REMUNOM
ISSN 2178-6925

**Received:** 25/01/2026 - **Accepted:** 10/03/2026
**Vol**: 13.02
**DOI**: 10.66104/bsgn8v13
**Pages:** 1-26

# UMA NOVA ERA NO COMBATE AOS CRIMES CIBERNÉTICOS: COMO A AUTOMAÇÃO E GOVERNANÇA DO MED 2.0 IMPULSIONAM A REDUÇÃO DE PERDAS E A DISSUASÃO DE GOLPES FINANCEIROS NO BRASIL

# A NEW ERA IN COMBATING CYBERCRIME: HOW THE AUTOMATION AND GOVERNANCE OF MED 2.0 DRIVE LOSS REDUCTION AND THE DETERRENCE OF FINANCIAL FRAUD IN BRAZIL

# UNA NUEVA ERA EN LA LUCHA CONTRA LOS DELITOS CIBERNÉTICOS: CÓMO LA AUTOMATIZACIÓN Y LA GOBERNANZA DEL MED 2.0 IMPULSAN LA REDUCCIÓN DE PÉRDIDAS Y LA DISUASIÓN DE FRAUDES FINANCIEROS EN BRASIL

**Gesson Eliésio Aguiar de Sousa**
Mestrando do Programa de Pós-Graduação em Segurança Pública, Cidadania e Direitos Humanos pela Universidade do Estado do Amazonas - UEA

**João Frederico Nascimento Araújo**
Mestrando do Programa de Pós-Graduação em Segurança Pública, Cidadania e Direitos Humanos pela Universidade do Estado do Amazonas - UEA

**Paulo César Diniz de Araújo**
Doutor em Administração pela Universidade Federal de Minas Gerais- UFMG

**Mário Jumbo Miranda Aufiero**
Doutor em Direito pela Faculdade Autônoma de Direito de São Paulo - FADISP

**Carlos Augusto Oliveira de Souza**
Pós-Graduado em Direito Processual pelo Centro Universitário de Ensino Superior do Amazonas – CIESA

**Danielle Costa de Souza Simas**
Doutoranda em Direito Ambiental pela Universidade do Estado do Amazonas – UEA

REMUNOM
ISSN 2178-6925

**Received:** 25/01/2026 - **Accepted:** 10/03/2026
**Vol**: 13.02
**DOI**: 10.66104/bsgn8v13
**Pages:** 1-26

## Resumo

O cenário contemporâneo das transações financeiras no Brasil é caracterizado pela ascensão de ilícitos digitais, cuja complexidade é amplificada pela contínua inovação tecnológica criminal. Diante desse panorama, o objetivo central desta análise é examinar o Mecanismo Especial de Devolução (MED) e sua evolução, o MED 2.0, investigando em que medida a automação e o aprimoramento da governança institucional potencializam a probabilidade e a celeridade na recuperação de ativos e dissuadem novas modalidades de golpes, fortalecendo a resiliência do ecossistema de pagamentos instantâneos. A metodologia consiste em uma pesquisa documental, de natureza qualitativa e descritivo-interpretativa. A coleta de dados baseou-se na leitura sistemática de documentos oficiais, com extração de estatísticas e conceitos-chave, seguida de categorização temática e análise de conteúdo. Os resultados indicam que o MED 2.0 apresenta-se como uma evolução promissora ao estender o bloqueio de recursos a contas de múltiplas camadas, integrar motores de risco e fortalecer a cooperação interinstitucional. Contudo, sua efetividade condiciona-se à calibração adequada de limites e prazos operacionais, à garantia da qualidade dos dados, à transparência procedimental, à educação do usuário e à estrita conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD). Conclui-se que o mecanismo aprimorado possui um potencial significativo para reduzir o valor esperado dos golpes financeiros, elevando a resiliência e a segurança de todo o sistema pix de pagamentos.

**Palavras-chave:** Pix; Mecanismo Especial de Devolução; Fraudes Eletrônicas; Governança; Cibersegurança.

## Abstract

The contemporary landscape of financial transactions in Brazil is characterized by the rise of digital illicit acts, whose complexity is amplified by continuous criminal technological innovation. Against this backdrop, the central objective of this analysis is to examine the Special Return Mechanism (MED) and its evolution, MED 2.0, investigating to what extent automation and the improvement of institutional governance enhance the probability and speed of asset recovery and deter new types of fraud, thereby strengthening the resilience of the instant payment ecosystem. The methodology consists of qualitative, descriptive-interpretative documentary research. Data collection was based on the systematic reading of official documents, involving the extraction of statistics and key concepts, followed by thematic categorization and content analysis. Results indicate that MED 2.0 represents a promising evolution by extending the freezing of funds to multi-layer accounts, integrating risk engines, and strengthening inter-institutional cooperation. However, its effectiveness is conditioned on the proper calibration of operational limits and deadlines, guaranteed data quality, procedural transparency, user education, and strict compliance with the General Personal Data Protection Law (LGPD). It is concluded that the improved mechanism has significant potential to reduce the expected value of financial crimes, increasing the resilience and security of the entire Pix payment system.

**Keywords:** Pix; Special Return Mechanism; Electronic Fraud; Governance; Cybersecurity.

## Resumen

El escenario contemporáneo de las transacciones financieras en Brasil se caracteriza por el ascenso de ilícitos digitales, cuya complejidad se ve amplificada por la continua innovación tecnológica criminal. Ante este panorama, el objetivo central de este análisis es examinar el Mecanismo

REMUNOM
ISSN 2178-6925

**Received:** 25/01/2026 - **Accepted:** 10/03/2026
**Vol**: 13.02
**DOI**: 10.66104/bsgn8v13
**Pages:** 1-26

Especial de Devolución (MED) y su evolución, el MED 2.0, investigando en qué medida la automatización y el perfeccionamiento de la gobernanza institucional potencian la probabilidad y la celeridad en la recuperación de activos y disuaden nuevas modalidades de fraude, fortaleciendo la resiliencia del ecosistema de pagos instantáneos. La metodología consiste en una investigación documental, de naturaleza cualitativa y descriptivo-interpretativa. La recolección de datos se basó en la lectura sistemática de documentos oficiales, con la extracción de estadísticas y conceptos clave, seguida de categorización temática y análisis de contenido. Los resultados indican que el MED 2.0 se presenta como una evolución prometedora al extender el bloqueo de recursos a cuentas de múltiples capas, integrar motores de riesgo y fortalecer la cooperación interinstitucional. No obstante, su efectividad está condicionada a la adecuada calibración de límites y plazos operativos, a la garantía de la calidad de los datos, a la transparencia procedimental, a la educación del usuario y al estricto cumplimiento de la Ley General de Protección de Datos Personales (LGPD). Se concluye que el mecanismo mejorado posee un potencial significativo para reducir el valor esperado de los fraudes financieros, elevando la resiliencia y la seguridad de todo el sistema de pagos instantáneos Pix.

