais de atendimento. A análise da atuação dessas empresas revela cenário complexo caracterizado por capacidades tecnológicas e exploração sistemática das plataformas por grupos criminosos.

6.1 PROBLEMAS SISTEMÁTICOS IDENTIFICADOS

A utilização das plataformas digitais pelos grupos criminosos evoluiu de uma atividade marginal para operações estruturadas que exploram as vulnerabilidades inerentes aos modelos de negócio baseados em publicidade e engajamento.

---

[7] Governo Federal aprova novas medidas para coibir práticas abusivas na realização de chamadas telefônicas em massa. Comunicações e Transparência Pública, Gov.br, 11/08/2025 14h59. Disponível em <https://www.gov.br/mcom/pt-br/noticias/2025/agosto/governo-federal-aprova-novas-medidas-para-coibir-praticas-abusivas-na-realizacao-de-chamadas-telefonicas-em-massa-1>

6.1.1 Falsas Páginas Patrocinadas em Ferramentas de Busca

A veiculação de páginas falsas de instituições financeiras como anúncios patrocinados em ferramentas de busca representa uma das modalidades mais sofisticadas e efetivas de golpe digital. Estes anúncios exploram a confiança dos usuários no posicionamento dos resultados de pesquisa, aproveitando-se do fato de que muitos consumidores não distinguem claramente entre resultados orgânicos e conteúdo patrocinado.

O investimento em *Search Engine Optimization* (SEO) e campanhas de *Google Ads* permite que páginas fraudulentas apareçam frequentemente nas primeiras posições dos resultados, superando muitas vezes os próprios sites oficiais das instituições que estão sendo falsificadas[8].

A análise de casos específicos revela que alguns grupos criminosos chegam a investir dezenas de milhares de reais mensalmente em campanhas publicitárias para suas páginas fraudulentas, demonstrando a lucratividade dessas operações e a inadequação dos mecanismos atuais de verificação de anunciantes.

O tempo de resposta para remoção de páginas fraudulentas constitui fator crítico na determinação do número de vítimas afetadas. As páginas fraudulentas podem permanecer ativas por dias ou mesmo semanas antes de serem removidas, período durante o qual podem capturar dados de centenas ou milhares de usuários. A falta de canais prioritários para denúncias de instituições financeiras legítimas agrava este problema, forçando essas organizações a utilizar os mesmos procedimentos burocráticos disponíveis para usuários comuns.

A Google e Meta, principais plataformas de impulsionamento de anúncios no Brasil, foram convidadas pela secretaria da ENCCLA para participar dos debates referentes à ação 1, porém não compareceram às reuniões.

6.1.2 Comercialização de Ferramentas Criminosas em Redes Sociais

A migração de ferramentas criminosas da *dark web* para redes sociais abertas representa mudança paradigmática que levou para a *clear web* o acesso a recursos antes restritos a criminosos com conhecimentos técnicos avançados. Plataformas como Facebook, Instagram, Telegram e WhatsApp tornaram-se mercados ativos para a comercialização de software de emulação de telefones, URAs falsas, bases de dados de clientes, informações bancárias e até mesmo treinamentos sobre técnicas de engenharia social.

A análise de grupos específicos nessas plataformas revela economia criminosa estruturada, com fornecedores especializados, avaliações de clientes etc. Alguns grupos chegam a ter milhares de membros e movimentam volumes significativos de recursos através da venda de ferramentas e informações criminosas.

A comercialização de contas "laranjas" representa segmento particularmente problemático deste mercado informal. Grupos especializados oferecem não apenas contas bancárias prontas para uso criminoso, mas também serviços completos que incluem abertura de

[8] Fraudadores espalham malware via Google Ads e DeepSeek. Ciso Advisor, 27/03/2025 21:05. Disponível em <https://www.cisoadvisor.com.br/fraudadores-espalham-malware-via-google-ads-e-deepseek/>

contas, manutenção de movimentação aparentemente legítima entre outros. Os preços praticados nestes mercados variam conforme o tipo de conta e a instituição financeira, com contas de bancos digitais geralmente sendo comercializadas por valores inferiores às de instituições tradicionais.

