Walter Faria Consultoria

ClearFi INSTITUTE

Segurança no Mercado Financeiro Brasileiro:

Prevenção a Fraudes, Prevenção à Lavagem de Dinheiro, Segurança Cibernética e Segurança Bancária na Era Digital

Riscos, ameaças, regulação, tecnologias e estratégias para proteção do Sistema Financeiro Nacional



Advancing Trust

Through Innovation, Governance & Education

RESEARCH | ADVISORY | EDUCATION | INNOVATION



Mensagem dos autores

Segurança não é apenas uma questão de tecnologia!

Durante muitos anos, organizações trataram segurança cibernética predominantemente como uma responsabilidade da área de tecnologia.

Investiram em ferramentas, controles, monitoramento, políticas e processos cada vez mais sofisticados. Tudo isso permanece essencial. Mas já não é suficiente.

A superfície de risco das organizações mudou. **Pessoas trabalham de diferentes lugares, decisões são tomadas em ambientes digitais, terceiros acessam informações críticas, ferramentas de inteligência artificial passaram a fazer parte da rotina e ataques exploram não apenas vulnerabilidades técnicas, mas também confiança, comportamento e contexto.**

Nesse novo cenário, vem o questionamento: **Estamos construindo organizações mais controladas ou organizações verdadeiramente mais seguras?**

Uma empresa pode possuir centenas de controles e, ainda assim, permanecer vulnerável quando seus profissionais não conseguem reconhecer uma situação de risco, quando responsabilidades não estão claras ou quando a pressão por velocidade faz com que decisões críticas sejam tomadas sem o julgamento adequado.

É por isso que segurança precisa deixar de ser compreendida exclusivamente como uma disciplina tecnológica. Ela é também uma questão de **governança, comportamento, cultura, liderança e capacidade de decisão**.

O desafio contemporâneo não é simplesmente adicionar novos controles. É construir ambientes nos quais tecnologia, processos e pessoas funcionem como um único sistema de proteção.

Organizações resilientes são aquelas capazes de **reduzir sua exposição, identificar riscos rapidamente, tomar boas decisões sob pressão e responder de maneira coordenada quando algo acontece.**

Essa mudança de perspectiva transforma também a agenda da liderança.

Segurança deixa de ser apenas uma discussão sobre ferramentas e passa a fazer parte das decisões sobre estratégia, operação, reputação, continuidade dos negócios e confiança.

Sumário Executivo

A transformação digital do mercado financeiro brasileiro ampliou eficiência, conveniência e inclusão, mas também trouxe uma nova dinâmica de riscos. A velocidade das transações, a expansão dos canais digitais e o uso crescente de APIs, biometria, computação em nuvem e inteligência artificial aumentaram a complexidade da prevenção a fraudes e ameaças cibernéticas.

Nesse ambiente, segurança financeira deixou de significar apenas proteger sistemas e credenciais. Uma parcela relevante dos golpes explora **engenharia social** para induzir clientes legitimamente autenticados a realizar operações fraudulentas. **O desafio passa a ser não apenas confirmar quem realizou uma transação, mas compreender se aquela operação é compatível com seu comportamento, contexto e intenção legítima**.

A resposta a esse cenário exige uma abordagem integrada entre **identidade, autenticação, inteligência de dados, monitoramento transacional, compartilhamento de informações, resposta e recuperação e educação do cliente**, acompanhada pelo fortalecimento dos mecanismos regulatórios e de segurança do sistema financeiro brasileiro.

A inteligência artificial adiciona uma nova camada de complexidade: ao mesmo tempo que amplia a capacidade de prevenção e detecção, aumenta a escala e a sofisticação dos ataques, incluindo deepfakes, clonagem de voz, engenharia social automatizada e identidades sintéticas.

A tendência é a evolução de modelos centrados em autenticação para uma arquitetura de confiança continuamente verificada, capaz de avaliar, em tempo real, identidade, dispositivo, comportamento, contexto, transação e destinatário.

A principal conclusão deste White Paper é que a **próxima fronteira da segurança bancária será proteger o cliente não apenas contra operações não autorizadas, mas também contra operações autorizadas sob manipulação, fraude ou engenharia social.**

Para a alta administração, isso transforma **fraude e cibersegurança** em uma **agenda estratégica de governança, confiança e resiliência operacional**, exigindo maior integração entre áreas, inteligência em tempo real, colaboração entre instituições e preparação para uma nova geração de ameaças impulsionadas por inteligência artificial.

Transformação do Sistema Financeiro



O sistema financeiro brasileiro tornou-se uma infraestrutura essencialmente digital. A disseminação de aplicativos móveis, pagamentos instantâneos, contratação remota, APIs e compartilhamento de dados reduziu custos de transação e ampliou a conveniência, mas também distribuiu a superfície de ataque por toda a jornada financeira.

A velocidade é hoje uma característica ambivalente: beneficia o cliente legítimo e, simultaneamente, permite rápida dispersão de recursos obtidos por fraude. Por isso, controles exclusivamente posteriores ao evento tendem a ser menos eficazes. A prevenção deve migrar para decisões em tempo real, com capacidade de interromper, desafiar ou submeter as operações de maior risco a validações adicionais.

Segurança financeira deve ser compreendida como disciplina transversal. Ela conecta governança, segurança cibernética, proteção de dados, identidade, autenticação, monitoramento transacional, gestão de terceiros, continuidade de negócios, resposta a incidentes e recuperação de ativos.

O desafio estratégico é equilibrar segurança, velocidade e experiência do cliente. A resposta mais sustentável não é impor fricção uniforme, mas aplicar fricção proporcional ao risco, preservando fluidez nas jornadas normais e elevando a exigência de validação quando sinais de anomalia aparecem.

Conceitos

2.1

Segurança é o conjunto de **políticas, processos, tecnologias e controles** destinados a preservar a integridade das relações financeiras e impedir uso ilícito, indevido ou não autorizado de contas, instrumentos, credenciais, sistemas e recursos. É conceito amplo, que incorpora **prevenção a fraudes, segurança da informação, segurança cibernética, proteção de dados e resiliência operacional.**

2.2

A segurança bancária **evoluiu da proteção predominantemente física para uma arquitetura híbrida**. Agências, cofres e terminais permanecem relevantes, mas o perímetro crítico inclui **aplicativos, internet banking, biometria, cartões, Pix, APIs, centrais de atendimento, dispositivos, credenciais e infraestrutura de terceiros**.

2.3

Segurança cibernética **protege sistemas, redes, aplicações, dados e infraestrutura contra acessos indevidos, interrupção, manipulação e destruição**. No ambiente financeiro, confidencialidade, integridade e disponibilidade devem ser complementadas por autenticidade, rastreabilidade e resiliência.

2.4

Segurança da informação **protege a informação** independentemente do suporte. A LGPD adiciona obrigações específicas sobre medidas técnicas e administrativas aptas a **proteger dados pessoais e sobre comunicação de incidentes** capazes de causar risco ou dano relevante aos titulares.



