BY-NC

—ARTÍCULO—

Ciberseguridad Poscuántica en América Latina: desafíos y estrategias regulatorias

Post-Quantum Cybersecurity in Latin America: challenges and regulatory strategies

Bruno Riquelme

Doctorando en Tecnologías de la Información y Comunicaciones. Magíster en Gestión por Procesos para la Transformación Digital. Magíster en Dirección de Tecnologías de la Información. Licenciado en Tecnología Educativa (UTN). Director de la Maestría Oficial en Dirección de Ciberseguridad en AICAD Business School (España). Director ejecutivo en Simbiosis Digital. baugusto343@gmail.com

Javier Pereyra

Licenciado en Seguridad (UCALP). Director de la Diplomatura en Seguridad Privada (UCALP). Profesor asociado de la materia Seguridad Privada (UCALP).

Recepción: 21/3/2025 | Aprobación: 1/5/2025

Resumen

La inminente llegada de la computación cuántica representa una amenaza sin precedentes para los sistemas criptográficos actuales. Este trabajo analiza la preparación de América Latina frente a este «riesgo cuántico», explorando el estado actual de las regulaciones y estrategias de ciberseguridad poscuántica en la región. Se presenta un panorama global y regional del problema, un marco teórico sobre criptografía poscuántica, y una metodología de análisis comparativo de políticas en varios países latinoamericanos. Mediante estudios de caso detallados (Brasil, México, Argentina, Colombia y Chile) se evalúan los avances y vacíos existentes. El artículo discute los desafíos regulatorios, la necesidad de soberanía tecnológica y las brechas en capacidades, proponiendo estrategias de mitigación. Finalmente, se ofrecen recomendaciones puntuales para fortalecer la ciberseguridad poscuántica en América Latina, enfatizando la urgencia de una acción proactiva y coordinada antes de la llegada de los computadores cuánticos capaces de romper la criptografía actual.

Palabras clave: computación cuántica; criptografía poscuántica; ciberseguridad; regulación; América Latina.

Abstract

The advent of quantum computing poses an unprecedented threat to current cryptographic systems. This paper examines Latin America's preparedness for this "quantum risk" by exploring the current state of post-quantum cybersecurity regulations and strategies in the region. It provides a global and regional context for the problem, a theoretical framework on post-quantum cryptography, and a comparative analytical methodology covering policies in several Latin American countries. Through detailed case studies (Brazil, Mexico, Argentina, Colombia, and Chile), the article evaluates existing progress and gaps. It discusses regulatory challenges, the need for technological sovereignty, and capacity gaps, and proposes mitigation strategies. Finally, it offers concrete recommendations to strengthen post-quantum cybersecurity in Latin America, emphasizing the urgency of proactive and coordinated action before quantum computers capable of breaking current cryptography become a reality.

Keywords: *quantum computing; post-quantum cryptography; cybersecurity; regulation; Latin America.*

1. Introducción

La posibilidad de que un computador cuántico de gran escala pueda romper los algoritmos criptográficos actuales ha encendido las alarmas en la comunidad de ciberseguridad (Mosca, 2015). Los sistemas de cifrado de clave pública (como RSA y ECC) serían vulnerables a ataques cuánticos utilizando algoritmos como el de Shor, y la criptografía simétrica podría debilitarse con aceleraciones cuánticas tipo Grover (Mosca, 2015). Ante este escenario, ha surgido la criptografía poscuántica (PQC, por sus siglas en inglés), que busca desarrollar algoritmos criptográficos resistentes a los ataques de futuros computadores cuánticos (NIST, 2022). A nivel global, Gobiernos y organismos internacionales ya han iniciado la transición hacia estándares criptográficos cuánticamente seguros. Por ejemplo, el Instituto Nacional de Estándares y Tecnología de EE. UU. (NIST) seleccionó en 2022 los primeros algoritmos poscuánticos para estandarización (NIST, 2022), y ha publicado en 2024 estándares finales para reemplazar gradualmente a RSA/ECC. Asimismo, Estados Unidos estableció mediante directivas federales un plan para migrar toda la criptografía gubernamental a algoritmos resistentes a cuántica antes de 2035. Otras potencias, como la Unión Europea, China y Australia, han delineado hojas de ruta nacionales para la adopción de PQC en esta década (GSMA, 2025).

En contraste, América Latina enfrenta este desafío emergente con rezagos en sus marcos normativos de ciberseguridad. Muchas naciones de la región aún están fortaleciendo sus capacidades básicas de ciberseguridad, y pocas han incorporado explícitamente la amenaza cuántica en sus políticas públicas. Un informe del Banco

Mundial indica que América Latina y el Caribe es la región menos preparada en compromisos de ciberseguridad a nivel global, con un puntaje promedio de 10.2/20 en índices internacionales, por debajo de otras regiones (World Bank, 2024). Si bien países como Brasil, México o Argentina han desarrollado estrategias nacionales de ciberseguridad en años recientes, estas raramente mencionan la computación cuántica o la necesidad de renovar la criptografía. No abordar oportunamente esta brecha regulatoria podría dejar expuestos datos sensibles y sistemas críticos cuando lleguen los «Q-day» —el día en que los adversarios dispongan de capacidades cuánticas para comprometer la seguridad actual—.

Este artículo tiene como objetivo analizar los desafíos y estrategias regulatorias de la ciberseguridad poscuántica en América Latina. Para ello, se examina el estado del arte de la criptografía poscuántica y su relevancia (contexto global y regional), se comparan las iniciativas y normativas existentes en distintos países latinoamericanos, y se presentan casos de estudio que ilustran la situación y esfuerzos de la región. Finalmente, se discuten las perspectivas y se proponen recomendaciones concretas para que América Latina fortalezca su postura de seguridad ante la era cuántica. Con ello, se espera contribuir a la concienciación sobre la urgencia de anticipar los riesgos cuánticos y ofrecer lineamientos para una transición ordenada hacia la criptografía poscuántica.

