UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Tecnura

https://revistas.udistrital.edu.co/index.php/Tecnura/issue/view/1327

DOI: https://doi.org/10.14483/22487638.24853

REVISIÓN

Ciberseguridad cuántica en sistemas ciberfísicos e infraestructuras críticas: un estado del arte

Quantum Cybersecurity in Cyber-Physical Systems and Critical Infrastructures: A State of the Art

Katerine Márceles Villalba [1], César Pardo Calvache [2] y Siler Amador Donado [3]

Fecha de Recepción: 12 de noviembre de 2025 **Fecha de Aceptación**: 12 de marzo de 2026

Cómo citar: K.M. Villalba, C. Pardo Calvache, S.A. Donado, «Ciberseguridad cuántica en sistemas ciberfísicos e infraestructuras críticas: un estado del arte», *Tecnura*, vol. 30, n.° 88, jun. 2026. 85–101. https://doi.org/10.14483/22487638.24853

Resumen

Contexto: este artículo presenta la creciente vulnerabilidad de los sistemas ciberfísicos en las infraestructuras críticas, producto del avance de la computación cuántica. Esta tecnología pone en entredicho los esquemas actuales de criptografía y coloca en riesgo servicios como la energía, la salud y otros esenciales para la sociedad.
Objetivo: caracterizar los estándares, marcos de trabajo y las vulnerabilidades emergentes encontradas en estudios científicos publicados en el período 2020-2025.
Metodología: marco metodológico basado en una revisión sistemática de la literatura, utilizando los protocolos PRISMA y Kitchenham. A través de este método, se eligieron un total de 40 estudios primarios.
Resultados: la revisión evidencia que, aunque normativas como ISO/IEC 27001 e IEC 62443 son ampliamente adoptadas, carecen de medidas de control específicas frente a amenazas cuánticas como los algoritmos de Shor y Grover. Asimismo, se identificó una desconexión entre los modelos taxonómicos actuales y la protección técnica de activos operativos.
Conclusiones: la investigación concluye que existe una urgencia por integrar la criptografía postcuántica y desarrollar marcos de gobernanza adaptativa que fortalezcan la resiliencia en las infraestructuras críticas. Finalmente, se propuso una hoja de ruta para la creación de modelos ontológicos que unifiquen la gestión de riesgos en esta era tecnológica.
Palabras clave: Ciberseguridad, Cuántica, Infraestructuras críticas, sistemas ciber-físicos.

Abstract

Context: This article presented the growing vulnerability of cyber-physical systems (CPS) in critical infrastructures resulting from the advancement of quantum computing. This technology challenges current cryptographic schemes and puts services such as energy, healthcare, and other essential social sectors at risk.

1 Ingeniera de Sistemas y Magíster en Seguridad Informática. Miembro del grupo de investigación In2Lab. Universidad de Antioquia. Email: katerine.marceles@udea.edu.co

2 Ingeniero de Sistemas y PhD. en Tecnologías Informáticas Avanzadas. Miembro del grupo de investigación GTI. Universidad del Cauca. Email: cpardo@unicauca.edu.co

3 Ingeniero de Sistemas y PhD. (c) Ciencias de la Computación. Miembro del grupo de investigación GTI. Universidad del Cauca. Email: samador@unicauca.edu.co

Objective: The goal was to characterize the standards, frameworks, and emerging vulnerabilities found in scientific studies published during the 2020-2025 period.
Methodology: The study was conducted through a methodological framework based on a systematic literature review using the PRISMA and Kitchenham protocols. Through this method, a total of forty primary studies were selected.
Results: The analysis evidenced that , although standards such as ISO/IEC 27001 and IEC 62443 are widely adopted, they lack specific control measures against quantum threats such as the Shor and Grover algorithms. Furthermore, a disconnection was identified between current taxonomic models and the technical protection of operational assets.
Conclusions: The research concluded that there is an urgent need to integrate post-quantum cryptography and develop adaptive governance frameworks to strengthen resilience in critical infrastructures. Finally, a roadmap was proposed for the creation of ontological models to unify risk management in this technological era.
Keywords: Cybersecurity, Critical Infrastructures, Cyber-physical systems, Quantum.

Introducción

La ciberseguridad en infraestructuras críticas (IC) se ha consolidado como campo estratégico para garantizar la continuidad y la estabilidad de servicios esenciales en la sociedad [1]. Infraestructuras como la energética, la sanitaria, las de agua o transporte están cada vez más integradas con sistemas ciber-físicos (SCF) que articulan componentes digitales y físicos para el monitoreo y control automatizado de procesos [2]. Los SCF son entornos en los cuales los sistemas computacionales interactúan con procesos físicos mediante sensores, actuadores y redes de comunicación, lo que los hace fundamentales, pero altamente vulnerables ante ciberataques. De hecho, esta integración ha ampliado la superficie de ataque y ha aumentado la exposición ante amenazas que pueden impactar tanto los sistemas de información como los dispositivos físicos que controlan entornos sensibles [3]. A pesar de su importancia, la protección de los SCF en entornos críticos aún presenta desafíos metodológicos y técnicos significativos. Actualmente es posible observar la falta de marcos formales de evaluación, así como de metodologías para la prevención de ataques avanzados [4].

La computación cuántica, entendida como un paradigma que utiliza principios de la mecánica cuántica para procesar información, ha generado nuevas amenazas en términos de ciberseguridad, ya que pone en riesgo los algoritmos criptográficos actuales. En particular, el algoritmo de Shor permite factorizar números grandes en tiempo polinomial, comprometiendo la seguridad de sistemas como RSA (Rivest-Shamir-Adleman) y ECC (Criptografía de Curva Elíptica), mientras que el algoritmo de Grover reduce drásticamente el tiempo de búsqueda en claves simétricas, lo cual afecta la fortaleza de mecanismos como AES (Advanced Encryption Standard)[4], [14].

La aparición de nuevas tecnologías disruptivas, como la computación cuántica, abre una línea de riesgo emergente para los mecanismos criptográficos tradicionales, especialmente en contextos en los cuales la seguridad y la disponibilidad son requisitos no negociables. Esto genera la necesidad revisar las medidas de seguridad, no solo desde una perspectiva técnica, sino también desde la planificación

estratégica al interior de las IC. Por tanto, la ausencia de una visión articulada de los SCF y las amenazas cuánticas ha desencadenado una serie de riesgos en el desarrollo de nuevas políticas, tecnologías y prácticas.