**Palabras clave:** Pix; Mecanismo Especial de Devolución; Fraudes Electrónicos; Gobernanza; Ciberseguridad.

## 1 INTRODUÇÃO

Nos últimos anos, a crescente digitalização dos serviços financeiros intensificou a proliferação de fraudes eletrônicas em escala global. Autoridades regulatórias e instituições financeiras de diversos países têm implementado medidas para recuperação de valores desviados e prevenção de novos golpes, alinhando-se a práticas internacionais de segurança de pagamentos. No Brasil, essa preocupação se materializou com a criação do Mecanismo Especial de Devolução (MED) do Pix, instituído pelo Banco Central em 2021. Esse mecanismo padroniza procedimentos e prazos para que clientes vítimas de fraudes ou de falhas operacionais solicitem a restituição de valores transferidos indevidamente. Entrou em operação em 16 de novembro de 2021, quando o Pix completou um ano de funcionamento, e passou a exigir que as instituições financeiras bloqueiem recursos suspeitos de fraude até a primeira conta recebedora informada pelo cliente vítima.

O MED veio fortalecer a proteção ao consumidor e reduzir a propagação de golpes, um problema que afeta milhões de brasileiros. A existência de um canal estruturado de devolução aumenta a confiança da população em geral no sistema

REMUNOM
ISSN 2178-6925

**Received:** 25/01/2026 - **Accepted:** 10/03/2026
**Vol**: 13.02
**DOI**: 10.66104/bsgn8v13
**Pages:** 1-26

de pagamentos digitais, sendo especialmente relevante para pessoas de menor renda ou menos instruídas financeiramente, que não contam com soluções complexas de seguros ou suporte jurídico imediato. Ao facilitar a retomada de valores perdidos, o MED colabora para diminuir o impacto social das fraudes, que normalmente levam a endividamento ou insegurança financeira. Essa proteção adicional também estimula a inclusão financeira, já que potenciais pessoas que hesitavam em adotar o Pix por medo de golpes passam a ter maior segurança ao saberem que existe um recurso formal de devolução. A padronização das regras garante ainda tratamento justo e uniforme a todos, independentemente da instituição, o que é um ganho para a transparência e equidade do mercado.

Na busca de aperfeiçoar a segurança, foi lançado o MED 2.0, que amplia o alcance do rastreamento de recursos, permitindo não só o bloqueio da primeira conta destino, mas também de camadas subsequentes de transferências relacionadas ao golpe. Essa evolução envolve integração tecnológica entre instituições financeiras e sistemas de análise de transações, com vistas a automatizar detecções de padrões suspeitos e agilizar o trâmite de devoluções. Em golpes via Pix com esquemas de engenharia social que induzem a vítima a gerar pagamentos fraudulentos, o MED permite às vítimas solicitar o estorno dos valores transferidos somente da conta destino. O MED 2.0 aumenta essa eficácia, identificando contas intermediárias utilizadas por fraudadores e bloqueando múltiplas etapas do fluxo criminoso. Este aprimoramento veio para reforçar a proteção contra crimes eletrônicos, como golpes via Pix, e aumentar a eficácia no bloqueio de recursos ilícitos e na devolução de quantias às vítimas, contribuindo de forma objetiva para a segurança pública, pois desestimula a atuação de quadrilhas digitais e reforça a confiança da população em transações eletrônicas.

Neste contexto, emerge o problema sobre a sua real eficácia: em que medida a automação e a governança do MED 2.0 aumentam a probabilidade e a velocidade de recuperação de valores, reduzem a taxa de perdas líquidas por fraude e produzem efeitos dissuasórios sobre a incidência e a sofisticação das

REMUNOM
ISSN 2178-6925

**Received:** 25/01/2026 - **Accepted:** 10/03/2026
**Vol**: 13.02
**DOI**: 10.66104/bsgn8v13
**Pages:** 1-26

fraudes eletrônicas, considerando a heterogeneidade entre instituições financeiras e possíveis efeitos indesejados e deslocamento do crime para outros canais? Esta pesquisa busca responder à pergunta central: O MED 2.0, com seus aprimoramentos de automação e governança, é eficaz para reduzir perdas e dissuadir novas modalidades de fraudes eletrônicas no ecossistema de pagamentos instantâneos no Brasil?

Concomitantemente, a evolução do Mecanismo Especial de Devolução, de sua implantação inicial à versão 2.0, reflete o esforço contínuo do Brasil em acompanhar padrões internacionais de combate a fraudes financeiras, equilibrando inovação tecnológica e governança para melhor proteger as pessoas. O Mecanismo Especial de Devolução do Pix representa um reforço estrutural à segurança do sistema de pagamentos instantâneos brasileiro. Espera-se que essas melhorias aumentem a confiança no sistema de pagamentos instantâneos e reduzam as perdas financeiras associadas a fraudes. Projeta-se que, com a automação e governança reforçadas no MED 2.0, o tempo de resposta às solicitações de devolução seja menor e a taxa de recuperação de valores seja maior, atuando ainda como fator de dissuasão para novos modos de golpe eletrônico.

Diante desse cenário, o presente estudo não busca mensurar empiricamente a eficácia do MED 2.0, dado que sua implementação obrigatória ocorreu recentemente no sistema financeiro brasileiro. O objetivo consiste em analisar institucionalmente a evolução do Mecanismo Especial de Devolução e discutir, à luz da literatura criminológica e da governança financeira, o potencial do MED 2.0 para ampliar a capacidade de resposta do sistema Pix frente às fraudes eletrônicas. Trata-se, portanto, de uma análise exploratória e interpretativa**,** baseada em evidências documentais e em referenciais teóricos da criminologia econômica e da gestão de risco.

Este artigo está estruturado em cinco seções. Após esta introdução, a seção 2 apresenta o referencial teórico que fundamenta a análise do MED 2.0. A

REMUNOM
ISSN 2178-6925

**Received:** 25/01/2026 - **Accepted:** 10/03/2026
**Vol**: 13.02
**DOI**: 10.66104/bsgn8v13
**Pages:** 1-26

seção 3 detalha a metodologia utilizada na pesquisa. A seção 4 discute os resultados e a análise dos dados. Por fim, a seção 5 apresenta as conclusões do estudo, suas contribuições e sugestões para futuras pesquisas.

## 2 CONSIDERAÇÕES TEÓRICAS SOBRE GOVERNANÇA DO MED 2.0 NA PREVENÇÃO DE GOLPES FINANCEIROS

A literatura sobre pagamentos instantâneos aponta que a irrevogabilidade e a liquidação em tempo real aumentam a eficiência, mas também ampliam a exposição a fraudes. Nesse cenário, o MED 2.0 buscas reequilibrar incentivos ao tornar mais provável e rápida a recuperação de recursos, reduzindo a recompensa esperada do crime (Banco Central do Brasil, 2025). Este referencial reúne bases teóricas e evidências para avaliar a eficácia da automação e da governança do MED 2.0 na redução de perdas e na dissuasão de novas fraudes.

### 2.1 Conceitos e Evolução do Mecanismo Especial de Devolução (MED)

Hipóteses centrais e modelos conceituais analíticos sustentam que automação e governança robusta aumentam a probabilidade de bloqueio e devolução em tempo útil, ao mesmo tempo em que reduzem a assimetria de informação entre os participantes do sistema de pagamentos. Conceitualmente, o Mecanismo Especial de Devolução (MED) pode ser definido como um arranjo institucional de pronta resposta a incidentes de fraudes e golpes no ecossistema de pagamentos instantâneos, com mensagens padronizadas, prazos, papéis e critérios de elegibilidade para devolução de valores em fraudes e falhas operacionais (Banco Central do Brasil, 2021).

