REVISTA INCAING
ISSN 2448 9131

EL AVANCE DE LA COMPUTACIÓN CUÁNTICA EN LA GESTIÓN DE RIESGOS, UNA REVISIÓN SISTEMÁTICA

THE ADVANCE OF QUANTUM COMPUTING IN RISK MANAGEMENT, A SYSTEMATIC REVIEW

Autores:
[1]**Castillo Rosas Charles Duck**; Universidad Nacional de Trujillo, Trujillo - Perú
[2]**Díaz Tomás Marcos Iván**; Universidad Nacional de Trujillo, Trujillo - Perú
[3]**Mendoza de los Santos Alberto Carlos**; Universidad Nacional de Trujillo, Trujillo - Perú.
ORCID
[1]https://orcid.org/0009-0005-9389-3323
[2]https://orcid.org/0009-0006-0210-1288
[3]https://orcid.org/0000-0002-0469-915X

Resumen - La computación cuántica es una tecnología emergente basada en los principios de la mecánica cuántica con potencial para transformar diversas industrias, incluida la gestión de riesgos financieros. Esta tecnología permite realizar cálculos complejos a una velocidad que supera las capacidades de los ordenadores convencionales, planteando oportunidades y retos, especialmente en el campo de la seguridad de la información. Uno de los principales desafíos que presenta la computación cuántica es su impacto en la criptografía existente. Los algoritmos de cifrado tradicionales, esenciales para proteger la información y las comunicaciones financieras, pueden ser vulnerables a la capacidad de la computación cuántica para resolver problemas matemáticos complejos de manera rápida y eficiente. Esto crea un riesgo significativo para la seguridad de los datos confidenciales y la integridad de las transacciones financieras. Con el cifrado poscuántico y el uso de qubits, representa una solución innovadora para la gestión de riesgos, por ejemplo, los riesgos financieros relacionados con la seguridad de la información. Esta tecnología no sólo mejora la capacidad de procesamiento de datos, sino que también garantiza la protección de la privacidad en un entorno en constante cambio. La adopción de estas nuevas técnicas será crucial para mantener la seguridad financiera a medida que la computación cuántica continúe desarrollándose.

Abstract - Quantum computing is an emerging technology based on the principles of quantum mechanics with the potential to transform various industries, including financial risk management. This technology allows complex calculations to be carried out at a speed that exceeds the capabilities of conventional computers, posing opportunities and challenges, especially in the field of information security. One of the main challenges that quantum computing presents is its impact on existing cryptography. Traditional encryption algorithms, essential for protecting financial information and communications, may be vulnerable to quantum computing's ability to solve complex mathematical problems quickly and efficiently. This creates a significant risk to the security of sensitive data and the integrity of financial transactions. With post-quantum encryption and the use of qubits, it represents an innovative solution for risk management, for example financial risks related to information security. This technology not only improves data processing capacity but also ensures privacy protection in an ever-changing environment. Adoption of these new techniques will be crucial to maintaining financial security as quantum computing continues to develop.

Palabras clave:
Computación cuántica, gestión de riesgos, beneficios.

Key words:
Quantum computing, risk management, benefits.

I. INTRODUCCÍÓN

Cuando hablamos de computación cuántica, nos referimos a un analizador capaz de realizar cualquier tarea simplemente adecuándose en un modelo procesado, con el objetivo tecnológico de construir máquinas capaces de resolver problemas que la mecánica cuántica suponga una verdadera ventaja, algo que los primeros en usarla serían instituciones o grandes compañías [1].

Teniendo en cuenta lo que acabamos de decir, la computación cuántica presenta un gran avance en base a los principales problemas que una computadora común no podría resolver. [2] Por ejemplo, podemos tener un escenario base con 4 incidentes no resueltos que afectan globalmente a 2 controles de seguridad. De esta forma, optimizando el conjunto de incidencias a resolver, es posible que solo sea necesario destinar recursos a dos de las incidencias, resolviendo las otras

dos directamente después de haber reforzado los controles correspondientes, ahorrando así tiempo y recursos.

