

EFFECTO DE LA COMPUTACIÓN CUÁNTICA EN LA CRIPTOGRAFÍA ACTUAL Y PREPARACIÓN PARA LA POST- CUÁNTICA: ARTÍCULO DE REVISIÓN

EFFECT OF QUANTUM COMPUTING ON CURRENT CRYPTOGRAPHY AND PREPARATION FOR POST- QUANTUM: REVIEW ARTICLE

Deyler Roca Malale

Universidad San Francisco Xavier

Roca.deyler@usfx.bo

<https://orcid.org/0009-0000-7476-3674>

Bolivia

Recibido: 10 Mayo 2026 / Revisado: 20 Julio 2026 / Aceptado: 31 Julio 2026 / Publicado: 4 Agosto 2026

Resumen

El avance acelerado de la computación cuántica ha despertado un creciente interés en la comunidad científica y tecnológica debido a su potencial para transformar profundamente diversos campos, entre ellos la criptografía. A diferencia de los sistemas computacionales clásicos, los ordenadores cuánticos aprovechan fenómenos como la superposición y el entrelazamiento para realizar cálculos de forma exponencialmente más eficiente. Esta capacidad pone en riesgo los algoritmos criptográficos actuales, especialmente aquellos basados en la factorización de enteros y el logaritmo discreto, pilares de la seguridad digital moderna. Este estudio tiene como objetivo analizar y evaluar los potenciales efectos que la computación cuántica tendría en los sistemas criptográficos vigentes y examinar las principales propuestas de criptografía post-cuántica desarrolladas como respuesta a esta amenaza emergente. Esto se realizó mediante una revisión de artículos publicados en el periodo comprendido entre los años 2020 y 2025, para ello se aplicó el protocolo PRISMA 2020 a 283 artículos consultados en bases de datos como Scopus, ScienceDirect y PubMed, aplicando una estrategia de búsqueda a través de palabras clave y operadores booleanos, descartando duplicados, y aplicando criterios de inclusión y exclusión, hasta seleccionar 15 artículos, que conformaron la muestra final de análisis, con la ayuda de Rayyan y VOSviewer. La revisión evidencia que la transición hacia la criptografía post-cuántica ya constituye un proceso tecnológico en desarrollo, impulsado por la estandarización de algoritmos resistentes como ML-KEM y ML-DSA, la implementación de esquemas criptográficos híbridos y la validación experimental de su desempeño en entornos como redes 5G, infraestructuras SDN, computación en la nube y centros de datos de alta capacidad.

Asimismo, los estudios analizados coinciden en que la principal amenaza no radica únicamente en el incremento de la capacidad de cómputo cuántico, sino también en la necesidad de rediseñar las estrategias de gestión criptográfica, la administración de claves y los mecanismos de migración hacia infraestructuras resilientes. En consecuencia, esta revisión concluye que, aunque la computación cuántica aún no posee la madurez suficiente para comprometer de forma generalizada los sistemas criptográficos actualmente desplegados, la adopción progresiva de soluciones post-cuánticas constituye una prioridad estratégica para preservar la seguridad de la información en el mediano y largo plazo.

Palabras clave: Computación cuántica, Algoritmos cuánticos, Criptografía post-cuántica, qubits, hash.

Abstract

The rapid advancement of quantum computing has sparked growing interest in the scientific and technological community due to its potential to profoundly transform various fields, including cryptography. Unlike classical computing systems, quantum computers leverage phenomena such as superposition and entanglement to perform calculations exponentially more efficiently. This capability puts current cryptographic algorithms at risk, especially those based on integer factorization and discrete logarithms, pillars of modern digital security. This study aims to analyze and verify the potential impact that quantum computing would have on current cryptographic systems and examine the main post-quantum cryptography proposals developed in response to this emerging threat. This was achieved through a review of articles published between 2020 and 2025. The PRISMA 2020 protocol was applied to 283 articles searched in databases such as Scopus, ScienceDirect and PubMed. A search formula was applied using keywords and Boolean operators, discarding duplicates, and applying inclusion and exclusion criteria. The final result was 15 articles, which were analyzed and studied with the help of Rayyan and VOSviewer. The discussion shows that while current cryptographic algorithms have evolved rapidly, obtaining robust cryptographic algorithms that are even highly resilient in terms of encryption and cryptography. The review concludes that, although quantum computing has not yet reached the maturity necessary to breach production systems, early preparation and the development of quantum-resistant cryptographic schemes are essential to guarantee information security in the near future.

Keywords: Quantum computing, Quantum algorithms, Post-quantum, cryptography, qubits, hash.

Introducción

En la era digital actual, la protección de la información se ha convertido en un pilar esencial para el funcionamiento de las sociedades modernas. Desde las comunicaciones personales hasta las infraestructuras críticas de los Estados, una vasta cantidad de datos circula diariamente por redes que dependen de sistemas criptográficos para garantizar la confidencialidad, integridad y autenticidad de la información. Estos sistemas se sustentan, en su mayoría, en supuestos de seguridad ligados a problemas matemáticos difíciles de resolver para los ordenadores clásicos, como la factorización de números primos y el cálculo de logaritmos discretos (Bernstein et al., 2017).