Entre estos riesgos se destacan: (i) decisiones de seguridad basadas en artefactos obsoletos [1], [10], [26], (ii) la subestimación de las vulnerabilidades emergentes [4], [14], (iii) la ausencia de estándares de protección cuántica [13], [15], (iv) inversiones en soluciones no escalables [13], [12], [26], (v) el diseño de infraestructuras centrado en la seguridad no postcuántica [4], [14], [24], (vi) la desarticulación entre sectores industriales y científicos [10], [13], [27], (vii) las limitaciones para generar respuestas resilientes [9], [22], [28]. Durante los últimos años se han realizado estudios relevantes que exploran temas como la seguridad en SCF, el uso de inteligencia artificial para defensa, y la criptografía resistente a computadoras cuánticas. En virtud de ello, revisiones previas como las de Amador et al. [24] y Borja Rivadeneira y Gómez [25] evidenciaron que aún son escasos los estudios que integran de forma articulada los tres dominios: SCF, IC y ciberseguridad cuántica, lo que constituye una brecha en el conocimiento actual.

Por consiguiente, este artículo se enfoca en la estructuración del estado del arte, basado en la necesidad de comprender la seguridad de SCF en IC ante la llegada de la era cuántica. Dado a lo anterior, el objetivo principal fue caracterizar los estándares, marcos de trabajo y vulnerabilidades emergentes reportadas en la literatura científica (comprendida entre los periodos 2020–2025) sobre ciberseguridad cuántica en SCF e IC, identificando brechas, patrones y enfoques metodológicos predominantes. Para ello, se siguió un protocolo híbrido basado en PRISMA 2020 [5] y en las directrices metodológicas de Kitchenham [6].

El resto del artículo se estructura así: la Sección 2 describe el protocolo metodológico; la Sección 3 presenta los resultados obtenidos; la Sección 4 desarrolla la discusión y limitaciones a partir de los hallazgos y la Sección 5 presenta las conclusiones y proyecciones futuras.

Metodología

Para la estructuración del estado del arte se adoptó un protocolo híbrido fundamentado en los lineamientos metodológicos de Kitchenham y Brereton [6] y PRISMA 2020 [5], complementado con el modelo GQM (Goal-Question-Metric). Este enfoque combina la rigurosidad conceptual del primero, orientado a la ingeniería del conocimiento, con la trazabilidad y transparencia del segundo, propio de revisiones en ciencias aplicadas. De esta manera, se minimizaron los sesgos en la formulación de preguntas, la selección de fuentes, la evaluación de pertinencia y la delimitación de objetivos. En el siguiente repositorio en Zenodo: https://doi.org/10.5281/zenodo.16944681, se presenta gráficamente el flujo de actividades realizadas durante la revisión. La metodología abordó literatura científica publicada entre los años 2020 y 2025, y se focalizó en estudios que articulan la intersección entre SCF, ciberseguridad e

impactos de la computación cuántica en IC. A pesar del esfuerzo por priorizar literatura revisada por pares, la escasez de investigaciones específicas sobre ciberseguridad cuántica en SCF e IC requirió complementar la búsqueda con fuentes emergentes de alto impacto, lo que permitió fortalecer la caracterización del dominio estudiado.

Las actividades desarrolladas en cada etapa del protocolo aplicadas al tema de dominio central fueron:

- *Objetivo de búsqueda y preguntas de investigación:* el objetivo (Ob) principal de este estado del arte fue analizar los estándares, marcos de trabajo y prácticas de ciberseguridad aplicados a SCF e IC, con el fin de caracterizar los requerimientos asociados con la gestión de las amenazas en la era cuántica. Para ello, se establecieron los siguientes objetivos de búsqueda:

Ob1: caracterizar los tipos de estándares y marcos de trabajo aplicados a SCF e IC mediante una búsqueda estructurada en bases académicas relevantes.

Ob2: identificar vulnerabilidades emergentes derivadas de la computación cuántica que afectan a SCF e IC a partir de una revisión de literatura.

Las preguntas que guiaron el desarrollo del estado del arte se formularon bajo el método Goal-Question-Metric (GQM) [6] presentados en la Tabla 1, combinando los criterios de refinamiento del enfoque PICOC [7] y la validación mediante FINER[8], lo que garantizó su viabilidad, interés y relevancia. Las preguntas fueron validadas por expertos antes de ser aplicadas y respondidas con el análisis de los estudios primarios.

Tabla 1. *Pregunta, métrica y motivación.*

ID	Pregunta	Métrica	Motivación
Ob1.	P1: ¿Cuáles son los principales estándares y marcos de trabajo utilizados en la ciberseguridad de SCF y IC?	Número de estándares y marcos de trabajo documentados que abordan la ciberseguridad en SCF e IC.	Identificar los marcos de referencia permite establecer las bases normativas y técnicas sobre las cuales se construyen las prácticas de seguridad actuales, y evaluar su pertinencia ante nuevos desafíos como la era cuántica.
Ob2.	P2: ¿Qué vulnerabilidades asociadas con la computación cuántica están emergiendo en la ciberseguridad de SCF e IC?	Número de vulnerabilidades cuánticas identificadas en el contexto de ataques de red a SCF e IC.	Comprender las vulnerabilidades emergentes asociadas a la computación cuántica para anticipar riesgos futuros.

Abreviaciones utilizadas: Objetivo (Ob), Pregunta (P).

Fuente: elaboración propia.

- *Búsqueda de literatura:* las fuentes de búsqueda seleccionadas fueron: *Scopus*, *Springer* y *Google Scholar*, escogidas por su pertinencia temática, disponibilidad de literatura actualizada y revisada por pares. Google Scholar se utilizó para acceder a investigaciones emergentes, debido a su cobertura y acceso abierto, lo que facilitó una búsqueda amplia y estructurada, así como el rastreo de estudios relevantes mediante funciones de citación, filtros por año y tipo de documento. En consecuencia, este enfoque permitió acceder a investigaciones que, aunque no siempre registradas en las bases principales, sí estaban revisadas por pares y vinculadas a dominios especializados de SCF y ciberseguridad cuántica.