A diferença conceitual mais relevante entre o MED original e o MED 2.0 reside no ponto de atuação do mecanismo. Na configuração anterior, a efetividade dependia fortemente da possibilidade de reter valores ainda disponíveis na primeira

REMUNOM
ISSN 2178-6925

**Received:** 25/01/2026 - **Accepted:** 10/03/2026
**Vol**: 13.02
**DOI**: 10.66104/bsgn8v13
**Pages:** 1-26

conta recebedora do Pix. Esse desenho mostrava desempenho relativamente melhor em eventos nos quais o valor permanecia temporariamente parado, mas era estruturalmente menos eficaz contra fraudes profissionalizadas. Nelas, a conta inicialmente utilizada funciona como conta de passagem (laranja), sendo rapidamente esvaziada por meio de sucessivas transferências, pulverização em diversos destinatários, saques ou conversões, o que reduzia drasticamente a chance de recuperação (Banco Central do Brasil, 2021).

O MED 2.0 altera esse cenário ao permitir que o rastreio do dinheiro, em casos de fraude ou golpe, ultrapasse a primeira conta recebedora, acompanhando todo o fluxo financeiro e viabilizando bloqueios em contas sucessoras (Banco Central do Brasil, 2025). Do ponto de vista da efetividade, essa mudança é decisiva porque enfrenta o principal vetor de evasão do MED anterior, a dissipação rápida. Ao não limitar a contenção ao primeiro recebedor, o MED 2.0 tende a elevar a probabilidade de localizar e reter saldo em algum elo da cadeia, mesmo quando o valor já foi repassado. Em termos sistêmicos, isso aumenta o custo operacional do crime, pois o fraudador precisa ampliar a complexidade da movimentação para tentar escapar dos bloqueios ao longo do percurso (Federação Brasileira de Bancos, 2024).

A comparação entre as duas versões também deve considerar o papel do tempo na dinâmica das fraudes com Pix. Embora o MED 2.0 estabeleça que o valor pode ser devolvido em até 11 dias após a contestação (Federação Brasileira de Bancos, 2024), a efetividade material não depende apenas do prazo final de devolução, mas principalmente do tempo até a contenção inicial. Em golpes via Pix, a janela crítica costuma ser de minutos ou poucas horas, pois a dissipação ocorre rapidamente para reduzir a rastreabilidade e a disponibilidade do saldo. Assim, o ganho real do MED 2.0 decorre de sua capacidade de atuar em cadeia, mesmo que a resolução formal leve dias, a chance de devolução aumenta se houver bloqueios oportunos em contas sucessoras antes que o dinheiro seja totalmente pulverizado (Banco Central do Brasil, 2025).

REMUNOM
ISSN 2178-6925

**Received:** 25/01/2026 - **Accepted:** 10/03/2026
**Vol**: 13.02
**DOI**: 10.66104/bsgn8v13
**Pages:** 1-26

No plano prático, a vantagem do MED 2.0 aparece com maior nitidez nos golpes de engenharia social como falso suporte, falsa central e falso atendimento, justamente porque estes se apoiam tipicamente em transferências imediatas seguidas de repasses sucessivos. No MED original, esvaziar a primeira conta era, muitas vezes, suficiente para frustrar a recuperação (Banco Central do Brasil, 2021). No MED 2.0, esse expediente deixa de ser uma estratégia de escape tão eficaz, porque as contas que recebem os repasses passam a estar no raio de ação do mecanismo. Como consequência, espera-se um aumento da taxa de bloqueio efetivo em algum ponto do percurso e, portanto, a elevação da taxa de recuperação em casos nos quais o dinheiro ainda permaneça dentro do sistema bancário em contas rastreáveis (Banco Central do Brasil, 2025).

Em síntese, ao comparar o MED original ao MED 2.0, observa-se uma mudança de paradigma, a transição de um mecanismo cuja eficácia era frequentemente neutralizada pela rapidez da dissipação para um desenho que busca recuperar a capacidade de resposta por meio do rastreio ampliado e da possibilidade de bloqueios ao longo da cadeia de transferências. A expectativa de maior efetividade é tecnicamente consistente com a lógica dos golpes predominantes no Pix, porque atinge precisamente o método mais utilizado para reduzir a chance de devolução e a circulação veloz por contas sucessoras (Banco Central do Brasil, 2025).

## 2.2 Teorias da Criminologia e Prevenção de Fraudes

Para além da compreensão de Golpes e fraudes Eletrônicas no Brasil, a literatura exige uma fundamentação teórica sólida que abranja a criminologia organizacional, a economia do crime e a sociologia das redes digitais. Para Shelley (2014) e Albanese (2016), o crime organizado, tradicionalmente definido por sua estrutura hierárquica, divisão de trabalho e busca por lucro através de atividades ilícitas, tem demonstrado uma notável capacidade de adaptação às transformações tecnológicas e sociais. O advento e a massificação da internet e das tecnologias digitais não apenas criaram novos vetores para

REMUNOM
ISSN 2178-6925

**Received:** 25/01/2026 - **Accepted:** 10/03/2026
**Vol**: 13.02
**DOI**: 10.66104/bsgn8v13
**Pages:** 1-26

a criminalidade, mas também reconfiguraram as dinâmicas financeiras e operacionais de grupos criminosos.

Neste sentido, a literatura sobre cibersegurança e cibecrime de Wall (2008) e Kshetri (2010) detalham a proliferação de vetores de ataque, como phishing, ransomware, fraudes de engenharia social e o uso de dark web para comercialização de dados e ferramentas ilícitas. Estes mecanismos não apenas geram lucro direto, mas também servem como ferramentas para a lavagem de dinheiro, dificultando o rastreamento e a apreensão de ativos.

Somado a isso, a teoria da Gestão de Risco, Incerteza e Lucro, apresenta um conjunto de princípios e métodos para identificar, analisar, avaliar, tratar e monitorar riscos. O objetivo é minimizar perdas potenciais e maximizar oportunidades, adaptando-se a um ambiente em constante mudança (Knight, 1921).

Ademais, ao mapear os riscos nas instituições Públicas, a aplicação dessa teoria permite propor diretrizes e boas práticas para agilizar o desenvolvimento de um conjunto de princípios e métodos para lidarem com as ameaças. Que nos leva a identificar os novos tipos de fraudes e suas variações impulsionadas por inteligência artificial, que no Brasil enfrenta, clonagem de voz, deepfakes em extorsões, engenharia social em massa e a probabilidade de ocorrência de cada tipo de fraude tendo impacto potencial financeiro, psicológico, reputacional, na confiança nas instituições.

Somado a isso, a teoria da escolha racional e a criminologia da economia do crime, ofensores avaliam benefícios esperados versus custos, probabilidade de captura, severidade e celeridade da sanção. Ao elevar a certeza e a rapidez de bloqueio e devolução, o MED 2.0 reduz o valor esperado do crime. A governança, ao padronizar procedimentos e impor *compliance* entre instituições financeiras, reduz brechas exploratórias e variações que criminosos poderiam arbitrar entre estas instituições (Cornish; Clarke, 1986).

Da mesma forma, a teoria da atividade rotineira enfatiza a convergência entre ofensor, alvo adequado e ausência de guardião. O MED 2.0, enquanto

REMUNOM
ISSN 2178-6925

**Received:** 25/01/2026 - **Accepted:** 10/03/2026
**Vol**: 13.02
**DOI**: 10.66104/bsgn8v13
**Pages:** 1-26

guardião formal, introduz controles que alteram o ambiente transacional, diminuindo a adequação do alvo e, por extensão, a oportunidade. A prevenção situacional, por sua vez, informa intervenções para elevar o esforço, aumentar o risco e reduzir a recompensa e as justificativas do ofensor (Cohen; Felson, 2010).

