

A Ilusão do Silêncio Quântico

A Realidade Comercial,
a Ameaça
Criptográfica e a
Transição Híbrida
da Indústria.

Guia Prático de
Governança e
Transição
Tecnológica.

O Cenário Mundial e as
Iniciativas do Ecosistema
Brasileiro.

EDITORA



João Roberto Peres

Significado da Capa: O Abismo de Luz

A concepção visual da capa sintetiza a tese central desta obra: o contraste entre a sobriedade da superfície e a efervescência tecnológica nos bastidores.

- **O Fundo Escuro em Azul-Petróleo/Grafite:** Representa o "silêncio editorial" da grande mídia e a aparente calma da superfície comercial B2C, onde a ausência de um produto de consumo de massa cria a falsa ilusão de que a computação quântica é uma promessa distante.
- **A Fenda Vertical Fina:** Simboliza a abertura estratégica conquistada pelo mercado B2B, pela infraestrutura em nuvem (QaaS) e pelas salvaguardas geopolíticas de Estado. É a ruptura por onde a realidade dos fatos se expõe aos líderes atentos.
- **A Luz Dourada e Azul-Ciano:** Representa a revolução operacional em curso. O dourado remete ao valor econômico tangível (mais de US\$ 12,6 bilhões captados só em 2025, ecossistemas industriais e investimentos estatais), enquanto o azul-ciano elétrico evoca a precisão científica dos qubits, dos átomos neutros e dos novos padrões de cibersegurança pós-quântica.

Trata-se de um convite visual para que executivos, juristas e decisões, ultrapassem a barreira do ceticismo e compreendam a transformação que já remodela o mercado global e o cenário brasileiro.

Declaração de Processo Criativo e Autoria

Esta obra foi produzida com o apoio de múltiplos sistemas de Inteligência Artificial Generativa (IAG), incluindo ferramentas como ChatGPT, Gemini, Claude, Copilot e outras, utilizadas nas etapas de pesquisa, levantamento técnico, estruturação de conteúdo e acabamento estilístico do texto.

O conteúdo não é resultado de uma geração autônoma ou isolada por algoritmos. É fruto de um processo iterativo, conduzido e supervisionado integralmente pelo autor, que definiu o escopo, a tese central, a estrutura dos capítulos e os prompts utilizados em cada etapa, além de revisar, corrigir e validar tecnicamente todo o conteúdo produzido com apoio dessas ferramentas.

A autoria intelectual desta obra é exclusivamente humana. As ferramentas de IAG atuaram como instrumentos de pesquisa e de apoio à redação, sob direção e responsabilidade integral do autor, único responsável pela precisão factual, pelas conclusões apresentadas e pelo conteúdo final publicado.

É possível que o processo de composição com apoio de diferentes ferramentas de IAG tenha deixado marcas estilísticas ou estruturais pontuais ao longo do texto. Tais marcas não alteram a autoria nem a responsabilidade intelectual da obra, que permanece integralmente do autor.

FICHA CATALOGRÁFICA E LICENÇA – simplificada.

A Ilusão do Silêncio Quântico: A Realidade Comercial, a Ameaça Criptográfica e a Transição Híbrida da Indústria

Versão Preliminar sem revisão, disponibilizada de forma livre e aberta.

AUTOR: João Roberto Peres - **ISNI:** 0000000530651258

Câmara Brasileira do Livro - **ISBN:** 978-65-02-33486-7

Distribuição - Digital em formato .PDF - tamanho final= 270321 kb~

LICENÇA: Esta obra não tem objetivo comercial - será distribuída de forma gratuita com base em licenciamento Creative Common **CC BY-NC** - Esta licença permite que os usuários distribuam, remixem, adaptem e criem obras derivadas a partir do material em qualquer meio ou formato, exclusivamente para fins não comerciais e desde que seja feita a devida atribuição ao criador/autor.

Hash SHA512 - do conteúdo original antes do pdf e do Hash:

e2e97d41a1f852affe6f133bae4b003919f62db7f113df1e36e9b829202b6d7abda4586c524e4f92ae22e2896b2c1ece50389fa278ab9e10a38210cf6a9242df F:\e-Book-Ilusão-do-silêncio-Quântico-26F\e-book-Ilusão-Quantica-26-vF.docx.

Prefácio do Autor

A Ponte Necessária para uma Nova Fronteira Digital

A evolução tecnológica raramente avança em linha reta. O que presenciamos nas últimas décadas, foi o salto vertiginoso dos microprocessadores, a onipresença dos sistemas em nuvem, a revolução dos dispositivos conectados na Internet das Coisas (IoT) e a consolidação da Inteligência Artificial em nossos fluxos de trabalho cotidianos, tudo isso é apenas o prólogo de um movimento incomparavelmente mais profundo. Estamos na iminência de testemunhar a fusão entre a capacidade de processamento quântico e a inteligência computacional, um evento estrutural que redefinirá a própria arquitetura do pensamento digital e levará os modelos de IA a patamares de processamento e descoberta até então restritos à ficção científica.

Um ponto merece destaque antes mesmo de o leitor avançar pelos capítulos seguintes: a tecnologia quântica não cresce em uma única direção. Ela se desdobra, simultaneamente, em processamento (a computação quântica propriamente dita), em comunicação (protocolos como a Distribuição Quântica de Chaves, ou QKD, sigla em inglês para Quantum Key Distribution) e em sensoriamento (magnetômetros, gravímetros e relógios atômicos de precisão extrema). Compreender apenas uma dessas vertentes e ignorar as demais é como avaliar o impacto da eletricidade observando somente o motor, sem considerar a rede de transmissão ou os sensores que a regulam. Por essa razão, este livro se esforça para tratar o fenômeno quântico de forma sistêmica, como um ecossistema de capacidades interdependentes, e não como uma tecnologia isolada esperando sua vez de amadurecer.

Esta pequena publicação nasce, precisamente, da necessidade de construir uma ponte.

Ao longo de minhas apresentações, conferências e diálogos com lideranças dos mais diversos setores, identifiquei uma lacuna persistente no mercado. De um lado, encontram-se especialistas técnicos imersos na matemática rigorosa dos estados quânticos, falando uma linguagem por vezes inacessível aos tomadores de decisão. Do outro, executivos corporativos, juristas, formuladores de políticas públicas, profissionais de cibersegurança e entusiastas da inovação que buscam compreender, de forma pragmática, o que está acontecendo nos bastidores e como essas transformações afetam suas estratégias de negócios, cadeias de suprimento e proteção de ativos.

Esta obra foi concebida para atuar como esse instrumento de apoio. A proposta que norteia cada capítulo a seguir é oferecer um guia preliminar, acessível e objetivo. Trata-se de um mapa de navegação inicial, desenhado para atingir múltiplos perfis de público, fornecendo o letramento técnico básico, o enquadramento regulatório e a clareza estratégica necessários para que qualquer profissional possa participar ativamente das discussões sobre o futuro da tecnologia, independentemente de sua formação de origem.

Do Silêncio Operacional à Urgência Prática

Há um fenômeno curioso no ecossistema da inovação: a grande mídia costuma medir o sucesso de uma tecnologia pela sua presença nas prateleiras de consumo de massa. Como o computador quântico não é, e provavelmente ainda vai demorar muito para ser, um dispositivo pessoal de consumo direto, criou-se a falsa sensação de que a tecnologia permanece confinada a laboratórios teóricos ou a um futuro distante, situado em algum ponto indeterminado das próximas décadas.

Nada poderia estar mais distante da realidade.

O silêncio que percebemos na superfície comercial B2C esconde uma efervescência sem precedentes nos bastidores B2B e na infraestrutura de Estado. Bilhões de dólares em investimentos privados e governamentais estão sendo injetados na criação de arquiteturas híbridas, onde CPUs e GPUs tradicionais trabalham em sintonia fina com Unidades de Processamento Quântico (QPUs). Avanços científicos práticos, como a manipulação de matrizes massivas de átomos neutros e a aprovação dos novos padrões globais de Criptografia Pós-Quântica (PQC) pelo NIST, demonstram que a corrida não é para o amanhã; ela é a realidade operacional de hoje.

Mais do que isso: a convergência entre a computação quântica e as redes neurais de Inteligência Artificial promete resolver gargalos computacionais que a infraestrutura clássica de supercomputadores jamais conseguiria superar. Desde a otimização de redes elétricas inteligentes (Smart Grids), rotas de logística de frotas autônomas e precificação de riscos financeiros em tempo real até a simulação molecular para a indústria farmacêutica e a resiliência operacional na Indústria 5.0, a aceleração quântica será o motor primário da próxima geração de IA e automação industrial.

Vale aqui uma distinção que retomaremos ao longo do livro. A Indústria 4.0 nos trouxe a conectividade digital e a automação em larga escala, mas o fez a partir de uma lógica centrada na máquina. A Indústria 5.0 propõe o movimento inverso: humaniza a produção industrial ao recolocar o trabalhador no centro da decisão, ao lado de robôs colaborativos e gêmeos digitais (digital twins), sem abrir mão da eficiência conquistada na fase anterior. Essa humanização, contudo, não é gratuita: ela exige um salto de capacidade que a infraestrutura clássica isolada não entrega, combinando poder computacional para processar cenários de complexidade exponencial, robótica avançada capaz de colaborar com segurança ao lado de seres humanos, e um sensoriamento de precisão excepcional para captar, em tempo real, variáveis físicas que hoje escapam aos instrumentos convencionais. É exatamente nesse ponto que as tecnologias quânticas, em suas três vertentes de processamento, comunicação e sensoriamento, deixam de ser curiosidade científica e passam a compor a espinha dorsal técnica da Indústria 5.0.

Contudo, essa mesma capacidade de processamento traz consigo uma sombra proporcional: o colapso iminente das barreiras criptográficas que protegem nossos dados, nossas transações financeiras e nossa infraestrutura crítica. A ameaça do Harvest Now, Decrypt Later (Capturar Agora, Decifrar Mais Tarde), somada aos novos marcos regulatórios compulsórios, como a Executive Order 14412 nos EUA, o EU Cyber Resilience Act na Europa e as diretrizes do US Cyber Trust Mark, impõe a necessidade de agir imediatamente na revisão de nossas matrizes de cibersegurança, governança corporativa e conformidade legal. Como o leitor verá adiante, a resposta a essa ameaça também não é única: a Criptografia Pós-Quântica desponta como o caminho primário e mandatório, enquanto a Distribuição Quântica de Chaves surge como recurso complementar para os ativos de maior valor estratégico.

Como evidenciado por iniciativas de destaque no país, a exemplo das discussões promovidas pela FAPESP, pela infraestrutura do Sistema S (SENAI CIMATEC e SENAI-SP) e pelo hub CIQuanta na Paraíba, a adequação dos ativos digitais e dos dispositivos de IoT/AIoT deixou de ser um projeto futuro de TI para se consolidar como imperativo presente de sobrevivência comercial e conformidade regulatória.

Aqui cabe uma última observação, talvez a mais importante para situar corretamente o alcance desta obra. O conjunto de estruturas tecnológicas que reunimos sob o termo genérico de IoT, Internet das Coisas, não é uma tecnologia única, mas o resultado de uma alta interdependência entre inúmeras outras tecnologias: sensores, redes de comunicação, protocolos de segurança, plataformas de nuvem e, cada vez mais, capacidade de processamento quântico na ponta. Este livro aglutina apenas um breve panorama dessa teia. Os benefícios das tecnologias quânticas não caminham sozinhos; eles se somam e se potencializam com o avanço simultâneo da Inteligência Artificial, dos gêmeos digitais que replicam ativos físicos em ambiente virtual, dos metaversos industriais que permitem simular processos produtivos inteiros antes de sua

execução física, e das tecnologias hápticas de interface cérebro-computador, que começam a aproximar a intenção humana da resposta da máquina em tempo real. Não é objetivo desta obra esgotar cada uma dessas frentes, mas sim deixar claro ao leitor que nenhuma delas deve ser avaliada isoladamente. O impacto real só se revela quando olhamos para o ecossistema como um todo.

Uma Contribuição no Vasto Horizonte da Transição Quântica

É de fundamental importância ressaltar que esta publicação não pretende, e nem poderia esgotar a complexidade do tema. Ela cumpre o seu papel ao atuar como um material de apoio conciso, um catalisador de discussões e um nivelador de conhecimento para apresentações, treinamentos e palestras.

Esta obra é uma breve contribuição complementar que se conecta e serve de introdução a um trabalho de fôlego muito mais amplo e aprofundado: o meu livro "Ameaças Quânticas: Riscos Reais, Verdades Técnicas e Ações Práticas 2026-2035" (Registrado na Câmara Brasileira do Livro - CBL sob o ISBN 978-65-01-87573-6).

Portanto, convido o leitor a encarar as poucas páginas a seguir como o primeiro passo de uma jornada contínua. Se este pequeno guia conseguir despertar a sua curiosidade, esclarecer os conceitos fundamentais sobre arquiteturas híbridas e alertar sua organização sobre a urgência de mapear seus ativos criptográficos e seu ecossistema tecnológico de forma ampla, ele terá cumprido plenamente a sua missão.

Agradecimentos e Diálogo Aberto

Agradeço sinceramente pela sua leitura, pela confiança dedicada a este material e pelo interesse genuíno em se antecipar a uma das maiores transformações tecnológicas da história da humanidade. A construção de uma cultura de inovação consciente e segura no Brasil e no mundo depende diretamente do engajamento de lideranças como você, dispostas a aprender, questionar e liderar a transição.

Coloco-me inteiramente à disposição para consultas, trocas de ideias, palestras e debates sobre como aplicar esses conceitos na realidade específica da sua empresa, instituição ou projeto. O futuro pós-quântico e a Indústria 5.0 não precisam ser um mistério assustador; com a informação correta, a visão sistêmica do ecossistema e a preparação adequada, ele se torna uma extraordinária janela de oportunidade.

Boa leitura e excelente jornada de assimilação!

João Roberto Peres

Sumário

Prefácio do Autor.....	3
Capítulo 1: O Paradoxo da Visibilidade e o Mercado Quântico	8
1.1. As Barreiras Estruturais da Visibilidade Midiática	8
1.2. A Realidade Econômica e a Maturidade do Mercado Global	9
1.3. O Paradigma do Hardware: Da Criogenia à Miniaturização em Temperatura Ambiente	10
1.4. O Provedor de Serviços Quânticos via Nuvem (QaaS).....	11
Referências Capítulo 1	13
Capítulo 2: A Ameaça Criptográfica, Cibersegurança Post-Quantum e a Proteção de Ativos Críticos	14
2.1. O Apocalipse Criptográfico: Do Algoritmo de Shor ao Encurtamento do Q-Day pelo Caltech	14
2.2. A Ameaça Imediata: O Fenômeno Harvest Now, Decrypt Later (HNDL)	14
2.2.1. A Resposta Física ao Risco Quântico: Distribuição Quântica de Chaves (QKD) e sua Complementaridade com o PQC	16
2.3. Impactos no Setor Financeiro: Da Operação de Pagamentos ao Open Finance	17
2.4. A Convergência Regulatória Global em IoT/AIoT: EU Cyber Resilience Act e US Cyber Trust Mark	17
2.5. A Resposta Regulatória: Os Padrões PQC do NIST e a Mandatariedade da Executive Order 14412	18
2.6. Governança, LGPD e Responsabilidade Civil para Lideranças e Juristas.....	20
Referências Capítulo 2	21
Capítulo 3: A Tese Central: A Arquitetura Híbrida e as Aplicações Práticas do Presente	22
3.1. A Desmistificação da Substituição: O Conceito de QPU e Aceleração Especializada.....	22
3.2. A Mecânica do Processamento Híbrido: Algoritmos Variacionais e Orquestração	24
3.3. Casos de Uso no Setor Financeiro: Eficiência de Capital e Gestão de Risco	25
3.4. Casos de Uso em IoT e AIoT: Otimização na Ponta e Redes Inteligentes	26
Referências Capítulo 3	27
Capítulo 4: O Ecossistema Brasileiro: O Papel do Sistema S, P&D e a Capacitação da Indústria Nacional	28
4.1. O Panorama da Computação Quântica no Brasil	28
4.2. O Papel Estratégico do Sistema S: Do SENAI CIMATEC às Escalas Locais	29
4.3. Oportunidades de Fomento, Incentivos Fiscais e Parcerias Público-Privadas	29
4.4. O Cenário de Negócios: Startups e o Ecossistema de Inovação Aberta	31
4.5. A Década da Indústria 5.0: Da Origem com Michael Rada e Sociedade 5.0 à Resiliência Quântica	31
4.5.1. A Quarta Dimensão: Sensoriamento Quântico e Manutenção Preditiva na Indústria 5.0	32
Nota do Autor: Colaboração com o Sistema S	34
Referências Capítulo 4	35
Capítulo 5: Roadmap Estratégico, Governança Jurídica e o Plano de Ação para Líderes	36
5.1. O Roadmap Estratégico para Lideranças Corporativas	36
5.2. Checklist de Prontidão Operacional: Setor Financeiro e IoT/AIoT	37
5.3. Matriz de Governança Jurídica, LGPD e Responsabilidade Civil	38
Referências Capítulo 5	40
Anexo 1: Glossário Executivo Quântico-Técnico	41

Anexo 2: Checklist de Auditoria e Readiness (Matriz de Prontidão PQC)	45
Anexo 3: Modelo de Cláusula Contratual PQC (Criptografia Pós-Quântica)	49
Anexo 4: Matriz Comparativa dos Padrões PQC do NIST (FIPS 203, 204 e 205).....	51
Criptografia para IoT	52
Referências Anexo 4	53
Anexo 5: Evidência Recente de Mercado – O Ecossistema de São Paulo e o Debate FAPESP	54
Referência Anexo 5	54
Anexo 6: Tabela de Enquadramento Regulatório Internacional de IoT/AIoT e Indústria 5.0	55
Anexo 7: A Consolidação da Indústria 5.0 e o Horizonte Ainda Aberto da Indústria 6.0	57
Nota do Autor: Um Registro Pessoal Nesta Trajetória	60
Referências Anexo 7	61
Sobre o Autor	62

Capítulo 1: O Paradoxo da Visibilidade e o Mercado Quântico

A percepção pública sobre a computação quântica é marcada por um contraste profundo. Para o público em geral e a grande imprensa, o tema ainda é retratado como um conceito de ficção científica, um experimento restrito a laboratórios universitários ou uma promessa distante reservada para as próximas décadas. No entanto, longe dos holofotes da mídia tradicional, o ecossistema corporativo, financeiro e estatal já movimenta bilhões de dólares, estabelecendo as bases de uma infraestrutura operacional e comercial ativa.

Compreender o momento atual do setor exige investigar as causas estruturais desse desalinhamento entre a percepção pública e a realidade do mercado, analisar as métricas econômicas globais e examinar as tecnologias e modelos de negócios que já viabilizam a comercialização dessas arquiteturas no presente.

1.1. As Barreiras Estruturais da Visibilidade Midiática

A baixa frequência com que a computação quântica aparece notícias de grande circulação não reflete uma falta de progresso tecnológico, mas sim a convergência de fatores geopolíticos, mercadológicos e de comunicação. Ao contrário da revolução da computação pessoal ou da internet, a transformação quântica não ocorre na camada visível do consumo diário.

Geopolítica, Soberania e Salvaguardas de Estado

A computação quântica ultrapassou as fronteiras da pesquisa acadêmica pura e tornou-se um dos ativos mais críticos de segurança nacional e soberania do século XXI. As principais potências mundiais, com destaque para Estados Unidos, China e algumas nações da União Europeia, enxergam a tecnologia sob a ótica da computação de alto desempenho com implicações diretas na defesa, indústria de consumo, finanças, cibersegurança e criptografia.

Dispositivos e algoritmos capazes de quebrar os padrões internacionais de criptografia ou de simular materiais estratégicos para a indústria de defesa estão sujeitos a rígidos regimes de segredo de Estado e controles severos de exportação. A Lei de Controle de Exportação de Tecnologia dos Estados Unidos e as diretrizes de segurança de dados da China restringem severamente a divulgação de avanços em hardware de ponta e algoritmos específicos. Consequentemente, uma parcela expressiva dos desenvolvimentos mais avançados do setor permanece resguardada sob sigilo governamental, longe das coletivas de imprensa e dos relatórios públicos.

O mesmo regime de controle e sigilo se estende, com igual ou maior intensidade, ao **sensoriamento quântico** apresentado no Capítulo 4, item 4.5.1. Magnetômetros, gravímetros e relógios atômicos de precisão têm aplicação civil evidente na Indústria 5.0, mas também aplicação direta em navegação inercial sem sinal de satélite, detecção de submarinos e vigilância geofísica, o que os classifica como tecnologia de uso dual (dual-use technology, aquela que serve simultaneamente a propósitos civis e militares). Por essa razão, sensores quânticos de alta sensibilidade frequentemente aparecem nas mesmas listas de controle de exportação que regulam componentes de hardware de computação quântica, e sua aquisição por empresas e centros de pesquisa brasileiros pode estar sujeita a licenciamento prévio junto às autoridades do país de origem do equipamento.

