SEGURANÇA DAS COMUNICAÇÕES BANCÁRIAS EM RISCO COM A CRIPTOGRAFIA QUÂNTICA

Autores: Marcelo Branquinho e Plataforma Safer

09/12/2025

Resumo: A segurança das comunicações bancárias modernas depende fortemente de algoritmos de criptografia clássicos, como RSA e AES, para proteger dados financeiros e garantir a privacidade dos clientes.

Entretanto, a rápida evolução da computação quântica e o surgimento de processadores quânticos cada vez mais poderosos colocam em xeque a eficácia desses algoritmos. Este artigo explora de forma didática como os princípios da criptografia quântica (incluindo a computação quântica e técnicas como distribuição quântica de chaves) ameaçam os métodos de segurança atuais.

Discutimos os conceitos básicos de criptografia e computação quântica, explicando como um computador quântico plenamente funcional poderia quebrar algoritmos criptográficos atuais em minutos, comprometendo transações bancárias e comunicações confidenciais.

Apresentamos também as possíveis soluções em desenvolvimento – desde criptografia pós-quântica (algoritmos resistentes a ataques quânticos) até a distribuição quântica de chaves (QKD) – que visam preservar a segurança na era quântica. Por fim, destacamos a necessidade urgente de adaptação do setor bancário a essa nova realidade, sob pena de vermos vulnerabilizadas as bases da confiança digital nos serviços financeiros.

Palavras-chave: Criptografia Quântica, Computação Quântica, Criptografia Pós-Quântica, Segurança Bancária, Distribuição Quântica de Chaves (QKD), Algoritmo de Shor, Processador Quântico Majorana, Vulnerabilidade Criptográfica.

POWERED BY SAFER

1. Introdução

A criptografia é a base da segurança digital moderna. Trata-se do conjunto de técnicas que permite proteger informações sensíveis convertendo-as de um formato legível para um formato ilegível, de modo que apenas destinatários autorizados possam reverter essa conversão (decifrar a mensagem). Bancos e instituições financeiras dependem crucialmente da criptografia para proteger dados financeiros, garantir a privacidade dos clientes e prevenir fraudes, sendo essa proteção indispensável para a segurança de transações bancárias, senhas, operações com cartões de crédito e demais dados sigilosos. Em essência, sem criptografia robusta, todo o sistema bancário digital – de pagamentos on-line a transferências eletrônicas – ficaria exposto a interceptações e acessos indevidos.

Atualmente, os algoritmos criptográficos amplamente utilizados devem sua segurança a problemas matemáticos de difícil resolução. Por exemplo, o algoritmo RSA (muito usado em protocolos de segurança na web e em sistemas bancários) baseia-se na dificuldade de fatorar números primos muito grandes, enquanto métodos de chave pública como ECC (criptografia de curva elíptica) dependem da dificuldade de resolver logaritmos discretos. Já algoritmos simétricos como o AES (Advanced Encryption Standard) utilizam chaves secretas e, embora não dependam de fatoração, exigem que um invasor tente inúmeras combinações para adivinhar a chave correta. Contra os computadores clássicos atuais, esses esquemas são efetivamente inquebráveis em tempo hábil – mesmo os supercomputadores mais poderosos levariam milhares de anos para quebrar algoritmos modernos como RSA ou AES[1]. Não é por acaso que RSA e ECC são considerados seguros e estão presentes em praticamente todas as formas de comunicação segura na Internet hoje.

O panorama, contudo, pode mudar radicalmente com a chegada da computação quântica. Computadores quânticos exploram princípios da física quântica para realizar certos tipos de cálculo em velocidades astronomicamente superiores às dos computadores atuais. Enquanto um bit clássico assume valor 0 ou 1, o qubit (bit

quântico) pode estar em uma superposição de 0 e 1 simultaneamente, permitindo que um computador quântico teste múltiplas soluções de uma só vez [4]. Além disso, qubits podem ficar emaranhados, de forma que o estado de um depende instantaneamente do estado de outro, fenômeno que pode ser explorado para processamento de informações em paralelo. Graças a essas propriedades, um computador quântico de escala suficiente é capaz de resolver alguns problemas complexos com uma eficiência proibitiva para computadores clássicos.