6.1.3 Ineficiência dos Mecanismos de Controle

A análise dos sistemas de moderação de conteúdo das principais plataformas revela descompasso significativo entre as capacidades tecnológicas disponíveis e sua aplicação efetiva no combate a fraudes bancárias. Plataformas que conseguem detectar e remover rapidamente conteúdo relacionado a direitos autorais ou discurso de ódio frequentemente falham na identificação de conteúdo criminoso relacionado a golpes bancários.

Esta discrepância pode ser atribuída parcialmente às diferenças nos incentivos econômicos e regulatórios. Violações de direitos autorais expõem as plataformas a riscos legais diretos e significativos, criando forte motivação para desenvolvimento de sistemas de detecção eficazes. Em contraste, a responsabilização legal por conteúdo fraudulento publicado por terceiros ainda é limitada no Brasil, reduzindo os incentivos para investimento em sistemas especializados de detecção de fraudes e golpes.

6.2 CAPACIDADES TECNOLÓGICAS SUBUTILIZADAS

As grandes plataformas tecnológicas desenvolveram capacidades de análise de dados e detecção de padrões que poderiam ser aplicadas efetivamente no combate a golpes bancários, mas que atualmente são subutilizadas para esse propósito. A experiência acumulada no desenvolvimento de sistemas para combate a *spam*, *fake news* e outros tipos de conteúdo problemático fornece base tecnológica sólida que poderia ser adaptada para identificação de conteúdo relacionado a golpes bancários.

6.4 IMPACTO NA CONFIANÇA DOS CONSUMIDORES

A utilização sistemática das plataformas digitais para perpetração de fraudes e golpes tem impacto direto na confiança dos consumidores tanto nas próprias plataformas quanto no ecossistema digital mais amplo, como por exemplo a desconfiança dos usuários brasileiros em relação a anúncios online e comunicações recebidas através de redes sociais ou SMS, tendência que pode prejudicar o desenvolvimento da economia digital no país.

A associação entre determinadas plataformas e experiências fraudulentas cria externalidades negativas que afetam não apenas as empresas diretamente envolvidas, mas todo o ecossistema de serviços digitais. A redução na confiança dos consumidores pode resultar em menor adesão a serviços financeiros digitais legítimos, prejudicando esforços de inclusão financeira e digitalização da economia.

7. LACUNAS E VULNERABILIDADES IDENTIFICADAS

A análise sistemática dos golpes bancários por falsas centrais de atendimento revela conjunto complexo de lacunas e vulnerabilidades que transcendem setores individuais, caracterizando-se como deficiências sistêmicas que facilitam a perpetuação e expansão dessas

práticas criminosas. Essas vulnerabilidades podem ser categorizadas em quatro dimensões principais que se inter-relacionam e se reforçam mutuamente: fragmentação de competências, limitações tecnológicas, gaps regulatórios e vulnerabilidades sociais.

7.1 FRAGMENTAÇÃO DE COMPETÊNCIAS INSTITUCIONAIS

A estrutura institucional brasileira para combate às fraudes bancárias caracteriza-se por divisão de responsabilidades entre múltiplos órgãos e entidades que frequentemente operam de forma descoordenada, criando lacunas que são sistematicamente exploradas pelos grupos criminosos. Esta fragmentação manifesta-se em diversos níveis, desde a definição de competências regulatórias até a execução de ações operacionais de combate.

A ausência de coordenação sistemática entre setores resulta em situações em que instituições financeiras implementam medidas de segurança que podem ser contornadas através de vulnerabilidades em sistemas de telecomunicações, enquanto melhorias na segurança das comunicações podem ser neutralizadas por lacunas nos controles bancários. Os criminosos demonstram capacidade superior de adaptação e coordenação em comparação com as respostas institucionais, frequentemente migrando suas operações para os setores menos protegidos ou aproveitando-se da falta de comunicação entre diferentes órgãos de controle.

A sobreposição de competências em algumas áreas, combinada com lacunas de responsabilidade em outras, cria ambiente de incerteza que prejudica a implementação de medidas efetivas.

7.2 LIMITAÇÕES TECNOLÓGICAS SISTÊMICAS

As limitações tecnológicas identificadas no sistema brasileiro de combate a fraudes e golpes refletem não apenas deficiências em tecnologias específicas, mas também problemas estruturais na abordagem tecnológica ao problema. A predominância de sistemas reativos sobre mecanismos preditivos representa uma das principais vulnerabilidades, pois permite que os criminosos mantenham vantagem temporal significativa na implementação de novas técnicas fraudulentas.

