ISSN: 1692-7257 - Volume 2 – Issue 48 - 2026

ORIGINAL

RCTA
Revista Colombiana de Tecnologías de Avanzada
UNIPAMPLONA

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

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

**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.**

Received: 22 February 2026. Revised: 05 May 2026. Accepted: 09 June 2026. Published: 03 July 2026.
**Corresponding Author:** Katerine Márceles Villalba

**How to cite:** 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

This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International License.

**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.

**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.

## INTRODUCTION

The fourth industrial revolution has consolidated a major link between the physical and digital domains through Cyber-Physical Systems (SCF). These systems have become the operational core of Critical Infrastructures (IC), spanning vital sectors such as energy, health, transport and finance, among others. By integrating sensors, actuators and distributed computing capabilities, SCF enable the continuity of essential services for society [1], [2].

However, the transition toward hyperconnected environments supported by technologies such as the Industrial Internet of Things (IIoT), Artificial Intelligence, 5G networks and Blockchain architectures, has created an attack surface, transforming digital vulnerabilities into physical risks with tangible consequences[3]-[5].

For decades, trust in these ecosystems has rested on public-key protocols such as RSA (Rivest, Shamir and Adleman) and Elliptic Curve Cryptography (ECC). However, the emergence of quantum computing caused a paradigm shift for system security. Shor's algorithm theoretically has the capacity to break these schemes in polynomial time, which poses an existential threat to the integrity of industrial control systems (ICS) [6], [7]. Despite the urgency of this scenario, a critical gap still persists in the scientific literature: most research is limited to analyzing algorithms in isolation, ignoring the technical complexity of implementing Post-Quantum Cryptography (PQC) in infrastructures with legacy components and protocols with latency constraints such as Modbus or SCADA [8], [9].

This gap becomes evident when contrasting the present review with the most representative works in the area, see Table 1. El-Kady et al.[7]and Turk et al.[18]address the cybersecurity of SCF from an organizational and risk-management perspective, but neither of the two incorporates the quantum threat or critical infrastructures as a domain of application. At the opposite end, reviews focused on quantum cryptography, such as those by Babu et al.[23]and Vasani et al.[37], delve into authentication and quantum communication protocols for IoT, but they do not address the resilience of CI nor do they use semantic models for its evaluation. The works closest to the present research are those of Sarker et al.[17], who propose an explainable AI taxonomy for SCF and CI with a first level of semantic modeling, and Ahmad et al.[38], who integrate quantum-safe cybersecurity, SCF and CI in smart microgrids; however, neither of the two simultaneously combines the four axes quantum threat, SCF, CI and cybersecurity ontologies, which underpin this study. This absence of conceptual integration constitutes the specific knowledge gap that the present review seeks to close. Table 1 synthesizes this comparison based on four dimensions of analysis —quantum threat/PQC, resilience in critical infrastructures, cybersecurity ontologies and cyber-physical systems—, evaluated in each study under the following convention: the symbol ✓ indicates that the dimension is addressed explicitly and centrally in the study; the symbol X indicates that the dimension is not treated; and the label "Partial" is reserved for cases in which the study touches on the dimension incidentally, without constituting a substantive methodological contribution to that dimension. The last row, corresponding to the present review, makes it possible to visualize that no previous work satisfies the four dimensions simultaneously.

***Table 1: Comparison of dimensions.***

| Study | Year | Approach | A | B | C | D |
|---|---|---|---|---|---|---|
| Turk et al. [18] | 2021 | Systemic IT/OT/CPS framework (Parker Hexagon). | x | x | x | ✓ |
| El-Kady et al. [7] | 2023 | Safety and security challenges in CPS | x | x | x | ✓ |
| Babu et al. [23] | 2024 | Taxonomy of quantum-attack-resistant AKA protocols in IoT. | ✓ | x | x | x |
| Vasani et al. [37] | 2024 | Quantum communication and cryptography (QKD). | ✓ | x | x | x |
| Sarker et al. [17] | 2024 | Rule-based AI taxonomy for cybersecurity in IC. | x | ✓ | P | ✓ |
| Wicaksana [35] | 2025 | Quantum-secure blockchain infrastructure. | ✓ | ✓ | x | x |
| Singh et al. [26] | 2025 | Cyber-resilience in e-government. | ✓ | ✓ | x | x |
| Lezzi et al. [9] | 2025 | AI for sustainable cybersecurity in industry. | x | ✓ | x | ✓ |
| Ahmad et al. [38] | 2025 | Quantum-safe cybersecurity in microgrids (blockchain-FL). | ✓ | ✓ | x | ✓ |
| This study | 2026 | Ontological quantum resilience assessment model for SCF in IC | ✓ | ✓ | ✓ | ✓ |

*Abbreviations used: A= Quantum threat / PQC, B= Resilience in CI, C= Cybersecurity ontologies, D= Cyber-Physical Systems (SCF), P= Partial.*
*Source: Own elaboration by the authors.*

The relevance of this research goes beyond the mere protection of data; it is about maintaining systemic resilience. A security compromise arising from quantum capabilities could trigger cascading failures in energy networks, jeopardizing national stability and human safety [10], [11]. For this reason, developing evaluation frameworks that link physical security with cybersecurity is a strategic necessity [12], [13].

Building on this premise, this research is grounded in Cyber-Physical Resilience and Lattice-Based Cryptography (Lattice-based), the central pillar of NIST standardization for the transition toward resistant algorithms, such as Crystals-Kyber (standardized as ML-KEM in FIPS 203) and Crystals-Dilithium (standardized as ML-DSA in FIPS 204)[9],[14],[44],[45]. The integration of these solutions is vital to ensure interoperability in modern infrastructures, such as smart microgrids, where technological decentralization requires a robust defense against persistent threats[1],[15].

