UNIVERSIDAD DISTRITAL
FRANCISCO JOSÉ DE CALDAS

Revista Científica

http://revistas.udistrital.edu.co/ojs/index.php/revcie/index

Artículo de investigación científica

MoRCiTO: hacia un modelo de referencia de ciberseguridad para la tecnología de la operación como preparación para la era cuántica, a fin de prevenir ataques de red a sistemas ciber-físicos en infraestructuras críticas

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

MoRCiTO: em busca de um modelo de referência de cibersegurança para a tecnologia da operação como preparação para a era quântica, a fim de prevenir ataques de rede contra sistemas ciber-físicos em infraestruturas críticas

Siler Amador-Donado[1]
César-Jesús Pardo-Calvache[2]
Raúl Mazo-Peña[3]

Recibido: 15 de Agosto de 2024 **Aceptado:** 03 de Diciembre de 2024

Para citar este artículo: Amador-Donado, S., Pardo-Calvache, C. J. y Mazo-Peña, R. (2024). MoRCiTO: hacia un modelo de referencia de ciberseguridad para la tecnología de la operación como preparación para la era cuántica, a fin de prevenir ataques de red a sistemas ciber-físicos en infraestructuras críticas. *Revista Científica*, *51*(3), 22-46. https://doi.org/10.14483/23448350.22581

Resumen

En esta publicación se propone un modelo de referencia de ciberseguridad para la tecnología de la operación (MoRCiTO) como preparación para la era cuántica para prevenir ataques de red a sistemas ciber-físicos (SCF) en infraestructuras críticas (IC). El modelo propuesto es el resultado de una revisión de estudios primarios que abordan diferentes aspectos como, entre otros, las amenazas de los equipos cuánticos contra los sistemas criptográficos actuales (así como las que aún están por aparecer), permitiendo caracterizar el modelo de referencia propuesto. Este trabajo contribuye significativamente al campo de la ciberseguridad, proporcionando un modelo de referencia adaptado a la inminente llegada de la era cuántica. Es un paso crucial hacia la preparación de IC contra amenazas avanzadas y establece una base sólida para investigaciones futuras en el área de la ciberseguridad cuántica. Además, el modelo puede ser adoptado por entidades gubernamentales y organizaciones encargadas de la gestión de IC para fortalecer su resiliencia ante posibles ataques cuánticos. Su implementación ayudará a garantizar la continuidad operativa y la protección de sistemas vitales en un entorno de amenazas en constante evolución.

Palabras clave: amenazas; ciberseguridad; criptografía; distribución de clave cuántica; era cuántica; infraestructuras críticas; modelo de referencia; sistemas ciber-físicos; tecnología de la operación; vulnerabilidades.

1. Ph. D. Universidad del Cauca (Popayán, Colombia). samador@unicauca.edu.co
2. Ph. D. Universidad del Cauca (Popayán, Colombia). cpardo@unicauca.edu.co
3. Ph. D. Universidad del Cauca (Popayán, Colombia). raul.mazo@ensta-bretagne.fr

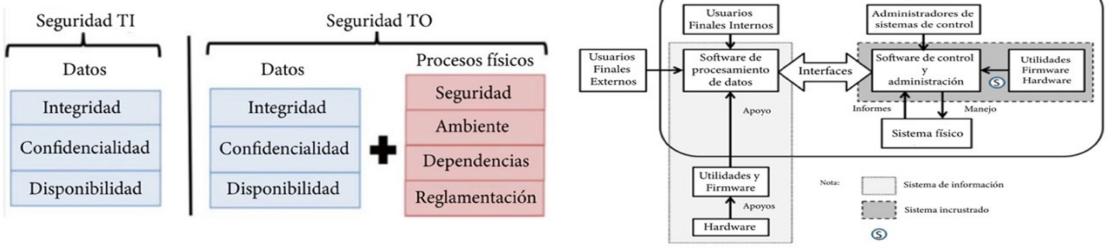
Abstract
This publication proposes a cybersecurity reference model for operation technology (MoRCiTO) as preparation for the quantum era to prevent network attacks on cyber-physical systems (CPS) in critical infrastructures (CI). The proposed model is the result of a review of primary studies that address different aspects such as, among others, the threats of quantum equipment against current cryptographic systems (as well as those that are yet to appear), enabling the characterization of the proposed reference model. This work contributes significantly to the field of cybersecurity, providing a reference model tailored to the imminent arrival of the quantum era. It is a crucial step towards CI preparedness against advanced threats and establishes a solid foundation for future research in quantum cybersecurity area. In addition, the model can be adopted by government entities and organizations in charge of CI management to strengthen their resilience against potential quantum attacks. Its implementation will help to ensure operational continuity and the protection of vital systems in a constantly evolving threat environment.
Keywords: critical infrastructures; cryptography; cyber-physical systems; cybersecurity; operation technology; quantum era; Quantum Key Distribution; reference model; threats; vulnerabilities.

Resumo
Esta publicação propõe um modelo de referência de segurança cibernética para a tecnologia de operação (MoRCiTO) como preparação para a era quântica, a fim de evitar ataques de rede a sistemas ciberfísicos (CPS) em infraestruturas críticas (CI). O modelo proposto é o resultado de uma revisão de estudos primários que abordam diferentes aspectos, como, entre outros, as ameaças de equipamentos quânticos contra os sistemas criptográficos atuais (bem como aqueles que ainda estão por surgir), permitindo a caracterização do modelo de referência proposto. Este trabalho contribui significativamente para o campo da segurança cibernética, fornecendo um modelo de referência adaptado à chegada iminente da era quântica. É uma etapa crucial para a preparação da CI contra ameaças avançadas e estabelece uma base sólida para pesquisas futuras na área de segurança cibernética quântica. Além disso, o modelo pode ser adotado por entidades governamentais e organizações responsáveis pela gestão de IC para fortalecer sua resiliência contra possíveis ataques quânticos. Sua implementação ajudará a garantir a continuidade operacional e a proteção de sistemas vitais em um ambiente de ameaças em constante evolução.
Palavras-chaves: ameaças; criptografía; distribuição de chaves quânticas; era quântica; infraestruturas críticas; modelo de referencia; segurança cibernética; sistemas ciberfísicos; tecnologia de operação; vulnerabilidades.

INTRODUCCIÓN

Las ciber-amenazas y los ciber-ataques en las tecnologías de la información (TI) y su impacto directo sobre los datos son bastante comunes, estudiados y difundidos por expertos de ciberseguridad. Sin embargo, en las tecnologías de la operación (TO), estos mismos problemas pueden impactar de diferentes formas, como causar la muerte de una persona que opere o utilice un dispositivo ciber-físico (DCF), *e.g.*, el uso de un implante, válvula cardíaca o marca paso. Incluso, un descuido de un operario de una planta de energía nuclear al usar un dispositivo de almacenamiento universal serial bus (USB) infectado podría causar una catástrofe nuclear o incluso una guerra entre naciones si el ciber-ataque es sobre una infraestructura crítica (IC) (Figura 1a). Para aclarar términos, es necesario hacer la siguiente distinción: mientras que la TI se ocupa del mantenimiento, el desarrollo y el uso de *software*, sistemas informáticos y redes para procesar y distribuir datos, la TO se relaciona con el funcionamiento conjunto de *hardware* y *software*, y su fin es detectar o provocar cambios a través del monitoreo y/o control directo de dispositivos físicos,

procesos y eventos en un ente, organización o IC (Hahn, 2016). La Figura 1b presenta cómo se fusionan los componentes *ciber* que hacen parte del *sistema de información* junto con los componentes *físicos* que hacen parte del *sistema embebido*, obteniendo como resultado final un *sistema ciber-físico* (SCF) que pertenece a la TO.



(a). Requerimientos operacionales de TO vs TI.
Fuente: Traducido de (Hahn, 2016)

(b). Componentes ciber y físicos de SCF.
Fuente: Traducido de (Axelrod, 2013)

Figura 1. Requerimientos operacionales y componentes de los SCF.

En noviembre de 2017, se presentaron 82 algoritmos criptográficos candidatos al Instituto Nacional de Estándares y Tecnología (NIST) para participar en una competencia pública, cuyo fin era seleccionar algoritmos de criptografía post-cuántica (PQC) (Alagic *et al.*, 2019). Esta iniciativa se lanzó para contrarrestar las ciber-amenazas inminentes de los equipos cuánticos, que podrían volverse una realidad para el año 2030, cuando estén disponibles y sean completamente funcionales (Hoschek, 2021). Estos equipos cuánticos podrán ejecutar algoritmos con la capacidad de vulnerar la mayoría de los algoritmos criptográficos asimétricos actuales, como es el caso de los algoritmos Rivest, Shamir y Adleman (RSA) o el cifrado de curvas elípticas (ECC), muy utilizados en la mayoría de las IC (Raheman, 2022).

Por esta razón, y a partir de una revisión sistemática de la literatura presentada en (Amador Donado *et al.*, por publicar), se pudo observar que, aunque existen marcos de trabajos de ciberseguridad y de gestión del riesgo, modelos de amenazas cuánticas y de referencia de ciberseguridad, y estándares que consideran la ciberseguridad de los SCF en IC, es muy probable que se identifiquen nuevas vulnerabilidades ante el advenimiento de la era cuántica. Según las capacidades de los adversarios con respecto a los ciber-ataques de red a través de los algoritmos criptográficos que se usan actualmente en las TO, estas amenazas podrían prevenirse a través de modelos de referencia como el de Purdue (W. Xu *et al.*, 2019; Haney, 2019; Cruz & Simões, 2021; Tao *et al.*, 2019; Simonov *et al.*, 2019; Cook *et al.*, 2016), un modelo adoptado por el estándar IEC-62443 que incluye una zona empresarial, una zona desmilitarizada (DMZ) y una zona de control. Sin embargo, aún no se evidencia un modelo de referencia que caracterice los componentes necesarios y que le permita a las IC prepararse para las ciber-amenazas que se proyectan con el advenimiento de la era cuántica. Algunas de las principales ciber-amenazas y vulnerabilidades son, entre otras, (i) la interceptación cuántica: la implementación de enlaces cuánticos y la infraestructura de comunicación cuántica presentarán desafíos significativos que deben abordarse para prevenir la interceptación (Dutta & Bhuyan, 2024); (ii) la manipulación de qubits: la revisión sobre criptografía cuántica destaca la necesidad de mecanismos robustos para prevenir la manipulación de qubits y asegurar la comunicación (Pirandola *et al.*, 2020); (iii) los ataques a protocolos de criptografía cuántica: la distribución de claves cuánticas (QKD) puede ser vulnerable a fallos en el *hardware* o a errores en la implementación del *software* (Vermeer *et al.*, 2023; Akter, 2023); (iv) amenazas internas: los ataques internos, donde empleados o infiltrados comprometen la infraestructura clásica o actual –y, a mediano plazo, la cuántica– dentro de una organización representan

un riesgo considerable (Vermeer *et al.*, 2023); (v) limitaciones en la estandarización: la falta de estándares globales para la seguridad cuántica conllevar implementaciones vulnerables (Pirandola *et al.*, 2020).

Con el objetivo de proponer un modelo que describa de forma detallada los aspectos a considerar por parte de la industria de TO y profesionales de la ciberseguridad, se definió MoRCiTO, un modelo que caracteriza los aspectos de seguridad más significativos en este campo, junto con los siguientes elementos: objetivos, alcance, componentes, principios, adaptaciones al advenimiento de la cuántica, evaluación y validación, y adaptaciones e implementación. Además de la presente introducción, este artículo está estructurado de la siguiente manera: una sección que describe los métodos de investigación utilizados para la definición del modelo propuesto, otra que presenta los resultados obtenidos respecto a la definición de los aspectos que conforman el modelo y una última que discute las conclusiones, el trabajo futuro, los resultados obtenidos y las principales observaciones de esta investigación.

METODOLOGÍA

Se llevó a cabo una revisión sistemática de la literatura presentada en Amador Donado *et al*. (por publicar), mediante la cual fue posible identificar 20 aspectos (Tabla 1). Estos aspectos se detallaron a través de un conjunto de preguntas que permitieron determinar sus elementos relevantes. Debido a la limitación en el espacio de esta revista, las respuestas a las preguntas planteadas para los 12 primeros aspectos se pueden consultar en detalle en el siguiente link:

https://drive.google.com/file/d/1aR6MrvXIwl7I5F7qncr3Yo3tOe7KmpA5/view. Estos aspectos fueron clasificados como elementos de interés muy alto, según la escala de calor que se muestra en la Tabla 2.

