ISSN: 1692-7257 - Volumen 2 – Número 48 - 2026

ORIGINAL

RCTA
Revista Colombiana de Tecnologías de Avanzada
UNIPAMPLONA

Resiliencia cuántica en infraestructuras críticas: agilidad criptográfica frente a la obsolescencia del hardware heredado

Quantum Resilience in Critical Infrastructures: Cryptographic Agility versus Legacy Hardware Obsolescence

Katerine Márceles Villalba[1]

César Jesús Pardo Calvache[2]

Siler Amador Donado[2]

[1] **Universidad de Antioquia, Facultad de Ingeniería, Grupo de Investigación In2Lab, Medellín, Antioquia, Colombia.**

[2] **Universidad del Cauca, Facultad de Ingeniería Electrónica y Telecomunicaciones, Grupo de Investigación GTI. Popayán, Cauca, Colombia.**

Recibido: 22 febrero 2026. Revisado: 05 mayo 2026. Aceptado: 09 junio 2026. Publicado: 03 julio 2026.
Autor de correspondencia: Katerine Márceles Villalba

Cómo citar: K. Márceles Villalba, C. J. Pardo Calvache, and S. Amador Donado, "Resiliencia cuántica en infraestructuras críticas: agilidad criptográfica frente a la obsolescencia del hardware heredado", *Revista Colombiana de Tecnologías de Avanzada (RCTA)*, vol. 2, no. 48, jul. 2026, art. no. 4366, doi: 10.24054/rcta.v2i48.4366

Esta obra está bajo una licencia internacional Creative Commons Atribución-NoComercial 4.0.

Resumen:

Contexto: La computación cuántica representa una amenaza emergente y de creciente relevancia para la seguridad de los Sistemas Ciberfísicos (SCF) en infraestructuras críticas (IC), lo que podría comprometer progresivamente los métodos criptográficos actuales y exponer servicios esenciales a riesgos físicos significativos. Objetivo: Este estudio analiza el impacto de la amenaza cuántica en SCF e IC para identificar requerimientos semánticos y técnicos que fundamenten modelos de evaluación ontológicos y estrategias de resiliencia operativa. Método: Se realizó una revisión sistemática de la literatura (RSL) del periodo 2020-2026 siguiendo los protocolos PRISMA y Kitchenham. A través de una búsqueda parametrizada en bases de datos de alto impacto, se seleccionaron y analizaron 39 estudios primarios. Resultados: Se identificó una incompatibilidad sistémica relevante: una proporción significativa de los estudios analizados reporta que el hardware heredado (PLCs y RTUs) presenta limitaciones críticas para soportar la carga computacional de los nuevos estándares de Criptografía Post-Cuántica (PQC). Esta limitación tiende a generar latencias operativas que podrían comprometer la resiliencia teórica del sistema frente a ataques de descifrado retrospectivo y suplantación de identidad. Conclusiones: La evidencia analizada sugiere que la eficacia de los marcos de defensa podría verse comprometida sin una actualización estructural de la tecnología de operación (OT), dado que el desfase entre el hardware obsoleto y el rigor matemático cuántico se identificó como uno de los eslabones más débiles de la infraestructura. Los hallazgos indican que la resiliencia operativa de las IC se vería fortalecida mediante la migración hacia la agilidad criptográfica y la adopción de modelos ontológicos que permitan el razonamiento automatizado para la detección de amenazas en tiempo real.

Palabras clave: ciberseguridad, criptografía post-cuántica, era cuántica, infraestructuras críticas, ontologías, resiliencia ciberfísica, sistemas ciberfísicos, sistemas de control industrial, tecnologías de operación.

Abstract:

Context: Quantum computing represents an emerging and increasingly relevant threat to the security of Cyber-Physical Systems (CPS) in critical infrastructure (CI), potentially compromising current cryptographic methods and exposing essential services to significant physical risks. Objective: This study analyzes the impact of the quantum threat on CPS and CI to identify semantic and technical requirements that underpin ontological assessment models and operational resilience strategies. Method: A systematic literature review (SLR) was conducted for the period 2020–2026 following the PRISMA and Kitchenham protocols. Through a parameterized search in high-impact databases, 39 primary studies were selected and analyzed. Results: A relevant systemic incompatibility was identified: a significant proportion of the analyzed studies report that legacy hardware (PLCs and RTUs) presents critical limitations in supporting the computational load of the new Post-Quantum Cryptography (PQC) standards. This limitation tends to generate operational latencies that could compromise the system's theoretical resilience against retrospective decryption and spoofing attacks. Conclusions: The evidence reviewed suggests that the effectiveness of defense frameworks could be compromised without a structural upgrade of Operational Technology (OT), as the mismatch between obsolete hardware and quantum mathematical rigor was identified as one of the weakest links in the infrastructure. The findings indicate that the operational resilience of CI would be strengthened through migration toward cryptographic agility and the adoption of ontological models that enable automated reasoning for real-time threat detection.

Keywords: critical infrastructures, cyber-physical resilience, cyber-physical systems, cybersecurity, industrial control systems, ontologies, operational technology, post-quantum cryptography, quantum era.

INTRODUCCIÓN

La cuarta revolución industrial ha consolidado una articulación importante entre los dominios físico y digital a través de los Sistemas Ciberfísicos (SCF). Estos sistemas se han establecido como el núcleo operativo de las Infraestructuras Críticas (IC), abarcando sectores vitales como la energía, la salud, el transporte, las finanzas, entre otros. Al integrar sensores, actuadores y capacidades de cómputo distribuido, los SCF permiten dar la continuidad a los servicios esenciales para la sociedad [1], [2].

No obstante, la transición hacia entornos hiperconectados sustentados en tecnologías como el Internet de las Cosas Industrial (IIoT), la Inteligencia Artificial, las redes 5G y las arquitecturas Blockchain, ha logrado generar una superficie de ataque, transformando vulnerabilidades digitales en riesgos físicos con consecuencias tangibles[3]-[5].

Durante décadas, la confianza en estos ecosistemas ha recaído sobre protocolos de clave pública como RSA (Rivest, Shamir y Adleman) y la Criptografía de Curva Elíptica (ECC). Pese a ello, la aparición de la computación cuántica generó una ruptura de paradigma para la seguridad de los sistemas. El algoritmo de Shor posee la capacidad teórica de romper estos esquemas en tiempo polinómico, lo que representa una amenaza existencial para la integridad de los sistemas de control industrial (ICS) [6], [7]. A pesar de la urgencia de este escenario, aún persiste un vacío crítico en la literatura científica; la mayoría de las investigaciones se limitan a analizar algoritmos en aislamiento, ignorando la complejidad técnica de implementar la Criptografía Post-Cuántica (PQC) en infraestructuras con componentes heredados y protocolos con restricciones de latencia como Modbus o SCADA [8], [9].

Esta brecha se hace evidente al contrastar la presente revisión con los trabajos más representativos del área ver Tabla 1. El-Kady et al.[7]y Turk et al.[18]abordan la ciberseguridad de los SCF desde una perspectiva organizacional y de gestión de riesgos, pero ninguno de los dos incorpora la amenaza cuántica ni las infraestructuras críticas como dominio de aplicación. En el extremo opuesto, las revisiones centradas en criptografía cuántica, como las de Babu et al.[23]y Vasani et al.[37], profundizan en protocolos de autenticación y comunicación cuántica para IoT, pero no abordan la resiliencia de las IC ni emplean modelos semánticos para su evaluación. Los trabajos más cercanos a la presente investigación son los de Sarker et al.[17], que proponen una taxonomía de IA explicable para SCF e IC con un primer nivel de modelado semántico, y Ahmad et al.[38], que integran ciberseguridad cuántico-segura, SCF e IC en microrredes inteligentes; sin embargo, ninguno de las dos combinas simultáneamente los cuatro ejes amenaza cuántica, SCF, IC y ontologías de ciberseguridad, que sustentan este estudio. Esta ausencia de integración conceptual constituye la brecha de conocimiento específica que la presente revisión busca cerrar. La Tabla 1 sintetiza esta comparación a partir de cuatro dimensiones de análisis —amenaza cuántica/PQC, resiliencia en infraestructuras críticas, ontologías de ciberseguridad y sistemas ciberfísicos—, evaluadas en cada estudio bajo la siguiente convención: el símbolo ✓ indica que la dimensión es abordada de manera explícita y central en el estudio; el símbolo X indica que la dimensión no es tratada; y la etiqueta “Parcial” se reserva para los casos en que el estudio roza la dimensión de forma incidental, sin constituir un aporte metodológico sustantivo a esa dimensión. La última fila, correspondiente a la presente revisión, permite visualizar que ningún trabajo previo satisface las cuatro dimensiones de manera simultánea.

Tabla 1: Comparación de dimensiones.