No contexto da criptografia, essa diferença de paradigma tem consequências preocupantes. Em 1994, o matemático Peter Shor desenvolveu um algoritmo quântico capaz de fatorar números inteiros grandes de forma eficiente – o famoso Algoritmo de Shor. Na prática, isso significa que um computador quântico executando o algoritmo de Shor poderia quebrar o RSA e outros sistemas de chave pública baseados em fatoração ou logaritmo discreto, quebrando a base matemática que os protege [5]. De modo análogo, Lov Grover apresentou um algoritmo quântico que acelera a busca não ordenada (o Algoritmo de Grover), permitindo uma redução quadrática no tempo de quebra de chaves simétricas por tentativa exaustiva. Embora o Algoritmo de Grover não quebre completamente cifras simétricas como o AES, ele efetivamente reduz a segurança – por exemplo, *encurtando pela raiz quadrada* o espaço de chaves a testar, de forma que uma chave de 128 bits poderia oferecer uma segurança equivalente a uma de 64 bits diante de um atacante quântico. Em resumo, os computadores quânticos trazem uma "ameaça existencial" mesmo aos algoritmos criptográficos tradicionais mais seguros [1].

Importantes players de tecnologia já vislumbram essa realidade. Em fevereiro de 2025, a Microsoft anunciou o processador quântico Majorana 1, primeiro chip quântico com um núcleo topológico, capaz de comportar múltiplos qubits estáveis. Esse avanço sugere um caminho claro para escalar até um milhão de qubits em um único chip que cabe na palma da mão [3]. Segundo a Microsoft, tal arquitetura pode colocar em prática computadores quânticos de utilidade prática em questão de anos, e não décadas [3], tornando real em um horizonte próximo a capacidade de esses sistemas resolverem problemas hoje

intratáveis. Por mais empolgantes que sejam as aplicações positivas dessa tecnologia, o contraponto alarmante é evidente: um computador quântico funcional com milhões de qubits poderia quebrar em minutos os ciframentos que usamos para proteger comunicações bancárias e transações financeiras sigilosas. Conforme destacou o banco BBVA em comunicado recente, *"a computação quântica promete revolucionar diversos setores... No entanto, esse avanço também representa um desafio para a segurança digital, pois os computadores quânticos podem violar os algoritmos criptográficos que atualmente protegem as transações financeiras, as comunicações e a integridade dos dados"* [2]. Diante dessa perspectiva, torna-se urgente compreender os riscos que a era da criptografia quântica traz e quais medidas podem ser tomadas para preservar a segurança das comunicações bancárias num futuro próximo.

Nos próximos tópicos, explicaremos de maneira acessível os conceitos de computação e criptografia quântica, detalhando por que os métodos de criptografia atuais estão em risco. Em seguida, discutiremos as estratégias em desenvolvimento para mitigar esses riscos – incluindo novas técnicas de criptografia quântica e algoritmos pós-quânticos – e como o setor bancário pode se preparar para a transição que se avizinha.

2. Criptografia Quântica: Conceitos e Distribuição Quântica de Chaves (QKD)

O termo criptografia quântica refere-se a técnicas de segurança da informação que aproveitam diretamente as leis da mecânica quântica para proteger dados, em vez de depender apenas de problemas matemáticos difíceis. A mais conhecida aplicação de criptografia quântica é a Distribuição Quântica de Chaves (QKD, *Quantum Key Distribution*), proposta inicialmente em 1984 por Bennett e Brassard (protocolo BB84). O objetivo da QKD é permitir que duas partes (comumente chamadas *Alice* e *Bob*) estabeleçam uma chave secreta compartilhada com segurança *absoluta*, garantida pelas leis da física.