O Modelo B2B e a Ausência de Apelo de Massa

A computação clássica conquistou espaço no ecossistema de mídia porque gerou produtos de consumo de massa, operando no modelo B2C, sigla em inglês para *Business-to-Consumer* (operações voltadas diretamente ao consumidor final). O surgimento dos computadores pessoais, dos smartphones e

dos aplicativos de uso cotidiano criou uma relação direta e perceptível entre a inovação tecnológica e a vida diária dos indivíduos.

A computação quântica, contudo, opera estritamente no modelo B2B, sigla para *Business-to-Business* (operações comerciais realizadas entre empresas), voltando-se para o mercado corporativo, grandes instituições financeiras, centros de pesquisa e infraestruturas críticas. O valor gerado pela tecnologia não se materializa em um software de uso pessoal, mas em otimizações complexas de cadeias de suprimentos globais, simulações moleculares para a indústria farmacêutica, análise de risco financeiro em tempo real e treinamento de modelos de inteligência artificial. Por não gerar um produto de prateleira ou uma interface direta com o público geral, o setor perde o apelo sensacionalista que costuma pautar a grande mídia.

A Barreira da Tradução Jornalística nas Redações

A cobertura de tecnologias profundas (*deep techs*) exige um nível de especialização técnica que escasseia nas redações tradicionais. Os princípios fundamentais da mecânica quântica, como a superposição de estados (a capacidade de um sistema existir em múltiplos estados simultaneamente) e o emaranhamento quântico (a correlação instantânea entre partículas independentes da distância), desafiam a intuição clássica e são difíceis de traduzir para o público leigo sem incorrer em simplificações excessivas ou imprecisões conceituais.

O custo elevado de apuração, somado à falta de letramento científico especializado nos veículos de imprensa generalistas, resulta em uma esquiva editorial. Na maioria das vezes, o tema só é abordado diante de anúncios institucionais de grandes corporações ou quando associado a termos alarmistas, omitindo a evolução gradual e consistente que ocorre nos bastidores da indústria.

1.2. A Realidade Econômica e a Maturidade do Mercado Global

Apesar do silêncio na imprensa de massa, os dados de inteligência de mercado revelam um ecossistema econômico em consolidação, amparado por volumes expressivos de capital privado e estatal.

Conforme apontam os relatórios *McKinsey Quantum Technology Monitor 2024,2025 e 2026* os investimentos os investimentos em tecnologias quânticas atingiram a marca de 12,6 bilhões de dólares somente em 2025, um salto de 6,3 vezes em relação ao ano anterior, e as projeções seguem exponenciais. Além disso, governos de diversos países já anunciaram mais de 40 bilhões de dólares em compromissos públicos de longo prazo para pesquisa, desenvolvimento e infraestrutura no setor.

- Investimento Privado e Capital de Risco acumulado: > US\$ 12,6 bilhões
- Compromissos Públicos e Estatais Globais: > US\$ 40,0 bilhões - com o Japão sozinho comprometendo US\$ 7,4 bilhões.
- Empresas mapeadas na Cadeia de Valor Quântica: > 1.100 companhias
- Companhias com Capital Aberto em Bolsa: 29 empresas

O ecossistema global é composto por mais de 1.100 empresas mapeadas ao longo de toda a cadeia de valor. Essa estrutura abrange desde fabricantes de componentes altamente especializados (como lasers de precisão, isoladores criogênicos e materiais de altíssima pureza) até desenvolvedores de algoritmos, provedores de software e grandes fornecedores de infraestrutura de nuvem.

Atualmente, cerca de 30 companhias focadas no desenvolvimento quântico possuem capital aberto em bolsas de valores globais (como a NYSE e a NASDAQ), submetendo suas operações a auditorias financeiras rigorosas, governança corporativa e divulgação pública de resultados operacionais. Esse cenário demonstra

que o setor deixou de ser um campo restrito ao financiamento universitário e passou a integrar a dinâmica do mercado de capitais internacional.

1.3. O Paradigma do Hardware: Da Criogenia à Miniaturização em Temperatura Ambiente

Para compreender a aplicação prática do hardware quântico, é necessário desconstruir um dos maiores mitos do setor: o de que todos os computadores quânticos exigem instalações gigantescas e sistemas de refrigeração complexos.

Sistemas Criogênicos Tradicionais

Os modelos mais conhecidos de computadores quânticos, como os desenvolvidos por gigantes de tecnologia utilizando qubits supercondutores ou íons aprisionados, dependem de ambientes térmicos extremos. Para que os bits quânticos (qubits) mantenham a coerência e realizem operações sem a interferência do ruído térmico do ambiente, os processadores precisam ser abrigados em criostatos de diluição (equipamento de laboratório avançado usado para alcançar temperaturas ultrabaixa). Esses equipamentos mantêm o chip a temperaturas próximas ao zero absoluto, cerca de -273 graus Celsius (ou 15 milikelvins), tornando o hardware dependente de instalações de grande porte e com alto consumo energético.

A Fronteira da Temperatura Ambiente e os Dispositivos Compactos

A visão tradicional de que o hardware quântico jamais sairá de centros de dados especializados está sendo ativamente desafiada por novas arquiteturas baseadas em física de estado sólido e óptica.

Um exemplo emblemático é a tecnologia desenvolvida pela *Quantum Brilliance*, empresa que utiliza centros de vacância de nitrogênio (*NV centers*) em diamantes sintéticos. Nesses sistemas, os spins dos elétrons e dos núcleos atômicos no diamante funcionam como qubits capazes de operar em temperatura ambiente, dispensando completamente os sistemas de refrigeração criogênica ou sistemas a vácuo complexos.

Essa abordagem permite a miniaturização do hardware quântico para formatos compactos, operáveis em servidor montável em *rack* (*rack-mountable*). O objetivo dessa arquitetura é integrar os aceleradores quânticos diretamente em ambientes de computação de alto desempenho (HPC), nas plataformas de *Edge Computing* (computação na ponta convencional aditivada) e até de pequenos data centers.



Aplicação na Educação e Formação Profissional no Brasil

A miniaturização e a viabilização de sistemas em temperatura ambiente já possuem aplicações concretas na formação de mão de obra e na pesquisa aplicada no Brasil desde 20225. Um exemplo prático é a adoção pelo SENAI-SP (Serviço Nacional de Aprendizagem Industrial) de computadores quânticos didáticos e de bancada, como os desenvolvidos pela empresa **SpinQ**.

Esses equipamentos, baseados na tecnologia de Ressonância Magnética Nuclear (RMN) operam em temperatura ambiente, são dispositivos portáteis para salas de aula e laboratórios de inovação. Eles permitem que alunos, engenheiros e pesquisadores executem algoritmos quânticos reais, compreendam a manipulação de qubits e desenvolvam aplicações práticas sem a necessidade de infraestrutura industrial complexa.

Essas iniciativas comprovam que o hardware quântico não é apenas viável em formatos reduzidos, mas já está sendo utilizado como ferramenta de capacitação técnica no ecossistema industrial brasileiro.

SPINQ Triângulo™ II

Computador quântico NMR de mesa de 3 qubits

Oferece uma solução completa para o ensino e demonstrações de computação quântica, suportando qualquer algoritmo quântico de 3 qubits e permitindo que os usuários escrevam programas quânticos livremente. Também apresenta edição de sequência de pulsos em nível de hardware aberto. Além disso, é econômico, não requer manutenção e é altamente estável.



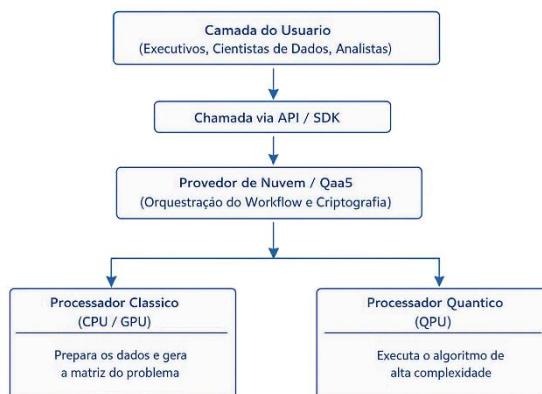
<https://www.notebookcheck.info/A-SpinQ-apresenta-os-primeiros-computadores-quanticos-portateis-do-mundo.675355.0.html>

1.4. O Provedor de Serviços Quânticos via Nuvem (QaaS)

A coexistência entre supercomputadores criogênicos de alto desempenho e aceleradores compactos em temperatura ambiente é viabilizada comercialmente pelo modelo QaaS, acrônimo em inglês para *Quantum-as-a-Service* (Computação Quântica como Serviço).

No modelo tradicional de tecnologia da informação, a aquisição de infraestrutura física exige grandes investimentos de capital (*CAPEX - Capital Expenditure*). No cenário quântico, a complexidade de manutenção do hardware torna a compra direta inviável para a imensa maioria das corporações.

O modelo QaaS resolve essa barreira ao integrar o hardware quântico à infraestrutura da computação em nuvem clássica:



Por meio de APIs, sigla em inglês para *Application Programming Interface* (Interface de Programação de Aplicações), que são conjuntos de rotinas e padrões que permitem a comunicação entre diferentes

softwares), desenvolvedores e analistas conectam-se remotamente a processadores quânticos (QPUs, ou *Quantum Processing Units*).

O usuário escreve o código utilizando bibliotecas de programação padrão, envia o problema via nuvem e recebe o resultado do processamento. O pagamento é realizado sob demanda com base no tempo de uso do processador, transformando o custo de capital em despesa operacional (*OPEX - Operational Expenditure*). Esse formato democratiza o acesso à tecnologia e permite que empresas testem algoritmos de otimização, simulações e modelos de risco no presente, preparando suas operações para a era híbrida.

Referências Capítulo 1

ASSOCIATION FOR COMPUTING MACHINERY. **ACM TechNews: Public Sector Quantum Funding Tops \$40B Globally**. New York: ACM, 2024.

BCG - BOSTON CONSULTING GROUP. **Can Quantum Computing Fight Climate Change?** Boston: BCG, 2023. Disponível em: <https://www.bcg.com>. Acesso em: 24 ago. 2026.

MCKINSEY & COMPANY. **McKinsey Quantum Technology Monitor 2024**. [S. l.]: McKinsey & Company, 2024. Disponível em: <https://www.mckinsey.com>. Acesso em: 24 ago. 2026.

MCKINSEY & COMPANY. **McKinsey Quantum Technology Monitor 2026**. [S. l.]: McKinsey & Company, 2026. Disponível em: <https://www.mckinsey.com>. Acesso em: 24 ago. 2026.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). **Post-Quantum Cryptography Standardization**. Gaithersburg: U.S. Department of Commerce, 2024. Disponível em: <https://csrc.nist.gov>. Acesso em: 24 ago. 2026.

PUPILLO, Lorenzo; FERREIRA, Afonso; LIPIÄINEN, Valtteri; POLITO, Carolina. Quantum Technologies and Cybersecurity: Technology, Governance and Policy Challenges. Task Force Report. Bruxelas: Centre for European Policy Studies (CEPS), dez. 2023. Disponível em: <https://cdn.ceps.eu/wp-content/uploads/2023/12/CEPS-TFR-Quantum-Technologies-and-Cybersecurity.pdf>. Acesso em: 24 ago. 2026.

QUANTUM BRILLIANCE. **Diamond Quantum Microprocessors: Edge Computing and Ambient Temperature Architecture**. Canberra: Quantum Brilliance White Paper Series, 2023.

QUANTUM BRILLIANCE - **Universidade Nacional da Austrália** (ANU). Disponível em: <https://postquantum.com/quantum-computing-companies/quantum-brilliance/>. Acesso em 24 ago. 2026.

Quantum Brilliance Opens Commercial Quantum Diamond Foundry in Australia – disponível em: <https://thequantuminsider.com/2025/11/05/quantum-brilliance-opens-commercial-quantum-diamond-foundry-in-australia/>. Acesso em 24 ago. 2026;

Software for Massively Parallel Quantum Computing – disponível em: <https://arxiv.org/abs/2211.13355>. Acesso em: 24 ago. 2026.

Fabrication of oriented NV center arrays in diamond via femtosecond laser writing and reorientation – disponível em: https://www.researchgate.net/publication/395784408_Fabrication_of_oriented_NV_center_arrays_in_diamond_via_femtosecond_laser_writing_and_reorientation. Acesso em 24 ago. 2026.

Incorporating physical footprint into quantum computing performance benchmarks – disponível em: <https://arxiv.org/pdf/2303.02138>

SENAI-SP. **Computação Quântica na Indústria: Capacitação e Adoção de Tecnologias Emergentes**. São Paulo: Editora SENAI, 2024.

SENAI-SP lança pós-graduação em Computação Quântica – disponível em: <https://www.sp.senai.br/noticia/senai-sp-lanca-pos-graduacao-em-computacao-quantica>. Acesso em: 24 ago. 2026.

Primeiro computador quântico para fins educacionais chega ao Brasil – 09/04/2024 – Disponível em: <https://dobsliit.com/primeiro-computador-quantico-para-fins-educacionais-chega-ao-brasil/>. acesso em 24 de ago. 2026.

SENAI-cimatec LAQCC – disponível em: <https://guiin.senaicimatec.com.br/laqcc/>. Acesso em: 24 ago. 2026.

Primeiro centro de computação quântica no Brasil é inaugurado no SENAI CIMATEC – Disponível em: <https://noticias.portaldaindustria.com.br/noticias/inovacao-e-tecnologia/primeiro-centro-de-computacao-quantica-no-brasil-e-inaugurado-no-senai-cimatec/>. Acesso em: 24 ago. 2026

Capítulo 2: A Ameaça Criptográfica, Cibersegurança Post-Quantum e a Proteção de Ativos Críticos

A expansão da computação quântica impõe uma dualidade inevitável ao ambiente de negócios: ao mesmo tempo em que oferece avanços inéditos em capacidade de processamento, a tecnologia coloca em risco direto a infraestrutura de cibersegurança que sustenta o comércio eletrônico, a privacidade de dados e as operações financeiras globais.

Para executivos do setor financeiro, gestores de redes de IoT, sigla em inglês para *Internet of Things* (Internet das Coisas), AIoT, combinação de *Artificial Intelligence* e *Internet of Things* (Inteligência Artificial aplicada à Internet das Coisas), e profissionais do Direito Digital, a transição para arquiteturas quânticas não é um debate acadêmico, mas um imperativo de governança, conformidade e mitigação de riscos operacionais.

2.1. O Apocalipse Criptográfico: Do Algoritmo de Shor ao Encurtamento do Q-Day pelo Caltech

A base da segurança digital contemporânea repousa na criptografia de chave pública, ou criptografia assimétrica. Sistemas amplamente disseminados como RSA, acrônimo referente aos criadores Rivest, Shamir e Adleman, e ECC, sigla para *Elliptic Curve Cryptography* (Criptografia de Curva Elíptica), protegem desde transações bancárias e assinaturas digitais até o tráfego de dados na internet via protocolos HTTPS.

Esses métodos baseiam sua segurança na complexidade de resolver problemas matemáticos específicos em computadores clássicos, tais como a fatoração de números inteiros primos gigantescos ou o problema do logaritmo discreto. Um supercomputador clássico levaria milhares de anos de processamento contínuo para reverter uma chave RSA de 2048 bits por força bruta.

Em 1994, o matemático Peter Shor demonstrou que um computador quântico suficientemente potente, executando o chamado Algoritmo de Shor, é capaz de resolver esses problemas em tempo polinomial, derivando a chave privada a partir da chave pública em questão de minutos.

O momento em que um computador quântico atingir escala técnica para quebrar esses padrões criptográficos é denominado no mercado como Q-Day (Dia Quântico). Até recentemente, a projeção do mercado estimava que o Q-Day exigiria milhões de qubits físicos para viabilizar a correção de erros quânticos. No entanto, pesquisas de ponta desenvolvidas no Caltech (*California Institute of Technology*), lideradas pelo laboratório do professor Manuel Endres, alteraram drasticamente esse horizonte.

Ao montar uma matriz de 6.100 qubits de átomos neutros (átomos de césio aprisionados por pinças ópticas a laser) operando com alta fidelidade e conectividade dinâmica, o Caltech provou que novos códigos de correção de erros de alta taxa (*high-rate codes*) reduzem a necessidade de redundância em mais de 100 vezes. Da mesma forma indicou ser capaz de produzir matrizes muito maiores de imediato.

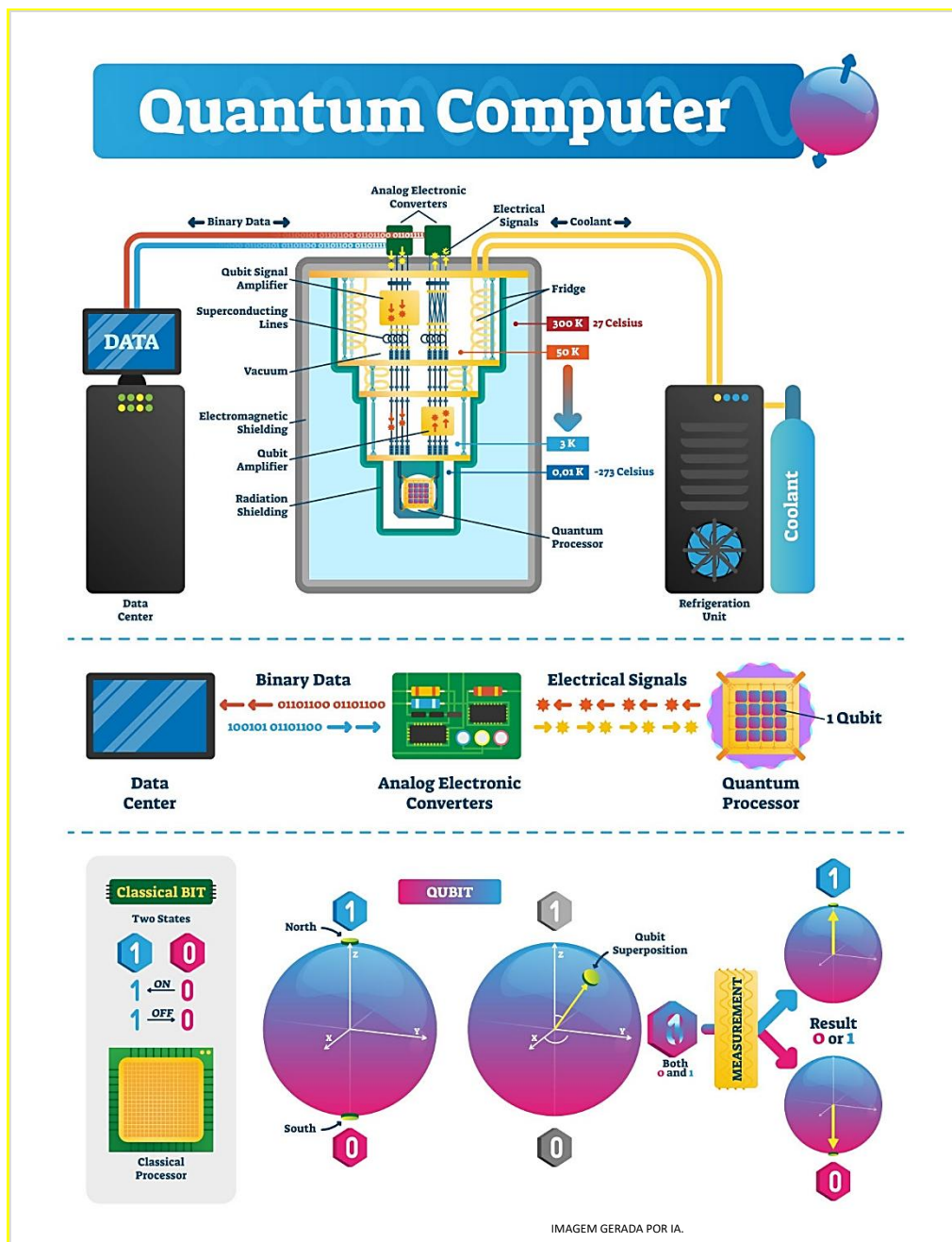
Isso significa que a quantidade de qubits físicos necessária para construir um computador quântico tolerante a falhas (capaz de executar o Algoritmo de Shor) caiu do patamar em qubits físicos, reduzindo a janela estimada para o Q-Day de forma expressiva. **Obs.:** Esse é um campo de muita polemica acadêmica.