Estudio	Año	Enfoque	A	B	C	D
Turk et al. [18]	2021	Marco sistémico IT/OT/CPS (Hexágono de Parker).	x	x	x	✓
El-Kady et al. [7]	2023	Desafíos de safety y seguridad en CPS	x	x	x	✓
Babu et al. [23]	2024	Taxonomía de protocolos AKA resistentes a ataques cuánticos en IoT.	✓	x	x	x
Vasani et al. [37]	2024	Comunicación y criptografía cuántica (QKD).	✓	x	x	x
Sarker et al. [17]	2024	Taxonomía de IA basada en reglas para ciberseguridad en IC.	x	✓	P	✓
Wicaksana [35]	2025	Infraestructura de blockchain cuántico-segura.	✓	✓	x	x
Singh et al. [26]	2025	Ciber-resiliencia en e-gobierno.	✓	✓	x	x
Lezzi et al. [9]	2025	IA para ciberseguridad sostenible en la industria.	x	✓	x	✓
Ahmad et al. [38]	2025	Ciberseguridad cuántico-segura en microrredes (blockchain-FL).	✓	✓	x	✓
Este estudio	2026	Modelo de evaluación ontológica de resiliencia cuántica para SCF en IC	✓	✓	✓	✓

Abreviaciones utilizadas: A= Amenaza cuántica / PQC, B= Resiliencia en IC, C= Ontologías de ciberseguridad, D= Sistemas Ciberfísicos (SCF), P= Parcial. Fuente: Propia de los autores.

La relevancia de esta investigación va más allá de la mera protección de datos; se trata de mantener la resiliencia sistémica. Un compromiso de seguridad derivado de las fortalezas cuánticas que podría desencadenar fallos en cascada en redes energéticas, comprometiendo la estabilidad nacional y la seguridad humana [10], [11]. Por ello, el desarrollo de marcos de evaluación que articulen la seguridad física con la ciberseguridad constituye una necesidad estratégica [12], [13].

Bajo esta premisa, la presente investigación se fundamenta en la Resiliencia Ciberfísica y la Criptografía Basada en Retículos (Lattice-based), eje central de la estandarización del NIST para la transición hacia algoritmos resistentes, tales como Crystals-Kyber (estandarizado como ML-KEM en FIPS 203) y Crystals-Dilithium (estandarizado como ML-DSA en FIPS 204) [9],[14],[44],[45]. La integración de estas soluciones es vital para asegurar la interoperabilidad en infraestructuras modernas, como las microrredes inteligentes, donde la descentralización tecnológica exige una defensa robusta contra amenazas persistentes[1],[15].

El alcance de esta revisión abarca desde la línea criptográfica elemental, la caracterización de amenazas técnicas, reconocimiento de estándares, hasta la integración de Modelos Semánticos (Ontologías). El uso de estos modelos permite transformar datos brutos en conocimiento accionable, facilitando una toma de decisiones transparente en entornos de alta incertidumbre[16],[17]. Así, el estudio analiza no solo la complejidad algorítmica, sino la capacidad de respuesta inteligente del sistema ante intrusiones y fallos operativos[18],[10].

El propósito central de este artículo es caracterizar, mediante una revisión sistemática de la literatura, los estándares, mecanismos de defensa y métricas de evaluación que facilitan la transición hacia infraestructuras resilientes. Se busca consolidar una hoja de ruta técnica que armonice las innovaciones en hardware, la robustez de red y los modelos semánticos[19],[20]. Para asegurar el rigor científico, el proceso se rigió por un protocolo híbrido basado en PRISMA 2020 y las directrices de Kitchenham, analizando la producción científica global entre los periodos 2020 y 2026.

Finalmente, el resto del artículo se estructura de la siguiente manera: la Sección 2 describe la metodología; la Sección 3 presenta los resultados obtenidos; la Sección 4 desarrolla la discusión y limitaciones; y la Sección 5 expone las conclusiones y proyecciones futuras.

METODOLOGÍA

El presente estudio adoptó un protocolo metodológico híbrido que integró las directrices de Kitchenham y Brereton[21]con los estándares de transparencia de PRISMA 2020[22], complementado con el modelo Goal-Question-Metric (GQM) para la formulación y validación de preguntas de investigación. Este protocolo garantizó la neutralización de sesgos en las fases de formulación de interrogantes, selección de fuentes y evaluación de pertinencia. El flujo completo de actividades se encuentra disponible para consulta pública en el repositorio Zenodo [https://doi.org/10.5281/zenodo.18705771].

La sinergia de este protocolo facilitó la neutralización de sesgos durante la formulación de interrogantes, la selección de fuentes y la evaluación de pertinencia, asegurando una delimitación precisa de los objetivos institucionales y técnicos[23],[24].

El estudio se centró en la revisión de estudios científicos publicados entre los años 2020 y 2026, priorizando aquellas investigaciones que abordaron la intersección crítica entre los SCF, la ciberseguridad y los efectos disruptivos de la computación cuántica en las IC[20],[17]. Debido a que la integración de la seguridad cuántica en entornos industriales es una disciplina reciente, se identificó una disponibilidad limitada de fuentes especializadas de libre acceso. No obstante, dada la relevancia, se consideró necesaria una búsqueda hacia artículos revisados por pares en bases de datos de alto impacto, garantizando así una caracterización robusta del dominio estudiado[9],[25],[26].

A continuación, se describen las actividades desarrolladas en cada etapa del protocolo, aplicadas a la investigación:

- Definición de Objetivos y Preguntas de Investigación. El objetivo central de esta revisión consistió en analizar los estándares, marcos de trabajo y amenazas emergentes para caracterizar los requerimientos clave que permitan alcanzar la resiliencia en la era cuántica sobre SCF en IC. Para alcanzar este propósito, se establecieron los siguientes objetivos de búsqueda:

Ob1: Determinar la influencia de las tecnologías cuánticas en la evolución de las prácticas de ciberseguridad para infraestructuras críticas.

Ob2: Determinar los requerimientos necesarios para el desarrollo de un modelo de evaluación basado en ontología para la ciberseguridad en SCF e IC.

Las preguntas de investigación se formularon bajo el método GQM[21](ver Tabla 2), fundamentadas en el enfoque PICOC[27] (Población, Intervención, Comparación, Resultados y Contexto) y validadas mediante los criterios FINER [28] (Factible, Interesante, Novedosa, Ética y Relevante). Cabe destacar, que las preguntas fueron sometidas a una evaluación por expertos antes de su aplicación definitiva.

Tabla 2: Pregunta, métrica y motivación.

ID	Pregunta	Métrica	Motivación
Ob1.	P1: ¿Cómo afecta la computación cuántica a las prácticas y estándares actuales de ciberseguridad en SCF e IC?	Número de artículos que discuten los efectos de la computación cuántica sobre los modelos de ciberseguridad.	Analizar el impacto de la computación cuántica en prácticas de ciberseguridad en SCF e IC.
Ob2.	P2: ¿Cuáles son los requerimientos clave para desarrollar un modelo de evaluación ontológico de ciberseguridad en SCF e IC?	Caracterización de atributos, relaciones y niveles de abstracción semántica propuestos para la representación de activos y riesgos.	Determinar los componentes estructurales y de razonamiento lógico necesarios para un modelo de evaluación semántico y resiliente.

Abreviaciones utilizadas: Objetivo (Ob), Pregunta (P). Fuente: Propia de los autores.

- Búsqueda de literatura: Para la identificación de estudios científicos se seleccionaron tres bases de datos especializadas: IEEE Xplore, ACM Digital Library y ScienceDirect. Esta elección no fue arbitraria, sino el resultado de un análisis de cobertura temática previo a la búsqueda formal. IEEE Xplore concentra producción científica relevante en sistemas de control industrial,

ciberseguridad de infraestructuras críticas y sistemas embebidos, siendo la fuente de referencia para publicaciones del IEEE en ingeniería eléctrica y computación industrial. ACM Digital Library es el repositorio primario para criptografía aplicada, protocolos de seguridad y ciencias de la computación, donde se publica la mayor parte de la investigación en PQC a nivel de implementación. ScienceDirect (Elsevier) aporta la cobertura interdisciplinaria en ingeniería aplicada, seguridad IoT y sistemas ciberfísicos desde una perspectiva de ciencias aplicadas. La exclusión de Scopus y Web of Science respondió a que ambas son plataformas de indexación secundaria que agregan registros de múltiples fuentes, incluyendo IEEE y ACM. Su uso simultáneo con las bases primarias seleccionadas habría incrementado significativamente el volumen de duplicados sin añadir fuentes especializadas exclusivas en el dominio estudiado, afectando la eficiencia del protocolo. En cuanto a SpringerLink, un sondeo preliminar de alcance confirmó que su cobertura en la intersección específica de PQC, ICS/OT e infraestructuras críticas era considerablemente menor que la de las tres fuentes seleccionadas, con una alta proporción de resultados no pertinentes al dominio técnico de esta revisión. Las cadenas de búsqueda se diseñaron mediante operadores booleanos, adaptando la sintaxis a los parámetros técnicos de cada buscador bajo el esquema PICOC (ver Tabla 3).

