UFSM

InterAção

ISSN 2357-7975
ACESSO ABERTO

IA., Santa Maria, v. 17, n. 3, e99408, p. 1-15, 2026 • https://dx.doi.org/10.5902/2357797599408
Submissão: 16/10/2026 • Aprovação: 16/11/2026 • Publicação: 23/11/2026

Artigos Dossiê

Industrialização seletiva da computação quântica e prontidão PQC: framework QRA-PQC

Selective industrialization of quantum computing and PQC readiness: the QRA-PQC framework

Manoel Fernandes Amaral Filho[I]
Max Fortunato Cohen[II]
Anderson Fernandes Pereira dos Santos[III]

[I]Universidade Federal do Amazonas, Manaus, AM, Brasil
[II]Empresa Arapaima, Manaus, AM, Brasil
[III]Instituto Militar de Engenharia, Rio de Janeiro, RJ, Brasil

Resumo

A computação quântica transita para uma fase de industrialização seletiva, marcada por apoio estatal massivo, plataformas fullstack e pluralidade arquitetural. Este artigo mapeia os relacionamentos causais e associativos entre vetores tecnológicos do setor quântico e a pressão de migração para criptografia pós-quântica (PQC), propondo o framework QRA-PQC (Quantum-Readiness Acceleration for PQC). O framework organiza a decisão migratória em três eixos – maturidade do vetor de ameaça (M), pressão de adoção (P) e exposição setorial (E) – e os aplica a setores críticos globais e brasileiros. Demonstra-se que o modelo de ataque "colher agora, decifrar depois" (HNDL) converte incerteza tecnológica em risco presente, tornando a migração preventiva uma decisão de gestão de risco temporal. O trabalho avança ao conectar o framework ao contexto normativo e institucional do Brasil, identificando lacunas regulatórias em defesa, sistema financeiro e infraestrutura crítica, e formulando recomendações setoriais concretas.

Palavras-chave: Criptografia pós-quântica; Computação quântica; Segurança da informação; Gestão de risco; Defesa cibernética

Artigo publicado por InterAção sob uma licença CC BY-NC-SA 4.0.

Abstract

Quantum computing is entering a phase of selective industrialization, marked by extensive state support, full-stack platforms and architectural diversity. This article maps causal and associative relationships between technological drivers in the quantum sector and the pressure to migrate to post-quantum cryptography (PQC), proposing the QRA-PQC (Quantum-Readiness Acceleration for PQC) framework. The framework structures migration decisions around three axes: threat-vector maturity (M), adoption pressure (P) and sectoral exposure (E), and applies them to critical sectors worldwide and in Brazil. The harvest-now-decrypt-later (HNDL) attack model is argued to turn technological uncertainty into a present risk, making preventive migration a matter of time-sensitive risk management. The study also connects the framework to the Brazilian institutional and regulatory context, identifies gaps in defense, the financial system and critical infrastructure, and proposes sector-specific recommendations.

Keywords: Post-quantum cryptography; Quantum computing; Information security; Risk management; Cyber defense

1 INTRODUÇÃO

A computação quântica ingressou em uma fase de aceleração institucional e comercial, cujos efeitos sobre a segurança da informação são assimétricos e de difícil avaliação sem um instrumento analítico adequado. O problema central não é a existência de um computador quântico criptograficamente relevante hoje, mas a antecipação racional de que tal capacidade poderá existir dentro do horizonte de vida útil de dados e sistemas atualmente em produção. Esse risco é amplificado pelo modelo harvest-now-decrypt-later (HNDL), no qual adversários capturam tráfego cifrado presente para decifração futura (MOSCA, 2018).

Pesquisa KPMG/BSI com 28 grandes organizações concluiu que, em média, a migração estaria concluída com 6,5 anos de atraso em relação ao prazo necessário (KPMG; BSI, 2023). Diante desse quadro, a migração para PQC – algoritmos resistentes a ataques quânticos executados em hardware convencional (NIST, 2024a; NIST, 2024b; NIST, 2024c; SHOR, 1997; BERNSTEIN; LANGE, 2017) – configura uma decisão de gestão de risco temporal, não de adoção tecnológica.