Fonte: Lei nº 13.709/2018 (LGPD), arts. 46 e 48; ANPD, Resolução CD/ANPD nº 15/2024; Banco Central, Resolução CMN nº 4.893/2021.

Fraude, Golpe e Crime Cibernético

Para fins operacionais, fraude é categoria ampla: ação intencional para obtenção de vantagem indevida por falsidade, manipulação, apropriação de identidade, abuso de credenciais, exploração de processo ou comprometimento de sistema. Golpe é frequentemente a manifestação da fraude em que predomina a engenharia social, isto é, a manipulação da vítima para que ela própria execute a ação desejada pelo criminoso.

DIMENSÃO	FRAUDE	GOLPE
INTERAÇÃO DA VÍTIMA	Pode ocorrer sem interação	Normalmente depende de interação ou indução
VETOR PREDOMINANTE	Identidade, credencial, documento, sistema	Confiança, urgência, medo ou oportunidade
AUTORIZAÇÃO	Pode gerar operação não autorizada	Pode resultar em operação formalmente autorizada
EXEMPLO	Tomada de Conta *(Account takeover)*	Falsa central bancária
CONTROLE CENTRAL	Identidade, autenticação, cibersegurança	Comportamento, contexto e monitoramento



Essa distinção muda a pergunta central da segurança. Em uma invasão, pergunta-se se é realmente o cliente. Em um golpe de engenharia social, é preciso perguntar também se, embora seja o cliente, a operação corresponde à sua vontade econômica legítima.

Fonte: FEBRABAN, materiais públicos de prevenção a golpes; TransUnion, Consumer Pulse e H1 2026 Fraud Trends; CERT.br, Cartilha de Segurança para Internet.

Cenário Atual BRASILEIRO

Walter Faria Consultoria

ClearFi INSTITUTE

O Brasil combina elevada bancarização digital, ampla utilização de smartphones e pagamentos instantâneos disponíveis continuamente. Esse ambiente amplia a conveniência e a inclusão, mas cria múltiplos pontos de entrada para o fraudador.

A superfície de ataque deixou de coincidir com a infraestrutura interna do banco. O ataque pode começar no cliente, em uma rede social, no telefone, em um dispositivo comprometido, em uma identidade roubada, em um fornecedor ou em uma conta destinatária usada para receber e dispersar recursos.

Pesquisa da FEBRABAN divulgada em julho de 2025 indicou que quase 4 em cada 10 brasileiros já haviam sofrido algum golpe, reforçando a dimensão social do problema. Em paralelo, a TransUnion informou em fevereiro de 2026 que 32% dos entrevistados haviam sido alvo de tentativa de fraude nos três meses anteriores e 7% declararam ter sido vítimas.

Para a alta administração, fraude deve ser tratada simultaneamente como risco financeiro, operacional, reputacional, regulatório e de confiança.

A perda direta é apenas uma parcela do custo: **atendimento, investigação, ressarcimentos, contingências, litígios, reforço tecnológico e erosão da confiança** também precisam ser considerados.



GOLPES SOFRIDOS
(JULHO-2025)

38%

dos brasileiros já sofreram algum golpe.

TENTATIVA E VÍTIMA DE FRAUDE
(FEV-2026)

32%

foram alvo de tentativa de fraude

7%

foram vítimas.

Fraude é um desafio multidimensional que exige visão integrada, dados, tecnologia, colaboração e foco permanente em **prevenção, detecção, resposta e recuperação.**

Fonte: FEBRABAN, 'Quase 4 em cada 10 brasileiros já sofreram golpe', 22/7/2025; TransUnion Consumer Pulse, 26/2/2026.

Principais FRAUDES, GOLPES E AMEAÇAS



Segundo a **FEBRABAN**, os três tipos mais comunicados por clientes aos bancos associados em **2025** foram:

- ↔ **Golpe do WhatsApp**
- ↔ **Falsas vendas**
- ↔ **Falsa central / falso funcionário**

A Federação também informou investimento de aproximadamente

R$ 5 bilhões

em segurança e prevenção a fraudes e crimes cibernéticos em 2025, sendo aproximadamente **10%** do total investido em tecnologia.

AMEAÇA	COMO OPERA
Golpe do WhatsApp / falso perfil	Criação ou comprometimento de perfil para pedir transferências a contatos da vítima.
Falsa central / falso funcionário	Criminoso simula contato legítimo do banco e induz transferência, instalação de app ou entrega de credenciais.
Phishing e smishing	Links e páginas falsas capturam dados ou instalam código malicioso.
Vishing	Engenharia social por ligação telefônica, muitas vezes com spoofing e dados pessoais.
Account takeover	Tomada de conta por credenciais comprometidas, malware ou recuperação fraudulenta.
pix Fraudes com Pix	Uso do Pix como trilho de liquidação após engenharia social ou comprometimento de conta.

Principais FRAUDES, GOLPES E AMEAÇAS

Walter Faria Consultoria

ClearFi INSTITUTE

AMEAÇA	COMO OPERA
Conta laranja	Conta usada para receber, fracionar e dispersar recursos ilícitos.
Identidade sintética	Combinação de dados reais e artificiais para criar identidade aparentemente legítima.
SIM Swap	Apropriação indevida da linha para interceptar autenticação ou recuperar contas.
Malware e ransomware	Código malicioso para captura de credenciais, manipulação ou indisponibilidade.
Supply chain	Comprometimento de fornecedor ou serviço tecnológico conectado.
Deepfake e clonagem de voz	Conteúdo sintético usado para simular pessoa legítima e aumentar credibilidade do golpe.

> Estar um passo à frente em segurança exige mais do que tecnologia. Exige colaboração entre instituições, integração de esforços e, sobretudo, uma população cada vez mais informada e preparada para reconhecer riscos.
>
> **Walter Faria**

Como se proteger

Walter Faria Consultoria

ClearFi INSTITUTE



GOLPES MAIS COMUNS. CONHECER PARA NÃO CAIR.

Informação é sua melhor proteção.

Regra de ouro

Desconfie sempre.

Golpistas criam urgência, medo e falsas oportunidades para enganar você.