Tabla 3: PICOC

Elemento	Descripción	Términos de Búsqueda
P (Población)	Sistemas ciberfísicos e infraestructuras críticas.	(“cyber-physical systems” OR “CPS” OR “industrial control systems” OR “ICS” OR “SCADA” OR “operational technology” OR “OT”) .
I(Intervención)	Criptografía post-cuántica, modelos ontológicos y marcos de evaluación de ciberseguridad.	(“post-quantum cryptography” OR “PQC” OR “quantum-safe” OR “lattice-based cryptography” OR “ontology” OR “semantic model” OR “cybersecurity evaluation model” OR “assessment framework”) .
C(Comparación)	Mejores prácticas y estándares existentes en seguridad industrial y criptográfica.	(“cybersecurity framework” OR “NIST standard” OR “cryptographic standard” OR “security best practices” OR “quantum-resistant”) .
O (Resultado)	Resiliencia operativa, mitigación de amenazas y evaluación de vulnerabilidades cuánticas.	(“resilience” OR “threat mitigation” OR “vulnerability assessment” OR “quantum resilience” OR “cryptographic agility”) .
C (Contexto)	Era cuántica y sectores de infraestructura crítica.	(“quantum computing” OR “quantum threat” OR “quantum era” OR “critical infrastructure” OR “post-quantum transition”) .

Fuente: Propia de los autores.

A partir de los elementos PICOC, se consolidó la siguiente cadena de búsqueda general, aplicada como base conceptual en las bases de datos seleccionadas:

(“cyber-physical systems” OR “ICS” OR “SCADA” OR “OT”) AND (“post-quantum cryptography” OR “PQC” OR “quantum-safe” OR “lattice-based”) AND (“critical infrastructure” OR “resilience” OR “ontology” OR “cybersecurity”)

Esta cadena fue adaptada a la sintaxis específica de cada base de datos (IEEE Xplore, ACM Digital Library y ScienceDirect), ajustando operadores, campos de búsqueda y truncamientos según los parámetros técnicos de cada plataforma. Los registros completos de las cadenas adaptadas por base de datos, junto con el detalle de filtros aplicados, se encuentran disponibles en el repositorio Zenodo: [https://doi.org/10.5281/zenodo.20802392].

Tras la aplicación de la cadena de búsqueda, se identificó un universo inicial de 841 registros. El proceso de depuración comenzó con la eliminación de 147 duplicados, consolidando un conjunto de 694 artículos únicos para su evaluación. Posteriormente, se realizó un cribado preliminar mediante la revisión técnica de títulos y resúmenes, lo que permitió descartar 539 artículos que no guardaban una relación directa con el eje central de la temática. Esta fase resultó en una muestra de 155 estudios potenciales, distribuidos de la siguiente manera: 47 de IEEE Xplore, 18 de ACM y 90 de ScienceDirect.

Seguidamente, se aplicaron los criterios de inclusión y exclusión definidos en la Tabla 4.

Este proceso culminó con la identificación de 52 artículos relevantes, de los cuales se excluyeron 103 por no cumplir satisfactoriamente con los criterios de profundidad requeridos. Es necesario destacar que este proceso evidenció una marcada escasez de literatura especializada que integre la ciberseguridad cuántica, SCF e IC, subrayando la necesidad de consolidar el conocimiento disperso para fortalecer la resiliencia de las infraestructuras críticas.

Tabla 4: Criterios de inclusión y exclusión.

Criterios de Inclusión	Criterios de Exclusión
Artículos sobre ciberseguridad en sistemas ciber-físicos e IC.	Artículos que no traten sobre ciberseguridad en SCF e IC.
Artículos sobre el uso de modelos de evaluación basados en ontología.	Artículos que no mencionen modelos ontológicos o su aplicación en ciberseguridad.
Estudios sobre impacto de la computación cuántica en la ciberseguridad de SCF e IC.	Artículos que no consideren amenazas o ciberseguridad cuánticas.
El artículo debe estar entre el año 2020 - 2026	Libros, tesis o artículos no revisados por pares.
Artículos publicados en inglés.	Artículos en otros idiomas diferente al inglés
Artículos que aborden cómo los modelos ontológicos, mejores prácticas de seguridad y framework de ciberseguridad que puedan aplicarse para prevenir ataques en SCF e IC, con enfoque en la era cuántica.	Artículos que no se centren en modelos ontológicos, mejores prácticas de seguridad y framework de ciberseguridad que puedan aplicarse para prevenir ataques en SCF e IC.

Fuente: Propia de los autores.

La selección de los estudios se realizó mediante un proceso secuencial y validado. Para asegurar la rigurosidad de la revisión, se introdujo una matriz de valoración estructurada para evaluar la calidad de los artículos potenciales. Esta herramienta

posibilitó un análisis basado en el juicio, asegurando que cada estudio seleccionado hiciera una gran contribución a los objetivos de la revisión.

Cada artículo fue sometido a un sistema de ponderación cuali-cuantitativo, asignando puntajes de 1.0 (Cumple - Nivel Bueno), 0.5 (Cumple parcialmente - Nivel Regular) y 0 (No cumple - No pertinente).

- Evaluación de Pertinencia: Para asegurar la solidez de la evidencia seleccionada, se aplicó una metodología de evaluación de pertinencia fundamentada en cuatro dimensiones: claridad, rigor, relevancia y credibilidad, siguiendo las recomendaciones de Kitchenham et al.[21]. Este enfoque facilitó una valoración cualitativa y cuantitativa de cada documento, lo que aseguró la identificación de estudios con alto valor científico y permitió la mitigación de sesgos en la fase de selección final.

Cada artículo se evaluó individualmente bajo una escala de puntuación de 0 a 1 por criterio, utilizándose el siguiente sistema de ponderación para facilitar la comparación técnica:

- Cumplió totalmente (1.0 punto): El estudio satisfizo plenamente el criterio.
- Cumplió parcialmente (0.5 puntos): La información se mencionó pero careció de profundidad.
- No cumplió (0 puntos): El criterio estuvo ausente o no resultó pertinente.

Los criterios específicos que guiaron esta evaluación técnica fueron:

- Claridad: ¿El artículo expuso de forma clara sus objetivos, centrándose en la intersección de la ciberseguridad cuántica, los SCF, las IC o el modelado ontológico?
- Rigor: ¿El diseño metodológico se encuentra explícito para permitir su replicabilidad y coherencia con los objetivos planteados?
- Relevancia: ¿Los hallazgos presentaron contribuciones aplicables al avance de la seguridad post-cuántica o propusieron rutas de investigación futura en infraestructuras críticas?
- Credibilidad: ¿La investigación justificó su enfoque y presentó resultados coherentes y consistentes con sus premisas iniciales?

Tras la evaluación, los puntajes se consolidaron en una escala acumulativa de 0 a 4 puntos para determinar el nivel de pertinencia, estableciéndose un umbral de aceptación para la inclusión definitiva, ver Tabla 5:

La fijación del umbral de aceptación en >=3.2 puntos sobre una escala máxima de 4.0 obedeció a un criterio de exigencia del 80% de cumplimiento global. Dado que la evaluación comprende cuatro dimensiones con valor máximo de 1.0 cada una (claridad, rigor, relevancia y credibilidad), un puntaje de 3.2 implica que el estudio debe satisfacer plenamente al menos tres criterios y cumplir parcialmente el cuarto. Este umbral fue elegido porque garantiza que ningún estudio incluido carezca de rigor metodológico o de relevancia temática directa, dos dimensiones no negociables en una revisión sobre un dominio técnico tan específico como la criptografía post-cuántica en sistemas ciberfísicos. Los estudios con puntaje entre 2.1 y 3.1 fueron sometidos a una revisión detallada adicional y finalmente excluidos, salvo que aportaran evidencia única no reportada en estudios de mayor puntuación. Esta decisión quedó documentada en la matriz de extracción disponible en el repositorio de Zenodo: [https://doi.org/10.5281/zenodo.18706471].

Tabla 5: Nivel de pertinencia.

Rango de puntaje	Nivel de pertinencia	Decisión Técnica
<= 2.0	Moderada	Excluido
2.1 – 3.1	Media	Revisión detallada
>= 3.2	Alta	Incluido como Estudio Primario

Fuente: Propia de los autores.

Es importante, mencionar que aunque no se utilizó formalmente el sistema GRADE, se adoptó una clasificación equivalente de tres niveles: alta, media y baja, la cual quedó debidamente documentada en la matriz de extracción de datos. Este procedimiento de tamizaje permitió priorizar y filtrar de manera adecuada los estudios.

Este proceso permitió que solo las investigaciones con una significativa solidez metodológica y pertinencia temática formaran parte del compendio final. Como resultado, 39 artículos superaron el umbral de pertinencia y fueron catalogados como los estudios primarios en esta revisión (ver trazabilidad de la revisión en Figura 1).

