Modelo de referencia de ciberseguridad para prevenir ataques de red a infraestructuras críticas en la era cuántica

Siler Amador Donado

Departamento de sistemas – Universidad del Cauca (Unicauca)
Calle 5 # 4 -70 – Popayán – Colombia

samador@unicauca.edu.co

Resumen. *Este documento presenta un modelo de referencia de ciberseguridad para proteger sistemas ciber-físicos (CPS) en infraestructuras críticas (IC) ante las amenazas de la computación cuántica. La revisión sistemática de la literatura (RSL) revela la urgencia de incorporar criptografía post-cuántica y de abordar retos como la interoperabilidad con sistemas heredados y los altos costos de implementación. MoRCiTO integra controles de acceso, monitorización continua y métodos de detección y mitigación de ciberataques de red, desarrollado mediante investigación-acción en tres ciclos.*

Palabras claves. *Modelo de referencia MoRCiTO, ciberseguridad post-cuántica, infraestructura crítica, sistema ciber-físico, tecnología de la operación.*

Abstract*. This paper presents a cybersecurity reference model for protecting cyber-physical systems (CPS) in critical infrastructures (CI) from quantum computing threats. The systematic literature review (SLR) reveals the urgency of incorporating post-quantum cryptography and addressing challenges such as interoperability with legacy systems and high implementation costs. MoRCiTO integrates access controls, continuous monitoring, and network cyberattack detection and mitigation methods, developed through action research in three cycles.*

Keywords*. MoRCiTO reference model, post-quantum cybersecurity, critical infrastructure, cyber-physical system, operation technology.*

1. Introducción y principales desafíos

Problema: La convergencia entre los CPS y las IC ha incrementado significativamente la dependencia tecnológica en sectores fundamentales como energía, salud, transporte, sistemas financieros y telecomunicaciones. Aunque esta integración proporciona beneficios en eficiencia y control, también expone a estos sistemas a ciberataques potencialmente devastadores, comprometiendo no solo la estabilidad económica, sino también la seguridad pública. Los CPS implementados en IC generalmente son sistemas heredados, difíciles y costosos de reemplazar o actualizar, incrementando aún más su vulnerabilidad. Además, con la llegada de la computación cuántica, se enfrentan a nuevas amenazas, debido a que los algoritmos cuánticos como los propuestos por Shor y Grover podrían romper las soluciones criptográficas actuales (Amador-Donado et al., 2024a, 2024b). Entre los desafíos específicos identificados se destacan la interoperabilidad

tecnológica, ausencia de estándares globales, escalabilidad de soluciones, altos costos de implementación, validación práctica limitada, dificultad en detección de amenazas cuánticas, falta de personal capacitado y problemas prácticos en la implementación segura de criptografía post-cuántica (Bernstein & Lange, 2017; Liu et al., 2022; Kalinin & Krundyshev, 2022; Kayan et al., 2022).

Motivación: La relevancia de abordar este problema radica en la necesidad urgente de proteger la integridad operativa y funcional de las IC, dado su impacto directo en la seguridad nacional, estabilidad económica y bienestar social. La llegada de la computación cuántica impone una transición acelerada y planeada hacia soluciones de ciberseguridad robustas, capaces de enfrentar nuevas categorías de ciber-amenazas. Garantizar la continuidad operativa segura en sectores estratégicos constituye una prioridad global, dada la magnitud potencial de las consecuencias asociadas a fallas en estos sistemas críticos.

Contribución: Esta investigación contribuye al cuerpo de conocimiento existente mediante el desarrollo de un modelo de referencia orientado explícitamente hacia la prevención de ataques de red en CPS utilizados en IC, específicamente en el contexto de la era cuántica. Este modelo se destaca por proponer mecanismos de integración efectiva entre tecnologías heredadas y emergentes, fomentar el establecimiento de bases para la estandarización global de soluciones criptográficas post-cuánticas, y proporcionar lineamientos para la escalabilidad y validación práctica de las soluciones implementadas. De esta manera, el estudio pretende reducir la brecha identificada en investigaciones previas y ofrecer un camino viable para enfrentar los retos planteados por el paradigma cuántico en entornos críticos reales.