	ATENÇÃO!	COMO SE PROTEGER
FALSA VENDA	Cuidado com sites ou perfis falsos de lojas que anunciam promoções mirabolantes.	Prefira lojas conhecidas. Desconfie de preços muito abaixo do mercado e evite pagamentos fora da plataforma.
FALSA CENTRAL FALSO FUNCIONÁRIO	O criminoso se passa por funcionário do banco e informa supostas irregularidades, solicitando dados, senhas ou transferências.	Bancos nunca pedem senhas ou dados sigilosos por telefone ou mensagem. Na dúvida, desligue e acione os canais oficiais.
GOLPE DO WHATSAPP	O golpista tenta assumir o WhatsApp da vítima ou utiliza um falso perfil para pedir dinheiro aos seus contatos.	Ative a verificação em duas etapas no WhatsApp e nunca compartilhe seu código de verificação. Mantenha o seu aplicativo atualizado.
PHISHING (PESCARIA DIGITAL)	Mensagens falsas por e-mail, SMS ou redes sociais tentam roubar seus dados por meio de links ou sites enganosos.	Não clique em links suspeitos. Acesse o site digitando o endereço no navegador e mantenha seus dispositivos e antivírus atualizados.
FALSO BOLETO	Boletos são falsificados ou adulterados para direcionar o pagamento para contas de criminosos.	Confira sempre os dados do beneficiário antes de pagar e confirme com a empresa em caso de dúvida.
TROCA DE CARTÃO	Após observar sua senha, o fraudador troca seu cartão por outro semelhante.	Confira o valor na maquininha antes de digitar a senha e não perca seu cartão de vista durante a compra.
DEVOLUÇÃO DE EMPRÉSTIMO	Golpistas contratam empréstimos em seu nome e pedem a devolução do dinheiro para contas de terceiros.	Não devolva valores sem confirmar a situação diretamente com o banco pelos canais oficiais.
MÃO FANTASMA (ACESSO REMOTO)	Criminosos induzem a vítima a instalar aplicativos maliciosos que dão acesso remoto ao celular.	Não instale aplicativos por links ou de fontes desconhecidas. Baixe apenas nas lojas oficiais e mantenha o sistema atualizado.
DELIVERY (VALOR ALTERADO)	Entregadores ou falsos entregadores adulteram o valor na maquininha ou cobram mais do que o devido.	Confira o valor na tela da maquininha antes de confirmar a senha ou o pagamento. Prefira pagamentos pelo aplicativo.

Segurança é atitude. Informação é proteção. Compartilhe.

Walter Faria Consultoria

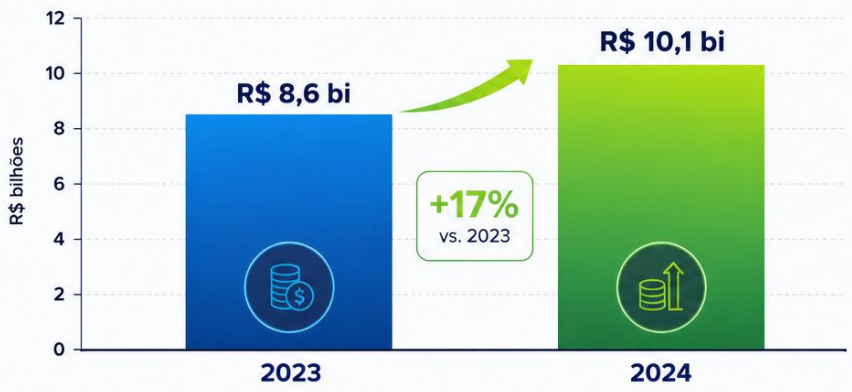
ClearFi INSTITUTE

FEBRABAN:
PERDAS E EXPOSIÇÃO DOS CLIENTES



Perdas com golpes e fraudes bancárias alcançaram cerca de **R$ 10,1 bilhões** em 2024, alta de **17%** sobre 2023, quando o montante foi de aproximadamente **R$ 8,6 bilhões.** A Federação também registrou crescimento relevante de fraudes e golpes via **Pix** em horizonte de dois anos, evidenciando a adaptação do crime aos trilhos instantâneos.

PERDAS COM GOLPES E FRAUDES BANCÁRIAS
(R$ BILHÕES)



DESTAQUES

R$ 10,1 bilhões
em perdas com golpes e fraudes bancárias em 2024.

17% **Alta de 17%**
em relação a 2023 (R$ 8,6 bilhões).

Crescimento relevante
de fraudes e golpes via **Pix** em horizonte de dois anos.

Fonte: FEBRABAN Tech, "Inteligência artificial no combate a fraudes financeiras", 11/3/2026; FEBRABAN, pesquisas e comunicados de segurança.

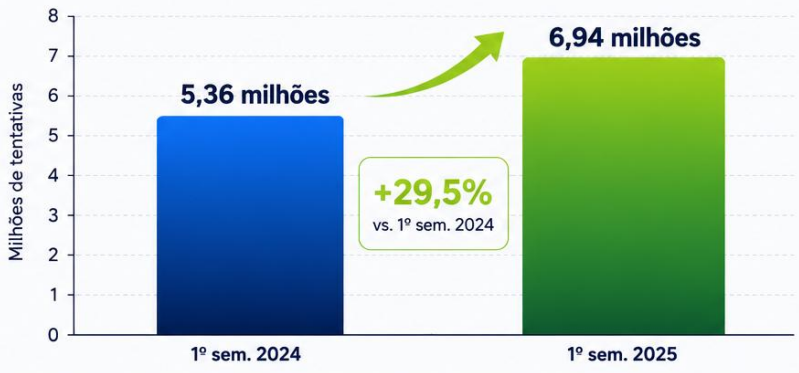
SERASA EXPERIAN:
RECORDE DE TENTATIVAS EM 2025



O Indicador de Tentativas de Fraude da Serasa Experian registrou **6.937.832** tentativas no primeiro semestre de 2025, aumento de **29,5%** sobre o mesmo período de 2024 e média de uma ocorrência a cada **2,3** segundos. Bancos e emissores de cartões concentraram **53,7%** das tentativas, sendo o principal alvo setorial.

No acumulado de janeiro a setembro de 2025, a Serasa Experian informou **10.886.982** tentativas, **28,6%** acima do mesmo período de 2024. O dado reforça que o problema não se restringe a picos episódicos: trata-se de pressão persistente sobre os processos digitais.

TENTATIVAS DE FRAUDE NO BRASIL
(SERASA EXPERIAN)



DESTAQUES-CHAVE

1 tentativa
a cada **2,3 segundos**

53,7%
das tentativas têm como alvo bancos e emissores de cartões.

10.886.982
tentativas de fraude
de jan. a set./2025
+28,6% vs. jan. a set./2024

Fonte: Serasa Experian, Indicador de Tentativas de Fraude, 30/9/2025 e 22/12/2025.

Walter Faria Consultoria

ClearFi INSTITUTE

SERASA EXPERIAN:
IDENTIDADE DIGITAL EM 2026

No primeiro trimestre de 2026, a Serasa Experian identificou **1.495.696** tentativas de fraude em cadastros e validações de identidade, alta de **36,6%** na comparação anual.

Segundo a empresa, o potencial de prejuízo, caso as tentativas não fossem bloqueadas, poderia alcançar **R$ 1,98 bilhão.**

Seis em cada dez tentativas estavam concentradas em bancos, cartões, meios de pagamento e serviços financeiros ou de crédito.