No funcionamento típico de um sistema QKD, bits quânticos (qubits) são enviados na forma de fótons individuais através de um canal de comunicação (por exemplo, fibra óptica). Esses fótons são preparados por Alice em estados quânticos específicos (por exemplo, polarizações distintas representando 0 ou 1 em bases diferentes). Bob, ao receber os fótons, mede cada um em bases aleatórias. Em seguida, Alice e Bob se comunicam por um canal clássico (que pode ser público mas autêntico) para comparar quais medições de Bob coincidiram com as preparações de Alice. Os casos em que ambos usaram a mesma base produzem bits que serão aproveitados para compor a chave secreta. Crucialmente, se um espião (*Eve*) tentar interceptar os fótons no caminho, o simples ato de medir os qubits perturba seus estados (de acordo com o princípio da não-clonagem quântica e do colapso de estado). Essa perturbação causa discrepâncias detectáveis quando Alice e Bob comparam partes das sequências de bits. Assim, qualquer tentativa de espionagem em um canal QKD legítimo é percebida imediatamente, e a chave interceptada é descartada. Quando nenhuma intervenção é detectada, Alice e Bob podem ter alta confiança de que sua chave permaneceu secreta.

Diferentemente da criptografia convencional, que poderia ser vulnerável a avanços computacionais (como os computadores quânticos), a segurança de protocolos quânticos como QKD é provavelmente incondicional – isto é, independe do poder computacional do adversário, baseando-se em princípios fundamentais da física (por exemplo, a impossibilidade de medir um estado quântico sem perturbá-lo). Em teoria, a criptografia quântica oferece métodos invioláveis de comunicação segura, desde que os dispositivos funcionem conforme esperado. Por essas características, a QKD vem sendo considerada uma alternativa segura e testada para proteger dados confidenciais em um mundo pós-quântico, especialmente em infraestruturas críticas, comunicações governamentais e no setor financeiro. De fato, já existem relatos de bancos centrais e instituições financeiras experimentando redes de QKD para garantir troca de chaves entre agências ou data centers com máxima segurança. Projetos piloto na Europa e Ásia, por exemplo,

conectaram bancos e bolsas de valores via links quânticos, provando a viabilidade técnica da solução.

Contudo, é importante notar que a criptografia quântica, apesar de promissora, não substitui completamente os algoritmos clássicos em todos os cenários. A QKD resolve o problema da distribuição de chaves com segurança perfeita, mas ainda requer que a comunicação de dados em si use algoritmos simétricos (geralmente, após a chave quântica ser estabelecida, utiliza-se um cifrador como AES para a mensagem, pois transmitir cada bit por fóton não é prático). Ou seja, a QKD funciona em conjunto com a criptografia tradicional, fortalecendo a etapa mais vulnerável (a troca de chaves). Além disso, há desafios práticos: a distância alcançada pelos sistemas QKD em fibra óptica é limitada (devido à atenuação do sinal quântico, embora repetidores quânticos estejam em desenvolvimento) e os equipamentos envolvem detectores sensíveis, emissão de fótons únicos e rigoroso controle de ruído ambiental. A infraestrutura necessária é diferente da internet clássica, o que torna a adoção escalável da QKD um desafio de engenharia e custo. Ainda assim, em cenários de alto valor (como transferência interbancária de grandes somas ou comunicação entre centrais bancárias e órgãos reguladores), o investimento em links quânticos pode ser justificável para assegurar um nível máximo de segurança.

Em resumo, a criptografia quântica representa o outro lado da moeda: se por um lado a computação quântica ameaça a criptografia atual, por outro os fenômenos quânticos oferecem novas ferramentas para construir sistemas de segurança *intrinsecamente seguros*. Estamos testemunhando o nascimento de uma nova era de comunicação segura, em que as leis da física garantem a confidencialidade. No entanto, a aplicação dessas tecnologias ainda conviverá com a criptografia clássica e enfrenta obstáculos práticos. Por isso, além da QKD, uma frente de defesa mais imediata contra ataques quânticos está ganhando destaque: a criptografia pós-quântica, da qual trataremos a seguir.