2. Preguntas y objetivos de la investigación

Objetivo general de la investigación: Proponer un modelo de referencia de ciberseguridad para la tecnología de la operación que apoye la prevención de ataques de red a CPS en IC como advenimiento a la era cuántica. Objetivos específicos de la investigación: **OE1**: Caracterizar los elementos fundamentales a tener en cuenta para la ciberseguridad en la tecnología de la operación por medio del análisis de la literatura existente, que permita clarificar la prevención de los tipos de ataques de red contra CPS en IC como advenimiento a la era cuántica. **OE2**: Proponer un modelo de referencia que clarifique las prácticas a tener en cuenta para prevenir ataques de red a CPS en IC como advenimiento a la era cuántica, con base en los elementos caracterizados en el objetivo anterior. **OE3**: Evaluar el modelo de referencia propuesto a través de un estudio de caso para prevenir ataques de red a CPS en IC.

Para lograr el primer objetivo de la investigación se llevó a cabo una RSL basados en (Kitchenham & Charters, 2007). En https://acortar.link/Y0uU8u se detallan los objetivos de búsqueda y sus correspondientes preguntas de investigación.

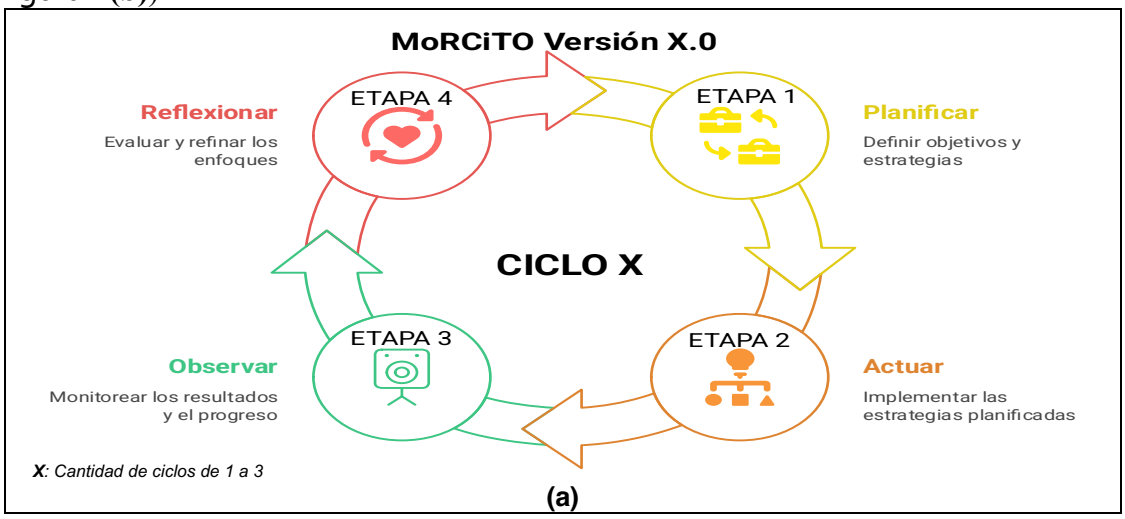
3. Resumen del conocimiento actual del dominio del problema