1.495.696
TENTATIVAS DE FRAUDE
em cadastros e validações de identidade no 1º tri. 2026

↗ **36,6%**
na comparação anual

R$ 1,98 BILHÃO
POTENCIAL DE PREJUÍZO
caso as tentativas não fossem bloqueadas

FRAUDE DE IDENTIDADE DIGITAL POR SETOR
1º TRIMESTRE DE 2026



6 EM CADA 10
tentativas concentradas em **bancos, cartões, meios de pagamento e serviços financeiros ou de crédito.**

TRANSUNION:
SEVERIDADE DA PERDA E ENGENHARIA SOCIAL

A atualização H1 2026 da TransUnion apontou perda média relatada de **R$ 10.699** entre brasileiros que disseram ter perdido dinheiro em fraudes digitais, ante **R$ 6.311** no levantamento anterior – **aumento de 60%.**

41% DOS BRASILEIROS pesquisados declararam ter sido alvo de tentativa de fraude digital.

R$ 6.311
PERDA MÉDIA RELATADA
no levantamento anterior

R$ 10.699
PERDA MÉDIA RELATADA
no H1 2026

+60%

A fraude digital vai além da tecnologia.
Ela explora comportamentos, relações de confiança e vulnerabilidades humanas.
Proteger pessoas é tão importante quanto proteger sistemas.

PERDA MÉDIA RELATADA POR VÍTIMA DE FRAUDE DIGITAL



PRINCIPAIS FORMAS DE FRAUDE
ENTRE CONSUMIDORES QUE SOFRERAM PERDAS

32%
VISHING
(ligações fraudulentas)

19%
USO DE CONTAS DE TERCEIROS / LARANJAS

18%
INVASÃO DE CONTA
(ACCOUNT TAKEOVER)

Fonte: TransUnion, Atualização H1 2026 do Relatório de Principais Tendências de Fraude, 15/6/2026.

Banco Central:
Indicadores de Resposta e Prevenção

BC PROTEGE+
Lançado em dezembro de 2025 para impedir abertura de contas com uso indevido de identidade.

1 MILHÃO
DE ATIVAÇÕES
Em fevereiro de 2026

PIX: MED E MARCAÇÕES DE FRAUDE
Em 2025, o Banco Central anunciou aprimoramentos do MED para permitir rastreamento e devolução a partir de múltiplas contas utilizadas na dispersão do dinheiro, além de disponibilizar contestação por autoatendimento para casos de fraude, golpe e coerção.

Objetivo: reduzir o tempo entre percepção de fraude, contestação, bloqueio e tentativa de recuperação.

RASTREAMENTO AMPLIADO
a partir de múltiplas contas

MARCAÇÕES E BLOQUEIOS
mais rápidos e assertivos

CONTESTAÇÃO POR AUTOATENDIMENTO
mais agilidade para o usuário

DEVOLUÇÃO E RECUPERAÇÃO
mais efetivas



Leitura Executiva dos números

INDICADOR	RESULTADO	LEITURA EXECUTIVA
FEBRABAN — Perdas 2024	**R$ 10,1 bi** | +17% a/a	Impacto financeiro agregado permanece **elevado**.
Serasa — Tentativas H1 2025	**6,94 mi** | +29,5% a/a	Pressão **crescente** sobre as jornadas digitais.
Serasa — Bancos e cartões H1 2025	**53,7%** das tentativas	Setor financeiro permanece como **principal alvo**.
Serasa — Identidade Q1 2026	**1,50 mi** | +36,6% a/a	Identidade tornou-se **frente crítica de risco**.
TransUnion — Perda média H1 2026	**R$ 10.699**	A severidade financeira individual é **material**.
TransUnion — Vishing	**32%** entre perdas relatadas	Engenharia social exige controles **além da autenticação**.
BC Protege+	**1 milhão** de ativações em fev/2026	Prevenção à fraude de identidade ganha **escala sistêmica**.

CONCLUSÃO

Os indicadores apontam para mesma direção: a **fraude cresce em volume, sofisticação e severidade.** A resposta exige uma **arquitetura multicamada,** combinando prevenção, identicade, inteligência compartilhada, monitoramento e **reação em tempo real.**

Arquitetura de Proteção Contra Fraudes

7 Pilares para reduzir o risco e aumentar resiliência

1. Identidade e KYC

2. Autenticação e controle de acesso

3. Inteligência e análise de dados



4. Monitoramento transacional

5. Compartilhamento de inteligência

6. Resposta, bloqueio e recuperação

7. Educação e proteção do cliente

1. IDENTIDADE E KYC

Impedir entrada e permanência de identidades falsas, roubadas ou sintéticas. KYC deve ser **contínuo**, com validação **documental**, **biometria**, **prova de vida *(liveness)***, sinais de **dispositivo** e **reavaliação cadastral**.

2. AUTENTICAÇÃO E CONTROLE DE ACESSO

MFA, **biometria**, vínculo de dispositivo, tokens e autenticação **adaptativa** reduzem o risco de tomada de conta. A autenticação, porém, não prova a legitimidade econômica da intenção.

3. INTELIGÊNCIA E ANÁLISE DE DADOS

Modelos analíticos **e IA** devem correlacionar histórico, dispositivo, horário, valor, localização, beneficiário, velocidade e relações entre contas.

Continuação:

7 Pilares para reduzir o risco e aumentar resiliência

Fraudes são dinâmicas, coordenadas e exploram vulnerabilidades humanas e tecnológicas. A proteção exige uma **arquitetura integrada**, **contínua** e orientada por **inteligência**.

4. MONITORAMENTO TRANSACIONAL



A operação deve ser avaliada no **contexto**. A mesma transferência pode ser normal para um cliente e altamente anômala para outro. Fricção deve ser **proporcional ao risco**.

5. COMPARTILHAMENTO DE INTELIGÊNCIA



Fraudes atravessam instituições. Compartilhar indícios **reduz assimetria informacional** e permite reconhecer contas, dispositivos e padrões já associados a eventos suspeitos.

6. RESPOSTA, BLOQUEIO E RECUPERAÇÃO



Detecção rápida deve acionar investigação, bloqueio, preservação de evidências, comunicação e tentativa de recuperação. No Pix, o **MED** materializa parte dessa capacidade.

7. EDUCAÇÃO E PROTEÇÃO DO CLIENTE



Educação reduz vulnerabilidade, mas **não substitui controles**. A instituição deve reconhecer sinais de que o cliente legítimo pode estar sendo manipulado.



Camadas se complementam



Processos contínuos



Inteligência compartilhada



Fricção proporcional



Resposta em tempo real

Proteção eficaz é engenharia, pessoas e processos trabalhando juntos para **reduzir risco, proteger clientes** e **fortalecer o sistema financeiro**.

PIX e Pagamentos Digitais

Arquitetura de Segurança e Resposta à Fraude

O ecossistema Pix combina controles preventivos, detecção inteligente e mecanismos de resposta para proteger usuários e instituições.