La Tabla 2 presenta la cadena de búsqueda básica , construida a partir de los términos clave definidos en el protocolo y optimizada según el esquema PICOC. En el siguiente repositorio en Zenodo: https://doi.org/10.5281/zenodo.17129173 se presenta el PICOC definido para la cadena de búsqueda de este estado del arte.

Tabla 2. *Cadena de búsqueda básica.*

"cyber-physical systems" **OR** "CPS" **AND** "cybersecurity evaluation model" **OR** "ontology evaluation model" **OR** "assessment model" **OR** "quantum cybersecurity model" **AND** "best practices" **OR** "cybersecurity frameworks" **AND** "quantum era" **OR** "critical infrastructure"

Fuente: elaborción propia.

La cadena de búsqueda se adaptó cuidadosamente para cada fuente seleccionada, para garantizar la consistencia en el uso de operadores booleanos y la compatibilidad con los parámetros específicos de cada buscador. En el repositorio disponible en Zenodo (https://doi.org/10.5281/zenodo.17545367) se puede consultar la versión específica de la cadena para cada plataforma. Durante el proceso, se identificaron un total de 420 artículos. De estos, se eliminaron 7 por duplicación, quedando 413. Posteriormente, se evaluaron preliminarmente por título y resumen, con lo cual se redujo el conjunto a 140 artículos. Finalmente, tras aplicar los criterios de inclusión y exclusión definidos en la Tabla 3, se seleccionaron 64 estudios relevantes.

La distribución de artículos por fuente fue: Google Scholar: 256 identificados, 130 incluidos preliminarmente, 54 relevantes; Springer: 89 identificados, 10 relevantes; Scopus: 75 identificados, 0 relevantes. Este resultado reflejó dos aspectos clave: por un lado, la escasa representación de literatura especializada en ciberseguridad cuántica dentro de bases como Scopus; y por otro, la importancia de incluir buscadores más amplios como Google Scholar en revisiones sistemáticas sobre áreas en rápido desarrollo.

Cabe resaltar que varios artículos identificados en Google Scholar provenían de congresos de alto impacto y revistas indexadas no necesariamente cubiertas por Scopus, lo cual refuerza su valor como repositorio complementario. De esta forma, se garantizó la cobertura de literatura emergente relevante en dominios como criptografía post-cuántica y evaluación ontológica aplicada a SCF e IC.

Tabla 3. 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 - 2025	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: elaboración propia.

Tras la aplicación de los criterios de inclusión, de 420 artículos iniciales se obtuvieron 64 artículos finales relevantes, lo que corresponde aproximadamente a un 15.2%, (Figura 1).

La selección de los estudios se realizó mediante un proceso secuencial y validado, en el cual un primer revisor efectuó la identificación y preselección inicial, seguida de una revisión independiente por un segundo evaluador experto. Para asegurar la objetividad del proceso, no se calculó el coeficiente Kappa, sino que se aplicó una matriz de valoración estructurada que permitió estimar el grado de acuerdo entre revisores con base en criterios definidos. Cada artículo fue evaluado utilizando una tabla de valoración por criterios de inclusión, donde se asignaron los siguientes puntajes: 1 (Cumple – Nivel Bueno), 0.5 (Cumple parcialmente – Nivel Regular) y 0 (No cumple – No pertinente). Este sistema de ponderación permitió cuantificar la pertinencia de los artículos y establecer umbrales mínimos para su selección (≥ 0.75), lo que garantizó un proceso sistemático, reproducible y libre de sesgos individuales.

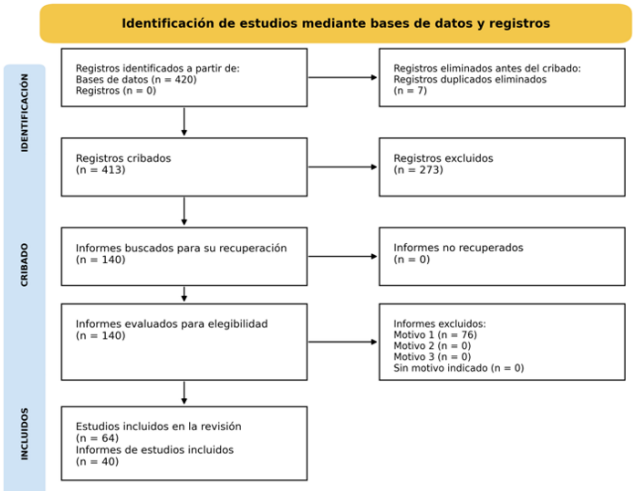

Figura 1. Proceso de selección de los estudios primarios.

Fuente: elaboración propia.

- *Evaluación de pertinencia:* para seleccionar los estudios primarios, se aplicó una metodología basada en cuatro categorías: claridad, rigor, relevancia y credibilidad, inspirada en el enfoque de Kitchenham et al. [6]. Esta herramienta permitió una evaluación cualitativa y cuantitativa, lo que facilitó la identificación de estudios pertinentes y la detección de posibles sesgos en la selección. Cada artículo fue calificado en una escala de 1 a 3 por criterio, distribuidos en las siguientes categorías: Claridad (2 criterios), Rigor (4 criterios), Relevancia (2 criterios) y Credibilidad (2 criterios), para un total de 10 criterios evaluativos por artículo. Por tanto, el puntaje total posible por artículo osciló entre 10 y 30 puntos, siendo convertido a una escala de promedio entre 1 y 3 para facilitar la comparación.

Los criterios de evaluación utilizados son:

- **Claridad:** eelevancia temática y aporte del estudio al campo.

- **Rigor:** objetivo explícito, metodología adecuada, replicabilidad del entorno experimental y representatividad de los datos.

- **Relevancia:** aplicabilidad al dominio de SCF e IC, y posibilidad de proyección a investigaciones futuras.

- **Credibilidad:** discusión metodológica clara y resultados comprensibles.

Se estableció un umbral mínimo de aceptación de 2.75 sobre 3 como promedio general, lo que garantizó la inclusión de estudios con una significativa calidad metodológica y pertinencia temática. Las exclusiones fueron justificadas documentalmente, con el fin de garanrtizar transparencia en el proceso. Como resultado, 40 artículos cumplieron con los criterios establecidos y fueron incluidos como estudios primarios (ver Figura 1). La lista completa está disponible en Zenodo: https://doi.org/10.5281/zenodo.16945744.