2. Computación cuántica y amenaza criptográfica

La computación cuántica explota principios de la mecánica cuántica (superposición, entrelazamiento) para procesar información de maneras imposibles para la computación clásica. Un computador cuántico suficientemente potente podría ejecutar algoritmos especializados que socavan la base de la criptografía moderna. El ejemplo más conocido es el algoritmo de Shor, que puede factorizar números enteros grandes y calcular logaritmos discretos de forma exponencialmente más rápida que los algoritmos clásicos, quebrando sistemas de clave pública como RSA y ECC (Mosca, 2015). Otro es el algoritmo de Grover, que acelera la búsqueda en espacios no estructurados y reduce a la mitad el esfuerzo necesario para romper por fuerza bruta claves simétricas, obligando a duplicar el tamaño de claves como AES para mantener la seguridad. Si bien los ordenadores cuánticos universales capaces de estas hazañas aún no existen, los avances en investigación sugieren que podrían materializarse en el mediano plazo (una década o dos) (Mosca, 2015). Este riesgo latente ha dado lugar al concepto de *Q-day*, el día en que los adversarios dispondrán de capacidad cuántica suficiente para comprometer los cifrados actuales.

3. Criptografía poscuántica (PQC)

Como respuesta, la criptografía poscuántica se refiere a nuevos esquemas criptográficos diseñados para resistir ataques tanto de computadores clásicos como cuánticos (NIST, 2022). A diferencia de la criptografía cuántica (por ejemplo, distribución cuántica de claves, que requiere canales cuánticos), la PQC consiste en algoritmos ejecutables en computadores tradicionales pero basados en problemas matemáticos que se consideran intratables incluso con capacidades cuánticas. Entre las familias de algoritmos poscuánticos destacan: cifrados basados en retículos algebraicos (*lattice-based*) como Kyber; criptografía de códigos correccionales (*code-based*) como Classic McEliece; funciones hash (*hash-based*) para firmas digitales, como SPHINCS+; esquemas multivariantes; y basados en isogenias de curvas supersingulares, entre otros (GSI, 2024). Estos algoritmos han sido estudiados durante más de una década por la comunidad científica, y han pasado por rigurosos procesos de evaluación.

En 2016, el NIST lanzó un concurso público para estandarizar algoritmos poscuánticos, atrayendo decenas de propuestas académicas. Tras varias rondas de criptoanálisis, en julio de 2022 anunció cuatro algoritmos seleccionados (uno para intercambio de claves y tres para firma digital) como candidatos para estándares poscuánticos (NIST, 2022). En 2023 y 2024 se finalizaron los estándares iniciales, incluyendo a CRYSTALS-Kyber (para cifrado/encapsulamiento de claves) y CRYSTALS-Dilithium (para firmas digitales) como partes centrales del nuevo conjunto criptográfico cuántico-seguro del NIST. La Agencia de Seguridad Nacional de EE. UU. (NSA) actualizó igualmente sus lineamientos de seguridad (Suite CNSA 2.0) para incluir únicamente algoritmos resistentes a cuántica en la protección de información clasificada (NIST, 2022). Todo esto refleja un consenso: la transición a la criptografía poscuántica debe comenzar de inmediato, antes de que la amenaza se concrete (NIST, 2022).

4. Riesgos y urgencia de migración temprana

Aunque las estimaciones varían, expertos advierten que hay una probabilidad significativa de que en la próxima década se logren computadores cuánticos capaces de comprometer cifrados como RSA-2048 (Mosca, 2015). Un peligro crítico es la estrategia de «almacenar ahora, descifrar después»: actores maliciosos pueden interceptar y guardar hoy comunicaciones cifradas (por ejemplo, datos gubernamentales o bancarios), a la espera de un futuro en que puedan descifrarlos con un computador cuántico. Esto significa que incluso datos actualmente seguros podrían quedar expuestos retroactivamente si no se adoptan medidas proactivas. Por tanto, para información que requiera confidencialidad a largo plazo (ej. secretos de Estado, datos personales), la

migración a algoritmos poscuánticos debe anticiparse con varios años de antelación (Mosca, 2015). La transición no es trivial: conlleva identificar y actualizar una amplia infraestructura de seguridad (hardware, software, protocolos) (GSI, 2024), garantizar la interoperabilidad durante el cambio (muchos proponen soluciones híbridas que combinen cifrados clásicos y poscuánticos durante un período) (GSI, 2024), y certificar la fiabilidad de los nuevos algoritmos. Sin embargo, las instituciones que retrasen esta adaptación corren el riesgo de enfrentar una crisis de seguridad apresurada en el futuro. En este contexto, se vuelve fundamental la *criptoagilidad*: la capacidad de los sistemas para sustituir algoritmos criptográficos de manera rápida y eficiente conforme evolucionen las amenazas y los estándares (GSI, 2024).

5. Metodología

Para evaluar la preparación de América Latina ante la amenaza cuántica, este estudio adoptó un enfoque de análisis comparativo-cualitativo de políticas y marcos normativos. En primer lugar, se recopilaron fuentes primarias gubernamentales de cada país: estrategias nacionales de ciberseguridad vigentes, leyes y regulaciones relacionadas con criptografía o infraestructura crítica, comunicados oficiales y proyectos públicos específicos en materia de criptografía poscuántica. Asimismo, se revisaron informes de organismos internacionales (como la Organización de los Estados Americanos [OEA], el Banco Interamericano de Desarrollo [BID] (OAS & BID, 2020) y el Banco Mundial) que proveen indicadores regionales de capacidad de ciberseguridad. Complementariamente, se consideró literatura académica relevante sobre criptografía poscuántica y evaluaciones de riesgo, para enmarcar los hallazgos en las mejores prácticas globales.