1. ARQUITETURA EM CAMADAS

O Banco Central descreve a segurança do Pix como conjunto de mecanismos que inclui autenticação, rastreabilidade, proteção das informações, limites e instrumentos específicos de tratamento de fraude.

2. DISPOSITIVOS E LIMITES

Desde novembro de 2024, operações Pix iniciadas em dispositivos não cadastrados estão sujeitas, nas condições regulamentares, a limites de R$ 200 por transação e R$ 1.000 por dia. A medida reduz o potencial de perda imediata após comprometimento de credenciais.

3. MARCAÇÕES DE FRAUDE

O ecossistema Pix utiliza marcações associadas a chaves e CPFs/CNPJs. O Banco Central informa que, havendo marcação de fraude ativa, a instituição responsável deve adotar os procedimentos previstos, inclusive restrições aplicáveis.

4. MED E CONTESTAÇÃO

O MED é mecanismo exclusivo do Pix para facilitar devoluções em casos de fraude, golpe ou crime. O pedido deve ser iniciado junto à instituição dentro das condições e prazos aplicáveis. O autoatendimento de contestação reduz dependência de canais humanos e acelera a resposta.

5. DESAFIO ESTRATÉGICO

O objetivo não é desacelerar universalmente o Pix. É identificar em tempo real operações de maior risco e introduzir fricção seletiva, preservando a experiência nas transações normais.

SEGURANÇA QUE HABILITA CONFIANÇA

Controles proporcionais ao risco, inteligência em tempo real e mecanismos eficazes de resposta sustentam a confiança no Pix e impulsionam a inclusão financeira.

Marco Regulatório BRASILEIRO

A revisão normativa realizada até **15 de agosto de 2026** reúne o arcabouço central aplicável **à segurança e à Prevenção a Crimes Financeiros**. Além das regras específicas de prevenção a fraudes, segurança cibernética, Pix, identidade e contas, a análise deve incorporar as bases legais e regulatórias de **PLD/FTP, sanções financeiras e sigilo bancário**.

	NORMA / CONJUNTO NORMATIVO	EIXO	RELEVÂNCIA PARA PREVENÇÃO A CRIMES FINANCEIROS
PLD/FTP	**Lei nº 9.613/1998 + Lei nº 12.683/2012**	**PLD/FTP — Marco Legal**	Marco legal brasileiro de lavagem ou ocultação de bens, direitos e valores; estabelece deveres preventivos para pessoas obrigadas e comunicações ao Coaf.
	Lei nº 13.260/2016	**Financiamento do Terrorismo**	Disciplina o terrorismo no Brasil e tipifica o financiamento do terrorismo, fundamentando políticas e controles de PLD/FTP.
	Circular BCB nº 3.978/2020 + Res. BCB nº 119/2021	**PLD/FTP — BCB**	Estabelece política, procedimentos e controles internos de PLD/FTP para instituições autorizadas pelo BCB, com abordagem baseada em risco, KYC e monitoramento.
	Carta Circular BCB nº 4.001/2020	**Monitoramento e Comunicação ao Coaf**	Relaciona operações e situações que podem configurar indícios de lavagem de dinheiro ou financiamento do terrorismo para fins de monitoramento e comunicação.
SANÇÕES	**Lei nº 13.810/2019 + Decreto nº 9.825/2019**	**Sanções Financeiras e Indisponibilidade de Ativos**	Disciplina o cumprimento de sanções da ONU, incluindo indisponibilidade de ativos e medidas relacionadas a pessoas e entidades vinculadas a terrorismo.
	Resolução BCB nº 44/2020	**Sanções Financeiras**	Estabelece procedimentos para execução, pelas instituições autorizadas pelo BCB, das medidas de indisponibilidade de ativos previstas em lei.
SIGILO	**Lei Complementar nº 105/2001**	**Sigilo Bancário**	Estabelece o dever de sigilo sobre operações e serviços das instituições financeiras e as hipóteses legais de acesso, compartilhamento ou afastamento do sigilo.
PROTEÇÃO DE DADOS	**Lei nº 13.709/2018 (LGPD)**	**Proteção de Dados e Incidentes**	Arts. 46 e 48: medidas técnicas e administrativas de segurança e comunicação de incidentes envolvendo dados pessoais.

Marco Regulatório BRASILEIRO

	NORMA / CONJUNTO NORMATIVO	EIXO	RELEVÂNCIA PARA PREVENÇÃO A CRIMES FINANCEIROS
SEGURANÇA CIBERNÉTICA	**Resolução CMN nº 4.893/2021 + Res. CMN nº 5.274/2025**	Segurança Cibernética	Política de segurança cibernética e controles sobre autenticação, criptografia, intrusão, vazamento, malware, rastreabilidade e vulnerabilidades.
	Resolução BCB nº 85/2021 + Res. BCB nº 538/2025	Segurança Cibernética	Disciplina equivalente para instituições supervisionadas pelo BCB, atualizada em 2025 e hoje alcançando também PSAV autorizadas.
FRAUDES	**Resolução BCB nº 142/2021**	Prevenção a Fraudes em Pagamentos	Norma-base de procedimentos e controles antifraude em cartões, TED, Pix, DOC e boletos; exige limites, registros diários e avaliação consolidada de fraudes e tentativas.
	Resolução Conjunta nº 6/2023	Inteligência Compartilhada	Compartilhamento de dados e informações sobre indícios de ocorrência ou tentativa de fraude entre instituições abrangidas.
	Res. BCB nº 343/2023 + Res. BCB nº 569/2026	Operacionalização do Compartilhamento	Define sistema, dados mínimos, segurança, interoperabilidade e registro de indícios de fraude; disciplina atualizada em 2026.
PIX	**Res. BCB nº 1/2020 e alterações**	Regulamento do Pix	Base normativa do Pix e de seus mecanismos de segurança, incluindo suspeita de fraude, bloqueios, DICT e devolução.
	Res. BCB nº 402/2024 + IN BCB nº 491/2024	Segurança do Pix e Dispositivos	Reforça informações de segurança na autorização e rejeição de operações e estabelece controles para Pix iniciado em dispositivo não cadastrado.
	Res. BCB nº 482/2025	Pix Automático	Inclui controles de idoneidade e ausência de indícios de fraude para usuários recebedores do Pix Automático.
	Res. BCB nº 493/2025 + IN BCB nº 589/2025	MED 2.0 e Contestação	Aprimora a recuperação de valores e o autoatendimento para contestação de Pix em situações de fraude, golpe ou coerção.