Sin embargo, el desarrollo de la computación cuántica está reconfigurando radicalmente este escenario. A diferencia de la computación tradicional, la computación cuántica emplea principios de la mecánica cuántica, como la superposición y el entrelazamiento, para realizar operaciones con una eficiencia exponencialmente mayor en ciertos tipos de cálculos. Esta capacidad ha demostrado, al menos teóricamente, su potencial para romper los sistemas criptográficos que hoy se consideran seguros (Arute et al., 2019). El conocido algoritmo de Shor, por ejemplo, puede factorizar grandes números primos en un tiempo significativamente menor al requerido por los métodos clásicos, comprometiendo la seguridad de estándares como RSA y ECC (Shor, 1997; Chen et al., 2016).

Este panorama plantea un problema de gran envergadura: ¿qué tan preparada está la infraestructura digital actual frente al avance de la computación cuántica? Y más aún, ¿Cuáles son los caminos tecnológicos y científicos que se están desarrollando para

proteger la información en una era post-cuántica?. La revisión de la literatura evidencia una creciente preocupación, pero también una serie de vacíos teóricos y prácticos. Por un lado, existen múltiples propuestas de algoritmos resistentes a ataques cuánticos, conocidos colectivamente como criptografía post-cuántica; por otro, la estandarización, la evaluación empírica y la adopción práctica de estas tecnologías todavía se encuentran en una fase inicial (National Institute of Standards and Technology [NIST], 2022).

El presente artículo tiene por objetivo analizar de manera crítica y reflexiva el efecto que puede tener la computación cuántica sobre la criptografía actual, con énfasis en la preparación hacia un entorno post-cuántico. Para ello se han revisado artículos publicados en el periodo comprendido entre los años 2020 y 2025, analizando las principales amenazas, los avances en criptografía resistente a la computación cuántica y las iniciativas institucionales en torno a la estandarización. La presente revisión bibliográfica se limita al análisis de investigaciones publicadas entre 2020 y 2025 e indexadas en las bases de datos Scopus, ScienceDirect y PubMed, seleccionadas mediante el protocolo PRISMA 2020 y criterios previamente establecidos de inclusión y exclusión.

En consecuencia, los resultados obtenidos representan el estado del conocimiento derivado únicamente de los estudios que cumplieron dichos criterios metodológicos. Esta revisión no incluye literatura gris, capítulos de libros, actas de congresos, tesis, documentos técnicos ni investigaciones no indexadas, así como tampoco aborda el desarrollo experimental del hardware cuántico o aplicaciones de la computación cuántica ajenas al ámbito de la criptografía y la seguridad de la información. Por ello, las

conclusiones deben interpretarse dentro del alcance de la evidencia científica analizada y no como una evaluación exhaustiva de todas las investigaciones existentes sobre computación cuántica. La variable central de esta revisión es la relación entre capacidad computacional cuántica y robustez de los sistemas criptográficos actuales y futuros. El marco conceptual se apoya en la teoría de la complejidad computacional, la seguridad informática y los modelos de transición tecnológica ante disrupciones emergentes. Todo ello permitió sintetizar el estado actual de la criptografía y comprender el funcionamiento y las posibilidades de aplicación de los principales algoritmos resistentes a la computación cuántica.

Metodología

Para llevar adelante la presente investigación, se realizó una revisión sistemática y pormenorizada de la literatura científica con el propósito de identificar y analizar los estudios más relevantes relacionados con la computación cuántica y cuáles podrían ser los efectos en la criptografía actual y qué estrategias de mitigación pueden adoptarse en la era post-cuántica, para ello, se consultaron bases de datos indexadas como Scopus, PubMed y ScienceDirect. La búsqueda se efectuó utilizando combinaciones de palabras clave como: “Efecto de la computación cuántica”, “criptografía”, “criptografía actual”, “post-cuántica”. Los términos de búsqueda se formularon en inglés con el propósito de ampliar la recuperación de publicaciones internacionales indexadas, empleando operadores booleanos como AND y OR para delimitar los resultados obtenidos en las búsquedas.

El rango temporal considerado comprendió los años 2020 a 2025. La búsqueda inicial permitió identificar 283 artículos,

posteriormente se establecieron como criterios de inclusión, artículos originales de investigación, en idioma inglés y solo artículos de acceso abierto. Se excluyeron artículos de revisión, conferencias, capítulos de libro, libros y duplicados, así como áreas temáticas como física y astronomía, ciencias de la decisión y materiales. Posteriormente, los artículos fueron exportados al software Rayyan, el cual facilitó el proceso de cribado y la identificación de 46 artículos duplicados, que fueron eliminados. Finalmente, se seleccionaron para el análisis completo 15 artículos que cumplieran los criterios de inclusión y abordaban directamente la temática del estudio de este artículo de revisión.

Para el presente artículo, se adoptó el protocolo PRISMA 2020 para estructurar el proceso de revisión sistemática, el cual permitió visualizar de forma clara y transparente el flujo de identificación, cribado, elegibilidad e inclusión de los artículos (Haddaway et al., 2022). La figura correspondiente al diagrama de flujo PRISMA 2020 (Figura 1) resume cada etapa del proceso, indicando el número de artículos identificados, los duplicados eliminados y los criterios de inclusión y exclusión aplicados para la selección final.

Complementariamente, se utilizó el software VOSviewer para realizar un análisis bibliométrico de los artículos incluidos, construyendo mapas de coocurrencia de palabras clave y redes de coautoría, con el objetivo de visualizar de manera más clara y precisa las tendencias temáticas predominantes con respecto al tema investigado y las colaboraciones académicas más significativas dentro del campo estudiado.