7.3 FALTA DE INTEGRAÇÃO ENTRE SISTEMAS

A ausência de integração efetiva entre sistemas bancários, de telecomunicações e de autoridades representa lacuna fundamental que impede a correlação de informações que poderiam facilitar a identificação de fraudes.

Esta falta de integração estende-se também aos sistemas de diferentes instituições dentro do mesmo setor. Embora a Resolução Conjunta nº 6 tenha estabelecido mecanismos de compartilhamento de informações no setor bancário, a implementação prática ainda enfrenta limitações técnicas relacionadas à padronização de dados.

7.4 PRINCIPAIS LACUNAS LEGAIS

Análise do marco regulatório brasileiro revela lacunas que facilitam a operação de grupos criminosos especializados em golpes bancários por falsas centrais de atendimento. Essas

lacunas não se limitam à ausência de regulamentações específicas, mas incluem também inadequações nas regulamentações existentes e dificuldades na aplicação prática das normas estabelecidas.

7.4.1 Ausência de Tipificação Penal Específica

O Código Penal brasileiro não contempla tipificação específica para golpes bancários eletrônicos, forçando o enquadramento desses crimes em tipos penais genéricos que não capturam adequadamente a especificidade e gravidade dessas condutas. A aplicação do artigo 171 (estelionato comum) para fraudes sofisticadas que envolvem múltiplas vítimas e organização criminosa complexa resulta em penas frequentemente inadequadas à dimensão dos danos causados.

Esta inadequação da tipificação penal tem impactos que transcendem a questão das sanções, afetando também a priorização desses crimes pelos órgãos de investigação, a especialização dos operadores do direito e a percepção social sobre a gravidade dessas condutas. A ausência de tipos penais específicos também dificulta a coleta de estatísticas precisas sobre a incidência desses crimes, prejudicando o desenvolvimento de políticas públicas baseadas em evidências.

7.4.2 Competência Territorial Inadequada

As regras tradicionais de competência territorial mostram-se inadequadas para crimes digitais que frequentemente envolvem vítimas em um estado, criminosos operando em outro e infraestrutura tecnológica distribuída em múltiplas jurisdições. Esta inadequação resulta em distribuição de casos para comarcas onde frequentemente não se encontram nem os principais elementos de prova nem os investigados, prejudicando significativamente a efetividade das investigações.

A fragmentação jurisdicional permite que grupos criminosos organizados explorem as dificuldades de coordenação entre diferentes unidades do Ministério Público e da Polícia Judiciária, mantendo operações que transcendem fronteiras estaduais enquanto as investigações permanecem limitadas por divisões administrativas que não correspondem à realidade do crime digital.

7.4.3 Responsabilização Limitada de Plataformas Digitais

A ausência de marco legal específico para responsabilização de plataformas digitais por conteúdo fraudulento representa lacuna crítica no sistema de combate a fraudes. Enquanto outros países desenvolveram regulamentações que estabelecem obrigações claras para remoção de conteúdo fraudulento e cooperação com autoridades, o Brasil ainda carece de framework regulatório adequado que equilibre liberdade de expressão com proteção contra crimes financeiros.

Esta lacuna regulatória é particularmente problemática considerando o papel crescente das plataformas digitais na disseminação de fraudes e recrutamento de vítimas. A dependência de cooperação voluntária das plataformas resulta em respostas inconsistentes e frequentemente inadequadas às demandas das autoridades brasileiras.

7.5 VULNERABILIDADES SOCIAIS ESTRUTURAIS

As vulnerabilidades sociais que facilitam a vitimização por golpes bancários refletem características estruturais da sociedade brasileira que transcendem questões de educação individual, incluindo desigualdades no acesso à educação digital, confiança excessiva em instituições e limitações na disseminação de informações de segurança.

7.5.1 Baixo Letramento Digital

O letramento digital limitado de parcela significativa da população brasileira cria vulnerabilidades que são sistematicamente exploradas pelos grupos criminosos. Esta limitação não se restringe ao uso básico de tecnologias, mas estende-se à compreensão de conceitos fundamentais de segurança digital, identificação de ameaças e adoção de práticas preventivas.