The scope of this review ranges from elementary cryptographic foundations and the characterization of technical threats, to the recognition of standards and the integration of Semantic Models (Ontologies). The use of these models makes it possible to transform raw data into actionable knowledge, facilitating transparent decision-making in highly uncertain

environments[16],[17]. Thus, the study analyzes not only algorithmic complexity but also the system's intelligent response capacity to intrusions and operational failures[18],[10].

The central purpose of this article is to characterize, through a systematic literature review, the standards, defense mechanisms and evaluation metrics that facilitate the transition toward resilient infrastructures. It seeks to consolidate a technical roadmap that harmonizes innovations in hardware, network robustness and semantic models[19],[20]. To ensure scientific rigor, the process followed a hybrid protocol based on PRISMA 2020 and the guidelines of Kitchenham, analyzing global scientific output between 2020 and 2026.

Finally, the remainder of the article is structured as follows: Section 2 describes the methodology; Section 3 presents the results obtained; Section 4 develops the discussion and limitations; and Section 5 sets out the conclusions and future projections.

## METHODOLOGY

This study adopted a hybrid methodological protocol that combined the guidelines of Kitchenham and Brereton[21]with the transparency standards of PRISMA 2020[22], complemented by the Goal-Question-Metric (GQM) model for formulating and validating research questions. This protocol ensured that bias was neutralized in the phases of question formulation, source selection and relevance assessment. The complete flow of activities is available for public consultation in the Zenodo repository [https://doi.org/10.5281/zenodo.20802392].

The synergy of this protocol facilitated the neutralization of bias during the formulation of research questions, the selection of sources and the assessment of relevance, ensuring a precise definition of institutional and technical objectives[23],[24].

The study focused on reviewing scientific studies published between 2020 and 2026, prioritizing research that addressed the critical intersection between SCF, cybersecurity and the disruptive effects of quantum computing on IC[20],[17]. Because the integration of quantum security into industrial environments is a recent discipline, limited availability of specialized open-access sources was identified. Nevertheless, given its relevance, a search for peer-reviewed articles in high-impact databases was considered necessary, thereby ensuring a robust characterization of the domain studied[9],[25],[26].

The activities carried out in each stage of the protocol, as applied to the research, are described below:

- Definition of Objectives and Research Questions. The central objective of this review was to analyze the standards, frameworks and emerging threats in order to characterize the key requirements for achieving resilience in the quantum era for SCF in IC. To achieve this purpose, the following search objectives were established:

Ob1: Determine the influence of quantum technologies on the evolution of cybersecurity practices for critical infrastructures.

Ob2: Determine the necessary requirements for the development of an ontology-based assessment model for cybersecurity in SCF and IC.

The research questions were formulated using the GQM method[21](see Table 2), grounded in the PICOC approach[27] (Population, Intervention, Comparison, Outcomes and Context) and validated using the FINER criteria [28] (Feasible, Interesting, Novel, Ethical and Relevant). It should be noted that the questions were subjected to expert evaluation before their final application.

***Table 2: Question, metric, and motivation.***

| ID | Question | Metric | Motivation |
|---|---|---|---|
| | | | |
| Ob1. | P1: How does quantum computing affect current cybersecurity practices and standards in SCF and CI? | Number of articles that discuss the effects of quantum computing on cybersecurity models. | Analyze the impact of quantum computing on cybersecurity practices in SCF and IC. |
| | | | |
| Ob2. | P2: What are the key requirements for developing an ontological assessment model of cybersecurity in SCF and IC? | Characterization of the attributes, relationships and levels of semantic abstraction proposed for the representation of assets and risks. | Determine the structural and logical reasoning components required for a semantic and resilient evaluation model. |

*Abbreviations used: Objective (Ob), Question (Q). Source: Own elaboration by the authors.*

- Literature search: Three specialized databases were selected to identify scientific studies: IEEE Xplore, ACM Digital Library and ScienceDirect. This choice was not arbitrary; it followed from an analysis of thematic coverage carried out before the formal search. IEEE Xplore concentrates relevant scientific output in industrial control systems, cybersecurity of critical infrastructures and embedded systems, and is the reference source for IEEE publications in electrical engineering and industrial computing. ACM Digital Library is the primary repository for applied cryptography, security protocols and computer science, where most implementation-level PQC research is published. ScienceDirect (Elsevier) provides interdisciplinary coverage in applied engineering, IoT security and Cyber-Physical Systems from an applied sciences perspective. Scopus and Web of Science were excluded because both are secondary indexing platforms that aggregate records from multiple sources, including IEEE and ACM. Using them alongside the selected primary databases would have significantly increased the volume of

duplicates without adding specialized sources exclusive to the domain studied, which would have affected the efficiency of the protocol. As for SpringerLink, a preliminary scoping probe confirmed that its coverage in the specific intersection of PQC, ICS/OT and critical infrastructures was considerably lower than that of the three selected sources, with a high proportion of results not pertinent to the technical domain of this review. The search strings were designed using Boolean operators, adapting the syntax to the technical parameters of each search engine under the PICOC scheme (see Table 3).