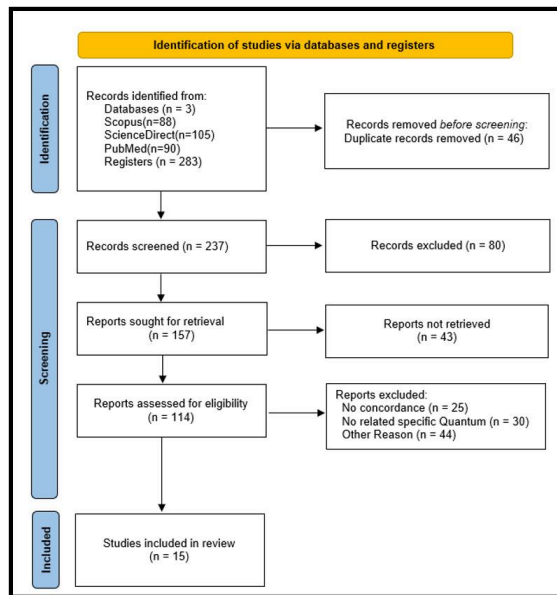


Figura 1. Diagrama de flujo PRISMA 2020.

Nota. Adaptado de McGuinness, L. A. (2022).PRISMA2020

Desarrollo y resultados

En la Tabla 1, se presenta un resumen estructurado de los 15 artículos científicos seleccionados para este estudio. En ella se detallan el título, los autores, el resultado principal, el año de publicación y el DOI.

Esta recopilación permite observar de forma comparativa la diversidad de enfoques, estudios, tendencias de los algoritmos criptográficos y distintas propuestas de soluciones criptográficas para la era pos-cuántica.

Tabla 1. Artículos incluidos en la investigación

No	Título	Autores	Resultado	Año	DOI
1	Understanding instance hardness for optimisation algorithms: Methodologies, open challenges and post-quantum implications	Kate Smith-Miles	El artículo se centra posteriormente en los algoritmos cuánticos para la optimización y argumenta que las lecciones clave aprendidas sobre la prueba de algoritmos de optimización en las últimas décadas son muy relevantes para los esfuerzos actuales por explorar la ventaja cuántica para la optimización.	2025	https://doi.org/10.1016/j.apm.2025.115965
2	Hybrid Quantum-Safe integration of TLS in SDN networks	Jaime S. Buruaga a,*, Ruben B. Méndez a, Juan P. Brito b, Vicente Martin	En este trabajo, se ha seleccionado la Seguridad de la Capa de Transporte (TLS), uno de los protocolos más utilizados, como base para hibridar la criptografía clásica, cuántica y poscuántica de forma que se adapte a su amplia adopción en las Redes Definidas por Software (SDN) el paradigma de red más flexible utilizado para implementar redes cuántico-clásicas integradas.	2025	https://doi.org/10.1016/j.comnet.2025.111355
3	Review of Distributed Quantum Computing: From single QPU to High Performance Quantum Computing	David Barral A , F. Javier Cardama B , Guillermo Díaz Camacho A, Daniel Fáilde A.	Este artículo presenta un estudio exhaustivo del estado actual del arte en el campo de la computación cuántica distribuida, explorando sus principios fundamentales, el panorama de logros, los desafíos y las prometedoras direcciones para futuras investigaciones.	2025	https://doi.org/10.1016/j.cosrev.2025.100747
4	An approach for automated generation of quantum computing models using deep learning.	Niyazi Furkan Bar ,* Mehmet Karakose	El estudio propone un enfoque basado en la generación automática de circuitos y códigos cuánticos mediante aprendizaje profundo.	2025	https://doi.org/10.1016/j.asej.2025.103327
5	Post-quantum cryptography Algorithm's standardization and performance analysis	Manish Kumar	Este artículo analiza en detalle el esfuerzo global para el diseño, desarrollo y estandarización de diversos algoritmos de criptografía de seguridad cuántica, junto con el análisis del rendimiento de algunos de los posibles algoritmos de seguridad cuántica. El objetivo del artículo es analizar la viabilidad de diversos algoritmos de criptografía cuántica segura.	2022	https://doi.org/10.1016/j.array.2022.100242