Pesquisas específicas sobre o tema indicam que aproximadamente 60% da população brasileira possui letramento digital básico ou inexistente[9], criando base ampla de potenciais vítimas que não possuem conhecimentos necessários para identificar e evitar tentativas de fraude ou golpe. Esta vulnerabilidade é particularmente significativa entre idosos, grupo que representa 65% das vítimas de golpes bancários segundo dados consolidados pelas instituições participantes desta Ação.

7.5.2 Confiança Excessiva em Canais Tradicionais

A confiança tradicional dos brasileiros em canais telefônicos como meio de comunicação legítimo cria vulnerabilidade específica que é explorada pelos golpes de falsas centrais. Esta confiança baseia-se em décadas de experiência com atendimento telefônico legítimo de empresas e órgãos públicos, criando predisposição psicológica que facilita a manipulação por criminosos que se apresentam como representantes de instituições confiáveis.

A persistência desta confiança mesmo diante do crescimento dos golpes telefônicos sugere necessidade de campanhas educativas específicas que abordem não apenas técnicas de identificação de fraudes, mas também a necessidade de mudança de paradigmas sobre a segurança das comunicações telefônicas.

8. PRINCIPAIS AÇÕES MAPEADAS

Ofensor	Ação Mapeadas
Contratação de serviços de telefonia por golpistas	Ampliação do uso de bases negativas de mercado, a exemplo da Resolução Conjunta nº 6, para impedimento na contratação de serviços de telefonia, como linhas pré-pagas e números 0800.
Spoofing e números não autenticados	Ampliação do uso da Origem Verificada (*Stir/Shaken*) e Notificação Falsa Central
Identificação e vinculação de chips pré-pagos	Avaliar: (i) Implementação de biometria facial para o *opt-in* do serviço. (ii) Limitação de linhas por CPF. (iii) Bases atualizadas de vínculo/posse

[9] TIC DOMICÍLIOS. Pesquisa sobre o Uso das Tecnologias de Informação e Comunicação nos Domicílios Brasileiros. Cetic.br, 2024. Disponível em <https://cetic.br/media/docs/publicacoes/2/20240826111431/tic_domicilios_2023_livro_eletronico.pdf>

Tempestividade no *take-down* de números e páginas falsas	Criação de Canal de Denúncias, fomentado por instituições financeiras e autoridades públicas, para derrubada de páginas falsas ou linhas telefônicas utilizadas para aplicação de golpes.
Compartilhamento de dados	Incentivar a adoção e adesão por meio de Acordos de Cooperação entre instituições financeiras, empresas de telecomunicações, autoridades públicas e *big techs* para compartilhamento de dados envolvendo fraudes e golpes, a fim de auxiliar em medidas preventivas, investigativas e repressivas, por meio da Plataforma Tentáculos da Polícia Federal.
Conscientização Origem Verificada (*Stir/Shaken*) e Notificação Falsa Central	Criação de campanhas de conscientização para a população acerca dos serviços Origem Verificada (*Stir/Shaken*) e Notificação de Falsa Central
Conscientização Golpes de Falsa Central	Criação de campanhas de conscientização para a população sobre Golpes de Falsa Central

9. CONCLUSÕES DO DIAGNÓSTICO

9.1 SÍNTESE DOS PRINCIPAIS ACHADOS

A análise abrangente dos golpes bancários por falsas centrais de atendimento no Brasil revela fenômeno de complexidade crescente que transcende as fronteiras tradicionais entre diferentes setores e competências, caracterizando-se como desafio sistêmico que exige resposta coordenada e multidisciplinar. Os achados desta investigação evidenciam que o problema não pode ser adequadamente compreendido ou combatido através de abordagens fragmentadas que considerem apenas aspectos isolados da questão.

A concentração de vítimas em grupos específicos - idosos e pessoas com menor escolaridade formal - indica que as vulnerabilidades exploradas pelos criminosos não são aleatórias, mas refletem características estruturais da sociedade brasileira que criam oportunidades sistemáticas para vitimização.

