EBOOK ESTRATÉGICO · ALTA GESTÃO

PARA CEOS, CIOS, CROS, CISOS, HEADS OF RISK, HEADS OF AML E CONSELHOS DOS MAIORES BANCOS, FINTECHS E GESTORAS BRASILEIRAS E GLOBAIS

A Conta que se *Mantém Fechada*.

Como a Criptografia Totalmente Homomórfica permite ao banco fazer scoring, AML, fraud detection e M&A — sem nunca decifrar o que pertence ao cliente. E como sobreviver à transição pós-quântica que já começou.

VOLUME I · EDIÇÃO 2026 · CONFIDENCIAL

SUMÁRIO

O que você vai *ler*.

- Apêndices

00 · SUMÁRIO EXECUTIVO

O argumento em *uma* página.

Se você só vai ler uma coisa deste eBook, leia isto.

A indústria financeira é, há cinco séculos, a indústria da confiança. Mais que produto, mais que tecnologia, mais que inovação — banco vende a promessa de que o dinheiro do cliente está seguro, e que as informações sobre esse dinheiro não vão cair em mãos erradas. Tudo o mais é detalhe operacional. Esta promessa atravessou crises, guerras, pânicos, hiperinflações. Sobreviveu porque era — e em grande parte ainda é — verdadeira.

Mas a tecnologia que sustenta essa promessa está mudando de forma rápida e silenciosa. Por dois motivos:

1

CRQC

Computador quântico criptograficamente relevante estimado para 2029. Quebra ECDSA, RSA, ECDH. Toda a criptografia bancária atual.

2

HNDL

"Harvest Now, Decrypt Later" — adversários estão guardando dado cifrado hoje para decifrar em 2029.

3

AML COLABORATIVO

Lavagem de dinheiro custa USD 2 trilhões/ano. Combate exige cooperação entre bancos — hoje impossível.

4

SCORING JUSTO

Modelos de crédito sob escrutínio regulatório por viés. Auditoria precisa ver o modelo sem expor cliente.

FHE — Criptografia Totalmente Homomórfica — é a tecnologia central para resolver os quatro problemas simultaneamente. Permite AML colaborativo entre bancos concorrentes. Permite scoring sobre dado cifrado. Permite due diligence de M&A sob criptografia. E permite migração estruturada para criptografia pós-quântica que protege dado **presente e futuro**.

> *"A próxima década do sistema financeiro será definida por quais instituições aprenderem primeiro a colaborar matematicamente — e a sobreviver à transição pós-quântica sem perder dado cifrado hoje."*

A DECISÃO

A pergunta para o conselho não é "se" investir em arquitetura criptográfica de próxima geração. É "quanto custa esperar até descobrir que o adversário já estava esperando".

CAPÍTULO I

A Indústria da *Confiança*.

O banco moderno é uma operação de dado disfarçada de instituição financeira. E a maior parte da sua vantagem competitiva mora exatamente no dado que ele tem mais dificuldade em usar.

Em 1990, um banco competia por agência, gerente, taxa, produto. Em 2025, compete por modelo de risco, infraestrutura digital, capacidade de processar transação em tempo real, qualidade de IA, e — invisível para a maioria — capacidade criptográfica de proteger dado e transação. As dimensões antigas continuam relevantes; as novas viraram decisivas.

Essa transição criou uma contradição estrutural. Banco acumula dado de cliente em volume sem precedentes — transação, comportamento, score, garantia, risco. Esse dado é o ativo central para qualquer modelo preditivo, qualquer detecção de fraude, qualquer scoring, qualquer onboarding de novo cliente. Mas é também o ativo mais regulado, mais sensível, mais disputado por reguladores e mais cobiçado por adversários.