Tabla 1. Caracterización de 20 aspectos de ciberseguridad en SCF ante el advenimiento de la era cuántica

#	Aspectos	Evaluación de los aspectos caracterizados	Identificador	Referencias
I	Establecer estándares de ciberseguridad cuántica	1.1 ¿Cómo participar en la creación de estándares y regulaciones relacionados con la ciberseguridad cuántica? 1.2 ¿Qué estándares y regulaciones existen relacionadas con la ciberseguridad cuántica? 1.3 ¿Cómo identificar las mejores prácticas de ciberseguridad cuántica?	**A1, A2, A3, A4, A5, A6, A7, A8, A9, A10**	(Pitwon & Lee, 2021; Rodríguez, 2023; Yesina, Ostrianska, *et al.*, 2022; Hossain Faruk *et al.*, 2022; Walenta *et al.*, 2015; Taiber, 2020; Teodoraș *et al.*, 2023; Ahn *et al.*, 2021; Mosca, 2018), (F. Xu *et al.*, 2020)
II	Escalada de amenazas	2.1 ¿De qué manera el aumento en las capacidades cuánticas de los atacantes contribuye a una escalada de amenazas cibernéticas que afectan la seguridad de los sistemas informáticos e infraestructuras? 2.2 ¿Cuáles son los desafíos y requisitos para desarrollar e implementar respuestas de seguridad sofisticadas y avanzadas capaces de contrarrestar efectivamente la escalada de amenazas impulsada por las capacidades cuánticas crecientes de los atacantes?	**A11, A12, A13, A14, A15, A16, A17, A18**	(Caicedo, 2017; Yao & Almohri, 2013; Sperotto *et al.*, 2015; Ponnusamy *et al.*, 2020; Streich, 2023; Olofinbiyi, 2022; Shane, 2012; Flowers *et al.*, 2013)
III	Integración de tecnologías cuánticas	3.1 ¿Cuáles son los desafíos y complejidades involucrados en la incorporación de tecnologías cuánticas, como la computación cuántica y la comunicación cuántica, en las infraestructuras existentes? 3.2 ¿Qué riesgos potenciales y problemas de seguridad pueden surgir si la integración de tecnologías cuánticas en infraestructuras existentes no se realiza de manera adecuada y cuidadosa?	**A19, A20, A21, A22, A23, A24, A25, A26**	(I. Khan, 2018; Hughes *et al.*, 2013; Karol & Życzkowski, 2015; Schwalb, 2007; Carle *et al.*, 2012; Hamza *et al.*, 2020; Mistry *et al.*, 2021; Majumder *et al.*, 2023)
IV	Cambios tecnológicos continuos	4.1 ¿Cuál es la importancia de que las infraestructuras críticas se adapten continuamente a nuevas tecnologías, incluidas las cuánticas, para garantizar un nivel de seguridad óptimo? 4.2 ¿Cuáles son los principales desafíos y necesidades que enfrentan las infraestructuras críticas para mantenerse al día con los avances rápidos y constantes en la tecnología cuántica?	**A19, A27, A28, A29, A30, A31, A32, A33**	(I. Khan, 2018; Ståhl, 2013; Antoliš *et al.*, 2015; European Commission, 2017; Alcaraz & Zeadally, 2015; Popescu, 2019; Goy *et al.*, 2021; Pătrașcu, 2021)

V	Gestión de recursos	5.1 ¿Cuál es el impacto financiero y de recursos que implica la implementación de medidas de seguridad cuántica en organizaciones y entidades? 5.2 ¿Cómo contribuye la falta de fondos y de recursos adecuados a debilitar la ciberseguridad y la protección frente a amenazas cibernéticas emergentes?	**A15, A16, A17, A18, A25, A34, A35, A36**	(Streich, 2023; Olofinbiyi, 2022; Shane, 2012; Flowers *et al.*, 2013; Mistry *et al.*, 2021; Campbell, Sr., 2020; Pohasii *et al.*, 2022; Sturgeon, 2012)
VI	Resiliencia y continuidad operativa	6.1 ¿Qué planes de contingencia y recuperación existen que tengan en cuenta ataques cuánticos y su impacto en la operación? 6.2 ¿Cómo garantizar la resiliencia de sistemas ciberfísicos y la continuidad de las operaciones críticas?	**A9, A37, A38, A39, A40, A41, A42, A43**	(Mosca, 2018; Alcaraz, 2018; Woo *et al.*, 2008; Zobel & Khansa, 2012; Rieffel *et al.*, 2015; Mihalache *et al.*, 2019; Abdi *et al.*, 2018; Ali, 2021)
VII	Colaboración interdisciplinaria	7.1 ¿Cómo fomentar la colaboración entre expertos en ciberseguridad, computación cuántica y tecnología de la operación? 7.2 ¿Cómo abordar los desafíos desde una perspectiva interdisciplinaria para proponer soluciones integrales?	**A44, A45, A46, A47, A48, A49, A50, A51**	(Holley, 2009; Hui *et al.*, 2010; Bililign, 2013; Witteman & Stahl, 2013; Ramírez & Choucri, 2016; Rajamaki, 2018; Kneller & Fayans, 2019; Albataineh & Nijim, 2021)
VIII	Actualizar infraestructuras heredadas	8.1 ¿Cómo actualizar las infraestructuras ciberfísicas para aplicar medidas de seguridad cuántica? 8.2 ¿Cómo evaluar la compatibilidad de las tecnologías cuánticas con los sistemas heredados y diseñar estrategias de transición?	**A8, A52, A53, A54, A55, A56, A57, A58**	(Ahn *et al.*, 2021; Serrano *et al.*, 2023; A. A. Khan *et al.*, por publicar; Linke *et al.*, 2017; Malina *et al.*, 2023; Aguado *et al.*, 2018; Paul *et al.*, 2022; Pérez-Castillo *et al.*, 2021)
IX	Gestionar claves cuánticas	9.1 ¿Qué protocolos se deben establecer para la generación, distribución y administración de llaves cuánticas? 9.2 ¿Cómo asegurar la integridad y autenticidad de las llaves cuánticas para prevenir ataques?	**A59, A60, A61, A62, A63, A64, A65, A66**	(Singh *et al.*, 2014; G. Xu *et al.*, 2015; Kalra & Poonia, 2017; Bruß & Lütkenhaus, 2000; Goorden *et al.*, 2014; Jain *et al.*, 2016; Cerf *et al.*, 2002; Dixon *et al.*, 2017)
X	Implementar QKD	10.1 ¿Cómo implementar QKD para garantizar la distribución segura de claves en sistemas ciberfísicos? 10.2 ¿Cómo diseñar e integrar QKD en la infraestructura de TO?	**A67, A68, A69, A70, A71, A72, A73, A74**	(Luo *et al.*, 2023; Cao *et al.*, 2017; Tomita, 2019; Mink *et al.*, 2010; Gatto *et al.*, 2022; Martelli *et al.*, 2021; Zavitsanos *et al.*, 2022; Lancho *et al.*, 2010)
XI	Desarrollar algoritmos cuántico-resistentes	11.1 ¿Cuáles son los algoritmos criptográficos resistentes a ataques cuánticos que existen? 11.2 ¿Qué mecanismos de cifrado y autenticación pueden soportar la capacidad de cálculo cuántico?	**A75, A76, A77, A78, A79, A80, A81, A82**	(Kumar Rao *et al.*, 2017; Perlner & Cooper, 2009; Fernández-Carames & Fraga-Lamas, 2020; S. Mao *et al.*, 2014; Kumar *et al.*, 2019; Kanamori *et al.*, 2009; Kanamori *et al.*, 2005; Fehr & Salvail, 2017)
XII	Identificar amenazas cuánticas	12.1 ¿Cómo reconocer nuevas amenazas cuánticas contra los algoritmos criptográficos actuales de los SCF? 12.2 ¿Cómo las amenazas pueden afectar los sistemas ciberfísicos en infraestructuras de TO?	**A42, A83, A84, A85, A86, A87, A88, A89**	(Ali, 2021; Raheman, 2022; Käppler & Schneider, 2021; Yesina, Potii, *et al.*, 2022; Taylor & Sharif, 2017; Zhang *et al.*, 2013; Karim & Phoha, 2014; Huang *et al.*, 2018)
XIII	Amenazas Internas	13.1 ¿De qué manera las amenazas internas, provenientes de empleados malintencionados o descuidados, comprometen la seguridad de las infraestructuras críticas? 13.2 ¿Cuáles son las estrategias y medidas más efectivas y esenciales que se deben implementar para proteger las infraestructuras críticas contra amenazas internas específicas?	**A11, A22, A23, A90, A91, A92**	(Caicedo, 2017; Schwalb, 2007; Carle *et al.*, 2012; Lu *et al.*, 2019; Nkongolo *et al.*, 2022; Dacier *et al.*, 2014),
XIV	Amenazas cibernéticas en evolución	14.1 ¿Cómo influye el avance de la tecnología cuántica en la evolución y el fortalecimiento de las amenazas cibernéticas? 14.2 ¿En qué medida las defensas cibernéticas actuales son insuficientes para contrarrestar las amenazas emergentes y de rápida evolución asociadas a las capacidades ofensivas cuánticas?	**A34, A36, A93, A94, A95, A96**	(Campbell Sr., 2020; Sturgeon, 2012; Rajna, 2015; Nair & Patil, 2020; McMurdo, 2014; Jahanian, 2011)

XV	Regulaciones Insuficientes	15.1 ¿Cuál es el impacto de la falta de regulaciones específicas para la ciberseguridad cuántica en la protección de infraestructuras críticas? 15.2 ¿Por qué es esencial que los gobiernos y organismos reguladores desarrollen pautas claras y eficaces para la ciberseguridad cuántica, y cuál sería el papel de estas pautas en la mitigación de riesgos asociados?	**A31, A36, A97, A98, A99, A100, A101**	(Popescu, 2019; Sturgeon, 2012; Haber & Zarsky, 2017; Knapp & Langill, 2015; Ludvigsen & Nagaraja, 2022; Clark-Ginsberg & Slayton, 2019; Laughlin, 2016)
XVI	Entrenar y concienciar en ciberseguridad cuántica	16.1 ¿Cómo educar al personal sobre amenazas y soluciones en ciberseguridad cuántica? 16.2 ¿Cómo capacitar a los equipos de operación en la detección y respuesta a los ataques cuánticos?	**A4, A102, A103, A104, A105, A106, A107**	(Hossain Faruk *et al.*, 2022; Holdsworth & Apeh, 2017; Sharevski *et al.*, 2018; Schneider, 2013; Zhao *et al.*, 2008; Choi *et al.*, 2020; Gras *et al.*, 2021)
XVII	Colaboración internacional	17.1 ¿Por qué es esencial la colaboración a nivel internacional para fortalecer la seguridad de las infraestructuras críticas y cuáles son los beneficios derivados de esta cooperación global? 17.2 ¿Cómo puede la falta de cooperación y coordinación internacional generar brechas y vulnerabilidades en la ciberseguridad de las infraestructuras críticas, y cuáles son los riesgos asociados a esta falta de colaboración global?	**A11, A22, A23, A108, A109**	(Caicedo, 2017; Schwalb, 2007; Carle *et al.*, 2012; (Busby, 2000; Fu, 2015)
XVIII	Monitorizar y detectar ataques cuánticos	18.1 ¿Qué sistemas de monitorización existen que puedan detectar actividades inusuales o ataques cuánticos en tiempo real? 18.2 ¿Cómo integrar tecnologías de análisis de datos y aprendizaje automático que identifiquen patrones de ataque cuántico?	**A110, A111, A112, A113, A114, A115**	(Adam *et al.*, 2008; W. Liu *et al.*, 2017; Baykara *et al.*, 2018; Y. Mao *et al.*, 2020; Al-Mohammed *et al.*, 2021; Payares & Martínez-Santos, 2021)
XIX	Resistencia a la era cuántica	19.1 ¿Cuáles son las principales dificultades y desafíos inherentes a la era cuántica y comprensión completa de las amenazas cuánticas en el ámbito de la ciberseguridad? 19.2 ¿Cómo afectan estas dificultades y desafíos en la evaluación efectiva de riesgos y en la toma de decisiones informadas relacionadas con la protección contra amenazas cuánticas?	**A23, A24, A25, A116, A117**	(Carle *et al.*, 2012; Hamza *et al.*, 2020; Mistry *et al.*, 2021; Hartman, 2012; Tian *et al.*, 2020)
XX	Vulnerabilidades de proveedores y terceros	20.1 ¿De qué manera puede la participación de proveedores y terceros con acceso a sistemas críticos introducir vulnerabilidades en estos sistemas? 20.2 ¿Cuál es el rol crucial de la gestión de la cadena de suministro y la debida diligencia en la mitigación de riesgos y vulnerabilidades introducidas por proveedores y terceros en sistemas críticos?	**A11, A22, A23, A109, A118**	(Caicedo, 2017; Schwalb, 2007; Carle *et al.*, 2012; Fu, 2015; Tyshyk, 2022)

