ESCUDO CUÁNTICO

LA VENTANA CRÍTICA PARA LA SOBERANÍA DIGITAL ANTE LA AMENAZA CRIPTOGRÁFICA EMERGENTE

Por **ADRIANA BARAVALLE**

Palabras Clave:
> Criptografía post-cuántica
> Inteligencia artificial
> Computación cuántica
> Infraestructuras críticas
> Ciberseguridad

Abstract
La convergencia de computación cuántica, inteligencia artificial y criptografía post-cuántica configura un nuevo paradigma geopolítico donde la supremacía tecnológica define ventajas estratégicas decisivas. Este artículo presenta un análisis exhaustivo del estado del arte global, identificando brechas críticas en capacidades nacionales y proponiendo un pensar en un marco de trabajo estratégico para el desarrollo de arquitecturas híbridas de ciberdefensa. La investigación revela que escasas publicaciones abordan la intersección de estos tres dominios críticos, mientras potencias tecnológicas consolidan ventajas asimétricas que comprometen la soberanía digital nacional.

Introducción

La revolución cuántica contemporánea representa una discontinuidad tecnológica de magnitud equivalente al desarrollo de la computación electrónica o la energía nuclear, con implicaciones geopolíticas que trascienden el ámbito puramente científico. La convergencia de tres dominios tecnológicos críticos —computación cuántica, inteligencia artificial y criptografía post-cuántica— configura un nuevo paradigma estratégico donde la supremacía tecnológica define ventajas asimétricas decisivas en el escenario internacional.[1]

La computación cuántica ha alcanzado un punto crítico donde las capacidades criptográficamente relevantes están proyectadas para 2028-2030. IBM Starling promete 100 millones de qubits para 2029, mientras Google Willow ha demostrado corrección de errores escalable. Estas capacidades permitirán descifrar RSA-2048 con aproximadamente 1 millón de

qubits físicos, comprometiendo el 95% de las comunicaciones militares actuales.

China[2] y Rusia lideran programas cuánticos estatales con objetivos militares específicos. Se suman países con capacidad financiera para adquirir esta tecnología desarrollada por los países líderes, programas civiles cuánticos civiles de aplicación dual, grupos de cibercrimen organizado y organizaciones que operan con apoyo de Estados.

Estados Unidos tiene un enfoque híbrido público-privado, con $1.2 mil millones de inversión federal.

La asimetría actual invita a pensar en marcos de cooperación regional en materia de innovación e investigación. Las fuerzas armadas argentinas ya enfrentan amenazas de phishing dirigido, ransomware, y espionaje cibernético. Las capacidades cuánticas futuras representan una escalación de estas amenazas existentes, donde los datos comprometidos hoy podrán ser descifrados retroactivamente, los sistemas de comando y control (C4ISR) actuales necesitan protección prospectiva y las vulnerabilidades de transición crean ventanas de oportunidad para adversarios.

Este artículo pretende iluminar sobre la necesidad apremiante de evaluar el estado actual del conocimiento global en estos campos convergentes, identificar las brechas críticas que comprometen la capacidad nacional de respuesta ante amenazas cuánticas emergentes, y proponer un marco de trabajo estratégico integral para la investigación y el desarrollo de arquitecturas defensivas híbridas. De este modo, la ventana de acción 2025-2027 es crítica para la implementación de criptografía post-cuántica en sistemas críticos, 2027-2029 para el desarrollo de capacidades cuánticas defensivas, y 2029-2032 para la operacionalización de sistemas híbridos cuántico-clásicos.