Os ativos invisíveis do banco

ATIVO	O QUE É	POR QUE É ÚNICO
Histórico transacional	Cada movimentação do cliente por anos	Único ator com visão temporal completa
Score de crédito real	Inadimplência observada vs prevista	Cada banco tem o seu, ninguém compartilha
Padrões AML	Movimentações suspeitas detectadas	Visíveis isoladamente; mais valiosas em consórcio
Conhecimento de cliente	KYC, perfil, comportamento	Replicar custa caro; compartilhar é tabu
Garantias e colateral	Avaliação de imóvel, veículo, equipamento	Mercado fragmentado, oportunidade de cooperação

O paradoxo do dado financeiro

Banco tem o dado mais valioso, mais sensível e mais regulado da economia. E a maior parte das decisões de negócio mais importantes — onboarding, scoring, AML, fraud — exige cruzar esse dado de formas que a regulação dificulta e que a cultura de competição entre bancos torna politicamente impossível.

O resultado é uma indústria que sabe muito sobre o cliente individual de cada banco e quase nada sobre o cliente do mercado como um todo. Cada banco conhece seu próprio histórico e olha o cliente do concorrente através de bureau de crédito (Serasa, SPC) que oferece visão parcial e atrasada.

O PROBLEMA SILENCIOSO

Toda a criptografia bancária atual — TLS, AES, ECDSA, RSA — é vulnerável a computador quântico. O CRQC está estimado para 2029. Adversários sofisticados estão coletando ciphertext bancário hoje, esperando para decifrar amanhã. Cada transação cifrada com criptografia clássica gerada hoje é potencialmente vulnerável retroativamente.

CAPÍTULO II

O Cerco *Regulatório*.

Banco vive sob mais regulação que qualquer outra indústria. O que mudou é que a regulação começou a exigir prova matemática.

LGPD, BACEN e o duplo padrão

Banco brasileiro vive sob LGPD (proteção de dado pessoal) e BACEN (regulação financeira). As duas regulações às vezes pedem coisas opostas: LGPD quer minimização, BACEN quer rastreabilidade. A resposta tradicional é "compliance documental robusto". A resposta moderna é "arquitetura técnica que satisfaz ambas" — exatamente o que FHE permite.

Basel III, IV e a exigência de modelos auditáveis

As regulações de Basel exigem que modelos de risco sejam auditáveis pelo regulador. Auditoria tradicional exige acesso a dado em claro. Sob FHE, é possível auditar modelo sem expor dado individual — preservando soberania de dado e conformidade simultaneamente.

FATF e AML

O Financial Action Task Force pressiona globalmente por colaboração entre bancos no combate a lavagem de dinheiro. Bancos resistem porque compartilhar nominalmente é juridicamente complexo. FHE com PSI resolve: bancos descobrem padrões em comum sem revelar bases.

CRQC e a transição pós-quântica

Esta é a pressão regulatória mais subestimada e a mais urgente. NIST padronizou em agosto de 2024 os primeiros algoritmos pós-quânticos (ML-KEM, ML-DSA, SLH-DSA). Em 2025, autoridades de cibersegurança (CISA, NSA, ENISA, BSI) começaram a publicar diretrizes que essencialmente exigem

migração até 2030. **Banco que não tiver plano de migração PQC em 2027 vai ser objeto de fiscalização específica.**

Aqui FHE e PQC se conectam: os esquemas modernos de FHE (CKKS, BFV, BGV, TFHE) são todos baseados em RLWE — o mesmo problema matemático sobre o qual ML-KEM e ML-DSA são construídos. **Adotar FHE é, simultaneamente, adotar a base matemática da próxima geração de criptografia bancária.** Os dois investimentos são o mesmo investimento.

O custo de não agir

RISCO	PROBABILIDADE 5 ANOS	IMPACTO
Multa LGPD por uso secundário sem base legal	Alta	R$ 50M+
Sanção BACEN por modelo de risco mal documentado	Média	Restrição operacional
Sanção FATF/Coaf por falha em AML	Média	Reputação + contratos internacionais
Vazamento retroativo pós-CRQC	Alta após 2029	Catastrófico — toda a criptografia clássica
Crise reputacional pós-breach de scoring	Baixa-média	Perda de carteira premium

CAPÍTULO III

FHE em Linguagem *Executiva*.

Sem matemática. O que a diretoria precisa entender.

Cofre transparente. Você vê que há algo dentro, não vê o que é. Manipula o conteúdo de fora — soma, multiplica, compara, computa modelos de risco inteiros — sem nunca abrir. Devolve fechado. Isto é FHE.