No	Título	Autores	Resultado	Año	DOI
6	Investigating Quantum-Resilient Security Mechanisms for Flying Ad-Hoc Networks (FANETs)	Abdulnasser AbdulJabbar Abbood, Mahmood A. Al-Shareeda 1, Faris K. AL-Shammri 2, Zainab marid Alzamili 3*, Mohammed Amin Almaiah 5, Rommel AlAli 6*	El estudio analiza algoritmos clásicos y esquemas post-cuántico actuales para FANET, incluyendo soluciones criptográficas lo suficientemente ligeras para entornos con recursos limitados. Los resultados numéricos del experimento muestran que, si bien la criptografía basada en celosía implica un riesgo mínimo de infracciones, su consumo de energía es un 25 % mayor que el de otros sistemas y su tiempo de procesamiento un 30 % más lento. Por el contrario, la criptografía polinómica multivariante es mejor en métricas como el consumo de electricidad: solo consume un 10 % más de energía y necesita un 15 % más de ciclos de CPU para el procesamiento. La introducción de algoritmos y arquitecturas post-cuántico resultó en una reducción del 5-10 % en el rendimiento de la red y un aumento de la latencia del 20 % en algunos escenarios.	2025	https://doi.org/10.18196/jrc.v6i1.25351
7	Quantum Assisted Blockchain Security Model Using Artificial Intelligence to Reduce Quantum Attacks	Ammar AbdRaba Sakran 1,*, Ruwaida Mohammed Yas2, Ali Fadhil Rashid 3, Massila Kamalrudin 4, Mustafa Musa 5	En esta investigación se ha propuesto un modelo mejorado de seguridad de blockchain asistido por cuántica mediante la técnica de inteligencia artificial (EQ-BSM-AI). Este modelo valida los criptosistemas y las tecnologías blockchain para determinar su vulnerabilidad a ataques cuánticos.	2025	https://doi.org/10.54216/FPA.180210
8	Generic Quantum Blockchain-Envisioned Security Framework for IoT Environment: Architecture, Security Benefits and Future Research	Mohammad Wazid 1 Ashok Kumar Das and Oungho Park 2,3 4 (member, iee)	En este artículo, se propone un marco de seguridad genérico, basado en blockchain cuántico, para un entorno del Internet de las Cosas (IoT). A continuación, se analiza algunas posibles aplicaciones del marco propuesto. También se destaca las ventajas de seguridad de los sistemas basados en criptografía cuántica. Se explica el funcionamiento de blockchain, sus aplicaciones, tipos de blockchain, su estructura, la estructura de blockchain en una blockchain clásica y la estructura de un bloque en un contexto de blockchain cuántico.	2024	https://doi.org/10.1109/OJCS.2024.3397307
9	Post-Quantum Key Exchange and Subscriber Identity Encryption in 5G Using ML-KEM (Kyber)	Kaiser Khan *, Sourav Purification and Sang-Yoon hang	En este artículo, se estudia la incorporación de los cifrados post-cuánticos en el cálculo de SUCI tanto en el equipo del usuario como en la red central, lo que implica el intercambio de claves compartidas y el uso posterior de la clave resultante para el cifrado del ID. Se experimenta en diferentes plataformas de hardware para analizar el intercambio de claves post-cuántico y el cifrado utilizando CRYSTALS-Kyber estandarizado por el NIST (que ahora se denomina ML-KEM después de la selección de estandarización por parte del NIST).	2025	https://doi.org/10.3390/info16070617
10	The Impact of Quantum Computing on Cryptographic Security Protocols	Mrs. Swati Dixit 1, Dr. Ujwal amesh Shirode ,Dr. Yogita D. Bhise 2 ,Santoshkumar Vaman Chobe 3 , Swati Nikam 4 5	Este breve resumen analiza los importantes efectos que la computación cuántica tendrá en la seguridad de la criptografía. Examina las vulnerabilidades de seguridad que crean los algoritmos cuánticos y destaca la importancia de encontrar soluciones para la criptografía post-cuántica (CPQ). La CPQ busca crear programas que no puedan ser descifrados por ataques cuánticos. Esto garantizará que las interacciones digitales sigan siendo privadas, seguras y reales en un mundo impulsado por computadoras cuánticas. Además, la transición al post-cuántico conlleva numerosos problemas, como la implementación de algoritmos, la garantía de que sean uniformes y la adaptación a entornos tecnológicos muy diversos.	2024	https://doi.org/10.52783/anvi.v27.1419
11	Practical Implementation of Post-Quantum Cryptography for Secure Wireless Communication	Babatunde Ojetunde 1, *, Takuya Kurihara 1,1., Kazuto Yano, Toshikazu Sakano 1 and Hiroyuki Yokoyama 2	Este artículo presenta un nuevo marco para protocolos de cifrado de clave pública (PKE) post-cuántico independientes y post-cuántico-AES (Estándar de Cifrado Avanzado). Con base en resultados previos, nos centramos en la seguridad de aplicaciones como la transferencia de archivos, la transmisión de vídeo y la comunicación por chat mediante protocolos mejorados basados en post-cuántico.	2025	https://doi.org/10.3390/network5020020
12	Quantum-computing-and-the-law-navigating-the-legal-implications-of-a-quantum-leap	Kasim Balarabe	Este artículo investiga las principales implicaciones legales de la computación cuántica, centrándose en la propiedad intelectual, la seguridad de los datos, la regulación y las consideraciones éticas. Las características únicas de los algoritmos y el hardware cuánticos plantean desafíos significativos para el sistema de patentes actual, lo que requiere un marco claro y consistente para proteger las innovaciones cuánticas y fomentar la colaboración.	2025	https://doi.org/10.1017/err.2025.8