2.2. A Ameaça Imediata: O Fenômeno Harvest Now, Decrypt Later (HNDL)

Existe uma percepção equivocada de que o risco criptográfico só se materializará no dia em que o hardware quântico estiver plenamente construído. No entanto, agentes maliciosos, grupos de cibercrime

organizado e serviços de inteligência estatal já praticam ativamente o ataque HNDL, sigla em inglês para *Harvest Now, Decrypt Later* (Capturar Agora, Decifrar Mais Tarde).

Essa tática consiste em interceptar e armazenar hoje volumes massivos de dados criptografados que trafegam em redes públicas e privadas (como segredos industriais, dados médicos, registros bancários e comunicações governamentais). Embora o invasor não consiga ler o conteúdo no momento da captura, ele guarda esses pacotes de dados até que um processador quântico os decifre retrospectivamente.



Para organizações que lidam com dados cuja confidencialidade precisa ser preservada por dez, vinte ou trinta anos (como informações de patentes, dados contratuais e registros de segredo de estado), o risco do HNDL não é uma hipótese futura: é uma vulnerabilidade ativa no presente.

A urgência dessa migração pode ser formalizada ou compreendida tecnicamente por meio do framework de referência na literatura de cibersegurança pós-quântica nominado “Desigualdade de Mosca” (Mosca, 2018), para determinar o momento correto de agir. O modelo compara três variáveis temporais: **X**, o tempo necessário para migrar integralmente os sistemas de uma organização para a Criptografia Pós-Quântica; **Y**, o tempo de vida útil da confidencialidade dos dados protegidos (quanto tempo essa informação

precisa permanecer sigilosa); e **Z**, o tempo estimado até que um computador quântico criptograficamente relevante (CRQC) esteja operacional. Sempre que $X + Y > Z$, a organização já está, hoje, em situação de risco: seus dados serão decifrados antes mesmo que a migração seja concluída. Para setores que lidam com sigilo de longo prazo, segredos industriais, dados médicos, registros de patentes, em que **Y** hipoteticamente pode ultrapassar dez ou vinte anos, a inequação frequentemente já está desfavorável mesmo sob estimativas conservadoras de **Z**, reforçando o caráter presente, e não hipotético, do risco HNDL discutido nesta seção.

2.2.1. A Resposta Física ao Risco Quântico: Distribuição Quântica de Chaves (QKD) e sua Complementaridade com o PQC

Diante do risco representado pelo Algoritmo de Shor e pelo fenômeno HNDL, sigla em inglês para Harvest Now, Decrypt Later (Capturar Agora, Decifrar Mais Tarde), o mercado e os órgãos reguladores discutem duas respostas tecnológicas distintas, que não devem ser confundidas pelo leitor: a Criptografia Pós-Quântica (PQC), já apresentada nas seções anteriores, e a Distribuição Quântica de Chaves, conhecida pela sigla em inglês QKD, para Quantum Key Distribution.

Enquanto a PQC é uma solução matemática, executada em software sobre hardware clássico convencional, a QKD é uma solução física. Ela utiliza as propriedades da mecânica quântica, especificamente o princípio da não clonagem (no-cloning theorem, que estabelece a impossibilidade de copiar um estado quântico desconhecido sem alterá-lo), para transmitir chaves criptográficas por meio de fótons individuais. Qualquer tentativa de interceptação da chave por um agente malicioso perturba fisicamente o estado quântico transmitido, revelando a presença do invasor aos usuários legítimos antes mesmo que a comunicação sensível seja iniciada. O protocolo pioneiro nessa técnica, conhecido como BB84, foi proposto em 1984 e permanece como referência conceitual para a maioria das implementações comerciais atuais.

Apesar do apelo teórico de uma segurança baseada em leis da física, e não em complexidade matemática, a QKD enfrenta limitações práticas relevantes que a diferenciam do caminho adotado pelo NIST para a PQC:

- **Dependência de Infraestrutura Física Dedicada:** a QKD exige fibras ópticas especializadas ou enlaces de satélite dedicados, com alcance limitado a algumas centenas de quilômetros sem o uso de repetidores quânticos, tecnologia ainda em estágio experimental. A China opera hoje a rede de maior escala do mundo nesse campo, incluindo o satélite Micius e o backbone terrestre Pequim-Xangai, mas trata-se de investimento de infraestrutura de Estado, de custo elevado e replicação limitada.
- **Ausência de Autenticação Nativa:** a QKD protege a distribuição da chave, mas depende de um canal de autenticação clássico adicional para garantir a identidade das partes, o que significa que ela não substitui integralmente a infraestrutura de chave pública tradicional, apenas complementa uma etapa específica dela.
- **Escalabilidade e Custo:** por não trafegar sobre a internet convencional, a QKD não se beneficia da mesma economia de escala que a PQC, que pode ser distribuída via atualização de software em bilhões de dispositivos já existentes.

Por essas razões, a própria Agência de Segurança Nacional dos Estados Unidos (NSA), em suas diretrizes de Criptografia Comercial Nacional (CNSA 2.0), não aprova o uso de QKD para a proteção de Sistemas de Segurança Nacional, recomendando a PQC como caminho primário de migração. O posicionamento do NIST segue a mesma linha. Para o leitor executivo e jurídico, a conclusão prática é que a QKD deve ser compreendida como uma tecnologia complementar e de nicho, aplicável a enlaces ponto a ponto de altíssimo valor (como comunicação entre data centers de instituições financeiras centrais ou redes de defesa), e não como substituta do esforço de migração para PQC tratado ao longo deste capítulo.

2.3. Impactos no Setor Financeiro: Da Operação de Pagamentos ao Open Finance

O ecossistema financeiro é um dos alvos mais expostos e críticos do cenário quântico, dada a dependência intensiva de assinaturas digitais e canais seguros para validação de transações.

Open Finance e APIs Bancárias

As arquiteturas de Open Finance (sistema financeiro aberto) e de pagamentos instantâneos funcionam por meio de integrações de APIs protegidas pelo protocolo TLS, sigla em inglês para *Transport Layer Security* (Segurança da Camada de Transporte). O TLS utiliza o algoritmo ECC para o handshake (mecanismo de estabelecimento de conexão segura entre cliente e servidor). Caso o ECC seja comprometido, o tráfego de dados entre instituições bancárias e fintechs fica exposto a ataques de interceptação do tipo *Man-in-the-Middle* (Homem no Meio), em que o invasor pode alterar o valor ou o destino de transações.

Assinaturas Digitais e Não Repúdio

A infraestrutura de chaves públicas adotada pelo sistema financeiro utiliza certificados digitais baseados em RSA para garantir o não repúdio (princípio jurídico que impede a negação de autoria de uma transação ou contrato). Se a chave privada de uma autoridade certificadora ou de uma instituição financeira for derivada por um computador quântico, a autenticidade de contratos, transferências de custódia e registros contábeis perde validade jurídica, desestabilizando as garantias de mercado.

2.4. A Convergência Regulatória Global em IoT/AIoT: EU Cyber Resilience Act e US Cyber Trust Mark

Se no setor financeiro a migração de software em servidores centrais é um desafio complexo, porém gerenciável, no universo de IoT e AIoT o problema assume proporções físicas e estruturais.

Os ecossistemas de IoT abrangem bilhões de dispositivos conectados, como sensores industriais, medidores inteligentes de energia, atuadores de redes de transmissão, dispositivos médicos e unidades de controle veicular. Esses ecossistemas apresentam limitações severas quando expostos ao risco quântico:

- **Ciclo de Vida Extenso:** Dispositivos instalados em redes elétricas, turbinas ou automação predial são projetados para operar por 15 a 25 anos sem substituição de hardware.
- **Recursos Computacionais Limitados:** Chips embutidos em microcontroladores de IoT possuem restrições extremas de memória RAM e capacidade de processamento, sendo muitas vezes incapazes de executar algoritmos criptográficos que exijam chaves muito longas ou processamento pesado.
- **Ausência de Agilidade Criptográfica (*Crypto-Agility*):** A esmagadora maioria dos módulos de IoT atuais não possui capacidade de atualização remota de firmware segura para substituir os algoritmos de criptografia gravados no silício.

Um dispositivo de IoT implantado hoje que utilize criptografia assimétrica tradicional estará inevitavelmente vulnerável durante seu ciclo de vida útil. Se a rede de sensores for invadida por decifração quântica, agentes maliciosos poderão enviar comandos falsos para a infraestrutura física, paralisando plantas industriais ou manipulando redes de energia.

Critério	Criptografia Clássica (ECC/RSA)	Criptografia Pós-Quântica (PQC)
Tamanho da Chave	Pequeno (Ex: ECC 256 bits)	Elevado (Ex: ML-KEM-768 > 1KB)
Consumo de Memória RAM	Baixo	Moderado a Alto
Impacto no Hardware IoT	Compatível com microcontroladores simples	Requer suporte a novos processadores e memória
Resistência ao Q-Day	Nenhuma	Alta

A vulnerabilidade inerente aos dispositivos de Internet das Coisas (IoT) e Inteligência Artificial das Coisas (AIoT) deixou de ser encarada apenas como uma falha de engenharia para se tornar o foco central de novas barreiras regulatórias e comerciais internacionais. Com a consolidação do **EU Cyber Resilience Act (CRA)** na União Europeia e a implementação do programa **US Cyber Trust Mark** nos Estados Unidos, os dois maiores blocos econômicos do Ocidente estabeleceram requisitos compulsórios de cibersegurança baseados no princípio de *Security by Design* (segurança desde a concepção).

Essas normas introduzem obrigações diretas que afetam frontalmente a cadeia global de suprimentos (*supply chain*):

- **Inventário Criptográfico Obrigatório (CBOM):** Fabricantes e desenvolvedores de soluções conectadas são legalmente obrigados a mapear e declarar todos os componentes, bibliotecas e algoritmos criptográficos embarcados em seus dispositivos.
- **Capacidade de Atualização Remota (OTA):** Dispositivos que não possuam suporte nativo a atualizações remota de firmware (*Over-The-Air*) para a substituição de algoritmos vulneráveis perdem a certificação de conformidade e são proibidos de ser comercializados ou importados nesses territórios.
- **Vedação a Protocolos Legados:** Dispositivos com ciclo de vida longo mantidos sob algoritmos de criptografia assimétrica clássica (como RSA e ECC) sem um plano formal de agilidade criptográfica (*crypto-agility*) passam a ser classificados como ativos de alto risco regulatório.

Para a indústria transformadora brasileira, exportadores de tecnologia e startups do ecossistema de IoT/AIoT, a adequação a esses padrões e a preparação para a Criptografia Pós-Quântica (PQC) deixaram de ser meros diferenciais competitivos. Trata-se de uma **condição de acesso a mercados internacionais** e de proteção contra a responsabilização civil objetiva em casos de vazamento ou comprometimento de dados sensíveis na ponta.

2.5. A Resposta Regulatória: Os Padrões PQC do NIST e a Mandatariedade da Executive Order 14412

Frente ao avanço da ameaça quântica e à aceleração do risco HNDL, a Criptografia Pós-Quântica (PQC) deixou de ser uma recomendação voluntária e passou à condição de política de Estado vinculante.

Em agosto de 2024, o NIST (*National Institute of Standards and Technology*) oficializou os padrões FIPS 203 (ML-KEM, para estabelecimento de chaves), FIPS 204 (ML-DSA, para assinaturas digitais) e FIPS 205 (SLH-DSA, para assinaturas baseadas em hash).

Contudo, o marco decisivo de execução ocorreu em **22 de junho de 2026**, com a assinatura da **Executive Order 14412** ("*Securing the Nation Against Advanced Cryptographic Attacks*"). A ordem presidencial estabeleceu o primeiro cronograma mandatório com responsabilização legal e administrativa direta:

- **Nomeação de Liderança (PQC Migration Lead):** Obrigação de designação de um gestor executivo para responder pelo inventário criptográfico e plano de migração.
- **Marco de Estabelecimento de Chaves (31/12/2030):** Todos os sistemas federais e de infraestrutura crítica devem substituir mecanismos obsoletos (RSA/ECC) pelo padrão FIPS 203 para proteção de tráfego e chaves.
- **Marco de Assinaturas Digitais (31/12/2031):** Transição completa das infraestruturas de autenticação, certificados digitais e não repúdio para os padrões FIPS 204 e 205.

Reflexos Diretos e Extraterritoriais no Mercado Brasileiro

A Executive Order 14412 atinge diretamente o ecossistema corporativo brasileiro por meio do seu impacto nas compras públicas e nas cadeias globais de suprimento de TI:

1. **Inclusão do CBOM (*Cryptographic Bill of Materials*):** A norma exige que fornecedores identifiquem de forma automatizada toda a criptografia embarcada em softwares e dispositivos hardware. Empresas de IoT/AIoT no Brasil que não mapearem seus componentes perderão contratos de fornecimento.
2. **Adequação da Nuvem e do Sector Financeiro:** Instituições financeiras brasileiras que realizam transações transfronteiriças ou dependem de infraestruturas de nuvem norte-americanas são forçadas a antecipar seus cronogramas para não serem desconectadas dos nós de liquidação internacional.

Observação Importante: A Antecipação das Big Techs e o Protocolo TLS 1.3

As principais empresas de infraestrutura de comunicação e serviços de nuvem norte-americanas, como Google, Microsoft, Amazon Web Services (AWS) e Cloudflare, já implementaram o suporte padrão aos protocolos SSL 3.0 / TLS 1.3 com mecanismos de agilidade criptográfica em suas arquiteturas globais.

A adoção do TLS 1.3 é um marco estratégico fundamental para a era pós-quântica por dois motivos centrais:

Suporte Nativo a Algoritmos Híbridos: O protocolo TLS 1.3 foi projetado com flexibilidade para realizar a negociação de chaves (handshake) combinando algoritmos clássicos tradicionais (como ECDHE) com os novos padrões de Criptografia Pós-Quântica (PQC, como o ML-KEM/FIPS 203) em uma única operação. **Obs.:** enquanto suportar ECDHE não será totalmente resistente a QC.

Mitigação Antecipada do Risco HNDL: Ao adotar esquemas híbridos PQC na camada de transporte (TLS), os grandes provedores de nuvem garantem que o tráfego de dados entre servidores já trafegue protegido contra a captura passiva (Harvest Now, Decrypt Later) nos nós centrais da internet global.

Reflexo para as Empresas Brasileiras: Embora a infraestrutura básica fornecida por essas gigantes da tecnologia já esteja preparada na camada de nuvem, o gargalo operacional desloca-se para a ponta das aplicações locais e dispositivos de IoT/AIoT. Se os sistemas legados ou os microcontroladores das empresas

brasileiras não forem atualizados para suportar o TLS 1.3 e as novas bibliotecas de chaves expandidas, eles não conseguirão se comunicar com esses servidores globais à medida que as chaves legadas ECDHE forem descontinuadas em cumprimento à Executive Order 14412.

2.6. Governança, LGPD e Responsabilidade Civil para Lideranças e Juristas

A transição para a era pós-quântica introduz deveres diretos de governança corporativa e conformidade legal, alterando o padrão de diligência exigido de diretores, conselheiros e gestores de tecnologia.

Dever de Diligência (*Duty of Care*) e Governança

Sob a ótica do Direito Corporativo e das boas práticas de governança, o desconhecimento da ameaça quântica deixa de ser uma justificativa aceitável. Executivos e membros do conselho de administração podem ser responsabilizados por omissão caso não estabeleçam um plano de mapeamento e migração criptográfica para ativos críticos, especialmente considerando a existência formal dos padrões FIPS do NIST e os alertas de agências de cibersegurança.

LGPD e Proteção de Dados Pessoais

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 - LGPD) estabelece no artigo 6º, inciso VII, o princípio da segurança, exigindo a utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados. No artigo 46, a lei impõe aos controladores e operadores a obrigação de adotar medidas de segurança desde a concepção do produto ou serviço (*security by design*).

À luz do fenômeno HNDL, a manutenção de dados sensíveis de longo prazo sob algoritmos criptográficos sabidamente vulneráveis (como RSA sem planejamento de transição) pode ser caracterizada pela Autoridade Nacional de Proteção de Dados (ANPD) ou pelo Poder Judiciário como uma falha no dever de segurança, sujeitando as organizações a sanções administrativas e reparações civis por danos causados aos titulares.

Adequação Contratual na Cadeia de Suprimentos de TI

Juristas e departamentos jurídicos corporativos devem revisar imediatamente os contratos de fornecimento de software, serviços de nuvem e dispositivos conectados:

- **Inclusão de Cláusulas de Agilidade Criptográfica:** Exigência contratual para que fornecedores de software e hardware garantam suporte aos padrões PQC do NIST ao longo da vigência dos contratos.
- **Matriz de Responsabilidade sobre Atualizações:** Definição clara de qual parte responderá pelos custos e pela execução do plano de substituição de certificados digitais e bibliotecas criptográficas obsoletas.
- **Auditoria de Cibersegurança em Terceiros:** Mecanismos de verificação para garantir que parceiros da cadeia de suprimentos (*supply chain*) estejam alinhados com o inventário criptográfico e com as diretrizes de migração pós-quântica.

A segurança da informação na era pós-quântica deixa de ser uma questão estritamente técnica para se consolidar como pauta central do direito digital, da conformidade regulatória e da continuidade dos negócios.

Referências Capítulo 2

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Lei Geral de Proteção de Dados Pessoais - LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: <http://www.planalto.gov.br>. Acesso em: 24 ago. 2026.

ENDRES, Manuel et al. **A Neutral-Atom Quantum Processor with 6,100 Qubits and High-Rate Error Correction**. Physical Review X, College Park, v. 14, n. 3, p. 031020, jul. 2024.

MOSCA, Michele; PIANI, Marco. 2022 Quantum Threat Timeline Report. Toronto: Global Risk Institute, 2022. Disponível em: <https://globalriskinstitute.org/publication/2022-quantum-threat-timeline-report/>. Acesso em: 24 ago. 2026.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). **FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard**. Gaithersburg: U.S. Department of Commerce, 2024. Disponível em: <https://csrc.nist.gov>. Acesso em: 24 ago. 2026.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). **FIPS 204: Module-Lattice-Based Digital Signature Standard**. Gaithersburg: U.S. Department of Commerce, 2024. Disponível em: <https://csrc.nist.gov>. Acesso em: 24 ago. 2026.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). **FIPS 205: Stateless Hash-Based Digital Signature Standard**. Gaithersburg: U.S. Department of Commerce, 2024. Disponível em: <https://csrc.nist.gov>. Acesso em: 24 ago. 2026.

SHOR, Peter W. **Algorithms for Quantum Computation: Discrete Logarithms and Factoring**. In: PROCEEDINGS OF THE 35TH ANNUAL SYMPOSIUM ON FOUNDATIONS OF COMPUTER SCIENCE. Santa Fe: IEEE Computer Society Press, 1994. p. 124-134.

UNITED STATES. Executive Office of the President. **National Security Memorandum 10 (NSM-10): Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems**. Washington, D.C.: The White House, 2022. Disponível em: <https://www.whitehouse.gov>. Acesso em: 24 ago. 2026.

WEF - WORLD ECONOMIC FORUM. **Transitioning to Post-Quantum Cryptography: A Strategic Roadmap for Leaders**. Geneva: World Economic Forum in collaboration with Deloitte, 2024. Disponível em: <https://www.weforum.org>. Acesso em: 24 ago. 2026.

TRUMP, Donald J. **Executive Order 14412: Securing the Nation Against Advanced Cryptographic Attacks**. Washington, D.C.: The White House, 22 jun. 2026. Disponível em: <https://www.whitehouse.gov/presidential-actions/2026/06/securing-the-nation-against-advanced-cryptographic-attacks/>. Acesso em: 24 ago. 2026.

Bancos brasileiros e a Post-Quantum Cryptography: a hora de se preparar é agora – disponível em: <https://www.ecommercebrasil.com.br/artigos/bancos-brasileiros-e-a-post-quantum-cryptography-a-hora-de-se-preparar-e-agora> . Acesso em: 27 ago. 2026.

Capítulo 3: A Tese Central: A Arquitetura Híbrida e as Aplicações Práticas do Presente

Um dos equívocos mais persistentes no ecossistema corporativo é a premissa de que a computação quântica surgirá para substituir integralmente a infraestrutura de computação clássica. Essa visão de substituição irrestrita distorce o planejamento tecnológico e induz lideranças a esperarem por um salto definitivo de obsolescência que não ocorrerá nos moldes imaginados.

A realidade da computação de alto desempenho (*High-Performance Computing* - HPC) aponta para um paradigma de coexistência e integração. A computação quântica atua, fundamentalmente, como uma arquitetura de aceleração especializada. Este capítulo detalha a mecânica dessa integração híbrida e mapeia os casos práticos de geração de valor econômico nos setores financeiro, de IoT e de AIoT.