Marco Regulatório BRASILEIRO

	NORMA / CONJUNTO NORMATIVO	EIXO	RELEVÂNCIA PARA PREVENÇÃO A CRIMES FINANCEIROS
PIX + BCB	**Res. BCB nº 501/2025**	Segurança do Pix	Amplia a prevenção de fraudes da detecção para o bloqueio preventivo, impedindo que contas com fundada suspeita de fraude recebam pagamentos.
	Res. BCB nº 506/2025	Segurança do Pix	Amplia bloqueio cautelar, permite limites conforme perfil de risco e comportamento e restringe Pix e chaves de clientes reconhecidos como fraudadores.
	Res. CMN nº 5.261/2025 + Res. BCB nº 518/2025	Identificação e Uso de Contas	Reforça a identificação e o encerramento de contas utilizadas para movimentações em nome de terceiros com finalidade de ocultar ou substituir obrigações.
	Res. BCB nº 475/2025 + nº 476/2025 + Res. CMN nº 5.218/2025 + IN BCB nº 661/2025	BC Protege+	Institui e operacionaliza restrições a contratações e abertura ou inclusão em contas, reduzindo o uso fraudulento de identidade.
	Res. BCB nº 496/2025, nº 497/2025 e nº 498/2025	Resiliência de Pix/ TED e PSTI	Estabelece limites e reforços de governança e risco para instituições não autorizadas e conexões via PSTI.
	Res. BCB nº 150/2021 + Res. BCB nº 522/2025	Arranjos de Pagamento	Aprimora estruturas centralizadas de gerenciamento de riscos, incluindo prevenção e combate a fraudes e golpes.
	Res. CD/ANPD nº 15/2024	Incidentes de Dados Pessoais	Regulamenta a comunicação de incidentes capazes de gerar risco ou dano relevante, com prazo geral de três dias úteis, ressalvada legislação específica.

O conjunto normativo evidencia mudança de paradigma: o regulador avança de controles predominantemente institucionais para uma arquitetura sistêmica baseada em inteligência compartilhada, prevenção na conta destinatária, rastreabilidade, identidade, análise comportamental e capacidade de recuperação.

Para a alta administração, o ponto central é demonstrar efetividade: políticas formais devem estar conectadas a métricas, modelos de risco, decisões em tempo real, testes, auditoria e evidências de resposta.



Leitura Executiva da REGULAÇÃO

Walter Faria Consultoria

ClearFi INSTITUTE

PREVENÇÃO A FRAUDES EM PAGAMENTOS

A **Res. BCB nº 142/2021** é a norma central de prevenção a fraudes em pagamentos, com controles de limites, registros diários, consolidação mensal e manutenção de documentação.

A **Res. BCB nº 501/2025** determina que, diante de fundada suspeita de fraude na conta destinatária, a instituição deve rejeitar a transação.

LEITURA DE GOVERNANÇA

A prevenção passa a considerar também o risco associado ao **destinatário dos recursos**, não apenas a origem da transação.

EVOLUÇÃO REGULATÓRIA EM 2026

A **Res. BCB nº 569/2026** atualizou a disciplina do compartilhamento de indícios de fraude.

A **Res. BCB nº 584/2026** ampliou o regime da **Res. BCB nº 142** para serviços de ativos virtuais e introduziu retenção cautelar em situações de maior risco.

Publicada em 07/08/2026, entra em vigor em 01/01/2027.

LEITURA DE GOVERNANÇA

O perímetro regulatório se expande para **novos serviços, novos ativos e novas formas** de movimentação financeira.

PIX: PREVENÇÃO, MARCAÇÃO, BLOQUEIO E RECUPERAÇÃO

A prevenção no Pix se baseia na **Res. BCB nº 1/2020** e suas alterações.

A **Res. BCB nº 506/2025** reforçou bloqueio cautelar, limites por risco e restrições a fraudadores.

A **Res. BCB nº 493/2025** ampliou a recuperação de valores.

A **IN BCB nº 589/2025** viabilizou o botão de contestação do MED.

LEITURA DE GOVERNANÇA

Combater a fraude significa **impedir que identidades e contas sejam utilizadas como infraestrutura para o crime financeiro**.

PROTEÇÃO DA IDENTIDADE E DAS CONTAS

O **BC Protege+** permite que pessoas e empresas comuniquem restrições a contratações no SFN.

As **Res. CMN nº 5.261/2025 e BCB nº 518/2025** reforçam requisitos de identificação e tratamento de contas usadas em nome de terceiros, aproximando prevenção a fraude da governança cadastral e do monitoramento de **contas laranja**.

LEITURA DE GOVERNANÇA

A segurança do Pix evolui para uma abordagem que combina **comportamento, risco, bloqueio, rastreamento e recuperação**.

LEITURA DE GOVERNANÇA

A evolução regulatória revela uma mudança estrutural na prevenção a crimes financeiros.

A efetividade do modelo dependerá menos de controles isolados e mais da capacidade de **conectar sinais e tomar decisões em tempo real**.

LEITURA DE GOVERNANÇA

Integração entre **PLD/FTP, fraude, segurança cibernética, dados, pagamentos, cadastro e gestão de riscos** é essencial.

Papel do BANCO CENTRAL DO BRASIL

na prevenção a fraudes e na segurança financeira

Regulação: estabelecer requisitos mínimos de segurança, governança e controles.

Supervisão: avaliar aderência e efetividade das estruturas das instituições autorizadas.

Infraestrutura e Pix: definir regras de segurança, rastreabilidade, **marcação de fraude, bloqueio cautelar, contestação e recuperação de valores**.

Inteligência compartilhada: estabelecer obrigações e infraestrutura para o **compartilhamento de indícios de fraude**, permitindo que instituições reconheçam contas, usuários e padrões associados a eventos suspeitos.

Proteção preventiva: desenvolver instrumentos sistêmicos como o BC Protege+.

Coordenação: induzir padrões que elevem a resiliência do SFN e do Sistema de Pagamentos Brasileiro.

O BC Protege+ ilustra a passagem de uma postura exclusivamente reativa para uma **barreira preventiva** controlada pelo próprio cidadão ou empresa. Atingir **1 milhão de ativações** em poucos meses demonstra demanda por instrumentos que reduzam fraude de identidade **antes da abertura da conta.**

O papel do regulador é criar as condições para uma defesa sistêmica: estabelecer regras, viabilizar inteligência compartilhada e induzir mecanismos que permitam prevenir, detectar, bloquear e responder à fraude em todo o sistema financeiro.

Fonte: Banco Central do Brasil, BC Protege+, 1/12/2025 e 20/2/2026; Resolução Conjunta nº 6/2023; Segurança no Pix.

Papel dos BANCOS e demais instituições

A infraestrutura regulatória compartilhada não substitui a responsabilidade de cada instituição. Os bancos e demais participantes devem admistrar o risco ao longo de **todo o ciclo de relacionamento**.

MOMENTO	RESPONSABILIDADES ESSENCIAIS
Antes do relacionamento	KYC, validação de identidade, prevenção a identidade sintética, análise de dispositivo e risco cadastral.
Durante o relacionamento	Autenticação, atualização cadastral, segurança de canais, análise comportamental e gestão de credenciais.
Na transação	Scoring de risco, análise do destinatário, detecção de anomalias, autenticação adaptativa e fricção seletiva.
Após alerta/fraude	Bloqueio, investigação, compartilhamento, preservação de evidências, recuperação e comunicação.
Aprendizagem	Retroalimentação dos modelos, revisão de regras, testes e acompanhamento de indicadores.