Este artigo tem três contribuições principais: (i) sistematizar sinais recentes do ecossistema quântico em três frentes (computação, segurança quântica e PQC);

(ii) propor o framework QRA-PQC, que estrutura a decisão de migração preventiva em eixos M, P e E; e (iii) aplicar o framework ao contexto brasileiro, identificando lacunas regulatórias e recomendações para setores de defesa, financeiro e infraestrutura crítica.

2 MATERIAIS E MÉTODOS

A pesquisa é qualitativa, exploratória e descritiva, apoiada em análise documental de sinais recentes de mercado e institucionais. O corpus reuniu notícias de mídia especializada, anúncios corporativos, movimentos de capital (aportes, IPOs e aquisições), políticas públicas e roadmaps tecnológicos de empresas líderes. O procedimento analítico compreendeu: (a) codificação dos sinais em três frentes temáticas; (b) mapeamento de vínculos causais e associativos entre os elementos; e (c) abstração dos relacionamentos em framework de decisão. Reconhece-se a limitação do método à leitura de fontes secundárias em campo de alta volatilidade: os relacionamentos propostos devem ser lidos como hipóteses estruturantes, e não como leis determinísticas.

3 PANORAMA DOS VETORES TECNOLÓGICOS

Três movimentos definem o período. Primeiro, o apoio estatal migrou de P&D para política industrial: os EUA anunciaram US$ 2 bilhões em incentivos com participação acionária governamental em nove companhias (ESTADOS UNIDOS, 2026); a IBM comprometeu mais de US$ 10 bilhões e criou a foundry Anderon (IBM, 2026); a Quobly levantou €115 milhões para silício quântico (QUOBLY, 2026); e a UE comprometeu mais de €8 bilhões desde 2018, classificando tecnologias quânticas entre os quatro maiores riscos à segurança econômica da União (ESTADOS-MEMBROS DA UNIÃO EUROPEIA, 2023; QURECA, 2025; COMISSÃO EUROPEIA, 2023). Segundo, o foco competitivo deslocou-se de qubits brutos para plataformas fullstack: a Quantinuum

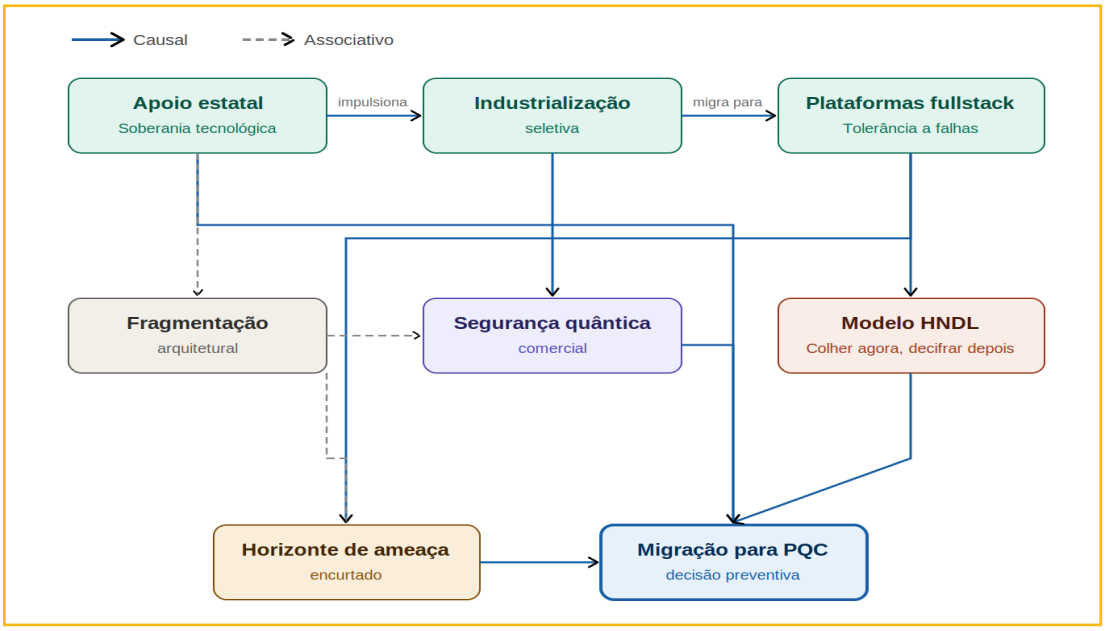
realizou IPO de US$ 1,68 bilhão (QUANTINUUM, 2026) e a a Microsoft anunciou como meta 2029 para um computador quântico escalável (MICROSOFT, 2025; MICROSOFT, 2026). Terceiro, a fragmentação arquitetural – íons aprisionados (IonQ (IONQ, 2026)), annealing e gate-model (D-Wave (D-WAVE QUANTUM, 2026)), silício (Quobly (QUOBLY, 2026)), fotônica (QCi (QUANTUM COMPUTING INC., 2026)) e código aberto (OQD (OPEN QUANTUM DESIGN, 2026)) – distribui o avanço por múltiplas frentes, reduzindo a probabilidade de um gargalo técnico único atrasar indefinidamente a ameaça criptográfica.