No	Título	Autores	Resultado	Año	DOI
13	In-line rate encrypted links using pre-shared post-quantum keys and DPUs	Abraham Cano Aguilera 1,2*, Carlos Rubio Garcia 1, Daniel Lawo 1,2, José Luis Imaña 3, Idelfonso Tafur Monroy 1 & Juan José Vegas Olmos 2	Este trabajo tiene como objetivo ayudar con la transición a esquemas criptográficos resistentes a la cuántica mediante la provisión de una comparación experimental exhaustiva del rendimiento de los cuatro algoritmos seleccionados por el Instituto Nacional de Estándares y Tecnología (NIST) para la estandarización cuando se implementan en una unidad de procesamiento de datos (DPU). Los experimentos se llevan a cabo a velocidad de línea, lo que demuestra por primera vez el funcionamiento a casi 100 Gbit/s y, por tanto, la idoneidad para entornos de centros de datos de alta capacidad.	2024	https://dx.doi.org/10.1038/s41598-024-71861-x
14	Post-quantum cryptography and the quantum future of cybersecurity	Yi-Kai Liu 1, Dustin Moody	Este artículo revisa el estado actual de los esfuerzos para desarrollar e implementar criptografía post-cuántica en Internet. Luego sugerimos formas específicas en las que se podrían utilizar las tecnologías cuánticas para mejorar la ciberseguridad en el futuro cercano y más allá. Nos centramos en dos objetivos: proteger las claves secretas que se utilizan en la criptografía clásica y garantizar la confiabilidad de los cálculos cuánticos.	2024	https://dx.doi.org/10.1103/physrevapplied.21.040501
15	A compact public key encryption with equality test for lattice in cloud computing	Junfei He 1 1, Qing Ye, Zhichao Yang , Shixiong Wang 2 & Jiasheng Wang 1	En este artículo se propone un esquema PKEET compacto. El nuevo esquema no cifra inmediatamente el valor hash del texto simple, sino que lo incorpora a la trampa de prueba. El estudio demuestra que una nueva construcción es unidireccional y segura según el modelo de seguridad cuántica. Con esos esfuerzos, nuestro esquema puede resistir los ataques de texto cifrado elegidos siempre que se cumpla el supuesto de aprendizaje con errores (LWE). Además, evaluamos el rendimiento del nuevo esquema y descubrimos que solo cuesta aproximadamente la mitad del espacio de almacenamiento en comparación con los esquemas anteriores.	2021	https://dx.doi.org/10.1038/s41598-025-12018-2

Las Figuras 2 y 3 muestran los resultados del análisis bibliométrico realizado con el software VOSviewer v1.6.20. La Figura 2 destaca las palabras clave más frecuentes en la literatura revisada, revelando los principales enfoques temáticos sobre el efecto de la computación

cuántica en los algoritmos criptográficos. La Figura 3 representa la red de coautoría, ilustrando las colaboraciones entre los autores más influyentes del campo. La Figura 4 representa el mapa de calor de concurrencia de palabras clave, con más relevancia.

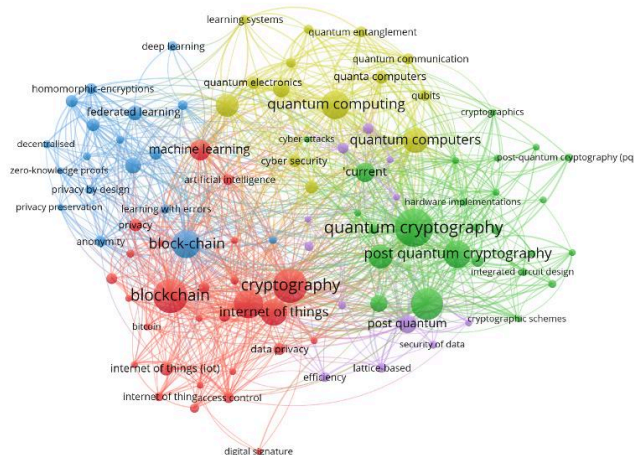


Figura 2. Red de concurrencia de palabras clave.

Nota. Elaboración propia mediante VOSviewer.

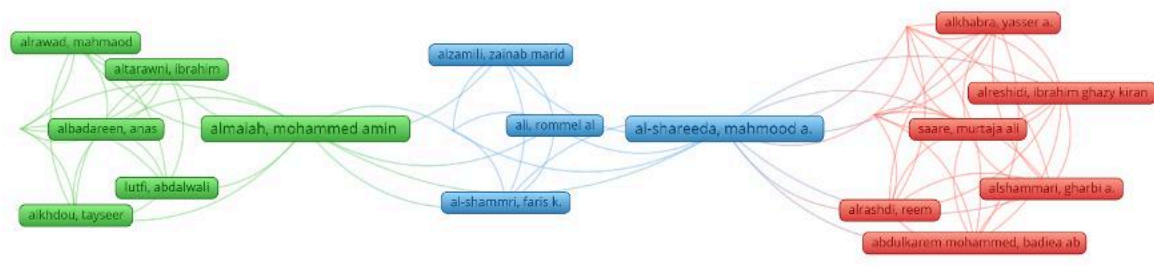


Figura 3. Contribuciones realizadas entre las redes de coautores.

Nota. Elaboración propia mediante VOSviewer.