Luego de analizar los estudios más relevantes, de donde se obtuvo la caracterización de los elementos del modelo, se elaboró un mapa de calor para identificar la mayor cantidad de publicaciones que tuvieron alta relevancia en los aspectos caracterizados. La Tabla 2 revela una evolución significativa en la investigación en ciberseguridad cuántica a lo largo de diferentes periodos. La escala de calor muestra un aumento notorio en la actividad investigativa, alcanzando su punto máximo en el periodo 2020-2023. Múltiples aspectos experimentan crecimientos diversos, desde aquellos con una baja respuesta inicial, como *establecer estándares de ciberseguridad cuántica* y *escalada de amenazas*, los cuales presentan un aumento significativo en las publicaciones; hasta temas con alta y muy alta respuesta, como *desarrollar algoritmos cuántico-resistentes* y *amenazas cibernéticas en evolución*, que reciben una atención sustancial. El promedio por periodo revela una tendencia creciente, indicando diversificación y profundización en la investigación en ciberseguridad cuántica. En conjunto, estos hallazgos destacan un aumento generalizado en la atención y dedicación a una variedad de aspectos cruciales para abordar los desafíos emergentes en el ámbito de la ciberseguridad cuántica.

Tabla 2. Mapa de calor de la cantidad de publicaciones por aspectos caracterizados en los cuatro periodos

	Aspectos/contextos caracterizados	Periodo 2000-2011	Periodo 2012-2015	Periodo 2016-2019	Periodo 2020-2023	Total
1	Establecer estándares de ciberseguridad cuántica	0	1	1	8	10
2	Escalada de Amenazas	0	4	1	3	8
3	Integración de Tecnologías Cuánticas	1	3	1	3	8
4	Cambios Tecnológicos Continuos	0	3	3	2	8
5	Gestión de Recursos	0	3	0	5	8
6	Resiliencia y continuidad operativa	1	2	4	1	8
7	Colaboración interdisciplinaria	2	2	3	1	8
8	Actualizar infraestructuras heredadas	0	0	2	6	8
9	Gestionar claves cuánticas	2	4	2	0	8
10	Implementar QKD	2	0	2	4	8
11	Desarrollar algoritmos cuántico-resistentes	3	1	3	1	8
12	Identificar amenazas cuánticas	0	2	2	4	8
13	Regulaciones Insuficientes	0	2	4	1	7
14	Entrenar y concienciar en ciberseguridad cuántica	1	1	2	3	7
15	Amenazas Internas	1	2	2	1	6
16	Amenazas Cibernéticas en Evolución	1	3	0	2	6
17	Monitorizar y detectar ataques cuánticos	1	0	2	3	6
18	Colaboración Internacional	2	2	1	0	5
19	Resistencia a la era cuántica	0	2	0	3	5
20	Vulnerabilidades de Proveedores y Terceros	1	2	1	1	5
	Promedio por periodo	0.90	1.95	1.8	2.6	7.25

ESCALA DE CALOR	
0 - 1	**Ninguna o muy poca** cantidad de publicaciones que dieron resapuesta a los aspectos caracterizados evaluados.
2 - 3	**Poca** cantidad de publicaciones que dieron resapuesta a los aspectos caracterizados evaluados.
4 - 5	**Suficiente** cantidad de publicaciones que dieron resapuesta a los aspectos caracterizados evaluados.
6 - 7	**Alta** cantidad de publicaciones que dieron resapuesta a los aspectos caracterizados evaluados.
8 - 10	**Muy alta** cantidad de publicaciones que dieron resapuesta a los aspectos caracterizados evaluados.

RESULTADOS

En esta sección se presenta el modelo de referencia de ciberseguridad MorCiTO, junto con sus objetivos, alcance, componentes, principios, adaptaciones al advenimiento de la era cuántica, evaluación, validación, ajustes e implementación. Además, al final de esta sección se presenta una adaptación al mapa de dominios de Jiang, presentado en el 2021 en https://app.box.com/s/sj5xaz8a1461e7u7si3ip1361r070fed/file/822847297651, el cual permite analizar la ciberseguridad desde el punto de vista de sus componentes para la toma de decisiones –esta propuesta ha sido actualizada.

Modelo de referencia de ciberseguridad – MorCiTO

Luego de caracterizar los elementos del modelo de referencia de ciberseguridad para prevenir ataques de red a SCF en IC ante el advenimiento de la tecnología cuántica, se elaboró su versión 1.0, que se presenta en la Figura 2. Esta Figura resume los elementos que conforman el modelo, entre ellos sus objetivos, alcance, componentes, principios, adaptaciones al advenimiento de la era cuántica, evaluación, validación, ajustes e implementación. Estos elementos se detallan a continuación.

Objetivos y alcance

A continuación, en la Tabla 3 se presentan minuciosamente los objetivos establecidos para el modelo, así como el alcance del mismo. Estos elementos, en conjunto con los presentados en las siguientes secciones, se describen teniendo en cuenta su caracterización, procedimientos, actividades y referencias relacionadas.

Tabla 3. Objetivos y alcance del modelo de referencia

Procesos	Caracterización	Procedimientos	Actividades	Referencias
Definición de los objetivos del modelo de referencia	Proteger la integridad y confidencialidad de los SCF	Desarrollar y documentar políticas y procedimientos robustos de seguridad	Crear un protocolo de cifrado de datos utilizando AES y establecer políticas de acceso basado en roles (RBAC)	(NIST, 2020)
	Mitigar los riesgos de ataques de red cuánticos	Implementar técnicas de criptografía poscuántica	Utilizar algoritmos de criptografía resistentes a ataques cuánticos como Lattice-Based Cryptography	(Bernstein *et al.*, 2017)
	Establecer mejores prácticas de ciberseguridad	Desarrollar y mantener un manual de mejores prácticas de ciberseguridad	Publicar un manual con pautas actualizadas para la gestión de contraseñas y autenticación multifactor (MFA)	(ENISA, 2018)
	Promover la colaboración y el intercambio de conocimientos	Organizar talleres y seminarios periódicos	Realizar seminarios mensuales sobre las últimas amenazas cibernéticas y estrategias de mitigación	(Zhao & White, 2014)
Delimitación del alcance del modelo. Se especifican las áreas o aspectos de la ciberseguridad y las infraestructuras críticas que se abarcan	Tipos de infraestructuras críticas	Identificar y catalogar las IC	Crear un registro detallado de infraestructuras, *e.g.*, plantas de energía, sistemas de transporte, hospitales y redes de telecomunicaciones, entre otras	(CISA, 2021)
	Sistemas ciber-físicos involucrados	Enumerar y describir los sistemas ciber-físicos que serán protegidos	Documentar todos los sistemas de control industrial (ICS) y dispositivos IoT en uso	(NIST, 2015)
	Amenazas y ataques específicos	Realizar un análisis de amenazas detallado para identificar posibles vectores de ataque	Identificar posibles vectores de ataque, *e.g.*, *malware* cuántico y ataques cuánticos de denegación de servicio	(Schneier, 2018)
	Aspectos de ciberseguridad abarcados	Definir claramente los dominios de ciberseguridad que el modelo abarcará	Incluir protección de datos, gestión de identidad, seguridad de red y respuesta a incidentes	(ISO/IEC 27001, 2013)
	Consideraciones tecnológicas	Evaluar las tecnologías actuales y emergentes relevantes para la ciberseguridad	Analizar la compatibilidad de los sistemas actuales con tecnologías de criptografía cuántica y su impacto en la infraestructura existente	(Campagna *et al.*, 2015)

Figura 2. Modelo de referencia de ciberseguridad de tecnología de la operación (MoRCiTO), ver. 1.0

Componentes

A continuación, en la Tabla 4 se presentan de manera detallada los componentes definidos para el modelo. Estos componentes funcionan de manera integrada para establecer un enfoque holístico de seguridad en las IC: las *políticas de seguridad* brindan las directrices generales, los *controles de acceso* garantizan la protección de los sistemas y los datos, la *detección y respuesta a incidentes* permite una respuesta eficiente a los ciberataques, la *gestión de riesgos* identifica y mitiga los riesgos potenciales, la *criptografía* y la *seguridad de la comunicación* protegen la confidencialidad de los datos y las *actualizaciones* y los *parches de seguridad* mantienen los sistemas actualizados y protegidos.

Tabla 4. Componentes esenciales del modelo de referencia

Procesos	Caracterización	Procedimientos	Actividades	Referencias
Identificación de los componentes esenciales del modelo, descripción de sus funciones y el propósito de cada uno, así como su interacción con otros elementos del mismo	Políticas de seguridad	Redactar y mantener políticas de seguridad que cubran todos los aspectos de la protección de datos y sistemas	Crear una política de uso aceptable (*acceptable use policy*, AUP) para dispositivos y redes	(Whitman & Mattord, 2018)
	Controles de acceso	Implementar y gestionar mecanismos de control de acceso adecuados	Configurar sistemas de autenticación biométrica y tarjetas inteligentes para garantizar que solo el personal autorizado tenga acceso a ciertos sistemas	(Sandhu *et al.*, 1996)
	Detección y respuesta a incidentes	Desarrollar un plan de respuesta a incidentes que permita una respuesta eficiente y efectiva	Establecer un equipo de respuesta a incidentes de ciberseguridad (CSIRT) y definir protocolos de actuación ante incidentes	(NIST, 2012)
	Gestión de riesgos	Realizar evaluaciones periódicas de riesgos para identificar y mitigar amenazas potenciales	Utilizar matrices de riesgos para priorizar y mitigar amenazas específicas a la IC	(ISO, 2018)
	Criptografía y seguridad de la comunicación	Implementar soluciones criptográficas robustas para proteger la confidencialidad e integridad de las comunicaciones	Utilizar criptografía de clave pública (*public key infrastructure*, PKI) para proteger las comunicaciones entre sistemas	(Diffie & Hellman, 1976)
	Actualizaciones y parches de seguridad	Establecer un proceso continuo de gestión de parches y actualizaciones de seguridad	Programar actualizaciones de *software* regulares y automatizadas para asegurar que todos los sistemas estén protegidos contra vulnerabilidades conocidas	(Microsoft, 2021)

Principios y enfoque de seguridad

A continuación, en la Tabla 5 se presentan en detalle los principios fundamentales que guían el diseño y los enfoques específicos del modelo.