O salto conceitual

Toda criptografia atual protege dado em trânsito (TLS) e em repouso (AES). O terceiro estado — em uso — sempre exigiu plaintext. É nesse instante que o motor de scoring acessa histórico em claro. É onde o sistema AML processa transação. **FHE elimina o terceiro estado.**

FHE e PQC — a mesma matemática

Os esquemas modernos de FHE são construídos sobre o problema RLWE (Ring Learning With Errors). É exatamente o mesmo problema sobre o qual NIST padronizou ML-KEM (FIPS 203) e ML-DSA (FIPS 204) — a próxima geração de criptografia pós-quântica. **Adotar FHE é adotar PQC implicitamente.** O time que aprende FHE aprende PQC. A infraestrutura que suporta FHE suporta PQC.

Como funciona

> **ANALOGIA PARA O BANCO**
>
> Os dados do cliente ficam permanentemente cifrados. O motor de scoring roda sobre as cifras. O algoritmo AML processa transação cifrada. A análise de risco computa exposição sobre cifras. Em nenhum momento o servidor central viu dado individual em claro. Auditoria do regulador verifica o modelo, não o dado.

FHE vs alternativas

TECNOLOGIA	PROMETE	FALHA
Anonimização	"Removemos identificadores"	Re-identificação trivial
TEE (SGX, SEV)	"O chip isola"	Confia no fabricante; ataques laterais documentados
Federated Learning	"Dado fica no banco"	Gradientes vazam dado individual
Differential Privacy	"Adicionamos ruído"	Inadequado para decisão individual de crédito
FHE	**"Servidor nunca vê em claro"**	**Custo computacional alto — mas decrescente**

CAPÍTULO IV

Casos de Uso por *Linha*.

AML colaborativo entre bancos

Lavagem de dinheiro custa ao sistema financeiro global USD 2 trilhões/ano. O combate é estruturalmente ineficaz porque exige cooperação entre bancos concorrentes. Hoje impossível.

Sob FHE com PSI: bancos cifram listas de CPFs/CNPJs/IPs/contas suspeitas. Descobrem **apenas a interseção** — quem aparece em três ou mais bancos com padrão de movimentação anômalo. Sem revelar bases. Coaf e FATF estão sinalizando suporte regulatório explícito a essa abordagem. **É a maior oportunidade colaborativa não-explorada do setor financeiro.**

Scoring de crédito sob cifra

O score de crédito é o ativo mais valioso e mais regulado do banco. Auditoria regulatória do modelo exige acesso ao dado de treinamento, criando tensão entre supervisão e privacidade. Sob FHE, é possível auditar o modelo (verificar fairness, viés, accuracy) sem que o auditor jamais veja dados individuais de cliente.

Open Banking sob privacidade verificável

Open Banking depende de o cliente autorizar compartilhamento de dados entre instituições. A confiança é frágil — clientes hesitam, bancos receptores desconfiam. Sob FHE, as análises agregadas (consolidação, cash flow analysis, risk scoring) acontecem sobre dado cifrado. **Open Banking ganha base técnica de confiança que hoje não tem.**

Due diligence de M&A sob criptografia

M&A exige uma das partes mostrar dados sensíveis à outra antes de o deal estar fechado. Vazamento ou desistência do comprador é risco constante. Sob FHE, comprador pode fazer due diligence sobre dados

cifrados, validando hipóteses sem que a contraparte exponha base. **Reduz risco de vazamento de informação confidencial em deals que não se concretizam.**

Detecção de fraude em tempo real

Modelos de fraude precisam analisar padrão em tempo real. Hoje exigem dados em claro em pipelines complexos. Sob FHE, modelos de fraude podem rodar sobre transação cifrada — útil especialmente para escalar fraud detection para parceiros (gateway de pagamento, marketplaces) sem entregar dado de cliente.

Análise atuarial com dado clínico

Banco com produto de seguro precisa precificar risco com dado clínico. Sob LGPD, dado de saúde é categoria especial. FHE permite precificação atuarial sobre dado clínico cifrado (vindo de operadora ou hospital), preservando privacidade do segurado.