3. Criptografia Pós-Quântica: Preparando-se para a Era Pós-Quântica

Enquanto tecnologias quânticas puras como o QKD vão gradativamente amadurecendo, a comunidade de segurança da informação também busca soluções mais imediatas e de fácil implementação para mitigar a ameaça quântica. Surge assim o conceito de Criptografia Pós-Quântica – um conjunto de novos algoritmos criptográficos (de chave pública, assinaturas digitais, etc.) desenvolvidos para serem seguros mesmo contra atacantes munidos de computadores quânticos. A grande vantagem desses algoritmos pós-quânticos é que a maioria deles pode ser executada em computadores clássicos e integrar-se à infraestrutura existente, diferentemente da criptografia quântica que exige hardware especializado. Ou seja, a criptografia pós-quântica busca substituir ou atualizar os algoritmos vulneráveis (RSA, ECC, DH, etc.) por outros que não sucumbem aos algoritmos de Shor ou Grover.

Desde 2016, o Instituto Nacional de Padrões e Tecnologia dos EUA (NIST) lidera um esforço global para padronizar algoritmos pós-quânticos. Após várias rodadas de avaliação envolvendo a submissão de propostas de criptógrafos de todo o mundo, em 2022-2024 foram selecionados os primeiros candidatos para se tornarem padrões. Em julho de 2022, o NIST anunciou quatro algoritmos aprovados (um para criptografia de chave pública e três para assinaturas digitais). Subsequentemente, em 2024, formalizou três novos padrões de criptografia pós-quântica para uso imediato. Entre eles estão:

- Kyber (ML-KEM): um algoritmo de acordo de chaves baseado em redes de lattices (estruturas reticulares). É projetado para substituir RSA/ECC nos mecanismos de troca de chaves em protocolos como TLS, oferecendo eficiência e alta segurança contra ataques quânticos.
- Dilithium (ML-DSA): um esquema de assinatura digital também fundamentado em problemas de reticulados. Permite assinar transações e documentos digitais de forma segura contra

adversários quânticos, com desempenho aceitável para aplicações práticas.

- SPHINCS+ (SLH-DSA): um algoritmo de assinatura digital baseado em funções hash (sem estrutura algebraica subjacente), proporcionando um nível muito alto de segurança. Embora suas assinaturas sejam maiores e mais lentas de gerar, sua força reside em não depender de problemas matemáticos que poderiam ter atalhos quânticos conhecidos.

Esses algoritmos foram exaustivamente testados em termos de segurança e performance. A orientação de especialistas do NIST é clara: as organizações devem começar a integrar os algoritmos pós-quânticos o quanto antes, já que a transição completa levará tempo. Isso significa atualizar softwares, bibliotecas de criptografia, sistemas operacionais, dispositivos embarcados e possivelmente hardware de segurança (como módulos HSM) para suportar os novos algoritmos.

No setor bancário e financeiro, essa transição é particularmente crítica. Instituições financeiras lidam com grande volume de dados sensíveis e transações vitais que precisam permanecer seguros mesmo em face de avanços tecnológicos disruptivos. Conforme destacou o NIST e especialistas, nos setores bancário e financeiro, onde a segurança é vital, a adoção rápida desses novos padrões será crucial para garantir que transações e dados sensíveis permaneçam protegidos. Grandes bancos internacionais já estão se mobilizando: o BBVA, por exemplo, anunciou em 2025 uma estratégia pioneira chamada *"Cryptography Transformation Journey"* para inventariar todos os mecanismos criptográficos em uso na instituição e planejar sua migração para esquemas seguros contra quânticos. Nesse plano, enfatiza-se a importância de ter uma arquitetura flexível, capaz de atualizar algoritmos criptográficos sem perturbar os sistemas, e de cumprir tanto regulações atuais quanto futuras de segurança digital. Outras organizações, como a Europol (agência policial europeia), têm alertado para que o setor financeiro transite o quanto antes para sistemas de segurança "impossíveis de hackear" do ponto de vista

quântico, numa coordenação global para evitar brechas exploráveis por criminosos cibernéticos.