Cabe mencionar que se descartaron todos los artículos provenientes de Scopus (n = 75), al no alcanzar los umbrales mínimos de pertinencia contextual, profundidad técnica y/o enfoque explícito en ciberseguridad cuántica aplicada a SCF e IC.

- *Extracción de datos:* se realizó con base en las preguntas y los objetivos definidos en la primera etapa, a través de un instrumento que incluyó campos como ID del artículo, título, fuente, resumen, puntajes por criterio —claridad, rigor, relevancia, credibilidad— y puntaje total. Esto permitió identificar estándares aplicados a SCF e IC, así como vulnerabilidades emergentes relacionadas con la computación cuántica, los cuales fueron insumos claves. Para garantizar la validez de los hallazgos, se aplicó un análisis de certeza de la evidencia considerando criterios como reputación de la fuente (priorizando bases indexadas), claridad metodológica, pertinencia temática en el dominio cuántico de SCF en IC y revisión por pares. Aunque no

se utilizó formalmente el sistema GRADE (marco metódico usado internacionalmente para evaluar la calidad de la evidencia y determinar la fuerza de las recomendaciones en revisiones sistemáticas) se adoptó una clasificación equivalente: alta, media y baja, documentada en la matriz de extracción, la cual se puede consultar en el siguiente enlace en Zenodo: https://doi.org/10.5281/zenodo.17540633. Esta evaluación permitió filtrar estudios especulativos y priorizar evidencia robusta y confiable.

- *Síntesis y análisis de resultados:* el análisis mostró un aumento progresivo en la producción académica sobre ciberseguridad cuántica, con el año 2024 como aquel de mayor producción como se muestra en la Figura 2. Este crecimiento refleja el interés creciente en el impacto de la computación cuántica sobre las IC. Por otra parte, el análisis de palabras claves reveló una alta frecuencia en términos como: "ciberseguridad", "cuántico", "infraestructura crítica", "ontología" y "frameworks de ciberseguridad", agrupados en la Figura 3. Las palabras clave "infraestructura crítica" y "sistemas ciberfísicos (CPS)" fueron las más recurrentes, cada una con una frecuencia del 29,4%, lo que evidencia una fuerte orientación temática hacia la seguridad de entornos industriales complejos. También destacan los términos "mejores prácticas" (14,7%) y "ontología" (13,7%), lo que sugiere un creciente interés por enfoques estructurados de gestión del conocimiento y aplicación de marcos normativos. No se realizó análisis de subgrupos debido a la heterogeneidad metodológica, lo que se reconoce como una limitación y oportunidad para investigaciones futuras más específicas por sector o región.

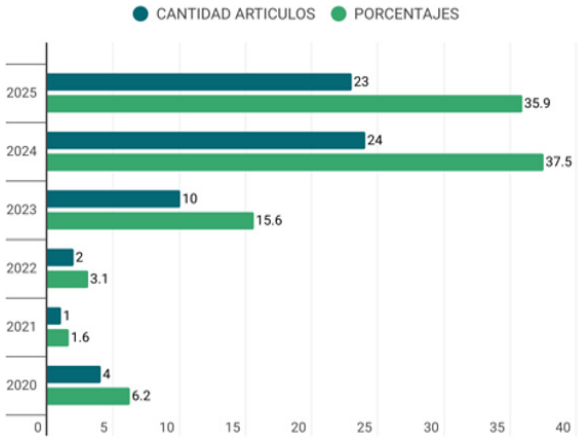

Figura. 2. Cantidad de artículos publicados por año

Fuente: elaboración propia.

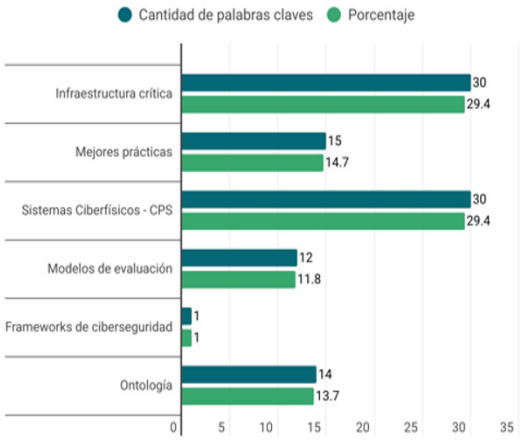

Figura. 3. Frecuencia de palabras claves en los estudios primarios

Fuente: elaboración propia.

Resultados

A continuación, se responden las preguntas de investigación formuladas que orientaron el estado del arte.

P1: ¿Cuáles son los principales estándares y marcos de trabajo utilizados en la ciberseguridad de SCF e IC?

A partir de la revisión realizada, se identificaron diversos marcos y estándares adoptados por organizaciones vinculadas con las IC. Los análisis mostraron una tendencia hacia la aplicación de marcos basados en estándares, muchos de ellos certificables, lo cual favorece el cumplimiento normativo y la seguridad organizacional [1], [9], [10].

Entre los marcos más destacados se encuentran NIST e IEC 62443, reconocidos por su disponibilidad documental y facilidad de acceso. No obstante, la implementación del IEC 62443 presenta desafíos técnicos y económicos, ya que demanda personal con la preparación, lo cual puede limitar su adopción, especialmente en pymes [1], [9], [10]. Por otro lado, se ha evidenciado un incremento en la adopción del estándar ISO/IEC 27001 debido a su flexibilidad y enfoque adaptable a múltiples sectores, especialmente a través de la implementación de controles del Anexo A (documento normativo o guía que apoya la implementación de los controles de seguridad establecidos en la norma ISO 27001) [11], [12], [13]. Mientras tanto, IEC 62443 y NIST SP 800-82 se utilizan más en sectores industriales como energía y manufactura. En cuanto a la adopción por regiones, los estudios señalan que en Estados Unidos predominan NIST SP 800-82 y NIST CSF, en parte por exigencias regulatorias. En Europa, se emplean ampliamente IEC 62443 e ISO/IEC 27001, asociados también con normativas como GDPR [11], [12], [13], [2]. En Asia y Oriente Medio se observa una integración creciente de ISO/IEC 27001 junto con IEC 62443, mientras que en Latinoamérica aumenta la aplicación de ISO/IEC 27001 por presión de regulaciones gubernamentales. A pesar de su popularidad, la aplicación práctica de estos marcos varía según factores como el tamaño de la empresa, cultura organizacional y la disponibilidad de recursos.