[3] Para hablar de la computación cuántica debemos hablar acerca de los qubit, los cuales se presentan por medio de un spin de electrons o fotones; que a diferencia de un bit clásico, que toma los valores de 0 y 1, un qubit es un sistema cuántico con multiples estados o varias probabilidades, entonces un qubit puede asumir valores diversos simultáneamente y su valor exacto solo será determinado al momento de cuantificarlo, estado por el cual el qubit estaya y no se puede usar hasta que se reinicie.

Muchos de los problemas de gestion de riesgo, puede enfocarse en el [4] ámbito financiero, de lo cual la computación cuántica puede encargarse, ofreciendo un enfoque computacional que mejora la eficiencia de tareas específicas.

Otros de los riesgos se basan en la [5] simulación de Monte Carlo, generando una distribución de "posibles estados futuros del mundo", obteniendo medidas y aplicación de controles de riesgo, como por ejemplo la imposición de límites.
[6] Instituciones financieras y reguladores deberían facilitar que la industria financiera debe poner sus esfuerzos para invertir sustancialmente en sistemas que prevengan las amenazas cibernéticas modernas y futuras en la infraestructura.

Vemos que algunos de los riesgos que puede solucionar la computación cuántica son los riesgos financieros, pero otro punto es la introducción de la IA a esta nueva tecnología, dándonos así la IA cuántica; la cual proporciona soluciones a desafíos industrials complejos con el aprendizaje automático dándonos avances significativos en la industria 4.0.

Teniendo estos riesgos mencionados, podríamos decir que, ¿el avance de la computación cuántica brindaría mejoras para la Gestión de Riesgos?

II. OBJETIVOS

Uno de los objetivos principales e importantes que se tuvo en cuenta, fue encontrar los conceptos y explicaciones de la Computación cuántica y que beneficios puede traer para muchos campos, en este caso para la gestión de riesgos, averiguar cómo influye la computación cuántica para evitar la pérdida de datos y qué puede ofrecer a las empresas para entrar en la industria 4.0.

III. METODOLOGÍA

En el trabajo presente, la metodología PRISMA fue nuestra guía para la revisión sistemática, verificando la importancia y los beneficios de la computación cuántica.

Para ello se tuvo un riguroso proceso de selección de artículos, tesis y libros. Por lo cual, se presentan las verificaciones de la metodología PRISMA que ayudaron para dicha selección.