3.1. A Desmistificação da Substituição: O Conceito de QPU e Aceleração Especializada

Para entender por que o computador quântico não tornará a CPU, acrônimo em inglês para *Central Processing Unit* (Unidade Central de Processamento), ou a GPU, sigla para *Graphics Processing Unit* (Unidade de Processamento Gráfico), obsoletas, é necessário examinar como cada arquitetura lida com a informação.

CPU's clássicas foram projetadas para executar sequências de instruções lógicas e cálculos aritméticos com extrema velocidade e precisão determinística. GPUs foram otimizadas para processamento em paralelo de volumes massivos de dados homogêneos, sendo o pilar atual dos modelos de inteligência artificial generativa e visão computacional.

As QPUs, sigla para *Quantum Processing Units* (Unidades de Processamento Quântico), por sua vez, não são adequadas para tarefas computacionais cotidianas, como processamento de texto, gestão de bancos de dados relacionais ou execução de sistemas operacionais. A utilidade fundamental de uma QPU reside na capacidade de manipular espaços de estados matemáticos exponencialmente grandes por meio dos princípios de superposição e emaranhamento.

Portanto, a QPU atua exatamente como um coprocessador especializado, assim como a GPU foi adicionada às arquiteturas de servidores para acelerar cálculos de matrizes de inteligência artificial. O

computador do futuro próximo é uma arquitetura heterogênea composta pela combinação integrada de CPUs, GPUs e QPUs.

Componente de Hardware	Função Principal na Arquitetura	Vantagem Competitiva Central	Limitação Operacional
CPU (Unidade Central)	Controle de fluxo, lógica de negócios e orquestração do sistema.	Baixa latência e alta velocidade em tarefas sequenciais.	Capacidade limitada em problemas de crescimento exponencial.
GPU (Unidade Gráfica)	Processamento matricial paralelo massivo para inteligência artificial.	Alto rendimento em multiplicação de matrizes em lote.	Ineficiência em problemas de otimização combinatória extrema.
QPU (Unidade Quântica)	Amostragem de espaços de estados complexos e otimização avançada.	Resolução de problemas exponenciais em tempo reduzido.	Exige orquestração clássica e tratamento rigoroso de ruído.

A Terceira Via do Hardware: A Revolução dos Átomos Neutros do Caltech

Além das abordagens de qubits supercondutores (que exigem congelamento criogênico extremo) e de íons aprisionados, a tecnologia de **átomos neutros** consolidou-se como uma das vias mais promissoras e escaláveis para o hardware quântico de alta fidelidade.

O avanço histórico obtido pelo laboratório do professor Manuel Endres no Caltech (*California Institute of Technology*) alterou o paradigma de escalabilidade do setor ao demonstrar uma matriz funcional de **6.100 qubits de átomos neutros de céσιο**, manipulados dinamicamente por pinças ópticas a laser em temperatura de câmara de vácuo.

Essa arquitetura introduz três vantagens operacionais decisivas para o modelo híbrido:

- 1. **Topologia Dinâmica e Conectividade Reconfigurável:** Enquanto os qubits supercondutores estão gravados rigidamente no silício de um chip, os átomos neutros podem ser fisicamente movimentados por lasers durante a execução do algoritmo. Isso permite conectar diretamente qubits distantes sem a necessidade de uma malha complexa de fiação física.
- 2. **Atuação em Temperatura Ambiente Relativa:** O controle dos qubits por laser reduz a dependência de criostatos de diluição massivos, viabilizando o desenvolvimento de unidades de processamento mais compactas e eficientes do ponto de vista energético.
- 3. **Drástica Redução do Custo de Correção de Erros:** A combinação de alta densidade atômica com códigos de correção de erro de alta taxa (*high-rate codes*) permite construir processadores quânticos tolerantes a falhas (*Fault-Tolerant Quantum Computing*) utilizando ordens de grandeza menos qubits físicos do que as abordagens anteriores.

Essa inovação do Caltech reforça a tese de que o mercado não será dominado por uma única tecnologia de hardware. O futuro ecossistema de TI integrará **CPUs, GPUs e QPUs baseadas em diferentes física de suporte**, selecionadas de acordo com a natureza específica do problema de otimização, simulação ou aprendizado de máquina demandado pela corporação.

Tabela de Comparação de Hardware:

Componente / Arquitetura	Vantagem Competitiva Central	Limitação / Gargalo Atual	Papel na Arquitetura Híbrida
CPU (Processador Clássico)	Baixa latência e alta velocidade em tarefas sequenciais.	Ineficiência em problemas de crescimento exponencial.	Controle de fluxo, interface e lógica de negócios.
GPU (Processador Gráfico)	Alto rendimento em processamento paralelo e matrizes de IA.	Alto consumo energético em otimização combinatória densa.	Treinamento de modelos massivos e pré-processamento.
QPU Supercondutora (Ex: IBM)	Veloz na execução de portas quânticas.	Dependência de criogenia a temperaturas de - 273°C.	Co-processamento intensivo em nuvens centrais (QaaS).
QPU de Átomos Neutros (Ex: Caltech)	Alta densidade de qubits (6.100+) e conectividade dinâmica via laser.	Exige controle óptico e estabilização de laser de alta precisão.	Aceleração em supercomputação (HPC) e correção de erros.

Nota: a tabela acima descreve exclusivamente as arquiteturas de processamento (CPU, GPU e duas variantes de QPU). Ela não inclui os sensores quânticos (magnetômetros, gravímetros e relógios atômicos de escala de chip), apresentados no Capítulo 4, item 4.5.1, que constituem uma categoria de hardware quântico distinta, voltada à medição de grandezas físicas de precisão, e não ao processamento ou à otimização de dados.

3.2. A Mecânica do Processamento Híbrido: Algoritmos Variacionais e Orquestração

A integração prática entre computadores clássicos e quânticos no estado atual da tecnologia (caracterizado pela era NISQ, sigla em inglês para *Noisy Intermediate-Scale Quantum*, que descreve processadores quânticos de escala intermediária ainda sujeitos ao ruído ambiental) ocorre por meio de algoritmos híbridos variacionais.

Nesses algoritmos, a tarefa computacional é dividida em um ciclo contínuo de cooperação entre o processador clássico e o processador quântico:

- Decomposição e Preparação (Clássica):** A CPU ou GPU recebe o problema corporativo (como uma equação química ou um portfólio de ativos) e o traduz em uma matriz matemática conhecida como **Hamiltoniano** do sistema.
- Execução de Estado (Quântica):** A QPU prepara os bits quânticos em um estado específico, executa um circuito quântico parametrizado e realiza medições de amostragem.
- Ajuste e Otimização (Clássica):** O resultado da medição é enviado de volta à CPU, que utiliza algoritmos de otimização clássicos para ajustar os parâmetros e enviar um novo conjunto de instruções para a QPU.

4. **Convergência:** Esse ciclo iterativo se repete até que o sistema encontre a solução de menor energia ou de máxima eficiência para o problema.

Dois algoritmos se destacam nesse modelo híbrido: o VQE, acrônimo em inglês para *Variational Quantum Eigensolver* (Eigensolver Quântico Variacional), amplamente aplicado na simulação de estruturas moleculares para a indústria farmacêutica e química; e o QAOA, sigla para *Quantum Approximate Optimization Algorithm* (Algoritmo de Otimização Quântica Aproximada), voltado para a resolução de problemas combinatórios complexos em logística e finanças.

3.3. Casos de Uso no Setor Financeiro: Eficiência de Capital e Gestão de Risco

O setor financeiro é o segmento corporativo que mais investe em aplicações quânticas devido ao impacto direto que pequenas melhorias percentuais em algoritmos de precisão geram na rentabilidade e no gerenciamento de risco.

Otimização Combinatória de Portfólios

A seleção ideal de ativos em um portfólio financeiro envolve balancear retorno esperado, volatilidade, liquidez, restrições regulatórias e correlações entre centenas de instrumentos. À medida que o número de ativos cresce, o número de combinações possíveis cresce de forma exponencial, tornando a análise exaustiva impossível para computadores clássicos.

A utilização do algoritmo QAOA em ambientes híbridos permite mapear o espaço de combinações com eficiência superior, encontrando configurações de portfólio que maximizam o retorno ajustado ao risco em frações do tempo exigido por métodos tradicionais.

Aceleração da Simulação de Monte Carlo

As Simulações de Monte Carlo são o padrão da indústria financeira para precificação de derivativos complexos e cálculo do VaR, sigla em inglês para *Value at Risk* (Valor em Risco, métrica que estima a perda máxima potencial de uma carteira em determinado período). No entanto, atingir altos níveis de precisão estatística exige a execução de milhões de cenários simulados, demandando poder de processamento massivo.

Por meio do algoritmo de Estimativa de Amplitude Quântica (QAE, acrônimo para *Quantum Amplitude Estimation*), a QPU é capaz de oferecer um ganho de velocidade quadrático na convergência das simulações. Isso significa que um cálculo de risco que exigiria um milhão de simulações clássicas pode ser realizado com equivalente precisão teórica na ordem de mil operações quânticas, permitindo análises de risco intradiárias em tempo quase real.

Deteção de Fraudes e Modelagem de Crédito

A combinação do aprendizado de máquina com algoritmos quânticos dá origem ao QML, acrônimo para *Quantum Machine Learning* (Aprendizado de Máquina Quântico). Modelos de classificação baseados em *Quantum Support Vector Machines* (Máquinas de Vetores de Suporte Quânticas) conseguem identificar padrões ocultos de correlação em bases de dados multidimensionais extremamente densas, aumentando a taxa de detecção de transações fraudulentas e reduzindo falsos positivos em redes de pagamento.

3.4. Casos de Uso em IoT e AIoT: Otimização na Ponta e Redes Inteligentes

No ecossistema de dispositivos conectados, o volume de dados gerado pela convergência entre IoT e inteligência artificial exige capacidades de otimização que superam a capacidade de processamento de servidores tradicionais.

Otimização da Carga e Roteamento em Smart Grids

As redes elétricas inteligentes, conhecidas como *Smart Grids*, integram milhares de fontes geradoras distribuídas (como painéis solares residenciais e parques eólicos) a pontos de consumo dinâmicos e frotas de veículos elétricos em recarga.

O balanceamento em tempo real da oferta e da demanda de energia ao longo de uma infraestrutura continental é um problema de otimização combinatória de altíssima complexidade. QPUs operando via nuvem ou integradas a centros regionais de controle conseguem recalcular o fluxo de energia da rede em tempo real, mitigando picos de sobrecarga, reduzindo perdas de transmissão e prevenindo apagões sistêmicos.

Gestão de Tráfego e Logística de Frotas Conectadas em AIoT

Em ecossistemas de AIoT voltados à mobilidade urbana e logística de transporte, milhares de veículos autônomos e sensores de tráfego geram dados contínuos de localização e velocidade.

A determinação da rota global otimizada para uma frota inteira (evitando o gargalo em que todos os veículos são redirecionados para a mesma via alternativa) não pode ser resolvida eficientemente calculando rotas individuais isoladas. Algoritmos quânticos de otimização conseguem processar o estado de todos os veículos de forma simultânea, redistribuindo o tráfego de maneira global e reduzindo tempos de deslocamento e emissões de carbono.

Processamento de Sinais e Aprendizado de Máquina em Edge Computing

Com o avanço de arquiteturas em temperatura ambiente (como os chips em diamante sintético), surge a perspectiva de acoplamento de aceleradores quânticos compactos em estações rádio-base de redes 5G e 6G.

Essa infraestrutura permite que o processamento de modelos de IA de alta complexidade ocorra na ponta da rede (*Edge Computing*), reduzindo a latência de comunicação e permitindo que sensores industriais identifiquem falhas mecânicas por análise vibracional complexa antes que acidentes graves ocorram na linha de produção.

A adoção da computação quântica, portanto, não é um evento futuro de substituição total de hardware, mas um processo gradual de integração de coprocessadores quânticos para resolver os gargalos computacionais que a infraestrutura clássica já não consegue superar isoladamente.

Referências Capítulo 3

EGERER, Julian et al. **Quantum Computing for Power Flow Optimization in Smart Grids**. IEEE Transactions on Power Systems, New York, v. 38, n. 4, p. 3412-3423, jul. 2023.

EPRINCE, Herman et al. **Quantum Machine Learning in Financial Fraud Detection: A Performance Benchmark**. Journal of Financial Crime, London, v. 31, n. 2, p. 410-428, mar. 2024.

HERMAN, Charles et al. **A Survey of Quantum Computing for Finance**. ACM Computing Surveys, New York, v. 55, n. 11, p. 1-37, nov. 2023.

IBM QUANTUM. **Variational Quantum Eigensolver (VQE) and Quantum Approximate Optimization Algorithm (QAOA) in Practice**. Armonk: IBM Corporation, 2024. Disponível em: <https://docs.quantum.ibm.com>. Acesso em: 24 ago. 2026.

PRESST, John. **Quantum Computing in the NISQ Era and Beyond**. Quantum, Vienna, v. 2, p. 79-101, jan. 2018.

WOERNER, Stefan; EGERER, Daniel. **Quantum Risk Analysis**. NPJ Quantum Information, London, v. 5, n. 1, p. 1-8, jun. 2019.

ENDRES, Manuel et al. **A Neutral-Atom Quantum Processor with 6,100 Qubits and High-Rate Error Correction**. Physical Review X, College Park, v. 14, n. 3, p. 031020, jul. 2024.

EVERED, Simon J. et al. **High-Fidelity Parallel Entangling Gates on a Neutral-Atom Quantum Computer**. Nature, London, v. 622, n. 7982, p. 273-279, oct. 2023.

Itaú reforça time de computação quântica para combate às fraudes – Disponível em: <https://convergenciadigital.com.br/inovacao/itau-reforca-time-de-computacao-quantica-para-combate-as-fraudes/> . Acesso em 31 de ago. 2026.

Capítulo 4: O Ecossistema Brasileiro: O Papel do Sistema S, P&D e a Capacitação da Indústria Nacional

A consolidação da computação quântica como um ativo estratégico global exige que economias emergentes ultrapassem a condição de meras consumidoras passivas de tecnologia. No Brasil, o avanço em direção à era quântica ocorre de forma estruturada, combinando a tradição acadêmica em física de altas energias e óptica com a atuação pragmática de centros de inovação aplicada, ecossistemas estaduais e o apoio fundamental do Sistema S.

Para empresários, gestores de tecnologia e juristas, compreender o mapa da inovação quântica nacional é indispensável. É nesse ambiente local que surgem as oportunidades de captação de recursos de P&D (Pesquisa e Desenvolvimento), parcerias público-privadas e a formação de mão de obra qualificada para sustentar a transição para arquiteturas híbridas.

4.1. O Panorama da Computação Quântica no Brasil

Historicamente, o Brasil construiu uma sólida reputação científica em mecânica quântica, informação quântica e óptica quântica por meio de seus institutos de pesquisa e universidades públicas. Contudo, o grande gargalo da tecnologia no país sempre foi a transferência desse conhecimento teórico para a cadeia de valor industrial e comercial.

Nos últimos anos, o cenário nacional passou por uma mudança institucional impulsionada pela criação de redes nacionais de pesquisa e programas de fomento específicos. O Ministério da Ciência, Tecnologia e Inovação (MCTI), em conjunto com a Sociedade para Promoção da Excelência do Software Brasileiro (Softex), lançou iniciativas de articulação nacional para estruturar o ecossistema de tecnologias quânticas.

Nesse contexto, o LNCC (Laboratório Nacional de Computação Científica), vinculado ao MCTI e sediado em Petrópolis (RJ), destaca-se como o nó central da infraestrutura computacional do país. Abrigando o supercomputador Santos Dumont, o LNCC conduz pesquisas avançadas em inteligência artificial e computação de alto desempenho (HPC), atuando como um catalisador para a integração de emuladores quânticos e plataformas de teste para a comunidade científica e empresarial.

Instituição / Organização	Foco Principal de Atuação	Impacto Prático no Mercado Nacional
MCTI / Softex	Fomento e coordenação da Rede Nacional de Tecnologias Quânticas.	Articulação de políticas públicas e atração de recursos para infraestrutura.
LNCC (MCTI)	Infraestrutura de HPC e simulação de algoritmos quânticos.	Integração de supercomputação clássica com emuladores de algoritmos quânticos.
SENAI CIMATEC	Pesquisa aplicada, segurança quântica e prototipagem industrial.	Centro de inovação voltado à resolução de gargalos operacionais da indústria.

Instituição / Organização	Foco Principal de Atuação	Impacto Prático no Mercado Nacional
CIQuanta (Paraíba)	P&D em fotônica, cooperação internacional e formação de talentos.	Atração de parcerias globais e consolidação do hub quântico do Nordeste.
SENAI-SP	Formação profissional, pós-graduação e hardware QC educacional.	Capacitação de engenheiros e técnicos com uso de computadores quânticos de bancada.

4.2. O Papel Estratégico do Sistema S: Do SENAI CIMATEC às Escalas Locais

O Sistema S, com destaque para o Serviço Nacional de Aprendizagem Industrial (SENAI), assumiu o papel de ponte entre o conhecimento acadêmico avançado e as demandas de eficiência da indústria brasileira. Por meio de seus Institutos de Inovação, o SENAI lidera a introdução de infraestruturas quânticas operacionais no país.

SENAI CIMATEC: O Primeiro Centro Quântico Industrial

Localizado em Salvador (BA), o SENAI CIMATEC consolidou-se como a principal referência nacional na aplicação da computação quântica para a indústria de manufatura, energia, logística e defesa. O centro abriga a iniciativa *Quantum Industrial Innovation* (QIIN), estruturada especificamente para atuar no desenvolvimento de algoritmos de otimização, cibersegurança e simulação de materiais.

O SENAI CIMATEC atua em cooperação direta com grandes corporações estatais e privadas, como a Petrobras, investigando o uso de processamento quântico para a otimização da logística de exploração de petróleo, simulação de reservatórios e otimização da cadeia de suprimentos de combustíveis.

SENAI-SP: Adoção de Hardware Didático e Formação Técnica

Enquanto o SENAI CIMATEC foca em projetos de alta complexidade industrial e segurança quântica, o SENAI-SP atua na base da formação de talentos. A instituição protagonizou a chegada do primeiro computador quântico educacional ao país, baseado em tecnologia de Ressonância Magnética Nuclear (RMN) operando em temperatura ambiente (desenvolvido pela SpinQ).

A instalação desse tipo de equipamento em salas de aula e a criação de programas de pós-graduação específicos em computação quântica pelo SENAI-SP introduzem uma mudança metodológica relevante: os estudantes aprendem a manipular qubits reais, parametrizar circuitos quânticos e integrar bibliotecas de código em linguagens de uso industrial (como Python e Qiskit) diretamente no ambiente acadêmico.

Essa abordagem descentralizada garante que o mercado de trabalho brasileiro comece a formar engenheiros de software e cientistas de dados com letramento quântico nativo, suprimindo a carência de profissionais capacitados que afeta o setor globalmente.

4.3. Oportunidades de Fomento, Incentivos Fiscais e Parcerias Público-Privadas

A estruturação de projetos em tecnologias emergentes no Brasil conta com mecanismos de incentivo fiscal e financiamento reembolsável e não reembolsável que reduzem os custos e os riscos para as empresas privadas.

Lei do Bem e Créditos de P&D

A Lei nº 11.196/2005 (conhecida como Lei do Bem) permite que empresas operando sob o regime de Lucro Real deduzam da base de cálculo do Imposto de Renda Pessoa Jurídica (IRPJ) e da Contribuição Social sobre o Lucro Líquido (CSLL) os gastos efetuados em atividades de pesquisa tecnológica e desenvolvimento de inovação. A contratação de horas de uso de serviços quânticos via nuvem (QaaS) ou a contratação de consultorias especializadas para adequação à Criptografia Pós-Quântica (PQC) enquadram-se perfeitamente nos incentivos previstos na legislação.

Embrapii (Empresa Brasileira de Pesquisa e Inovação Industrial)

A Embrapii atua financiando projetos de inovação industrial em parceria com instituições qualificadas (como as Unidades Embrapii presentes no SENAI CIMATEC e em universidades públicas). No modelo de tripartição de custos da Embrapii:

- A **Embrapii** aporta recursos não reembolsáveis que cobrem até um terço do valor total do projeto.
- A **Unidade Embrapii (Executora)** entra com a infraestrutura técnica e recursos próprios (cobrindo cerca de um terço do valor).
- A **Empresa Parceira** financia o restante do projeto, obtendo acesso a uma solução customizada com custo de desenvolvimento significativamente reduzido.