Tabla 5. Principios y enfoque de ciberseguridad

Procesos	Caracterización	Procedimientos	Actividades	Referencias
Establecimiento de los principios fundamentales que guían el diseño y la implementación del modelo de referencia	Integralidad	Asegurar que todas las medidas de ciberseguridad sean integrales y abarquen todos los aspectos necesarios	Desarrollar un plan de seguridad que integre la protección física y lógica, incluyendo sistemas de detección de intrusos (IDS) y controles de acceso físico	(Tummala & Schoenherr, 2011)
	Adaptabilidad	Garantizar que el modelo de ciberseguridad pueda adaptarse a nuevos desafíos y amenazas emergentes	Revisar y actualizar las políticas de ciberseguridad periódicamente e incorporar las últimas investigaciones y tecnologías	(Baracaldo & Joshi, 2009)
	Enfoque basado en riesgos	Priorizar acciones de ciberseguridad basadas en la evaluación continua de riesgos y la implementación de medidas de mitigación	Concentrar recursos en proteger activos de alto valor o vulnerabilidad crítica, utilizando análisis de riesgos detallados	(NIST, 2002)
	Colaboración y coordinación	Fomentar la cooperación y coordinación entre distintas entidades y equipos de ciberseguridad	Crear comités interdepartamentales de ciberseguridad que se reúnan regularmente para discutir amenazas y estrategias	(SANS Institute, 2019)
	Actualización continua	Mantenerse al día con las últimas amenazas y tecnologías emergentes mediante actualizaciones continuas de las políticas y procedimientos de ciberseguridad	Asistir a conferencias de ciberseguridad y actualizar las prácticas según las tendencias actuales y futuros desarrollos tecnológicos	(Ponemon Institute, 2020)
	Cumplimiento normativo	Asegurar que todas las acciones de ciberseguridad cumplan con las regulaciones y normativas aplicables a la industria	Verificar y garantizar el cumplimiento con normativas como ISO 27001, NIST SP 800-53, y el Reglamento General de Protección de Datos (GDPR)	(European Union, 2018)
Consideraciones de los enfoques de ciberseguridad específicos	Criptografía cuántica o poscuántica	Implementar métodos criptográficos que sean seguros contra ciber-ataques cuánticos	Adoptar algoritmos como Criptografía Lattice, Multivariate Quadratic Equations y Hash-Based Cryptography	(Bernstein *et al.*, 2017)
	Autenticación cuántica	Utilizar técnicas de autenticación basadas en principios de la física cuántica	Implementar sistemas de autenticación basados en entrelazamiento cuántico para garantizar la autenticidad de las comunicaciones	(Y. Liu *et al.*, 2014)
	Otros mecanismos de seguridad cuántica	Explorar y adoptar nuevas tecnologías y mecanismos de ciberseguridad cuántica que proporcionen protección adicional	Desarrollar un programa de investigación para evaluar la viabilidad y la implementación de nuevas tecnologías cuánticas como QKD	(Cerf *et al.*, 2002)

Adaptabilidad al advenimiento de la era cuántica

A continuación, la Tabla 6 describe adaptabilidad del modelo propuesto ante el advenimiento de la era cuántica. Para cada IC, se evalúan los diferentes aspectos a tener en cuenta y su adaptación según el tipo de servicio que ofrecen.

Tabla 6. Adaptabilidad al advenimiento cuántico

Procesos	Caracterización	Procedimientos	Actividades	Referencias
Análisis de cómo se adapta el modelo de referencia a los desafíos y riesgos asociados al advenimiento de la tecnología cuántica	Actualización de políticas y procedimientos	Revisar y actualizar continuamente las políticas y procedimientos de ciberseguridad para reflejar las amenazas y tecnologías cuánticas emergentes	Modificar las políticas de cifrado para incluir algoritmos poscuánticos y asegurar la protección contínua de los datos	(NIST, 2016)
	Implementación de medidas de ciberseguridad cuántica	Integrar tecnologías cuánticas en la infraestructura de ciberseguridad existente para proteger contra amenazas cuánticas	Incorporar sistemas de comunicación cuántica (QKD) para redes críticas	(Scarani *et al.*, 2009)
	Evaluación y gestión de riesgos cuánticos	Realizar evaluaciones de riesgos específicos a las amenazas cuánticas y desarrollar estrategias de mitigación	Evaluar la vulnerabilidad de los sistemas actuales contra ataques cuánticos y desarrollar planes de contingencia	(Gisin *et al.*, 2002)
	Capacitación y concientización	Capacitar al personal sobre las ciber-amenazas y tecnologías cuánticas para asegurar que estén preparados para enfrentar estos desafíos	Organizar talleres y seminarios sobre criptografía cuántica y sus aplicaciones prácticas en la ciberseguridad	(Ponemon Institute, 2020)
	Colaboración con expertos en tecnología cuántica	Colaborar con instituciones académicas y expertos en tecnología cuántica para asegurar la implementación de las mejores prácticas	Establecer alianzas con universidades e institutos de investigación especializados en criptografía cuántica	(Zhao & White, 2014)
Consideraciones de la resistencia del modelo ante ciberataques cuánticos	Evaluación de resistencia	Realizar pruebas de resistencia y simulaciones contra ciberataques cuánticos para evaluar la efectividad del modelo de ciberseguridad	Simular ciberataques cuánticos en un entorno de prueba controlado para identificar y corregir posibles vulnerabilidades	(Bernstein *et al.*, 2017)
	Aprovechamiento de ventajas cuánticas	Investigar y aplicar las ventajas que ofrece la tecnología cuántica para mejorar la ciberseguridad de la IC	Implementar algoritmos de optimización cuántica para mejorar la eficiencia y seguridad de las redes críticas	(Lloyd *et al.*, 2010)
	Compatibilidad con sistemas y algoritmos cuánticos	Asegurar la compatibilidad del modelo de ciberseguridad con tecnologías y algoritmos cuánticos emergentes	Evaluar y adaptar la infraestructura de TI para soportar la implementación de criptografía cuántica y otros mecanismos de ciberseguridad avanzados	(Campagna *et. al.*, 2015)

Evaluación y validación de mejora continua del modelo

A continuación, en la Tabla 7 se presentan algunos elementos a considerar en la implementación del modelo, entre ellos los criterios de evaluación y las métricas para medir la efectividad y la aplicabilidad del modelo de referencia, y las pruebas y validaciones del modelo en entornos de simulación o implementaciones piloto para obtener resultados concretos sobre su rendimiento.

Tabla 7. Evaluación y validación de mejora continua del modelo

Procesos	Caracterización	Procedimientos	Actividades	Referencias
Establecimiento de criterios de evaluación y métricas para medir la efectividad y la aplicabilidad del modelo de referencia	Efectividad en la protección contra ciberataques	Definir métricas claras para evaluar la efectividad del modelo en la protección que brinda el modelo contra ciberataques y cuánticos	Medir la reducción en la cantidad de incidentes de ciberseguridad y el tiempo de respuesta a los mismos	(NIST, 2008a)
	Adaptabilidad a la tecnología cuántica	Evaluar la capacidad del modelo para adaptarse y responder eficazmente a las tecnologías cuánticas emergentes	Realizar auditorías periódicas de adaptación cuántica para asegurar que las medidas de ciberseguridad sean adecuadas	(NIST), 2016)
	Aplicabilidad a las infraestructuras críticas	Evaluar la aplicabilidad del modelo en diferentes tipos de infraestructuras críticas y su efectividad en cada caso	Implementar pilotos en distintas infraestructuras y comparar resultados para ajustar el modelo según sea necesario	(CISA, 2021)
	Cumplimiento de estándares y regulaciones	Asegurar el cumplimiento con las normativas y estándares de ciberseguridad aplicables a la industria	Verificar el cumplimiento con el estándar ISO 27001 y otras regulaciones específicas de la industria	(ISO/IEC 27001, 2013)
	Usabilidad y aceptación por parte de los usuarios	Medir la aceptación y facilidad de uso del modelo de ciberseguridad por parte de los usuarios finales	Realizar encuestas de satisfacción entre los usuarios del sistema para obtener retroalimentación y ajustar el modelo según sea necesario	(Ponemon Institute, 2020)
Realización de pruebas y validaciones del modelo en entornos de simulación o implementaciones piloto para obtener resultados concretos sobre su rendimiento	Diseño de escenarios de prueba	Crear escenarios de prueba realistas y desafiantes que reflejen posibles ciber-amenazas y ciberataques	Diseñar escenarios que simulen ciberataques cuánticos en entornos controlados para evaluar la efectividad del modelo	(NIST, 2008b)
	Selección de métricas de rendimiento	Definir métricas claras y específicas para evaluar el rendimiento del modelo en diferentes escenarios	Medir el tiempo de respuesta a incidentes, la efectividad de las medidas de mitigación y la reducción de vulnerabilidades	(NIST, 2008a)
	Implementación de pruebas en entornos de simulación o pilotos	Realizar pruebas en entornos simulados o pilotos para obtener resultados concretos sobre el rendimiento del modelo	Desplegar el modelo en una infraestructura piloto y evaluar su desempeño en condiciones controladas	(Microsoft, 2018)
	Recopilación de datos y análisis	Recopilar y analizar los datos obtenidos durante las pruebas para identificar patrones y áreas de mejora	Analizar los *logs* de seguridad y eventos de red para identificar tendencias y ajustar el modelo en consecuencia	(ISO, 2018)
	Iteración y refinamiento del modelo	Refinar y ajustar el modelo con base en los resultados de las pruebas y la retroalimentación obtenida	Ajustar políticas y procedimientos según los resultados de las pruebas y las recomendaciones de los expertos	(Tummala & Schoenherr, 2011)
	Validación externa	Obtener validaciones y certificaciones externas para asegurar que el modelo cumpla con los estándares de la industria	Someter el modelo a auditorías de terceros y obtener certificaciones como ISO 27001 para validar su efectividad y cumplimiento	(European Union, 2018)

Para validar MoRCiTO en una IC del sector eléctrico, por ejemplo, el modelo se puede adaptar de la siguiente forma:

I. Evaluación y gestión de riesgos específicos. Se debe realizar un análisis exhaustivo de los riesgos y requerimientos específicos de la IC, como lo serían los sistemas de generación y distribución de energía. Esto implica identificar las amenazas cuánticas y cómo podrían afectar a los SCF involucrados en la operación de la red eléctrica.

II. Pruebas en entornos de simulación o implementaciones piloto. MoRCiTO debe ser validado en entornos controlados mediante simulaciones de ciberataques cuánticos y otros tipos de amenazas avanzadas. Esto permitirá medir su efectividad en condiciones similares a las del mundo real antes de su implementación completa.

III. **Capacitación del personal.** Es crucial que el personal encargado de la gestión de la infraestructura eléctrica reciba capacitación en los aspectos técnicos del modelo, incluyendo las nuevas políticas y procedimientos de seguridad, con un enfoque en los desafíos que trae la computación cuántica.
IV. **Monitorización y mantenimiento continuos.** El modelo debe estar en constante evolución, por lo que es necesario implementar herramientas de monitorización en tiempo real para evaluar su eficacia de manera continua. Las evaluaciones periódicas permiten hacer ajustes para asegurar la protección frente a las amenazas emergentes.
V. **Colaboración con expertos y adaptación a nuevas tecnologías.** Involucrar a expertos en ciberseguridad cuántica y criptografía post-cuántica es esencial para garantizar la efectividad del modelo. Además, MoRCiTO debe ser adaptable para integrar nuevas tecnologías a medida que evolucionen las amenazas.

Adaptación e implementación

A continuación, en la Tabla 8 se presentan consideraciones relacionadas con los mecanismos para adaptar el modelo de referencia a las características específicas de las IC y los SCF involucrados. Asimismo, se identifican los pasos y consideraciones necesarios para la implementación del modelo de referencia en un entorno real, incluyendo la planificación, la capacitación del personal y la integración con otros sistemas existentes.