GRÁFICO 1. QPUS POR PAÍS Y MODALIDAD

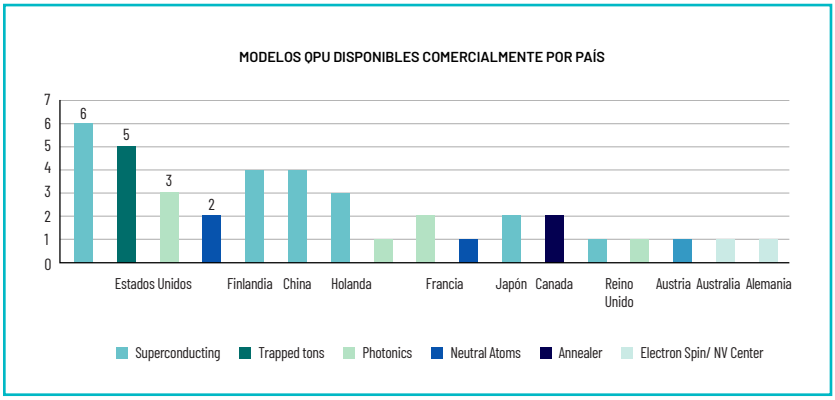
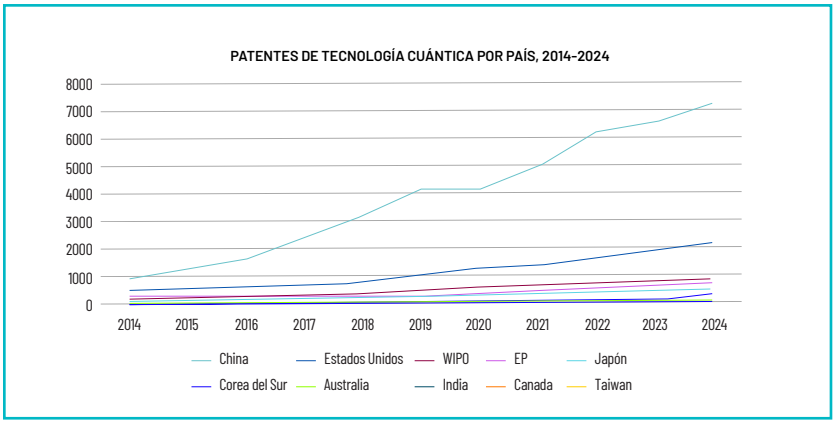


GRÁFICO 2. PATENTES POR PAÍS



Fuente: "The Quantum Index Report 2025"

Ecosistema global de computación cuántica

El ecosistema internacional de *Quantum Processing Units* revela una concentración geográfica crítica de capacidades avanzadas que configura un mapa geopolítico altamente asimétrico. Estados Unidos mantiene el liderazgo tecnológico mediante una combinación estratégica de iniciativas corporativas y gubernamentales, con IBM Quantum qque ha alcanzado los 100 qubits superconductores y Google Quantum AI superando los 200 qubits en sus sistemas más avanzados. Paralelamente, China ha desarrollado una ruta tecnológica alternativa centrada en sistemas fotónicos de escala masiva con Jiuzhang-2.0, que ha demostrado supremacía cuántica fotónica en problemas específicos de muestreo gaussiano.[3]

La aceleración exponencial de los desarrollos cuánticos, particularmente los avances de Google Willow[4] en corrección de errores cuánticos y el anuncio de IBM Starling[5] para 2029, comprimen dramáticamente las proyecciones temporales sobre la

1. https://revistafal.com/la-guerra-cuantica-el-nuevo-frente-de-batalla-geopolitico/
2. Especialización en sistemas fotónicos con Jiuzhang-2.0. Programa estatal centralizado con objetivos militares explícitos y red de comunicación cuántica nacional operativa.
3. https://qir.mit.edu/wp-content/uploads/2025/06/MIT-QIR-2025.pdf
3. https://qir.mit.edu/wp-content/uploads/2025/06/MIT-QIR-2025.pdf
4. https://blog.google/technology/research/google-willow-quantum-chip/
5. https://www.ibm.com/quantum/blog/large-scale-ftq

Fuente: *npj Quantum Inf*

CV

ADRIANA BARAVALLE

Magister en Explotación de Datos y Gestión del Conocimiento y Doctoranda en Ingeniería por la Universidad Austral. Profesora adjunta en Inteligencia Artificial aplicada a Estrategia Militar y Ciberseguridad. Investigadora principal en proyectos de IA aplicada a la defensa, Universidad de la Defensa Nacional. Directora académica synapsIA, Universidad Austral. Autora de múltiples publicaciones en ACM y Springer sobre IA y frameworks de gobernanza para IA en sistemas críticos. Especialista en intersección de tecnologías cuánticas, criptografía e inteligencia artificial para aplicaciones de seguridad nacional.

disponibilidad de computadoras cuánticas criptográficamente relevantes. Esta realidad tecnológica emergente exige una estrategia coordinada que trascienda los enfoques reactivos tradicionales hacia sistemas verdaderamente adaptativos y resilientes.