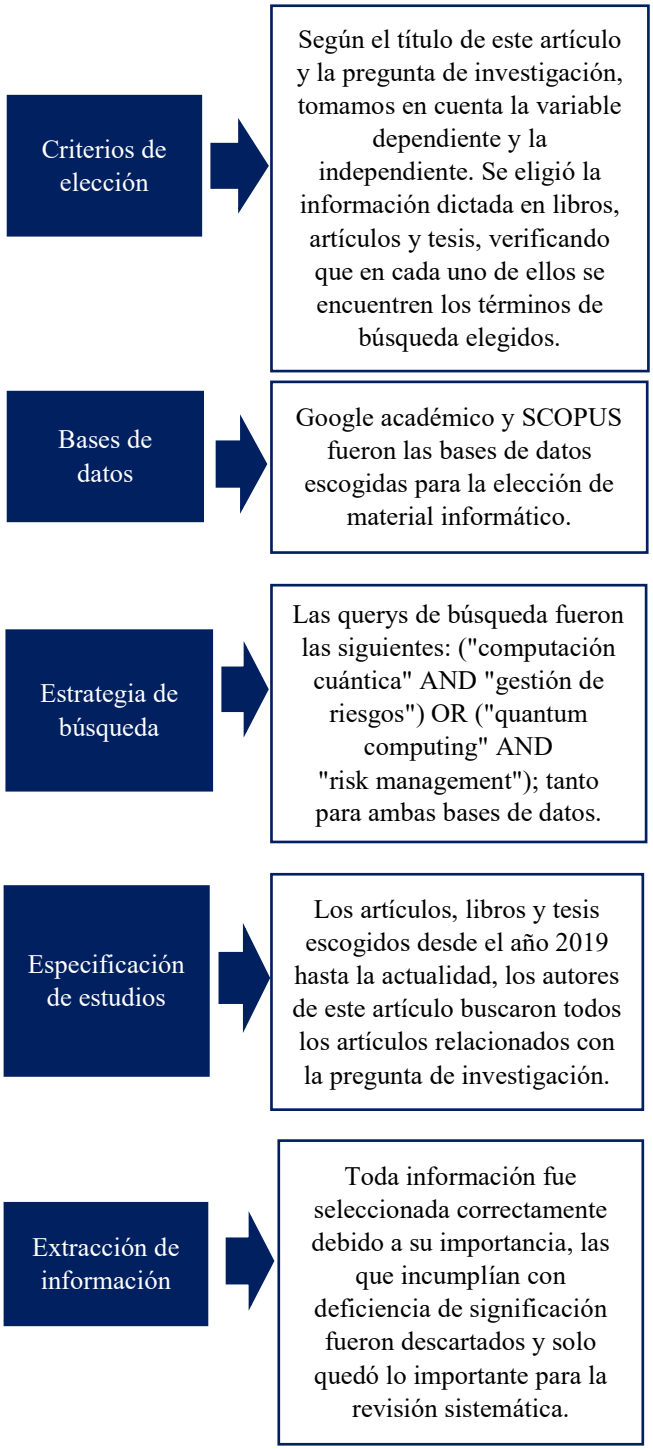

Figura 1. Verificación de metodología PRISMA

Según la metodología PRISMA, para seleccionar la información requerida se implementa el diagrama de flujo de 4 fases (Figura 2), pues dicho diagrama ayuda para la sustracción de información.

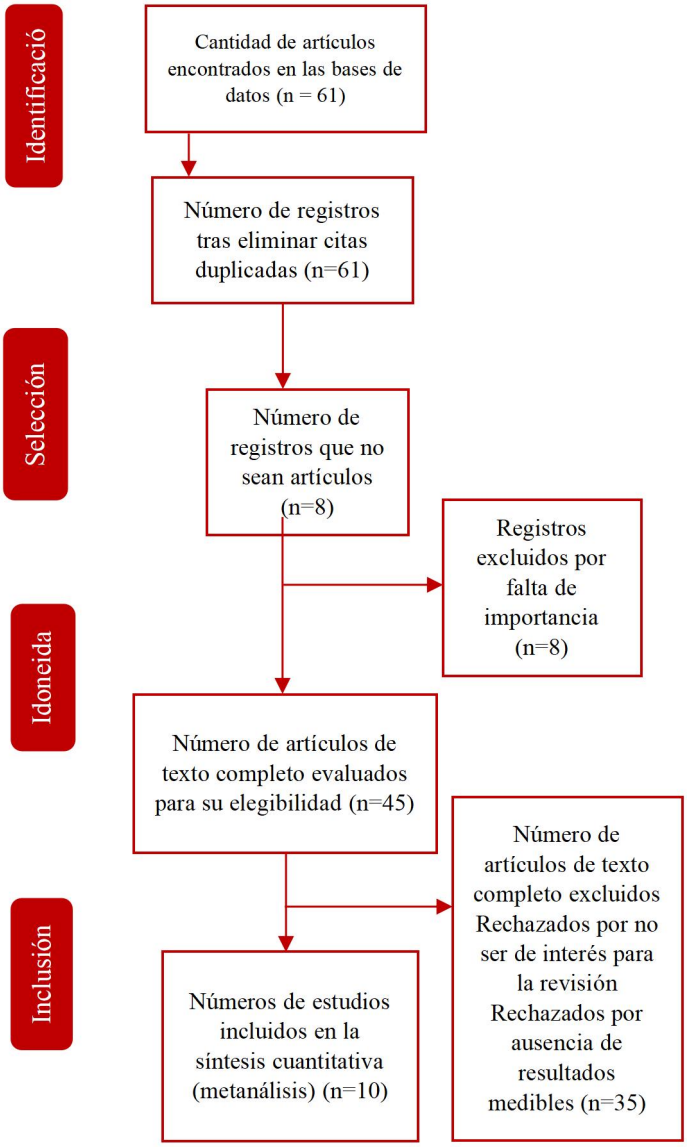

Figura 2. Diagrama de flujos de 4 estados

Resultados de la investigación

[7] En el entorno actual, la gestión de riesgos y seguridad, especialmente la gestión eficaz de los problemas de protección de datos, son más importantes que nunca. La velocidad para responder a incidentes y restaurar la seguridad del sistema es fundamental. Sin embargo, las soluciones tradicionales enfrentan desafíos debido al aumento exponencial del número de problemas y son cada vez menos útiles en situaciones de la vida real.