Paralelamente, segurança e comunicações quânticas consolidaram-se como vertical própria: a QCi adquiriu a NuCrypt e demonstrou redes seguras com a Ciena (QUANTUM COMPUTING INC., 2026); a IonQ incorporou a ID Quantique (IONQ; ID QUANTIQUE, 2025). Esses movimentos criam canal comercial que aproxima soluções PQC do ciclo de produto de fornecedores de segurança, reduzindo o atrito de adoção independentemente de qual arquitetura quântica prevalecer.

4 ANÁLISE DE RELACIONAMENTOS

A leitura conjunta dos sinais permite mapear vínculos entre os elementos da pesquisa. A Figura 1 representa graficamente os relacionamentos causais (setas sólidas) e associativos (setas tracejadas) que conectam os vetores tecnológicos à pressão de migração para PQC. Quatro cadeias causais são centrais: (1) apoio estatal → proteção criptográfica como requisito de soberania; (2) plataformas fullstack → horizonte de ameaça encurtado; (3) comercialização da segurança quântica → oferta PQC no ciclo de produto; (4) modelo HNDL → risco presente sobre dados longevos, independentemente da data da quebra (KPMG; BSI, 2023; CLOUD SECURITY ALLIANCE, 2023). Os vínculos associativos – fragmentação arquitetural e seletividade do mercado de capitais – moldam o ambiente de incerteza sem, contudo, reverter a tese de migração preventiva. A Tabela 1 sintetiza os vínculos.

Figura 1 – Mapa de relacionamentos causais e associativos entre vetores tecnológicos e a pressão de migração para PQC



Fonte: Autores (2026)

Tabela 1 – Relacionamentos entre vetores e efeitos sobre a migração PQC

Origem → Destino	Tipo	Efeito sobre PQC
Apoio estatal → Proteção como requisito de defesa	Causal	Eleva prioridade de migração em defesa e infraestrutura crítica
Fullstack/tolerância a falhas → Horizonte de ameaça	Causal	Aproxima relevância criptográfica; encurta prazo seguro
Segurança quântica comercial → Oferta de produtos PQC	Causal	Reduz atrito de adoção; insere PQC no ciclo de produto
Modelo HNDL → Risco presente sobre dados longevos	Causal	Torna a migração urgente independentemente da data da quebra
Fragmentação arquitetural → Incerteza de cronograma	Associativo	Reduz chance de gargalo único adiar a ameaça
Seletividade do mercado de capitais → Disciplina de execução	Associativo	Modera expectativas sem reverter a tese de migração

Fonte: Autores (2026)

5 FRAMEWORK QRA-PQC

Os relacionamentos mapeados convergem para um problema de decisão: dado que a quebra prática não está disponível hoje, mas múltiplos vetores pressionam seu horizonte, quando e onde migrar para PQC? O framework QRA-PQC organiza a resposta em três eixos ortogonais.

5.1 Eixos ortogonais

Eixo 1 – Maturidade do Vetor de Ameaça (M)

O eixo M mede a proximidade do ecossistema a uma capacidade criptograficamente relevante. Seus indicadores incluem: progresso de qubits lógicos e operações tolerantes a falhas; redução de taxa de erro físico; e diversidade de arquiteturas avançando em paralelo. A fragmentação arquitetural eleva M de forma agregada, pois elimina a dependência de um único caminho técnico. M é o eixo de maior incerteza, mas justamente por isso não deve ser a condição necessária para a migração: aguardar sua confirmação é precisamente a armadilha explorada pelo HNDL.