Esta convergencia tecnológica es particularmente significativa considerando que el algoritmo de Shor puede factorizar números enteros grandes en tiempo polinómico $O((\log N)^3)$, requiriendo aproximadamente 1 millón de qubits físicos para comprometer efectivamente claves RSA de 2048 bits según las estimaciones más recientes de Gidney y colaboradores del equipo de Google AI Quantum[6].

La distribución geográfica de estas capacidades revela patrones estratégicos claramente definidos. Estados Unidos concentra su fortaleza en empresas como IBM, Google, Rigetti e IonQ, y mantiene el liderazgo tanto en arquitecturas de qubits superconductores como en sistemas de iones atrapados. China, por su parte, ha desarrollado expertise específico a través de la Universidad Jiao Tong de Shanghai, focalizándose en sistemas fotónicos que ofrecen ventajas inherentes para aplicaciones de comunicación cuántica[7].

Europa muestra una estrategia de diversificación tecnológica mediante iniciativas como IQM en Finlandia y Oxford Quantum Computing en Reino Unido, mientras que Israel ha consolidado un ecosistema especializado altamente eficiente, con empresas como Quantum Machines y Classiq, que han recibido inversiones superiores a 100 millones de shekels durante 2023 para el establecimiento del Israel Quantum Computing Center.

Panorama de criptografía post-cuántica

El *National Institute of Standards and Technology*[8] ha culminado un proceso de estandarización crítico mediante la selección de cuatro algoritmos fundamentales que definen el nuevo paradigma criptográfico post-cuántico. CRYSTALS-Kyber establece el estándar para encapsulación de claves basada en problemas de retículos, mientras que CRYSTALS-Dilithium y FALCON proporcionan esquemas de firmas digitales cuántico-resistentes con diferentes perfiles de rendimiento y seguridad. SPHINCS+ complementa esta suite como sistema de firmas basado en funciones hash, y ofrece garantías de seguridad conservadoras fundamentadas en primitivas criptográficas bien establecidas.

Sin embargo, la evolución del panorama de amenazas revela la naturaleza dinámica de este campo tecnológico. El ataque de Castryck-Decru[9] contra SIKE en 2022 demostró cómo nuevos desarrollos matemáticos pueden comprometer sistemas considerados seguros e invalidar completamente a un candidato que había superado múltiples rondas de evaluación del proceso NIST. Más preocupante aún, la vulneración de CRYSTALS-Kyber[10] mediante técnicas de inteligencia artificial documentada por Sim,

Park y Han (2022) evidencia la emergencia de amenazas híbridas que combinan vectores cuánticos, clásicos y de aprendizaje automático de maneras anteriormente imprevistas.

Estos desarrollos ilustran la complejidad fundamental de desarrollar sistemas verdaderamente resistentes a amenazas multidimensionales que evolucionan a velocidades exponenciales. La investigación actual sugiere que la seguridad post-cuántica no puede concebirse como un problema estático de selección algorítmica, sino como un desafío dinámico que requiere arquitecturas adaptativas para sistemas militares (centros de operaciones, plataformas navales e infraestructura crítica) capaces de evolucionar proactivamente ante amenazas emergentes.