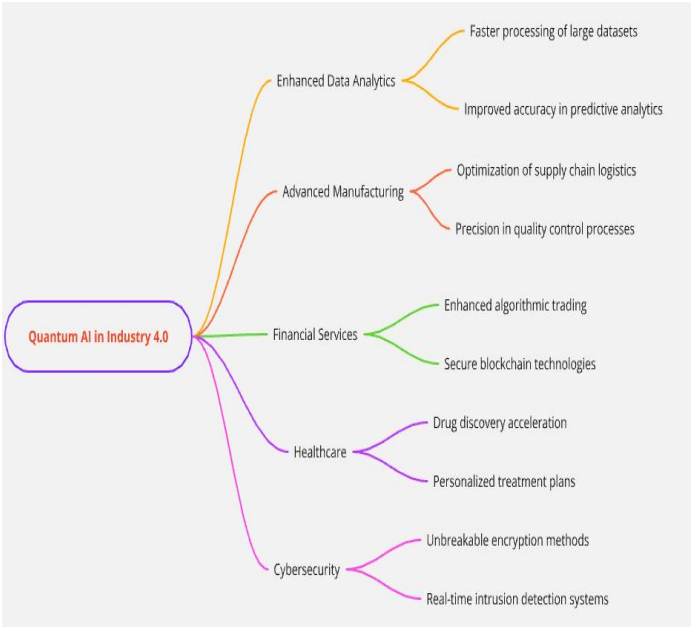

Figura 3. Vista simplificada de las posibles influencias de la IA cuántica en la Industria 4.0.

[7] La computación cuántica emerge como una solución revolucionaria en la gestión de riesgos y seguridad en la era de la Industria 4.0. Al ofrecer la capacidad de procesar grandes volúmenes de información de manera extremadamente eficiente, la computación cuántica transforma la forma en que las organizaciones pueden responder a incidentes de seguridad. Sin embargo, es en la combinación de la computación cuántica con la inteligencia artificial (IA) donde se desbloquea todo su potencial. Esta sinergia no solo permite un análisis más rápido y preciso de datos complejos, sino que también posibilita la toma de decisiones en tiempo real, lo cual es crucial para gestionar los riesgos en un entorno digital cada vez más complejo y dinámico.

La aplicación de la IA cuántica en la gestión de riesgos abarca varios sectores críticos. En ciberseguridad, por ejemplo, la capacidad de detectar intrusiones en tiempo real y desarrollar métodos de cifrado inquebrantables garantiza una protección robusta frente a amenazas avanzadas. En los servicios financieros, la IA cuántica optimiza el trading algorítmico y refuerza la seguridad de las tecnologías blockchain, asegurando la integridad y confiabilidad de las transacciones. En la manufactura avanzada, esta tecnología mejora la precisión en los procesos de control de calidad y optimiza la logística de la cadena de suministro, reduciendo vulnerabilidades en el sistema.

Además, la IA cuántica tiene un impacto significativo en la salud, acelerando el descubrimiento de fármacos y permitiendo la creación de planes de tratamiento personalizados, lo que contribuye a una gestión de riesgos más efectiva en la atención médica. En el análisis de datos, la capacidad de procesar y analizar grandes conjuntos de datos con mayor rapidez y exactitud mejora las capacidades predictivas, facilitando la identificación temprana de riesgos potenciales y la implementación de medidas preventivas.