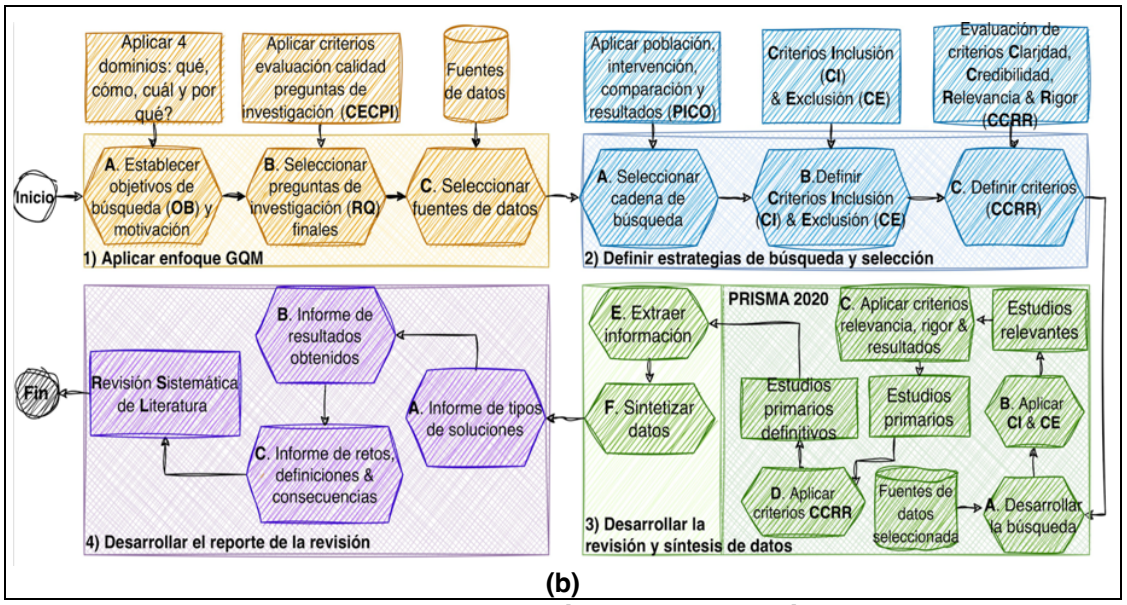
El dominio de la ciberseguridad en CPS ha avanzado significativamente en áreas como detección de amenazas, criptografía y gestión de incidentes. Sin embargo, la llegada de la computación cuántica introduce nuevos riesgos, especialmente por su potencial para vulnerar sistemas criptográficos actuales.

Una RSL preliminar realizada por (Amador Donado et al., 2024a) revela brechas importantes, como la falta de estandarización en protocolos criptográficos post-cuánticos y la necesidad de modelos específicos para CPS. Se identificó que el 65% de los estudios revisados ofrecen soluciones teóricas sin validación empírica, y solo el 20% exploran escenarios concretos en IC. Por ejemplo, la integración de Quantum Key Distribution (QKD) presenta desafíos prácticos relacionados con la complejidad y costos elevados (Diamanti et al., 2016). Aunque la criptografía basada en lattice muestra promesas para la resistencia post-cuántica, aún enfrenta limitaciones de rendimiento. Asimismo, menos del 10% de los estudios abordan la interoperabilidad con sistemas legados. Es crucial superar retos relacionados con interoperabilidad, escalabilidad y adaptación efectiva de estas tecnologías en entornos complejos y distribuidos propios de los CPS (Bernstein & Lange, 2017).

4. Metodología de investigación

Se utilizó la metodología investigación-acción (Mertler, 2020) mediante 3 ciclos, en el primero se realizó la caracterización del modelo mediante la RSL obteniéndose la versión 1.0 de MoRCiTO (Modelo de Referencia de Ciberseguridad para la Tecnología de la Operación), en el segundo ciclo se está realizando la evaluación por expertos para así obtener la versión 2.0 del modelo, y en el tercer ciclo se espera realizar mejoras a partir de los ajustes realizados al modelo y obtener la versión 3 (ver Figura 1**(a)**). Para llevar a cabo la RSL se diseñó el protocolo basados en (Kitchenham & Charters, 2007) (ver Figura 1**(b)**).





(b)

Figura 1. Metodologías de investigación

A continuación se presenta un resumen de las actividades de investigación realizadas en cada uno de los 3 ciclos:

Ciclo 1-RSL preliminar (MoRCiTO V1.0): Este ciclo tuvo una duración de 19 meses, ya fue desarrollado en su totalidad y se llevaron a cabo las siguientes etapas: **Etapa 1-Planeación:** En esta etapa se identificó y delimitó el tema, se recolectó información pertinente, se revisó la literatura relacionada y se desarrolló un plan de investigación. También se establecieron los objetivos de búsqueda y su motivación, se seleccionaron las preguntas finales de investigación, se seleccionaron las fuentes de datos adecuadas y se aplicaron criterios de evaluación de calidad a dichas preguntas. **Etapa 2-Ejecución:** Se recolectaron y analizaron los datos. Además, se seleccionó la cadena de búsqueda utilizando la técnica PICO (población, intervención, comparación y resultados). También se definieron los criterios de inclusión y exclusión para seleccionar los estudios, así como los criterios de claridad, credibilidad, relevancia y rigor (CCRR). **Etapa 3- Desarrollo**: Se desarrolló un plan de acción, que incluyó la ejecución de la búsqueda bibliográfica, aplicando los criterios previamente definidos de inclusión y exclusión. A partir de esto, se obtuvieron los estudios relevantes, se aplicaron criterios adicionales relacionados con relevancia, rigor y resultados, identificando finalmente los estudios primarios definitivos. Posteriormente, se aplicaron criterios CCRR, se extrajo la información necesaria y se sintetizaron los datos obtenidos. **Etapa 4-Reflexión:** Se compartieron los resultados y se reflexionó profundamente sobre todo el proceso llevado a cabo. Se elaboraron informes sobre los tipos de soluciones encontradas, se presentaron los retos enfrentados y finalmente se preparó el informe detallado con los resultados obtenidos, consolidando la elaboración de la publicación de la RSL preliminar (Amador Donado et al., 2024a) y en proceso de evaluación para su publicación la RSL final en la revista IEEE Access. Otra publicación realizada fue MoRCiTO versión 1.0 (Amador Donado et al., 2024b). También se realizaron 2 presentaciones: 1. En la modalidad de keynote, la charla titulada "Ciberseguridad en IC". 2. En la modalidad de ponencia titulada "Characterization of MoRCiTO: Cybersecurity reference model for operation technology" en el "VI International conference on advances in emerging trends and technologies – ICAETT

2024" celebrado en la Escuela Superior Politécnica del Chimborazo (ESPOCH) en Riobamba, Ecuador, el 17 y 18 de octubre de 2024.

Ciclo 2-Evaluación por juicio de expertos (MoRCiTO V2.0): Para este ciclo se estimó una duración de 13 meses. Este ciclo se encuentra aún en desarrollo y se llevaran a cabo las siguientes etapas: **Etapa 1-Planeación:** Se delimitó el tema de investigación relacionado con la evaluación del modelo versión 1.0. Se recolectó información y se tomó como base de referencia la RSL preliminar realizada en el ciclo 1 para sustentar la investigación. Además, se desarrolló un plan de investigación y se definió con precisión el objetivo de la evaluación por expertos, especificando los criterios que evaluarán: comprensibilidad, aplicabilidad, idoneidad y completitud del modelo versión 1.0, estableciendo el alcance y resultados esperados. **Etapa 2-Ejecución:** Se realizará la recolección y análisis preliminar de datos relacionados con el modelo versión 1.0, determinando su estado actual. Se seleccionarán cuidadosamente los 4 expertos que participarán en la evaluación, considerando criterios como trayectoria académica, experiencia profesional en ciberseguridad, experiencia en CPS e IC. Se elaborará un instrumento para la evaluación del modelo en relación con los criterios definidos (comprensibilidad, aplicabilidad, idoneidad y completitud), utilizando cuestionarios, entrevistas o matrices de valoración mediante la técnica de grupo focal. **Etapa 3-Desarrollo:** Se desarrollará un plan de acción que contemplará la evaluación por expertos del modelo versión 1.0. Se realizará el contacto formal con los expertos, proporcionando los documentos necesarios del modelo junto con el instrumento para la evaluación de comprensibilidad, aplicabilidad, idoneidad y completitud. Posteriormente, se recolectarán las respuestas aportadas por los expertos y se realizará el procesamiento y organización sistemática de los datos obtenidos para facilitar un análisis claro y detallado. **Etapa 4-Reflexión:** Se analizarán los resultados de la evaluación de expertos de la versión 1.0, determinando niveles de concordancia, áreas de mejora y recomendaciones asociadas a la comprensibilidad, aplicabilidad, idoneidad y completitud del modelo. Se formularán ajustes y recomendaciones de mejora, se elaborará un informe de todo el proceso de evaluación, la metodología empleada, los perfiles de los expertos participantes, resultados detallados y las decisiones del análisis realizado. Se espera realizar la publicación de los resultados obtenidos de MoRCiTO versión 2.0.