Tabla 8. Adaptación e implementación del modelo

Procesos	Caracterización	Procedimientos	Actividades	Referencias
Consideraciones de los mecanismos de adaptación	Análisis de riesgos y requerimientos	Realizar un análisis exhaustivo de riesgos y requerimientos específicos de la IC	Evaluar los riesgos específicos de una planta de energía y adaptar el modelo a esos riesgos específicos	(Stoneburner *et al.*, 2002)
	Personalización de políticas y controles	Ajustar las políticas y controles de seguridad a las necesidades específicas de la IC	Personalizar las políticas de acceso y autenticación según las funciones específicas de cada usuario en la organización	(Sandhu *et al.*, 1996)
	Integración con sistemas existentes	Asegurar la integración sin problemas del modelo con los sistemas de seguridad y TI existentes	Implementar API y herramientas de interoperabilidad que permitan la integración con sistemas de gestión de seguridad existentes	(NIST, 2015)
	Adaptabilidad a cambios tecnológicos	Preparar el modelo para adaptarse a futuros cambios tecnológicos y asegurar su relevancia continua	Crear un comité de revisión tecnológica que evalúe y adopte nuevas tecnologías de ciberseguridad de manera regular	(Baracaldo & Joshi, 2009)
	Capacitación y concientización	Capacitar al personal sobre las nuevas políticas y procedimientos de seguridad para asegurar una implementación exitosa	Realizar sesiones de capacitación y simulacros de respuesta a incidentes para preparar al personal	(Ponemon Institute, 2020)
	Evaluación y retroalimentación continua	Implementar un ciclo de retroalimentación continua para ajustar y mejorar el modelo de ciberseguridad	Realizar encuestas de retroalimentación periódicas entre los usuarios y ajustar el modelo según los comentarios recibidos	(Whitman & Mattord, 2018)

Identificación de los pasos y consideraciones necesarias para la implementación del modelo de referencia en un entorno real	Planificación de la implementación	Desarrollar un plan detallado de implementación que incluya todas las etapas y responsabilidades	Crear un cronograma con etapas claras y asignar responsabilidades específicas a cada equipo	(Project Management Institute, 2017)
	Evaluación del entorno existente	Evaluar el entorno de TI y las infraestructuras actuales para identificar posibles desafíos y requerimientos	Realizar una auditoría completa de los sistemas actuales y su estado de seguridad	(NIST SP 800-30, 2012)
	Adaptación del modelo	Ajustar el modelo de ciberseguridad basado en la evaluación del entorno y los riesgos específicos	Modificar las políticas de ciberseguridad para alinear con las prácticas actuales de la organización y los riesgos identificados	
	Integración con otros sistemas	Integrar el modelo de ciberseguridad con los sistemas de gestión y seguridad existentes para asegurar una protección integral	Utilizar herramientas de gestión de identidad (*identity and access management*, IAM) para sincronizar con los sistemas de control de acceso	(Microsoft, 2021)
	Capacitación del personal	Capacitar al personal sobre el nuevo modelo de ciberseguridad y sus componentes para asegurar una implementación exitosa	Organizar talleres de formación y distribuir manuales de usuario que expliquen los nuevos procedimientos y tecnologías	(Ponemon Institute, 2020)
	Implementación gradual	Desplegar el modelo de ciberseguridad de manera gradual para asegurar una transición suave y manejable	Implementar el modelo en una sola planta de energía y, después de evaluar su efectividad, expandirlo a otras infraestructuras	(Microsoft, 2018)
	Monitoreo y mantenimiento	Establecer un sistema continuo de monitoreo y mantenimiento para asegurar la efectividad continua del modelo	Configurar herramientas de monitoreo en tiempo real y planificar mantenimientos periódicos para revisar y actualizar el sistema	(ISO/IEC 27001, 2013)

Mapa de dominios de ciberseguridad cuántica para SCF en IC

Tomando como referencia el mapa de dominios de ciberseguridad propuesto por Jiang (Figura 3), la Figura 4 presenta una actualización que sigue el mapa de dominios de ciberseguridad pero se centra en el advenimiento de la tecnología cuántica y los SCF que se utilizan en las IC.

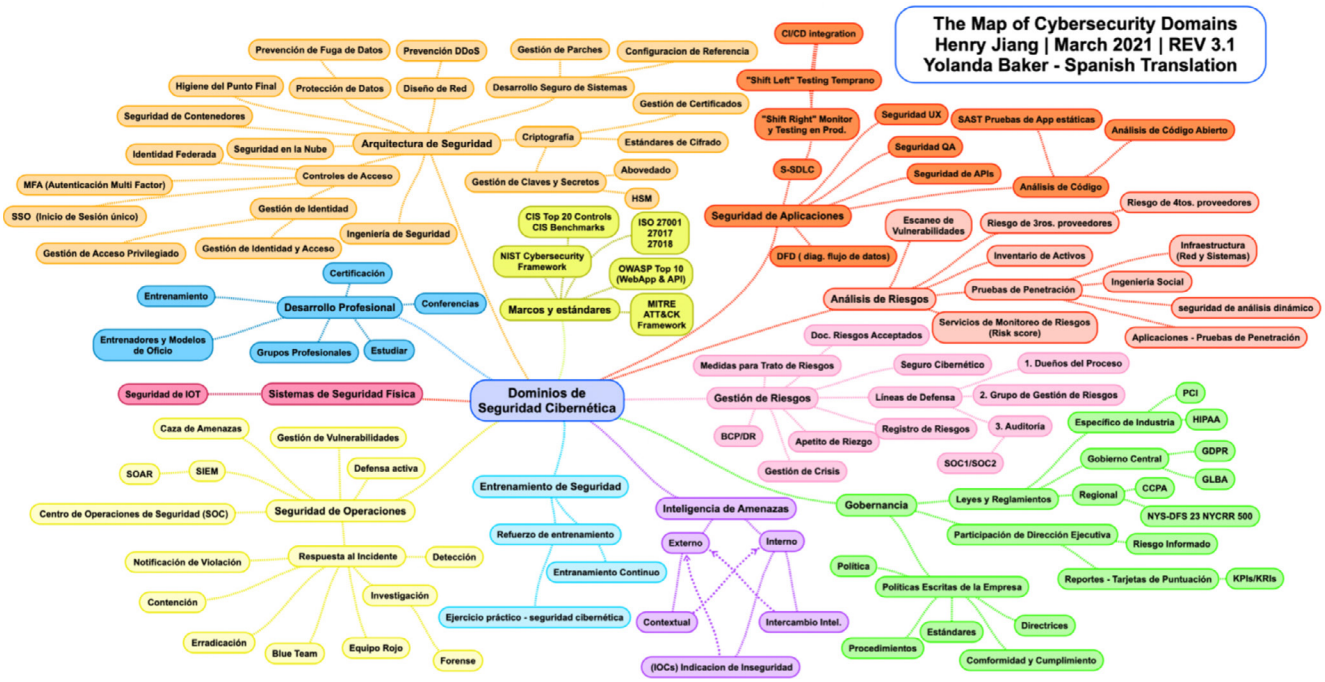


Figura 3. Mapa de dominios de ciberseguridad.
Fuente: Elaborado por Jiang en 2021- https://app.box.com/s/sj5xaz8a1461e7u7si3ip1361r070fed/file/822847297651

Figura 4. Mapa de dominios de ciberseguridad cuántica para SCF en IC

CONCLUSIONES

Este estudio presenta la versión preliminar de MoRCiTO, un modelo diseñado para prevenir ataques de red a SCF en IC ante la inminente llegada de la era cuántica. A través de un proceso metodológico basado en la caracterización de los aspectos y elementos que lo conforman –producto de una revisión sistemática de la literatura–, se logró determinar y caracterizar los elementos claves del modelo, incluyendo la identificación de amenazas cuánticas, el desarrollo de algoritmos resistentes a los ataques cuánticos y la implementación de técnicas avanzadas de QKD.

El modelo propone un marco sólido que permitirá a las IC prepararse y adaptarse a las nuevas amenazas que surgirán con la computación cuántica. Nuestra propuesta no solo provee soluciones de seguridad avanzadas, sino que también promueve la integración de tecnologías emergentes como la criptografía cuántica, lo que podría convertirse en un estándar de de la ciberseguridad en el futuro.

Una de las principales fortalezas de este estudio es la adopción de una metodología integral que combina revisiones sistemáticas con la aplicación práctica de un modelo en un entorno controlado. Sin embargo, es necesario destacar que esta investigación se encuentra en una etapa preliminar, por lo que el trabajo futuro requiere la implementación real del modelo y su validación a través de diferentes enfoques, entre ellos la evaluación de expertos y estudios de caso adicionales en diversos contextos de IC. Esto podría arrojar nuevos desafíos y oportunidades de mejora en relación con la integración de nuevas técnicas de detección y respuesta a ataques cuánticos. Además, es crucial explorar la estandarización de esta solución y su aplicación en entornos operativos reales para garantizar su efectividad a largo plazo.

La ciberseguridad en la era cuántica no es una opción, sino una necesidad urgente. MorCiTO ofrece un marco práctico y robusto para mitigar riesgos y garantizar la seguridad en IC, estableciendo incluso un modelo de referencia que podría ser la base para el establecimiento de un estándar de ciberseguridad operativa.

AGRADECIMIENTOS

Los profesores Siler Amador Donado y César Jesús Pardo Calvache agradecen el aporte del grupo de investigación GTI de la Universidad del Cauca, donde se desempeñan como profesores titulares. De igual manera, agradecen al profesor Raúl Mazo Peña y a su grupo de investigación Lab-STICC, vinculado a la Universidad ENSTA Bretagne.

CONTRIBUCIÓN DE AUTORÍA

Siler Amador Donado: conceptualización, curado de datos, análisis formal, investigación, *software*, visualización y redacción (borrador original)
César Jesús Pardo Calvache: conceptualización, administración del proyecto, metodología, supervisión y redacción (revisión y edición)
Raúl Mazo Peña: conceptualización, administración y redacción (revisión y edición) del proyecto

REFERENCIAS

Abdi, F., Chen, C.-Y., Hasan, M., Liu, S., Mohan, S., Caccamo, M. (2018). *Guaranteed physical security with restart-based design for cyber-physical systems* [Artículo de conferencia]. ACM/IEEE 9th International Conference on Cyber-Physical Systems (ICCPS). https://doi.org/10.1109/ICCPS.2018.00010

Adam, A., Rivlin, E., Shimshoni, I., Reinitz, D. (2008). Robust real-time unusual event detection using multiple fixed-location monitors. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *30*(3), 555-560. https://doi.org/10.1109/TPAMI.2007.70825

Aguado, A., López, V., Martinez-Mateo, J., Peev, M., López, D., Martin, V. (2018). Virtual network function deployment and service automation to provide end-to-end quantum encryption. *Journal of Optical Communications and Networking*, *10*(4), e421. https://doi.org/10.1364/JOCN.10.000421

Ahn, J., Chung, J., Kim, T., Ahn, B., Choi, J. (2021). *An overview of quantum security for distributed energy resources* [Artículo de conferencia]. IEEE 12th International Symposium on Power Electronics for Distributed Generation Systems (PEDG). https://doi.org/10.1109/PEDG51384.2021.9494203

Akter, M. S. (2023). *Quantum cryptography for enhanced network security: A comprehensive survey of research, developments, and future directions*. https://doi.org/10.48550/arXiv.2306.09248

Alagic, G., Alperin-Sheriff, J., Apon, D., Cooper, D., Dang, Q., Liu, Y.-K., Miller, C., Moody, D., Peralta, R., Perlner, R., Robinson, A., Smith-Tone, D. (2019). *Status report on the first round of the NIST post-quantum cryptography standardization process*. https://doi.org/10.6028/NIST.IR.8240

Albataineh, H., Nijim, M. (2021). Enhancing the cybersecurity education curricula through quantum computation. En K. Daimi, H. R. Arabnia, L. Deligiannidis, M. S. Hwang & F. G. Tinetti (Eds.), *Advances in Security, Networks, and Internet of Things* (pp. 223-231). Springer International Publishing. https://doi.org/10.1007/978-3-030-71017-0_16

Alcaraz, C. (2018). Cloud-assisted dynamic resilience for cyber-physical control systems. *IEEE Wireless Communications*, *25*(1), 76-82. https://doi.org/10.1109/MWC.2018.1700231

Alcaraz, C., Zeadally, S. (2015). Critical infrastructure protection: Requirements and challenges for the 21st century. *International Journal of Critical Infrastructure Protection*, *8*, 53-66. https://doi.org/10.1016/j.ijcip.2014.12.002

Ali, A. (2021). *A pragmatic analysis of pre- and post-quantum cyber security scenarios* [Artículo de conferencia]. International Bhurban Conference on Applied Sciences and Technologies (IBCAST). Https://doi.org/10.1109/IBCAST51254.2021.9393278

Al-Mohammed, H. A., Al-Ali, A., Yaacoub, E., Qidwai, U., Abualsaud, K., Rzewuski, S., Flizikowski, A. (2021). Machine learning techniques for detecting attackers during quantum key distribution in IoT networks with application to railway scenarios. *IEEE Access*, *9*, 136994-137004. https://doi.org/10.1109/ACCESS.2021.3117405

Amador Donado, S., Pardo Calvache, C. J., Mazo Peña, R. (2024). Revisión preliminar: ciberseguridad para tecnología de la operación en la era cuántica contra ataques de red a infraestructuras críticas. *Revista INGE CUC*, *20*(2), por publicar.