Migração pós-quântica estruturada

Adoção de FHE traz, como subproduto, a maturidade técnica para migração PQC. O time que aprende FHE aprende RLWE, lattices, ML-KEM. A infraestrutura que suporta FHE em produção é a infraestrutura que precisa estar pronta para PQC. **Investir em FHE é investir em sobreviver ao CRQC.**

HNDL — combate ao "Harvest Now, Decrypt Later"

Adversários (estados-nação, crime organizado sofisticado) estão coletando ciphertext bancário hoje para decifrar quando o computador quântico estiver pronto. Banco que migra para PQC **agora** protege também os dados cifrados *retroativamente*. Banco que espera até 2029 perde tudo o que foi cifrado nos últimos cinco anos.

Análise de portfolio cifrado

Gestoras de recursos analisam carteiras de cliente sob restrições de privacidade. Cliente quer aconselhamento sem expor totalidade do patrimônio. Sob FHE, a gestora pode analisar a carteira cifrada e devolver recomendação sem nunca ver as posições individuais.

Compliance sob auditoria privada

Auditorias internas e externas precisam ver dados sensíveis. Sob FHE, auditor pode validar conformidade regulatória sobre dado cifrado, sem que precise ter acesso a dado individual.

CAPÍTULO V

A Economia do *Banco que Não Vê*.

Capex inicial

COMPONENTE	INVESTIMENTO
Time fundador (cripto + ML + risk + jurídico + advisor PQC)	R$ 6M – 10M / ano
Licenças e tooling	R$ 400k – 1.5M
Infra computacional + HSMs	R$ 3M – 6M
Consultoria estratégica	R$ 1.5M – 3M
Estudo regulatório (BACEN, ANPD, FATF)	R$ 600k – 1.5M
Integração com core banking	R$ 3M – 8M
Total ano 1	**R$ 14M – 30M**

Opex anual

ITEM	ESTIMATIVA
Compute	R$ 3M – 8M
Time de manutenção	R$ 5M – 9M
Auditoria	R$ 800k – 2M
Opex anual estabilizado	**R$ 8.8M – 19M**

Para um banco top 10 brasileiro com receita acima de R$ 30B, isto representa **menos de 0,1% do faturamento**. É arredondamento orçamentário.

O retorno — sete vetores

1. Combate a AML colaborativo

Cada banco perde anualmente em multas Coaf, custos de remediação e investigações entre R$ 30M-150M. AML colaborativo reduz drasticamente: **R$ 50-200M anuais**.

2. Scoring mais preciso

Acesso a dado de outros bancos via consórcio FHE melhora modelos de crédito em 5-15%. Para banco top 10: **R$ 100-500M anuais em redução de inadimplência**.

3. Open Banking como ativo

Banco que oferece Open Banking com privacidade verificável captura share. **R$ 50-200M anuais**.

4. Detecção de fraude em tempo real

Redução de fraude transacional em 20-40%. **R$ 30-150M anuais**.

5. Migração PQC sem retrabalho

Banco que adota FHE migra para PQC quase de graça. Banco que não adota gasta **R$ 100-500M em migração emergencial** em 2028-2029.

6. Proteção de dado retroativo (HNDL)

Cada ano de atraso na migração PQC é mais um ano de ciphertext exposto retroativamente. Difícil de quantificar mas potencialmente catastrófico.

7. Vantagem em parcerias

Bancos com capacidade FHE viram parceiros preferenciais para fintechs, gestoras, marketplaces que precisam de processamento privado.

Caso de negócio

~R$ 22M INVESTIMENTO ANO 1	~R$ 14M OPEX ANUAL ESTABILIZADO
R$ 1B+ VALOR HABILITADO EM 5 ANOS	40×–80× ROI ESPERADO EM 5 ANOS

> *“Para qualquer banco top 10, FHE é o investimento de transformação digital com maior assimetria de retorno disponível em 2026 — combinando AML, scoring, migração PQC e proteção retroativa. ”*

CAPÍTULO VI

Vantagem Competitiva e *Posicionamento*.