Em síntese, a articulação dessas bases teóricas evidencia que, embora o crime organizado tenha se adaptado ao ambiente digital explorando novas tecnologias e inteligência artificial para maximizar lucros e contornar a detecção, o enfrentamento institucional ganha robustez com ferramentas como o MED 2.0. Sob a ótica da Gestão de Risco e da Criminologia, o mecanismo atua de forma multidimensional, funciona como um guardião formal que altera a dinâmica da atividade rotineira, diminuindo a oportunidade e a atratividade do alvo, simultaneamente, incide sobre a escolha racional do ofensor, desequilibrando a relação de custo benefício da fraude. Ao garantir celeridade e certeza no rastreio e bloqueio de ativos, o MED 2.0 materializa os princípios da dissuasão, esvaziando a viabilidade econômica das campanhas criminosas e fortalecendo a resiliência de todo o ecossistema financeiro e tecnológico.

## 2.3 Gestão de Risco, Governança e Ética Algorítmica

A gestão de risco operacional e resiliência destacam que perdas decorrem de falhas de processos, pessoas, sistemas e eventos externos. A automação do MED 2.0 reduz variância de execução e lista priorizada de tarefas manual, mitigando erros e atrasos. A integração com *frameworks* de continuidade de negócios e de resposta a incidentes fortalece a resiliência, ao permitir escalonamento e contenção coordenados durante ondas de ataque (Federação Brasileira de Bancos, 2024).

A literatura regulatória recomenda abordagens responsivas, nas quais supervisores calibram exigências com base no risco e no desempenho das

REMUNOM
ISSN 2178-6925

**Received:** 25/01/2026 - **Accepted:** 10/03/2026
**Vol**: 13.02
**DOI**: 10.66104/bsgn8v13
**Pages:** 1-26

instituições. O MED 2.0 é consistente com princípios de proporcionalidade e compromisso com o alcance de metas, pois permite medir e comparar indicadores de eficácia entre participantes, aplicando incentivos, penalidades e suporte técnico de forma direcionada para elevar a linha de base do ecossistema.

Os modelos de justiça procedimental sustentam que transparência, voz e consistência nas decisões elevam a confiança e a adesão às regras. Ao fornecer trilhas de auditoria e critérios claros de elegibilidade para devolução, o MED 2.0 tende a reforçar a percepção de justiça, preservando legitimidade e reduzindo contestações. Essa confiança é um ativo de segurança, pois amplia a colaboração das vítimas na sinalização de incidentes.

A literatura alerta que controles bem-sucedidos podem deslocar o crime para modalidades adjacentes ou para segmentos mais vulneráveis. A governança do MED 2.0 deve, portanto, incluir monitoramento de segunda ordem, com painéis que rastreiem mudanças no mix de golpes, geografias e perfis de vítima, antecipando contramedidas e inibindo ciclos de inovação criminosa (Idec, 2024).

A conformidade com princípios de minimização de dados, finalidade e segurança é condição para a legitimidade do MED 2.0. A literatura de ética algorítmica recomenda avaliações de impacto, testes de viés e mecanismos de contestação. O equilíbrio entre compartilhamento de sinais e proteção de dados pessoais exige técnicas de agregação, pseudonimização e controles de acesso, sob governança clara de papéis e responsabilidades.

Em síntese, as implicações para pesquisa aplicada do corpo teórico indicam que a eficácia do MED 2.0 repousa na conjunção de automação de alta velocidade, governança multilateral com a responsabilização e o compromisso com o alcance de metas e ciclos rápidos de aprendizado. Pesquisas futuras devem quantificar elasticidades de dissuasão por modalidade, estimar custos de oportunidade de atrito legítimo e avaliar a robustez do arranjo frente a choques coordenados. A maturidade do mecanismo depende de sua capacidade de manter proporcionalidade, transparência e desempenho mensurável ao longo do tempo.

REMUNOM
ISSN 2178-6925

**Received:** 25/01/2026 - **Accepted:** 10/03/2026
**Vol**: 13.02
**DOI**: 10.66104/bsgn8v13
**Pages:** 1-26

## 3 ASPECTOS METODOLÓGICOS

Esta pesquisa caracteriza-se como um estudo qualitativo de natureza exploratória e interpretativa, fundamentado em análise documental. O objetivo é examinar a evolução institucional do Mecanismo Especial de Devolução (MED) e discutir as implicações do MED 2.0 no contexto da governança do sistema Pix e da prevenção de fraudes eletrônicas.

O corpus documental foi composto por quatro categorias de fontes:
(i) normativos e documentos regulatórios, especialmente resoluções do Banco Central do Brasil relacionadas ao funcionamento do Pix e ao Mecanismo Especial de Devolução;
(ii) relatórios institucionais e estudos setoriais, produzidos por entidades como a Federação Brasileira de Bancos (Febraban), o Instituto Brasileiro de Defesa do Consumidor (Idec) e o Fórum Brasileiro de Segurança Pública;
(iii) estudos técnicos e relatórios de mercado sobre fraudes financeiras digitais e cibercrime;
(iv) literatura acadêmica relacionada à criminologia econômica, economia do crime, governança financeira e cibersegurança.

A seleção das fontes seguiu critérios de relevância temática, atualidade regulatória e disponibilidade pública, priorizando documentos publicados entre 2021 e 2025, período correspondente à criação do MED e ao desenvolvimento do MED 2.0.

O procedimento analítico adotado combinou análise temática e análise de conteúdo, estruturadas em três etapas:

REMUNOM
ISSN 2178-6925

**Received:** 25/01/2026 - **Accepted:** 10/03/2026
**Vol**: 13.02
**DOI**: 10.66104/bsgn8v13
**Pages:** 1-26

1. Leitura exploratória e identificação das principais categorias analíticas;

2. Codificação temática dos documentos, organizando os dados em quatro eixos: evolução institucional do MED, dinâmica das fraudes eletrônicas, governança regulatória e mecanismos de dissuasão criminal;

3. Comparação cruzada entre fontes regulatórias, relatórios institucionais e literatura acadêmica, buscando identificar convergências, divergências e lacunas interpretativas.

Considerando que o MED 2.0 entrou em fase obrigatória apenas em fevereiro de 2026, o estudo não pretende testar empiricamente seus resultados, mas sim discutir sua plausibilidade institucional e seus possíveis impactos à luz de referenciais teóricos e evidências documentais disponíveis.

## 4 A EFICÁCIA DO MED 2.0 NA DISSUASÃO DAS FRAUDES ELETRÔNICAS NO BRASIL

Esta seção apresenta uma análise interpretativa e prospectiva do papel do Mecanismo Especial de Devolução no enfrentamento das fraudes eletrônicas no Brasil. Considerando que a implementação obrigatória do MED 2.0 ocorreu recentemente, a discussão baseia-se em dados documentais sobre fraudes digitais, na avaliação das limitações do modelo original do MED e na análise institucional das mudanças introduzidas pela nova arquitetura regulatória.