La comparación se centró en identificar la presencia (o ausencia) de estrategias explícitas para enfrentar la amenaza cuántica en las políticas nacionales latinoamericanas. Se definieron criterios como: mención de computación cuántica o criptografía poscuántica en documentos estratégicos, existencia de grupos de trabajo o iniciativas oficiales sobre PQC, participación en proyectos internacionales al respecto, y desarrollo de normativas técnicas (estándares, guías) en el sector público. A partir de estos criterios, se elaboró una tabla comparativa sintetizando la situación de varios países. Adicionalmente, se seleccionaron cinco países representativos para un análisis profundo como casos de estudio: Brasil, México, Argentina, Colombia y Chile. La selección se basó en su peso regional y estado de avance diverso en materia de ciberseguridad, buscando cubrir ejemplos desde líderes en iniciativas poscuánticas hasta países con brechas notables. Para cada caso, se examinaron en detalle sus políticas de

ciberseguridad, proyectos puntuales implementados y el grado de coordinación entre el sector público, la academia y la industria.

Finalmente, a partir de la comparación y los estudios de caso, se identificaron desafíos comunes y particulares, lo que alimentó una discusión sobre brechas y oportunidades. Las recomendaciones propuestas emergen del contraste entre la situación actual en la región y las estrategias adoptadas en otras latitudes (por ejemplo, estándares NIST, programas europeos, etc.), adaptadas al contexto latinoamericano.

6. Análisis comparativo de regulaciones en ciberseguridad poscuántica

La revisión de las políticas nacionales revela que, hasta el momento, ningún país latinoamericano ha promulgado una regulación específica dedicada a la criptografía poscuántica. Sin embargo, existen diferencias en el grado de reconocimiento del problema y en las acciones preparatorias emprendidas en cada nación. En la Tabla 1 se presenta un resumen comparativo de la situación en varios países claves de la región.

Tabla 1. Comparativa de estrategias e iniciativas de ciberseguridad post-cuántica en países de América Latina

País	Estrategia/Política Nacional	Iniciativas Poscuánticas Destacadas
Brasil	Estrategia Nacional de Seguridad Cibernética (E-Ciber, 2020) reconoce la computación cuántica como tendencia futura, pero sin plan específico PQC (GSI, 2024). Discusiones oficiales en 2024 sobre directrices PQC (GSI/PR).	Biblioteca criptográfica poscuántica «libharpia» (ABIN, 2022) para elecciones (ABIN, 2022). Estudio del Banco Central sobre algoritmos PQC en pagos (Pix, 2022). Banco Bradesco inició migración criptográfica con IBM (2023).
México	No cuenta con estrategia nacional de ciberseguridad vigente (borrador de 2017 no implementado). No hay políticas públicas explícitas sobre PQC.	Participación en piloto de *blockchain* resistente a cuántica (BID Lab & Tec de Monterrey, 2021) (Allende López *et al*., 2021). Comunidades académicas (UNAM, CINVESTAV) investigan algoritmos cuánticos; concientización creciente en sector financiero.
Argentina	Segunda Estrategia Nacional de Ciberseguridad (2023) menciona	Desarrollo de CryptoComm (ARSAT, 2022), sistema de

	tecnologías emergentes como la computación cuántica (Presidencia de la Nación Argentina, 2023), pero sin medidas concretas sobre PQC.	comunicación cifrada poscuántica (ARSAT, 2022). Proyectos de I+D nacionales en criptografía resistente (*ej.*, colaboración UBA-Defensa).
Colombia	Política Nacional de Confianza y Seguridad Digital (CONPES 3995 de 2020), sin referencias a riesgo cuántico. Estrategia enfocada en fortalecer capacidades básicas de ciberseguridad.	Primer computador cuántico académico de la región instalado (Uniandes, 2023). Discusiones sobre hoja de ruta cuántica (MinCiencias/TIC). Participación en redes internacionales de criptografía cuántica aún incipiente.
Chile	Política Nacional de Ciberseguridad (2017) no contempló PQC. En 2024, comisión experta entregó recomendaciones para integrar tecnologías cuánticas en estrategia nacional (MinCiencia, 2024).	Gobierno impulsa liderazgo en tecnologías cuánticas: >300 proyectos de investigación financiados desde 1983 (MinCiencia, 2024). Planes para infraestructura criptográfica cuántica en sectores como minería y finanzas (en desarrollo).
Otros países	Uruguay, Costa Rica y otros han mejorado capacidades ciber (Uruguay lidera índices regionales (OAS & BID, 2020)), pero no reportan iniciativas PQC específicas a 2024.	En general, la región depende de estándares internacionales (ej. NIST, ISO) para futuras implementaciones. Se observa escasa inversión dedicada a PQC fuera de países mayores.

Fuente: elaboración propia.

Como se aprecia, países como Brasil y Argentina han dado pasos iniciales integrando el tema en discusiones estratégicas o desarrollando prototipos tecnológicos mientras que otros, como México, aún carecen de directrices formales. Brasil destaca por esfuerzos prácticos tempranos: su comunidad de inteligencia desarrolló una biblioteca de cifrado poscuántico (libharpia) aplicada al sistema electoral (ABIN, 2022), y el regulador financiero exploró la viabilidad de algoritmos PQC en la plataforma de pagos instantáneos (Pix) en 2022. Argentina, por su parte, incorporó el desafío cuántico en su estrategia nacional reciente y, a través de la empresa estatal ARSAT, creó una solución de comunicaciones seguras poscuánticas para uso gubernamental (ARSAT, 2022). En cambio, México evidencia un vacío institucional en ciberseguridad desde 2018, aunque su sector académico y algunos proyectos puntuales (ej., *blockchain* cuántico de BID Lab)

muestran consciencia del problema. Chile y Colombia han empezado a considerar la cuestión cuántica en agendas de innovación tecnológica más amplias (por ejemplo, Chile con la Comisión de Tecnologías Cuánticas en 2024, y Colombia mediante iniciativas científicas), pero aún no traducen eso en políticas públicas concretas de ciberseguridad. El resto de la región presenta, en general, rezagos similares: si bien hay avances en marcos legales de protección de datos y ciberseguridad, la dimensión poscuántica permanece mayormente ausente. Esta comparativa sugiere que América Latina, en su conjunto, se encuentra en una etapa temprana de preparación regulatoria frente al riesgo cuántico, con un fuerte potencial de aprendizaje de las experiencias internacionales para cerrar la brecha.