Los principales desafíos se centran en la implementación técnica, especialmente en normas como IEC 62443, debido a su complejidad técnica, necesidad de interoperabilidad entre sistemas legados y nuevos y el alto costo asociado a su adopción en infraestructuras críticas. En contraste, ISO/IEC 27001 tiende a ser más accesible para diferentes tamaños de organizaciones debido a su estructura modular y sus guías de implementación más flexibles.

En términos de frecuencia, ISO/IEC 27001 fue referenciado porel 27% de los estudios primarios, seguido por IEC 62443 (22%) y NIST SP 800-82 (18%). Otras normativas como NIST CSF, ISO/IEC 27019 y el marco COBIT también fueron identificadas, aunque con menor presencia porcentual.

La Tabla 4 presenta la frecuencia de aparición de los principales marcos normativos en los estudios analizados entre 2020 y 2025, lo que permite observar el liderazgo de ISO/IEC 27001, seguido por IEC 62443 y NIST SP 800-82 como los más representativos en el dominio de SCF e IC.

Tabla 4. *Análisis comparativo de estándares y marcos normativos aplicados a SCF e IC (2020–2025).*

Marco Normativo	Frecuencia de aparición	% de estudios	Sectores de Aplicación	Ventajas	Limitaciones
ISO/IEC 27001	18	27%	Multisectorial	Flexible, adaptable, certificable	Puede requerir ajustes específicos para entornos industriales
IEC 62443	15	22%	Industria, energía, manufactura	Alta especificidad técnica	Complejidad técnica y alto costo de implementación
NIST SP 800-82	12	18%	Industria, energía	Enfoque técnico en ICS	Menor adopción fuera de EE.UU.
NIST CSF	9	14%	Gobierno, servicios públicos	Claridad y alineación con políticas públicas	Enfocado en contexto estadounidense
ISO/IEC 27019	7	11%	Energía eléctrica	Adaptado a sistemas de gestión energética	Aplicación más restringida a sector energético
COBIT	3	5%	TI y gobernanza corporativa	Integración con gobierno de TI	No especializado en ciberseguridad industrial o cuántica
No aplica	-	3%	-	-	-

Fuente: elaboración propia.

P2: ¿Qué vulnerabilidades asociadas con la computación cuántica están emergiendo en la ciberseguridad de SCF e IC?

La computación cuántica introdujo nuevas vulnerabilidades en los SCF e IC, lo cual afectó especialmente a los algoritmos criptográficos tradicionales como RSA y ECC (algoritmos de clave pública o asimétrica), que son vulnerables ante el algoritmo cuántico de Shor (algoritmo para factorizar números grandes) [14], [15], [16], [17]. Asimismo, el algoritmo cuántico de Grover (algoritmo para la búsqueda en una secuencia no ordenada de datos con N componentes) reduce la seguridad de los algoritmos simétricos [14], [17]. Se destaca también las debilidades en sistemas heredados como SCADA (Supervisory Control And Data Acquisition), que presentan dificultades de actualización [13], [18], y los riesgos en la cadena de suministro por componentes vulnerables [19]. Los protocolos de autenticación y distribución de claves como Diffie-Hellman también son susceptibles a ataques cuánticos [17], [20]. Además, se evidenció el surgimiento de amenazas vinculadas con inteligencia artificial (IA) y modelos de lenguaje, incluyendo técnicas como: inyección de prompts, *jailbreaking* y *backdoors* [21], [22]. Los ataques más frecuentes incluyen: ataques cuánticos (Shor y Grover), ataques a QKD (Distribución de Clave Cuántica), y amenazas tradicionales como: *ransomware*, *malware*, DoS/DDoS e ingeniería social siguen aún vigentes [3], [10], [23], [24]. Frente a este panorama, varios estudios recomiendan la migración urgente a algoritmos postcuánticos, la protección de activos de tecnología de la operación (TO) y la gestión de amenazas internas [14], [18], [24], [25].

Para clarificar la naturaleza y el impacto de estas vulnerabilidades, se estructuró una categorización comparativa que agrupa los hallazgos en cinco dominios clave: criptográficas, de comunicación, de dispositivos/IoT, humanas y de terceros.La Tabla 5 resume esta clasificación y establece para cada categoría

el tipo de vulnerabilidad más relevante, su causa raíz, su impacto directo sobre la tríada de la seguridad (confidencialidad, integridad, disponibilidad) y un ejemplo representativo extraído de los estudios revisados.

Esta tabla facilita la lectura transversal del problema al conectar las vulnerabilidades emergentes con escenarios específicos de amenaza y permite identificar patrones comunes, como la recurrencia de debilidades en infraestructuras heredadas, la presión regulatoria para adoptar nuevos protocolos, o la falta de controles para mitigar riesgos provenientes de proveedores externos. Las vulnerabilidades identificadas se agruparon en cinco categorías y estas se alinean con la tríada de seguridad: confidencialidad, integridad y disponibilidad [25], [26], [27], [28]. También se evidenció que las investigaciones analizaron y aplicaron ontologías y taxonomías especializadas como CVO (*Conceptual Vulnerability Ontology*) y TRACI (*Taxonomy for Risk Assessment of Cyberattacks on Critical Infrastructure*), las cuales fueron utilizadas para clasificar los ataques con base en los activos comprometidos, los riesgos asociados y las motivaciones subyacentes. Estas herramientas conceptuales permitieron estructurar el conocimiento sobre amenazas emergentes en entornos críticos, facilitando una mejor comprensión de los vectores de ataque en función del contexto operacional de los SCF e IC [25], [26], [27].

Por último, se identificaron múltiples causas subyacentes a las vulnerabilidades descritas: los avances en computación cuántica, la persistencia de sistemas heredados con limitadas capacidades de actualización, los errores humanos durante procesos operativos, la ausencia de estándares unificados en entornos industriales y las restricciones presupuestales y técnicas que dificultaron la migración a esquemas de criptografía postcuántica [16], [18], [25]. Las consecuencias reportadas en la literatura incluyeron la exposición de datos sensibles, la interrupción de servicios críticos, daños físicos en infraestructuras estratégicas y el deterioro de la reputación institucional ante brechas de seguridad [17], [19], [23].