Entretanto, implementar a criptografia pós-quântica em larga escala traz desafios. Muitas soluções pós-quânticas envolvem chaves públicas ou assinaturas de tamanho bem maior que as atuais, o que pode impactar protocolos (por exemplo, aumentando o tempo de handshake em conexões seguras ou o espaço ocupado por certificados digitais). Há também o desafio da interoperabilidade: sistemas legados e dispositivos antigos podem não suportar imediatamente os novos algoritmos, exigindo atualizações ou substituições custosas. Além disso, a falta de mão de obra qualificada em criptografia pós-quântica significa que serão necessários treinamentos para as equipes de TI e desenvolvimento adotarem corretamente as novas bibliotecas e seguirem boas práticas na transição.

Apesar dos desafios, a direção é inevitável. Um provérbio no meio de segurança diz: *"não espere para trocar o guarda-chuva até começar a chover"*. Transposto ao nosso contexto: não devemos esperar pelo primeiro ataque quântico bem-sucedido para agir. A adoção de algoritmos pós-quânticos deve ocorrer preventivamente, evitando um cenário em que dados financeiros fiquem desprotegidos. Empresas especializadas já oferecem ferramentas e ambientes de teste para ajudar nessa migração; por exemplo, kits de avaliação que permitem testar internamente protocolos pós-quânticos (em simulações de sessões TLS, assinaturas de código, etc.) sem afetar sistemas de produção. Esses testes ajudam a identificar pontos frágeis e a ajustar infraestruturas antes da adoção definitiva.

Em síntese, a criptografia pós-quântica representa o esforço de tornar a internet e os sistemas atuais resilientes à ameaça quântica, usando novas armas matemáticas contra as futuras armas computacionais. Bancos, em particular, devem encarar essa atualização tecnológica não como opção, mas como necessidade estratégica para continuar garantindo a confiança dos clientes na era pós-quântica.

4. Impacto e Adaptação no Setor Bancário

As instituições financeiras sempre estiveram na linha de frente da segurança da informação, pois a confiança dos clientes e a estabilidade do sistema dependem de sigilo e integridade. A perspectiva da criptografia quântica introduz um novo fator de risco que o setor bancário não pode ignorar. Comunicações bancárias seguras incluem uma variedade de fluxos de dados: conexões de internet banking entre clientes e bancos (protegidas por TLS/HTTPS), redes interbancárias (como a SWIFT, que interliga bancos globalmente), VPNs e canais internos que transmitem dados financeiros críticos, autenticação de usuários e funcionários (tokens, OTPs, assinaturas digitais), além do armazenamento cifrado de dados sensíveis em bancos de dados. Todos esses cenários hoje dependem de algoritmos criptográficos clássicos.

Se algoritmos como RSA e ECC forem quebrados, as consequências podem ser severas:

- Quebra de sigilo de comunicações: Transações bancárias online e comunicações por e-mail seguro poderiam ser interceptadas e decifradas por atacantes quânticos, expondo informações como números de contas, valores, credenciais e dados pessoais. Informações confidenciais de clientes privadas hoje poderiam tornar-se públicas amanhã caso estejam armazenadas por atacantes à espera de capacidade quântica.
- Comprometimento de autenticação e identidade: Grande parte da infraestrutura de certificação digital (PKI), incluindo os certificados que garantem que você está realmente se conectando ao site do seu banco e não a um impostor (*HTTPS/TLS certificates*), baseia-se em assinaturas digitais RSA/ECC. Um invasor com um computador quântico poderia forjar assinaturas digitais, permitindo a criação de sites falsos com certificados aparentemente válidos ou a falsificação de documentos e contratos eletrônicos. Assinaturas de transferências eletrônicas e transações interbancárias também

poderiam ser forjadas, abrindo brechas para fraudes de alto impacto.