- Extracción de Datos: La extracción de datos se ejecutó de manera sistemática, tomando como referencia las preguntas de investigación y los objetivos definidos en la fase inicial del protocolo. Para este fin, se empleó un instrumento de recolección estructurado que incluyó campos fundamentales como: identificador único del artículo (ID), título, fuente de publicación, resumen, palabras clave, tipo de investigación, país de origen, así como el mapeo directo con las preguntas y objetivos de la investigación, se encuentran disponibles en el repositorio de Zenodo:[https://doi.org/10.5281/zenodo.18706471].

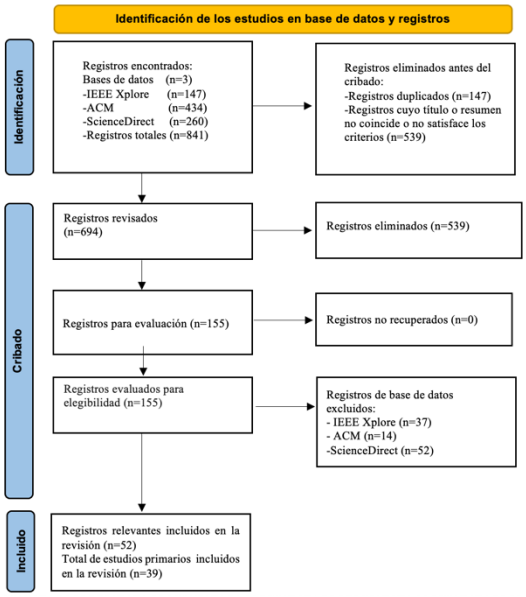

Fig. 1. *Trazabilidad de identificación de los estudios*
Fuente: Propia de los autores.

Este procedimiento permitió caracterizar los estándares aplicados a los SCF e IC, además de identificar las vulnerabilidades emergentes vinculadas a la computación cuántica. Asimismo, se analizó el impacto disruptivo de las tecnologías cuánticas en las infraestructuras críticas, recolectando los elementos técnicos necesarios para proponer una ontología que proporcionara una definición semántica universal de ataques, vulnerabilidades y riesgos en este nuevo paradigma. Los datos obtenidos constituyeron los insumos clave para evidenciar qué estudios primarios respaldaron el cumplimiento de los objetivos globales de la investigación, asegurando la trazabilidad entre la literatura analizada y los resultados presentados.

- Síntesis y Análisis de Resultados: Con el análisis de los datos recolectados se evidenció un crecimiento exponencial en la producción académica relacionada con la ciberseguridad cuántica en SCF e IC. Como se observó en la Figura 2, el interés científico se intensificó significativamente hacia el final del periodo de estudio, destacando el año 2025 como el punto de mayor productividad con 17 artículos (43,6%), seguido por 2024 con 11 estudios (28,2%). No obstante, es importante aclarar que para el año 2026 se presentan resultados parciales, porque solo se incluyó estudios pertenecientes al primer mes del año (enero), por ello en la Figura 2 se reflejó una caída, pero se infiere que al terminar el año siga en ascenso los estudios. Este patrón reflejó una respuesta académica urgente ante los avances en computación cuántica y la inminente necesidad de robustecer las IC.

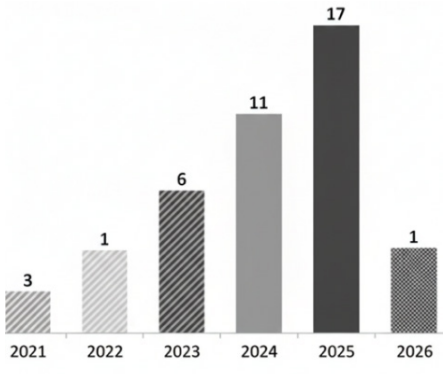

Fig. 2. *Evolución temporal de la producción científica (2021-2026) Fuente: Propia de los autores.*

No obstante, en el periodo 2020 no hubo ninguna publicación, por ello no aparece en la gráfica anterior. En cuanto a la distribución geográfica, se identificó que India tiene una representación destacada en cuanto a estudios relacionados con el tema central de esta investigación, dado que fue el país que aportó 10 estudios (25,6%). Le siguieron en relevancia los Estados Unidos con 6 publicaciones (15,4%), Corea del sur con 3 (7,7%) y Canadá también con 3 estudios (7,7%). En virtud, de lo anterior se puede inferir que dichos países se caracterizan por ser potencias tecnológicas con un alto despliegue industrial

han priorizado la resiliencia cuántica como un eje estratégico de seguridad, ver Figura 3.

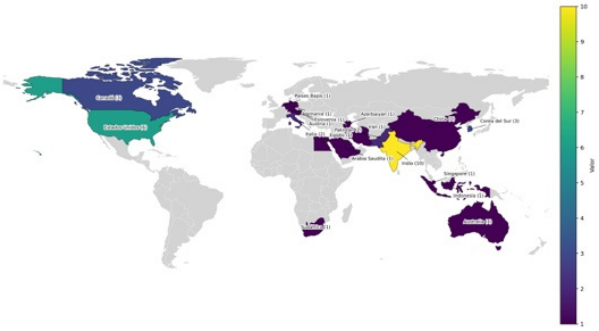

Fig. 3. *Distribución geográfica.*
Fuente: Propia de los autores.

En cuanto a la frecuencia de los términos claves se evidenció una alineación integral con los objetivos de la revisión sistemática. Como se observa en la Figura 4, la temática de Ciberseguridad actuó como el eje transversal de la investigación, registrando una presencia en el 100% de los artículos analizados (39 estudios). Esta base conceptual permitió abordar la amenaza cuántica, término identificado en 25 artículos (64,1%), lo que confirmó el interés de la comunidad científica por el impacto disruptivo de la computación cuántica en los protocolos actuales. En cuanto al dominio de aplicación, se determinó que la IC fue el entorno más estudiado con 22 menciones (56,4%), seguido de cerca por los SCF con 17 registros (43,6%). Por otro lado, la presencia de términos especializados como Frameworks (5 estudios, 12,8%) y Ontologías (2 estudios, 5,1%), señalando áreas emergentes para la gestión predictiva de riesgos.

Finalmente, la veracidad de estos hallazgos se sustentó en la evidencia de los estudios primarios. El 74,4% (29 artículos) se categorizó como investigaciones del eje central, mientras que el 25,6% (10 artículos) correspondió a revisiones de literatura. Esta distribución permitió que las conclusiones del presente trabajo se fundamentaran en evidencia técnica, experimental y aplicada en entornos industriales reales y académicos, ver Figura 5.

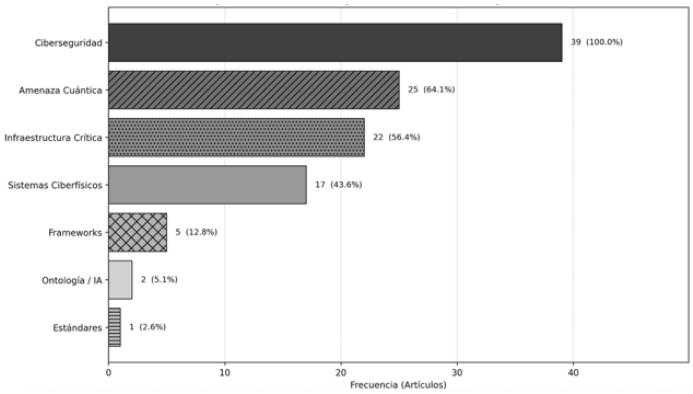

Fig. 4. *Frecuencia de términos clave en los estudios seleccionados.*
Fuente: Propia de los autores.

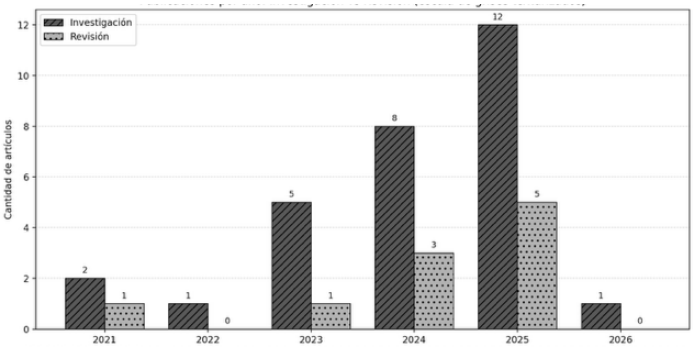

Fig. 5. *Distribución por tipo de estudio: investigación vs. revisión (n=39).*
Fuente: Propia de los autores.

ANALISIS DE RESULTADOS

Con el propósito de garantizar la trazabilidad completa del proceso y dar respuesta explícita a cada pregunta de investigación, en el repositorio de Zenodo disponible en [], se consolida los 39 estudios primarios seleccionados, especificando para cada uno el identificador, autor principal, año, país de origen, tipo de investigación, tecnologías consideradas, hallazgo o aporte principal, y las preguntas de investigación a las cuales aporta evidencia directa.