GRÁFICO 3. BANCO DE PRUEBAS DE REDES CUÁNTICAS EN ESTADOS UNIDOS

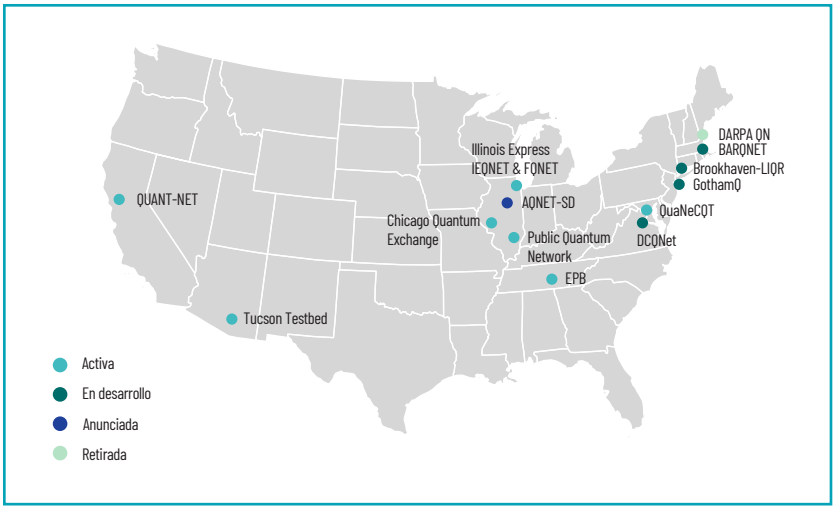
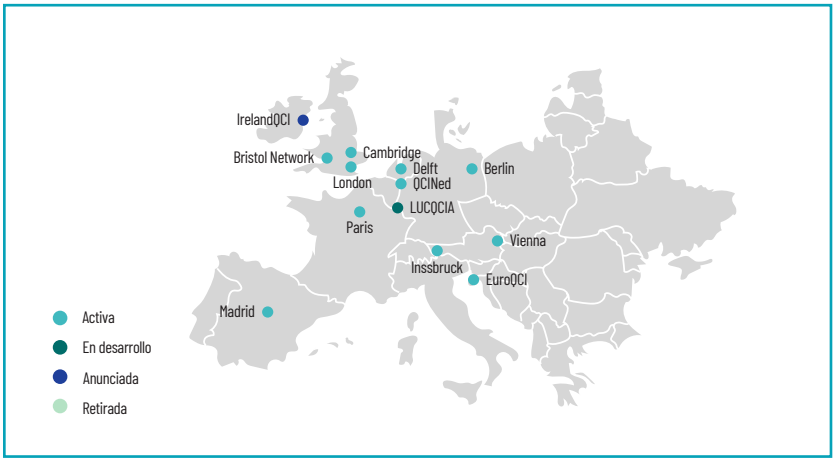


GRÁFICO 4. BANCO DE PRUEBAS DE REDES CUÁNTICAS EN EUROPA



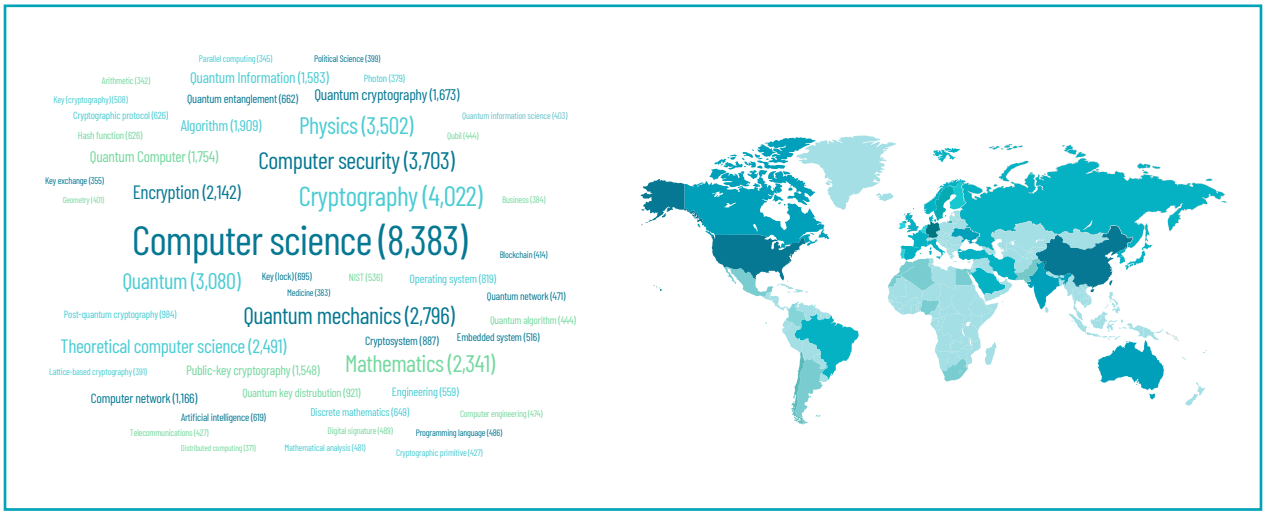
Fuente: "The Quantum Index Report 2025"