Tabla 5. *Categorización comparativa de vulnerabilidades emergentes en SCF e IC frente a la computación cuántica.*

Categoría	Tipo de vulnerabilidad	Causa raíz	Impacto principal	Ejemplo representativo
Criptográfica	Ruptura de algoritmos RSA, ECC y AES	Algoritmos cuánticos (Shor, Grover)	Compromiso de la confidencialidad	Ataques a certificados digitales
Comunicación	Intercepción de canales QKD, Diffie-Hellman	Debilidades en protocolos	Pérdida de integridad de datos	Suplantación de identidad remota
Dispositivos/IoT	Dispositivos heredados, sin actualizaciones	Limitaciones en SCADA y TO antiguos	Interrupción de servicios críticos	Falla en sensores de planta eléctrica
Humanas	Ingeniería social, mal uso de IA	Errores humanos o manipulación	Acceso no autorizado o fuga de datos	Inyección de prompts en IA
Terceros	Suministro de componentes no confiables	Dependencia de proveedores externos	Pérdida de disponibilidad o sabotaje	***Firmware* modificado en routers**

Fuente: elaboración propia.

Discusión y limitaciones: los resultados de la revisión mostraron que, si bien existen marcos internacionales consolidados en ciberseguridad para IC, el surgimiento de la computación cuántica plantea retos inéditos. Estos desafíos aún no han sido abordados integralmente en la literatura reciente. En particular, se evidenció una escasa articulación entre los enfoques de seguridad cuántica y los modelos ontológicos o taxonómicos existentes, lo que limita el desarrollo de herramientas semánticas avanzadas. Los hallazgos revelan que, aunque existen ontologías como CSO [25] y TRACI [26], su aplicación en contextos cuánticos aún es incipiente. Esto limita su utilidad para afrontar amenazas emergentes en SCF e IC.

La mayoría de los estudios revisados se centraron en componentes técnicos o criptográficos, dejando de lado las dimensiones organizacionales, regulatorias y humanas. Esta concentración temática puede dificultar la implementación de soluciones holísticas, especialmente en sectores donde la operación confiable de los Sistemas Ciberfísicos (SCF) resulta esencial para la estabilidad nacional, como los de energía, transporte y salud.

Asimismo, se observó que los trabajos con mayor profundidad técnica y alcance institucional fueron desarrollados en contextos del hemisferio norte, particularmente en Estados Unidos, Europa y Asia. En contraste, en Latinoamérica se identificaron esfuerzos aún emergentes, lo que evidencia la necesidad de consolidar agendas regionales de investigación orientadas hacia la transición postcuántica y de fortalecer capacidades institucionales para la adaptación de estándares internacionales. Este hallazgo coincide con lo expuesto por Liyanage *et al.* [7] quienes destacan la asimetría en la adopción de marcos de madurez y evaluación de capacidades de ciberseguridad a nivel global.

Se identificó como hallazgo clave la necesidad de cooperación internacional en el desarrollo de ontologías y taxonomías adaptadas a amenazas tradicionales y cuánticas en IC y SCF. Además, se subraya la urgencia de integrar los conceptos clave entre dominios, evitando la fragmentación conceptual que limita el avance del campo.

En esta línea, algunos avances preliminares han sido formulados en estudios como los de Amador *et al.* [24], quienes realizaron una revisión sistemática sobre SCF, IC y ciberseguridad cuántica; Plachkinova y Vo con su taxonomía TRACI [26]; Martins et al. con un marco conceptual para la caracterización de ontologías en ciberseguridad [27]; y Kozlenko , quien propone una ontología difusa para la evaluación de riesgos y el impacto de ataques [28]. Sin embargo, estos desarrollos permanecen en fases iniciales y dispersas, lo cual es un obstáculo para su adopción industrial y su integración en marcos regulatorios consolidados. Cabe aclarar, que todos los estudios citados forman parte del conjunto de 40 artículos analizados en esta revisión sistemática, los cuales se encuentran documentados en el repositorio Zenodo (https://doi.org/10.5281/zenodo.17540633). Aunque no todos se mencionan explícitamente en el cuerpo del texto, han contribuido directamente en distintas etapas del trabajo, ya sea como soporte de las preguntas de investigación, en la construcción del marco teórico o en la fundamentación metodológica del estudio.

Otro aspecto que emergió con fuerza fue la ausencia de mecanismos estandarizados de interoperabilidad entre sistemas ontológicos aplicados a IC y SCF, lo cual limita la integración de herramientas automatizadas en entornos operativos reales. Esta limitación afecta directamente la capacidad de anticipación, correlación y respuesta coordinada frente a amenazas avanzadas, particularmente aquellas potenciadas por algoritmos cuánticos o técnicas de inteligencia artificial maliciosa. Desde una perspectiva práctica y política, los resultados evidencian la necesidad de formular estrategias nacionales e internacionales que promuevan la estandarización semántica, la inversión en infraestructura de ciberseguridad postcuántica y la formación de talento humano especializado. Esto implica también el fortalecimiento de marcos de gobernanza digital adaptativa, que permitan responder de manera flexible a la evolución acelerada del riesgo tecnológico, garantizando resiliencia institucional y la protección de activos críticos.

Finalmente, los hallazgos fueron interpretados considerando las principales limitaciones del estudio. En primer lugar, la disponibilidad de literatura científica reciente en bases indexadas de acceso abierto pudo haber restringido la incorporación de ciertos estudios relevantes. En segundo lugar, la ausencia de resultados relevantes en *Scopus* evidencia la subrepresentación de la temática en repositorios académicos tradicionales, lo que refuerza la importancia de integrar buscadores amplios como *Google Scholar* para garantizar una cobertura más inclusiva en campos de investigación emergentes. Asimismo, la heterogeneidad metodológica de los estudios incluidos impidió realizar análisis cuantitativos o metaanálisis estadísticos; sin embargo, la síntesis cualitativa obtenida proporciona una base sólida para avanzar hacia modelos de evaluación integrales, contextualizados y validados empíricamente en el dominio de la ciberseguridad cuántica aplicada a infraestructuras críticas.