Distribuição de Custos em Projetos de Inovação Quântica via Embrapii:

- [Recursos Não Reembolsáveis Embrapii] ---> Até 33% do custo total
- [Infraestrutura do Centro / SENAI] ---> Cerca de 33% do custo total
- [Aporte da Empresa Privada] ---> Aproximadamente 34% do custo total

O Hub do Nordeste: O Centro Internacional de Computação Quântica da Paraíba (CIQuanta)

A consolidação da estratégia quântica brasileira ganhou um vetor crucial de descentralização e liderança regional com a criação do **CIQuanta (Centro Internacional de Computação Quântica da Paraíba)**. Sediado em João Pessoa, o centro nasceu com a missão de posicionar o Estado da Paraíba e a Região Nordeste como um polo internacional de desenvolvimento em tecnologias quânticas.

Fruto da articulação entre o Governo do Estado da Paraíba, a Universidade Federal da Paraíba (UFPB), a Universidade Federal de Campina Grande (UFCG) e redes de cooperação internacional, o CIQuanta atua com foco em três pilares fundamentais:

- **Pesquisa Avançada de Hardware e Algoritmos:** Desenvolvimento de pesquisas voltadas a fotônica quântica, informação quântica e simulação de materiais.
- **Atração de Investimentos Globais:** Articulação com ecossistemas de inovação da Europa e América do Norte para atração de fundos e transferência tecnológica.
- **Formação de Mão de Obra de Alta Performance:** Criação de um corredor de talentos no Nordeste focado em capacitar cientistas e engenheiros para a indústria de software quântico e cibersegurança.

A presença do CIQuanta demonstra que o mapa quântico nacional não se restringe ao eixo Sudeste, construindo uma rede complementar em que o LNCC (RJ) provê infraestrutura de supercomputação, o SENAI CIMATEC (BA) foca na aplicação industrial pesada, o SENAI-SP lidera a capacitação técnica de base e o CIQuanta (PB) projeta o país em redes internacionais de P&D.

A Cooperação Sino-Brasileira e a Geopolítica da Infraestrutura Quântica

A trajetória do CIQuanta atingiu um marco histórico e estratégico ao viabilizar a aquisição dos dois primeiros computadores quânticos operacionais da América Latina (sistemas de 20 e 100 qubits). Fruto de uma parceria de cerca de R\$ 150 milhões entre o Ministério da Ciência, Tecnologia e Inovação (MCTI), o Governo da Paraíba e a estatal chinesa CETC (*China Electronics Technology Group Corporation*), a iniciativa prevê não apenas a instalação dos equipamentos em João Pessoa, mas também um plano de transferência tecnológica e treinamento de pesquisadores brasileiros em centros chineses.

A escolha do ecossistema chinês como fornecedor tecnológico principal introduziu o Brasil diretamente no centro do atrito geopolítico entre Washington e Pequim:

- **Inquietações Washington-Brasília:** A diplomacia norte-americana enxerga o avanço da infraestrutura tecnológica chinesa na América Latina com forte reserva. Como a CETC e suas subsidiárias estão sujeitas a sanções e controles de exportação por parte do Departamento de Comércio dos Estados Unidos devido a implicações em defesa e vigilância, a presença de seu hardware quântico em solo brasileiro gera questionamentos sobre a segurança de redes de comunicação e a futura interoperabilidade do ecossistema de TI nacional com parceiros ocidentais.
- **Neutralidade Pragmática e Soberania Digital:** Em resposta aos questionamentos diplomáticos, o governo brasileiro e a coordenação científica sustentam a postura de não alinhamento automático. A justificativa institucional baseia-se no caráter estritamente científico e educacional do CIQuanta, ressaltando que o Brasil busca soberania digital ao diversificar parceiros estratégicos e absorver conhecimento onde a tecnologia está mais acessível.
- **Desafios de Compliance e Governança:** Para juristas, instituições financeiras e empresas com capital aberto no Ocidente, a utilização de uma infraestrutura quântica baseada em componentes chineses exigirá matrizes claras de governança e segregação de dados, garantindo que o processamento em nuvem local atenda simultaneamente aos parâmetros da LGPD e aos requisitos de cibersegurança e compliance internacionais.

4.4. O Cenário de Negócios: Startups e o Ecossistema de Inovação Aberta

Além das grandes corporações e dos centros do Sistema S, o Brasil assiste ao surgimento das primeiras startups especializadas na cadeia de valor quântica, focando principalmente no desenvolvimento de software algorítmico, integração de sistemas e consultoria para transição criptográfica.

A dinâmica da inovação aberta (*Open Innovation*) tem permitido que bancos tradicionais, seguradoras, indústrias químicas e empresas de logística lancem desafios tecnológicos para conectar-se com essas startups. Esses projetos de demonstração de conceito (PoC, sigla para *Proof of Concept*) servem para validar a aplicação de algoritmos híbridos sem que a corporação precise estruturar uma equipe interna completa de física quântica.

O Brasil encontra-se em uma posição estratégica favorável: possui uma infraestrutura de computação científica estabelecida, um centro de inovação industrial ativo no Sistema S com capacidade de prototipagem e instrumentos regulatórios e fiscais capazes de atrair o investimento privado. A decisão para executivos locais não é se a tecnologia deve ser adotada, mas como estruturar a transição tecnológica utilizando as ferramentas de fomento e capacitação já disponíveis no território nacional.

4.5. A Década da Indústria 5.0: Da Origem com Michael Rada e Sociedade 5.0 à Resiliência Quântica

Para compreender o papel da computação quântica na manufatura avançada em 2026, é indispensável resgatar a evolução conceitual da Indústria 5.0, detalhada com suas fontes primárias no Anexo 7 desta obra. Embora

o termo tenha sido cunhado originalmente em dezembro de 2015 pelo consultor industrial Michael Rada, que propôs o resgate do valor humano e a eliminação do desperdício no chão de fábrica, o conceito ganhou escala global ao se entrelaçar com a iniciativa de Sociedade 5.0 (Super Smart Society), lançada pelo governo do Japão em 2016, e com outras formulações independentes surgidas ao longo da década seguinte.

O divisor de águas que transformou esses conceitos dispersos em política industrial estruturada ocorreu em janeiro de 2021, quando a Comissão Europeia publicou o relatório fundador que consolidaria, um ano depois, o policy brief definitivo de 2022. Ao completar uma década de maturação da sua concepção, a Indústria 5.0 consolida a transição da mera automação e conectividade digital (pilares da Indústria 4.0) para um modelo pautado em três eixos inegociáveis: centralidade humana (human-centric), sustentabilidade ambiental (ESG) e, essencialmente, resiliência sistêmica.

A Convergência entre a Indústria 5.0 e a Computação Quântica

No contexto brasileiro e global, a resiliência pregada pela Indústria 5.0 é frontalmente incompatível com ecossistemas industriais que operam sob a vulnerabilidade de algoritmos criptográficos obsoletos (RSA/ECC). A aplicação prática da computação quântica atua como a infraestrutura de suporte para os três pilares da Indústria 5.0:

1. **Resiliência Operacional e Cibersegurança na Ponta:** A colaboração direta entre operadores humanos e robôs colaborativos (*cobots*) ou gêmeos digitais (*digital twins*) em redes de AIoT exige comunicação em tempo real com criptografia pós-quântica (PQC), impedindo paralisações físicas por ataques de ransomware ou interceptação passiva (*Harvest Now, Decrypt Later - HNDL*).
2. **Sustentabilidade e Descarbonização:** A aceleração quântica via algoritmos variacionais (VQE) permite simular novas reações químicas e materiais ecológicos em escala molecular, otimizando catalisadores industriais e reduzindo a pegada de carbono do setor manufatureiro.
3. **Centralidade Humana na Tomada de Decisão:** Modelos de aprendizado de máquina quântico (QML) e otimização combinatória (QAOA) filtram o ruído de bilhões de dados de sensores IoT, entregando aos gestores industriais cenários preditivos ultraprecisos para prevenção de acidentes e gestão da cadeia de suprimentos em tempo real.

4.5.1. A Quarta Dimensão: Sensoriamento Quântico e Manutenção Preditiva na Indústria 5.0

Os três pilares descritos anteriormente concentram-se na capacidade de processamento das QPUs. Existe, contudo, uma quarta frente da tecnologia quântica com maturidade comercial igual ou superior à computação quântica e aplicação direta e imediata na Indústria 5.0/IoT: o sensoriamento quântico (quantum sensing).

Diferente das QPUs, que manipulam qubits para resolver problemas de otimização e simulação, os sensores quânticos exploram a extrema sensibilidade dos sistemas quânticos a perturbações externas para medir grandezas físicas, como campo magnético, gravidade e tempo, com precisão muito superior à dos sensores clássicos equivalentes. Essa característica torna o sensoriamento quântico uma tecnologia habilitadora natural para os pilares de resiliência operacional e sustentabilidade já discutidos nesta seção.

Magnetometria Quântica e Inspeção Não Destrutiva

Sensores baseados em centros de vacância de nitrogênio em diamante sintético, a mesma tecnologia de qubits em temperatura ambiente apresentada no Capítulo 1 na discussão sobre a Quantum Brilliance, também funcionam como magnetômetros de altíssima sensibilidade. Aplicados à inspeção não destrutiva de estruturas metálicas, dutos e componentes industriais, esses sensores permitem identificar microfissuras

e defeitos estruturais antes que se tornem falhas catastróficas, reforçando diretamente o pilar de resiliência operacional da Indústria 5.0 ao antecipar a manutenção preditiva de ativos físicos críticos.

Gravimetria Quântica e Mapeamento de Infraestrutura Subterrânea

Gravímetros quânticos, baseados em interferometria de átomos frios, medem variações mínimas no campo gravitacional local. No contexto industrial e de infraestrutura, essa tecnologia já é aplicada ao mapeamento de cavidades subterrâneas, à detecção de vazamentos em dutos enterrados e à exploração geológica de precisão, sem a necessidade de escavação exploratória. Para o setor de energia brasileiro, que já mantém cooperação com o SENAI CIMATEC em otimização de reservatórios conforme descrito na seção 4.2, a gravimetria quântica representa uma extensão natural e complementar aos algoritmos de otimização quântica ali mencionados.

Relógios Atômicos de Escala de Chip e Sincronização de Redes

A precisão de temporização é um requisito crítico tanto para as Smart Grids quanto para as redes de telecomunicação 5G e 6G discutidas no Capítulo 3, item 3.4. Relógios atômicos de escala de chip, conhecidos pela sigla em inglês CSAC (Chip-Scale Atomic Clock), oferecem sincronização de altíssima precisão em formato compacto e de baixo consumo energético, permitindo que estações-base e centros de controle regional de energia mantenham sincronismo mesmo em cenários de perda temporária de sinal de satélite, cenário relevante tanto para resiliência de infraestrutura crítica quanto para operação de dispositivos de AIoT em áreas remotas.

A Convergência das Quatro Frentes

O sensoriamento quântico, portanto, não compete com a computação quântica pela atenção das lideranças industriais, mas a complementa. Enquanto QPUs processam e otimizam, os “SQs” sensores quânticos capturam dados físicos de precisão inédita que alimentam os próprios modelos de inteligência artificial e os algoritmos de otimização quântica discutidos ao longo deste livro. Essa convergência entre captação de dados de precisão extrema e capacidade de processamento avançado é o que torna a Indústria 5.0 tecnicamente viável em sua ambição de resiliência sistêmica, e reforça a tese central desta obra de que a era quântica já opera, hoje, como infraestrutura híbrida silenciosa por trás da manufatura avançada.

Nota do Autor: Colaboração com o Sistema S

O relato institucional acima não vem de observação externa. Este autor fica feliz em testemunhar a sua atuação com o Comitê Técnico Setorial Nacional de Automação, TI e Mecatrônica do SENAI, fórum técnico-consultivo multidisciplinar que reúne representantes do SENAI, do poder público, do meio acadêmico, de associações de classe, de sindicatos patronais e de trabalhadores, com a missão de definir os perfis profissionais que sustentam a formação técnica do país.

Nessa condição, este autor colaborou diretamente na definição dos cursos técnicos que o SENAI passou a aplicar em todo o Brasil a partir de 2020, incluindo o “Técnico em Cbersistemas para Automação” e o “Técnico em Internet das Coisas (IoT)”, ao lado de representantes de organizações como o Ministério da Ciência, Tecnologia, Inovação e Comunicações, a WEG, a Festo Didactic, a Associação Brasileira de Internet das Coisas (Abinc), e a própria comunidade Tudo Sobre IoT, já mencionada neste livro, entre outros.

Essa proximidade permite a este autor afirmar, com conhecimento de causa e não por impressão distante, o poder de mobilização e a determinação genuína do Sistema S em fomentar, na prática curricular do país, a cultura de novas tecnologias que este capítulo descreve.



Instituições

- Ministério da Ciência, Tecnologia, Inovação e Comunicações – Adriana Regina Martins e Guilherme de Paula Corrêa.
- EngeBot Tecnologia – Cirineu Carvalho Fernandes e Erick Luiz Vilela Lustosa.
- Sindicato dos Tecnólogos (SP) – Cláudio Buiat.
- Festo Didactic – Felipe Gabriel Anaya.
- Associação Brasileira de Internet das Coisas (Abinc) – Flávio Maeda.
- Pollux – Geraldo Veroneze.
- Komp-FGV – João Roberto Peres.
- WEG – Equipamentos Elétricos Gilberto Schneider.
- Auttom – Gilvan Menegotto.
- De Lorenzo do Brasil – Jackson Avelino.
- Conselho Federal dos Técnicos Industriais (CFT) – Luzimar Pereira da Silva.
- Tudo Sobre IoT – Thelma Troise.
- GS1 Brasil – Associação Brasileira de Automação – Roberto Matsubayashi.
- Autentica – Vinicius carneiro Rodrigues.



CURSOS

- Técnico em cbersistemas para automação
- Técnico em internet das coisas – IoT



Prof. João Roberto Peres

Membro do Comitê Técnico Setorial Nacional de Automação, TI e Mecatrônica do SENAI, onde colaborou na definição dos novos cursos que passam a ser aplicados no Brasil a partir de 2020.

O COMITÊ TÉCNICO SETORIAL (CTS) é um fórum técnico-consultivo multidisciplinar, estruturado com representantes do SENAI, de empresas do poder público, do meio acadêmico, de associações/órgãos de classe, de sindicatos patronais e de trabalhadores, o qual possibilita a aproximação entre os mundos do trabalho e da Educação Profissional, constituindo-se na estratégia institucional para a definição de perfis profissionais.

Referências Capítulo 4

- BRASIL. **Lei nº 11.196, de 21 de novembro de 2005**. Institui incentivos fiscais às pessoas jurídicas que realizem pesquisa tecnológica e desenvolvimento de inovação tecnológica (Lei do Bem). Brasília, DF: Presidência da República, 2005. Disponível em: <http://www.planalto.gov.br>. Acesso em: 24 ago. 2026.
- EMBRAPII - EMPRESA BRASILEIRA DE PESQUISA E INOVAÇÃO INDUSTRIAL. **Relatório de Gestão e Impacto na Indústria Nacional**. Brasília: Embrapii, 2024. Disponível em: <https://embrapii.org.br>. Acesso em: 24 ago. 2026.
- LNCC - LABORATÓRIO NACIONAL DE COMPUTAÇÃO CIENTÍFICA. **Supercomputador Santos Dumont e a Infraestrutura de Processamento Científico**. Petrópolis: LNCC/MCTI, 2024. Disponível em: <https://www.gov.br/lncc>. Acesso em: 24 ago. 2026.
- SENAI CIMATEC. **Primeiro Centro de Computação Quântica no Brasil é Inaugurado no SENAI CIMATEC**. Salvador: Sistema FIEB, 2021. Disponível em: <https://www.fieb.org.br>. Acesso em: 24 ago. 2026.
- SENAI-SP. **SENAI-SP Lança Pós-Graduação em Computação Quântica e Recebe Computador Didático Quântico**. São Paulo: Editora SENAI, 2024. Disponível em: <https://www.sp.senai.br>. Acesso em: 24 ago. 2026.
- SOFTEX. **Rede MCTI Softex de Tecnologias Quânticas Computacionais: Mapeamento do Ecossistema Nacional**. Brasília: Softex/MCTI, 2022.
- ORIGEM DA INDÚSTRIA 5.0 - Michael Rada – Medium – disponível em: <https://michael-rada.medium.com/industry-5-0-origin-887fb6df7162> . Acesso em: 24 ago. 2026.
- Industry 5.0, a transformative vision for Europe - Governing systemic transformations towards a sustainable industry – disponível em: <https://op.europa.eu/en/web/eu-law-and-publications/publication-detail/-/publication/38a2fa08-728e-11ec-9136-01aa75ed71a1> . Acesso em: 24 ago. 2026.
- DEGEN, C. L.; REINHARD, F.; CAPPELLARO, P. **Quantum Sensing**. Reviews of Modern Physics, College Park, v. 89, n. 3, p. 035002, jul. 2017.
- BONGS, Kai et al. **Taking Atom Interferometric Quantum Sensors from the Laboratory to Real-World Applications**. Nature Reviews Physics, London, v. 1, p. 731-739, dez. 2019.
- Brasil entra na corrida quântica – Disponível em: <https://mittechreview.com.br/brasil-corrida-quantica-formacao-especialistas/> . Acesso em 31 de ago. 2026.
- CPQD testa transmissão quântica por 200 km em fibra óptica – disponível em: <https://teletime.com.br/23/04/2026/cpqd-transmissao-quantica-fibra-optica/> . Acesso em 24 ago. 2026.
- SENAI vai coordenar Rede Nacional de Computação Quântica MCTI/SOFTEX – 07/02/2022 – Disponível em: <https://www.fieb.org.br/noticias/senai-vai-coordenar-rede-nacional-de-computacao-quantica-mcti-softex/> . Acesso em 24 ago. 2026.
- Brasil lança centro quântico de R\$ 150 milhões com apoio da China na Paraíba – Disponível em: <https://consecti.org.br/brasil-lanca-centro-quantico-de-r-150-milhoes-com-apoio-da-china-na-paraiba/> . Acesso em 24 ago. 2026.

Capítulo 5: Roadmap Estratégico, Governança Jurídica e o Plano de Ação para Líderes

A transição para a era quântica não deve ser encarada como uma corrida desesperada por aquisição de hardware, mas como uma jornada estruturada de maturidade tecnológica, cibersegurança e governança. O maior erro das organizações na gestão de disrupções tecnológicas é a paralisia decisória motivada pela falsa percepção de que a tecnologia ainda pertence ao futuro.

Enquanto a computação quântica avança em modelos híbridos e o risco do ataque HNDL, sigla em inglês para *Harvest Now, Decrypt Later* (Capturar Agora, Decifrar Mais Tarde), expõe dados do presente, os executivos de tecnologia, financeiros e juristas precisam estabelecer um plano de ação pragmático. Este capítulo final entrega um roadmap estratégico executável, ferramentas de auditoria e a matriz de governança jurídica necessária para blindar as organizações no cenário pós-quântico.

5.1. O Roadmap Estratégico para Lideranças Corporativas

A implementação de um plano de prontidão quântica em empresas do setor financeiro, indústrias e operadoras de infraestrutura de IoT deve seguir cinco etapas sucessivas e interligadas.

Fase 1: Inventário e Mapeamento Criptográfico

O primeiro passo consiste em identificar onde os algoritmos criptográficos vulneráveis estão implantados na organização. As equipes de TI e segurança cibernética devem inventariar todas as chaves públicas, certificados digitais, conexões TLS, sigla para *Transport Layer Security* (Segurança da Camada de Transporte), e bibliotecas criptográficas em uso nos servidores, banco de dados, aplicações web e dispositivos de borda.

Fase 2: Análise de Impacto e Avaliação do Risco HNDL

Nesta fase, a organização deve categorizar seus dados e ativos de informação com base no tempo de vida útil da confidencialidade. Dados financeiros estratégicos, segredos industriais e registros médicos que exigem proteção por período superior a cinco ou dez anos devem ser classificados como ativos de alto risco para o ataque HNDL, priorizando a substituição de seus esquemas de proteção.

Fase 3: Plano de Migração PQC e Agilidade Criptográfica

Com o diagnóstico concluído, a empresa deve desenhar a estratégia de transição para os novos padrões de PQC, sigla para Post-Quantum Cryptography (Criptografia Pós-Quântica), aprovados pelo NIST, sigla em inglês para National Institute of Standards and Technology (Instituto Nacional de Padrões e Tecnologia dos Estados Unidos). Isso envolve adotar o conceito de agilidade criptográfica (crypto-agility), que é a capacidade de um sistema alternar algoritmos de criptografia via software sem exigir a reconstrução do sistema ou a substituição total do hardware legado.

Nesta fase, cabe também avaliar, para o subconjunto restrito de ativos de altíssimo valor e enlaces ponto a ponto dedicados, a aplicabilidade complementar da Distribuição Quântica de Chaves (QKD), apresentada no Capítulo 2. Reforça-se, contudo, que a QKD não substitui o esforço de migração para PQC: conforme orientação da própria NSA norte-americana em suas diretrizes CNSA 2.0, a PQC permanece o caminho primário e obrigatório de migração, cabendo à QKD um papel estritamente complementar e de nicho.