Convergencia con inteligencia artificial

La integración sinérgica de inteligencia artificial con computación cuántica representa uno de los desarrollos más significativos en el panorama tecnológico contemporáneo. La incorporación de Deep Neural Networks desarrolladas por Nvidia[11] para algoritmos de decodificación cuántica ha demostrado mejoras sustanciales en corrección de errores, y prácticamente ha validado el *threshold theorem*[12], que durante décadas permaneció como una construcción puramente teórica. Esta convergencia no solo acelera el desarrollo de sistemas cuánticos prácticos, sino que establece las bases para arquitecturas híbridas que aprovechan las fortalezas complementarias de ambos paradigmas computacionales.

Paralelamente, las técnicas de *quantum machine learning*[13] emergen como multiplicadores de fuerza para aplicaciones críticas de detección de amenazas y optimización criptográfica para el descifrado de comunicaciones en tiempo real, navegación, guiado y redes de comunicación resistentes a la interferencia cuántica. Los algoritmos cuánticos variacionales demuestran ventajas prometedoras en problemas de clasificación y reconocimiento de patrones, particularmente en contextos donde la dimensionalidad y complejidad de los datos exceden las capacidades efectivas de métodos clásicos. La investigación reciente sugiere que estos enfoques híbridos pueden proporcionar capacidades defensivas superiores, especialmente en la identificación de anomalías sutiles y la predicción de vectores de ataque emergentes. Este campo emergente presenta una oportunidad estratégica de gran magnitud.

6. https://arxiv.org/abs/2505.15917
7. Chen, HZ., Li, MH., Wang, Y.Z. *et al.* Implementation of carrier-grade quantum communication networks over 10000 km. *npj Quantum Inf* 11, 137 (2025). https://doi.org/10.1038/s41534-025-01089-8. https://www.nature.com/articles/s41534-025-01089-8
8. https://qir.mit.edu/wp-content/uploads/2025/06/MIT-QIR-2025.pdf
9. https://cacm.acm.org/news/nist-post-quantum-cryptography-candidate-cracked/
10. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9786796
11. https://www.nvidia.com/es-la/training/
12. https://quantum.cloud.ibm.com/learning/en/courses/foundations-of-quantum-error-correction/fault-tolerant-quantum-computing/threshold-theorem
13. https://arxiv.org/abs/2502.01146



Las publicaciones especializadas en criptografía post-cuántica hoy alcanzan un número aproximado de 11.317, mientras que son 37 los trabajos enfocados en inteligencia artificial cuántica, lo cual representa un corpus sustancial de conocimiento especializado.

Respecto de patentes la base de conocimiento, Lens.org cuenta con 12.217 relacionadas con criptografía post-cuántica y 1 relacionada con inteligencia artificial cuántica.

Sin embargo, la intersección específica de estos dominios con arquitecturas de ciberdefensa práctica está representada por escasos trabajos de investigación (4 publicaciones y ninguna patente). Esto evidencia un campo emergente con inmensas oportunidades estratégicas para contribuciones pioneras y desarrollo de ventajas competitivas sostenibles[14].

Casos de estudio internacionales

Un caso de estudio internacional exitoso que podría tomarse como referencia de modelo para marcos de trabajo conceptuales para el desarrollo de capacidades cuánticas, es el paradigma israelí, materializado en el *Israel Quantum Computing Center*[15][16], que representa un caso ejemplar de coordinación estratégica efectiva donde se integran sinérgicamente academia, industria y sector defensa. La inversión coordinada superior a 100 millones de shekels (aproximadamente 30 millones de dólares) ha generado un ecosistema altamente eficiente donde instituciones académicas de prestigio como el Technion colaboran estrechamente con empresas especializadas como Classiq y Quantum Machines, de modo que crean ciclos virtuosos de desarrollo tecnológico y transferencia de conocimiento.

La iniciativa europea materializada en el programa Quantum Flagship[17] constituye un modelo complementario de coordinación supranacional que demuestra cómo la agregación estratégica de recursos y expertise puede acelerar el desarrollo de capacidades críticas. El presupuesto de €1,000 millones distribuido a lo largo del período 2018-2028 ha permitido el pooling efectivo de recursos de investigación, la coordinación de estándares técnicos, y el desarrollo de masa crítica en áreas especializadas donde ningún país individual podría alcanzar competitividad global de manera independiente.