A governança deve **integrar** fraude, cibersegurança, risco operacional, dados, jurídico, compliance, atendimento e prevenção à lavagem de dinheiro. A separação rígida entre essas áreas reduz a **visão sobre ataques que atravessam múltiplos canais**.



Fonte: Banco Central do Brasil, Resolução CMN nº 4.893/2021 e alterações; Resolução Conjunta nº 6/2023; FEBRABAN, Segurança.

Inteligência Artificial e Nova GERAÇÃO DE FRAUDES

Walter Faria Consultoria

ClearFi INSTITUTE

Uma tecnologia com dois lados.
O futuro depende do uso que fazemos dela hoje.



1 IA COMO DEFESA

IA e machine learning ampliam a capacidade de detectar **anomalias, redes de contas, comportamentos atípicos, identidades sintéticas** e sinais de comprometimento em escala incompatível com análise exclusivamente humana.

O QUE A IA PERMITE FAZER MELHOR

- **Detecção de anomalias em tempo real**
- **Mapeamento de redes e contas laranja**
- **Identificação de identidades sintéticas**
- **Análise de dispositivo e comportamento**
- **Priorização inteligente de alertas**

2 IA COMO ATAQUE

A mesma tecnologia reduz custo de personalização do crime: **mensagens convincentes, clonagem de voz, deepfakes, documentos sintéticos e automação de abordagens.**

COMO A IA ESTÁ SENDO USADA PELOS FRAUDADORES

- **Mensagens altamente personalizadas**
- **Clonagem de voz**
- **Deepfakes (imagem e vídeo)**
- **Documentos e dados sintéticos**
- **Automação de abordagens e fraude como serviço (FaaS)**

serasa experian

A Serasa Experian identifica uso indevido de IA, fraude como serviço e identidades sintéticas entre as principais **tendências de 2026**.

TransUnion

A TransUnion registra preocupação dos consumidores com aumento de tentativas de fraude associadas à IA.

3 CONSEQUÊNCIA PARA IDENTIDADE

Imagem, vídeo e voz deixam de ser evidências isoladamente suficientes. Biometria deve ser acompanhada por **prova de vida, sinais de dispositivo, contexto, histórico e verificação de consistência.**

O NOVO PARADIGMA: CONFIANÇA CONTÍNUA

Coleta de múltiplos sinais → **Avaliação de contexto e risco** → **Verificação contínua** → **Confiança dinâmica e adaptativa** → **Decisão em tempo real**

Do momento da autenticação à jornada completa do cliente:
a identidade é validada o tempo todo.



A IA pode ser a maior aliada na proteção do sistema financeiro ou o maior acelerador do crime. A diferença está em **governança, dados de qualidade, modelos responsáveis e colaboração.**

Tendências e Desafios

O cenário de pagamentos está em rápida evolução.
Novas tecnologias, modelos de negócio e comportamentos digitais ampliam possibilidades e também riscos.
Sete movimentos-chave moldam o futuro da segurança financeira.

1 Segurança comportamental
Padrões de navegação, digitação, dispositivo e histórico de uso tornam-se sinais adicionais de confiança, permitindo identificar comportamentos anômalos além das credenciais tradicionais.

2 Análise de Redes (Network Analytics)
A análise evolui da conta isolada para a identificação de redes, conectando usuários, dispositivos e movimentações para revelar estruturas coordenadas e padrões suspeitos.

3 Convergência entre Fraude e Cibersegurança
Phishing, malware, roubo de credenciais e pagamentos instantâneos passam a integrar uma mesma cadeia de ataque, exigindo respostas cada vez mais coordenadas.

4 Open Finance e APIs
A expansão de ecossistemas abertos aumenta a superfície de integração entre instituições e terceiros. Autenticação, consentimento, segurança de APIs e gestão de terceiros tornam-se críticos para preservar confiança e interoperabilidade.

5 Instantaneidade
Pagamentos em tempo real reduzem a janela para identificar e interromper fraudes. Quanto menor o tempo de liquidação, maior a necessidade de decisões preventivas ou simultâneas à transação.

6 Industrialização do Crime
Fraude como serviço, automação e redes de distribuição reduzem as barreiras de entrada para criminosos, ampliando a escala, a velocidade e a sofisticação dos ataques.

7 Segurança como vantagem competitiva
Segurança deixa de ser apenas proteção contra perdas ou requisito regulatório. Confiança e capacidade de proteção passam a influenciar reputação, retenção e preferência do cliente.



A evolução da segurança financeira não será determinada apenas pela capacidade de detectar fraudes, mas pela capacidade de **antecipá-las** em ecossistemas cada vez mais **conectados**, **instantâneos** e **inteligentes**.

Tendências e Desafios

Walter Faria Consultoria

ClearFi INSTITUTE

Convergência entre Fraudes e PLD/FTP

A evolução para uma abordagem integrada de Prevenção a Crimes Financeiros

Fraude, lavagem de dinheiro e movimentação de recursos ilícitos frequentemente integram uma mesma cadeia. Estruturas isoladas podem fragmentar justamente os sinais necessários para compreender o evento em sua totalidade.

A convergência conecta **KYC, identidade, comportamento transacional, dispositivos, beneficiários, alertas de fraude e vínculos entre contas**, ampliando a visão sobre o risco.

EVOLUÇÃO DO MODELO



MUDANÇA DE PARADIGMA

> De controles organizados por tipo de risco para uma visão integrada da cadeia do crime financeiro.

GANHOS DE CONVERGÊNCIA

Maior efetividade	Menor tempo de resposta
Maior assertividade	Eficiência operacional
Visão integrada	Governança consistente

> A próxima geração da prevenção não será definida apenas pela **qualidade dos controles individuais**, mas pela **capacidade de conectar sinais** que hoje ainda estão distribuídos por **diferentes** áreas da organização.