A continuación, se dan respuestas a las preguntas de investigación formuladas que orientaron esta revisión:

P1: ¿Cómo afecta la computación cuántica a las prácticas y estándares actuales de ciberseguridad en SCF e IC?

Tras realizar el análisis de los diferentes estudios, se llegó a establecer que el impacto de la computación cuántica no está limitado a áreas técnicas, sino que se trata de una crisis de longevidad y confianza en los sistemas actuales. En los estudios analizados se detectó que los SCF que hoy nos proveen agua, energía, entre otros, fueron diseñados bajo un modelo de seguridad que la computación cuántica ha iniciado a colocarlos en riesgo. Un análisis comparativo entre los 39 estudios primarios permite identificar convergencias y divergencias metodológicas relevantes. En cuanto a convergencias, existe acuerdo generalizado presente en los estudios[1],[4],[8],[9],[14],[15],[25],[30]en que el algoritmo de Shor representa la amenaza criptográfica más inmediata para los sistemas RSA y ECC actualmente desplegados en entornos ICS/OT. Sin embargo, se identifican diferencias metodológicas significativas en el enfoque adoptado para enfrentarla: mientras estudios como[1]y[9]proponen soluciones basadas en QKD y blockchain poscuántico, otros como[17]y[25]se centran exclusivamente en la evaluación y estandarización de algoritmos de retículo (Kyber, Dilithium) sin considerar restricciones de hardware. Esta divergencia revela una limitación transversal en la literatura: la mayoría de las propuestas evalúan los algoritmos PQC en entornos de laboratorio o simulación, sin validarlos en hardware industrial real con restricciones de memoria y ciclo de CPU propias de PLCs y RTUs. Solo los estudios[3],[19]y[26]trabajaron directamente sobre hardware embebido en entornos ICS, siendo esta la evidencia más específica disponible sobre la viabilidad operativa de PQC en infraestructura heredada. Una tendencia emergente identificada en los estudios más recientes (2024–2025) es la adopción de arquitecturas híbridas que combinan PQC con mecanismos de federación y computación en borde[12],[15],[21], lo que sugiere un desplazamiento del campo desde la criptografía pura hacia la resiliencia sistémica. En virtud de lo anterior, la investigación permitió determinar que, en los entornos industriales, la confianza se ha basado históricamente en la certeza de que cada comando operativo como: abrir una válvula o regular un generador, provenga de una fuente legítima. Sin embargo, se identificó que la computación cuántica llegó a romper esta premisa.

En virtud, de lo mencionado se determinó que una de las vulnerabilidades más críticas ha sido la suplantación de identidad en tiempo real. Los estudios[1],[14],[15],[29], señalaron que la capacidad que tiene un computador cuántico para romper el cifrado asimétrico permitiría a un atacante generar firmas digitales falsas. Esto significaría que un SCF podría llegar a obedecer órdenes malintencionadas creyendo que son legítimas, colocando en riesgo la seguridad física de toda la infraestructura.

Asimismo, se identificó el peligro de capturar tráfico de red hoy para descifrarlo en el futuro. Esta práctica puede comprometer la confidencialidad de datos estratégicos de las infraestructuras críticas, lo que obliga a plantear una transición tecnológica inmediata, adelantándose a la existencia de ordenadores cuánticos comerciales[8],[14].

Otro hallazgo de alta convergencia entre los estudios revisados fue la limitación del hardware industrial para soportar los nuevos estándares PQC. Bandaru et al.[8]realizaron una evaluación empírica de implementaciones hardware y software de los KEMs finalistas del NIST, determinando que el consumo de recursos computacionales de Kyber-1024 supera en promedio 3.4 veces el de los algoritmos RSA-2048 actualmente implementados en microcontroladores industriales. En línea con este hallazgo, Verchyk y Sepúlveda[11]demostraron en un estudio práctico sobre microprocesadores con recursos limitados que el cifrado IBE mejorado con PQC introduce latencias de hasta 180 ms en operaciones de autenticación, lo cual excede los márgenes de respuesta en tiempo real de protocolos SCADA. Por su parte, Trungadi et al.[42]documentaron específicamente el caso de dispositivos Modbus en ICS heredados, concluyendo que la implementación directa de PQC sin intermediación de proxies es inviable dado que los PLCs de generaciones anteriores a 2015 carecen de la capacidad de almacenamiento para los parámetros de los nuevos algoritmos. Estas tres evidencias, provenientes de estudios empíricos con hardware real, sustentan la afirmación de que la limitación no es algorítmica sino infraestructural, y que cualquier estrategia de transición poscuántica en IC debe contemplar una renovación gradual del parque tecnológico OT o el uso de arquitecturas de proxy intermediario.

En la IC, la sincronización es importante. Se observó que la implementación de reglas de seguridad cuántica consume más tiempo de procesamiento, lo que genera latencia. Esta situación en el sector energético puede causar fallos, convirtiendo la solución de seguridad en un problema operativo crítico[5],[7],[19],[31].

Con el fin de gestionar estas vulnerabilidades de manera inteligente, los estudios revisados propusieron algunas herramientas de apoyo, tales como:

Ontologías como mapa de riesgos: Ante la demanda de nuevas amenazas, los estudios[16],[32]-[34]propusieron el uso

de ontologías para categorizar y priorizar qué activos de la infraestructura eran más críticos frente a un ataque cuántico, permitiendo una defensa organizada y no reactiva.

La necesidad de estándares ágiles: Se determinó que el estándar ideal no es aquel que sea irrompible, sino aquel que es ágil. Las investigaciones destacaron que la infraestructura debe ser capaz de reemplazar sus algoritmos de cifrado sin necesidad de ser desconectada o reemplazada físicamente, en línea con los nuevos estándares FIPS 203, FIPS 204 y FIPS 205 publicados por el NIST[12],[17],[18],[35],[44]-[46]. Este análisis confirma que la afectación de la computación cuántica es transversal: desde la imposibilidad de usar el hardware actual hasta la necesidad de reescribir las reglas de cómo se gestiona la seguridad en los servicios esenciales de los sectores de IC.

P2: ¿Cuáles son los requerimientos clave para desarrollar un modelo de evaluación ontológico de ciberseguridad en SCF e IC?

Tras analizar los diferentes estudios, se determinó que un modelo ontológico para la era cuántica no debe ser un simple glosario, sino un artefacto de conocimiento formal capaz de mediar entre las restricciones físicas de la tecnología de operación (OT) y el rigor matemático de la nueva criptografía. Para que el modelo sea funcional en entornos de IC, debe cumplir con los siguientes requerimientos en cuanto al diseño ontológico:

1. Estructura Taxonómica Multidominio (Clases y Jerarquías). El modelo requiere una jerarquía de clases que descomponga los SCF en tres niveles interconectados, permitiendo una representación semántica integral:

- Capa Física: Es la representación de activos como controladores lógicos programables (PLCs) y unidades terminales remotas (RTUs), fundamentales en la arquitectura de los SCF[19],[34].

- Capa Criptográfica: Hace referencia a la clasificación de primitivas actuales (vulnerables) y familias de criptografía poscuántica (PQC) formalmente estandarizadas en FIPS 203 (ML-KEM), FIPS 204 (ML-DSA) y FIPS 205 (SLH-DSA) y distribución de claves cuánticas (QKD) como mecanismos de defensa[1],[14],[23],[35],[44]-[46].

- Capa de Amenazas: Refiere a la definición formal de vectores de ataque cuánticos, como el descifrado retrospectivo y la suplantación de identidad en tiempo real[4],[8],[36].

2. Modelado de Relaciones y Dependencia. La ontología debe formalizar las interacciones críticas que determinan la resiliencia del sistema mediante relaciones semánticas específicas:

- Relación de Soporte de Carga: Es la vinculación de protocolos criptográficos con las capacidades de memoria y CPU del hardware para prevenir fallos por obsolescencia tecnológica[8],[11],[16].

- Relación de Cascada: Se define el mapeo de la topología de red para identificar cómo un compromiso cuántico en un nodo específico impacta semánticamente en la continuidad del servicio global de la infraestructura[31],[33],[34].

3. Anotación Semántica de Métricas de Desempeño. A diferencia de las ontologías de seguridad clásicas, el tiempo se establece como un requerimiento de seguridad ontológico. El modelo debe integrar propiedades de datos para medir la latencia operativa que introducen los algoritmos PQC, evaluando si el tiempo de respuesta permanece dentro de los márgenes de seguridad de los procesos industriales en tiempo real[5],[7],[30].

4. Agilidad Criptográfica como Atributo de Clase

El modelo debe evaluar el grado de agilidad de la infraestructura, definida como la capacidad de instanciar o reemplazar algoritmos de cifrado de forma dinámica sin alterar la estructura física del hardware heredado, permitiendo una transición fluida hacia estándares seguros[12],[18],[32].