### 4.1 Panorama das Fraudes Eletrônicas no Brasil

O Brasil enfrenta uma epidemia nacional de golpes e fraudes digitais, um fenômeno que se intensifica com o avanço tecnológico e a crescente engenhosidade dos criminosos. A complexidade e a gravidade dos crimes

REMUNOM
ISSN 2178-6925

**Received:** 25/01/2026 - **Accepted:** 10/03/2026
**Vol**: 13.02
**DOI**: 10.66104/bsgn8v13
**Pages:** 1-26

cibernéticos têm aumentado, impulsionadas pela criação de ambientes virtuais falsos, engenharia social hiperpersonalizada e, notavelmente, pelo uso de Inteligência Artificial. Além disso, a criminalidade digital tem demonstrado uma migração estratégica do ambiente físico para o digital.

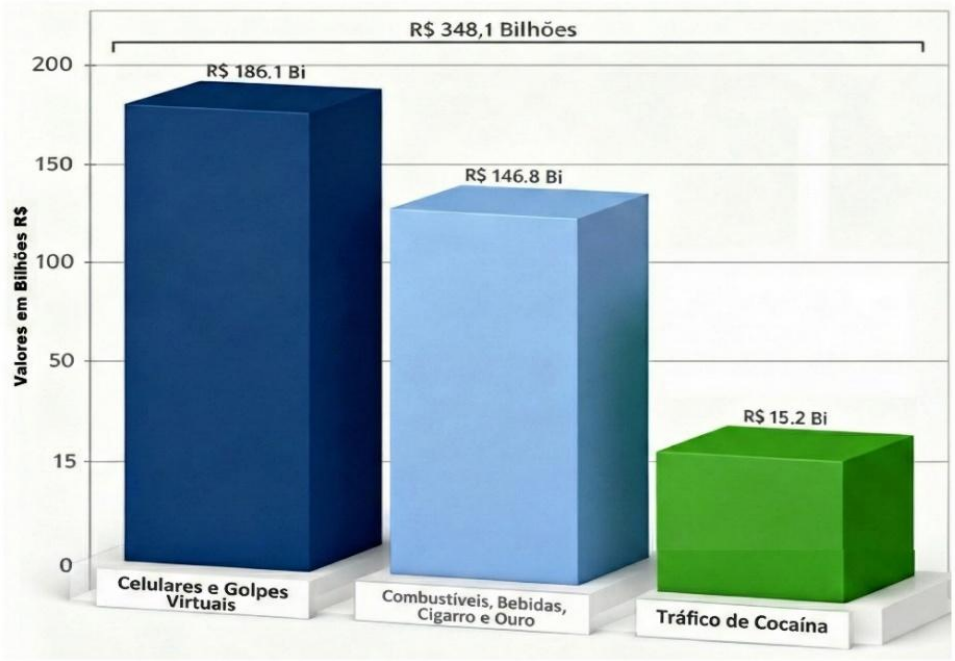
Uma pesquisa intitulada *Follow the Products: Rastreamento de Produtos e enfrentamento ao Crime Organizado no Brasil*, conduzida pelo Fórum Brasileiro de Segurança Pública em 2025, analisa as novas fronteiras econômicas do crime organizado. Por meio de dados de apreensões, revisão de literatura especializada e entrevistas em profundidade com especialistas dos setores público e privado, o estudo avalia os impactos dos mercados ilícitos na arrecadação tributária, na segurança pública e no meio ambiente. Como principal estratégia de mitigação, o documento destaca o rastreamento de produtos como uma ferramenta essencial para descapitalizar essas organizações.

O documento destaca o rastreamento de produtos como estratégia primordial para descapitalizar organizações criminosas. A análise revela as principais fontes de receita do crime organizado a partir de 2022, abrangendo os mercados de combustíveis, bebidas, cigarros e ouro, bem como os crimes virtuais e furtos de celulares, que geraram receitas significativas. O estudo também estima os rendimentos provenientes do tráfico de cocaína, consolidando uma análise abrangente das atuais fontes de financiamento dessas organizações (Nascimento; Pazinato, 2025).

REMUNOM
ISSN 2178-6925

**Received:** 25/01/2026 - **Accepted:** 10/03/2026
**Vol**: 13.02
**DOI**: 10.66104/bsgn8v13
**Pages:** 1-26

Gráfico 1: Receita estimada do crime organizado no Brasil (2022-2024)




Fonte: Follow the products: rastreamento de produtos e enfrentamento ao crime organizado no Brasil

À luz do exposto, o Gráfico 1, detalha a receita estimada do crime organizado por produtos selecionados entre os anos de 2022 e 2024, onde depreende-se que a categoria Celulares e Golpes Virtuais emerge como a principal, com aproximadamente R$ 186,1 bilhões, evidenciando uma drástica e lucrativa migração para o ambiente digital, onde crimes patrimoniais como fraudes e golpes cibernéticos superam as fontes mais tradicionais. Em segundo lugar, a exploração de Combustíveis, Bebidas, Cigarro e Ouro movimenta cerca de R$ 146,8 bilhões, sinalizando uma profunda infiltração do crime organizado em setores lícitos da economia, aproveitando-se de brechas regulatórias e falhas de fiscalização para gerar receita através de sonegação, contrabando, falsificação e adulteração (Nascimento; Pazinato, 2025).

Não obstante, em contraste marcante com as duas primeiras categorias, o Tráfico de Cocaína, historicamente visto como a principal fonte de renda do crime organizado, representa a menor parcela, com uma estimativa de R$ 15,2 bilhões. Os dados apresentados, sublinham a urgência de uma reorientação nas estratégias de segurança

REMUNOM
ISSN 2178-6925

**Received:** 25/01/2026 - **Accepted:** 10/03/2026
**Vol**: 13.02
**DOI**: 10.66104/bsgn8v13
**Pages:** 1-26

pública, exigindo uma abordagem multifacetada que não se restrinja ao combate às drogas, mas que se amplie para o enfrentamento dos crimes digitais com a implementação do MED 2.0 e a intensificação do rastreamento de produtos e da inteligência financeira em mercados aparentemente formais.

No entanto, esta migração estratégica do crime para o ambiente digital, onde a escalabilidade e o anonimato são maiores, corrobora a necessidade de mecanismos de defesa igualmente sofisticados, como o MED 2.0, que buscam elevar o custo operacional do crime, conforme preconizado pela teoria da escolha racional (Cornish; Clarke, 1986).

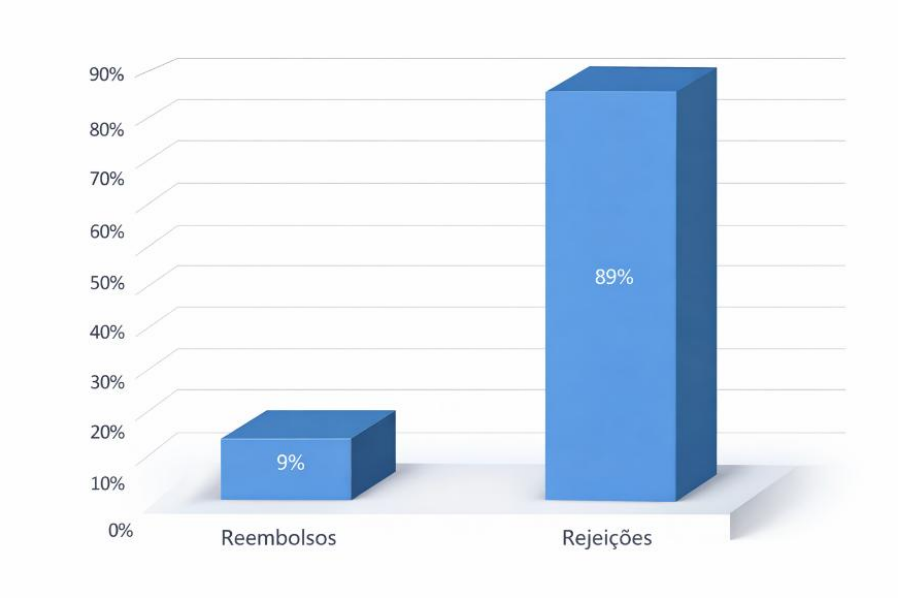
## 4.2 Eficácia do MED e a Transição para o MED 2.0