Antoliš, K., Mišević, P., Miličević, A. (2015). *Vulnerabilities of new technologies and the protection of CNI*. https://hrcak.srce.hr/file/206704

Axelrod, C. W. (2013). *Managing the risks of cyber-physical systems* [Artículo de conferencia]. IEEE Long Island Systems, Applications and Technology Conference (LISAT). https://doi.org/10.1109/LISAT.2013.6578215

Baracaldo, N., Joshi, J. B. D. (2009). Mitigating insider threats to database security: A role-based approach. *ACM Transactions on Information and System Security (TISSEC)*, *12*(4), 1-29.

Baykara, M., Gurturk, U., Das, R. (2018). *An overview of monitoring tools for real-time cyber-attacks* [Artículo de conferencia]. 6th International Symposium on Digital Forensic and Security (ISDFS). Https://doi.org/10.1109/ISDFS.2018.8355339

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

Bililign, S. (2013). The need for interdisciplinary research and education for sustainable human development to deal with global challenges. *International Journal of African Development, 1*(1), e18. https://scholarworks.wmich.edu/ijad/vol1/iss1/8

Bruß, D., Lütkenhaus, N. (2000). Quantum key distribution: From principles to practicalities. *Applicable Algebra in Engineering, Communication and Computing*, *10*(4-5), 383-399. https://doi.org/10.1007/s002000050137

Busby, D. J. (2000). *Peacetime use of computer network attack*. https://doi.org/https://doi.org/10.21236/ada377624

Caicedo, D. S. (2017). *Global critical infrastructure: Attacking the vulnerability of global cyber networks to create societal collapse*. https://api.semanticscholar.org/CorpusID:55418315

Campagna, M., Chen, L., Dagdelen, O., Ding, J., Fernick, J., Gisin, N., Zhang, Z. (2015). *Quantum Safe Cryptography and Security: An introduction, benefits, enablers and challenges*. European Telecommunications Standards Institute.

Campbell Sr., R. E. (2020). The need for cyber resilient enterprise distributed ledger risk management framework. *The Journal of The British Blockchain Association*, *3*(1), 1-9. https://doi.org/10.31585/jbba-3-1-(5)2020

Cao, Y., Zhao, Y., Colman-Meixner, C., Yu, X., Zhang, J. (2017). Key on demand (KoD) for software-defined optical networks secured by quantum key distribution (QKD). *Optics Express*, *25*(22), e26453. https://doi.org/10.1364/OE.25.026453

Carle, G., Debar, H., Dressler, F., König, H. (2012). Network attack detection and defense early warning systems - Challenges and perspectives (Dagstuhl Seminar 12061). *Dagstuhl Reports*, *2*(2), 1-20. https://doi.org/10.4230/DagRep.2.2.1

Cerf, N. J., Bourennane, M., Karlsson, A., Gisin, N. (2002). Security of quantum key distribution using d-level systems. *Physical Review Letters*, *88*(12), e127902. https://doi.org/10.1103/PhysRevLett.88.127902

Choi, J.-W., Kang, M.-S., Heo, J., Hong, C., Yoon, C.-S., Han, S.-W., Moon, S., Yang, H.-J. (2020). Quantum challenge-response identification using single qubit unitary operators. *Physica Scripta*, *95*(10), e105104. https://doi.org/10.1088/1402-4896/abaf8e

CISA (2021). *Critical Infrastructure Sectors*. https://www.cisa.gov/sites/default/files/publications/21-0860_EOY_REPORT_508c.pdf

Clark-Ginsberg, A., Slayton, R. (2019). Regulating risks within complex sociotechnical systems: Evidence from critical infrastructure cybersecurity standards. *Science and Public Policy*, *46*(3), 339-346. https://doi.org/10.1093/scipol/scy061

Cook, A., Nicholson, A., Janicke, H., Maglaras, L., Smith, R. (2016). Attribution of cyber-attacks on industrial control systems. *EAI Endorsed Transactions on Industrial Networks and Intelligent Systems*, *3*(7), e151158. https://doi.org/10.4108/eai.21-4-2016.151158

Cruz, T., Simões, P. (2021). Down the rabbit hole: Fostering active learning through guided exploration of a SCADA cyber range. *Applied Sciences*, *11*(20), e23. https://doi.org/10.3390/app11209509

Dacier, M., Kargl, F., König, H., Valdes, A. (2014). Network attack detection and defense: Securing industrial control systems for critical infrastructures (Dagstuhl Seminar 14292). *Dagstuhl Reports*, *4*(7), 62-79. https://doi.org/10.4230/DagRep.4.7.62

Diffie, W., Hellman, M. E. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, *22*(6), 644-654.

Dixon, A. R., Dynes, J. F., Lucamarini, M., Fröhlich, B., Sharpe, A. W., Plews, A., Tam, W., Yuan, Z. L., Tanizawa, Y., Sato, H., Kawamura, S., Fujiwara, M., Sasaki, M., Shields, A. J. (2017). Quantum key distribution with hacking countermeasures and long-term field trial. *Scientific Reports*, *7*(1), e1978. https://doi.org/10.1038/s41598-017-01884-0

Dutta, H., Bhuyan, A. K. (2024). *Quantum communication: From fundamentals to recent trends, challenges and open problems*. http://arxiv.org/abs/2406.04492

European Commission (2017). *Critical infrastructures – Enhancing preparedness & resilience for the security of citizens and services supply continuity* [Artículo de conferencia]. Proceedings of the 52nd ESReDA Seminar Hosted by the Lithuanian Energy Institute & Vytautas Magnus University.

European Union (2018). *General Data Protection Regulation (GDPR)*. https://gdpr-info.eu/

European Union Agency for Network, ENISA (2018). *Good practices for security of internet of things in the context of smart manufacturing*. https://www.enisa.europa.eu/publications/good-practices-for-security-of-iot/@@download/fullReport

Fehr, S., Salvail, L. (2017). *Quantum authentication and encryption with key recycling* [Artículo de conferencia]. Advances in Cryptology – EUROCRYPT 2017. https://doi.org/10.1007/978-3-319-56617-7_11

Fernández-Carames, T. M., Fraga-Lamas, P. (2020). Towards post-quantum blockchain: A review on blockchain cryptography resistant to quantum computing attacks. *IEEE Access*, *8*, 21091-21116. https://doi.org/10.1109/ACCESS.2020.2968985

Flowers, A., Zeadally, S., Murray, A. (2013). Cybersecurity and US legislative efforts to address cybercrime. *Journal of Homeland Security and Emergency Management*, *10*(1), 29-55. https://doi.org/10.1515/jhsem-2012-0007

Fu, H. (2015). *Legal protection of cyberspace infrastructure and information safety in china-a response to cyberspace challenges to china's national security*. https://doi.org/10.2991/meita-15.2015.6

Gatto, A., Ferrari, M., Brunero, M., Gagliano, A., Tarable, A., Bodanapu, D., Giorgetti, A., Andriolli, N., Paganelli, R., Strambini, L., Martelli, P., Martinelli, M. (2022). *Integration of QKD technologies in advanced optical networks* [Artículo de conferencia]. IEEE 15th Workshop on Low Temperature Electronics (WOLTE). Https://doi.org/10.1109/WOLTE55422.2022.9882652

Gisin, N., Ribordy, G., Tittel, W., Zbinden, H. (2002). Quantum cryptography. *Reviews of Modern Physics*, *74*(1), 145-195.

Goorden, S. A., Horstmann, M., Mosk, A. P., Škorić, B., Pinkse, P. W. H. (2014). Quantum-secure authentication of a physical unclonable key. *Optica*, *1*(6), e421. https://doi.org/10.1364/OPTICA.1.000421

Goy, M., Berlich, R., Kržič, A., Rieländer, D., Kopf, T., Sharma, S., Steinlechner, F. O. (2021). High performance optical free-space links for quantum communications. En Z. Sodnik, B. Cugny & N. Karafolas (Eds.), *International Conference on Space Optics — ICSO 2020* (p. 18). SPIE. https://doi.org/10.1117/12.2599163

Gras, G., Rusca, D., Zbinden, H., Bussières, F. (2021). Countermeasure against quantum hacking using detection statistics. *Physical Review Applied*, *15*(3), e034052. https://doi.org/10.1103/PhysRevApplied.15.034052

Haber, E., Zarsky, T. Z. (2017). Cybersecurity for infrastructure: A critical analysis. *Information Privacy Law eJournal*. https://api.semanticscholar.org/CorpusID:158139470

Hahn, A. (2016). Operational technology and information technology in industrial control systems. En E. Colbert 7 A. Kott (Eds.), *Advances in Information Security* (vol. 66, pp. 51-68). Springer New York. https://doi.org/10.1007/978-3-319-32125-7_4

Hamza, A., Gharakheili, H. H., Sivaraman, V. (2020). *IoT network security: Requirements, threats, and countermeasures*. http://arxiv.org/abs/2008.09339

Haney, M. (2019). Leveraging cyber-physical system honeypots to enhance threat intelligence. En J. Staggs & S. Shenoi (Eds.), *IFIP Advances in Information and Communication Technology* (vol. 570 IFIP, pp. 209-233). Springer International Publishing. https://doi.org/10.1007/978-3-030-34647-8_11

Hartman, S. M. (2012). *Protecting accelerator control systems in the face of sophisticated cyber-attacks*. https://api.semanticscholar.org/CorpusID:55389350

Holdsworth, J., Apeh, E. (2017). *An effective immersive cyber security awareness learning platform for businesses in the hospitality sector* [Artículo de conferencia]. IEEE 25th International Requirements Engineering Conference Workshops (REW). https://doi.org/10.1109/REW.2017.47

Holley, K. A. (2009). Special issue: Understanding interdisciplinary challenges and opportunities in higher education. *Ashe Higher Education Report*, *35*, 1-131. https://api.semanticscholar.org/CorpusID:146511487

Hoschek, M. (2021). Quantum security and 6G critical infrastructure. *Serbian Journal of Engineering Management*, *6*(1), 1-8. https://doi.org/10.5937/SJEM2101001H

Hossain Faruk, M. J., Tahora, S., Tasnim, M., Shahriar, H., Sakib, N. (2022). *A review of quantum cybersecurity: Threats, risks and opportunities* [Artículo de conferencia]. 1st International Conference on AI in Cybersecurity (ICAIC). Https://doi.org/10.1109/ICAIC53980.2022.9896970

Huang, K., Zhou, C., Tian, Y. C., Yang, S., Qin, Y. (2018). Assessing the physical impact of cyberattacks on industrial cyber-physical systems. *IEEE Transactions on Industrial Electronics*, *65*(10), 8153-8162. https://doi.org/10.1109/TIE.2018.2798605

Hughes, R. J., Nordholt, J. E., McCabe, K. P., Newell, R. T., Peterson, C. G., Somma, R. D. (2013). Network-centric quantum communications. *Frontiers in Optics*, *2013*, FW2C.1. https://doi.org/10.1364/FIO.2013.FW2C.1

Hui, P., Bruce, J., Fink, G., Gregory, M., Best, D., McGrath, L., Endert, A. (2010). *Towards efficient collaboration in cyber security* [Artículo de conferencia]. International Symposium on Collaborative Technologies and Systems. https://doi.org/10.1109/CTS.2010.5478473

International Organization for Standardization (ISO) (2018). *Risk management – Guidelines (número ISO 31000:2018)*. International Organization for Standardization.

ISO/IEC 27001 (2013). *Information technology – Security techniques – Information security management systems – Requirements (número ISO/IEC 27001:2013)*. International Organization for Standardization.