Conclusiones

Este trabajo permitió identificar una baja integración entre los modelos taxonómicos, ontológicos y la ciberseguridad cuántica, especialmente en el contexto de IC y SCF. La mayoría de los estudios se enfocó en aspectos técnicos, dejando de lado dimensiones organizacionales y regulatorias necesarias para enfrentar riesgos emergentes. Los hallazgos mostraron que, si bien existen avances en la formulación de marcos y modelos orientados a la protección de los sistemas ciberfísicos, aún no se ha consolidado un enfoque holístico que articule conceptos ontológicos, criterios de gobernanza y mecanismos de adaptabilidad frente al entorno cuántico. En particular, se evidenció una fragmentación entre las propuestas dirigidas a la protección de activos, la evaluación de riesgos y la gestión institucional, lo cual limita la construcción de políticas públicas y planes estratégicos con enfoque integral. En respuesta, se propone como trabajo futuro una de ruta en tres fases. Estas tres fases fueron sintetizadas en la Tabla 6, la cual permite visualizar el tránsito progresivo desde la conceptualización semántica, pasando por el diseño institucional, hasta la validación contextual de las propuestas. Este esquema busca orientar la futura investigación y el desarrollo de soluciones prácticas, particularmente en sectores industriales sensibles como energía, salud o transporte.

La primera fase plantea el desarrollo del Modelo Ontológico de Resiliencia Ciber-Cuántica (MORCC), orientado a representar, mediante estructuras semánticas, las relaciones entre activos críticos, tipos de amenazas (clásicas y cuánticas) y capacidades de respuesta. La segunda fase propone el diseño del Marco de Gobernanza Adaptativa Cuántica (MGAC), que articula políticas, roles institucionales y procesos de toma de decisiones frente a riesgos emergentes en SCF e IC. La tercera fase contempla la ejecución de estudios piloto en sectores priorizados, con el fin de validar empíricamente los modelos propuestos. Esta etapa incluiría una evaluación sistemática mediante indicadores comocobertura de amenazas, capacidad de respuesta, interoperabilidad semántica y alineación con marcos regulatorios nacionales o internacionales.

Tabla 6. *Ruta para el desarrollo de un modelo ontológico y marco de gobernanza adaptativa cuántica.*

Fase	Nombre	Objetivo	Resultados esperados
1	MORCC	Diseñar un modelo ontológico que represente relaciones entre activos, amenazas cuánticas y capacidades de defensa en IC y SCF.	Ontología formalizada y repositorio de conceptos normalizados.
2	MGAC	Proponer un marco de gobernanza adaptativa cuántica para guiar respuestas organizacionales y normativas.	Directrices y políticas para respuesta institucional en contextos críticos.
3	Validación en casos de estudio	Implementar los modelos en entornos reales o simulados y evaluar su impacto.	Evidencia empírica, lecciones aprendidas y recomendaciones de mejora.

Fuente: elaboración propia.

Con el fin de fortalecer la validación empírica de la propuesta anterior, se plantearon indicadores preliminares que permitirán evaluar la implementación de los modelos MORCC y MGAC en entornos piloto. Estos indicadores abordan aspectos técnicos, organizacionales y estratégicos, alineándose con los principios de gobernanza adaptativa, resiliencia operativa y ciberseguridad post-cuántica. La Tabla 7 resume estos indicadores clave.

Estos indicadores podrán ser refinados según el contexto del piloto y su análisis permitirá evaluar la pertinencia, escalabilidad y adaptabilidad de las soluciones propuestas, así como su alineación con estándares emergentes en ciberseguridad cuántica. Además, facilitarán la comparación entre distintas instituciones o sectores, generando evidencia para la formulación de políticas públicas más robustas en entornos críticos. Finalmente, aunque este estudio se centró en la proyección metodológica sin aplicación directa en entornos reales, se reconoce la necesidad de validación empírica. El desarrollo de pilotos en infraestructuras críticas de sectores estratégicos, a fin de evaluar los modelos propuestos, ajustar supuestos teóricos y fortalecer su aplicabilidad bajo marcos regulatorios específicos es una perspectiva de trabajo futuro

Tabla 7. *Propuesta de indicadores para evaluar pilotos de implementación del modelo ontológico y de gobernanza cuántica.*

Categoría	Indicador Propuesto	Métrica / Unidad	Nivel de Evaluación
Técnico	Porcentaje de cobertura de activos modelados en la ontología	Porcentaje activos críticos representados	Completo / Parcial / Bajo
	Tiempo medio de respuesta ante un incidente cuántico simulado	Minutos / horas	Cuantitativo
	Nivel de interoperabilidad entre sistemas heredados y soluciones nuevas	Índice de compatibilidad	Bajo / Medio / Alto
Organizacional	Nivel de apropiación del modelo por parte de los equipos técnicos	Escala Likert (1 a 5)	Percepción cualitativa
	Porcentaje de implementación de controles post-cuánticos	Porcentaje controles aplicados del marco	Cuantitativo
	Presencia de roles y responsabilidades definidos en MGAC	Sí / No	Binario
Estratégico / Gobernanza	Existencia de un plan de continuidad actualizado con enfoque cuántico	Documento validado	Sí / Parcial / No
	Frecuencia de actualización del modelo ontológico	Número de revisiones por año	Cuantitativo
	Inclusión del modelo en la política institucional de seguridad	Grado de integración	Ninguno / Parcial / Total

Fuente: elaboración propia.

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.

Referencias

[1] A. Pinto, L. C. Herrera, Y. Donoso, and J. A. Gutierrez, "Enhancing critical infrastructure security: Unsupervised learning approaches for anomaly detection," *Int. J. Comput. Intell. Syst.*, Dec. 2024. https://doi.org/10.1007/s44196-024-00644-z.

[2] M. Habibul Arif, H. Rahman Rabby, N. Yasmin Nadia, M. Iftekhar Monzur Tanvir, and A. Al Masum, "AI-driven risk assessment in national security projects: Investigating machine learning models to predict and mitigate risks in defense and critical infrastructure projects," *J. Comput. Sci. Technol. Stud.*, 2025. https://doi.org/10.32996/jcsts

[3] M. T. Islam, M. R. Mission, T. K. Refat, and M. Kynatun, "Cybersecurity Risk Assessment Frameworks For Engineering Databases: A Systematic Literature Review", *SDMI*, vol. 2, no. 01, pp. 224–243, Feb. 2025. https://doi.org/10.71292/sdmi.v2i01.22 .