***Table 3: PICOC***

| Element | Description | Search Terms |
|---|---|---|
| P (Population) | Cyber-Physical Systems and critical infrastructures. | (“cyber-physical systems” OR “CPS” OR “industrial control systems” OR “ICS” OR “SCADA” OR “operational technology” OR “OT”). |
| I (Intervention) | Post-Quantum Cryptography, ontological models and cybersecurity evaluation frameworks. | (“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 (Comparison) | Existing best practices and standards in industrial and cryptographic security. | (“cybersecurity framework” OR “NIST standard” OR “cryptographic standard” OR “security best practices” OR “quantum-resistant”) . |
| O (Outcome) | Operational resilience, threat mitigation and assessment of quantum vulnerabilities. | (“resilience” OR “threat mitigation” OR “vulnerability assessment” OR “quantum resilience” OR “cryptographic agility”) . |
| C (Context) | Quantum era and critical infrastructure sectors. | (“quantum computing” OR “quantum threat” OR “quantum era” OR “critical infrastructure” OR “post-quantum transition”) . |

*Source: Own elaboration by the authors.*

Based on the PICOC elements, the following general search string was consolidated and applied as a conceptual basis in the selected databases:

(“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”)

This string was adapted to the specific syntax of each database (IEEE Xplore, ACM Digital Library and ScienceDirect), adjusting operators, search fields and truncations according to the technical parameters of each platform. The complete records of the strings adapted for each database, together with the details of the filters applied, are available in the Zenodo repository: [].

After applying the search string, an initial universe of 841 records was identified. The screening process began with the removal of 147 duplicates, consolidating a set of 694 unique articles for evaluation. A preliminary screening then followed, based on a technical review of titles and abstracts, which made it possible to discard 539 articles that were not directly related to the central focus of the topic. This phase resulted in a sample of 155 potential studies, distributed as follows: 47 from IEEE Xplore, 18 from ACM and 90 from ScienceDirect.

Next, the inclusion and exclusion criteria defined in Table 4 were applied.

***Table 4: Inclusion and exclusion criteria.***

| Inclusion Criteria | Exclusion Criteria |
|---|---|
| Articles on cybersecurity in cyber-physical systems and CI. | Articles that do not address cybersecurity in SCF and IC. |
| Articles on the use of ontology-based assessment models. | Articles that do not mention ontological models or their application in cybersecurity. |
| Studies on the impact of quantum computing on the cybersecurity of SCF and IC. | Articles that do not consider quantum threats or cybersecurity. |
| The article must be between 2020 - 2026 | Books, theses, or non-peer-reviewed articles. |
| Articles published in English. | Articles in languages other than English |
| Articles that address how ontological models, security best practices and cybersecurity frameworks can be applied to prevent attacks on SCF and CI, with a focus on the quantum era. | Articles that do not focus on ontological models, security best practices and cybersecurity frameworks that can be applied to prevent attacks on SCF and IC. |

*Source: Own elaboration by the authors.*

This process culminated in the identification of 52 relevant articles, of which 103 were excluded for not satisfactorily meeting the required depth criteria. It should be noted that this process revealed a marked scarcity of specialized literature integrating quantum cybersecurity, SCF and IC, underscoring the need to consolidate dispersed knowledge to strengthen the resilience of critical infrastructures.

Studies were selected through a sequential and validated process. To ensure the rigor of the review, a structured assessment matrix was introduced to evaluate the quality of potential articles. This tool enabled a judgment-based analysis, ensuring that each selected study made a substantial contribution to the review’s objectives.

Each article was subjected to a quali-quantitative weighting system, assigning scores of 1.0 (Meets - Good Level), 0.5 (Partially meets - Fair Level) and 0 (Does not meet - Not relevant).

- Relevance Assessment: To ensure the robustness of the selected evidence, a relevance assessment methodology was applied, based on four dimensions: clarity, rigor, relevance and credibility, following the recommendations of Kitchenham et al.[21]. This approach enabled a qualitative and quantitative assessment of each document, which ensured the identification of studies with high scientific value and allowed the mitigation of bias in the final selection phase.

Each article was evaluated individually under a scoring scale from 0 to 1 per criterion, using the following weighting system to facilitate technical comparison:

- Fully met (1.0 point): The study fully satisfied the criterion.
- Partially met (0.5 points): The information was mentioned but lacked depth.
- Did not meet (0 points): The criterion was absent or was not relevant.

The specific criteria that guided this technical evaluation were:

- Clarity: Did the article clearly state its objectives, focusing on the intersection of quantum cybersecurity, SCF, IC or ontological modeling?
- Rigor: Is the methodological design explicit enough to allow its replicability and coherence with the stated objectives?
- Relevance: Did the findings present contributions applicable to advancing post-quantum security or propose future research avenues in critical infrastructures?
- Credibility: Did the research justify its approach and present results that were coherent and consistent with its initial premises?

After the evaluation, the scores were consolidated into a cumulative scale from 0 to 4 points to determine the level of relevance, and an acceptance threshold was established for definitive inclusion; see Table 5:

The acceptance threshold was set at >=3.2 points on a maximum scale of 4.0 based on a requirement of 80% overall compliance. Since the evaluation comprises four dimensions with a maximum value of 1.0 each (clarity, rigor, relevance and credibility), a score of 3.2 implies that the study must fully satisfy at least three criteria and partially satisfy the fourth. This threshold was chosen because it guarantees that no included study lacks methodological rigor or direct thematic relevance, two non-negotiable dimensions in a review on a technical domain as specific as post-quantum cryptography in Cyber-Physical Systems. Studies scoring between 2.1 and 3.1 underwent an additional detailed review and were ultimately excluded, unless they provided unique evidence not reported in higher-scoring studies. This decision was documented in the extraction matrix available in the Zenodo repository: [].

This process ensured that only research with substantial methodological rigor and thematic relevance formed part of the final compendium. As a result, 39 articles exceeded the relevance threshold and were catalogued as the primary studies in this review (see review traceability in Figure 1).