9.2 PADRÕES SISTÊMICOS IDENTIFICADOS

9.2.1 Fragmentação Institucional

A principal vulnerabilidade sistêmica identificada reside na fragmentação de competências e responsabilidades entre múltiplos órgãos e setores que operam sem coordenação adequada. Enquanto a Plataforma Tentáculos demonstra efetividade quando aplicada (570+ operações), sua integração atual com apenas 4 polícias civis estaduais de 27 possíveis exemplifica o potencial do modelo.

A Resolução Conjunta nº 6 do Banco Central, apesar de representar avanço significativo no compartilhamento de informações no setor financeiro, permanece limitada ao escopo das instituições supervisionadas pelo BACEN, excluindo importantes segmentos do ecossistema financeiro digital que são crescentemente explorados pelos criminosos.

9.2.2 Descompasso Tecnológico

A análise revela descompasso fundamental entre a sofisticação das técnicas criminosas e a capacidade de resposta tecnológica das instituições.

O projeto "Origem Verificada" da ANATEL, embora tecnicamente avançado, alcança poucas empresas de milhares que poderiam se beneficiar da tecnologia, demonstrando desafios na velocidade de implementação de soluções tecnológicas mesmo quando disponíveis.

9.2.3 Vulnerabilidades Sociais Estruturais

O baixo letramento digital (60% da população com letramento básico ou inexistente, segundo CETIC.br) cria base ampla de vulnerabilidade que é sistematicamente explorada pelos criminosos. Esta vulnerabilidade é exacerbada pela confiança tradicional em canais telefônicos, criando predisposição psicológica que facilita a manipulação.

9.3 NECESSIDADES PRIORITÁRIAS IDENTIFICADAS

9.3.1 Coordenação Institucional

A necessidade mais urgente identificada é o estabelecimento de mecanismos permanentes de coordenação entre todos os setores afetados, superando a fragmentação atual que permite aos criminosos explorar lacunas entre diferentes competências e responsabilidades.

9.3.2 Atualização Tecnológica Sistêmica

A implementação coordenada de tecnologias de segurança avançadas em todos os setores relevantes é essencial para reduzir as oportunidades de migração criminosa entre canais menos protegidos.

9.3.3 Marco Regulatório Integrado

O desenvolvimento de marco regulatório específico para crimes digitais que considere sua natureza transetorial e facilite a cooperação entre diferentes órgãos é fundamental para superar as limitações das regulamentações fragmentadas atuais.

9.3.4 Educação e Conscientização Massiva

A implementação de programas massivos de educação digital e conscientização sobre riscos de fraude é essencial para reduzir as vulnerabilidades sociais estruturais que facilitam a vitimização.

9.3 IMPLICAÇÕES PARA POLÍTICAS PÚBLICAS

9.4.1 Abordagem Sistêmica

Os achados desta análise indicam que políticas públicas fragmentadas ou setoriais têm efetividade limitada no combate a golpes bancários. É necessária abordagem sistêmica que considere as interconexões entre diferentes setores e as dinâmicas de adaptação dos grupos criminosos.

9.4.2 Fundamentos para as Medidas Propostas

Este diagnóstico fundamenta as medidas operacionais e normativas apresentadas no Produto 2 desta Ação, que abordam de forma sistemática as vulnerabilidades identificadas através de propostas coordenadas nos eixos tecnológico, institucional, regulatório, penal e administrativo.

A implementação articulada dessas medidas é essencial para alterar o cenário atual, pois abordagens fragmentadas mostraram-se inadequadas diante da natureza sistêmica e evolutiva do problema. O sucesso no combate às fraudes bancárias por falsas centrais de atendimento depende fundamentalmente da capacidade de coordenação interinstitucional e da implementação simultânea de medidas em todos os setores afetados.

A experiência acumulada pelas instituições participantes desta Ação demonstra que soluções isoladas, embora possam produzir resultados positivos localizados, não conseguem produzir impacto sistêmico duradouro. Apenas através de resposta coordenada, tecnologicamente avançada e socialmente abrangente será possível proporcionar proteção efetiva à sociedade brasileira contra essas práticas criminosas em constante evolução.

ENCCLA 2025

Estratégia Nacional de Combate à Corrupção e à Lavagem de Dinheiro

AÇÃO 01/2025

PRODUTO I

DIAGNÓSTICO DETALHADO SOBRE OS GOLPES VIA FALSA CENTRAL E CONDUTAS CONEXAS.