Fase 4: Experimentos Práticos via QaaS e Arquitetura Híbrida

Simultaneamente à proteção de dados, as áreas de inovação e negócios devem identificar gargalos computacionais que podem ser acelerados por algoritmos quânticos. Utilizando o modelo QaaS, acrônimo para *Quantum-as-a-Service* (Computação Quântica como Serviço), a organização testa soluções de otimização combinatória e aprendizado de máquina em nuvens quânticas sem necessidade de investimento em capital fixo (CAPEX).

Fase 5: Governança Contínua e Monitoramento Regulatório

A última etapa estabelece a revisão periódica das diretrizes de cibersegurança e o acompanhamento das normas emitidas pelos órgãos reguladores (como Banco Central do Brasil, Autoridade Nacional de Proteção de Dados e agências internacionais de cibersegurança).

5.2. Checklist de Prontidão Operacional: Setor Financeiro e IoT/AIoTT

Para apoiar a execução do roadmap, a tabela a seguir apresenta os indicadores de verificação operacional essenciais para os dois setores mais impactados pela tecnologia. Vale registrar que, além do EU Cyber Resilience Act e do US Cyber Trust Mark já referenciados na tabela, o cenário internacional conta com outros esquemas de certificação e normas técnicas de segurança IoT relevantes para a cadeia de suprimentos, detalhados no painel comparativo do Anexo 6.

Vetor de Análise	Checklist para o Setor Financeiro	Checklist para IoT e AIoT
Infraestrutura de Rede	Mapeamento de certificados digitais RSA/ECC em canais de Open Finance e APIs de transações.	Identificação de microcontroladores sem capacidade de atualização remota de firmware (OTA).
Arquitetura de Software	Teste de compatibilidade de bibliotecas PQC (FIPS 203, 204 e 205) em sistemas legados.	Validação da capacidade de memória RAM para suporte aos novos tamanhos de chaves pós-quânticas.
Segurança da Informação	Avaliação do tempo de retenção de dados confidenciais frente ao risco de interceptação HNDL.	Implementação de isolamento físico e lógico para sensores industriais críticos de longo ciclo de vida.
Projetos de Inovação	Execução de testes conceituais via QaaS em otimização de carteiras e cálculo de risco (VaR).	Avaliação de simuladores quânticos para balanceamento de carga em redes de energia ou tráfego.
Cadeia de Suprimentos	Auditoria de conformidade PQC em provedores de nuvem, <i>core banking</i> e meios de pagamento.	Exigência contratual de agilidade criptográfica nos módulos de comunicação vendidos por terceiros, verificada frente ao conjunto de normas e selos de certificação aplicáveis à jurisdição de destino do produto (ver Anexo 6).

5.3. Matriz de Governança Jurídica, LGPD e Responsabilidade Civil

A transição quântica impõe responsabilidades diretas aos departamentos jurídicos, advogados corporativos e membros dos conselhos de administração. A conformidade regulatória e a mitigação da responsabilidade civil dependem do alinhamento entre o conhecimento técnico e a prática do Direito Digital.

O Dever de Diligência (*Duty of Care*) e a Responsabilidade dos Administradores

No âmbito do Direito Societário e da Lei das Sociedades por Ações (Lei nº 6.404/1976), os administradores de empresas têm o dever de empregar, no exercício de suas funções, o cuidado e a diligência que todo homem ativo e probo costuma empregar na administração dos seus próprios negócios.

Frente ao fato de que o NIST já publicou os padrões oficiais de Criptografia Pós-Quântica e que o ecossistema financeiro e governamental iniciou a migração, o desconhecimento da ameaça quântica deixa de ser uma excludente de ilicitude. Caso uma organização sofra um vazamento massivo decorrente da quebra de chaves RSA obsoletas por omissão em planejar a transição, os diretores e conselheiros poderão responder por descumprimento do dever de diligência.

A LGPD e o Risco de Segurança por Concepção (*Security by Design*)

A Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 - LGPD) determina no artigo 46 que os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais. O parágrafo 1º do mesmo artigo ressalta que a autoridade reguladora considerará o estado da tecnologia no momento do tratamento ao avaliar a adequação das medidas de segurança.

À medida que os padrões PQC se consolidam como o estado atual da tecnologia de proteção, a manutenção de dados pessoais sensíveis criptografados por algoritmos sabidamente vulneráveis e com risco iminente de decifração via HNDL pode ser enquadrada como falha de segurança pela Autoridade Nacional de Proteção de Dados (ANPD). Isso sujeita a empresa às sanções administrativas previstas no artigo 52 da LGPD, incluindo multas de até 50 milhões de reais por infração, além de reparações civis por danos morais individuais e coletivos.

Estruturação de Contratos e Gestão da Cadeia de Suprimentos

A governança jurídica exige a revisão imediata dos instrumentos contratuais da organização com seus fornecedores de tecnologia da informação, parceiros de nuvem e fabricantes de dispositivos conectados:

- **Inclusão de Garantia de Atualização PQC:** Os contratos de fornecimento de software e serviços em nuvem devem prever expressamente a obrigação do prestador de disponibilizar atualizações de segurança baseadas nos padrões FIPS 203, 204 e 205 do NIST sem custos adicionais desproporcionais.
- **Matriz de Responsabilidade por Incidentes:** Delimitação clara de responsabilidades contratuais em caso de incidentes de segurança decorrentes de falhas na implementação de novos algoritmos criptográficos.
- **Cláusula de Transição e Agilidade Criptográfica:** Exigência de que novos equipamentos de IoT adquiridos pela empresa possuam arquitetura compatível com *crypto-agility*, garantindo a atualização de segurança ao longo de todo o ciclo de vida do ativo.

A computação quântica deixou de ser uma abstração da física teórica para se consolidar como um pilar de soberania nacional, eficiência de capital e cibersegurança. O paradoxo entre a baixa visibilidade na grande mídia e a movimentação bilionária nos bastidores do mercado não deve iludir as lideranças corporativas.

Aqueles que compreenderem que o presente é híbrido e que a proteção de dados deve ser atualizada no presente estarão posicionados na vanguarda da competitividade global. A preparação para a era quântica é uma decisão de governança, estratégia e visão de longo prazo que precisa ser tomada hoje.

Referências Capítulo 5

ANPD - AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia Orientativo de Segurança da Informação para Agentes de Tratamento de Pequeno Porte**. Brasília: ANPD, 2023. Disponível em:

<https://www.gov.br/anpd>. Acesso em: 24 ago. 2026.

BRASIL. **Lei nº 6.404, de 15 de dezembro de 1976**. Dispõe sobre as Sociedades por Ações. Brasília, DF: Presidência da República, 1976. Disponível em: <http://www.planalto.gov.br>. Acesso em: 24 ago. 2026.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais (Lei Geral de Proteção de Dados Pessoais - LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: <http://www.planalto.gov.br>. Acesso em: 24 ago. 2026.

CISA - CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY. **Preparing for Post-Quantum Cryptography: A Roadmap for Critical Infrastructure**. Washington, D.C.: U.S. Department of Homeland Security, 2023. Disponível em: <https://www.cisa.gov>. Acesso em: 24 ago. 2026.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST). **Migration to Post-Quantum Cryptography: Building a Quantum-Resilient Architecture**. Gaithersburg: U.S. Department of Commerce, 2024. (NIST Special Publication 1800-38). Disponível em: <https://csrc.nist.gov>. Acesso em: 24 ago. 2026.

WEF - WORLD ECONOMIC FORUM. **Post-Quantum Cryptography Readiness: Guidelines for Boards and Executive Leadership**. Geneva: World Economic Forum, 2024. Disponível em: <https://www.weforum.org>. Acesso em: 24 ago. 2026.

Anexo 1: Glossário Executivo Quântico-Técnico

Este glossário reúne e traduz os principais termos, acrônimos e conceitos da era quântica e da cibersegurança pós-quântica. O objetivo é fornecer uma ferramenta de consulta rápida para executivos, juristas, gestores de tecnologia e profissionais de cibersegurança durante reuniões estratégicas, auditorias e tomada de decisões corporativas.

A

- **Agilidade Criptográfica (*Crypto-Agility*):** Capacidade de um sistema de informação, software ou infraestrutura de hardware alternar ou atualizar algoritmos criptográficos via software sem exigir a reconstrução do sistema ou a substituição total do hardware legado.
- **Algoritmo de Shor:** Algoritmo quântico desenvolvido por Peter Shor em 1994, capaz de resolver problemas de fatoração de números inteiros primos e logaritmos discretos em tempo polinomial, tornando obsoletos os sistemas de criptografia assimétrica clássica (como RSA e ECC).
- **AIoT (*Artificial Intelligence of Things*):** Integração das tecnologias de Inteligência Artificial com a infraestrutura da Internet das Coisas (IoT), permitindo análise de dados e tomada de decisão automatizada diretamente nos dispositivos ou na ponta da rede.

B

- **BB84:** Primeiro protocolo de Distribuição Quântica de Chaves (QKD), proposto em 1984, que permanece como referência conceitual para a maioria das implementações comerciais atuais dessa tecnologia.

C

- **CBOM (*Cryptographic Bill of Materials*):** Lista estruturada e automatizada dos componentes criptográficos presentes em um software, firmware ou dispositivo conectado. Inclui algoritmos, tamanhos de chaves, bibliotecas e certificados digitais em uso.

Ferramentas CBOM

CBOMkit (IBM): Um kit de ferramentas de código aberto que inclui o componente **cbomkit-hyperion** para análise estática de código e detecção de ativos criptográficos. O repositório oficial e os exemplos de esquema podem ser acessados no [Repositório GitHub da IBM CBOM](#). [1, 2]

IBM Quantum Safe Explorer: Uma ferramenta corporativa da IBM que escaneia projetos e exporta o inventário criptográfico em formato .json automaticamente. [1]

CycloneDX CBOM Generator: Uma ferramenta online e gratuita que roda direto no navegador para criar arquivos JSON compatíveis com o padrão CycloneDX. Acesse o [CycloneDX CBOM Generator](#). [1]

CodeQL com scripts personalizados: É possível usar a CLI do CodeQL combinada com scripts em Python para analisar bases de código e mapear algoritmos e chaves em um arquivo cbom.json. [1]

- **CIQuanta (Centro Internacional de Computação Quântica):** Hub de pesquisa e inovação sediado na Paraíba (João Pessoa), focado em desenvolvimento de hardware, fotônica, simulação quântica e cooperação internacional no Brasil.
- **CPU (*Central Processing Unit*):** Unidade Central de Processamento clássica, otimizada para tarefas sequenciais, controle de fluxo e lógica de negócios tradicional.
- **CNSA 2.0 (Commercial National Security Algorithm Suite 2.0):** Conjunto de diretrizes da Agência de Segurança Nacional dos Estados Unidos (NSA) que orienta a migração criptográfica de Sistemas de Segurança Nacional, recomendando a Criptografia Pós-Quântica (PQC) como caminho primário e não aprovando o uso isolado de QKD para essa finalidade.
- **CSAC (Chip-Scale Atomic Clock):** Relógio Atômico de Escala de Chip. Dispositivo de sincronização de altíssima precisão em formato compacto e baixo consumo energético, aplicável a redes de telecomunicação, Smart Grids e dispositivos de AIoT em áreas remotas.

E

- **ECC (*Elliptic Curve Cryptography*):** Criptografia de Curva Elíptica. Método criptográfico assimétrico amplamente utilizado na internet e em dispositivos IoT devido às chaves de tamanho reduzido, porém vulnerável ao Algoritmo de Shor em computadores quânticos.
- **Edge Computing (Computação na Ponta):** Arquitetura de TI em que o processamento de dados ocorre fisicamente próximo do local onde o dado é gerado (em sensores ou gateways locais), reduzindo a latência de comunicação com a nuvem.

F

- **FIPS 203 (ML-KEM):** Padrão oficial do NIST denominado *Module-Lattice-Based Key-Encapsulation Mechanism Standard*. Algoritmo pós-quântico recomendado para troca e estabelecimento seguro de chaves criptográficas em redes globais.
- **FIPS 204 (ML-DSA):** Padrão oficial do NIST denominado *Module-Lattice-Based Digital Signature Standard*. Algoritmo pós-quântico destinado à proteção de assinaturas digitais gerais e autenticação de documentos.
- **FIPS 205 (SLH-DSA):** Padrão oficial do NIST denominado *Stateless Hash-Based Digital Signature Standard*. Algoritmo pós-quântico de assinatura digital baseado em funções hash, atuando como alternativa aos métodos de redes reticulares.

G

- **GPU (*Graphics Processing Unit*):** Unidade de Processamento Gráfico, especializada em cálculos matriciais paralelos massivos, amplamente utilizada no treinamento de modelos de Inteligência Artificial e simulações complexas.

H

- **HNDL (*Harvest Now, Decrypt Later*):** Tática cibernética que consiste em interceptar e armazenar dados criptografados hoje para decifrá-los retrospectivamente no futuro, assim que um computador quântico funcional estiver disponível.
- **HPC (*High-Performance Computing*):** Computação de Alto Desempenho. Uso de supercomputadores e aglomerados de servidores para resolver problemas científicos e industriais de alta complexidade.

I

- **IoT (*Internet of Things*):** Internet das Coisas. Rede de objetos físicos, veículos, edifícios e sensores industriais dotados de tecnologia embarcada para coleta e transmissão de dados.

M

- **Magnetometria Quântica:** Técnica de medição de campo magnético de altíssima sensibilidade, baseada em sensores quânticos (como centros de vacância de nitrogênio em diamante sintético), aplicada à inspeção não destrutiva de estruturas e à manutenção preditiva industrial.

N

- **NISQ (*Noisy Intermediate-Scale Quantum*):** Era Quântica de Escala Intermediária com Ruído. Fase atual das principais tecnologias quânticas, caracterizada por processadores contendo de dezenas a centenas de qubits que ainda sofrem interferência do ambiente e exigem correção de erros híbrida.
- **NIST (*National Institute of Standards and Technology*):** Instituto Nacional de Padrões e Tecnologia dos EUA. Órgão responsável pela padronização mundial dos novos algoritmos de Criptografia Pós-Quântica (PQC).
- **No-Cloning Theorem (Teorema da Não Clonagem):** Princípio da mecânica quântica que estabelece a impossibilidade de copiar um estado quântico desconhecido sem alterá-lo, fundamento físico que garante a segurança da Distribuição Quântica de Chaves (QKD).

P

- **PQC (*Post-Quantum Cryptography*):** Criptografia Pós-Quântica. Família de algoritmos matemáticos projetados para rodar em computadores clássicos existentes, mas estruturados sobre problemas matemáticos resistentes a ataques de computadores clássicos e quânticos.

Q

- **QaaS (*Quantum-as-a-Service*):** Computação Quântica como Serviço. Modelo de negócios que permite o acesso remoto a processadores quânticos localizados na nuvem via APIs ou SDKs, sem necessidade de compra de hardware físico pelas empresas. Dezenas de fornecedores.
- **QAOA (*Quantum Approximate Optimization Algorithm*):** Algoritmo Quântico de Otimização Aproximada. Algoritmo híbrido voltado para a resolução de problemas de otimização combinatória complexos em logística, redes e finanças.
- **Q-Day (Dia Quântico):** Marco temporal estimado em que um computador quântico atingirá a escala e a fidelidade necessárias para quebrar os padrões de criptografia assimétrica clássica (RSA/ECC) em tempo hábil.
- **QKD (*Quantum Key Distribution*):** Distribuição Quântica de Chaves. Técnica que utiliza fótons individuais e propriedades da mecânica quântica para transmitir chaves criptográficas, revelando fisicamente qualquer tentativa de interceptação. Complementar, e não substituta, da Criptografia Pós-Quântica (PQC).
- **QML (*Quantum Machine Learning*):** Aprendizado de Máquina Quântico. Subcampo da IA que combina algoritmos de aprendizado de máquina com o processamento em QPUs para acelerar o reconhecimento de padrões em bases de dados multidimensionais.

- **QPU (*Quantum Processing Unit*):** Unidade de Processamento Quântico. Processador de hardware projetado para manipular qubits utilizando os princípios da mecânica quântica (superposição e emaranhamento).
- **Qubit (*Bit Quântico*):** Unidade fundamental de informação na computação quântica. Diferente do bit clássico (que assume valor 0 ou 1), o qubit pode existir em estados de superposição simultânea.

R

- **RSA (*Rivest-Shamir-Adleman*):** Um dos primeiros sistemas de criptografia de chave pública amplamente adotados no mundo para transmissão segura de dados e assinaturas digitais, vulnerável ao processamento quântico.

T

- **TLS (*Transport Layer Security*):** Protocolo de Segurança da Camada de Transporte. Padrão de cibersegurança projetado para garantir a privacidade e a integridade de dados transmitidos entre aplicações na internet (base do HTTPS e de APIs bancárias). O atual TLS 1.3 é supostamente resistente a ataques de computação quântica (não sabemos na prática).

V

- **VQE (*Variational Quantum Eigensolver*):** Eigensolver Quântico Variacional. Algoritmo híbrido aplicado na simulação de química quântica, estrutura molecular e descoberta de materiais na indústria farmacêutica e de energia.

Anexo 2: Checklist de Auditoria e Readiness (Matriz de Prontidão PQC)

Esta ferramenta operacional foi desenhada para apoiar diretores de TI (CTO/CISO), gestores de riscos, auditores e departamentos jurídicos no diagnóstico e acompanhamento do nível de prontidão da organização frente à transição pós-quântica.

Recomenda-se a aplicação periódica deste checklist para acompanhamento do dever de diligência (*duty of care*) e conformidade com os requisitos da **Executive Order 14412** e da **LGPD**.

1. Mapeamento de Ativos e Governança Corporativa

Item	Ação de Auditoria / Verificação	Status	Responsável	Prazo
1.1	A organização nomeou formalmente um líder executivo de migração quântica (<i>PQC Migration Lead</i>)?	☐ Sim ☐ Não		
1.2	Foi realizado um inventário automatizado para emissão do <i>Cryptographic Bill of Materials</i> (CBOM) de softwares e firmware?	☐ Sim ☐ Não		
1.3	Os dados mantidos pela empresa foram classificados pelo tempo de retenção (identificando ativos com risco crítico para o ataque <i>Harvest Now, Decrypt Later</i> - HNDL)?	☐ Sim ☐ Não		
1.4	O conselho de administração ou diretoria executiva recebe relatórios periódicos sobre a evolução dos riscos quânticos nos ativos da empresa?	☐ Sim ☐ Não		

2. Infraestrutura de TI, Sistemas Legados e Nuvem

Item	Ação de Auditoria / Verificação	Status	Responsável	Prazo
2.1	As conexões de borda, APIs e servidores já suportam o protocolo TLS 1.3 com negociação de chaves em modo híbrido?	☐ Sim ☐ Não		
2.2	As chaves públicas, certificados digitais (RSA/ECC) e autoridades certificadoras internas foram mapeados com cronograma para substituição pelo padrão FIPS 203 (ML-KEM) ?	☐ Sim ☐ Não		
2.3	Os sistemas de autenticação, assinaturas digitais e não repúdio possuem plano de transição para os padrões FIPS 204 (ML-DSA) ou FIPS 205 (SLH-DSA) ?	☐ Sim ☐ Não		
2.4	Provedores de nuvem e parceiros de <i>core banking</i> /ERP apresentaram relatórios formais de conformidade com os novos padrões PQC do NIST?	☐ Sim ☐ Não		
2.5	Foi avaliada a aplicabilidade complementar da Distribuição Quântica de Chaves (QKD) para enlaces ponto a ponto de ativos de altíssimo valor, sem prejuízo da migração prioritária para PQC?	☐ Sim ☐ Não		

Obs.: A Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) iniciou uma modernização estrutural ao publicar a Instrução Normativa nº 35 do ITI (de 3 de fevereiro de 2026), estabelecendo formalmente a transição para a criptografia pós-quântica (PQC) em seus padrões técnicos (DOC-ICP-01.01 Versão 6.0). A medida visa antecipar ameaças da computação quântica incorporando os algoritmos mundiais ML-KEM e ML-DSA (padrões NIST), o que impacta diretamente a emissão de novos certificados digitais e o ecossistema da Assinatura Gov.br. Para coordenar essa migração gradual e estabelecer roteiros de transição híbridos, o governo instituiu também o Grupo de Trabalho Técnico (GTT-PQC/ICP-Brasil), garantindo a segurança de longo prazo em assinaturas de sistemas, documentos eletrônicos e plataformas homologadas.