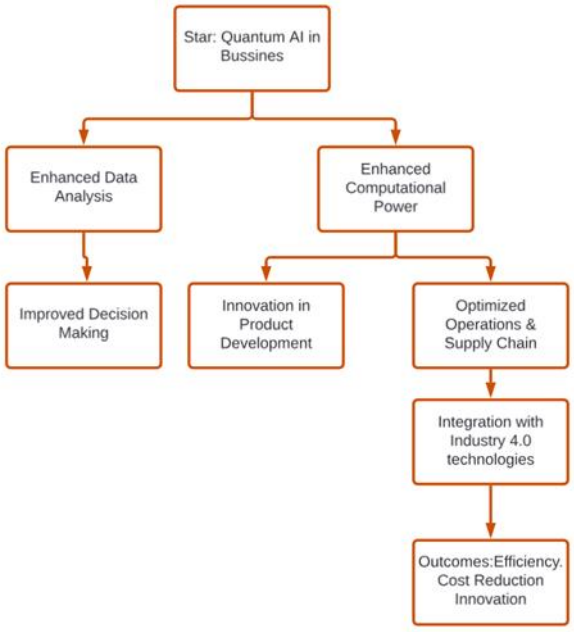

Figura 4. Cómo la IA cuántica contribuye potencialmente a los negocios innovadores.

[8] La comunicación a través de Internet es el pilar fundamental del mundo digitalizado. Cada paquete de datos viaja a través de múltiples canales inseguros y servidores no confiables antes de alcanzar su destino. Las filtraciones de datos y comunicaciones en el pasado llevaron al desarrollo de la criptografía de clave pública (PKC) para asegurar la seguridad y privacidad de las comunicaciones de extremo a extremo. Estos esquemas se basan en problemas matemáticos complejos como el logaritmo discreto y la factorización de números enteros.

[8] La amenaza inminente que representan las computadoras cuánticas para la criptografía tradicional ha impulsado el desarrollo de esquemas de criptografía de clave pública (PKC) post-cuánticos. Estos nuevos esquemas se basan en problemas matemáticos complejos que, según el conocimiento actual, son resistentes a la resolución eficiente por algoritmos cuánticos, incluso los más avanzados. Esta resistencia es crucial para mantener la seguridad en un entorno donde las capacidades de las computadoras cuánticas podrían comprometer los métodos criptográficos convencionales.

Para asegurar una transición efectiva hacia un futuro post-cuántico, se han lanzado numerosas iniciativas de estandarización a nivel global, lideradas por organizaciones como el Instituto Nacional de Estándares y Tecnología (NIST) de los Estados Unidos. Estas iniciativas buscan identificar y validar los mejores candidatos para los algoritmos de firma digital y encapsulación de claves post-cuánticos. Los esquemas seleccionados no solo deben ofrecer una seguridad robusta, sino también ser lo suficientemente eficientes para integrarse en los sistemas y protocolos existentes sin comprometer el rendimiento.

Los esquemas de encapsulación de claves post-cuánticos permiten que las partes involucradas acuerden una clave común de manera segura, incluso en presencia de un adversario con capacidades cuánticas. Esta clave compartida puede ser utilizada posteriormente para cifrar y descifrar mensajes mediante criptografía simétrica, garantizando así la seguridad y privacidad de las comunicaciones. De este modo, se asegura que la información intercambiada permanezca confidencial y protegida contra interceptaciones.

Por otro lado, los esquemas de firma digital post-cuánticos juegan un papel fundamental en la autenticación de mensajes y transacciones. Estos algoritmos permiten al receptor verificar la autenticidad del remitente y garantizar que el contenido no ha sido alterado durante el tránsito. En un entorno post-cuántico, donde la integridad de los datos es tan crucial como su confidencialidad, la adopción de estos nuevos esquemas será esencial para mantener la confianza en la seguridad digital.

Estos esquemas post-cuánticos están destinados a reemplazar los algoritmos PKC clásicos en una amplia variedad de aplicaciones, siendo el protocolo de red TLS (Transport Layer Security) uno de los más críticos. TLS es fundamental para asegurar las comunicaciones en Internet, y su adaptación a la criptografía post-cuántica es un paso necesario para garantizar la continuidad de la seguridad en la era digital.

Descripción de los enfoques de seguridad de datos.

Con la llegada de las computadoras cuánticas hace que los algoritmos de seguridad existentes que incluyen algoritmos de cifrado y descifrado como DSA, RSA y otros mecanismos de cifrado sean bastante débiles y vulnerables a los ataques de seguridad. [10] Se espera que cualquier sistema que dependa del cifrado de clave pública duplique la longitud de su clave actual para inmune a los ataques de ciberseguridad mundial poscuánticos. Se espera que los algoritmos asimétricos basados en la factorización de números primos grandes sean los más vulnerables.