Em relação ao Pix, o Relatório de Golpes e Fraudes Eletrônicas apresentado pelo Idec (2024) registra um aumento de 43% nas transações fraudulentas entre 2023 e 2024, totalizando R$ 2,7 bilhões em prejuízos no referido biênio. Corroborando com esse cenário se evidencia a crescente demanda pelo Mecanismo Especial de Devolução (MED). As solicitações de reembolso por fraude saltaram de 1,5 milhão, em 2022, para 2,5 milhões, em 2023, atingindo a marca de 1,6 milhão apenas entre janeiro e maio de 2024. Apesar da alta procura, a efetividade do mecanismo se mostrou baixa (Idec, 2024).

REMUNOM
ISSN 2178-6925

**Received:** 25/01/2026 - **Accepted:** 10/03/2026
**Vol**: 13.02
**DOI**: 10.66104/bsgn8v13
**Pages:** 1-26

Gráfico 2: Pedidos de reembolso via Mecanismo Especial de Devolução (2022-2024)




Fonte: Relatório de Golpes e Fraudes Eletrônicas apresentado pelo Idec (2024).

Do Gráfico 2 depreende-se, que os dados disponibilizados pelo Idec (2024), referentes aos anos de 2022 a 2024 evidenciam uma assimetria significativa na eficácia do Mecanismo Especial de Devolução (MED) em sua formatação original. Com uma taxa de rejeição de 89% frente a apenas 9% de solicitações efetivamente reembolsadas, constata-se que a ferramenta enfrenta severas limitações operacionais na mitigação de perdas

Essa discrepância não decorre necessariamente de falhas sistêmicas na recepção das denúncias, mas sim da velocidade com que os agentes criminosos promovem a pulverização dos ativos ilícitos. A alta taxa de rejeição reflete, em grande medida, o esvaziamento imediato da conta recebedora primária. Ao utilizar redes de contas laranja para realizar a rápida triangulação e o saque dos valores, os infratores conseguem exaurir o saldo antes que a vítima perceba a fraude e o bloqueio cautelar seja efetivado pela instituição financeira.

REMUNOM
ISSN 2178-6925

**Received:** 25/01/2026 - **Accepted:** 10/03/2026
**Vol**: 13.02
**DOI**: 10.66104/bsgn8v13
**Pages:** 1-26

Este cenário corrobora a insuficiência do rastreamento de camada única, limitado à primeira conta de destino, que justificou a urgência de aprimoramentos no ecossistema de pagamentos. Fica demonstrado que a eficácia na recuperação patrimonial exige arranjos mais sofisticados, fundamentando a necessidade de transição para o MED 2.0, cuja arquitetura propõe o alcance das camadas subsequentes de transferência para interromper a cadeia de lavagem de dinheiro e descapitalizar as organizações criminosas.

A implementação do MED 2.0 na fase de adequação, facultativa para os bancos e instituições financeiras, teve início em 23 de novembro de 2025, conforme regulamentado pelo Banco Central do Brasil (2025). Nesta etapa, as instituições puderam aderir de forma opcional aos novos parâmetros de rastreamento de contas e iniciar os testes práticos e de mensageria em seus sistemas. Contudo, a fase definitiva e obrigatória entrou em vigor em 2 de fevereiro de 2026.

A partir desta data, a adoção do MED 2.0 e de suas ferramentas de rastreamento em múltiplas camadas passou a ser exigida para todos os participantes do Pix (Banco Central do Brasil, 2025). Vale pontuar que, embora a obrigatoriedade tenha começado em fevereiro de 2026, o Banco Central do Brasil (2025) estabeleceu um período de transição e estabilização técnica que irá até maio de 2026. Esse prazo foi concedido para que os bancos concluam os ajustes finais de integração sistêmica antes do início da fiscalização plena.

## 4.3 Tipologia dos Golpes e Vulnerabilidades Humanas

Nesse contexto, a *fintech* de proteção financeira digital Silverguard (2024) conduziu um estudo abrangente sobre a incidência de fraudes envolvendo o Pix no Brasil. Concluída em agosto de 2023, a pesquisa estruturou-se em três fases metodológicas. A primeira consistiu no levantamento de dados do Banco Central, obtidos via Lei de Acesso à Informação, referentes ao uso do Mecanismo Especial de Devolução (MED) entre dezembro de 2021 e maio de 2023. A segunda etapa

REMUNOM
ISSN 2178-6925

**Received:** 25/01/2026 - **Accepted:** 10/03/2026
**Vol**: 13.02
**DOI**: 10.66104/bsgn8v13
**Pages:** 1-26

baseou-se em uma pesquisa quantitativa com 1.910 entrevistas *on-line*, realizadas entre junho e julho de 2023, contemplando uma amostra demograficamente diversa em termos de faixa etária, gênero, classe social e região geográfica. Por fim, a terceira fase analisou 5.000 denúncias registradas entre maio e julho de 2023 no serviço de apoio a vítimas SOS Golpe, mantido pela própria instituição (Silverguard, 2025).

A partir desse cruzamento de dados empíricos, o estudo traçou uma radiografia detalhada das tipologias criminais, dos perfis das vítimas e do *modus operandi* dos fraudadores. Os resultados apontam que, apenas em 2022, os brasileiros sofreram 1,7 milhão de golpes financeiros via Pix, evidenciando que quatro em cada dez usuários já vivenciaram alguma tentativa de fraude na plataforma. O relatório conclui que a alta taxa de sucesso dessas infrações que atingem vítimas independentemente de gênero ou idade decorre fundamentalmente do uso refinado da engenharia social, estruturada em narrativas persuasivas, bem elaboradas e altamente contextualizadas.

Segundo a Silverguard (2025), o aplicativo de mensagens Whatsapp destaca-se como o principal ponto de origem das fraudes envolvendo o sistema Pix no Brasil, seguido por uma incidência considerável de casos iniciados nas plataformas Instagram e Facebook. O levantamento evidencia, ainda, uma clara assimetria geracional na vitimização. As redes sociais constituem o vetor predominante para os golpes aplicados contra a população mais jovem, cujas fraudes ocorrem frequentemente via Instagram ou Facebook. Em contrapartida, a incidência de estelionatos e fraudes eletrônicas originadas nestas plataformas é substancialmente menor entre os indivíduos idosos.