3. Internet das Coisas (IoT) e AIoT na Ponta

Item	Ação de Auditoria / Verificação	Status	Responsável	Prazo
3.1	Os dispositivos de IoT/AIoT com ciclo de vida superior a 5 anos foram identificados e isolados logicamente em segmentos protegidos?	☐ Sim ☐ Não		
3.2	Os microcontroladores e módulos de comunicação embutidos nos sensores possuem capacidade física de memória para suportar o tamanho das chaves PQC?	☐ Sim ☐ Não		
3.3	Existe suporte nativo a atualizações remotas de firmware (<i>Over-The-Air</i> - OTA) protegidas por assinaturas resistentes a ataques quânticos?	☐ Sim ☐ Não		
3.4	Novos editais ou pedidos de compra de hardware exigem contratualmente a funcionalidade de agilidade criptográfica (<i>crypto-agility</i>)?	☐ Sim ☐ Não		
3.5	Os módulos de IoT/AIoT da empresa foram submetidos a testes de conformidade com o EU Cyber Resilience Act (CRA) e o programa US Cyber Trust Mark ?	☐ Sim ☐ Não		

4. Governança Jurídica, Contratos e LGPD

Item	Ação de Auditoria / Verificação	Status	Responsável	Prazo
4.1	Os contratos com terceiros e fornecedores de tecnologia contêm cláusulas de garantia de atualização para Criptografia Pós-Quântica sem custo adicional?	☐ Sim ☐ Não		
4.2	A Política de Segurança da Informação e os relatórios de impacto à proteção de dados (RIPD/LGPD) foram atualizados considerando o estado da arte do PQC?	☐ Sim ☐ Não		
4.3	Há previsão de matriz de responsabilidade civil para eventuais vazamentos decorrentes da descontinuação ou quebra de algoritmos legados (RSA/ECC)?	☐ Sim ☐ Não		
4.4	As operações transfronteiriças de dados e contratações de serviços de TI atendem aos requisitos de conformidade impostos pela Executive Order 14412 ?	☐ Sim ☐ Não		Sem prazo definido ainda para o Brasil.
4.5	As políticas de privacidade e segurança da informação incluem o mapeamento de riscos para a Indústria 5.0 e resiliência cibernética na cadeia de suprimentos?	☐ Sim ☐ Não	Jurídico / CISO	

Anexo 3: Modelo de Cláusula Contratual PQC (Criptografia Pós-Quântica)

A minuta abaixo destina-se à inserção em instrumentos contratuais de prestação de serviços de Tecnologia da Informação (TI), contratação de serviços de nuvem (Cloud Computing), licenciamento de software e aquisição de dispositivos ou módulos de Internet das Coisas (IoT/AIoT).

O objetivo do dispositivo é resguardar a empresa Contratante contra a descontinuação de suporte técnico, garantir a conformidade com os novos padrões mundiais de segurança (NIST FIPS 203, 204 e 205), acompanhar a convergência regulatória internacional detalhada no Anexo 6 desta obra, e assegurar o dever de segurança exigido pelo Artigo 46 da LGPD (Lei nº 13.709/2018).

Nota de uso: esta é uma minuta de referência, não uma cláusula de aceitação automática. Sua redação final deve ser negociada e ajustada conforme o poder de barganha das partes, o porte do fornecedor e a natureza do fornecimento. As Subcláusulas Primeira, Terceira, Quarta e Quinta aplicam-se de forma geral. A Subcláusula Segunda oferece duas variantes, conforme o tipo de fornecimento contratado, detalhadas abaixo.

CLÁUSULA DE GARANTIA DE AGILIDADE CRIPTOGRÁFICA E CONFORMIDADE PÓS-QUÂNTICA (PQC)

Subcláusula Primeira – Da Agilidade Criptográfica (Crypto-Agility):

A CONTRATADA declara e garante que as soluções de software, infraestrutura em nuvem, firmware e/ou dispositivos de hardware fornecidos sob o presente Contrato foram desenvolvidos com suporte à agilidade criptográfica (crypto-agility). Isso significa que os sistemas possuem capacidade técnica de atualizar, substituir ou alternar algoritmos criptográficos, comprimentos de chaves e bibliotecas de segurança sem interrupção catastrófica do serviço, sem custos adicionais de reconstrução da arquitetura e sem necessidade de substituição precoce do hardware.

Subcláusula Segunda – Do Alinhamento aos Padrões PQC e às Normas de Certificação Aplicáveis:

A CONTRATADA compromete-se a manter as soluções fornecidas em estrita conformidade com o estado da arte em cibersegurança, adotando os padrões PQC do NIST (FIPS 203, 204 e 205), bem como as normas técnicas e esquemas de certificação de segurança aplicáveis à jurisdição de destino do produto ou serviço, incluindo, mas não se limitando a: EU Cyber Resilience Act e norma técnica ETSI EN 303 645 (União Europeia), US Cyber Trust Mark e NIST IR 8425 (Estados Unidos), UK PSTI Act (Reino Unido), Cybersecurity Labelling Scheme (Singapura), e os frameworks setoriais GSMA IoT SAFE e IoT Security Foundation (IoTSF), conforme detalhado no Anexo 6 desta obra.

Variante (a), para fornecimento de software, licenciamento e serviços em nuvem: a obrigação de conformidade recai sobre os protocolos de criptografia, mecanismos de autenticação e canais de comunicação da solução, sem exigência de certificação de hardware físico.

Variante (b), para fornecimento de dispositivos conectados, firmware embarcado ou hardware IoT/AIoT: a obrigação de conformidade estende-se também à segurança física do dispositivo, à capacidade de atualização remota de firmware (Over-The-Air) e à vedação de credenciais padrão de fábrica, nos termos exigidos pelas normas de certificação aplicáveis.

Caso a CONTRATADA integre a cadeia de suprimento de sistemas ou infraestrutura crítica sujeitos à jurisdição federal dos Estados Unidos, aplica-se adicionalmente o cronograma de transição estabelecido pela Executive Order 14412, nos limites de seu alcance normativo: mandado direto sobre sistemas federais classificados como ativos de alto valor (High Value Assets), com prazo de 31 de dezembro de 2030 para

estabelecimento de chaves e 31 de dezembro de 2031 para assinaturas digitais; e apoio técnico, não mandado direto, a operadores de infraestrutura crítica privada. Esta subcláusula não deve ser interpretada como imposição automática de obrigações da Executive Order 14412 a fornecedores que não integrem essa cadeia específica.

Subcláusula Terceira – Da Lista de Componentes Criptográficos (CBOM) e Transparência:

A CONTRATADA deverá disponibilizar à CONTRATANTE, mediante solicitação formal ou no momento da entrega/atualização das soluções, a Lista de Ingredientes Criptográficos, denominada Cryptographic Bill of Materials (CBOM). O CBOM deverá detalhar:

- Todos os algoritmos de criptografia assimétrica e simétrica atualmente embarcados;
- Os comprimentos de chaves e algoritmos de hash utilizados;
- A identificação de bibliotecas de terceiros e a presença de protocolos legados (como RSA e ECC);
- O plano e cronograma detalhado para substituição de mecanismos vulneráveis ao risco de interceptação e decifração retroativa (Harvest Now, Decrypt Later - HNDL).

Subcláusula Quarta – Das Atualizações Gratuitas de Segurança:

Todas as atualizações de software, patches de correção, migrações de firmware via rede (Over-The-Air - OTA) e substituição de bibliotecas criptográficas necessárias para implementar os padrões de Criptografia Pós-Quântica deverão ser fornecidas pela CONTRATADA sem qualquer ônus financeiro adicional para a CONTRATANTE, estando tais obrigações cobertas pelo valor de manutenção, suporte ou licenciamento já pactuado no Contrato.

Subcláusula Quinta – Da Responsabilidade por Incidentes e Inconformidade:

A recusa, omissão ou inércia injustificada da CONTRATADA em disponibilizar atualizações de segurança pós-quântica dentro dos prazos estabelecidos pelo NIST e pelas normas de certificação aplicáveis nos termos da Subcláusula Segunda será considerada infração contratual grave, sujeitando a CONTRATADA às penalidades rescisórias previstas neste Contrato. A CONTRATADA responderá integralmente pelos danos materiais, lucros cessantes, multas administrativas impostas por autoridades reguladoras (incluindo a ANPD) e indenizações decorrentes de incidentes de segurança decorrentes do uso continuado de algoritmos sabidamente descontinuados ou vulneráveis, observados os limites de responsabilidade e as demais condições gerais negociadas entre as partes neste Contrato.

Anexo 4: Matriz Comparativa dos Padrões PQC do NIST (FIPS 203, 204 e 205)

Esta matriz foi desenvolvida para servir como guia de referência técnica para arquitetos de software, especialistas em cibersegurança (CISOs), engenheiros de IoT e auditores de conformidade. Ela resume as especificações dos novos padrões de Criptografia Pós-Quântica (PQC) homologados pelo NIST, fornecendo os links oficiais e públicos para download da documentação técnica e implementação.

1. Tabela Comparativa de Especificações Técnicas

Parâmetro / Critério	FIPS 203 (ML-KEM)	FIPS 204 (ML-DSA)	FIPS 205 (SLH-DSA)
Algoritmo de Origem	CRYSTALS-Kyber	CRYSTALS-Dilithium	SPHINCS+
Função Principal	Encapsulamento de Chaves (KEM) e Troca Segura em Redes.	Assinaturas Digitais e Autenticação de Documentos/Código.	Assinaturas Digitais de Reserva Baseadas em Hash.
Fundamento Matemático	Problemas de Redes Reticulares Modulares (<i>Module Lattices</i>).	Problemas de Redes Reticulares Modulares (<i>Module Lattices</i>).	Árvores e Funções Hash Criptográficas (Sem Estado / <i>Stateless</i>).
Tamanho Típico da Chave	Média (~800 a 1.568 bytes).	Média a Grande (~1.312 a 2.592 bytes).	Pequena a Média (~32 a 64 bytes).
Tamanho da Assinatura / Pacote	Média (~768 a 1.568 bytes).	Média (~2.420 a 4.595 bytes).	Elevado (~7,8 KB a 49,8 KB).
Impacto na RAM e Latência	Baixo consumo; excelente desempenho para protocolos TLS.	Desempenho equilibrado para servidores e aplicações web.	Processamento mais intensivo e assinaturas maiores.
Caso de Uso Recomendado	Conexões HTTPS, TLS 1.3, VPNs, APIs bancárias e Open Finance.	Assinaturas de contratos, certificados digitais PKI e firmware OTA.	Aplicações de alta segurança como alternativa conservadora a redes reticulares.

Criptografia para IoT

Para IoT e AIOT a estratégia do NIST divide-se entre a padronização de criptografia leve simétrica e o desenvolvimento contínuo de assinaturas pós-quânticas leves: [\[1, 2\]](#)

1. O Padrão Oficial de Criptografia Leve para IoT: A Família ASCON

Finalizado oficialmente pelo NIST por meio da publicação da norma [NIST SP 800-232](#), a família **ASCON** é o padrão definitivo de criptografia leve para dispositivos de recursos extremamente restritos (como chips RFID, sensores de IoT e implantes médicos). [\[1, 2, 3, 4\]](#)

O ASCON é baseado em permutações e foi projetado para substituir o AES em cenários onde o consumo de energia e o espaço de silício são críticos. Ele opera nas seguintes vertentes principais: [\[1, 2\]](#)

- **ASCON-128 AEAD:** Focado em criptografia autenticada com dados associados, garantindo confidencialidade e integridade simultaneamente.
- **ASCON-Hash 256:** Voltado para a geração de assinaturas digitais leves e verificação de integridade de dados (hashing).
- **ASCON-XOF e CXOF:** Funções de saída estendida para flexibilidade no tamanho do hash. [\[1, 2, 3, 4\]](#)

Nota de segurança: Embora o ASCON proteja contra-ataques computacionais clássicos em ambientes miniaturizados, ele possui resistência quântica limitada às suas chaves simétricas (recomenda-se o uso de chaves maiores ou designs adaptados caso o atacante use a variante quântica do algoritmo de Grover). [\[1\]](#)

2. A Transição para o PQC Leve (Criptografia Pós-Quântica para IoT)

Como os primeiros padrões globais de PQC do NIST (como o FIPS 203 - ML-KEM e FIPS 204 - ML-DSA) geram chaves e assinaturas muito grandes para redes IoT pequenas, o NIST e a comunidade de pesquisa estão trabalhando na adaptação e otimização desses sistemas. As principais abordagens incluem: [\[1, 2, 3, 4\]](#)

- **FN-DSA (Fingerprint-N-Digital Signature Algorithm):** Um esquema de assinaturas de chaves públicas baseado em redes (*lattices*) derivado do FALCON, refinado especificamente para o ecossistema de baixo processamento em IoT por apresentar chaves menores e menor consumo de banda. [\[1, 2\]](#)
- **Abordagem Híbrida em Hardware e Software:** Chips modernos de segurança para IoT utilizam coprocessadores de aceleração física para executar implementações otimizadas do **Kyber-512 (ML-KEM)** de forma compacta e eficiente energeticamente. [\[1\]](#)

Vamos aguardar as novidades.

Referencias Anexo 4

Para obter a especificação completa dos padrões, bibliotecas de código e guias de implementação, acesse os canais oficiais do Governo dos Estados Unidos e do NIST:

Documentação Oficial do NIST e Repositórios Comprováveis

Padrões Oficiais FIPS (Documentos Finais):

- **NIST FIPS 203 (ML-KEM Standard):**

Documentação técnica oficial sobre o mecanismo de encapsulamento de chaves baseado em redes reticulares.

URL: <https://csrc.nist.gov/pubs/fips/203/final>

- **NIST FIPS 204 (ML-DSA Standard):**

Especificação completa do padrão de assinatura digital baseado em redes reticulares.

URL: <https://csrc.nist.gov/pubs/fips/204/final>

- **NIST FIPS 205 (SLH-DSA Standard):**

Padrão de assinatura digital baseado em funções hash sem estado.

URL: <https://csrc.nist.gov/pubs/fips/205/final>

Projetos de Migração, Testes e Ferramentas Práticas:

- **NIST Post-Quantum Cryptography Standardization Project:**

Página central do projeto do NIST contendo histórico, algoritmos adicionais em avaliação (Round 4) e relatórios de desempenho.

URL: <https://csrc.nist.gov/projects/post-quantum-cryptography>

- **NCCoE / NIST – Migration to Post-Quantum Cryptography:**

Centro de Excelência em Cibersegurança do NIST com guias práticos para mapeamento de ativos, emissão de CBOM e arquiteturas de migração.

URL: <https://www.nccoe.nist.gov/crypto-agility-migration-post-quantum-cryptography>

- **Open Quantum Safe (OQS Project):**

Projeto de código aberto (com suporte da indústria e comunidade global) que disponibiliza bibliotecas em C (liboqs), integrações com OpenSSL e TLS 1.3 para testes práticos dos algoritmos FIPS 203, 204 e 205.

URL: <https://openquantumsafe.org/>

Acessos em Agosto de 2026.

Anexo 5: Evidência Recente de Mercado – O Ecossistema de São Paulo e o Debate FAPESP

Tema: *A Transição da Computação Quântica dos Laboratórios para o Mercado*

1. Síntese do Evento e Contexto Estratégico

O anexo registra a conferência internacional promovida pela FAPESP (*Fundação de Amparo à Pesquisa do Estado de São Paulo*), reunindo lideranças científicas da USP e Unicamp, executivos de *big techs* globais (IBM e Google), o setor bancário e *deep techs* locais. O objetivo central foi debater a passagem da física teórica para a aplicação comercial em otimização, simulação molecular e cibersegurança no Brasil.

2. Os Três Pilares para o Aumento da Competitividade Nacional

- **Adoção Híbrida via QaaS (*Quantum-as-a-Service*):** Como corporações brasileiras estão realizando Provas de Conceito (*PoCs*) via nuvem sem a necessidade de adquirir hardware físico.
- **Fomento a Deep Techs (Programa PIPE/FAPESP):** O financiamento estatal não reembolsável para mitigar riscos na criação de startups brasileiras de software quântico e Criptografia Pós-Quântica (PQC).
- **Formação Interdisciplinar de Talentos:** Programas de capacitação conjunta entre universidades paulistas e o setor privado para suprir a escassez de profissionais com letramento quântico.

Referência Anexo 5

AGÊNCIA FAPESP. Conferência FAPESP debate a transição da computação quântica dos laboratórios para o mercado. São Paulo: FAPESP, 17 ago. 2026. Disponível em: <https://agencia.fapesp.br/conferencia-fapesp-debate-a-transicao-da-computacao-quantica-dos-laboratorios-para-o-mercado/58977>. Acesso em: 29 ago. 2026.

Anexo 6: Tabela de Enquadramento Regulatório Internacional de IoT/AIoT e Indústria 5.0

Esta matriz sintetiza as principais exigências regulatórias internacionais aplicáveis a dispositivos conectados, redes industriais e soluções de inteligência artificial na ponta, servindo de roteiro de conformidade para empresas brasileiras operando em cadeias globais de suprimento.

Marco Regulatório / Diretriz	Jurisdição / Órgão	Foco Principal de Exigência	Exigência Técnica de Criptografia / PQC	Impacto na Indústria Brasileira
Executive Order 14412	Estados Unidos (The White House)	Transição compulsória para PQC em sistemas federais e infraestrutura crítica.	Implementação dos padrões FIPS 203 até 2030 e FIPS 204/205 até 2031. Exigência de CBOM.	Restrição de fornecimento para órgãos ou parceiros norte-americanos sem CBOM.
EU Cyber Resilience Act (CRA)	União Europeia (Comissão Europeia)	Segurança cibernética compulsória para produtos com elementos digitais (IoT/AIoT).	Security by Design, suporte a atualizações OTA gratuitas e eliminação de protocolos obsoletos.	Barreira técnica para exportação de hardware e software brasileiro para o bloco europeu.
US Cyber Trust Mark	Estados Unidos (FCC)	Selo de garantia de cibersegurança para dispositivos de consumo e IoT industrial.	Testes de vulnerabilidade periódicos, ausência de senhas padrão e agilidade criptográfica.	Exigência dos importadores dos EUA para aceitação de produtos eletrônicos brasileiros.
Diretrizes da Indústria 5.0	União Europeia / Global	Resiliência cibernética, sustentabilidade (ESG) e centralidade humana.	Proteção contra paralisação de redes inteligentes, robôs colaborativos e gêmeos digitais.	Requisito de governança para atração de fundos de investimento e capital estrangeiro.
ETSI EN 303 645	União Europeia (ETSI)	Norma técnica de segurança (baseline) para IoT de consumo. Fundamenta tecnicamente tanto o EU Cyber Resilience Act quanto, indiretamente, esquemas de outras jurisdições.	Vedação a credenciais padrão, gestão segura de vulnerabilidades e atualização de firmware; não fixa algoritmo PQC específico, mas exige agilidade criptográfica.	Referência técnica de facto para fabricantes brasileiros que exportam para a União Europeia, independentemente da certificação formal exigida.

Marco Regulatório / Diretriz	Jurisdição / Órgão	Foco Principal de Exigência	Exigência Técnica de Criptografia / PQC	Impacto na Indústria Brasileira
UK PSTI Act (Product Security and Telecommunications Infrastructure Act)	Reino Unido	Lei de segurança de produtos conectados, em vigor desde 2024, equivalente britânico ao US Cyber Trust Mark.	Proibição de senhas padrão, canal de divulgação de vulnerabilidades e período mínimo declarado de suporte a atualizações de segurança.	Condição de acesso ao mercado britânico para exportadores brasileiros de dispositivos conectados, com exigências similares às do CRA europeu.
Cybersecurity Labelling Scheme (CLS)	Singapura (CSA)	Selo voluntário de classificação de segurança para dispositivos IoT de consumo, em níveis crescentes de rigor.	Avaliação por níveis, do básico (ausência de vulnerabilidades conhecidas) ao avançado (testes de penetração e resistência a ataques sofisticados).	Diferencial competitivo para fabricantes brasileiros que buscam o mercado asiático, sem caráter mandatório.
GSMA IoT SAFE / Framework IoTSEF	Global GSMA e IoT Security Foundation	Diretrizes setoriais de segurança para IoT conectado via redes móveis e frameworks de boas práticas de segurança por design.	Recomendação de armazenamento seguro de credenciais (SIM-based security) e adoção de agilidade criptográfica ao longo do ciclo de vida do dispositivo.	Referência voluntária amplamente adotada por operadoras de telecomunicações e fabricantes de módulos IoT que atuam no Brasil.

Anexo 7: A Consolidação da Indústria 5.0 e o Horizonte Ainda Aberto da Indústria 6.0

Já se discute, em periódicos científicos e comunidades técnicas ao redor do mundo, o que viria depois da Indústria 5.0. O termo "Indústria 6.0" começa a aparecer em artigos acadêmicos, ainda sem definição consensual, tratando de enxames de agentes de IA autônomos, controle descentralizado por inteligência artificial e manufatura hiperconectada.