Eixo 2 – Pressão de Adoção (P)

O eixo P agrega os vetores que empurram a migração independentemente da data da quebra: mandatos regulatórios e enquadramentos de soberania; disponibilidade comercial de produtos resistentes a quantum; e o próprio modelo HNDL, que antecipa o risco para o presente. P é o eixo que converte incerteza tecnológica em ação imediata. A pesquisa KPMG/BSI evidencia que os vetores de P atuam de forma desigual entre setores – 61% das organizações ainda não haviam incorporado a ameaça quântica em seus sistemas de gestão de risco (KPMG; BSI, 2023) –, reforçando a necessidade de mandatos regulatórios para universalizar a adoção.

Eixo 3 – Exposição Setorial (E)

O eixo E mede o quanto um setor tem a perder, combinando a vida útil dos dados protegidos, a criticidade do ativo e o custo de exposição retroativa via HNDL. Setores com dados de longa duração e alta criticidade – defesa, financeiro, infraestrutura crítica – situam-se no topo de E. Corroborando essa hierarquia, a pesquisa KPMG/BSI registrou que 89% das organizações avaliaram o risco a dados em nuvem como alto ou bastante alto, seguido por dados confidenciais de longo prazo (78%) e dados em trânsito (71%) (KPMG; BSI, 2023).

5.2 Regra de Decisão e Índice Q

A prioridade de migração resulta da combinação dos três eixos no índice Q = f(M, P, E). A regra de decisão aproxima-se de um limiar disjuntivo: basta que E e P sejam simultaneamente altos para justificar migração imediata, independentemente do nível de M. Quando E é baixo, mesmo M e P elevados recomendam migração oportunística e monitoramento, protegendo o framework contra sobremigração e alocação prematura de recursos. A Tabela 1I projeta o espaço de decisão sobre o plano P × E, mantendo M implícito – pois, para os sistemas de alta exposição que constituem o foco do framework, a incerteza de M é exatamente o que a migração preventiva busca neutralizar. A Tabela 2 apresenta uma avaliação exploratória dos setores brasileiros segundo os eixos M, P e E.

Tabela 2 – Espaço de decisão do framework QRA-PQC

Pressão de adoção (P)	E baixa	E alta
P baixa	Monitorar	Planejar inventário criptográfico
P alta	Migrar oportunisticamente	Migrar imediatamente (HNDL crítico)

Fonte: Autores (2026)

6 IMPLICAÇÕES SETORIAIS GLOBAIS

A aplicação do QRA-PQC aos cinco setores analisados revela prioridades distintas. Em armazenamento, a incorporação de mecanismos PQC pela Western Digital (WESTERN DIGITAL, 2026) fortalece a raiz de confiança, a inicialização segura e a proteção do firmware; tal medida, isoladamente, não implica migração da cifragem dos dados em repouso. Em chips e dispositivos, a colaboração SEALSQ-Quobly (SEALSQ; QUOBLY, 2025) voltada à convergência entre hardware seguro e tecnologias quânticas atua simultaneamente sobre P e E, levando PQC à base da cadeia de confiança de hardware. Em telecomunicações, as aquisições da NuCrypt (QCi) e da ID Quantique (IonQ) criam simultaneamente oferta (P) e necessidade (E), dado que o tráfego de telecom é particularmente vulnerável à captura para decifração futura. Em defesa e infraestrutura crítica, o enquadramento de soberania eleva P a patamar mandatório. Em finanças, a longevidade de obrigações contratuais e a sensibilidade de dados posicionam o setor no octante de migração imediata quando há pressão regulatória.

A volatilidade de valuation observada – IPO da Quantinuum com forte demanda inicial seguida de desempenho pós-estreia menos convincente – não deve ser confundida com volatilidade do risco criptográfico. A tese de migração preventiva permanece válida mesmo que o ciclo financeiro do setor corrija, porque o eixo dominante da decisão é o tempo (HNDL), e não o preço dos ativos quânticos.

7 IMPLICAÇÕES PARA O BRASIL: DEFESA, SISTEMA FINANCEIRO E INFRAESTRUTURA CRÍTICA

7.1 Contexto e Urgência

O Brasil ocupa posição singular nesse quadro: é simultaneamente ator com bases industriais e tecnológicas relevantes (Polo Industrial de Manaus, setor aeroespacial, sistema bancário digitalizado) e país com elevada exposição setorial em face de

capacidades de defesa cibernética ainda em consolidação. O Sistema Defesa, Indústria e Academia de Inovação (SisDIA), promovido pelo DCT-EB (IMBEL, 2022), evidencia iniciativas de cooperação em inovação para a defesa; já a Política Nacional de Defesa (BRASIL, 2022) trata do ambiente de defesa em termos amplos, sem explicitar uma agenda de migração pós-quântica. O modelo HNDL é particularmente crítico para o Brasil: comunicações governamentais e militares cifradas hoje com algoritmos RSA ou ECC podem ser capturadas por adversários e decifradas quando capacidade quântica relevante estiver disponível – um horizonte que os roadmaps analisados aproximam para menos de dez anos em algumas arquiteturas.