A indústria financeira é dominada por consolidação, escala e infraestrutura. Vence quem opera mais barato e processa mais transação. Mas há uma camada nova de competição emergindo — e os bancos que se posicionarem primeiro nela capturam vantagem que dura uma década.

Os três posicionamentos

1 — O Banco Pós-Quântico

Foco em ser o primeiro banco brasileiro publicamente preparado para CRQC. Posicionamento explícito como "o banco que protege seu dinheiro também contra ameaças que ainda não chegaram". Funciona melhor para bancos premium de carteira corporate.

2 — O Articulador AML Setorial

Foco em construir consórcio FHE de combate a AML. Captura papel de organizador setorial, ganha visibilidade em BACEN/Coaf. Funciona para bancos top 5.

3 — O Banco da Soberania

Foco em independência de fornecedores de IA estrangeiros. Modelo proprietário sob FHE como capacidade soberana. Funciona para bancos públicos ou de investimento.

O custo de não posicionar

O cenário a explicitar: o que acontece se nenhum dos grandes bancos brasileiros adotar FHE estruturalmente nos próximos 36 meses? Resposta: **chegarão em 2029 sem capacidade técnica para**

migração PQC ordenada. Vão pagar múltiplos elevados em emergência, vão perder dado retroativo cifrado com criptografia clássica, vão ficar para trás em iniciativas globais de AML colaborativo.

CAPÍTULO VII

Roadmap de *24 Meses*.

01

MESES 1–6 · APRENDER

Fundação e capacidade

Contratar cripto-engenheiro fundador. Identificar três casos de uso (recomendação: AML, scoring, PQC migration). Alinhar com BACEN, jurídico, compliance.

02

MESES 7–14 · CONSTRUIR

Piloto interno

Construir um caso ponta a ponta. Recomendação: detecção de fraude sob FHE OU scoring auditável.

03

MESES 15–20 · PRIMEIRA COLABORAÇÃO

Estudo conjunto com outro banco ou parceiro

Lançar primeiro caso de uso com PSI ou colaboração externa. Marketing dirigido a BACEN, Coaf, Febraban.

04

MESES 21–24 · CAPACIDADE INSTITUCIONAL

Adoção como pilar

Múltiplos casos sobre infraestrutura. Anúncio público de migração PQC. Possível primeiro consórcio AML entre bancos.

CAPÍTULO VIII

Riscos, Mitigações e *Armadilhas*.

1 · Não conseguir contratar talento

Mitigação: aquisição via consultoria especializada ou parceria com universidade.

2 · Resistência cultural

Banco é avesso a novidade técnica em core. **Mitigação:** começar por sandbox isolado.

3 · BACEN não entender ou rejeitar

Mitigação: engajar BACEN cedo, em modo consultivo.

4 · Outros bancos não topam consórcio AML

Mitigação: começar com bancos menores. Top 5 segue depois.

5 · Custo computacional para volume

Mitigação: arquitetura híbrida.

Armadilha 1 · Tratar como projeto de TI

FHE deve reportar a CRO ou Chief Risk Officer, não CIO.

Armadilha 2 · Esquecer migração PQC

FHE e PQC devem ser tratados como o mesmo projeto.

Armadilha 3 · Subestimar HNDL

Cada ano de atraso é mais ciphertext vulnerável retroativamente.

CAPÍTULO IX · MANIFESTO

Uma carta para a próxima década do *sistema financeiro*.

A indústria que vocês lideram foi construída sobre uma promessa antiga: a de que o dinheiro do cliente está seguro, e que as informações sobre esse dinheiro não vão cair em mãos erradas. Tudo o mais é detalhe operacional. Esta promessa atravessou cinco séculos. Sobreviveu porque era — e em grande parte ainda é — verdadeira.

Mas a tecnologia que sustenta essa promessa está mudando. O computador quântico, que parecia ficção há cinco anos, é hoje cronograma de engenharia. A criptografia que sustenta toda a operação bancária atual será obsoleta em poucos anos. O adversário sofisticado já sabe disso e está coletando ciphertext hoje para decifrar amanhã. Quem não migrar agora vai descobrir, em 2029, que protege apenas o presente — não o passado nem o futuro.