7. Casos de estudio detallados

7.1. Brasil: pionero en iniciativas poscuánticas

Brasil es uno de los países de la región que más tempranamente ha reconocido la amenaza cuántica en materia de seguridad. Su Estrategia Nacional de Seguridad Cibernética (E-Ciber), aprobada por Decreto 10.222/2020, identifica a la computación cuántica entre las tecnologías emergentes que impactarán la seguridad digital (GSI, 2024). Aunque dicha estrategia no detalla acciones específicas de criptografía poscuántica, estableció un marco general que ha permitido impulsar iniciativas posteriores.

En 2022, la Agência Brasileira de Inteligência (ABIN) anunció la librería criptográfica *libharpia*, con soporte para algoritmos poscuánticos, destinada a proteger la integridad del sistema de votación electrónica (ABIN, 2022). Esta biblioteca, presentada en el principal simposio de seguridad informática del país, representa un logro inédito en la región al incorporar cifrado resistente a cuántica en un proceso electoral nacional.

Paralelamente, el Banco Central do Brasil, en colaboración con el grupo Brazil Quantum y empresas tecnológicas, condujo pruebas de concepto sobre el uso de algoritmos poscuánticos en su sistema de pagos electrónico *Pix* (Banco Central do Brasil, 2022). En este estudio se evaluó un esquema de firma digital poscuántica (Picnic) en términos de seguridad y rendimiento, detectando desafíos de rendimiento, pero confirmando la viabilidad a futuro de tales soluciones.

Además de esfuerzos gubernamentales, el sector privado brasileño ha comenzado a movilizarse: en 2023, el banco Bradesco anunció el inicio de su «jornada poscuántica»,

incluyendo capacitación de personal e incorporación a una red de computación cuántica de IBM para prepararse ante el cambio (Alves, 2024).

Estas acciones posicionan a Brasil a la vanguardia regional, aunque aún carece de una regulación específica o un mandato formal de migración a PQC. El enfoque ha sido hasta ahora voluntario y experimental, impulsado por agencias pioneras y empresas innovadoras. No obstante, la experiencia brasileña sirve de referencia valiosa: muestra la importancia de combinar la formulación de estrategias (reconociendo la amenaza cuántica) con proyectos piloto concretos que informen la toma de decisiones regulatorias. Brasil enfrenta el reto de escalar estos esfuerzos aislados a políticas públicas integrales, integrando estándares poscuánticos en la infraestructura gubernamental y definiendo plazos y lineamientos obligatorios para sectores críticos.

7.2. México: Rezago Estratégico y Colaboraciones Internacionales

En contraste con Brasil, México aún no ha desarrollado una estrategia nacional de ciberseguridad vigente, lo cual influye en la ausencia de medidas específicas frente al riesgo cuántico. El último esfuerzo conocido fue un proyecto de estrategia en 2017 que no se concretó en política de Estado, dejando un vacío en la coordinación nacional de ciberseguridad. Como resultado, no existen actualmente lineamientos gubernamentales que aborden la criptografía poscuántica. Sin embargo, México no está ajeno a la temática en otros ámbitos. La academia y el sector privado han dado señales de alerta sobre la amenaza cuántica. Universidades líderes (UNAM, IPN, Tec de Monterrey) han incorporado la computación cuántica y la criptografía poscuántica en agendas de investigación y formación. Notablemente, a través de un laboratorio de innovación del BID, científicos mexicanos del Tec de Monterrey colaboraron en 2021 con Cambridge Quantum Computing para implementar una red *blockchain* resistente a ataques cuánticos (Allende López *et al.,* 2021). Este piloto —parte de la iniciativa LACChain— demostró con éxito transacciones aseguradas con cifrado poscuántico en una plataforma de cadena de bloques, marcando un hito regional. Además, instituciones financieras en México empiezan a interesarse en el tema ante regulaciones internacionales inminentes: la banca, acostumbrada a cumplir estándares globales (PCI-DSS, Basilea), sigue de cerca los desarrollos de NIST y podría adoptar soluciones PQC importadas cuando éstas se consoliden.

No obstante, estos avances aislados, la falta de una estrategia nacional limita la difusión y adopción amplia de la ciberseguridad post-cuántica en México. Actualmente, las iniciativas dependen más de esfuerzos individuales que de una coordinación estatal. Esto conlleva el riesgo de reacciones tardías: si no se establece pronto una hoja de ruta

oficial, México podría tener que realizar cambios apresurados en sus sistemas críticos para alinearse con estándares globales (por ejemplo, cuando proveedores de tecnología actualicen sus productos a algoritmos poscuánticos). En síntesis, México ilustra la situación de varios países latinoamericanos donde la conciencia sobre el problema existe en círculos técnicos, pero aún no se traduce en políticas públicas. La participación en proyectos internacionales sugiere un camino a seguir: aprovechar transferencia de conocimiento y resultados piloto para impulsar la formulación de directrices nacionales que preparen al país para la era poscuántica.