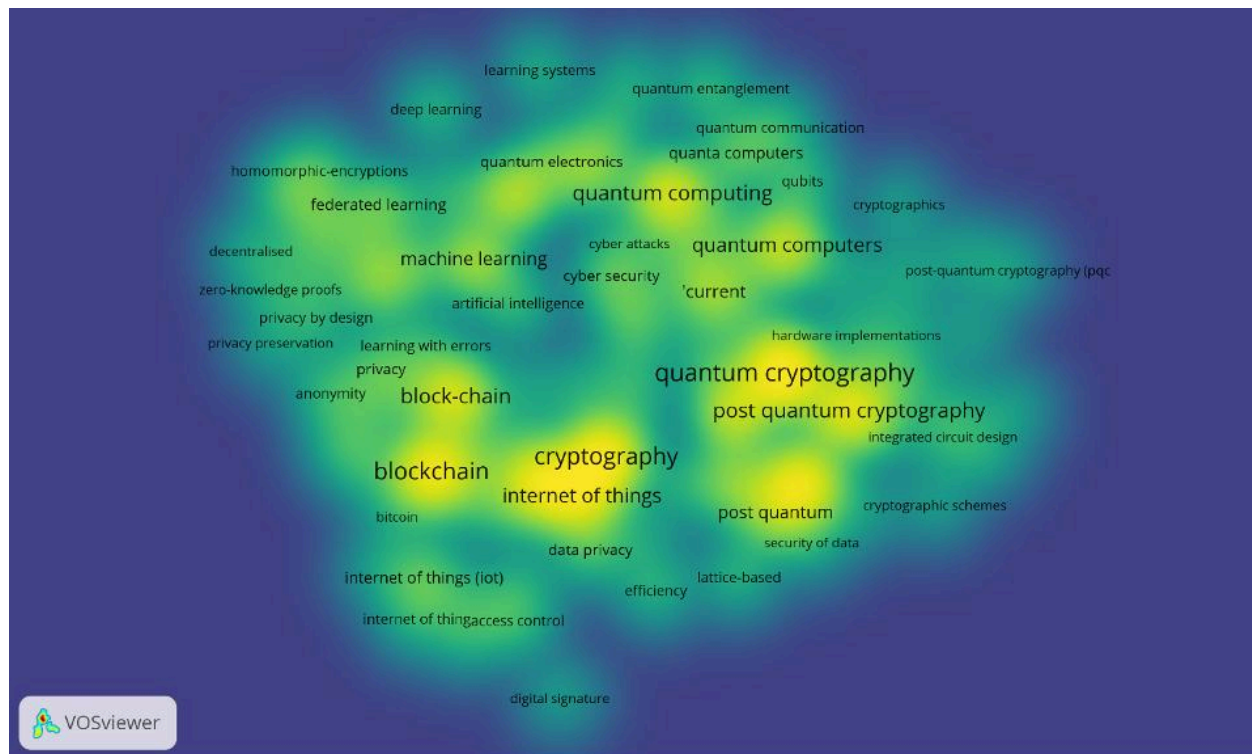


Figura 4. Mapa de calor de concurrencia de palabras clave, con más relevancia.

Nota. Elaboración propia mediante VOSviewer.

Discusión

Esta revisión sistemática, realizada conforme a la metodología PRISMA 2020 y basada en el análisis de 15 estudios, evidencia avances significativos en el desarrollo de la criptografía moderna, aunque también pone de manifiesto las debilidades de los algoritmos criptográficos convencionales frente al avance de la computación cuántica.

En este contexto, los estudios sobre TLS/SDN, VPN/IPsec y redes 5G muestran que la hibridación constituye una estrategia viable para mantener la compatibilidad con la infraestructura existente durante la transición hacia la criptografía post-cuántica, al tiempo que mitiga el riesgo asociado al escenario recolectar ahora y descifrar después (*harvest now, decrypt later*). Jaime S. Buruaga, et al. (2025). La evidencia se presenta en diferentes niveles de análisis.

En la capa de redes y seguridad TLS, las implementaciones de TLS poscuántico, basadas en integraciones PQ-TLS con ML-KEM optimizado mediante instrucciones AVX-512, permiten aumentar el rendimiento de los procesos de negociación criptográfica (*handshakes*) y acercar su desempeño al observado en TLS 1.3 clásico, lo que respalda despliegues a gran escala en entornos operativos extremos.

La propuesta de TLS híbrido en dominios programables mantiene control fino sobre qué flujos usan suites post-cuánticas y cuáles quedan en clásico, útil para migraciones por etapas (*"migración gradual"*). Diversos estudios experimentales muestran mejor tiempo y menor energía en el UE respecto a X25519/secp256r1, pese al aumento de tamaño de claves. Estos resultados sugieren que *"la idea de que la criptografía post-cuántica es necesariamente más lenta"* en todos los casos.

En redes y enlaces troncales, el cuello de botella puede mitigarse mediante la aceleración del procesamiento con unidades de procesamiento de datos (DPU), permitiendo alcanzar velocidades de cifrado de hasta 100 Gbit/s con claves post-cuánticas precompartidas, sin afectar significativamente la latencia, siempre que el diseño y la rotación de las claves sean adecuados. Estos hallazgos evidencian la utilidad de esta estrategia en entornos con elevados requerimientos de procesamiento, como los Centros de Operaciones de Seguridad (SOC).

Dirección estratégica NIST: ML-KEM/ML-DSA y futuro cuántico. El mapeo de NIST (Moody & Liu. 2024) sostiene el plan de estandarización (FIPS 203/204/205) dibuja un horizonte donde la PQC convive con tecnologías cuánticas (p.ej., QKD, RNGs cuánticos) para blindar llaves y verificar cómputos. Esto toma la noción de que paradigma, no es solo cambiar algoritmos, es rediseñar confianza y generación de entropía.