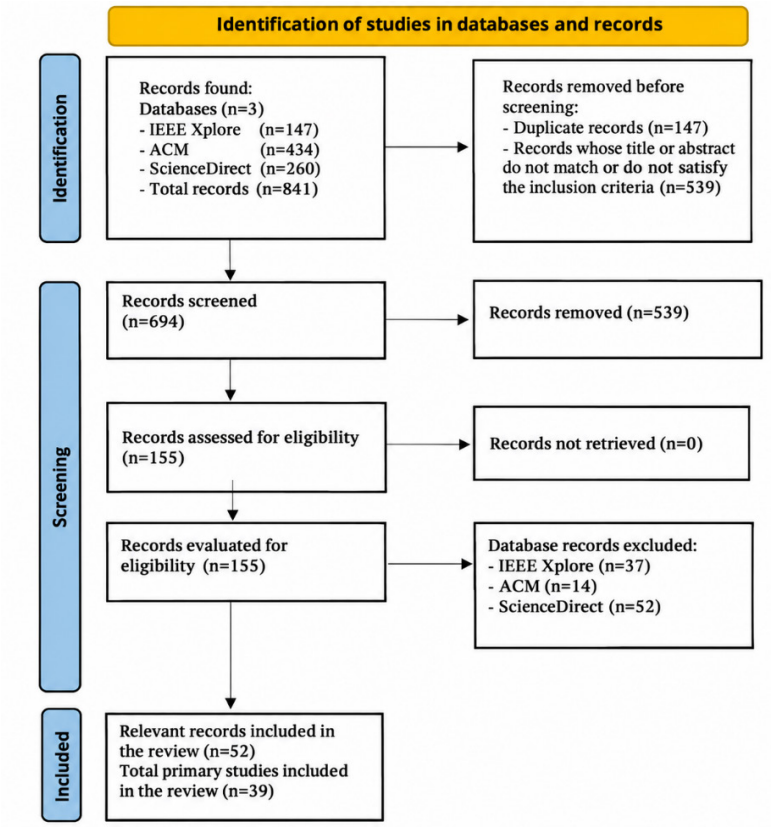


***Fig. 1.*** *Traceability of study identification*
*Source: Own elaboration by the authors.*

***Table 5: Level of relevance.***

| Score range | Level of relevance | Technical Decision |
|---|---|---|
| <= 2.0 | Moderate | Excluded |
| 2.1 – 3.1 | Medium | Detailed review |
| >= 3.2 | High | Included as a Primary Study |

*Source: Own elaboration by the authors.*

It is worth noting that although the GRADE system was not formally used, an equivalent three-level classification was adopted: high, medium and low, which was duly documented in the data extraction matrix. This screening procedure made it possible to appropriately prioritize and filter the studies.

- Data Extraction: Data extraction was carried out systematically, using the research questions and objectives defined in the initial phase of the protocol as reference. For this purpose, a structured data collection instrument was used, including key fields such as: unique article identifier (ID), title, publication source, abstract, keywords, type of research, country of origin, as well as the direct mapping to the research questions and objectives, which are available in the Zenodo repository:[ ].

This procedure made it possible to characterize the standards applied to SCF and IC, in addition to identifying emerging vulnerabilities linked to quantum computing. Likewise, the disruptive impact of quantum technologies on critical infrastructures was analyzed, collecting the technical elements necessary to propose an ontology that would provide a universal semantic definition of attacks, vulnerabilities and risks in this new paradigm. The data obtained constituted the key inputs to show which primary studies supported compliance with the overall research objectives, ensuring traceability between the literature analyzed and the results presented.

- Synthesis and Analysis of Results: The analysis of the data collected revealed exponential growth in academic output related to quantum cybersecurity in SCF and IC. As observed in Figure 2, scientific interest intensified significantly toward the end of the study period, with 2025 standing out as the point of greatest productivity with 17 articles (43.6%), followed by 2024 with 11 studies (28.2%). However, it is important to clarify that for 2026 partial results are presented, because only studies belonging to the first month of the year (January) were included; therefore, Figure 2 reflects a decline, but it is inferred that studies will continue to rise by the end of the year. This pattern reflected an urgent academic response to advances in quantum computing and the imminent need to strengthen IC.

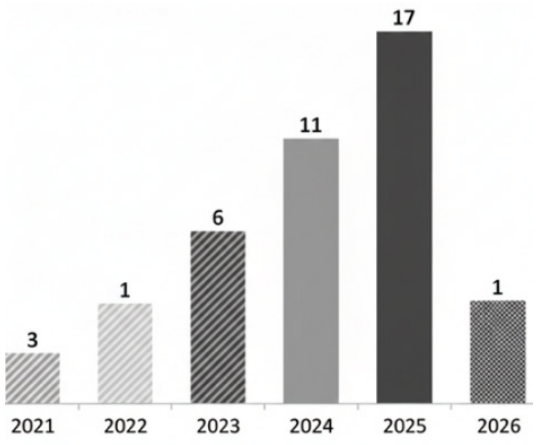


***Fig. 2.*** *Temporal evolution of scientific output (2021-2026) Source: Own elaboration by the authors.*

However, there were no publications in 2020, which is why that year does not appear in the previous graph. As for geographical distribution, India was found to have a prominent representation in studies related to the central theme of this research, since it was the country that contributed 10 studies (25.6%). It was followed in relevance by the United States with 6 publications (15.4%), South Korea with 3 (7.7%) and Canada also with 3 studies (7.7%). From the above, it can be inferred that these countries, characterized as technological powers with a high industrial deployment, have prioritized quantum resilience as a strategic security axis, see Figure 3.