En el ámbito de la protección de datos genómicos, nuestro estudio subraya que la criptografía post-cuántica representa una solución prometedora para garantizar la seguridad a largo plazo frente a las amenazas que las computadoras cuánticas podrían plantear. Aunque los algoritmos post-cuánticos aún se encuentran en una fase de desarrollo y deben superar una serie de desafíos técnicos, su capacidad para resistir ataques cuánticos podría ser decisiva en la preservación de la confidencialidad de los datos genómicos.

El cifrado post-cuántico ofrece ventajas significativas en comparación con los métodos criptográficos tradicionales, como el cifrado simétrico y asimétrico, que han sido la base de la seguridad digital durante décadas. Además, enfoques emergentes como la computación multipartita y el cifrado homomórfico, que permiten realizar operaciones en datos cifrados sin necesidad de descifrarlos, han mostrado avances importantes, pero aún enfrentan limitaciones en cuanto a

eficiencia y escalabilidad.

A medida que los algoritmos post-cuánticos evolucionan, se están desarrollando protocolos más prácticos y eficientes que no solo buscan reemplazar a los esquemas criptográficos actuales, sino también integrarse de manera efectiva en sistemas que manejan grandes volúmenes de datos sensibles, como los datos genómicos. Esta evolución es fundamental, dado que la naturaleza altamente personal y privada de la información genómica la convierte en un objetivo atractivo para los atacantes, y su protección debe ser una prioridad máxima.

El potencial del cifrado post-cuántico para proteger estos datos radica en su capacidad para ofrecer seguridad robusta incluso en un escenario donde las computadoras cuánticas sean una realidad. Esto no solo asegura la integridad y confidencialidad de la información genómica, sino que también permite a las instituciones que manejan estos datos, como hospitales y centros de investigación, cumplir con normativas de protección de datos más estrictas, garantizando la confianza del público en el manejo de su información más sensible.

Tabla 1. Ventajas y desventajas de diferentes enfoques de seguridad de datos.

Criterio	Rendimiento escalable	Adecuación para colaboración	Complejidad	Robustez
Cifrado simétrico	Rápido y eficiente para grandes conjuntos de datos genómico.	Menos adecuado si hay múltiples partes involucradas debido a la dependencia de una única clave.	Gestión de claves criptográficas sencilla debido a que solo se involucra una clave.	Riesgoso si se compromete la clave en entornos colaborativos; seguro con una gestión robusta de claves.
Cifrado asimétrico	Más lento para cifrar datos genómicos a gran escala, lo que puede retrasar la transferencia de datos.	La clave pública puede compartirse con colaboradores, asegurando transferencias de datos seguras entre instituciones sin comprometer la integridad.	La gestión de claves puede ser complicada para múltiples partes.	Riesgoso si se compromete la clave en entornos colaborativos; seguro con una gestión robusta de claves.
Computación multipartita	Computacionalmente caro, lo que lo hace menos práctico el estudio de información genómica	Permite el trabajo colaborativo entre instituciones sin revelar los datos de cada una.	Complejidad en la configuración y dependencia de las partes colaboradoras.	Seguridad máxima en la colaboración: los datos genómicos siempre están cifrados, lo que impide que los participantes alteren los datos.
Cifrado homomórfico	Bien adecuado para el procesamiento de datos genómicos en la nube, pero computacionalmente intensivo con tiempos de procesamiento prolongados.	Facilita la colaboración fácilmente a través de capacidades en la nube, pero es desafiante de configurar para todas las colaboraciones	La configuración inicial y la implementación pueden ser desafiantes.	Excelente debido a que el desarrollo de cálculos cifrados, no requiere necesidad de descifrar.
Post-cuántico	Difícil de escalar actualmente para conjuntos de datos a gran escala.	Potencialmente adecuado, pero depende del desarrollo de protocolos prácticos y eficientes que sean fácilmente adoptables por múltiples partes.	Complejo en términos de desarrollo e implementación; a menudo requiere experiencia y recursos significativos para implementarlo correctamente.	Actualmente, las defensas sólidas contra los ataques cuánticos para garantizar la seguridad a largo plazo de los datos genómicos son limitadas.