Los hallazgos de fondo que enriquecen o refuerzan los algoritmos criptográficos: FANETs / Mahmood A. Al-Shareeda (2025), redes aéreas y algoritmos resistentes a la computación cuántica para asignación de trayectorias demuestran que la criptografía post-cuántica (PQC) puede operar eficazmente bajo restricciones severas de energía, ancho de banda y tamaño de mensaje. Esto consolida la viabilidad operativa y la robustez del modelo en escenarios tácticos post-cuánticos.

Los avances en los esquemas de cifrado de clave pública con prueba de igualdad (PKEET) basados en retículos evidencian mejoras en la eficiencia del almacenamiento y mantienen un nivel adecuado de seguridad frente a ataques cuánticos. Estas características amplían su potencial de aplicación en entornos de computación en la nube, al facilitar la

realización de búsquedas seguras y tareas de análisis forense sobre información cifrada, tal como señalan He et al. (2025).

La revisión general de los artículos evidencia que la transición hacia la criptografía post-cuántica ya no es un ejercicio teórico, sino un proceso en marcha que combina avances técnicos y estrategias de despliegue pragmáticas. Se observa un consenso en que la hibridación entre algoritmos clásicos y post-cuánticos es la vía más segura para migrar sin interrumpir operaciones, aplicándose en protocolos como TLS, IPsec y 5G con mejoras notables en rendimiento y eficiencia energética. Tecnologías como ML-KEM y ML-DSA se perfilan como estándares de referencia, respaldadas por optimizaciones que permiten mantener un desempeño cercano al de soluciones clásicas. Además, el uso de hardware especializado como DPUs demuestra que es posible alcanzar velocidades de cifrado a nivel de línea sin comprometer la latencia, mientras que casos de uso en redes especializadas, como FANETs o aplicaciones en la nube con búsqueda segura, confirman que la resistencia cuántica puede adaptarse a entornos con restricciones críticas. En conjunto, el panorama refleja que el desafío no se limita a reemplazar algoritmos, sino a rediseñar la gestión de llaves, la observabilidad y las políticas de seguridad para un ecosistema digital que debe ser resiliente frente a amenazas de largo plazo.

Conclusiones

El artículo desarrolla una revisión sistemática de la literatura científica sobre los efectos que puede tener la computación cuántica, y como nos preparamos para la era post-cuántica a partir de los reportes indexados en Scopus, PubMed y ScienceDirect entre los años 2020 y 2025, seleccionados siguiendo el protocolo

PRISMA 2020. De los 283 artículos iniciales identificados, tras cribado y eliminación de duplicados, se analizaron 15 estudios originales que cumplen los criterios de inclusión y exclusión y que aportan datos experimentales sobre, cómo nos preparamos para la era post-cuántica. La era post-cuántica ya es operativa, no teórica. Hay evidencia de despliegues performantes (velocidad de línea con DPU; mejor consumo con ML-KEM en 5G) que valida el enfoque propuesto de adopción progresiva.

La hibridación es la ruta segura de migración. Combinar algoritmos de intercambio de claves post-cuánticos (KEM PQC) con ECC/RSA y utilizar suites por dominio/flujo en SDN o por perfil en 5G reduce riesgo de interrupción sin sacrificar seguridad “HNDL”. ML-KEM/ML-DSA son la nueva base de la dirección NIST y la evidencia de optimizaciones (AVX-512, batching) los vuelven candidatos por defecto en servidores, computadores cuánticos y equipos de usuarios (UEs), manteniendo un equilibrio entre costo-beneficio y seguridad. El problema ya no es solo “críptico”, es sistémico. Gestión de llaves, rotación, telemetría, y observabilidad deben actualizarse para detectar degradaciones de negociación criptográfica o establecimiento de sesión / MTU y outliers de latencia por tamaños de claves y firmas. Casos especiales validan el enfoque “altamente robusto”. FANETs y PKE-con-igualdad muestran que se puede ser cuántico-seguro sin romper los objetivos de nivel de servicio (SLO) de energía/latencia en contextos críticos.

A partir de los hallazgos obtenidos en la presente revisión sistemática, se plantean las siguientes recomendaciones, orientadas a favorecer la transición hacia la criptografía post-cuántica y a promover futuras investigaciones en este ámbito. Estas recomendaciones se fundamentan en la

evidencia científica analizada y buscan contribuir tanto a la adopción progresiva de tecnologías resistentes a ataques cuánticos como al fortalecimiento de las estrategias de seguridad en diferentes entornos tecnológicos.

- Promover la adopción gradual de la criptografía post-cuántica mediante estrategias de transición que permitan mantener la interoperabilidad con los sistemas criptográficos convencionales, considerando las recomendaciones emitidas por organismos internacionales como el NIST.
- Desarrollar estudios experimentales que evalúen el desempeño de algoritmos criptográficos post-cuánticos en diferentes escenarios de aplicación, particularmente en redes 5G, infraestructuras definidas por software (SDN), servicios en la nube y centros de datos.
- Fortalecer la gestión criptográfica mediante la actualización de políticas relacionadas con el ciclo de vida de las claves, la gobernanza de los algoritmos y los mecanismos de monitoreo, con el fin de facilitar una transición segura hacia infraestructuras resistentes a ataques cuánticos.
- Impulsar investigaciones orientadas a optimizar el rendimiento de los algoritmos post-cuánticos, especialmente en entornos con restricciones de procesamiento, consumo energético y latencia, donde la eficiencia operativa constituye un factor crítico.
- Ampliar las investigaciones sobre la integración de mecanismos criptográficos post-cuánticos con tecnologías emergentes, como redes definidas por software, Internet de las Cosas, blockchain y redes móviles de nueva generación, con el propósito de validar su aplicabilidad en entornos reales.