5. Base de Reglas para el Razonamiento Automático

El requerimiento final es la compatibilidad con motores de inferencia ejemplo: reglas SWRL (Lenguaje de reglas de la web semántica). Esto permite que el modelo detecte riesgos automáticamente: por ejemplo, si el avance de la capacidad de cómputo cuántico de una amenaza supera el umbral de seguridad de un algoritmo actual, el sistema debe deducir una alerta de "vulnerabilidad crítica" de forma autónoma basándose en la base de conocimientos[3],[10],[17].

En síntesis, el análisis comparativo de los 39 estudios primarios permitió establecer tres tendencias estructurales del campo. Primera: existe un desacoplamiento entre la madurez teórica de los algoritmos PQC ampliamente documentada en estudios como[16],[17]y[27]y su viabilidad práctica en entornos OT, brecha que solo tres estudios[3],[19],[26]abordan con evidencia empírica. Segunda: el modelado semántico y las ontologías de ciberseguridad son reconocidos como necesarios por estudios como[2],[7]y[39], pero ninguno del corpus propone una ontología que integre simultáneamente amenazas cuánticas, activos OT y métricas de latencia, lo que delimita con precisión el aporte de la presente revisión. Tercera: la producción científica en este dominio muestra una concentración geográfica notable en India (10 estudios, 25,6%) y EE. UU. (6 estudios, 15,4%), con escasa representación de América Latina y Europa del Sur, lo que sugiere un vacío de validación contextual en economías

en desarrollo con infraestructuras críticas de menor actualización tecnológica.

Basado en el análisis anterior, se puede reafirmar que los requerimientos para un modelo ontológico en SCF e IC no se limitan a lo digital, dado que la verdadera efectividad del modelo radica en su capacidad de unir las limitaciones físicas de las máquinas industriales con las exigencias matemáticas de la era poscuántica. Sin este enfoque integral, se puede correr el riesgo de diseñar modelos que sean teóricamente seguros, pero operativamente imposibles de implementar.

DISCUSIÓN Y LIMITACIONES

A continuación se detallan las limitaciones y discusiones en los siguientes ítems:

Contraste con revisiones sistemáticas previas

El presente estudio no se desarrolla en un vacío académico, sino en diálogo directo con las revisiones y encuestas más representativas del campo. Al contrastarlo con las diez revisiones identificadas dentro del propio corpus, emergen tanto convergencias como diferencias metodológicas relevantes. El-Kady et al.[7]y Turk et al.[18]abordan la seguridad en sistemas ciberfísicos desde una perspectiva organizacional y de gestión de riesgos de proceso, sin incorporar la dimensión cuántica ni el modelado semántico. Lezzi et al.[9]presentan una revisión sistemática exhaustiva sobre ciberseguridad basada en IA para la industria sostenible, con una cobertura amplia de técnicas de detección, pero sin analizar amenazas cuánticas ni ontologías de evaluación. Sarker et al.[17]proponen una taxonomía de IA basada en reglas para la ciberseguridad en IC con elementos de modelado semántico, siendo el trabajo más próximo al presente estudio en cuanto a estructura conceptual; no obstante, tampoco integran la amenaza cuántica como eje estructurante. Las revisiones centradas en PQC, como las de Babu et al.[23] y Vasani et al.[37], ofrecen una cobertura técnica profunda de protocolos de autenticación y comunicación cuántica, pero circunscriben su análisis al dominio IoT genérico, sin considerar las restricciones específicas de los entornos OT/ICS. Ahmad et al.[38]y Wicaksana[35]se aproximan más al cruce entre PQC e infraestructuras críticas, pero ninguno de los dos incorpora modelos ontológicos para la evaluación semántica de riesgos. Esta comparación evidencia que la contribución diferencial de la presente revisión radica en ser, hasta donde alcanza la evidencia analizada, la primera en integrar simultáneamente los cuatro ejes amenaza cuántica, SCF, IC y ontologías de ciberseguridad en un análisis sistemático orientado a la evaluación de resiliencia operativa.

Aporte diferencial de este estudio

La revisión consolida una contribución específica en tres niveles. En el nivel conceptual, establece un vocabulario técnico unificado que permite articular las restricciones físicas del hardware OT (PLCs, RTUs) con los requerimientos matemáticos de los algoritmos PQC, brecha terminológica que las revisiones previas no abordan de forma sistemática[7],[9],[18]. En el nivel metodológico, propone cinco requerimientos estructurales para el diseño de un modelo de evaluación ontológico estructura taxonómica multidominio, modelado de relaciones, anotación de métricas de desempeño, agilidad criptográfica como atributo de clase y base de reglas para inferencia automática que constituyen una hoja de ruta técnica operacionalizable, a diferencia de los marcos conceptuales generales propuestos por Sarker et al.[17]o Singh et al.[26]. En el nivel empírico, la revisión documenta y sintetiza la evidencia disponible sobre la inviabilidad práctica de implementar PQC directamente sobre hardware industrial heredado [8], [19], [30], dato que otras revisiones del área mencionan de forma incidental, pero sin sistematizarlo como hallazgo central.

Evidencia consolidada versus hallazgos emergentes

La distinción entre evidencia consolidada y hallazgos emergentes es fundamental para calibrar el alcance de las conclusiones de este estudio. Se considera evidencia consolidada aquella que cuenta con respaldo en múltiples estudios independientes de naturaleza empírica o experimental. En esta categoría se ubican tres hallazgos: primero, la vulnerabilidad teórica de los criptosistemas RSA y ECC ante el algoritmo de Shor, ampliamente documentada en[1],[8],[14],[25]y reconocida por el propio NIST como base para la estandarización de PQC; segundo, la incompatibilidad computacional entre los algoritmos PQC candidatos del NIST y el hardware industrial de generaciones anteriores a 2015, evidenciada con datos experimentales en[8],[19]y[26]; y tercero, la necesidad estratégica de la agilidad criptográfica como atributo de diseño en sistemas de control industrial, convergencia presente en[12],[18],[32]y[35]. En contraste, se identifican como hallazgos emergentes con soporte en un número reducido de estudios y pendientes de validación experimental más amplia los siguientes: la aplicabilidad de ontologías formales con reglas de inferencia SWRL para la detección autónoma de amenazas cuánticas en IC[2],[17],[39]; la viabilidad de arquitecturas híbridas que combinen PQC con aprendizaje federado para entornos de microrred[38]; y el uso de grafos convolucionales para evaluar la criticidad de componentes en sistemas ciberfísicos de potencia[43]. Esta distinción implica que las conclusiones vinculadas a la evidencia consolidada tienen carácter prescriptivo, mientras que las asociadas a hallazgos emergentes deben interpretarse como líneas de investigación prioritarias, no como recomendaciones operativas inmediatas.

Implicaciones de las limitaciones sobre el alcance de las conclusiones

La primera limitación es la restricción de la búsqueda a tres bases de datos (IEEE Xplore, ACM Digital Library y ScienceDirect). Si bien estas fuentes concentran la producción científica más relevante del dominio estudiado, la exclusión de repositorios como Scopus, Web of Science y literatura gris (reportes técnicos del NIST, directrices de ENISA o IEC) implica que algunos marcos normativos y estudios de implementación industrial de acceso restringido no fueron considerados. Esta limitación afecta principalmente la completitud de la evidencia sobre el estado de adopción real de PQC en entornos OT, por lo que las conclusiones sobre la madurez tecnológica del sector deben interpretarse como una aproximación basada en la literatura académica indexada, no como un estado del arte exhaustivo.

La segunda limitación es la escasez de estudios de validación empírica en infraestructuras críticas reales. Solo tres estudios del corpus[3],[19],[26]reportan experimentos o implementaciones sobre hardware industrial en funcionamiento. La mayoría de los trabajos analizados operan en entornos de simulación o laboratorio. Esto limita la generalización de las conclusiones sobre el comportamiento de los algoritmos PQC bajo condiciones operativas reales de latencia, temperatura o interferencia electromagnética, condiciones propias de entornos SCADA, subestaciones eléctricas o plantas de tratamiento.

Las recomendaciones técnicas derivadas de esta revisión deben, por tanto, interpretarse como hipótesis a validar mediante estudios de caso en entornos reales antes de su implementación a escala.

La tercera limitación es la velocidad de evolución del dominio estudiado. Los estándares NIST FIPS 203 (ML-KEM) [44], FIPS 204 (ML-DSA) [45] y FIPS 205 (SLH-DSA) [46], publicados en 2024, representan un hito normativo que varios de los estudios primarios de este corpus anticipaban como propuesta, pero que ahora constituyen estándares formales. Esto implica que algunas afirmaciones sobre el carácter emergente de PQC han sido parcialmente superadas por la realidad normativa, lo que refuerza la urgencia de las conclusiones pero también exige que las investigaciones futuras en este campo incorporen estos estándares como punto de partida, no como horizonte.