Regarding the frequency of the key terms, a comprehensive alignment with the objectives of the systematic review was evidenced. As observed in Figure 4, the theme of Cybersecurity acted as the cross-cutting axis of the research, registering a presence in 100% of the articles analyzed (39 studies). This conceptual base made it possible to address the quantum threat, a term identified in 25 articles (64.1%), which confirmed the interest of the scientific community in the disruptive impact of quantum computing on current protocols. Regarding the domain of application, it was determined that IC was the most studied environment with 22 mentions (56.4%), closely followed by SCF with 17 records (43.6%). On the other hand, the

presence of specialized terms such as Frameworks (5 studies, 12.8%) and Ontologies (2 studies, 5.1%), pointing to emerging areas for predictive risk management.

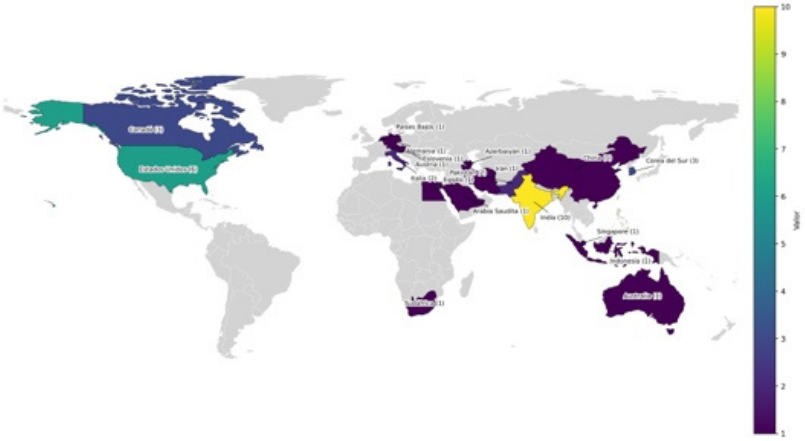

***Fig. 3.*** *Geographical distribution.*
*Source: Own elaboration by the authors.*

Finally, the veracity of these findings was supported by the evidence from the primary studies. 74.4% (29 articles) were categorized as research on the central axis, while 25.6% (10 articles) corresponded to literature reviews. This distribution allowed the conclusions of this work to be based on technical, experimental and applied evidence in real industrial and academic environments, see Figure 5.

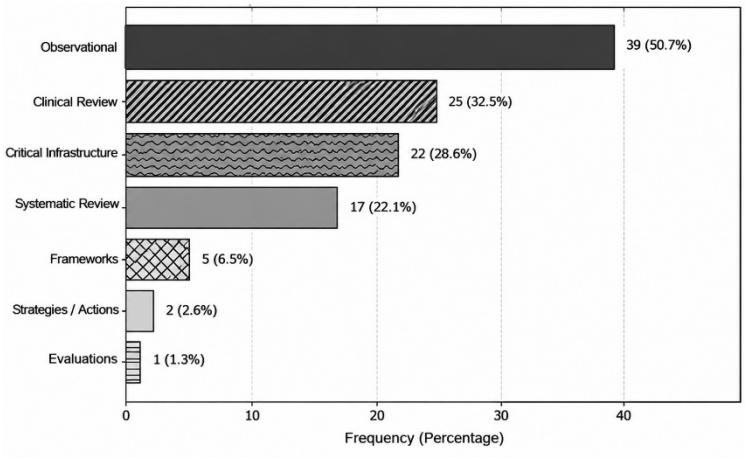


***Fig. 4.*** *Frequency of key terms in the selected studies.*
*Source: Own elaboration by the authors.*

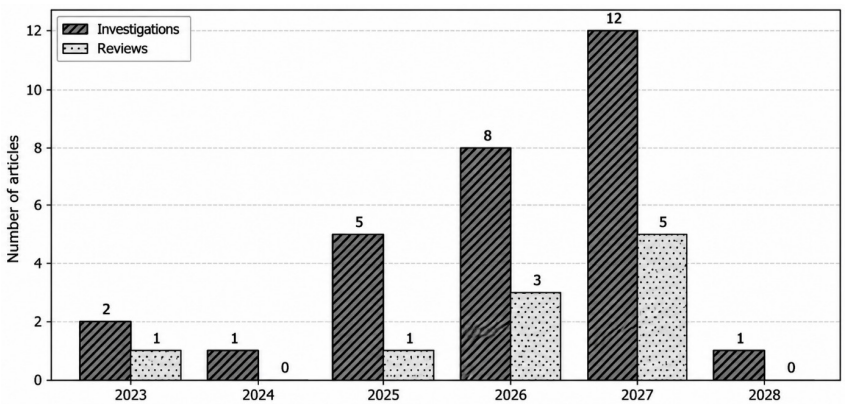


***Fig. 5.*** *Distribution by type of study: research vs. review (n=39).*
*Source: Own elaboration by the authors.*

## ANALYSIS OF RESULTS

To guarantee full traceability of the process and to answer each research question explicitly, the Zenodo repository available at [] consolidates the 39 selected primary studies, specifying for each one the identifier, main author, year, country of origin, type of research, technologies considered, main finding or contribution, and the research questions to which it provides direct evidence.

Below, answers are given to the research questions formulated that guided this review:

P1: How does quantum computing affect current cybersecurity practices and standards in SCF and CI?