Referencias bibliográficas

- Bernstein, D. J., Lange, T., & Dahmen, E. (Eds.). (2017). Post-quantum cryptography. Springer. <https://link.springer.com/book/10.1007/978-3-540-88702-7>
- Arute, F., Arya, K., Babbush, R., Bacon, D., Bardin, J. C., Barends, R., ... & Martinis, J. M. (2019). Quantum supremacy using a programmable superconducting processor. *Nature*, 574(7779), 505–510. <https://doi.org/10.1038/s41586-019-1666-5>
- Shor, P. W. (1997). Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing*, 26(5), 1484–1509. <https://doi.org/10.1137/S0097539795293172>
- Chen, L. K., Chen, L., Jordan, S., Liu, Y. K., Moody, D., Peralta, R., ... & Dang, Q. H. (2016). Report on Post-Quantum Cryptography. National Institute of Standards and Technology. <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.8105.pdf>
- National Institute of Standards and Technology (NIST). (2022). Post-Quantum Cryptography: Selected Algorithms. <https://csrc.nist.gov/projects/post-quantum-cryptography>
- Chen, L., et al. (2023). Quantum cryptanalysis of RSA and ECC: Practical thresholds for post-quantum migration. *Journal of Cybersecurity*, 15(2), 112–130. <https://doi.org/10.1093/cybsec/tyad007>
- Alagic, G., et al. (2022). NIST PQC standardization: Comparative analysis of lattice-based and code-based candidates. *IEEE Transactions on Quantum Engineering*, 3, 1–18. <https://doi.org/10.1109/TQE.2022.3148892>

Kelsey, J., & Cooper, D. (2024). Organizational challenges in post-quantum cryptography adoption: A multi-sector analysis. *International Journal of Information Security*, 41(3), 451–467. <https://doi.org/10.1007/s10207-023-00761-4>

Bernstein, D. J., & Lange, T. (2021). Hybrid post-quantum cryptography: Deployment strategies for critical infrastructures. *ACM Transactions on Privacy and Security*, 24(4), 1–31. <https://doi.org/10.1145/3473038>

Haddaway, N. R., Page, M. J., Pritchard, C. C., & McGuinness, L. A. (2022). PRISMA 2020: An R package and Shiny app for producing PRISMA 2020-compliant flow diagrams, with interactivity for optimised digital transparency and Open Synthesis. *Campbell Systematic Reviews*, 18(2), e1230. <https://doi.org/10.1002/cl2.1230>

Cano Aguilera, A., Rubio Garcia, C., Lawo, D., Imaña, J. L., Vegas Olmos, J. J., & Tafur Monroy, I. (2024). In-line rate encrypted links using pre-shared post-quantum keys and DPUs. *Scientific Reports*, 14, 21227. <https://doi.org/10.1038/s41598-024-71861-x> *Nature*

Liu, Y.-K., & Moody, D. (2024). Post-Quantum Cryptography, and the Quantum Future of Cybersecurity. *Physical Review Applied*, 21, 040501. <https://doi.org/10.1103/PhysRevApplied.21.040501> *NIST*

He, J., Ye, Q., Yang, Z., Wang, S., & Wang, J. (2025). A compact public key encryption with equality test for lattice in cloud computing. *Scientific Reports*, 15, 27426. <https://doi.org/10.1038/s41598-025-12018-2>

Zheng, J., Zhu, H., Dong, Y., Song, Z., Zhang, Z., Yang, Y., & Zhao, Y. (2024). Faster Post-Quantum TLS 1.3 Based on ML-KEM: Implementation and Assessment. preprint. <https://arxiv.org/abs/2404.13544>

(OJCS) Malik De-Vauchelle, S. (2024). Performance model for the selection of quantum-resistant ML-KEM public key in 5G mobile networks. *Open Journal of Cybersecurity*. <https://doi.org/10.1109/OJCS.2024.3397307> (metadatos verificados en el portal del editor; el artículo discute selección de ML-KEM para 5G SUCI/AKA). *Cambridge University Press & Assessment*

Hoque, S., Aydeger, A., & Zeydan, E. (2024). Exploring Post-Quantum Cryptography with Quantum Key Distribution for Sustainable Mobile Network Architecture Design. preprint. <https://arxiv.org/abs/2404.10602>

Ko, Y., Pawana, I. W. A. J., & You, I. (2025). 5G-AKA-HPQC: Hybrid Post-Quantum Cryptography Protocol for Quantum-Resilient 5G Primary Authentication with Forward Secrecy. preprint. <https://arxiv.org/abs/2502.02851>

Commey, D., Appiah, B., Klogo, G. S., Bagyl-Bac, W., & Gadze, J. D. (2025). Performance Analysis and Deployment Considerations of Post-Quantum Cryptography for Consumer Electronics. preprint. <https://arxiv.org/abs/2505.02239>

Quantum-Resistant Track Assignment Algorithm for FANETs. (2025). *Networks*, 5(2), 20. <https://doi.org/10.3390/network5020020> (artículo de acceso abierto en MDPI Networks; sobre asignación de rutas resistente a cuántica en FANETs).