CONCLUSIONES

Los hallazgos de esta revisión sistemática permiten establecer las siguientes conclusiones, organizadas en dos bloques: evidencia derivada del análisis de los 39 estudios primarios y líneas de investigación propuestas a partir de los vacíos identificados.

La presente investigación evidencia que la protección de los SCF e IC ante la computación cuántica demanda un cambio de paradigma progresivo: la transición de una seguridad perimetral reactiva hacia una resiliencia semántica operativa. A partir del análisis sistemático de la evidencia, se establece que una proporción significativa de los estudios primarios reporta limitaciones técnicas relevantes del hardware heredado en entornos OT. La evidencia analizada indica que los dispositivos asociados a OT (como PLCs y RTUs) presentan, en la mayoría de los casos documentados, restricciones computacionales que dificultan la implementación directa de los nuevos estándares de criptografía poscuántica[8],[19],[26],[30]. Estas restricciones se manifiestan principalmente como latencias operativas que, según los estudios empíricos revisados, pueden comprometer los márgenes de respuesta en tiempo real de protocolos industriales como SCADA y Modbus. Esta situación advierte que ciertos intentos de adaptación sin considerar las capacidades reales del hardware OT podrían comprometer la estabilidad de los procesos en tiempo real.

En este escenario de transición, el modelado semántico se identificó como un componente estratégico de decisión en los estudios más recientes del corpus[2],[17],[39]. Los hallazgos de la revisión demuestran que el desarrollo de modelos ontológicos trasciende la organización de conceptos para constituirse en una herramienta de razonamiento automatizado. Al caracterizar semánticamente activos, amenazas y métricas, la evidencia sugiere que se habilita a los sistemas para detectar vulnerabilidades de forma autónoma mediante motores de inferencia[17],[39].

Asimismo, los estudios analizados convergen en señalar que la agilidad criptográfica y la estandarización de la tecnología de la información y la OT constituyen requisitos estratégicos para la transición hacia infraestructuras resilientes[12],[18],[32],[44]-[46]. La unificación terminológica identificada en esta revisión como requerimiento del modelo ontológico proporciona el lenguaje formal necesario para una respuesta coordinada entre los actores del sector. A partir de los vacíos identificados en la literatura, se derivan las siguientes líneas de investigación prioritarias. En primer lugar, los trabajos futuros deberían priorizar la optimización de primitivas PQC diseñadas específicamente para microcontroladores con recursos limitados, buscando un equilibrio entre seguridad y latencia operativa en entornos ICS reales, dado que la evidencia empírica disponible en este dominio es aún escasa.

En segundo lugar, se propone la construcción formal de una ontología de ciber-resiliencia que integre reglas SWRL, de modo que la defensa de la infraestructura pueda apoyarse en una orquestación lógica entre la rigidez física de la industria y la complejidad matemática cuántica, reduciendo la dependencia del juicio humano en la detección de amenazas en tiempo real.

En tercer lugar, el camino hacia la creación de arquitecturas híbridas dinámicas representa una oportunidad de investigación

abierta. Estas arquitecturas deberían ser capaces de alternar entre métodos algorítmicos y QKD según el nivel de riesgo detectado y validadas en entornos de infraestructura real antes de su despliegue generalizado.

Finalmente, la prospectiva del campo sugiere que la integración de estos modelos inteligentes en Gemelos Digitales (Digital Twins) podría constituir una línea de validación relevante, permitiendo simular ataques de la era cuántica y evaluar la respuesta automatizada en entornos virtuales antes de su despliegue en infraestructuras críticas reales, lo que contribuiría a minimizar los posibles riesgos asociados a fallos durante la migración tecnológica.

REFERENCIAS

[1] R. Yan, Y. Wang, J. Dai, Y. Xu, and A. Q. Liu, "Quantum-Key-Distribution-Based Microgrid Control for Cybersecurity Enhancement," *IEEE Trans. Ind. Appl.*, vol. 58, no. 3, pp. 3076–3086, 2022, doi: 10.1109/TIA.2022.3159314.

[2] A. Alabdulatif, "FedCognis: An Adaptive Federated Learning Framework for Secure Anomaly Detection in Industrial IoT-Enabled Cognitive Cities," Saudi Arabia, Sep. 2025. doi: https://doi.org/10.32604/cmc.2025.066898.

[3] A. Babar, T. Halabi, and M. Zulkernine, "Autonomous and Adaptive Cyber Incident Detection and Response in Industrial Cyber-Physical Systems using Hierarchical Reinforcement Learning," ACM Transactions on Cyber-Physical Systems, Jan. 2025, doi: 10.1145/3765622.

[4] Y. Baseri, V. Chouhan, A. Ghorbani, and A. Chow, "Evaluation framework for quantum security risk assessment: A comprehensive strategy for quantum-safe transition," *Comput. Secur.*, vol. 150, Mar. 2025, doi: 10.1016/j.cose.2024.104272.

[5] R. Iqbal, M. Afzaal, and G. Rathee, "Hybrid and adaptive framework for secure and scalable authentication in healthcare IoT," *Array*, vol. 28, Dec. 2025, doi: 10.1016/j.array.2025.100527.

[6] A. K. Kar, W. He, F. C. Payton, V. Grover, A. S. Al-Busaidi, and Y. K. Dwivedi, "How could quantum computing shape information systems research – An editorial perspective and future research directions," Feb. 01, 2025, Elsevier Ltd. doi: 10.1016/j.ijinfomgt.2024.102776.

[7] A. H. El-Kady, S. Halim, M. M. El-Halwagi, and F. Khan, "Analysis of safety and security challenges and opportunities related to cyber-physical systems," *Process Safety and Environmental Protection*, vol. 173, pp. 384–413, May 2023, doi: 10.1016/j.psep.2023.03.012.

[8] M. Bandaru, S. E. Mathe, and C. Wattanapanich, "Evaluation of hardware and software implementations for NIST finalist and fourth-round post-quantum cryptography KEMs," Dec. 01, 2024, Elsevier Ltd. doi: 10.1016/j.compeleceng.2024.109826.

[9] M. Lezzi, P. Montefusco, M. Lazoi, and A. Corallo, "AI-based cybersecurity for a sustainable digital industry: Systematic literature review and future research directions," Nov. 01, 2025, Elsevier B.V. doi: 10.1016/j.jii.2025.100980.

[10] D. Lakshmi, N. Nagpal, S. Chandrasekaran, and J. H. D., "A quantum-based approach for offensive security against cyber attacks in electrical infrastructure," *Appl. Soft Comput.*, vol. 136, Mar. 2023, doi: 10.1016/j.asoc.2023.110071.

[11] D. Verchyk and J. Sepúlveda, "A practical study of post-quantum enhanced identity-based encryption," *Microprocess. Microsyst.*, vol. 99, Jun. 2023, doi: 10.1016/j.micpro.2023.104828.

[12] M. T. Naz, W. Elmedany, and M. Ali, "Securing SCADA systems in smart grids with IoT integration: A Self-Defensive Post-Quantum Blockchain Architecture," *Internet of Things (The Netherlands)*, vol. 28, Dec. 2024, doi: 10.1016/j.iot.2024.101381.

[13] C. Mangla, S. Rani, N. M. Faseeh Qureshi, and A. Singh, "Mitigating 5G security challenges for next-gen industry using quantum computing," *Journal of King Saud University - Computer and Information Sciences*, vol. 35, no. 6, Jun. 2023, doi: 10.1016/j.jksuci.2022.07.009.

[14] S. K. Singh et al., "Quantum-Resistant Cryptographic Primitives Using Modular Hash Learning Algorithms for Enhanced SCADA System Security," Computers, Materials and Continua, vol. 84, no. 2, pp. 3927–3941, 2025, doi: 10.32604/cmc.2025.059643.

[15] R. Pal, R. X. Sequeira, X. Yin, S. Zeijlemaker, and V. Kotala, "How Should Enterprises Quantify and Analyze (Multi-Party) APT Cyber-Risk Exposure in their Industrial IoT Network?," ACM Trans. Manag. Inf. Syst., Oct. 2023, doi: 10.1145/3605949.

[16] C. Ma, A. Shankar, S. Kumari, and C. M. Chen, "A lightweight BRLWE-based post-quantum cryptosystem with side-channel resilience for IoT security," *Internet of Things (The Netherlands)*, vol. 28, Dec. 2024, doi: 10.1016/j.iot.2024.101391.

[17] I. H. Sarker, H. Janicke, M. A. Ferrag, and A. Abuadbba, "Multi-aspect rule-based AI: Methods, taxonomy, challenges and directions towards automation, intelligence and transparent cybersecurity modeling for critical infrastructures," Apr. 01, 2024, Elsevier B.V. doi: 10.1016/j.iot.2024.101110.