Ciclo 3-Estudio de caso (MoRCiTO V3.0): Para este ciclo se estimó una duración de 13 meses. Este ciclo de la investigación se encuentra en desarrollo y se llevaran a cabo las siguientes etapas: **Etapa 1-Planeación:** Se identificará el estudio de caso enfocado en el análisis de la versión 2.0. Se delimitará el alcance y se definirán los objetivos específicos de la evaluación. Se recolectará información preliminar y con base en la RSL se elaborará el estudio del caso. Se desarrollará el protocolo del estudio de caso sobre la versión 2.0, especificando las preguntas, los métodos para recolectar datos, los criterios para seleccionar escenarios representativos para su implementación, y los métodos previstos para analizar los datos obtenidos. **Etapa 2-Ejecución:** Se recolectará sistemáticamente los datos específicos mediante la implementación práctica de la versión 2.0 del modelo en contextos seleccionados. Se utilizarán instrumentos definidos en el protocolo, tales como entrevistas a usuarios, observación directa durante la aplicación del modelo y análisis exhaustivo de documentos técnicos. Los datos recopilados serán organizados, registrados y preparados cuidadosamente para garantizar su calidad, precisión y coherencia, facilitando así un análisis riguroso y profundo posterior. **Etapa 3-Desarrollo:** Se desarrollará un análisis de los datos recolectados del estudio de caso

sobre la versión 2.0 del modelo. Se aplicarán métodos analíticos cualitativos y cuantitativos que permitan interpretar los datos obtenidos, identificando patrones, fortalezas, debilidades y aspectos relevantes de la implementación práctica del modelo. Posteriormente, se realizará una síntesis sistemática para extraer hallazgos específicos, conclusiones y resultados acerca de la aplicabilidad, efectividad y pertinencia de la versión 2.0. **Etapa 4-Reflexión:** Se publicaran los resultados del estudio de caso realizado sobre la versión 2.0, además, se formularán recomendaciones del análisis detallado del modelo. Finalmente, se elaborará un informe de los resultados obtenidos, conclusiones y las acciones a seguir derivadas del estudio sobre la versión 2.0. Se espera realizar la publicación de MoRCiTO versión 3.0.

5. Solución propuesta y resultados obtenidos

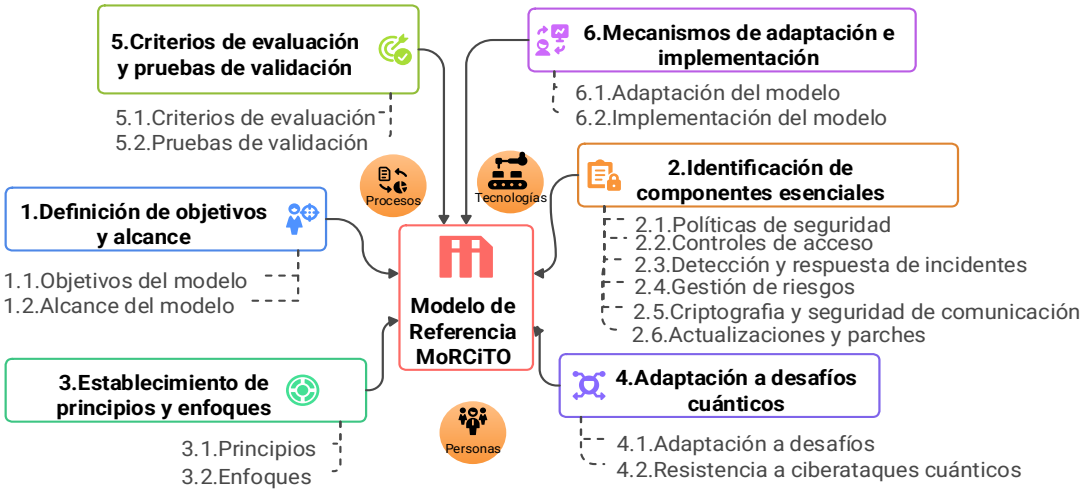


Figura 2. Vista resumida del Modelo de referencia propuesto

MoRCiTO se centra en: 1. Un enfoque modular que integra prevención de ciber-ataques de red y mitigación. 2. Lineamientos para la implementación de criptografía post-cuántica. 3. Un sistema de monitoreo continuo.