7.2 Setor de Defesa

O eixo P do setor de defesa brasileiro é alto por razão dupla: a crescente classificação internacional da capacidade quântica como ativo de soberania (ESTADOS-MEMBROS DA UNIÃO EUROPEIA, 2023; COMISSÃO EUROPEIA, 2023) e a existência de sistemas de comando e controle (C2), comunicações militares (SICCUL) e demais sistemas militares que empregam criptografia clássica. O eixo E é igualmente alto, pois dados operacionais, de inteligência e de planejamento estratégico têm vida útil que facilmente ultrapassa dez anos. A combinação E-alto e P-alto posiciona o setor de defesa no quadrante de migração imediata do framework QRA-PQC. A recomendação prioritária é a incorporação de PQC como requisito normativo nos documentos e programas pertinentes do Ministério da Defesa, com inventário criptográfico dos sistemas críticos como primeiro passo operacional e adoção dos padrões NIST FIPS 203 (ML-KEM), FIPS 204 (ML-DSA) e FIPS 205 (SLH-DSA) como referência técnica (NIST, 2024a; NIST, 2024b; NIST, 2024c).

7.3 Sistema Financeiro Nacional

O Sistema Financeiro Nacional (SFN) apresenta o quadro regulatório mais avançado do Brasil em cibersegurança: a Resolução CMN 4.893/2021 (CMN, 2021) exige políticas de segurança cibernética e a Resolução BCB 85/2021 (BCB, 2021) regula serviços de nuvem. Contudo, nenhuma dessas normas referencia o risco quântico ou exige inventário criptográfico. O eixo P é alto em razão da crescente pressão internacional: o BIS e o FSB já identificam a transição PQC como risco sistêmico para o setor financeiro. O eixo E é crítico: obrigações contratuais, registros de crédito e comunicações interbancárias têm vida útil que pode superar duas décadas, tornando o HNDL um vetor de risco real e imediato. A recomendação é avaliar a ampliação do escopo da Res. CMN 4.893/2021 para incluir obrigatoriedade de inventário criptográfico e roadmap de migração PQC, em alinhamento com os padrões NIST 2024 e com as melhores práticas do setor bancário global (CMN, 2021; BCB, 2021).

7.4 Infraestrutura Crítica e LGPD

Setores de energia (ANEEL), telecomunicações (Anatel) e petróleo/gás (ANP) operam sistemas de controle industrial (ICS/SCADA) com ciclos de vida que frequentemente ultrapassam 20 anos, combinando alta E com P crescente à medida que referências regulatórias internacionais incorporam o risco quântico. A Lei Geral de Proteção de Dados Pessoais (LGPD) (BRASIL, 2018) não aborda criptografia pós-quântica como medida de segurança, criando lacuna regulatória relevante: dados pessoais sensíveis coletados hoje e cifrados com algoritmos clássicos podem ser expostos retroativamente via HNDL, comprometendo a adequação das organizações mesmo décadas após a coleta. A Tabela 3 sintetiza o posicionamento de cada setor brasileiro no espaço QRA-PQC, e a Tabela 4 sistematiza as lacunas identificadas e as recomendações formuladas.

Tabela 3 – Posicionamento exploratório de setores brasileiros no QRA-PQC

Setor	M	P	E	Recomendação QRA-PQC
Defesa (SICCUL, SisDIA, C2)	Médio	Alto	Alto	Migração imediata — mandato soberania
Sistema Financeiro Nacional (SFN)	Médio	Alto	Alto	Migração imediata — pressão BCB/ CMN
Infraestrutura crítica (energia, água)	Médio	Alto	Alto	Migração imediata — risco HNDL severo
Telecomunicações (Anatel)	Médio	Médio	Alto	Planejar inventário e migrar progressivamente
Saúde / dados pessoais sensíveis	Baixo	Médio	Médio	Monitorar e preparar roadmap LGPD-PQC