Los modelos estadounidense y chino completan el panorama de estrategias nacionales diferenciadas. Estados Unidos ha desarrollado un enfoque híbrido que combina liderazgo corporativo privado con inversión gubernamental estratégica, donde empresas como IBM y Google mantienen autonomía operacional mientras reciben apoyo federal para investigación básica y aplicaciones de seguridad nacional. El programa *National Quantum Initiative Act* de 2018 estableció un marco de coordinación que preserva la competencia comercial mientras asegura el desarrollo de capacidades críticas para defensa nacional.

China, por el contrario, ha implementado un modelo de planificación centralizada que integra objetivos tecnológicos con prioridades geopolíticas explícitas. La concentración de recursos en la Universidad Jiao Tong de Shanghai y el desarrollo acelerado de infraestructura de comunicación cuántica de escala nacional demuestran las ventajas de coordinación estatal directa, aunque con costos potenciales en términos de diversificación

14. Análisis bibliométrico realizado con datos de la plataforma Lens.org de Microsoft https://www.lens.org/
15. https://i-qcc.com/
16. https://www.enlacejudio.com/2022/07/19/israel-establecera-centro-de-computacion-cuantica/
17. https://qt.eu/

tecnológica y capacidad de innovación disruptiva.

Capacidades nacionales

Argentina posee una base de investigación cuántica emergente significativa. El CONICET desarrolla investigación en computación cuántica a través del Instituto de Física La Plata (IFLP). Paralelamente, la CNEA ha establecido proyectos específicos en el Centro Atómico Bariloche para desarrollar procesadores cuánticos con circuitos superconductores, mientras que la División Óptica Cuántica del DEILAP opera desde 2008 como laboratorio pionero en fenómenos ópticos cuánticos, trabajando con pares de fotones entrelazados y sistemas de Distribución Cuántica de Claves.

Las universidades nacionales complementan este ecosistema con iniciativas formativas y de investigación aplicada. La Universidad Nacional de La Plata forma parte activa de los esfuerzos universitarios coordinados con institutos del CONICET, mientras que la Universidad Nacional de Quilmes ha establecido programas específicos de desarrollo en computación cuántica. La Universidad de Buenos Aires ofrece cursos especializados de introducción a la computación cuántica, y Buenos Aires fue sede en julio de 2024 de la 21° Conferencia Internacional *"Quantum Physics and Logic"*, que reunió a más de 100 investigadores internacionales. Estas iniciativas, aunque limitadas en escala comparada con potencias cuánticas, demuestran capacidades existentes que podrían constituir la base para desarrollos más ambiciosos.

Conclusiones

Las capacidades existentes y los casos internacionales descriptos antes ilustran principios fundamentales aplicables al