7.3. Argentina: estrategia nacional y desarrollo tecnológico propio

Argentina ha mostrado recientemente una comprensión creciente de la necesidad de abordar amenazas emergentes como la cuántica en su planificación estratégica. En 2023 aprobó su Segunda Estrategia Nacional de Ciberseguridad, la cual por primera vez menciona expresamente a la computación cuántica como parte del entorno tecnológico a considerar (Presidencia de la Nación Argentina, 2023). Si bien la estrategia no detalla acciones concretas en criptografía poscuántica, su inclusión en el texto marca un avance importante de conciencia a nivel político. Más allá del plano estratégico, Argentina destaca por un desarrollo tecnológico propio en la materia: el sistema *CryptoComm* de ARSAT (ARSAT, 2022). Presentado en 2022, CryptoComm es una plataforma de cifrado de alta velocidad para mensajería y archivos, diseñada por criptógrafos locales con métodos post-cuánticos, con el fin de proteger las comunicaciones gubernamentales por muchos años hacia el futuro. Esta iniciativa pública-privada (ARSAT es una empresa estatal de telecomunicaciones) posiciona a Argentina como el primer país de la región en desarrollar internamente una solución de comunicación segura con resiliencia cuántica. Su motivación provino de la amenaza que las potentes computadoras cuánticas representan para la confidencialidad de Internet y las firmas digitales actuales (ARSAT, 2022), y buscó anticiparse a esa amenaza asegurando la soberanía tecnológica en un área crítica (criptografía).

En cuanto al ecosistema normativo, Argentina cuenta con leyes de firma digital y protección de datos que, en el futuro, deberán actualizar sus requisitos criptográficos. Por ejemplo, la infraestructura de firma digital (PKI estatal) eventualmente tendrá que migrar a algoritmos poscuánticos para mantener su robustez. La experiencia de CryptoComm podría servir de base para estándares locales. Sin embargo, por ahora no existen normativas obligatorias sobre PQC. Las recomendaciones a partir de la estrategia 2023 aún deben traducirse en planes de acción concretos. El país enfrenta el desafío de coordinar a sus actores (agencias gubernamentales, fuerzas armadas, sector

académico con tradición en criptografía aplicada) para escalar prototipos como CryptoComm a implementaciones más amplias, y establecer políticas que fomenten la adopción temprana de estándares cuántico-seguros en infraestructura crítica y sector privado. Con su combinación de orientación estratégica y capacidad técnica demostrada, Argentina tiene la oportunidad de jugar un rol líder en la región si consolida estos esfuerzos en los próximos años.

7.4. Colombia: enfoque en capacidades y primera computadora cuántica

Colombia ha avanzado significativamente en políticas digitales en la última década, aunque de forma indirecta respecto a la amenaza cuántica. Su Política Nacional de Seguridad Digital (CONPES 3995/2020) estableció fundamentos para la gestión de riesgos cibernéticos en el gobierno y sectores productivos, pero no abordó la criptografía poscuántica explícitamente. La prioridad de Colombia ha sido fortalecer la ciberseguridad general y la confianza digital; temas emergentes como computación cuántica han sido tratados más en planes de ciencia, tecnología e innovación. En este ámbito, Colombia se convirtió en 2023 en el primer país latinoamericano en instalar un computador cuántico para fines académicos y de investigación, en la Universidad de los Andes. Aunque esta máquina (de pocos cúbits) no representa una amenaza, sí es un indicador de la apuesta colombiana por sumarse a la revolución cuántica. Mediante proyectos como el mencionado y la participación de universidades en redes internacionales, Colombia está construyendo capacidades humanas y técnicas que pueden facilitar a futuro la adopción de criptografía poscuántica.

Desde el punto de vista regulatorio, aún no existen guías específicas en Colombia para la transición criptográfica. Sin embargo, el país sí cuenta con un ecosistema institucional (colaboración entre el Ministerio TIC, MinCiencias y sector privado) capaz de reaccionar con agilidad. Se han llevado a cabo talleres y conferencias (p. ej., *Ecosistema Cuántico en Colombia*, 2022) para sensibilizar a tomadores de decisión sobre los retos de seguridad cuántica. Además, entidades financieras colombianas monitorean de cerca las recomendaciones de seguridad globales; algunas han expresado que actualizarán sus infraestructuras de cifrado conforme surjan estándares sólidos. En resumen, Colombia se encuentra en una posición intermedia: sin políticas poscuánticas dedicadas aún, pero con una base de talento y conciencia que podría traducirse rápidamente en acciones. Una vez que organismos internacionales establezcan lineamientos claros (NIST, ISO), es previsible que Colombia inicie proyectos pilotos en sectores como banca o telecomunicaciones, apoyándose en su creciente comunidad cuántica local. La clave será integrar estos esfuerzos dispersos en una estrategia nacional

coordinada, para no depender exclusivamente de adoptar tecnologías externas sino también aportar desarrollo propio.

7.5. Chile: planificación cuántica y visión de futuro

Chile se destaca por haber encarado de manera proactiva la planificación de las tecnologías cuánticas a nivel país. Si bien su Política Nacional de Ciberseguridad de 2017 no contempló la dimensión cuántica (dado que entonces la prioridad era fortalecer las capacidades básicas), en años recientes Chile ha dado pasos institucionales notables. En 2022 se conformó una Comisión Asesora en Tecnologías Cuánticas, integrada por expertos nacionales, que en 2024 entregó un informe con 15 recomendaciones para que Chile lidere la revolución cuántica (MinCiencia, 2024). Entre estas recomendaciones se incluyeron aspectos de gobernanza y regulación para asegurar la protección cuántica de la información en el futuro. La ministra de Ciencia destacó que en ciberseguridad la información pronto deberá estar protegida por «claves cuánticas imposibles de hackear» (MinCiencia, 2024), reflejando la visión de incorporar soluciones avanzadas como la distribución cuántica de claves (QKD), junto con la criptografía poscuántica tradicional.