- Violação da integridade de dados: Além de ler dados sigilosos, um ataque quântico poderia permitir a alteração de informações trafegadas ou armazenadas de forma indetectável, caso os mecanismos de hash/assinatura que garantem a integridade sejam enfraquecidos. Por exemplo, registros contábeis ou históricos de transações poderiam ser adulterados se os hashes de integridade (como SHA) se tornarem frágeis sem a devida compensação (como aumento de tamanho ou troca por funções pós-quânticas).
- Ataques a sistemas bancários legados: Muitas infraestruturas bancárias antigas usam padrões criptográficos mais antigos (como 3DES, RSA de 1024 bits, SHA-1 em alguns contextos legados). Esses já são considerados marginalmente seguros contra ataques clássicos e, portanto, seriam *ainda mais fáceis* de quebrar para um agente com capacidades quânticas, servindo como alvos preferenciais.

Diante desse panorama, reguladores e o próprio mercado financeiro têm demonstrado preocupação crescente. Conforme mencionamos, o BBVA na Europa posicionou-se publicamente ao afirmar que a computação quântica é "uma das maiores ameaças tecnológicas do futuro" para o setor financeiro e que antecipar-se é fundamental. Organismos reguladores poderão, em futuro próximo, emitir diretrizes exigindo que bancos realizem avaliações de risco quântico e planos de migração. A Febraban (Federação Brasileira de Bancos) e outras entidades já discutem criptografia quântica em relatórios técnicos, indicando a necessidade de conscientização no setor bancário brasileiro sobre o assunto.

Felizmente, o setor não parte do zero na adaptação. Muitas práticas de segurança já implementadas podem facilitar a transição:

- Bancos frequentemente fazem rotação periódica de chaves criptográficas e atualizações de protocolos (por exemplo, migração de TLS 1.1 para TLS 1.2/1.3, abandono de algoritmos

depreciados). Essa cultura de manutenção contínua de segurança deve agora incluir a ótica pós-quântica.

- Há uma tendência em aumentar tamanhos de chaves e usar curvas elípticas mais fortes (ex.: curvas de 521 bits) – embora isso por si só não resolva a ameaça quântica, demonstra disposição em adotar novas recomendações de criptografia.
- Muitas instituições possuem Hardware Security Modules (HSMs) para guardar chaves e realizar operações criptográficas de forma segura e flexível. Os principais fabricantes de HSM já anunciaram suporte ou roadmaps para incorporar algoritmos pós-quânticos assim que padronizados, o que deve tornar a troca de algoritmos mais simples nesses equipamentos.
- Testes e exercícios de recuperação de desastres de TI podem incluir agora cenários hipotéticos de "quebra quântica", para avaliar o quão exposto o banco estaria se determinados algoritmos fossem comprometidos subitamente, e assim priorizar os sistemas a serem reforçados primeiro.

Em paralelo, tecnologias quânticas defensivas começam a ser avaliadas em ambientes bancários. Por exemplo, a rede SECOQC na Europa e projetos na China implementaram redes metropolitanas de QKD envolvendo bancos, assegurando links de comunicação entre agências bancárias. O surgimento de satélites de comunicação quântica (como o satélite chinês Micius) também aponta para futuras aplicações de QKD de longa distância, o que poderia conectar sucursais globais de instituições financeiras com sigilo absoluto. Embora esses projetos ainda sejam pioneiros, eles indicam uma direção de investimento em pesquisa para o setor.

Por fim, é crucial perceber que a segurança na era quântica não é apenas um desafio tecnológico, mas também um compromisso de confiança. Nas palavras do líder do projeto Quantum Safe do BBVA, *"segurança cibernética não é apenas uma questão tecnológica, mas um compromisso com a confiança do cliente"*. Ou seja, os bancos que se anteciparem e comunicarem claramente suas iniciativas de proteção quântica poderão inclusive obter vantagem competitiva em

termos de confiança do mercado. Em contraste, uma instituição que seja lenta em reagir pode se ver exposta não somente a ataques, mas também a uma erosão da confiança dos clientes e investidores informados sobre riscos quânticos.

5. Conclusão

A iminente era da computação quântica traz um paradoxo para a segurança da informação: ao mesmo tempo em que promete resolver problemas complexos e impulsionar a inovação em diversos campos, ameaça tornar obsoletos os métodos criptográficos que sustentam a privacidade e a integridade dos dados na era digital. No âmbito das comunicações bancárias, esse paradoxo ganha contornos críticos – afinal, poucas áreas são tão dependentes de criptografia forte quanto o sistema financeiro, onde confiança e segurança caminham lado a lado.