Los componentes del modelo funcionan de integradamente estableciendo un enfoque holístico de seguridad en las IC. Las *políticas de seguridad* brindan directrices generales, los *controles de acceso* garantizan protección de los sistemas y los datos, la *detección y respuesta a incidentes* permiten respuestas eficientes a ciberataques, la *gestión de riesgos* identifica y mitiga riesgos potenciales, la *criptografía y la seguridad de la comunicación* protegen la confidencialidad de los datos y las *actualizaciones y parches de seguridad* mantienen los sistemas actualizados y protegidos. MoRCiTO se encuentra en evaluación por expertos y se validará a través de escenarios simulados que repliquen operaciones de IC. Los resultados permitirán la toma de decisiones en la detección de amenazas y la mitigación de riesgos (Amador Donado et al., 2024a, 2024b).

6. Aspectos de la solución sugerida que la hacen diferente o mejor

MoRCiTO se destaca por tres aspectos: su adaptabilidad a entornos operativos, integración de criptografía post-cuántica y un enfoque holístico desde la detección hasta la mitigación de amenazas. Su diseño modular facilita la integración progresiva en IC variadas, siendo eficaz en redes industriales centralizadas y sistemas distribuidos con CPS (Amador Donado et al., 2024b; Bernstein & Lange, 2017).

En una prueba de concepto aplicada a cable-modems Technicolor en Colombia, se evidenció que el 89.1% son vulnerables a ataques por diccionario, permitiendo su control, ataques de phishing e instalación de rootkits. Su evaluación con TRACI confirmó alta exposición de activos, gestión del riesgo y motivación del adversario. Se recomienda cambio de contraseñas, autenticación multifactor y monitoreo continuo (https://acortar.link/27T1Oo). Sin embargo, persisten limitaciones, como dificultad para gestionar escenarios en tiempo real e interoperabilidad con sistemas legados (Amador-Donado et al., 2024a, 2024b). Estas serán abordadas mediante escenarios simulados de ciberataques sin comprometer la IC real (https://acortar.link/8yMNIt).

7. Referencias

Amador Donado, S., Pardo Calvache, C. J., & Raúl Iván, M. P. (2024a). Preliminary Review: Cybersecurity for Operation Technology in Quantum Age Against Network Attacks to Critical Infrastructures. *INGE CUC*, *20*(2), 1-16. https://doi.org/10.17981/ingecuc.20.2.2024.06

Amador-Donado, S., Pardo-Calvache, C.-J., & Mazo-Peña, R. (2024b). *MoRCiTO: Towards a Cybersecurity Reference Model for Operation Technology in Preparation for the Quantum Era to Prevent Network Attacks on Cyber-Physical Systems in Critical Infrastructures*. 22-46. https://revistas.udistrital.edu.co/index.php/revcie/article/view/22581/20496

Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. *Nature*, *549*(7671), 188-194. https://doi.org/10.1038/nature23461

Diamanti, E., Lo, H.-K., Qi, B., & Yuan, Z. (2016). Practical challenges in quantum key distribution. *npj Quantum Information*, *2*(1). https://doi.org/10.1038/npjqi.2016.25

Kalinin, M., & Krundyshev, V. (2022). Security intrusion detection using quantum machine learning techniques. *Journal of Computer Virology and Hacking Techniques*, *19*(1), 125-136. https://doi.org/10.1007/s11416-022-00435-0

Kayan, H., Nunes, M., Rana, O., Burnap, P., & Perera, C. (2022). Cybersecurity of Industrial Cyber-Physical Systems: A Review. *ACM Computing Surveys*, *54*(11s), 1-35. https://doi.org/10.1145/3510410

Kitchenham, B., & Charters, S. (2007). *Guidelines for performing systematic literature reviews in software engineering*. UK.

Liu, R., Rozenman, G. G., Kundu, N. K., Chandra, D., & De, D. (2022). Towards the industrialisation of quantum key distribution in communication networks: A short survey. *IET Quantum Communication*, *3*(3), 151-163. https://doi.org/10.1049/qtc2.12044

Mertler, C. A. (2020). *Action Research*. SAGE Publications. https://a.co/d/iS4GfIr