After analyzing the different studies, it was established that the impact of quantum computing is not limited to technical areas, but rather constitutes a crisis of longevity and trust in current systems. In the studies analyzed, it was detected that the SCF that today provide us with water, energy, among others, were designed under a security model that quantum computing has begun to place at risk. A comparative analysis of the 39 primary studies allows relevant methodological convergences and divergences to be identified. Regarding convergences, there is widespread agreement in studies[1],[4],[8],[9],[14],[15],[25],[30] that Shor's algorithm represents the most immediate cryptographic threat to the RSA and ECC systems currently deployed in ICS/OT environments. However, significant methodological differences are identified in the approach adopted to address it: while studies such as[1]and[9]propose solutions based on QKD and post-quantum blockchain, others such as[17]and[25] focus exclusively on the evaluation and standardization of lattice algorithms (Kyber, Dilithium) without considering hardware restrictions. This divergence reveals a cross-cutting limitation in the literature: most proposals evaluate PQC algorithms in laboratory or simulation environments, without validating them on real industrial hardware with the memory and CPU cycle restrictions typical of PLCs and RTUs. Only studies[3],[19]and[26]worked directly on embedded hardware in ICS environments, this being the most specific evidence available on the operational viability of PQC in legacy infrastructure. An emerging trend identified in the most recent studies (2024–2025) is the adoption of hybrid architectures that combine PQC with federation and edge computing mechanisms[12],[15],[21], which suggests a shift in the field from pure cryptography toward systemic resilience. In light of the foregoing, the research made it possible to determine that, in industrial environments, trust has historically been based on the certainty that each operational command, such as opening a valve or regulating a generator, comes from a legitimate source. However, it was identified that quantum computing has come to break this premise.

Based on the foregoing, it was determined that one of the most critical vulnerabilities has been real-time identity spoofing. The studies[1],[14],[15],[29], reported that the ability of a quantum computer to break asymmetric encryption would allow an attacker to generate forged digital signatures. This would mean that an SCF could end up obeying malicious commands while believing them to be legitimate, putting the physical safety of the entire infrastructure at risk.

Likewise, the danger of capturing network traffic today to decrypt it in the future was identified. This practice can compromise the confidentiality of strategic data in critical infrastructures, which calls for an immediate technological transition, anticipating the existence of commercial quantum computers[8],[14].

Another finding that showed strong convergence across the reviewed studies was the limited capacity of industrial hardware to support the new PQC standards. Bandaru et al.[8]carried out an empirical evaluation of hardware and software implementations of the NIST finalist KEMs and found that Kyber-1024 consumes on average 3.4 times the computational resources of the RSA-2048 algorithms currently implemented in industrial microcontrollers. Consistent with this finding, Verchyk and Sepúlveda[11]showed in a practical study on resource-constrained microprocessors that IBE encryption enhanced with PQC introduces latencies of up to 180 ms in authentication operations, which exceeds the real-time response margins of SCADA protocols. Trungadi et al.[42]specifically documented the case of Modbus devices in legacy ICS and concluded that direct implementation of PQC without proxy intermediation is unfeasible, since PLCs from generations prior to 2015 lack the storage capacity for the parameters of the new algorithms. These three pieces of evidence, drawn from empirical studies with real hardware, support the claim that the limitation is not algorithmic but infrastructural, and that any post-quantum transition strategy in CI must contemplate a gradual renewal of the OT technology fleet or the use of intermediary proxy architectures.

In IC, synchronization is important. It was observed that the implementation of quantum security rules consumes more processing time, which generates latency. This situation in the energy sector can cause failures, turning the security solution into a critical operational problem[5],[7],[19],[31].

In order to manage these vulnerabilities intelligently, the reviewed studies proposed some support tools, such as:

Ontologies as a risk map: Given the demand for new threats, the studies[16],[32]-[34]proposed the use of ontologies to categorize and prioritize which infrastructure assets were most critical in the face of a quantum attack, enabling an organized rather than reactive defense.

The need for agile standards: The ideal standard was determined to be not the one that is unbreakable, but the one that is agile. The research highlighted that infrastructure must be able to replace its encryption algorithms without being disconnected or

physically replaced, in line with the new FIPS 203, FIPS 204 and FIPS 205 standards published by NIST[12],[17],[18],[35],[44]-[46]. This analysis confirms that the impact of quantum computing is cross-cutting: from the impossibility of using current hardware to the need to rewrite the rules of how security is managed in the essential services of the CI sectors.

Q2: What are the key requirements for developing an ontological cybersecurity assessment model in SCF and IC?

After analyzing the different studies, it was determined that an ontological model for the quantum era should not be a simple glossary, but a formal knowledge artifact capable of mediating between the physical constraints of Operational Technology (OT) and the mathematical rigor of the new cryptography. For the model to be functional in CI environments, it must meet the following requirements regarding ontological design:

1. Multidomain Taxonomic Structure (Classes and Hierarchies). The model requires a class hierarchy that decomposes SCF into three interconnected levels, allowing an integral semantic representation:

- Physical Layer: It is the representation of assets such as programmable logic controllers (PLCs) and remote terminal units (RTUs), fundamental in the architecture of SCF[19],[34].

- Cryptographic Layer: This refers to the classification of current (vulnerable) primitives and post-quantum cryptography (PQC) families formally standardized in FIPS 203 (ML-KEM), FIPS 204 (ML-DSA) and FIPS 205 (SLH-DSA), and quantum key distribution (QKD) as defense mechanisms[1],[14],[23],[35],[44]-[46].

- Threats Layer: This refers to the formal definition of quantum attack vectors, such as retrospective decryption and real-time spoofing[4],[8],[36].