FHE oferece uma resposta dupla. Resolve o problema atual da colaboração impossível entre bancos para AML, scoring e fraude. E posiciona o banco para a transição pós-quântica, porque a base matemática é a mesma. **Investir em FHE é investir em sobreviver ao CRQC.**

O que está em jogo não é uma feature técnica. É a continuidade da promessa antiga em um mundo tecnológico fundamentalmente novo.

> *“Em três anos, alguns bancos vão estar prontos para o CRQC. A pergunta é se o seu será um deles, ou se vai ser surpreendido junto com os demais.”*

APÊNDICE A

Glossário *Executivo*.

FHE

Computação sobre dado cifrado.

RLWE

Ring Learning With Errors — base matemática do FHE moderno e do PQC do NIST.

CRQC

Cryptographically Relevant Quantum Computer. Estimativa atual: 2029.

HNDL

Harvest Now, Decrypt Later — adversários coletam ciphertext hoje para decifrar quando tiverem CRQC.

ML-KEM, ML-DSA

Algoritmos pós-quânticos padronizados pelo NIST em 2024 (FIPS 203, 204). Baseados em RLWE.

PSI

Private Set Intersection. Caso central para AML colaborativo.

HSM

Hardware Security Module — onde chaves bancárias vivem hoje. FHE adiciona uma camada lógica acima.

FATF, COAF, BACEN, ANPD

Reguladores convergentes.

LATTIGO, OPENFHE, CONCRETE

Bibliotecas FHE.

APÊNDICE B

Fornecedores e *Parceiros*.

VENDOR	FOCO
Inpher	FHE+MPC, foco histórico em finanças
Duality	OpenFHE, foco em finanças e analytics
Zama	Concrete, TFHE, casos em fintech
Tune Insight	Lattigo
Stickybit	Boutique técnica brasileira em FHE/PQC

Iniciativas relevantes

- **NIST PQC** — padronização pós-quântica (FIPS 203/204/205)
- **FATF** — diretrizes globais sobre AML colaborativo
- **BIS Innovation Hub** — projetos de privacy-preserving finance

APÊNDICE C

30 Perguntas para o *CRO/CISO/CIO*.

Estratégia

1. Quem entende criptografia avançada e PQC na nossa empresa?
2. Temos plano formal de migração PQC?
3. Qual exposição atual a HNDL?
4. Inventário de algoritmos vulneráveis a CRQC?
5. Diálogo aberto com BACEN sobre PQC?

Casos prioritários

6. Quanto perdemos por ano em AML que não conseguimos combater sozinhos?
7. Quanto melhoraria nosso scoring com dado de outros bancos?
8. Quantos M&A frustrados por questões de privacidade?
9. Open Banking está atingindo o potencial?
10. Outros bancos topariam consórcio AML?

Técnica

11. Esquema FHE para nosso primeiro caso?
12. Latência aceitável para core banking?
13. Como integramos com HSMs e core?
14. Como gerenciamos chaves entre banco e parceiro?
15. Threshold cryptography compatível?

Custo

16. Custo FHE vs plaintext?
17. Construir interno ou via vendor?
18. Capex e opex 24 meses?
19. Sponsor C-level confirmado?

Regulação

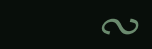
20. Conformidade LGPD, BACEN, Basel demonstrável?
21. Como BACEN vai auditar modelo sob FHE?
22. Diálogo com Coaf sobre AML colaborativo?

PQC

23. Quando começamos migração para ML-KEM/ML-DSA?
24. Qual nossa exposição se CRQC vier antes de 2029?
25. Como protegemos ciphertext já gerado?
26. Como nossos parceiros estão se preparando?

Comercial

27. Como precificamos a vantagem?
28. Que clientes pagariam por garantia matemática?
29. Qual narrativa de marca?
30. Pior cenário se concorrente liderar PQC primeiro?



A Conta que se Mantém Fechada

eBook estratégico para a alta gestão de bancos, fintechs e gestoras.
Volume I · Edição 2026 · Distribuição confidencial.

Composto em Iowan Old Style e SF Pro.

— fim —