Neste artigo, examinamos como os algoritmos de criptografia atuais correm perigo diante do poder de computação quântica, capaz de quebrar códigos antes considerados invioláveis em questão de minutos ou horas. Vimos que a ameaça não é mais teórica: avanços recentes, como o chip quântico Majorana 1 da Microsoft e outros desenvolvimentos, indicam que estamos progredindo continuamente rumo a máquinas quânticas de grande porte. Organizações financeiras e autoridades já soam o alarme, ressaltando que a janela para agir é limitada.

Por outro lado, também exploramos as soluções em gestação para enfrentar esse desafio sem precedentes. A criptografia quântica, especialmente a distribuição de chaves quânticas (QKD), demonstra que as mesmas leis quânticas podem ser nossas aliadas na construção de canais de comunicação seguros, imunes à espionagem. Paralelamente, a criptografia pós-quântica vem nos trazer novos algoritmos baseados em problemas matemáticos alternativos, resistentes aos algoritmos conhecidos de computação quântica. O esforço coordenado de comunidades científicas e governos já resultou nos primeiros padrões pós-quânticos, e a recomendação é clara: iniciar

imediatamente a transição para esses novos padrões, antes que os computadores quânticos atinjam sua maturidade operacional.

Para a comunidade de TI, especialmente aqueles atuando no setor bancário ou em empresas de tecnologia financeira (*fintechs*), a principal mensagem é a necessidade de proatividade e educação continuada. É vital manter-se atualizado sobre as evoluções em computação quântica e criptografia, avaliar o grau de exposição de seus sistemas (por exemplo, quais aplicações usam RSA/ECC e precisarão de substituição prioritária), e envolver as lideranças das instituições nesse diálogo sobre riscos e investimentos necessários. Assim como o ano 2000 motivou a revisão de sistemas legados e a GDPR/LGPD motivou a reformulação de políticas de privacidade, o "bug do quantum" deve ser encarado como um catalisador para melhorias estruturais na segurança da informação.

Em conclusão, embora os computadores quânticos representem uma ameaça real e significativa à segurança das comunicações bancárias, eles não precisam significar o colapso da confiança digital. Com planejamento, pesquisa e colaboração entre academia, indústria e governo, é possível evoluir nossos esquemas de criptografia para um patamar ainda mais robusto. A humanidade já enfrentou mudanças de paradigma tecnológico antes – da quebra de códigos manuais com máquinas eletromecânicas na Segunda Guerra, até o advento dos computadores e da criptografia de chave pública no final do século XX – e, em cada caso, a inovação em segurança surgiu para contrabalançar os novos riscos. Na corrida entre "espada e escudo" tecnológicos, estamos prestes a entrar em uma nova volta. Garantir que as comunicações bancárias permaneçam seguras na era quântica não é tarefa trivial, mas é um objetivo alcançável se agirmos com a devida antecipação e seriedade. O futuro da segurança bancária, assim como sua história, será escrito pela capacidade de adaptação frente às transformações – e a criptografia quântica, paradoxalmente, será ao mesmo tempo o agente do risco e a chave para a solução.

Referências Bibliográficas

1. IBM Think Blog. "O que é criptografia quântica?" *IBM Brasil*, 01 de dezembro de 2023.

2. Sonia Santos Dias. "BBVA antecipa ameaças quânticas com plano pioneiro de segurança cibernética." *Jornal PT50 - Inovação e Fintech*, 17 de março de 2025.

3. Catherine Bolgar. "Chip Majorana 1 da Microsoft abre um novo caminho para a computação quântica." *Microsoft Source Latam*, 19 de fevereiro de 2025.

4. Kryptus. "Distribuição Quântica de Chaves: a nova fronteira da segurança da informação." *Blog da Kryptus*, 2024.

5. Sabrina Gomes. "NIST Estabelece Três Padrões de Criptografia Pós-Quântica." *Blog Eval Digital*, 22 de agosto de 2024.