2. Modeling of Relationships and Dependency. The ontology must formalize the critical interactions that determine the resilience of the system through specific semantic relationships:

- Load Support Relationship: This is the linking of cryptographic protocols with the memory and CPU capabilities of the hardware to prevent failures due to technological obsolescence[8],[11],[16].

- Cascade Relationship: The mapping of the network topology is defined to identify how a quantum compromise at a specific node semantically impacts the continuity of the infrastructure's global service[31],[33],[34].

3. Semantic Annotation of Performance Metrics. Unlike classical security ontologies, time is established as an ontological security requirement. The model must integrate data properties to measure the operational latency introduced by PQC algorithms, evaluating whether the response time remains within the safety margins of real-time industrial processes[5],[7],[30].

**4. Cryptographic Agility as a Class Attribute**

The model must evaluate the degree of agility of the infrastructure, defined as the capacity to instantiate or replace encryption algorithms dynamically without altering the physical structure of legacy hardware, allowing a smooth transition toward secure standards[12],[18],[32].

**5. Rule Base for Automatic Reasoning**

The final requirement is compatibility with inference engines, for example: SWRL rules (Semantic Web Rule Language). This allows the model to detect risks automatically: for example, if the advancement of the quantum computing capability of a threat exceeds the security threshold of a current algorithm, the system must deduce a "critical vulnerability" alert autonomously based on the knowledge base[3],[10],[17].

In summary, the comparative analysis of the 39 primary studies made it possible to establish three structural trends in the field. First: there is a decoupling between the theoretical maturity of PQC algorithms, widely documented in studies such as[16],[17]and[27], and their practical viability in OT environments, a gap that only three studies[3],[19],[26]address with empirical evidence. Second: semantic modeling and cybersecurity ontologies are recognized as necessary by studies such as[2],[7]and[39], but none of the corpus proposes an ontology that simultaneously integrates quantum threats, OT assets and latency metrics, which precisely delimits the contribution of this review. Third: scientific production in this domain shows a notable geographic concentration in India (10 studies, 25.6%) and the USA (6 studies, 15.4%), with scarce representation from Latin America and Southern Europe, which suggests a gap in contextual validation in developing economies with critical infrastructures that are less technologically updated.

Based on the preceding analysis, it can be reaffirmed that the requirements for an ontological model in SCF and IC are not limited to the digital realm, given that the true effectiveness of the model lies in its capacity to bridge the physical constraints of industrial machines with the mathematical demands of the post-quantum era. Without this comprehensive approach, there is a risk of designing models that are theoretically secure but operationally impossible to implement.

## DISCUSSION AND LIMITATIONS

The limitations and discussions are detailed in the following items:

**Contrast with previous systematic reviews**

The present study does not develop in an academic vacuum, but rather in direct dialogue with the most representative reviews and surveys in the field. When contrasting it with the ten reviews identified within the corpus itself, both convergences and relevant methodological differences emerge. El-Kady et al.[7]and Turk et al.[18]address security in Cyber-Physical Systems from an organizational and process risk management perspective, without incorporating the quantum dimension or semantic modeling. Lezzi et al.[9]present an exhaustive systematic review on AI-based cybersecurity for sustainable industry, with broad coverage of detection techniques, but without analyzing quantum threats or assessment ontologies. Sarker et al.[17]propose a rule-based AI taxonomy for cybersecurity in CI with elements of semantic modeling, being the work closest to the present study in terms of conceptual structure; however, they also do not integrate the quantum threat as a structuring axis. Reviews focused on PQC, such as those by Babu et al.[23]and Vasani et al.[37], offer in-depth technical coverage of authentication protocols and quantum communication, but circumscribe their analysis to the generic IoT domain, without considering the specific constraints of OT/ICS environments. Ahmad et al.[38]and Wicaksana[35]come closer to the intersection between PQC and critical infrastructures, but neither incorporates ontological models for semantic risk assessment. This comparison shows that the differential contribution of the present review lies in being, as far as the analyzed evidence reaches, the first to simultaneously integrate the four axes quantum threat, SCF, CI and cybersecurity ontologies in a systematic analysis oriented toward the assessment of operational resilience.

**Distinctive contribution of this study**

The review consolidates a specific contribution at three levels. At the conceptual level, it establishes a unified technical vocabulary that allows the physical constraints of OT hardware (PLCs, RTUs) to be articulated with the mathematical requirements of PQC algorithms, a terminological gap that previous reviews do not address systematically[7],[9],[18]. At the methodological level, it proposes five structural requirements for the design of an ontological evaluation model: multidomain taxonomic structure, relationship modeling, annotation of performance metrics, cryptographic agility as a class attribute, and a rule base for automatic inference. Together these constitute an operationalizable technical roadmap, unlike the general conceptual frameworks proposed by Sarker et al.[17]or Singh et al.[26]. At the empirical level, the review documents and synthesizes the available evidence on the practical infeasibility of implementing PQC directly on legacy industrial hardware [8], [19], [30], a fact that other reviews in the area mention only incidentally, without systematizing it as a central finding.