Jahanian, F. (2011). *Reflections on the evolution of internet threats* [Artículo de conferencia]. 18th ACM Conference on Computer and communications security. https://doi.org/10.1145/2046707.2046709

Jain, N., Stiller, B., Khan, I., Elser, D., Marquardt, C., Leuchs, G. (2016). Attacks on practical quantum key distribution systems (and how to prevent them). *Contemporary Physics*, *57*(3), 366-387. https://doi.org/10.1080/00107514.2016.1148333

Kalra, M., Poonia, R. C. (2017). Design a new protocol for quantum key distribution. *Journal of Information and Optimization Sciences*, *38*(6), 1047-1054. https://doi.org/10.1080/02522667.2017.1374723

Kanamori, Y., Seong-Moo Yoo, Gregory, D. A., Sheldon, F. T. (2005). *On quantum authentication protocols* [Artículo de conferencia]. GLOBECOM '05. IEEE Global Telecommunications Conference. https://doi.org/10.1109/GLOCOM.2005.1577930

Kanamori, Y., Yoo, S.-M., Gregory, D. A., Sheldon, F. T. (2009). Authentication protocol using quantum superposition states. *International Journal of Network Security*, *9*(2), 101-108.

Käppler, S. A., Schneider, B. (2021). Post-quantum cryptography: An introductory overview and implementation challenges of quantum-resistant algorithms. En K. Hinkelmann & A. Gerber (Eds.), *Proceedings of the Society 5.0 Conference 2022 - Integrating Digital World and Real World to Resolve Challenges in Business and Society* (pp. 61-49). EasyChair. https://doi.org/10.29007/2tpw

Karim, M. E., Phoha, V. V. (2014). Cyber-physical systems security. En S. Suh, U. Tanik, J. Carbone, & A. Eroglu (Eds.), *Applied Cyber-Physical Systems* (pp. 75-83). Springer New York. https://doi.org/10.1007/978-1-4614-7336-7_7

Karol, M., Życzkowski, M. (2015). Quantum technology in critical infrastructure protection. *Safety and Security Engineering VI*, *1*, 109-119. https://doi.org/10.2495/SAFE150101

Khan, A. A., Ahmad, A., Waseem, M., Liang, P., Fahmideh, M., Mikkonen, T., Abrahamsson, P. (2022). Software architecture for quantum computing systems - Asystematic review. *SSRN Electronic Journal*, por publicar. https://doi.org/10.2139/ssrn.4040490

Khan, I. (2018). Quantum communication in space – Challenges and opportunities. *Imaging and Applied Optics, 2018*, AM5A.2. https://doi.org/10.1364/AIO.2018.AM5A.2

Knapp, E. D., Langill, J. T. (2015). Standards and regulations. En E. D. Knapp & J. T. Langill (Eds.), *Industrial Network Security* (pp. 387-407). Elsevier. https://doi.org/10.1016/B978-0-12-420114-9.00013-7

Kneller, V. Yu., Fayans, A. M. (2019). Solving interdisciplinary tasks: The challenge and the ways to surmount it. *Journal of Physics: Conference Series*, *1379*(1), e012011. https://doi.org/10.1088/1742-6596/1379/1/012011

Kumar, A., Dadheech, P., Singh, V., Raja, L., Poonia, R. C. (2019). An enhanced quantum key distribution protocol for security authentication. *Journal of Discrete Mathematical Sciences and Cryptography*, *22*(4), 499-507. https://doi.org/10.1080/09720529.2019.1637154

Kumar Rao, S., Mahto, D., Kumar Yadav, D., Ali Khan, D. (2017). The AES-256 cryptosystem resists quantum attacks. *International Journal of Advanced Research in Computer Science*, *8*(3), 404-408. https://doi.org/https://doi.org/10.26483/ijarcs.v8i3.3025

Lancho, D., Martinez, J., Elkouss, D., Soto, M., Martin, V. (2010). QKD in standard optical telecommunications networks. En A. Sergienko, S. Pascazio, & P. Villoresi (Eds.), *Quantum Communication and Quantum Networking* (pp. 142-149). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-11731-2_18

Laughlin, C. (2016). Cybersecurity in critical infrastructure sectors: a proactive approach to ensure inevitable laws and regulations are effective. *Colorado Technology Law Journal, 14*(2), 2871452. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2871452

Linke, N. M., Maslov, D., Roetteler, M., Debnath, S., Figgatt, C., Landsman, K. A., Wright, K., Monroe, C. (2017). Experimental comparison of two quantum computing architectures. *Proceedings of the National Academy of Sciences*, *114*(13), 3305-3310. https://doi.org/10.1073/pnas.1618020114

Liu, W., Peng, J., Huang, P., Huang, D., Zeng, G. (2017). Monitoring of continuous-variable quantum key distribution system in real environment. *Optics Express*, *25*(16), 19429. https://doi.org/10.1364/OE.25.019429

Liu, Y., Cao, Z., Curty, M., Liao, S.-K., Wang, J., Cui, K., Yin, J., Li, Y., Chen, K., , Peng, C.-Z. (2014). Experimental demonstration of quantum authentication. *Physical Review Letters*, *113*(4), e40505.

Lloyd, S., Mohseni, M., Rebentrost, P. (2010). Quantum algorithms for solving linear systems of equations. *Physical Review Letters*, *105*(15), e150502.

Lu, K.-C., Liu, I.-H., Liao, J.-W., Wu, S.-C., Liu, Z.-C., Li, J.-S., Li, C.-F. (2019). Evaluation and build to honeypot system about scada security for large-scale IoT devices. *Journal of Robotics, Networking and Artificial Life*, *6*(3), e157. https://doi.org/10.2991/jrnal.k.191202.008

Ludvigsen, K. R., Nagaraja, S. (2022). *The opportunity to regulate cybersecurity in the EU (and the World): Recommendations for the cybersecurity resilience act*. http://arxiv.org/abs/2205.13196

Luo, Y., Li, Q., Mao, H.-K. (2023). *How to achieve end-to-end key distribution for QKD Networks in the presence of untrusted nodes*. https://doi.org/https://doi.org/10.48550/arXiv.2302.07688

Majumder, S. R., Giani, A., Shen, W., Neculaes, B., Zhu, D., Johri, S. (2023). *Quantum computation: Efficient network partitioning for large scale critical infrastructures*. http://arxiv.org/abs/2302.02074

Malina, L., Dobias, P., Hajny, J., Choo, K.-K. R. (2023). *On deploying quantum-resistant cybersecurity in intelligent infrastructures* [Artículo de conferencia]. 18th International Conference on Availability, Reliability and Security. Https://doi.org/10.1145/3600160.3605038

Mao, S., Zhang, H., Wu, W., Liu, J., Li, S., Wang, H. (2014). A resistant quantum key exchange protocol and its corresponding encryption scheme. *China Communications*, *11*(9), 124-134. https://doi.org/10.1109/CC.2014.6969777

Mao, Y., Huang, W., Zhong, H., Wang, Y., Qin, H., Guo, Y., Huang, D. (2020). Detecting quantum attacks: A machine learning based defense strategy for practical continuous-variable quantum key distribution. *New Journal of Physics*, *22*(8), 083073. Https://doi.org/10.1088/1367-2630/aba8d4

Martelli, P., Gatto, A., Brunero, M., Bodanapu, D., Rapisarda, M., Comi, P. M., Martinelli, M. (2021). *Integration of QKD in WDM networks* [Artículo de conferencia]. 2021 International Conference on Optical Network Design and Modeling (ONDM). https://doi.org/10.23919/ONDM51796.2021.9492394

McMurdo, J. (2014). Cybersecurity firms cyber mercenaries. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.2556412

Microsoft (2018). *Security development lifecycle (SDL)*. https://www.microsoft.com/en-us/securityengineering/sdl

Microsoft (2021). *Security update guide*. https://msrc.microsoft.com/update-guide

Mihalache, S. F., Pricop, E., Fattahi, J. (2019). Resilience enhancement of cyber-physical systems: A review. En N. Mahdavi Tabatabaei, S. Najafi Ravadanegh N. Bizon (Eds.), *Power Systems Resilience* (pp. 269-287). Springer. https://doi.org/10.1007/978-3-319-94442-5_11

Mink, A., Frankel, S., Perlner, R. (2010). *Quantum key distribution (QKD) and commodity security protocols: Introduction and integration*. http://arxiv.org/abs/1004.0605

Mistry, N. R., Dholakiya, A. Y., Prajapati, J. P., Mistry, N. R., Dholakiya, A. Y., Prajapati, J. P. (2021). Security and privacy aspects using quantum internet. En N. Kumar, A. Agrawal, B. Chaurasia & R. Khan (Eds.), *Limitations and Future Applications of Quantum Cryptography* (pp. 62-81). IGI Global Scientific Publishing. https://doi.org/10.4018/978-1-7998-6677-0.ch004

Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? *IEEE Security & Privacy*, *16*(5), 38-41. https://doi.org/10.1109/MSP.2018.3761723

Nair, P., Patil, S. (2020). Quantum computing in data security: A critical assessment. *SSRN Electronic Journal, 2020,* e3565438. https://doi.org/10.2139/ssrn.3565438

National Institute of Standards (NIST) (2002). *Risk Management guide for information technology systems: Vol. SP 800-30*. https://doi.org/10.6028/NIST.SP.800-30

National Institute of Standards (NIST) (2008a). *Performance measurement guide for information security*. https://doi.org/10.6028/NIST.SP.800-55r1

National Institute of Standards (NIST) (2008b). *Technical guide to information security testing and assessment*. https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=152164

National Institute of Standards (NIST) (2012). *Computer security incident handling guide: Vol. Revision 2*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

National Institute of Standards (NIST) (2015). *Guide to industrial control systems (ICS) Security: Vol. Revision 2*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

National Institute of Standards (NIST) (2016). *Post-quantum cryptography: NIST's plan for the future*. https://nvlpubs.nist.gov/nistpubs/ir/2016/nist.ir.8105.pdf

National Institute of Standards (NIST) (2020). *Security and privacy controls for information systems and organizations*. https://doi.org/10.6028/NIST.SP.800-53r5

NIST SP 800-30 (2012). *Guide for conducting risk assessments*. https://doi.org/10.6028/NIST.SP.800-30r1

Nkongolo, M., Van Deventer, J. P., Kasongo, S. M., Van Der Walt, W., Kalonji, R., Pungwe, M. (2022). *Network policy enforcement: An intrusion prevention approach for critical infrastructures* [Artículo de conferencia]. 6th International Conference on Electronics, Communication and Aerospace Technology. https://doi.org/10.1109/ICECA55336.2022.10009524

Olofinbiyi, S. A. (2022). A reassessment of public awareness and legislative framework on cybersecurity in South Africa. *ScienceRise: Juridical Science*, *2(20)*, 34-42. https://doi.org/10.15587/2523-4153.2022.259764

Pătrașcu, P. (2021). Emerging technologies and national security: The impact of IoT in critical infrastructures protection and defence sector. *Land Forces Academy Review*, *26*(4), 423-429. https://doi.org/10.2478/raft-2021-0055

Paul, S., Scheible, P., Wiemer, F. (2022). Towards post-quantum security for cyber-physical systems: Integrating PQC into industrial M2M communication. *Journal of Computer Security*, *30*(4), 623-653. https://doi.org/10.3233/JCS-210037

Payares, E., Martínez-Santos, J. C. (2021). *Quantum machine learning for intrusion detection of distributed denial of service attacks: A comparative overview*. https://doi.org/10.1117/12.2593297

Pérez-Castillo, R., Serrano, M. A., Piattini, M. (2021). Software modernization to embrace quantum technology. *Advances in Engineering Software*, *151*, e102933. https://doi.org/10.1016/j.advengsoft.2020.102933

Perlner, R. A., Cooper, D. A. (2009). *Quantum resistant public key cryptography* [Artículo de conferencia]. 8th Symposium on Identity and Trust on the Internet. https://doi.org/10.1145/1527017.1527028

Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., Englund, D., Gehring, T., Lupo, C., Ottaviani, C., Pereira, J. L., Razavi, M., Shamsul Shaari, J., Tomamichel, M., Usenko, V. C., Vallone, G., Villoresi, P., Wallden, P. (2020). Advances in quantum cryptography. *Advances in Optics and Photonics*, *12*(4), 1012. https://doi.org/10.1364/AOP.361502

Pitwon, R. C. A., Lee, B. H. L. (2021). Harmonising international standards to promote commercial adoption of quantum technologies. En K. Bongs, M. J. Padgett, A. Fedrizzi, & A. Politi (Eds.), *Quantum Technology: Driving Commercialisation of an Enabling Science II* (vol. 11881, p. 16). SPIE. https://doi.org/10.1117/12.2602888

Pohasii, S., Milevskyi, S., Tomashevsky, B., Yoropay, N. (2022). Development of the double-contour protection concept in socio-cyberphysical systems. *Advanced Information Systems*, *6*(2), 57-66. https://doi.org/10.20998/2522-9052.2022.2.10

Ponemon Institute (2020). *The importance of training and awareness programs*. https://www.entrust.com/es/resources/reports/global-encryption-trends-study

Ponnusamy, V., Regunathan, N. D., Kumar, P., Annur, R., Rafique, K. (2020). A review of attacks and countermeasures in Internet of Things and cyber physical systems. En P. Kumar, V. Ponnusamy, & V. Jain (Eds.), *Industrial Internet of Things and Cyber-Physical Systems: Transforming the Conventional to Digital* (pp. 1-24). IGI Global Scientific Publishing. https://doi.org/10.4018/978-1-7998-2803-7.ch001

Popescu, L. (2019). *The cyber security of critical infrastructures in an increasingly connected world*. https://revista.unap.ro/index.php/bulletin/article/view/616/570

Project Management Institute (2017). *A guide to the Project Management Body of Knowledge (PMBOK® Guide)*. Project Management Institute.