REMUNOM
ISSN 2178-6925

**Received:** 25/01/2026 - **Accepted:** 10/03/2026
**Vol**: 13.02
**DOI**: 10.66104/bsgn8v13
**Pages:** 1-26

Gráfico 3: Fraudes por aplicativos

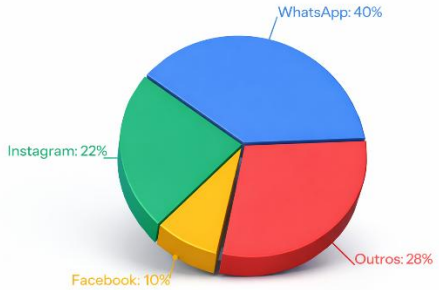
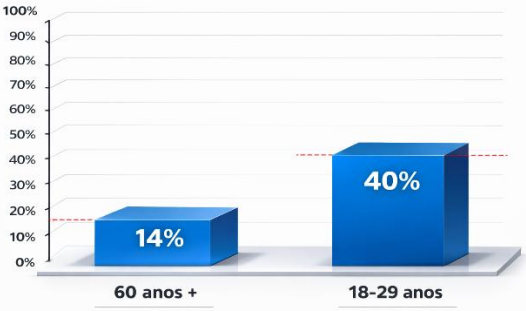



Gráfico 4: Fraudes nas redes por faixa etária (Instagram / Facebook)




Fonte: fintech de proteção financeira digital Silverguard (2025).

Conforme ilustram os dados dos Gráficos 3 e 4, que detalham os canais de contato preferenciais dos fraudadores e o perfil etário das vítimas, o Whatsapp consolida-se como o principal vetor de ataque, concentrando 40% das ocorrências. Na sequência, figuram o Instagram (22%) e o Facebook (10%). O cruzamento desses dados evidencia uma expressiva disparidade geracional, enquanto o Instagram e o Facebook, juntos, representam a origem de 40% das fraudes contra jovens de 18 a 29 anos, essa proporção cai para apenas 14% entre os indivíduos com 60 anos ou mais.

Apesar da expressividade desses números, a Silverguard (2025) estima que a incidência real seja de três a quatro vezes maior em virtude de uma crônica subnotificação. A pesquisa revela que apenas 45% das vítimas registram Boletim de Ocorrência e um terço sequer tenta reaver o prejuízo, frequentemente por desinteresse em quantias menores ou por desconhecimento dos trâmites de proteção. Essa desinformação é corroborada pela constatação de que 90% dos brasileiros ignoram o funcionamento do MED, sendo que 63% nunca ouviram falar da ferramenta (Silverguard, 2024).

REMUNOM
ISSN 2178-6925

**Received:** 25/01/2026 - **Accepted:** 10/03/2026
**Vol**: 13.02
**DOI**: 10.66104/bsgn8v13
**Pages:** 1-26

Em uma perspectiva macro, esse cenário reflete uma adaptação estratégica do crime organizado, caracterizada pela transição sistêmica do ambiente físico para o digital. Conforme aponta o Relatório de Golpes e Fraudes Eletrônicas da Silverguard (2025). Observou-se um aumento de 13,6% nos estelionatos virtuais, em contrapartida à redução dos crimes patrimoniais físicos. Essa migração é impulsionada pela percepção de menor risco e pela alta escalabilidade das fraudes no ciberespaço.

Tendo em vista que essas operações ilícitas frequentemente ocorrem em ambientes virtuais fechados como grupos de aplicativos de mensagens, a detecção e o monitoramento tornam-se altamente complexos. Isso não apenas reforça a subestimativa das estatísticas criminais oficiais, mas também exige que as autoridades de segurança pública desenvolvam estratégias investigativas substancialmente mais sofisticadas.

A prevalência de golpes de engenharia social demonstra que a vulnerabilidade reside frequentemente no fator humano. Criminosos exploram a confiança, o senso de urgência e a desinformação, utilizando táticas como *spoofing* para conferir legitimidade a abordagens fraudulentas. O golpe do Pix errado, descrito no relatório de golpes e fraudes eletrônicas, é um exemplo claro de como mecanismos de proteção como o MED podem ser manipulados para perpetrar fraudes duplas, subvertendo a finalidade original da ferramenta e minando a confiança no sistema. Esta análise reforça a teoria da atividade rotineira (Cohen; Felson, 1979), que destaca a importância da ausência de guardiões e da adequação do alvo para a ocorrência do crime, e a necessidade de estratégias de prevenção situacional que elevem o esforço e o risco para os ofensores.

Em síntese, a análise evidencia que, conquanto o Mecanismo Especial de Devolução (MED) tenha estabelecido um marco inicial na mitigação de perdas no ecossistema Pix, sua arquitetura vigente apresenta lacunas operacionais críticas diante da celeridade e sofisticação das organizações criminosas. Nesse cenário, a implementação do MED 2.0 transcende a ideia de mera atualização tecnológica,

REMUNOM
ISSN 2178-6925

**Received:** 25/01/2026 - **Accepted:** 10/03/2026
**Vol**: 13.02
**DOI**: 10.66104/bsgn8v13
**Pages:** 1-26

consolidando-se como uma necessidade estrutural e imperativa. A urgência dessa transição reside na capacidade do MED 2.0 de promover a rastreabilidade automatizada em múltiplas camadas, combatendo a fragmentação de recursos em contas de passagem, o principal gargalo do modelo atual. Ao elevar a tempestividade do bloqueio e a probabilidade real de recuperação, o novo protocolo altera a matriz de custo-benefício do delito, reduzindo drasticamente a utilidade esperada do crime.

Contudo, a eficácia plena dessa nova governança depende de sua integração a um ecossistema de segurança resiliente, que harmonize o aprimoramento tecnológico, o fortalecimento do arcabouço legal, a cooperação interinstitucional e programas robustos de educação digital para a população. As limitações do estudo, como a dependência de fontes secundárias e a ausência de validação empírica em tempo real, sugerem que futuras pesquisas poderiam se beneficiar de dados primários e estudos de caso para aprofundar a compreensão da eficácia do MED 2.0 em diferentes contextos e tipologias de fraude.

Deste modo, a baixa taxa de reembolso observada no MED original não pode ser atribuída exclusivamente à dinâmica criminosa. Fatores institucionais também desempenham papel relevante, como diferenças operacionais entre instituições financeiras, tempo de resposta na abertura de contestação pelo cliente, qualidade dos mecanismos internos de detecção de fraude e limitações na comunicação interbancária. Essas variáveis indicam que a eficácia do mecanismo depende não apenas de seu desenho regulatório, mas também da capacidade operacional e tecnológica dos participantes do sistema de pagamentos.

## CONCLUSÃO

Este estudo teve como objetivo analisar o cenário das fraudes eletrônicas no Brasil, com especial atenção ao impacto financeiro, à evolução dos *modus operandi* e à eficácia do Mecanismo Especial de Devolução (MED) no contexto do

REMUNOM
ISSN 2178-6925

**Received:** 25/01/2026 - **Accepted:** 10/03/2026
**Vol**: 13.02
**DOI**: 10.66104/bsgn8v13
**Pages:** 1-26

Pix. Os achados revelam um panorama desafiador, marcado por perdas financeiras bilionárias e uma constante sofisticação dos golpes, impulsionada pela migração de atividades criminosas do ambiente físico para o digital e pela exploração de vulnerabilidades humanas e sistêmicas. A agilidade inerente ao Pix, embora revolucionária para pagamentos legítimos, tem sido igualmente aproveitada por criminosos, culminando em um crescimento exponencial das transações fraudulentas.

Nesse contexto, o MED emerge como uma ferramenta crucial, mas com eficácia limitada no seu formato original, dada a baixa taxa de valores reembolsados e a dificuldade de recuperação de fundos já movimentados. A concepção do MED 2.0, buscando maior automação, governança robusta e a capacidade de rastrear e bloquear recursos em múltiplas camadas de triangulação, representa uma contribuição significativa ao campo da segurança de pagamentos. Essa evolução está ancorada em princípios teóricos da criminologia econômica e da prevenção situacional, que sugerem que a certeza e a celeridade do bloqueio e da devolução são fatores chave para dissuadir o comportamento fraudulento, elevando o custo percebido do crime.