GRÁFICO 5. EVOLUCIÓN DE TRABAJOS ACADÉMICOS

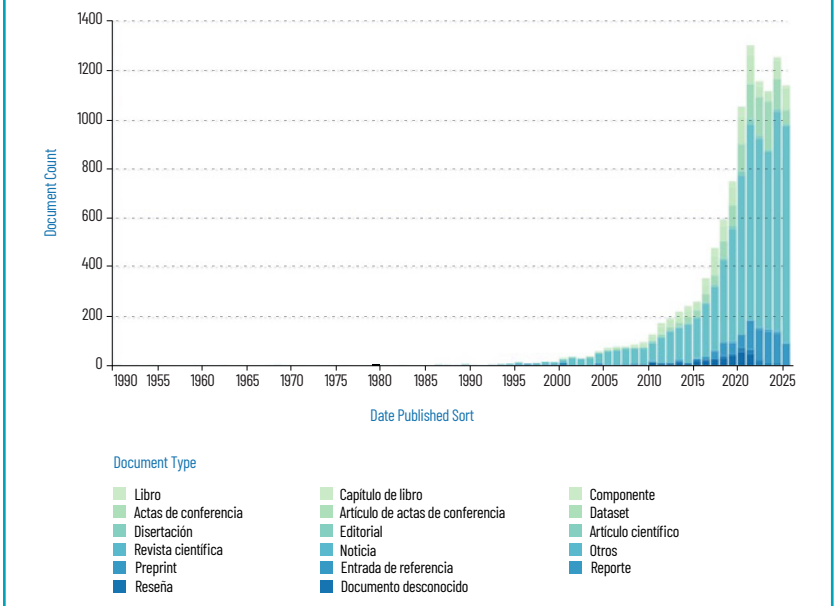
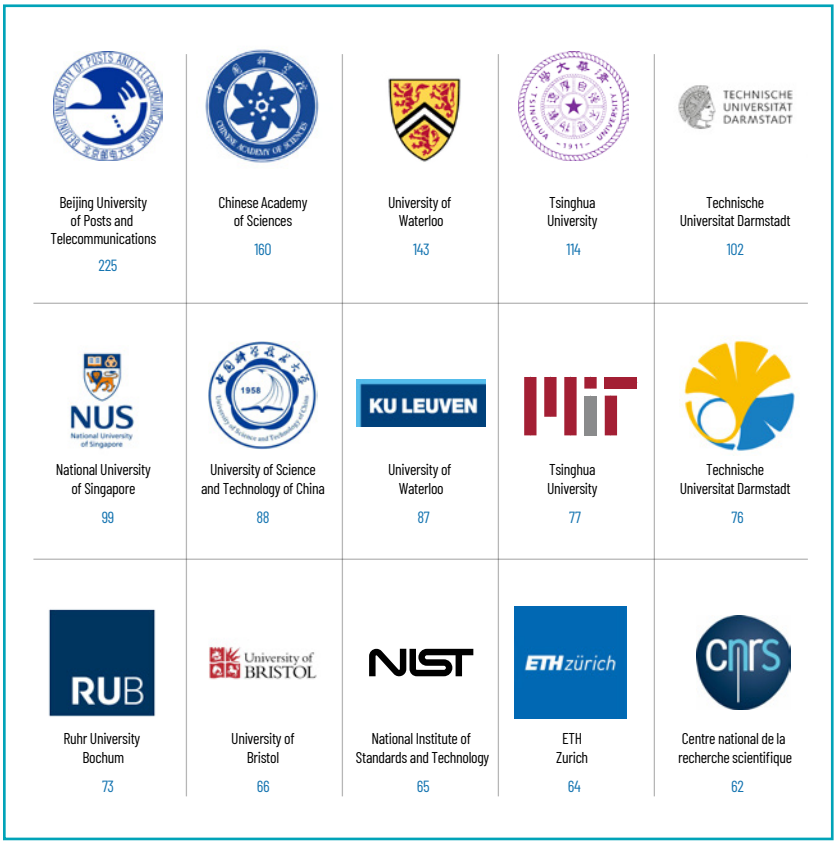


GRÁFICO 5. LOGOS DE LAS PRINCIPALES INSTITUCIONES



Fuente: Lens.org – query= "post-quantum cryptography"

contexto nacional. La coordinación efectiva entre sectores, la concentración estratégica de recursos en áreas de ventaja comparativa, y el desarrollo de marcos institucionales que faciliten la colaboración a largo plazo emergen como factores críticos de éxito. Es particularmente relevante la capacidad demostrada por estos modelos para mantener coherencia estratégica durante períodos gubernamentales múltiples, y asegurar continuidad en inversiones que requieren horizontes temporales extendidos para generar retornos tangibles.

La capacidad de respuesta efectiva ante amenazas cuánticas emergentes puede potenciarse sustancialmente mediante el fomento sistemático de investigación básica en la intersección crítica de inteligencia artificial y criptografía post-cuántica, creando nichos de expertise que complementen las capacidades globales existentes en lugar de replicar enfoques ya consolidados por las potencias dominantes.

Contar con un centro de excelencia en computación cuántica contribuiría a la transferencia de conocimiento entre universidades y el sector defensa en tecnologías emergentes que potencian el desarrollo de capacidades avanzadas.

Retener expertise crítico y acrecentar el número de especialistas en criptografía post-cuántica, a partir de la sinergia entre academia y gobierno sería factible con el diseño de programas de formación especializados, particularmente en la preparación de operadores de ciberdefensa capaces de gestionar sistemas híbridos complejos.