Fonte: Autores (2026)

Tabela 4 – Lacunas regulatórias e recomendações para o Brasil

Dimensão	Lacuna identificada	Recomendação
Defesa e segurança cibernética	Ausência de mandato explícito para PQC nos sistemas militares	Incorporar requisitos de PQC aos documentos e programas pertinentes do Ministério da Defesa e do DCT-EB
Sistema Financeiro	Regulação BCB/CMN ainda não referencia NIST FIPS 203-205	Ampliar escopo da Res. CMN 4.893/2021 para incluir inventário criptográfico e roadmap PQC
Proteção de dados (LGPD)	ANPD não aborda criptografia pós-quântica como medida de segurança	Regulamentação complementar da ANPD prevendo PQC como padrão de adequação futura
Infraestrutura crítica	Critérios de resiliência cibernética não contemplam risco quântico	Revisão dos planos setoriais de segurança cibernética (ANEEL, ANATEL, ANP) para incorporar eixo M-P-E

Fonte: Autores (2026)

7.5 Agenda de Transição PQC para o Brasil

A operacionalização do framework QRA-PQC no contexto brasileiro sugere uma agenda de transição estruturada em três horizontes. No curto prazo (até 2026), prioriza-se o inventário criptográfico nos sistemas de defesa e financeiro, mapeando

algoritmos em uso, suas dependências e os dados de maior vida útil. No médio prazo (2027–2029), a migração piloto deve contemplar os sistemas de C2 do Exército, as plataformas de liquidação financeira do SFN e os sistemas SCADA de infraestrutura crítica, com referência aos padrões NIST FIPS 203-205. No longo prazo (a partir de 2030), a migração plena deve estar concluída para todos os sistemas classificados como E-alto, com revisão periódica dos eixos M e P à medida que o ecossistema quântico evolui. Essa agenda é compatível com o horizonte identificado pela pesquisa KPMG/BSI – dez anos para áreas de alta segurança – e com o raciocínio de risco temporal discutido por Mosca (MOSCA, 2018), que relaciona a vida útil dos dados, o tempo necessário para a migração e o horizonte da ameaça quântica.

8 CONCLUSÃO

Este artigo demonstrou que a industrialização seletiva da computação quântica reorienta fundamentalmente a decisão de migração criptográfica: o risco não é a quebra imediata, mas a combinação de múltiplos vetores de pressão – maturação de roadmaps, comercialização de produtos adjacentes e o modelo HNDL – que tornam a proteção de dados futura uma questão presente. O framework QRA-PQC, estruturado nos eixos M (maturidade do vetor de ameaça), P (pressão de adoção) e E (exposição setorial), oferece instrumento analítico para priorizar a migração de forma racional, evitando tanto a inércia quanto a sobremigração.

A principal contribuição do trabalho, além da proposição do framework, é a sua aplicação ao contexto brasileiro: demonstrou-se que os setores de defesa, sistema financeiro e infraestrutura crítica do Brasil apresentam combinação E-alto e P-alto que justifica migração imediata, enquanto o arcabouço regulatório vigente – Res. CMN 4.893/2021, LGPD e normativos de defesa – apresenta lacunas significativas que precisam ser endereçadas com urgência. A agenda de transição proposta em três horizontes (inventário, migração piloto e migração plena) oferece caminho concreto para que organizações brasileiras não repitam o padrão identificado pela pesquisa KPMG/BSI: chegar atrasadas a uma janela de risco que o HNDL já tornou presente.

Como trabalhos futuros, sugere-se: a operacionalização quantitativa do índice Q = f(M, P, E) com calibração de pesos por setor a partir de inventários criptográficos reais; o desenvolvimento de métricas específicas para os eixos M e P no contexto regulatório brasileiro; e a validação empírica do framework em estudos de caso de organizações de defesa e infraestrutura crítica no Brasil, em particular nas instituições de defesa e no SFN.

REFERÊNCIAS

BANCO CENTRAL DO BRASIL (BCB). **Resolução BCB n. 85, de 8 de abril de 2021**. Dispõe sobre a política de segurança cibernética e serviços de dados e nuvem. Brasília, 2021. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?numero=85&tipo=Resolu%C3%A7%C3%A3o+BCB. Acesso em: 16 out. 2026.