Reflexiones Finales

Esta revision destaca la relevancia de la criptografía post-cuántica para proteger los datos genómicos frente a las futuras amenazas que podrían presentar las computadoras cuánticas. Aunque estos algoritmos están en desarrollo y enfrentan desafíos técnicos, su capacidad para resistir ataques cuánticos podría ser crucial para mantener la confidencialidad de los datos genómicos. Comparado con los métodos criptográficos tradicionales, el cifrado post-cuántico ofrece ventajas significativas. Además, enfoques como la computación multipartita y el cifrado homomórfico, que permiten operar en datos cifrados sin descifrarlos, están avanzando, aunque aún enfrentan limitaciones en eficiencia y escalabilidad. A medida que evolucionan, los algoritmos post-cuánticos buscan no solo reemplazar los esquemas actuales, sino también integrarse eficazmente en sistemas que manejan grandes volúmenes de datos sensibles, como los genómicos. La protección de esta información es esencial, dado su carácter personal y privado, lo que la convierte en un objetivo atractivo para atacantes. La criptografía post-cuántica podría asegurar tanto la integridad como la confidencialidad de estos datos, permitiendo a las instituciones cumplir con normativas más estrictas y mantener la confianza pública en la gestión de su información más sensible.

Todo esto planea descubrir nuevas y eficientes maneras de gestionar los riesgos para que las empresas lleguen a la industria 4.0, ya sea con el cifrado pos-cuántico o modelos que gestionan los datos junto a la computación cuántica

IV. REFERENCIAS

[1] Miranda, N. D. (2007). Computación cuántica. *Universidad de La Laguna*, *1*, 1-89. https://www.mundotec.com.ar/Computacion-Cuantica.pdf

[2] Serrano, M. A. Minimizing incident response time in real-world scenarios using quantum computing. Softw. Qual. J. 1–30 (2023). https://doi.org/10.1007/s11219-023-09632-6

[3] Piattini, M., Serrano, M., Pérez-Castillo, R., Petersen, G., & Hevia, J. L. (2021). Hacia una ingeniería de software cuántica. Profesional de TI, 23(1), 62–66. https://doi.org/10.1109/MITP.2020.3019522

[4] Leclerc, L., Ortiz-Gutiérrez, L., Grijalva, S., Albrecht, B., Cline, J. R., Elfving, V. E., ... & M'tamon, D. (2023). Financial risk management on a neutral atom quantum processor. Physical Review Research, 5(4), 043117. https://doi.org/10.1103/PhysRevResearch.5.043117

[5] Wilkens, S., & Moorhouse, J. (2023). Quantum computing for financial risk measurement. Quantum Information Processing, 22(1), 51. https://doi.org/10.1007/s11128-022-03777-2

[6] Grody, Allan D., Addressing Cyber-Risk in Financial Institutions and in the Financial System (February 21, 2020). Journal of Risk Management in Financial Institutions, Vol. 13 Issue 2, 2020. https://doi.org/10.69554/LCUN5985

[7] How, M. L., & Cheah, S. M. (2024). Forging the future: strategic approaches to quantum ai integration for industry transformation. AI, 5(1), 290-323 https://www.mdpi.com/2673-2688/5/1/15

[8] Aikata, A., Mert, A. C., Imran, M., Pagliarini, S., & Roy, S. S. (2022). KaLi: A crystal for post-quantum security using Kyber and Dilithium. IEEE Transactions on Circuits and Systems I: Regular Papers, 70(2), 747-758. https://doi.org/10.1109/TCSI.2022.3219555

[9] "Post-quantum cryptography- call for proposals," 2017. [Online]. Available: https://csrc.nist.gov/projects/post-quantum-cryptography

[10] Tripathy, B. K., Goel, S., & Guha, A. (2024). Quantum Computing for IoT Security. In B. Mishra (Ed.), Fostering Cross-Industry Sustainability With Intelligent Technologies (pp. 1-20). IGI Global. https://doi.org/10.4018/979-8-3693-1638-2.ch001