Chile ha invertido fuertemente en investigación científica cuántica durante décadas, financiando cientos de proyectos que sentaron las bases en física y computación cuántica (MinCiencia, 2024). Gracias a ello, el país cuenta con un capital humano e infraestructura de I+D que puede traducirse en desarrollos aplicados de ciberseguridad. Por ejemplo, laboratorios en la Universidad de Chile y otros centros investigan algoritmos poscuánticos y protocolos cuánticos de seguridad. En el sector productivo, Chile explora aplicaciones cuánticas en minería, energía y finanzas, reconociendo que la ciberseguridad es transversal a estas iniciativas.

Normativamente, Chile aún no emite regulaciones específicas de PQC, pero el Gobierno ha manifestado intenciones de actualizar su estrategia nacional de ciberseguridad para incorporar las recomendaciones de la Comisión Cuántica. Se espera la creación de un plan de acción que incluya: formación de especialistas en criptografía poscuántica, incentivos para que empresas adopten tempranamente certificados digitales cuántico-seguros, y eventualmente la exigencia de que los sistemas críticos del Estado migren a algoritmos aprobados por estándares internacionales (cuando estos estén disponibles formalmente). Chile muestra así una actitud prospectiva, tratando de adelantarse a la curva tecnológica. El desafío será pasar de la planificación a la ejecución: destinar recursos concretos para implementar pilotos de PQC en agencias gubernamentales, actualizar normativas técnicas (por ejemplo, los requisitos criptográficos de la infraestructura de firma electrónica avanzada) y coordinar con otros

países para el intercambio seguro de información en la era poscuántica. Con voluntad política ya encaminada, Chile podría convertirse en un modelo regional si logra implementar eficazmente su visión de ciberseguridad cuántica.

8. Implementaciones actuales y futuras en la región

El panorama regional de implementaciones poscuánticas es aún incipiente, pero ofrece ejemplos ilustrativos. En el sector público, las experiencias de Brasil (libharpia) y Argentina (CryptoComm) son hitos concretos: ambos son desarrollos propios que se han aplicado en entornos reales (elecciones y comunicaciones gubernamentales, respectivamente), demostrando la factibilidad técnica de la criptografía poscuántica en Latinoamérica. Asimismo, la colaboración internacional ha permitido a países como México y otros probar tecnologías de vanguardia (el piloto de *blockchain* cuántica con apoyo del BID). Estos esfuerzos actuales, aunque aislados, sientan las bases para una adopción más amplia.

En cuanto al sector privado, las instituciones financieras lideran la preparación: bancos globales con presencia regional (por ejemplo, Santander) han conformado equipos dedicados a amenazas cuánticas y participan en foros internacionales para facilitar la migración a PQC (Santander, 2025). Esto implica que, en los próximos años, filiales locales de estos bancos comenzarán a incorporar algoritmos poscuánticos en sus sistemas, aún si las regulaciones nacionales no lo exigen explícitamente. Por otro lado, empresas de seguridad y proveedores de infraestructura en la nube están desarrollando soluciones *quantum-safe* que eventualmente se ofrecerán en el mercado latinoamericano (ej.: servicios de VPN o certificados TLS con cifrado híbrido). La presencia de estas soluciones comerciales impulsará la adopción también en organizaciones más pequeñas.

Mirando al futuro, se anticipa que hacia finales de la década de 2020 surjan estándares internacionales definitivos (ISO/IEC) basados en los algoritmos seleccionados por NIST, lo cual facilitará a los países convertirlos en normativas locales. Para entonces, varios países de la región posiblemente habrán actualizado sus marcos legales: por ejemplo, es previsible que nuevas versiones de leyes de firma digital o lineamientos de infraestructura crítica incluyan la exigencia de algoritmos poscuánticos certificados. Un área de implementación futura clave será la actualización de las infraestructuras de clave pública (PKI) gubernamentales: los certificados digitales usados en e-Gobierno, identificación ciudadana y transacciones electrónicas deberán migrar a algoritmos como CRYSTALS-Dilithium o similares. Asimismo, las redes gubernamentales y militares sensibles podrían incorporar, además de PQC, técnicas de

distribución cuántica de claves (QKD) para lograr niveles adicionales de seguridad basados en las leyes físicas. De cara a estos desarrollos, es importante que la región no solo importe soluciones, sino que también participe en pruebas y pilotajes. Algunos países podrían crear laboratorios de ciberseguridad cuántica para evaluar el rendimiento de nuevos algoritmos en entornos locales (por ejemplo, probar su eficiencia en hardware disponible o condiciones de red regionales).

En síntesis, las implementaciones actuales sirven como demostradores tempranos y las futuras estarán determinadas por la evolución de estándares globales y la preparación que se haga en estos años. La ventana de oportunidad para que América Latina planifique una transición ordenada está abierta ahora, antes de que la presión de un adversario cuántico sea inminente.

9. Discusión y perspectivas

9.1. Retos regulatorios y de implementación

La principal dificultad que enfrentan los países latinoamericanos es anticipar una amenaza que, si bien es altamente probable, aún no se ha concretado. Esto puede restar urgencia política al tema de la criptografía poscuántica frente a problemas de ciberseguridad más inmediatos (como el *ransomware*). Sin embargo, el tiempo de acción preventiva es ahora (Mosca, 2015), cuando se pueden planificar transiciones graduales. Legislativamente, uno de los retos será actualizar marcos normativos (leyes de firmas digitales, esquemas de certificación, estándares bancarios) para incorporar nuevos algoritmos sin generar disrupción. También surge la cuestión de la criptoagilidad: muchas infraestructuras heredadas en la región no fueron diseñadas para una sustitución sencilla de algoritmos criptográficos (GSI, 2024). Los reguladores deberán promover evaluaciones de inventario criptográfico en entidades públicas y privadas, de modo que se identifiquen qué sistemas requieren actualizaciones y con qué prioridad. La coordinación interinstitucional es clave: la transición a PQC involucra a organismos de estandarización, autoridades de certificación, sectores de defensa, banca y telecomunicaciones, entre otros.