BERNSTEIN, D. J.; LANGE, T. Post-quantum cryptography. **Nature**, v. 549, p. 188–194, 2017.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais. Diário Oficial da União, Brasília, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 16 out. 2026.

BRASIL. Ministério da Defesa. **Política Nacional de Defesa e Estratégia Nacional de Defesa**. Brasília, 2022.

CLOUD SECURITY ALLIANCE. **The harvest now, decrypt later threat and the urgency of post-quantum migration**. white paper, 2023.

COMISSÃO EUROPEIA. C**ommission Recommendation of 3.10.2023 on critical technology areas for the EU's economic security**. C(2023) 6689 final, Strasbourg, Oct. 2023.

CONSELHO MONETÁRIO NACIONAL (CMN). **Resolução CMN n. 4.893, de 26 de fevereiro de 2021**. Dispõe sobre a política de segurança cibernética e contratação de serviços de dados e nuvem. Brasília, 2021. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?numero=4893&tipo=Resolu%C3%A7%C3%A3o+CMN. Acesso em: 16 out. 2026.

D-WAVE QUANTUM. **D-Wave Charts a New Course to Fault-Tolerant Quantum Computing with Gate-Model Roadmap**. comunicado de imprensa, Palo Alto, CA, 1 jun. 2026.

ESTADOS UNIDOS. Department of Commerce. **Department of Commerce Announces Letters of Intent With 9 Companies for $2 Billion to Accelerate U.S. Leadership in Quantum Computing**. Washington, 21 maio 2026. Disponível em: https://www.nist.gov/news-events/news/2026/05/department-commerce-announces-letters-intent-9-companies-2-billion. Acesso em: 16 out. 2026.

ESTADOS-MEMBROS DA UNIÃO EUROPEIA. **European Declaration on Quantum Technologies**. European Union, Brussels, 2023.

IBM. IBM Commits More Than $10 Billion to Quantum Computing, Funding Its Roadmap from Today's Leading Systems to the World's First Fault-Tolerant Quantum Computers. **IBM Newsroom**, 2 jun. 2026. Disponível em: https://newsroom.ibm.com/2026-06-02-ibm-commits-more-than-10-billion-to-quantum-computing%2C-funding-its-roadmap-from-todays-leading-systems-to-the-worlds-first-fault-tolerant-quantum-computers. Acesso em: 16 out. 2026.

INDÚSTRIA DE MATERIAL BÉLICO DO BRASIL (IMBEL). **Conheça a atuação da IMBEL no Sistema Defesa, Indústria e Academia (SisDIA) do Exército Brasileiro**. 22 dez. 2022. Disponível em: https://imbel.gov.br/noticias/conheca-a-atuacao-da-imbel-no-sistema-defesa-industria-e-academia-sisdia-do-exercito-brasileiro. Acesso em: 16 out. 2026.

IONQ. **Trapped-ion quantum systems (Aria, Forte, Forte Enterprise, Tempo) and XHV technology**. comunicados corporativos, 2026.

IONQ; ID QUANTIQUE. **IonQ Completes Acquisition of ID Quantique, Cementing Leadership in Quantum Networking and Secure Communications. comunicado de imprensa**, 6 mai. 2025.

KPMG; BSI. **Market Survey on Cryptography and Quantum Computing**. KPMG Germany, 2023.

MICROSOFT. Mi**crosoft unveils Majorana 1, the world's first quantum processor powered by topological qubits**. Microsoft Azure Quantum, 19 fev. 2025.

MICROSOFT. **Majorana 2**: Microsoft's scalable quantum processor with reliable, long-lasting qubits. Microsoft Quantum, 2 jun. 2026. Disponível em: https://quantum.microsoft.com/en-us/insights/blogs/majorana-2-scalable-quantum-processor. Acesso em: 16 out. 2026.

MOSCA, M. **Cybersecurity in an era with quantum computers**: Will we be ready? IEEE Security & Privacy, v. 16, n. 5, p. 38–41, 2018.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). **Module-Lattice-Based Key-Encapsulation Mechanism Standard**. FIPS 203. Gaithersburg: NIST, 2024a. Disponível em: https://csrc.nist.gov/pubs/fips/203/final. Acesso em: 16 out. 2026.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). **Module-Lattice-Based Digital Signature Standard**. FIPS 204. Gaithersburg: NIST, 2024b. Disponível em: https://csrc.nist.gov/pubs/fips/204/final. Acesso em: 16 out. 2026.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). **Stateless Hash-Based Digital Signature Standard**. FIPS 205. Gaithersburg: NIST, 2024c. Disponível em: https://csrc.nist.gov/pubs/fips/205/final. Acesso em: 16 out. 2026.