A relevância prática do MED 2.0 reside em sua capacidade de superar os desafios impostos pela dinâmica criminal, conforme demonstrado pela análise dos dados de fraudes e pela comparação com o MED original. Contudo, a baixa conscientização pública sobre o mecanismo e a complexidade na comunicação das regras representam barreiras à sua plena efetividade, sublinhando a necessidade de se considerar a dimensão sociotécnica e a justiça procedimental para garantir a adesão e a confiança dos usuários.

Em síntese, a luta contra as fraudes eletrônicas exige uma abordagem integrada e adaptativa, que transcenda a mera resposta tecnológica. É fundamental que as melhorias no MED 2.0 sejam acompanhadas por investimentos contínuos em educação digital para a população, fortalecimento do arcabouço legal e da capacidade investigativa das autoridades, e uma colaboração multissetorial

REMUNOM
ISSN 2178-6925

**Received:** 25/01/2026 - **Accepted:** 10/03/2026
**Vol**: 13.02
**DOI**: 10.66104/bsgn8v13
**Pages:** 1-26

robusta. Apenas por meio de um esforço conjunto e contínuo, capaz de se antecipar às novas táticas criminosas e de construir um ambiente digital pautado na confiança e segurança, será possível mitigar os prejuízos e garantir a integridade do sistema de pagamentos brasileiro.

Como contribuição principal, este estudo oferece uma análise aprofundada da evolução do MED e a justificativa para a implementação do MED 2.0, destacando a importância da automação e da governança na redução de perdas e na dissuasão de fraudes. Além disso, apresenta um panorama atualizado das fraudes eletrônicas no Brasil, com dados e gráficos que ilustram a magnitude do problema e a necessidade de ações eficazes.

Os resultados desta pesquisa devem ser interpretados com cautela, considerando as limitações inerentes a um estudo documental baseado em dados secundários. A análise não permite afirmar empiricamente a eficácia do MED 2.0, mas indica que sua arquitetura institucional possui potencial para ampliar a capacidade de resposta do sistema Pix frente às fraudes eletrônicas. Nesse sentido, o estudo contribui para o debate acadêmico ao oferecer uma interpretação analítica da evolução regulatória do mecanismo e de suas possíveis implicações para a governança da segurança financeira digital.

Para futuras pesquisas, sugere-se a realização de estudos empíricos com dados primários para validar a eficácia do MED 2.0 em tempo real, quantificar a elasticidade da dissuasão por modalidade de golpe e avaliar os impactos distributivos dos falsos positivos. A investigação sobre a efetividade de programas de educação digital para usuários e a análise comparativa com mecanismos de combate a fraudes em outros países também seriam valiosas.

## REFERÊNCIAS

ALBANESE, Jay S. **Organized Crime**: From the Mob to Transnational Organized Crime. New York: Routledge, 2016.

REMUNOM
ISSN 2178-6925

**Received:** 25/01/2026 - **Accepted:** 10/03/2026
**Vol**: 13.02
**DOI**: 10.66104/bsgn8v13
**Pages:** 1-26

BANCO CENTRAL DO BRASIL. **Resolução BCB nº 103, de 8 de junho de 2021**. Altera o Regulamento anexo à Resolução BCB nº 1, de 12 de agosto de 2020, que disciplina o funcionamento do arranjo de pagamentos Pix [instituindo o Mecanismo Especial de Devolução]. Brasília, DF: Banco Central do Brasil, 2021. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=103. Acesso em: 21 fev. 2026.

BANCO CENTRAL DO BRASIL. **Resolução BCB nº 493, de 28 de agosto de 2025**. Altera a Resolução BCB nº 1, de 12 de agosto de 2020, e aprimora os procedimentos operacionais e o Mecanismo Especial de Devolução (MED 2.0). Brasília, DF: Banco Central do Brasil, 2025. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=493. Acesso em: 21 fev. 2026.

COHEN, Lawrence E.; FELSON, Marcus. Social Change and Crime Rate Trends: A Routine Activity Approach (1979). In: **Classics in Environmental Criminology**. 0. ed. [S.l.]: Routledge, 2010. p. 203–232.

CORNISH, Derek B.; CLARKE, Ronald V. **The reasoning criminal: rational choice perspectives on offending**. New York: Springer-Verlag, 1986.

FEDERAÇÃO BRASILEIRA DE BANCOS (FEBRABAN). **Febraban propõe melhorias em ferramenta do Pix para devolução de dinheiro de golpe**. São Paulo: Febraban, 13 jun. 2024. Disponível em: https://portal.febraban.org.br/noticia/4136/pt-br/. Acesso em: 21 fev. 2026.

GERHARDT, Tatiana Engel; SILVEIRA, Denise Toledo. **Métodos de Pesquisa** - Volume 2. [Sl.: s.n.], 2009. Disponível em: files.cercomp.ufg.br . Acesso em: 9 set. 2025. Disponível em: https://lume.ufrgs.br/handle/10183/52806. Acesso em: 21 fev. 2026.

GIL, Antonio Carlos. **Métodos e Técnicas de Pesquisa Social**. [S.l.: s.n.], 1987. Disponível em: https://lume.ufrgs.br/handle/10183/206281. Acesso em: 9 set. 2025.

INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR (IDEC). **Considerações ao Fórum Pix sobre as discussões a respeito do MED 2.0**. São Paulo: Idec, 12 ago. 2024. Disponível em: https://idec.org.br/publicacao/consideracoes-ao-forum-pix-sobre-discussoes-respeito-do-med-20. Acesso em: 21 fev. 2026.

KNIGHT, Frank H. **Risk, uncertainty and profit**. Boston: Houghton Mifflin, 1921.

REMUNOM
ISSN 2178-6925

**Received:** 25/01/2026 - **Accepted:** 10/03/2026
**Vol**: 13.02
**DOI**: 10.66104/bsgn8v13
**Pages:** 1-26

KSHETRI, Nir. **The Global Cybercrime Industry**: Economic, Institutional and Strategic Perspectives. Berlin; Heidelberg: Springer, 2010.

NASCIMENTO, Nivio; PAZINATO, Eduardo (coord.). **Follow the products: rastreamento de produtos e enfrentamento ao crime organizado no Brasil.** São Paulo: Fórum Brasileiro de Segurança Pública, 2025. E-book (PDF). ISBN 978-65-89596-42-4. Disponível em: https://static.poder360.com.br/2025/02/FOLLOW-THE-PRODUCTS-2025-v06-digital_FINAL-1.pdf. Acesso em: 21 fev. 2026.

SHELLEY, Louise I. **Dirty Entanglements**: Corruption, Crime, and Terrorism. Cambridge: Cambridge University Press, 2014.

SILVERGUARD. **Central de Autoatendimento do MED no App**. São Paulo: Silverguard, [2025]. Disponível em: https://www.silverguard.com.br/autoatendimento-med-app. Acesso em: 9 set. 2025.

SILVERGUARD. **Golpes com Pix no Brasil: estudo 2024**. São Paulo: Silverguard, 2024. Disponível em: https://www.silverguard.com.br. Acesso em: 9 set. 2025.

WALL, David S. Cybercrime: **The Transformation of Crime in the Information Age**. Cambridge: Polity Press, 2008.