9.2. Soberanía tecnológica y colaboración internacional

Un tema transversal es la soberanía tecnológica. Si la región no desarrolla capacidades propias en PQC, dependerá completamente de soluciones importadas (principalmente de Europa, EE. UU. o China). Esto puede generar riesgos de

dependencia estratégica y dificulta auditar a profundidad la seguridad de los sistemas. Iniciativas locales como CryptoComm muestran que Latinoamérica puede innovar en este campo. Fomentar la investigación en criptografía (como la tradición que existe en Brasil o Argentina) e incluir a expertos regionales en los procesos globales de estandarización fortalecería la posición del continente. Al mismo tiempo, la colaboración internacional es indispensable: la amenaza cuántica trasciende fronteras, y alinear esfuerzos con coaliciones globales (ej. el Quantum Safe Financial Forum, del cual Banco Santander es miembro fundador [Santander, 2025]) permite a los países compartir mejores prácticas y recibir asistencia técnica. La OEA, a través de su Comité Interamericano contra el Terrorismo (CICTE) y las iniciativas de ciberseguridad, podría servir como plataforma para impulsar lineamientos regionales sobre PQC, facilitando que países más rezagados adopten políticas basadas en las experiencias de sus vecinos más avanzados.

9.3. Brechas de capacidades y mitigación

Existe una brecha notoria de talento especializado en criptografía poscuántica en la región. Pocos profesionales están familiarizados con los detalles matemáticos y de implementación de estos nuevos algoritmos. Para mitigar esto, se requieren programas de formación específicos y actualización curricular en carreras de seguridad informática y criptografía. Institutos como INCIBE en España han comenzado a crear «aulas poscuánticas» para entrenar expertos, un modelo que podría replicarse en universidades latinoamericanas. En términos de infraestructura, muchos países carecen de laboratorios de pruebas o centros de excelencia en seguridad cuántica. La creación de centros regionales de prueba (quizás auspiciados por el BID) permitiría a las naciones probar equipamiento y software poscuántico en entornos controlados antes de adoptarlos masivamente.

9.4. Estrategias de mitigación

A corto plazo, una recomendación es adoptar un enfoque de *criptografía híbrida*, combinando algoritmos tradicionales con poscuánticos en protocolos críticos (GSI, 2024). Esto brinda protección adicional sin esperar a una migración total, y ya es soportado por estándares como TLS 1.3 en implementaciones recientes. También se recomienda priorizar la protección de los datos de vida larga: información cuyo valor persiste por décadas (por ejemplo, secretos industriales, registros personales) debería cifrarse desde ya con algoritmos cuántico-resistentes o medidas compensatorias, para

frustrar intentos de «guardar ahora, atacar después». En el ámbito regulatorio, una estrategia de mitigación es incluir cláusulas de actualización criptográfica en contratos de tecnología gubernamentales: exigir que proveedores aseguren la disponibilidad de versiones poscuánticas o parches en cuanto los estándares estén listos. Finalmente, promover ejercicios de escenario (simulaciones de un «ataque cuántico») ayudaría a sensibilizar a las altas autoridades sobre el impacto potencial y a afinar planes de contingencia.

En perspectiva, América Latina enfrenta el desafío de ponerse al día rápidamente en ciberseguridad poscuántica para no agravar su brecha frente a regiones desarrolladas. No obstante, también tiene la ventaja de poder aprender de las experiencias y errores de otros, y de alinear su camino con estándares ya consolidados en lugar de improvisar. La ventana de los próximos cinco a diez años será crítica: los países que la aprovechen para prepararse tendrán una transición más suave y estarán mejor posicionados en la economía digital global; aquellos que la desaprovechen se verán forzados a reaccionar bajo presión, con mayores costos y riesgos.

10. Conclusiones y recomendaciones

América Latina se encuentra en una encrucijada ante la inminente era poscuántica. Si bien el riesgo que representan los computadores cuánticos para la ciberseguridad todavía puede percibirse como lejano, las acciones tomadas (o no tomadas) en estos años determinarán la resiliencia futura de la región. El análisis realizado muestra que la preparación es desigual: algunos países han dado pasos proactivos —desarrollando prototipos, incluyendo el tema en estrategias—, mientras otros aún no incorporan la amenaza cuántica en su radar político. No obstante, en todos los casos se evidencia una brecha entre el ritmo acelerado de los estándares internacionales y la capacidad de respuesta local.

Es imperativo que los gobiernos latinoamericanos eleven el tema de la criptografía poscuántica a la agenda estratégica de seguridad nacional. Como recomendaciones clave, se proponen: (1) Elaborar planes nacionales de migración criptográfica: inventariar sistemas críticos, establecer prioridades y cronogramas para adoptar algoritmos post-cuánticos, alineados con las guías de NIST y otros estándares globales. (2) Actualizar marcos normativos: reformar leyes y regulaciones existentes para exigir protección cuántico-segura en sectores sensibles (gobierno, finanzas, salud, infraestructuras críticas) en un plazo razonable, y definir responsabilidades claras de cumplimiento. (3) Fortalecer la criptoagilidad: invertir en modernizar infraestructuras de TI para que soporten cambios ágiles de algoritmos; esto incluye requerir en las

compras públicas que los productos tengan soporte para cifrado configurable y actualizaciones de seguridad de largo plazo. (4) Formación y talento: lanzar iniciativas de capacitación especializadas en seguridad cuántica para técnicos y decisores; incentivar postgrados y proyectos de investigación en criptografía poscuántica con financiamiento estatal y alianzas internacionales. (5) Cooperación regional e internacional: aprovechar organismos como la OEA, BID y ONU para compartir conocimientos, desarrollar ejercicios conjuntos y eventualmente negociar mejores condiciones de acceso a tecnologías cuánticas (por ejemplo, a través de consorcios público-privados regionales). (6) Involucrar al sector privado: establecer grupos de trabajo nacionales con bancos, empresas de telecomunicaciones y sector tecnológico para coordinar pruebas piloto de PQC y establecer estándares sectoriales voluntarios que puedan preceder a la regulación formal.