Esse dado, por si só, já deveria soar como um alerta. Parte expressiva da indústria brasileira ainda discute *como sair da terceira revolução industrial rumo à quarta*, enquanto o mundo debate os contornos da sexta. O intervalo entre elas não é uma curiosidade acadêmica. É a medida exata do gap competitivo que este livro busca expor.

Mas antes de olhar para a fronteira ainda indefinida da 6.0, é preciso corrigir uma percepção comum: a de que a Indústria 5.0 nasceu pronta, em um único documento europeu, em um único ano. Não foi assim. A trajetória até sua consolidação institucional levou quase uma década e passou por caminhos conceituais que, à primeira vista, pouco tinham em comum entre si.

Uma Pré-História Dispersa: Seis Fios Independentes (2015 a 2019)

Entre 2015 e 2019, ao menos seis linhas de pensamento distintas usaram o rótulo "5.0" para descrever o que viria depois da manufatura automatizada da Indústria 4.0. Nenhuma delas foi escrita em diálogo direto com as demais. O resultado é revelador: quando ideias parecidas nascem de forma independente, em geografias e disciplinas diferentes, isso costuma indicar que uma necessidade real estava amadurecendo no ambiente, à espera de um nome.

O primeiro fio veio de **Michael Rada**, que lançou o termo em dezembro de 2015 associado à prevenção sistemática de desperdício industrial, batizando sua metodologia de **Industrial Upcycling**. O foco original estava na eliminação de cinco categorias de perda (física, social, urbana, de processo e de tempo), não na automação avançada. Rada reivindica publicamente a paternidade do termo até hoje, e chegou a acusar a Comissão Europeia de ter ignorado seus direitos ao adotar, anos depois, um conceito de conteúdo substancialmente diferente.

O segundo fio partiu do governo japonês, que lançou em 2016 a iniciativa Sociedade 5.0 (**Society 5.0**), de escopo mais amplo que o industrial, propondo a integração entre espaço físico e espaço cibernético para resolver desafios sociais estruturais, como envelhecimento populacional e sustentabilidade urbana.

O terceiro fio é o mais rigoroso do ponto de vista acadêmico. Em janeiro de 2018, os pesquisadores Vural Özdemir e Nezih Hekim publicaram, no periódico revisado por pares OMICS: A Journal of Integrative Biology, um artigo propondo a Indústria 5.0 como resposta aos riscos sistêmicos da hiperconectividade extrema. Os autores argumentavam que redes totalmente integradas, aquelas em que "tudo está conectado a tudo", criam vulnerabilidades novas: colapsos em cascata diante de falhas pontuais, e concentração de poder político em quem controla a rede. A proposta central do artigo era um modelo de "simetria tridimensional" na inovação, que incluísse rotas de saída seguras, equilíbrio entre aceleração e desaceleração tecnológica, e um novo campo de avaliação social da tecnologia. É um texto denso, mais próximo da sociologia da ciência do que da engenharia industrial, mas que hoje conta com centenas de citações acadêmicas e segue sendo referenciado em pesquisas publicadas.

O quarto fio surgiu no jornalismo especializado britânico. Em março de 2018, o portal Raconteur publicou uma entrevista com Phill Cartwright, então presidente executivo do Centre for Modelling and Simulation, descrevendo a Indústria 5.0 como o movimento de personalização em massa e de devolução da responsabilidade de projeto ao ser humano, exemplificado por dispositivos médicos sob medida e pela mudança do modelo de negócio da Rolls-Royce, de venda de motores para serviços orientados por dados de campo em tempo real.

O quinto fio, talvez o mais influente entre os demais na formação da percepção popular do termo, veio de Esben H. Østergaard, cofundador e diretor de tecnologia da Universal Robots. Em artigos publicados em 2018 na revista técnica da International Society of Automation e replicados amplamente na imprensa setorial, Østergaard descreveu a Indústria 5.0 como o retorno do toque humano à manufatura, viabilizado pelos robôs colaborativos, os chamados cobots. Chegou a associar sua proposta, ainda que de forma não filosófica em suas próprias palavras, ao conceito marxista de alienação do trabalho.

O sexto e último fio carrega uma particularidade que merece registro à parte: uma nomenclatura própria, paralela à "Indústria 5.0", mas apontando para a mesma revolução. Em 26 de novembro de 2019, na feira "Smart Production Solutions", em Nuremberg, Aroop Zutshi, então Global President da consultoria americana Frost & Sullivan, apresentou a tese "5IR: The Emergence of an Experience-Driven Manufacturing Economy". A sigla 5IR, abreviação de Fifth Industrial Revolution (Quinta Revolução Industrial), descrevia uma economia manufatureira guiada pela experiência do cliente e pela hipercustomização, batizando o fenômeno de "era da experiência". O conteúdo dessa apresentação só viria a ser publicado formalmente no site da consultoria em março de 2021, poucos dias antes da própria consolidação europeia. É digno de nota que uma consultoria de capital e sede americana tenha cunhado, em solo europeu, uma nomenclatura própria e independente para a quinta revolução industrial, batizando-a com uma sigla que ecoa a estrutura de "4IR" já consagrada por Klaus Schwab para descrever a Indústria 4.0, e reforçando, com vocabulário próprio, o mesmo instinto de personalização que já apareceria também nos fios de Cartwright e Østergaard.

Seis fios, seis nomenclaturas, seis pontos de origem geográfica e institucional distintos, e nenhum ponto de contato direto entre eles até a convergência europeia de 2021. Essa dispersão, aliás, alcança até a própria escolha do nome: "Industry 5.0", "5IR" e "Society 5.0" nomeiam fenômenos parecidos sem que seus autores tenham necessariamente dialogado entre si.

A Consolidação Institucional: A Comissão Europeia (2020 a 2022)

O ponto de inflexão ocorreu quando a Direção-Geral de Pesquisa e Inovação da Comissão Europeia, após dois workshops preparatórios realizados em julho de 2020, publicou em janeiro de 2021 o policy brief que unificaria, sob um único guarda-chuva institucional, boa parte do que os seis fios anteriores já vinham insinuando separadamente.

O documento, assinado por Maija Breque, Lars De Nul e Athanasios Petridis, definiu a Indústria 5.0 em torno de três pilares: sustentabilidade ambiental, centralidade humana e resiliência sistêmica. Um relatório complementar, publicado já em 2020, havia detalhado seis tecnologias habilitadoras específicas: interação personalizada entre humanos e máquinas, biotecnologias industriais, gêmeos digitais e tecnologias de simulação, tecnologias de transmissão e análise de dados, inteligência artificial, e tecnologias de eficiência energética. Em janeiro de 2022, um segundo policy brief do grupo de especialistas ESIR consolidou essa visão como transformadora para o continente.

É interessante notar, à luz da pré-história dispersa que acabamos de reconstruir, o quanto o documento europeu absorveu, ainda que sem reconhecimento formal a cada um deles, elementos que já circulavam havia anos: a centralidade humana ecoa diretamente Østergaard e Cartwright; a resiliência sistêmica dialoga, em espírito, com a preocupação de Özdemir e Hekim sobre hiperconectividade; e a sustentabilidade retoma, ainda que por caminho distinto, a preocupação original de Rada com a eliminação de desperdício.

Por Que a Indústria 5.0 Precisa da Computação Quântica

Os seis pilares habilitadores definidos pela Comissão Europeia compartilham uma exigência comum, que raramente é explicitada nos debates sobre o tema: todos dependem de capacidade computacional, de precisão de sensoriamento e de robótica avançada em escalas que a infraestrutura clássica isolada tem dificuldade de sustentar.

Já discutimos, no Capítulo 4 deste livro, a convergência entre as tecnologias quânticas e os três pilares da Indústria 5.0. A aceleração quântica alimenta a resiliência operacional ao possibilitar simulação de cenários de falha em tempo real. O sensoriamento quântico, apresentado na seção 4.5.1, entrega ao pilar de centralidade humana a precisão de medição necessária para que gêmeos digitais e cobots operem com segurança ao lado de trabalhadores humanos. E a otimização quântica de cadeias de suprimento e de consumo energético dá corpo prático ao pilar de sustentabilidade, para além do discurso.

Esse cruzamento não é coincidência. É a razão pela qual este livro insiste em tratar a computação quântica não como um capítulo isolado de ficção científica corporativa, mas como infraestrutura silenciosa de um movimento industrial que a Europa já formalizou, os Estados Unidos e o Japão já perseguem, e que o Brasil, por meio do Sistema S e dos hubs regionais descritos no Capítulo 4, começa timidamente a acompanhar.

O Horizonte Ainda Não Consolidado: A Indústria 6.0

Se a Indústria 5.0 levou anos de dispersão conceitual até sua consolidação institucional, a Indústria 6.0 está, hoje, precisamente nessa fase de dispersão.

O termo não é novo. Já em 2017, o engenheiro FS Atwell o utilizava, em tom irônico, para criticar o excesso de versionamento apressado da indústria, sugerindo que uma futura "Indústria 6.0" eliminaria por completo qualquer interface entre humano e máquina. Mais recentemente, a literatura acadêmica retomou o termo com seriedade, mas sem consenso. Um levantamento publicado em 2025 na revista científica ScienceDirect define a Indústria 6.0 como manufatura ubíqua, hipercustomizada e voltada a fábricas hiperconectadas. Um artigo de 2024, produzido por pesquisadores do Instituto Skoltech, propõe outra definição, centrada em enxames de robôs heterogêneos orquestrados por inteligência artificial generativa, capazes de conduzir sozinhos todo o ciclo de projeto e fabricação de um produto a partir de uma descrição em linguagem natural. Uma análise bibliométrica do mesmo ano mapeou dezenas de trabalhos acadêmicos sobre o tema, concentrados principalmente na Índia, na China e em alguns países europeus, sem qualquer marco institucional equivalente ao relatório da Comissão Europeia de 2021.

Nenhum órgão governamental ou intergovernamental oficializou, até o fechamento desta obra, uma definição única de Indústria 6.0. Trata-se, portanto, de um campo de pesquisa emergente, não de uma política pública consolidada, e é assim que este anexo o trata: como sinal do que está por vir, não como fato estabelecido.

Para o leitor brasileiro, a lição prática talvez seja a mais valiosa deste anexo inteiro. A distância entre a dispersão conceitual e a consolidação institucional de uma revolução industrial não é curta, mas também não é infinita. Foram mais de 10 anos entre especulações e a efetividade para a 5.0. Se a 6.0 seguir ritmo semelhante, o tempo para as lideranças brasileiras se prepararem, em vez de reagirem, está se esgotando com rapidez.

Esse é, no fundo, o convite silencioso que este anexo faz ao leitor: acompanhar de perto o próximo capítulo da revolução industrial antes que ele, também, se torne consolidação institucional sem aviso prévio.

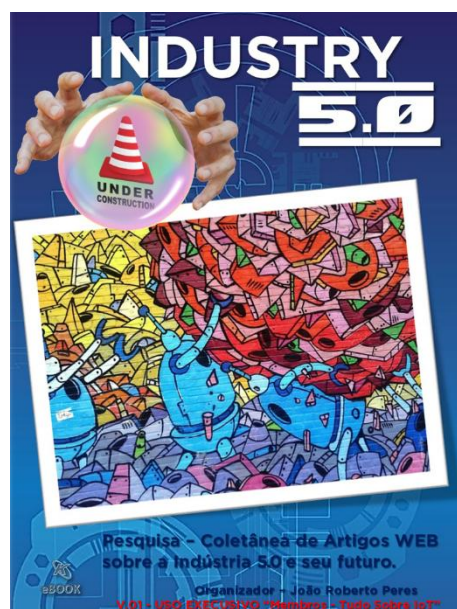
Nota do Autor: Um Registro Pessoal Nesta Trajetória

Ao reconstruir essa pré-história dispersa da Indústria 5.0, cabe um registro pessoal que não é vaidade, mas evidência de método. Este autor acompanha o tema desde antes da consolidação institucional europeia relatada neste anexo.

No início de 2017, eu João Peres, desenvolvi uma pesquisa preliminar sobre Indústria 5.0, que foi apresentada à comunidade WEB “Tudo Sobre IoT”, em formação na época. Essa iniciativa nasceu liderada e promovida por “Thelma Troise” e apoiada outros colaboradores fundadores.

Em 27 de julho de 2018, este autor apresentou à FIESP, no âmbito do Grupo de Estudo de Direito Digital e Compliance, a palestra **"Decolagem para a Quinta Revolução Industrial: Implicações para Sociedade e Manufatura"**, de uso interno da entidade. Ocorreu juntamente, com a versão 02 do compêndio "Industry 5.0: Fundamentos e Guia de Referências", organizado por este autor em julho de 2018, reunindo artigos internacionais que fundamentam a pré-história reconstruída neste anexo, incluindo o próprio artigo de Özdemir e Hekim.

Esse registro não pretende reivindicar paternidade sobre o conceito, na linha do que fez Michael Rada e que este anexo já tratou com a devida cautela. Pretende apenas demonstrar que o interesse por este tema não nasceu da atualidade do debate sobre Indústria 6.0, mas de um acompanhamento de quase uma década, desde antes mesmo da consolidação institucional que a Comissão Europeia formalizaria em 2021.



Solicite ao Autor essas publicações.



Referências Anexo 7

BERG, Andrew; BUFFIE, Edward F.; ZANNA, Luis-Felipe. Should We Fear the Robot Revolution? (The Correct Answer is Yes). IMF Working Paper, WP/18/116. Washington, D.C.: International Monetary Fund, 21 maio 2018.

BREQUE, Maija; DE NUL, Lars; PETRIDIS, Athanasios. Industry 5.0: towards a sustainable, human-centric and resilient European industry. Bruxelas: European Commission, Directorate-General for Research and Innovation, 2021. Disponível em: <https://research-and-innovation.ec.europa.eu>. Acesso em: 30 ago. 2026.

EUROPEAN COMMISSION. Enabling Technologies for Industry 5.0. Bruxelas: Directorate-General for Research and Innovation, 2020.

EUROPEAN COMMISSION, ESIR Expert Group. Industry 5.0, a transformative vision for Europe. Policy Brief. Bruxelas: European Commission, 13 jan. 2022.

ÖZDEMİR, Vural; HEKIM, Nezi. Birth of Industry 5.0: making sense of Big Data with artificial intelligence, "the Internet of Things" and next-generation technology policy. OMICS: A Journal of Integrative Biology, v. 22, n. 1, p. 65-76, jan. 2018. DOI: 10.1089/omi.2017.0194.

RACONTEUR. What will Industry 5.0 mean for manufacturing? Entrevista com Phill Cartwright, por Ben Rossi. Londres: Raconteur, 7 mar. 2018. Disponível em: <https://www.raconteur.net>. Acesso em: 30 ago. 2026.

ØSTERGAARD, Esben H. Bem vindo ao Industry 5.0. InTech Magazine, International Society of Automation, mar./abr. 2018.

RADA, Michael. Industry 5.0 origin. Medium, 26 jul. 2021. Disponível em: <https://michael-rada.medium.com>. Acesso em: 30 ago. 2026.

ATWELL, FS. Yes, the Industry 5.0 is already on the horizon. MachineDesign, Informa USA, 12 set. 2017. Industry 6.0: vision, technical landscape, and opportunities. ScienceDirect, 2025.

LYKOV, Artem et al. Industry 6.0: new generation of industry driven by generative AI and swarm of heterogeneous robots. arXiv, 2024. Disponível em: <https://arxiv.org/abs/2409.10106>. Acesso em: 30 ago. 2026.

Industry 6.0 as an emerging field of research: a systematic and bibliometric analysis. ResearchGate, 2025.

FROST & SULLIVAN. Industry 5.0—Bringing Empowered Humans Back to the Shop Floor. Excerto da apresentação "5IR: The Emergence of an Experience-Driven Manufacturing Economy", de Aroop Zutshi, na feira Smart Production Solutions (SPS), Nuremberg, 26 nov. 2019. Publicação formal: San Antonio, 29 mar. 2021. Disponível em: <https://www.frost.com/growth-opportunity-news/industry-5-0-bringing-empowered-humans-back-to-the-shop-floor/>. Acesso em: 30 ago. 2026.

Sobre o Autor



Dr. João Roberto Peres

Engenheiro Eletricista, Bacharel em Administração de Empresas, Mestre e Doutor em Ciência da Computação, com Ph.D em Segurança Corporativa. Ao longo de mais de três décadas de atuação profissional, construiu trajetória sólida nos campos da tecnologia, segurança cibernética, governança e direito digital. Atuou por mais de 20 anos no mercado financeiro em cargos executivos de Tecnologia da Informação, acumulando experiência direta em ambientes de alta complexidade regulatória e operacional. Paralelamente, desenvolveu carreira acadêmica e consultiva como Professor, Coordenador de Cursos de Educação Continuada e Consultor Especialista da FGV (Fundação Getúlio Vargas), por mais de 20 anos, com atuação nas áreas de

GRC (Governança, Risco e Conformidade), Governança Avançada de TI, Prevenção de Fraudes, Investigação de Corrupção, Forense Digital, Gestão de Riscos, Direito Digital, Segurança de Redes e Data Centers, Gestão de Continuidade de Negócios e Planejamento Estratégico Universitário.

É coautor do Guia de Referência em Segurança Corporativa da Comissão de Crimes de Alta Tecnologia da OAB-SP (2015), autor e editor internacional com registro ISBN e ISNI, com obras registradas na CBL, entre as quais se destacam: "Guia Básico de Compliance", "Manifesto Global de Direitos da IoT", "Compliance: Corrupção e Fraude Empresarial", "Investigação Forense Digital de IoT", "Compliance Urgente", "Guia de Fundamentos da Dark Analytics", "Indústria 5.0", "LGPD Now: Metodologia, Implementação e Soluções", "Privacidade e Conformidade para Desenvolvedores e Usuários de Soluções IoT", "Inteligência Artificial para Profissionais", "Autor Aumentado com IAG Assistente", "Forense Digital: Status Global", "Invisible Core", "Imunidade Digital", "Agentes Invisíveis", "Ameaças Quânticas", "São Paulo Smart City: Rumo à Cidade Ideal" e "Alerta Biométrico", entre diversas produções recentes que se estendem até o presente.

Como destaque João Roberto Peres, atuou como coautor do **Blue Book UE**, um conjunto de roadmaps e desafios de cibersegurança para pesquisadores e formuladores de políticas públicas, publicado em dezembro de 2022 no contexto do projeto piloto CyberSec4Europe (Grant Agreement No. 830929 do Programa Horizon 2020 da União Europeia). A obra, coordenada por Evangelos Markatos (Foundation for Research and Technology - Hellas) e Kai Rannenberg (Goethe-University Frankfurt), reuniu especialistas de instituições europeias e internacionais de ponta para mapear lacunas de pesquisa e propor desafios de longo prazo em áreas críticas da cibersegurança, incluindo aprendizado de máquina, privacidade por design, autenticação além de senhas, segurança de infraestruturas críticas, Internet das Coisas (IoT), execução confiável (Trusted Execution Environments), testes e certificação, ciclo de vida de software seguro, modelagem de ameaças entre outras. Entre os coautores dessa obra está o amigo Dr. Afonso Ferreira, pesquisador sênior do CNRS (Centre National de la Recherche Scientifique) junto ao IRIT (Institut de Recherche en Informatique de Toulouse), com longa trajetória em instituições europeias, incluindo doze anos de atuação na Comissão Europeia, e hoje uma das vozes mais atuantes no debate europeu sobre **tecnologias quânticas, inteligência artificial e cibersegurança**. O trabalho representa uma contribuição significativa ao desenvolvimento de um roteiro estratégico de pesquisa em cibersegurança na Europa, identificando problemas de pesquisa específicos para teses de doutoramento e grandes desafios que demandam colaboração de múltiplas organizações de pesquisa e agências de fomento. Baixar o Blue Book em: (<https://cybersec4europe.eu/wp-content/uploads/2023/02/The-Blue-Book.pdf>)

Atualmente é proprietário de empresas de tecnologia e serviços de segurança cibernética, cofundador de plataformas digitais, em especial sobre Tecnologias Avançadas e Inovadoras (tai.ia.br), membro fundador da comunidade "Tudo sobre IoT", Diretor de grupo Inteligência Artificial do Instituto Juristas, Conselheiro do Fórum Brasileiro de IoT e Conselheiro da Digital Law Academy.

Atua como colaborador da Comissão Especial de Privacidade e Inteligência Artificial da OAB-SP e como Consultor da Comissão de Direito Digital da OAB-SP.



Um diamante pode ser colocado diante de muitos olhos e ainda assim passar despercebido. Não porque lhe falte valor, mas porque nem todos estão dispostos a olhar com atenção.