[4] M. Ekerå, "On post-processing in the quantum algorithm for computing short discrete logarithms," *Des. Codes Cryptogr.*, vol. 88, no. 11, pp. 2313–2335, Nov. 2020. https://doi.org/10.1007/s10623-020-00783-2

[5] M. J. Page *et al.*, "The PRISMA 2020 statement: An updated guideline for reporting systematic reviews," *BMJ*, vol. 372, art. n71, Mar. 2021. https://doi.org/10.1136/bmj.n71

[6] 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. https://doi.org/10.1016/j.infsof.2013.07.010

[7] 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. [Online]. Available: https://arxiv.org/abs/2408.16140

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

[9] S. Islam, D. Javeed, M. S. Saeed, P. Kumar, A. Jolfaei, and A. K. M. N. Islam, "Generative AI and cognitive computing-driven intrusion detection system in industrial CPS," *Cognit. Comput.*, vol. 16, no. 5, pp. 2611–2625, Sep. 2024. https://doi.org/10.1007/s12559-024-10309-w

[10] A. AlHarmali, S. Ali, W. Aman, and O. Hussain, "Cyber risk assessment for cyber-physical systems: A review of methodologies and recommendations for improved assessment effectiveness," in *Proc. Comput. Sci. Inf. Technol. (CS & IT)*, AIRCC, Aug. 2024, pp. 77–94. https://doi.org/10.5121/csit.2024.141608

[11] A. Budžys, O. Kurasova, and V. Medvedev, "Deep learning-based authentication for insider threat detection in critical infrastructure," *Artif. Intell. Rev.*, vol. 57, no. 10, art. 263, Oct. 2024. https://doi.org/10.1007/s10462-024-10893-1

[12] A. Akbarzadeh and S. K. Katsikas, "Dependency-based security risk assessment for cyber-physical systems," *Int. J. Inf. Secur.*, vol. 22, pp. 563–578, Jun. 2023. https://doi.org/10.1007/s10207-022-00608-4

[13] B. G. de Soto, A. Georgescu, B. Mantha, Ž. Turk, A. Maciel, and M. S. Sonkor, "Construction cybersecurity and critical infrastructure protection: New horizons for construction 4.0," *J. Inf. Technol. Constr.*, vol. 27, pp. 571–594, 2022. https://doi.org/10.36680/j.itcon.2022.028

[14] S. Berríos, F. Alonso, B. Gana, and S. Contreras, "Advances and strategies in quantum computing integration for cybersecurity: A systematic literature review," in *Commun. Comput. Inf. Sci.*, Springer, 2025, pp. 269–282. https://doi.org/10.1007/978-3-031-84078-4_19

[15] D. Silva and R. Núñez, "Exploración de las posibilidades de la computación cuántica para la criptografía," *CIENCIA INTELIGENTE*, vol. 1, no. 2, pp. 35–53, 2023, Accessed: May 27, 2026. [Online]. Available: https://cienciainteligente.com/index.php/CIN/article/view/16

[16] S. Narula, M. Ghasemigol, J. Carnerero-Cano, A. Minnich, E. Lupu, and D. Takabi, "Exploring AI security: A systematic mapping study," *IEEE Access*, 2025. https://doi.org/10.1109/ACCESS.2025.3567195

[17] Í. Oliveira *et al.*, "An Ontological Model of the Phishing Attack Process," *Lecture Notes in Business Information Processing*, pp. 274–289, 2025, https://doi.org/10.1007/978-3-031-95397-2_17

[18] S. Dash, H. Seker, and M. Shahpasand, "From data to defense: How ontology fuels AI in cyber threat detection," in *Proc. 8th Int. Conf. Adv. Artif. Intell. (ICAAI 2024)*, ACM, Mar. 2025, pp. 121–133. https://doi.org/10.1145/3704137.3704176

[19] B. Cinar, "Supply chain cybersecurity: Risks, challenges, and strategies for a globalized world," *J. Eng. Res. Rep.*, vol. 25, no. 9, pp. 196–210, Oct. 2023. https://doi.org/10.9734/jerr/2023/v25i9993

[20] R. Ghosh, von Stockhausen, M. Schmitt, G. M. Vasile, S. K. Karn, and O. Farri, "CVE-LLM : Ontology-Assisted Automatic Vulnerability Evaluation Using Large Language Models," *arXiv.org*, 2025. https://doi.org/10.48550/arXiv.2502.15932

[21] U. Ullah, M. Haleem, and A. Ullah, "OntoSecAI: Ontology-driven security automation for AI-enabled systems," *PLOS ONE*, vol. 20, no. 12, art. e0337806, Dec. 2025. https://doi.org/10.1371/journal.pone.0337806

[22] Y. Guan, Y. Zhang, J. Yue, Y. Lu, and Y. Xie, "Enhancing cybersecurity situation awareness through knowledge graphs: An integrated survey including threats, vulnerabilities, and assets," *SSRN*, preprint, 2025. [Online]. Available: https://ssrn.com/abstract=5221263

[23] U. O. Obonna *et al.*, "Detection of man-in-the-middle (MitM) cyber-attacks in oil and gas process control networks using machine learning algorithms," *Future Internet*, vol. 15, no. 8, art. 280, Aug. 2023. https://doi.org/10.3390/fi15080280

[24] S. Amador Donado, C. J. Pardo Calvache, and R. Mazo Peña, "Revisión preliminar: ciberseguridad para tecnología de la operación en la era cuántica contra ataques de red a infraestructuras críticas," *Rev. INGE CUC*, vol. 20, no. 2, 2024.

[25] W. F. Borja Rivadeneira y O. S. Gómez Gómez, «Cybersecurity Ontologies: A Systematic Literature Review», *ReCIBE*, vol. 9, n.º 2, pp. C2–18, mar. 2021 https://doi.org/10.32870/recibe.v9i2.181.

[26] M. Plachkinova and A. Vo, "A taxonomy for risk assessment of cyberattacks on critical infrastructure (TRACI)," *Commun. Assoc. Inf. Syst.*, vol. 52, art. 2, 2023. https://doi.org/10.17705/1cais.05202.

[27] B. F. Martins *et al.*, "A framework for conceptual characterization of ontologies and its application in the cybersecurity domain," *Software and Systems Modeling*, vol. 21, no. 4, pp. 1437–1464, July 2022, https://doi.org/10.1007/s10270-022-01013-0

[28] O. Kozlenko, "Example of fuzzy ontology usage for risk assessment and attack impact," *Theor. Appl. Cybersecur.*, vol. 6, no. 1, 2024. https://doi.org/10.20535/tacs.2664-29132024.1.312677