OPEN QUANTUM DESIGN. **Open-source full-stack trapped-ion quantum computer**. 2026.

PRESKILL, J. Quantum computing in the NISQ era and beyond. **Quantum**, v. 2, p. 79, 2018. Disponível em: https://doi.org/10.22331/q-2018-08-06-79. Acesso em: 16 out. 2026.

QUANTINUUM. **Quantinuum Announces Closing of Upsized Initial Public Offering**. Comunicado, 5 jun. 2026. Disponível em: https://www.quantinuum.com/press-releases/quantinuum-announces-closing-of-upsized-initial-public-offering. Acesso em: 16 out. 2026.

QUANTUM COMPUTING INC. (QCI). **Acquisitions of Luminar Semiconductor and NuCrypt**; quantum-secured communications demonstration with Ciena at OFC 2026. comunicados corporativos, 2026.

QUOBLY. **Quobly secures €115 million Series A to bring silicon-based quantum computers to market**. comunicado de imprensa, Grenoble, França, 3 jun. 2026. Disponível em: https://www.quobly.io/press-releases/quobly-secures-e115-million-series-a-to-bring-silicon-based-quantum-computers-to-market/. Acesso em: 16 out. 2026.

QURECA. **Quantum Initiatives Worldwide**. QURECA, Glasgow, UK, 2025.

SEALSQ; QUOBLY. **SEALSQ and Quobly Announce Collaboration to Advance Secure and Scalable Quantum Technologies**. Comunicado, 21 nov. 2025. Disponível em: https://www.sealsq.com/investors/news-releases/sealsq-and-quobly-announce-collaboration-to-advance-secure-and-scalable-quantum-technologies. Acesso em: 16 out. 2026.

SHOR, P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. **SIAM Journal on Computing**, v. 26, n. 5, p. 1484–1509, 1997.

WESTERN DIGITAL. W**D Advances Next-Generation Trusted Infrastructure with Industry's First Post-Quantum Cryptography Hard Drives to Help Secure the Future of AI Data**. Comunicado, 18 maio 2026. Disponível em: https://www.westerndigital.com/en-se/company/newsroom/press-releases/2026/2026-05-18-wd-advances-next-generation-trusted-infrastructure-with-post-quantum-cryptography. Acesso em: 16 out. 2026.

Autoria

1 Manoel Fernandes Amaral Filho

Graduado em Direito pela Universidade Federal do Paraná; Professor de Propriedade Intelectual e Inovação na Universidade do Estado do Amazonas; Advogado; Oficial veterano do Exército Brasileiro; Pesquisador em criptografia pós-quântica, Doutorando em Engenharia Elétrica

https://orcid.org/0009-0006-6496-0539 • https://ror.org/02263ky35

2 Max Fortunato Cohen

Graduado em Ciências Econômicas pela Universidade Federal do Amazonas; Mestre em Administração pela Universidade Federal de Santa Catarina; Doutor em Administração de Empresas pela Fundação Getúlio Vargas; Empreendedor; Cientista de Dados

https://orcid.org/0009-0009-7440-4386 • maxfc@gvmail.br

3 Anderson Fernandes Pereira dos Santos

Graduado em Engenharia de Computação pelo Instituto Militar de Engenharia; Doutor em Modelagem Computacional pelo Laboratório Nacional de Computação Científica; Pós-Doutorado em Computação Quântica pelo Laboratório Nacional de Computação Científica; Pesquisador Associado ao Centro de Inovação Tecnológica Venturus; Oficial veterano do Exército Brasileiro; Professor

https://orcid.org/0000-0002-6754-4809 • anderson@ime.eb.br

Como citar este artigo

AMARAL FILHO, M. F.; COHEN, M. F.; SANTOS, A. F. P. Industrialização seletiva da computação quântica e prontidão PQC: framework QRA-PQC. **InterAção**, Santa Maria, v. 17, n. 3, e99408, p. 1-17, 2026. DOI 10.5902/2357797599408. Disponível em: https://dx.doi.org/10.5902/2357797599408. Acesso em: dia mês abreviado. ano.