**Consolidated evidence versus emerging findings**

The distinction between consolidated evidence and emerging findings is essential for calibrating the scope of this study's conclusions. Consolidated evidence is considered to be that which is supported by multiple independent studies of an empirical or experimental nature. Three findings fall into this category: first, the theoretical vulnerability of RSA and ECC cryptosystems to Shor's algorithm, widely documented in[1],[8],[14],[25]and recognized by NIST itself as the basis for PQC standardization; second, the computational incompatibility between NIST's candidate PQC algorithms and industrial hardware from generations prior to 2015, evidenced with experimental data in[8],[19]and[26]; and third, the strategic need for cryptographic agility as a design attribute in industrial control systems, a convergence present in[12],[18],[32]and[35]. By contrast, the following are identified as emerging findings supported by a small number of studies and pending broader experimental validation: the applicability of formal ontologies with SWRL inference rules for the autonomous detection of quantum threats in CI[2],[17],[39]; the feasibility of hybrid architectures combining PQC with federated learning for microgrid environments[38]; and the use of convolutional graphs to assess the criticality of components in cyber-physical power systems[43]. This distinction implies that the conclusions linked to consolidated evidence are prescriptive in nature, whereas those associated with emerging findings should be interpreted as priority lines of research, not as immediate operational recommendations.

**Implications of the limitations for the scope of the conclusions**

The first limitation is the restriction of the search to three databases (IEEE Xplore, ACM Digital Library and ScienceDirect). Although these sources concentrate the most relevant scientific output in the domain studied, the exclusion of repositories such as Scopus, Web of Science and grey literature (NIST technical reports, ENISA or IEC guidelines) means that some regulatory frameworks and industrial implementation studies with restricted access were not considered. This limitation mainly affects the completeness of the evidence on the actual state of PQC adoption in OT environments, so the conclusions on the technological maturity of the sector should be read as an approximation based on the indexed academic literature, not as an exhaustive state of the art.

The second limitation is the scarcity of empirical validation studies in real critical infrastructures. Only three studies in the

corpus[3],[19],[26]report experiments or implementations on industrial hardware in operation. Most of the works analyzed operate in simulation or laboratory environments. This limits the generalizability of the conclusions on the behavior of PQC algorithms under real operating conditions of latency, temperature or electromagnetic interference, conditions typical of SCADA environments, electrical substations or treatment plants.

The technical recommendations derived from this review should therefore be interpreted as hypotheses to be validated through case studies in real environments before their implementation at scale.

The third limitation is the speed of evolution of the domain studied. The NIST standards FIPS 203 (ML-KEM) [44], FIPS 204 (ML-DSA) [45] and FIPS 205 (SLH-DSA) [46], published in 2024, represent a regulatory milestone that several of the primary studies in this corpus anticipated as a proposal, but which now constitute formal standards. This means that some claims about the emerging nature of PQC have been partially overtaken by regulatory reality, which reinforces the urgency of the conclusions but also requires that future research in this field take these standards as a starting point, not as a horizon.

## CONCLUSIONS

The findings of this systematic review support the following conclusions, organized into two blocks: evidence derived from the analysis of the 39 primary studies and lines of research proposed on the basis of the gaps identified.

This research shows that protecting SCF and CI against quantum computing demands a progressive paradigm shift: the transition from reactive perimeter security toward operational semantic resilience. Based on the systematic analysis of the evidence, it is established that a significant proportion of the primary studies report relevant technical limitations of legacy hardware in OT environments. The evidence analyzed indicates that OT-associated devices (such as PLCs and RTUs) present, in most documented cases, computational constraints that hinder the direct implementation of the new post-quantum cryptography standards[8],[19],[26],[30]. These constraints manifest mainly as operational latencies that, according to the empirical studies reviewed, may compromise the real-time response margins of industrial protocols such as SCADA and Modbus. This situation warns that certain adaptation attempts without considering the actual capabilities of OT hardware could compromise the stability of real-time processes.

In this transition scenario, semantic modeling was identified as a strategic decision component in the most recent studies of the corpus[2],[17],[39]. The review findings show that developing ontological models goes beyond organizing concepts and becomes a tool for automated reasoning. By semantically characterizing assets, threats, and metrics, the evidence suggests that systems are enabled to detect vulnerabilities autonomously through inference engines[17],[39].

Likewise, the studies analyzed converge in pointing out that cryptographic agility and the standardization of information technology and OT are strategic requirements for the transition toward resilient infrastructures[12],[18],[32],[44]-[46]. The terminological unification identified in this review as a requirement of the ontological model provides the formal language needed for a coordinated response among sector actors. From the gaps identified in the literature, the following priority lines of research are derived. First, future work should prioritize the optimization of PQC primitives designed specifically for resource-constrained microcontrollers, seeking a balance between security and operational latency in real ICS environments, since the empirical evidence available in this domain is still scarce.

Second, the formal construction of a cyber-resilience ontology integrating SWRL rules is proposed, so that infrastructure defense can rely on a logical orchestration between the physical rigidity of industry and quantum mathematical complexity, reducing dependence on human judgment in real-time threat detection.

Third, the path toward creating dynamic hybrid architectures represents an open research opportunity. These architectures should be capable of alternating between algorithmic methods and QKD according to the level of risk detected, and should be validated in real infrastructure environments before their widespread deployment.

Finally, the field's outlook suggests that integrating these intelligent models into Digital Twins could be a relevant line of validation, allowing quantum era attacks to be simulated and automated responses to be evaluated in virtual environments before deployment in real critical infrastructures, which would help minimize the possible risks associated with failures during technological migration.

## REFERENCES

[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.

## ACKNOWLEDGMENTS

Thanks to Universidad del Cauca, especially the GTI research group, and to Universidad de Antioquia and its In2lab group for providing the resources and support for the development of this proposal.

## FUNDING

No financing

## CONFLICT OF INTEREST

None

## AUTHORSHIP CONTRIBUTIONS

Drafting – original draft: Katerine Márceles Villalba, César Jesús Pardo Calvache, Siler Amador Donado.

Writing–review and editing: Katerine Márceles Villalba, César Jesús Pardo Calvache, Siler Amador Donado.