[18] Ž. Turk, B. García de Soto, B. R. K. Mantha, A. Maciel, and A. Georgescu, "A systemic framework for addressing cybersecurity in construction," *Autom. Constr.*, vol. 133, Jan. 2022, doi: 10.1016/j.autcon.2021.103988.

[19] D. Allison, K. McLaughlin, and P. Smith, "Goosewolf: An Embedded Intrusion Detection System for Advanced Programmable Logic Controllers," *Digital Threats: Research and Practice*, vol. 4, no. 4, Oct. 2023, doi: 10.1145/3617692.

[20] C. I. Okafor, L. A. C. Ahakonye, J. M. Lee, and D.-S. Kim, "PureQuantum: Towards A Scalable Blockchain Channel Security in IoT Networks," Blockchain: Research and Applications, p. 100372, Aug. 2025, doi: 10.1016/j.bcra.2025.100372.

[21] B. Kitchenham and P. Brereton, "A systematic review of systematic review process research in software engineering," *Inf. Softw. Technol.*, vol. 55, no. 12, pp. 2049–2075, Dec. 2013, doi: 10.1016/j.infsof.2013.07.010.

[22] M. J. Page et al., "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," Mar. 29, 2021, BMJ Publishing Group. doi: 10.1136/bmj.n71.

[23] P. R. Babu, S. A. P. Kumar, A. G. Reddy, and A. K. Das, "Quantum secure authentication and key agreement protocols for IoT-enabled applications: A comprehensive survey and open challenges," Nov. 01, 2024, Elsevier Ireland Ltd. doi: 10.1016/j.cosrev.2024.100676.

[24] A. M. Aslam, A. Bhardwaj, and R. Chaudhary, "Quantum-resilient blockchain-enabled secure communication framework for connected autonomous vehicles using post-quantum cryptography," *Vehicular Communications*, vol. 52, Apr. 2025, doi: 10.1016/j.vehcom.2025.100880.

[25] S. Sadeghi, V. Chouhan, M. Aldarwbi, A. Ghorbani, A. Chow, and R. Burko, "Securing financial sector applications in the quantum era: a comprehensive evaluation of NIST's recommended algorithms through use-case analysis," *Expert Syst. Appl.*, vol. 288, Sep. 2025, doi: 10.1016/j.eswa.2025.128243.

[26] P. Singh, S. Sirpal, and O. Pal, "Cyber resilience in e-governance: A review of strategies, challenges, and directions," Sep. 01, 2025, Elsevier B.V. doi: 10.1016/j.iot.2025.101702.

[27] L. Liyanage, N. A. G. Arachchilage, and G. Russello, "SoK: Identifying Limitations and Bridging Gaps of Cybersecurity Capability Maturity Models (CCMMs)," arXiv preprint arXiv:2408.16140, 2024.

[28] S. Mohanan and N. Parameswaran, "FINER criteria – What does it mean?," *Cosmoderma*, vol. 2, p. 115, Nov. 2022, doi: 10.25259/csdm_123_2022.

[29] J. Lamp, C. E. Rubio-Medrano, Z. Zhao, and G. J. Ahn, "ExSol: Collaboratively assessing cybersecurity risks for protecting energy delivery systems," *Digital Threats: Research and Practice*, vol. 2, no. 3, Jun. 2021, doi: 10.1145/3428156.

[30] S. Y. Moon, B. H. Jo, A. El Azzaoui, S. K. Singh, and J. H. Park, "Edge-Fog Enhanced Post-Quantum Network Security: Applications, Challenges and Solutions," 2025, Tech Science Press. doi: 10.32604/cmc.2025.062966.

[31] O. O. Tooki and O. M. Popoola, "A critical review on intelligent-based techniques for detection and mitigation of cyberthreats and cascaded failures in cyber-physical power systems," Oct. 01, 2024, Elsevier Ltd. doi: 10.1016/j.ref.2024.100628.

[32] I. Kong, M. Janssen, and N. Bharosa, "Realizing quantum-safe information sharing: Implementation and adoption challenges and policy recommendations for quantum-safe transitions," *Gov. Inf. Q.*, vol. 41, no. 1, Mar. 2024, doi: 10.1016/j.giq.2023.101884.

[33] Monika and S. K. Sood, "A scientometric analysis of quantum driven innovations in intelligent transportation systems," Dec. 01, 2024, Elsevier Ltd. doi: 10.1016/j.engappai.2024.109258.

[34] R. Alguliyev, R. Aliguliyev, and L. Sukhostat, "An approach for assessing the functional vulnerabilities criticality of CPS components," *Cyber Security and Applications*, vol. 3, Dec. 2025, doi: 10.1016/j.csa.2024.100058.

[35] A. Wicaksana, "A survey on quantum-safe blockchain security infrastructure," Aug. 01, 2025, Elsevier Ireland Ltd. doi: 10.1016/j.cosrev.2025.100752.

[36] U. Song, G. Hur, S. Lee, and J. Park, "Unraveling the dynamics of the cyber threat landscape: Major shifts examined through the recent societal events," *Sustain. Cities Soc.*, vol. 103, Apr. 2024, doi: 10.1016/j.scs.2024.105265.

[37] V. Vasani, K. Prateek, R. Amin, S. Maity, and A. D. Dwivedi, "Embracing the quantum frontier: Investigating quantum communication, cryptography, applications and future directions," *J. Ind. Inf. Integr.*, vol. 39, 2024, doi: 10.1016/j.jii.2024.100594.

[38] J. Ahmad, M. Rizwan, S. F. Ali, U. Inayat, H. A. Muqeet, M. Imran, and T. Awotwe, "Cybersecurity in smart microgrids using blockchain-federated learning and quantum-safe approaches: A comprehensive review," *Appl. Energy*, vol. 393, 2025, doi: 10.1016/j.apenergy.2025.126118.

[39] A. A. Abd El-Latif, B. Abd-El-Atty, I. Mehmood, K. Muhammad, S. E. Venegas-Andraca, and J. Peng, "Quantum-Inspired Blockchain-Based Cybersecurity: Securing Smart Edge Utilities in IoT-Based Smart Cities," *Inf. Process. Manage.*, vol. 58, no. 4, Jul. 2021, doi: 10.1016/j.ipm.2021.102549.

[40] K. Jain and A. Singh, "IHKEM: A post-quantum ready hierarchical key establishment and management scheme for wireless sensor networks," *Microprocess. Microsyst.*, vol. 118, Sep. 2025, doi: 10.1016/j.micpro.2025.105205.

[41] M. M. Moslehi, "Exploring coverage and security challenges in wireless sensor networks: A survey," *Comput. Netw.*, vol. 260, Feb. 2025, doi: 10.1016/j.comnet.2025.111096.

[42] F. Trungadi, M. Fabiano, D. Aloisio, G. Brunaccini, F. Sergi, G. Merlino, and F. Longo, "Securing Modbus in legacy industrial control systems: A decentralized approach using proxies, Post-Quantum Cryptography and Self-Sovereign Identity," *J. Inf. Secur. Appl.*, vol. 94, Nov. 2025, doi: 10.1016/j.jisa.2025.104199.

[43] S. Soleimani, A. Afshar, and H. Atrianfar, "Critical component analysis of cyber-physical power systems in cascading failures using graph convolutional networks: An energy-based approach," *Sustain. Energy Grids Netw.*, vol. 42, Jun. 2025, doi: 10.1016/j.segan.2025.101653.

[44] National Institute of Standards and Technology (NIST), "Module-Lattice-Based Key-Encapsulation Mechanism Standard," Federal Information Processing Standards (NIST FIPS), NIST FIPS 203, Gaithersburg, MD, USA, Aug. 2024, doi: 10.6028/NIST.FIPS.203.

[45] National Institute of Standards and Technology (NIST), "Module-Lattice-Based Digital Signature Standard," Fed. Inf. Process. Stds. (NIST FIPS), NIST FIPS 204, Gaithersburg, MD, USA, Aug. 2024, doi: 10.6028/NIST.FIPS.204.

[46] National Institute of Standards and Technology (NIST), "Stateless Hash-Based Digital Signature Standard," Fed. Inf. Process. Stds. (NIST FIPS), NIST FIPS 205, Gaithersburg, MD, USA, Aug. 2024, doi: 10.6028/NIST.FIPS.205.

AGRADECIMIENTOS

Gracias a la Universidad del Cauca, especialmente al grupo de investigación GTI y a la Universidad de Antioquia y su grupo In2lab por proporcionar los recursos y el apoyo para el desarrollo de esta propuesta.

FINANCIACIÓN

Ninguna

CONFLICTOS DE INTERÉS

No existen

CONTRIBUCIÓN DE AUTORÍA

Redacción - borrador original: Katerine Márceles Villalba, César Jesús Pardo Calvache, Siler Amador Donado.

Redacción - revisión y edición: Katerine Márceles Villalba, César Jesús Pardo Calvache, Siler Amador Donado.