Alexandre Logli Alexandrino

Recomendações Estratégicas para a ALTA ADMINISTRAÇÃO

Walter Faria Consultoria

ClearFi INSTITUTE

FORTALECER CONFIANÇA · REDUZIR RISCOS · GERAR VALOR

1. Tratar fraude e cibersegurança como **riscos estratégicos**, com apetite de risco, métricas e reporte periódico ao conselho e à diretoria.
2. Consolidar uma visão de **Prevenção a Crimes Financeiros**, integrando Fraudes e PLD/FTP e conectando cibersegurança, identidade, dados e risco operacional em fóruns, processos e infraestrutura de inteligência comuns, com metas de efetividade, tempo de resposta e eficiência operacional.
3. Migrar de autenticação pontual para **confiança contínua**, correlacionando identidade, dispositivo, comportamento, contexto, transação e destinatário.
4. Intensificar **análise de recebedores e redes** de contas para reduzir a utilidade econômica de contas laranja.
5. Aplicar **fricção proporcional** ao risco, evitando tanto controles excessivos quanto permissividade uniforme.
6. Ampliar capacidade de **resposta em tempo real** e reduzir o intervalo entre detecção, bloqueio, compartilhamento e recuperação.
7. Usar o **compartilhamento regulatório de indícios** como insumo efetivo de decisão, e não apenas como obrigação de compliance.
8. Testar controles contra **deepfakes, clonagem de voz, identidades sintéticas e fraude automatizada por IA.**
9. Reforçar **gestão de terceiros, APIs, nuvem e cadeia de suprimentos**, incluindo testes, evidências e planos de contingência.
10. Padronizar **métricas internas:** tentativas, perdas brutas, perdas líquidas, recuperação, falso positivo, tempo de detecção, tempo de bloqueio e reincidência.
11. Manter programa permanente de **educação do cliente**, mas sem transferir ao usuário a responsabilidade exclusiva pela segurança.
12. Realizar **exercícios executivos de crise** que combinem incidente cibernético, fraude massiva, vazamento de dados e indisponibilidade operacional.

Decisões estratégicas **hoje** determinam a resiliência e a reputação de **amanhã**.

ClearFi INSTITUTE

O FUTURO DA SEGURANÇA FINANCEIRA

Walter Faria Consultoria

O Brasil construiu uma infraestrutura financeira digital altamente eficiente. Protegê-la exige um modelo igualmente **rápido, integrado e orientado por inteligência**.

Fraude, segurança cibernética, proteção de dados e risco operacional estão cada vez mais conectados. Ataques atravessam canais, dispositivos e instituições em segundos. **A resposta precisa operar com o mesmo nível de integração e velocidade**, transformando avanços regulatórios em capacidade operacional efetiva e mensurável.

A próxima fronteira será proteger o cliente não apenas contra operações não autorizadas, mas também contra **operações formalmente autorizadas sob manipulação, engenharia social ou coerção**.

Essa evolução favorece estruturas integradas de **Prevenção a Crimes Financeiros**, conectando **Fraudes e PLD/FTP** por meio de inteligência, dados, tecnologia e processos compartilhados.

O novo paradigma é o da **confiança continuamente verificada**: identidade, dispositivo, comportamento, contexto, transação e destinatário avaliados em conjunto e em tempo real.

> Segurança financeira deixa de ser apenas **proteção** e passa a ser um atributo estratégico de **confiança, resiliência e competitividade.**

Carolina Sansão M. Alexandrino

Sobre o autor



Alexandre Logli Alexandrino
https://www.linkedin.com/in/alexandrelogli/

- **Mais de 20 anos de experiência em Riscos, Compliance e Prevenção a Crimes Financeiros,** com atuação no setor financeiro e em ambientes altamente regulados.
- Executivo com sólida trajetória em **PLD/FTP (AML/CFT), Compliance, Controles Internos e Riscos Não Financeiros,** liderando estruturas de prevenção, governança e controles em grandes instituições financeiras.
- Experiência executiva em instituições como **Safra, Banco PAN, Itaú Unibanco e Citi**, além de atuação em auditoria na KPMG, construindo uma visão integrada entre riscos, controles, compliance e negócio.
- **Especialista em Prevenção a Crimes Financeiros**, com foco em AML/CFT, fraude, KYC, sanções, monitoramento, inteligência financeira, governança e efetividade dos controles. É certificado **CAMS – Certified Anti-Money Laundering Specialist.**
- **Fundador da ClearFi Advisory**, onde aplica sua experiência em projetos de advisory e controles internos, contribuindo para o desenvolvimento de modelos mais integrados de gestão de riscos e prevenção a crimes financeiros.

Sobre o ClearFi Institute

O ClearFi Institute é uma iniciativa independente dedicada à produção de pesquisas, white papers e análises sobre pagamentos, inovação financeira, governança, cibersegurança e transformação digital, contribuindo para o debate técnico e estratégico sobre a evolução do sistema financeiro.



Sobre a autora



Carolina Sansão M. Alexandrino
www.linkedin.com/in/carolina-sansao-moreira

- **28 anos de experiência** em Tecnologia da Informação, Transformação Digital e Gestão de Projetos, sendo mais de duas décadas dedicadas ao setor financeiro.
- **Co-criadora do Pix** e participante da construção de importantes iniciativas do Banco Central do Brasil, incluindo Open Finance e Piloto Drex.
- **Especialista em inovação financeira, pagamentos instantâneos (Pix), cibersegurança, governança e infraestrutura do sistema financeiro**, com atuação em projetos de alcance nacional.
- **Fundadora do ClearFi Institute**, iniciativa dedicada à produção de pesquisas, análises e conhecimento sobre inovação, confiança e transformação financeira.
- **Atualmente vive nos Estados Unidos**, acompanhando a evolução do mercado financeiro norte-americano e desenvolvendo estudos comparativos entre diferentes ecossistemas globais de pagamentos e serviços financeiros.

Sobre o ClearFi Institute

O ClearFi Institute é uma iniciativa independente dedicada à produção de pesquisas, white papers e análises sobre pagamentos, inovação financeira, governança, cibersegurança e transformação digital, contribuindo para o debate técnico e estratégico sobre a evolução do sistema financeiro.



Sobre o autor

Walter Faria
Consultoria



Walter Faria
https://www.linkedin.com/in/walter-faria-825248b0/

- **Mais de 50 anos de atuação no Sistema Financeiro Nacional,** com trajetória dedicada a serviços bancários, meios de pagamento, prevenção a fraudes, segurança bancária e transformação do setor financeiro.
- **Mais de três décadas na FEBRABAN (1991–2025),** onde atuou como Diretor Adjunto de Serviços e Segurança, participando de importantes iniciativas de modernização da infraestrutura financeira brasileira.
- Participação na evolução dos meios de pagamento e serviços bancários no Brasil, incluindo projetos relacionados ao SPB, TED, DDA, boletos, compensação de cheques, Pix e mecanismos de prevenção e combate a fraudes.
- **Especialista em prevenção a fraudes, segurança bancária e cibernética,** com atuação em temas como engenharia social, identidade digital, proteção dos clientes, inteligência artificial e evolução dos mecanismos de segurança dos meios de pagamento.
- **Fundador & CEO da Walter Faria Consultoria,** onde atua em consultoria, advisory, mentoria, palestras e treinamentos para instituições financeiras e demais participantes do ecossistema, com foco em pagamentos, segurança, prevenção a fraudes, operações e governança.

Sobre a Walter Faria Consultoria
A Walter Faria Consultoria atua no ecossistema financeiro brasileiro oferecendo consultoria, advisory, mentoria, palestras e treinamentos, com foco em pagamentos, cobrança, prevenção a fraudes, segurança, operações e governança. Atende instituições financeiras, novos participantes do mercado regulado e fornecedores de soluções para o setor.