Raheman, F. (2022). The future of cybersecurity in the age of quantum computers. *Future Internet*, *14*(11), 335. https://doi.org/10.3390/fi14110335

Rajamaki, J. (2018). *Industry-university collaboration on IoT cyber security education: Academic course: «Resilience of Internet of Things and cyber-physical systems»* [Artículo de conferencia]. IEEE Global Engineering Education Conference (EDUCON). https://doi.org/10.1109/EDUCON.2018.8363477

Rajna, G. (2015). *Quantum computing and cybersecurity*. https://vixra.org/pdf/1505.0109v1.pdf

Ramírez, R., Choucri, N. (2016). Improving interdisciplinary communication with standardized cyber security terminology: A literature review. *IEEE Access*, *4*, 2216-2243. https://doi.org/10.1109/ACCESS.2016.2544381

Rieffel, E. G., Venturelli, D., O'Gorman, B., Do, M. B., Prystay, E. M., Smelyanskiy, V. N. (2015). A case study in programming a quantum annealer for hard operational planning problems. *Quantum Information Processing*, *14*(1), 1-36. https://doi.org/10.1007/s11128-014-0892-x

Rodríguez, A. (2023). *A quantum cybersecurity agenda for Europe. Governing the transition to post-quantum cryptography*. https://api.semanticscholar.org/CorpusID:260055338

Sandhu, R., Coyne, E. J., Feinstein, H. L., Youman, C. E. (1996). Role-based access control models. *IEEE Computer*, *29*(2), 38-47.

SANS Institute (2019). *Collaborative defense: Lessons from the ICS cybersecurity conference*. https://www.sans.org/

Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., Peev, M. (2009). The security of practical quantum key distribution. *Reviews of Modern Physics*, *81*(3), 1301-1350.

Schneider, F. B. (2013). Cybersecurity education in universities. *IEEE Security & Privacy*, *11*(4), 3-4. https://doi.org/10.1109/MSP.2013.84

Schneier, B. (2018). *Click here to kill everybody: Security and survival in a hyper-connected world*. WW Norton & Company.

Schwalb, M. (2007). *Exploit derivatives & national security*. https://heinonline.org/HOL/LandingPage?handle=hein.journals/yjolt9&div=6&id=&page=

Serrano, M. A., Cruz-Lemus, J. A., Pérez-Castillo, R., Piattini, M. (2023). Quantum software components and platforms: Overview and quality assessment. *ACM Computing Surveys*, *55*(8), 1-31. https://doi.org/10.1145/3548679

Shane, P. M. (2012). *Texas law review see also response cybersecurity: Toward a meaningful policy framework*. https://doi.org/https://doi.org/10.31228/osf.io/b8hms

Sharevski, F., Trowbridge, A., Westbrook, J. (2018). *Novel approach for cybersecurity workforce development: A course in secure design* [Artículo de conferencia]. IEEE Integrated STEM Education Conference (ISEC). https://doi.org/10.1109/ISECon.2018.8340471

Simonov, M., Bertone, F., Goga, K., Terzo, O. (2019). Cyber kill chain defender for smart meters. *Advances in Intelligent Systems and Computing*, *772*, 386-397. https://doi.org/10.1007/978-3-319-93659-8_34

Singh, H., Gupta, D. L., Singh, A. K. (2014). Quantum key distribution protocols: A review. *IOSR Journal of Computer Engineering*, *16*(2), 01-09. https://doi.org/10.9790/0661-162110109

Sperotto, A., Hofstede, R., Dainotti, A., Schmitt, C., Rodosek, G. D. (2015). Special issue on measure, detect and mitigate–challenges and trends in network security. *International Journal of Network Management*, *25*(5), 261-262. https://doi.org/10.1002/nem.1905

Ståhl, B. (2013). *Monitoring infrastructure affordances* [Tesis de doctorado, Blekinge Institute of Technology]. http://urn.kb.se/resolve?urn=urn:nbn:se:bth-00544

Stoneburner, G., Goguen, A., Feringa, A. (2002). *Risk management guide for information technology systems*. https://sites.pitt.edu/~dtipper/2825/NIST_Risk.pdf

Streich, G. (2023). (Re-)configuring federal cybersecurity regulation: From critical infrastructures to the whole-of-the-nation. *Indiana Law Review*, *55*(4), 733-766. https://doi.org/10.18060/27133

Sturgeon, J. G. (2012). *Taking a quantum leap in cyber-deterrence*. https://api.semanticscholar.org/CorpusID:114567315

Taiber, J. (2020). *Unsettled topics concerning the impact of quantum technologies on automotive cybersecurity*. https://doi.org/10.4271/EPR2020026

Tao, Y., Xu, W., Li, H., Ji, S. (2019). *Experience and lessons in building an ICS security testbed* [Artículo de conferencia]. 1st International Conference on Industrial Artificial Intelligence (IAI), level 0. https://doi.org/10.1109/ICIAI.2019.8850804

Taylor, J. M., Sharif, H. R. (2017). *Security challenges and methods for protecting critical infrastructure cyber-physical systems* [Artículo de conferencia]. International Conference on Selected Topics in Mobile and Wireless Networking (MoWNeT). https://doi.org/10.1109/MoWNet.2017.8045959

Teodoraş, D.-A., Popovici, E.-C., Suciu, G., Sachian, M.-A. (2023). Quantum technology's role in cybersecurity. En M. Vladescu, I. Cristea & R. D. Tamas (Eds.), *Advanced Topics in Optoelectronics, Microelectronics, and Nanotechnologies XI* (vol. 12493, p. 99). SPIE. https://doi.org/10.1117/12.2643300

Tian, W., Ji, X., Liu, W., Liu, G., Zhai, J., Dai, Y., Huang, S. (2020). Prospect theoretic study of honeypot defense against advanced persistent threats in power grid. *IEEE Access*, *8*, 64075-64085. https://doi.org/10.1109/ACCESS.2020.2984795

Tomita, A. (2019). Implementation security certification of Decoy-BB84 quantum key distribution systems. *Advanced Quantum Technologies*, *2*(5-6), e1900005. https://doi.org/10.1002/qute.201900005

Tummala, V. M. R., Schoenherr, T. (2011). Assessing and managing risks using the supply chain risk management process (SCRMP). *Supply Chain Management*, *16*(6), 474-483.

Tyshyk, I. (2022). Testing the organization's corporate network for unauthorized access. *Cybersecurity: Education, Science, Technique*, *2*(18), 39-48. https://doi.org/10.28925/2663-4023.2022.18.3948

Vermeer, M. J. D., Heitzenrater, C., Parker, E., Moon, A., Lumpkin, D., Awan, J., Stapleton, P. A. (2023). *Evaluating cryptographic vulnerabilities created by quantum computing in industrial control systems*. RAND Corporation. https://doi.org/10.7249/RRA2427-1

Walenta, N., Soucarros, M., Stucki, D., Caselunghe, D., Domergue, M., Hagerman, M., Hart, R., Hayford, D., Houlmann, R., Legré, M., McCandlish, T., Page, J.-B., Tourville, M., Wolterman, R. (2015). Practical aspects of security certification for commercial quantum technologies. En D. A. Huckridge, R. Ebert, M. T. Gruneisen, M. Dusek, & J. G. Rarity (Eds.), *Electro-Optical and Infrared Systems: Technology and Applications XII; and Quantum Information Science and Technology* (vol. 9648, p. 96480U). SPIE. https://doi.org/10.1117/12.2193776

Whitman, M. E., Mattord, H. J. (2018). *Principles of information security*. Cengage Learning.

Witteman, H. O., Stahl, J. E. (2013). Facilitating interdisciplinary collaboration to tackle complex problems in health care: Report from an exploratory workshop. *Health Systems*, *2*(3), 162-170. https://doi.org/10.1057/hs.2013.3

Woo, H., Yi, J., Browne, J. C., Mok, A. K., Atkins, E., Xie, F. (2008). *Design and development methodology for resilient cyber-physical systems* [Artículo de conferencia]. 2008 The 28th International Conference on Distributed Computing Systems Workshops. https://doi.org/10.1109/ICDCS.Workshops.2008.62

Xu, F., Ma, X., Zhang, Q., Lo, H.-K., Pan, J.-W. (2020). Secure quantum key distribution with realistic devices. *Reviews of Modern Physics*, *92*(2), 025002. https://doi.org/10.1103/RevModPhys.92.025002

Xu, G., Chen, X.-B., Dou, Z., Yang, Y.-X., Li, Z. (2015). A novel protocol for multiparty quantum key management. *Quantum Information Processing*, *14*(8), 2959-2980. https://doi.org/10.1007/s11128-015-1021-1

Xu, W., Tao, Y., Yang, C., Chen, H. (2019). MSICST: Multiple-scenario industrial control system testbed for security research. *Computers, Materials & Continua*, *60*(2), 691-705. https://doi.org/10.32604/cmc.2019.05678

Yao, D. D., Almohri, H. M. J. (2013). *High assurance models for secure systems*. https://api.semanticscholar.org/CorpusID:110786313

Yesina, M. V., Ostrianska, Ye. V., Gorbenko, I. D. (2022). Status report on the third round of the NIST post-quantum cryptography standardization process. *Radiotekhnika*, *3*(210), 75-86. https://doi.org/10.30837/rt.2022.3.210.05

Yesina, M. V., Potii, O. V., Gorbenko, Yu. I., Ponomar, V. A. (2022). Risk estimation methodology in the post-quantum period. *Radiotekhnika*, *209*, 7-15. https://doi.org/10.30837/rt.2022.2.209.01

Zavitsanos, D., Ntanos, A., Toumasis, P., Raptakis, A., Kouloumentas, C., Stathopoulos, T., Setaki, F., Theodoropoulou, E., Lyberopoulos, G., Giannoulis, G., Avramopoulos, H. (2022). *Coexistence studies for DV-QKD integration in deployed RAN infrastructure* [Artículo de conferencia]. International Workshop on Fiber Optics in Access Networks (FOAN). https://doi.org/10.1109/FOAN56774.2022.9939691

Zhang, L., Wang, Q., Tian, B. (2013). Security threats and measures for the cyber-physical systems. *Journal of China Universities of Posts and Telecommunications*, *20*(Suppl. 1), 25-29. https://doi.org/10.1016/S1005-8885(13)60254-X

Zhao, Y., Fung, C.-H. F., Qi, B., Chen, C., Lo, H.-K. (2008). Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems. *Physical Review A*, *78*(4), 0e42333. https://doi.org/10.1103/PhysRevA.78.042333

Zhao, W., White, G. (2014). *Designing a Formal Model Facilitating Collaborative Information Sharing for Community Cyber Security* [Artículo de conferencia]. 47th Hawaii International Conference on System Sciences, Waikoloa, HI, USA. https://doi.org/10.1109/HICSS.2014.252

Zobel, C. W., Khansa, L. (2012). Quantifying cyberinfrastructure resilience against multi-event attacks. *Decision Sciences*, *43*(4), 687-710. https://doi.org/10.1111/j.1540-5915.2012.00364.x