En conclusión, la ciberseguridad poscuántica no es un lujo futurista, sino una necesidad emergente. La región latinoamericana, con sus limitaciones, ha demostrado capacidad de innovación y adaptación cuando hay visión estratégica. La transición hacia criptografía resistente a cuántica brindará no solo protección frente a amenazas futuras, sino que elevará en general el nivel de seguridad y confianza digital, habilitando una participación más segura en la economía digital global. Dar estos pasos ahora permitirá que América Latina enfrente el advenimiento de la computación cuántica desde una posición de fortaleza y no de vulnerabilidad. El reloj hacia la era poscuántica ya está en marcha: las decisiones que se tomen en el presente definirán la seguridad del mañana.

Referencias

Agência Brasileira de Inteligência (ABIN). (2022, 14 de septiembre). *ABIN lança criptografia com algoritmos pós-quânticos para as eleições*. https://www.gov.br/abin/pt-br/centrais-de-conteudo/noticias/abin-lanca-criptografia-com-algoritmos-pos-quanticos-para-as-eleicoes

Allende López, M., López León, D., Cerón, S., Leal Batista, A., Pareja, A., Da Silva, M., ... & Venegas-Andraca, S. E. (2021). *Quantum-Resistance in Blockchain Networks*. Inter-American Development Bank. https://doi.org/10.18235/0003313

Alves, S. (2024, 16 de abril). *Bradesco conta por que decidiu investir em criptografia pós-quântica*. Época NEGÓCIOS. https://epocanegocios.globo.com/tecnologia/noticia/2024/04/bradesco-conta-por-que-decidiu-investir-em-criptografia-pos-quantica.ghtml

ARSAT. (2022, 29 de junio). *ARSAT desarrolló CryptoComm, un sistema de seguridad criptográfica post-cuántica*. https://www.arsat.com.ar/arsat-desarrollo-cryptocomm-un-sistema-de-seguridad-criptografica-post-cuantica/

Banco Central do Brasil & Brazil Quantum (2022, 11 de mayo). *Estudo analisa uso de criptografia pós-quântica no Pix*. Microsoft News Center Brasil. https://news.microsoft.com/pt-br/com-apoio-da-fenasbac-banco-central-brazil-quantum-e-microsoft-exploram-o-uso-de-criptografia-pos-quantica-para-melhorar-seguranca-do-sistema-pix/

Gabinete de Segurança Institucional (Brasil). (2024). *Computação quântica e criptografia pós-quântica: impactos esperados e necessidades de regulação*. Observatório de Segurança Cibernética, OSIC 15/2024. Brasília, GSI/PR.

GSM Association (GSMA). (2025). *Post Quantum Government Initiatives by Country and Region* (Official Document PQ.03 v1.1). https://www.gsma.com/newsroom/wp-content/uploads/Post-Quantum-Government-Initiatives-by-Country-and-Region-02-Mar-2025-Clean.pdf

Li, S., Chen, Y., Chen, L., Liao, J., Kuang, C., Li, K., ... & Liang, W. (2023). Post-Quantum Security: Opportunities and Challenges. *Sensors, 23*(21), 8744. https://doi.org/10.3390/s23218744

Ministerio de Ciencia, Tecnología e Innovación (Chile). (2024, 27 de septiembre). *Chile quiere liderar la revolución cuántica: Ministra de Ciencia recibe informe de comisión experta con 15 recomendaciones*. https://www.minciencia.gob.cl/noticias/chile-quiere-liderar-la-revolucion-cuantica-ministra-de-ciencia-recibe-informe-de-comision-experta-con-15-recomendaciones/

Mosca, M. (2015). Cybersecurity in an era with quantum computers: will we be ready? *Cryptology ePrint Archive*, Paper 2015/1075. https://eprint.iacr.org/2015/1075

National Institute of Standards and Technology (NIST). (2022, 5 de julio). *NIST Announces First Four Quantum-Resistant Cryptographic Algorithms*. https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms

Organización de los Estados Americanos (OEA) & Banco Interamericano de Desarrollo (BID). (2020). *Ciberseguridad: Riesgos, avances y el camino a seguir en América Latina y el Caribe*. Washington, DC: OEA/BID. https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

Santander. (2025, 12 de febrero). *Santander's commitment to cybersecurity in a post-quantum cryptography world*. https://www.santander.com/en/press-room/press-releases/2025/02/santander-commitment-to-cybersecurity-in-a-post-quantum-cryptography-world

Presidencia de la Nación Argentina. (2023). *Segunda Estrategia Nacional de Ciberseguridad (2023-2027)*. Buenos Aires, Argentina. (Resolución JGM 44/2023).

The World Bank. (2024, 30 de octubre). *De la ficción a la realidad: cómo América Latina se convirtió en el campo de batalla cibernético más crítico del mundo*. Blogs Banco Mundial. https://blogs.worldbank.org/es/latinamerica/seguridad-cibernetica-en-america-latina-y-el-caribe