La incorporación sistemática del sector privado emerge como factor multiplicador crítico observado en todos los modelos exitosos. La generación de espacios de colaboración estructurada con la industria, especialmente con el ecosistema de empresas emergentes especializadas, puede aprovechar la dinámica y capacidad de inversión privada para acelerar procesos de desarrollo que tradicionalmente dependen exclusivamente de recursos públicos. Esta sinergia resulta particularmente relevante en el contexto de tecnologías cuánticas, donde los ciclos de innovación requieren tanto la estabilidad de financiamiento a largo plazo como la agilidad de respuesta ante oportunidades técnicas emergentes.

La transformación de capacidades técnicas en ventajas estratégicas requiere la convergencia de múltiples factores que median entre el desarrollo

La capacidad de respuesta efectiva ante amenazas cuánticas emergentes puede potenciarse sustancialmente mediante el fomento sistemático de investigación básica en la intersección crítica de inteligencia artificial y criptografía post-cuántica

científico y su aplicación geopolítica efectiva. Los factores económicos incluyen no solo la disponibilidad de recursos financieros, sino la capacidad de sustentar inversiones a largo plazo, desarrollar cadenas de suministro especializadas, y crear mercados domésticos que justifiquen la escala de producción. Los elementos institucionales abarcan marcos regulatorios apropiados, coordinación inter agencial efectiva, y la capacidad del sistema político para mantener coherencia estratégica durante múltiples ciclos gubernamentales. Los aspectos sociales involucran la formación de masa crítica de recursos humanos especializados, la creación de cultura organizacional que favorezca la innovación, y el desarrollo de redes de confianza entre academia, industria y gobierno que faciliten la transferencia efectiva de conocimiento y la colaboración a largo plazo.

La convergencia de la computación cuántica, inteligencia artificial y criptografía post-cuántica constituye una transformación tecnológica de alcances geopolíticos profundos y que redefine las bases sobre las cuales se construyen las ventajas competitivas entre naciones en el siglo XXI. La intersección de estos dominios críticos presenta una ventana única para el desarrollo de capacidades estratégicas diferenciadas, donde la supremacía no se define únicamente por el volumen de inversión, sino por la capacidad de integrar sinérgicamente estos campos emergentes en arquitecturas defensivas coherentes y adaptativas. De modo tal que permite la detección de amenazas en tiempo real mediante quantum machine learning, la optimización criptográfica adaptativa según amenazas emergentes y desarrollar sistemas de comunicación cuántica inmunes a intercepción clásica. Sin contar con capacidades propias, se acrecienta la asimetría informacional ante adversarios, los sistemas actuales entran en obsolescencia acelerada y se acrecienta la dependencia tecnológica de proveedores extranjeros.

BIBLIOGRAFÍA

Castryck, W. & Decru, T. (2022). An efficient key recovery attack on SIDH. *Advances in Cryptology - EUROCRYPT 2023*.

-

Chen, HZ., Li, MH., Wang, Y.Z. et al. Implementation of carrier-grade quantum communication networks over 10000 km. npj *Quantum* Inf 11, 137 (2025). https://doi.org/10.1038/s41534-025-01089-8. https://www.nature.com/articles/s41534-025-01089-8

-

Gidney, C. & Ekera, M. (2024). How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. *Arxiv Quantum Physics*. Cornell University.

Google Quantum AI and Collaborators. Quantum error correction below the surface code threshold. *Nature 638*, 920–926 (2025). https://doi.org/10.1038/s41586-024-08449-y

-

IBM Research. (2024). Large-scale fault-tolerant quantum computing. *IBM Quantum Blog*. https://www.ibm.com/quantum/blog/large-scale-ftqc

-

National Institute of Standards and Technology. (2024). NIST releases first 3 finalized post-quantum encryption standards. *NIST News*. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

-

Ruane, J., Kiesow, E., Galatsanos, J., Dukatz, C., Blomquist, E., Shukla, P., "The Quantum Index Report 2025", MIT Initiative on the Digital Economy, Massachusetts Institute of Technology, Cambridge, MA, May 2025.

-

Sim, B., Park, A., & Han, D. (2022). Chosen-Ciphertext Clustering Attack on CRYSTALS-KYBER Using the Side-Channel Leakage of Barrett Reduction. IEEE Internet of Things Journal.