Centro de Respuestas a Incidentes Informáticos
CSIRT Académico UNAD

Avances en Computación Cuántica: El Chip Majorana 1 y su Papel en la ciberseguridad

VIEM
Vicerrectoría de Innovación y Emprendimiento

ECBTI
Escuela de Ciencias Básicas, Tecnología e Ingeniería

Semillero de Investigación
Ceros y Unos

Centro de Respuestas a Incidentes Informáticos
CSIRT Académico UNAD

Boletín de Ciberseguridad

Medio de Divulgación del Centro de Respuestas a Incidentes Informáticos: CSIRT Académico UNAD

E-boletín Informativo CSIRT Académico UNAD

Medio de divulgación: Correo Electrónico, Sitio Web

Incluye: Noticias, alertas o informes relacionados con la disciplina de la ciberseguridad

Número Veintiocho
Febrero de 2025

Universidad Nacional Abierta y a Distancia (UNAD)
Vicerrectoría de Innovación y Emprendimiento (VIEM)
Escuela de Ciencias Básicas Tecnología Ingeniería (ECBTI)
Maestría en Ciberseguridad
Especialización en Seguridad Informática
CSIRT Académico UNAD

Universidad Nacional Abierta y a Distancia
Calle 14 sur No. 14-23 |Bogotá D.C
Correo electrónico: csirt@unad.edu.co
Página web: https://csirt.unad.edu.co

Edición electrónica, financiada por la Universidad Nacional Abierta y a Distancia (UNAD)

Vicerrectoría de Innovación y Emprendimiento (VIEM)
Ing. Andrés Ernesto Salinas - Vicerrector

Escuela de Ciencias Básicas Tecnología e Ingeniería (ECBTI)
Ing. Claudio Camilo González Clavijo – Decano

Maestría en Ciberseguridad (ECBTI)
Ing. Sonia Ximena Moreno Molano –
Líder Programa de Maestría en Ciberseguridad

Semillero de Investigación Ceros y Unos, adscrito al Grupo de Byte InDesign

Centro de Respuestas a Incidentes Informáticos CSIRT Académico UNAD
Ing. Luis Fernando Zambrano Hernández – Líder CSIRT Académico UNAD

Responsable de la Edición
Ing. Luis Fernando Zambrano Hernandez

Revisó
Libardo Cardenas Corral
Analista CSIRT Académico UNAD

Estado legal:
Periodicidad: Mensual
ISSN: 2806-0164

Tabla de Contenido

Centro de Respuestas a Incidentes Informáticos
CSIRT Académico UNAD

Boletín de Ciberseguridad

Boletín informativo Número 29

Febrero 2025

Avances en Computación Cuántica: El Chip Majorana 1 y su Papel en la ciberseguridad

Autores:

Luis Fernando Zambrano Hernández
CSIRT Académico UNAD
https://orcid.org/0000-0002-4690-3526

Hernando José Peña Hidalgo
CSIRT Académico UNAD
https://orcid.org/0000-0002-3477-2645

Sonia Ximena Moreno Molano
Líder Maestría en Ciberseguridad
https://orcid.org/0009-0002-6133-5157

Néstor Raúl Cárdenas Corral
CSIRT Académico UNAD
https://orcid.org/0000-0003-3691-0148

Introducción

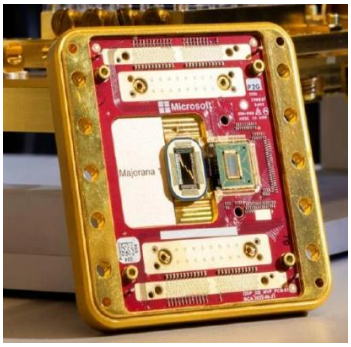


Ilustración 1.Fuente https://blog.masmovil.es/

En el actual panorama de la computación cuántica, los desarrollos en hardware han avanzado a pasos agigantados. Uno de los avances más prometedores es el Chip Majorana 1, el cual podría redefinir la ciberseguridad y la criptografía moderna. Este chip, basado en fermiones de Majorana[1], ofrece propiedades inéditas que lo hacen altamente resistente a errores cuánticos y robusto frente a ataques cibernéticos (Morales & Ávila, 2025).

La computación cuántica es un paradigma emergente que aprovecha principios de la mecánica cuántica, como la superposición y el entrelazamiento, para procesar información de manera exponencialmente más rápida que los sistemas clásicos (Dubey et al., 2025). A diferencia de la computación clásica, que almacena información en bits binarios (0 y 1), la computación cuántica utiliza qubits, que pueden existir en múltiples estados simultáneamente, aumentando la eficiencia de ciertos algoritmos (Lara Pérez, 2019).

En el ámbito de la ciberseguridad, esta capacidad disruptiva representa tanto una oportunidad como una amenaza. Por un lado, permite el desarrollo de nuevos algoritmos de cifrado cuánticamente seguros, como la distribución de claves cuánticas (QKD) (Morales & Ávila, 2025). Por otro lado, también hace obsoletos muchos de los sistemas criptográficos actuales, como RSA y ECC, al permitir su descifrado en tiempos prácticos mediante algoritmos como el de Shor (Shor, 1994). Este doble filo resalta la urgencia de investigar soluciones cuánticas para fortalecer la seguridad digital antes de que los sistemas actuales se vuelvan vulnerables (Sarma & Hartmann, 2023).

[1] Un fermión de Majorana es una partícula elemental que es su propia antipartícula. Fueron formulados como hipótesis por Ettore Majorana en 1937

Desarrollo

Pero, ¿Qué es la computación Cuántica?

La computación cuántica es un paradigma de procesamiento de información basado en los principios de la mecánica cuántica, lo que la hace fundamentalmente diferente de la computación clásica. Mientras que las computadoras tradicionales utilizan bits (que pueden representar valores de 0 o 1), las computadoras cuánticas operan con qubits, los cuales pueden estar en una superposición de ambos estados simultáneamente, permitiendo realizar cálculos con una eficiencia exponencialmente mayor en comparación con los sistemas clásicos (Lara Pérez, 2019).

Ilustración 2. Fuente (OpenAI, 2025)

Principios Fundamentales de la Computación Cuántica

La computación cuántica se basa en tres propiedades fundamentales de la mecánica cuántica:

- **Superposición**: diferencia de los bits tradicionales que pueden ser solo 0 o 1, los qubits pueden estar en una combinación de ambos estados simultáneamente. Esto permite realizar múltiples cálculos en paralelo, aumentando significativamente la velocidad de procesamiento.
- **Entrelazamiento Cuántico**: Es un fenómeno en el cual dos o más qubits se encuentran interconectados de tal manera que el estado de uno influye instantáneamente en el otro, sin importar la distancia. Esta propiedad es crucial para el desarrollo de sistemas de cifrado cuántico y algoritmos optimizados.
- **Interferencia Cuántica**: Los qubits pueden experimentar interferencias que permiten reforzar las soluciones correctas y cancelar las incorrectas, optimizando la ejecución de algoritmos complejos.

Ilustración 3. Comparación entre Computación Clásica y Computación Cuántica

Característica	Computación Clásica	Computación Cuántica
Unidad básica de datos	Bit (0 o 1)	Qubit (0 y 1 simultáneamente)
Capacidad de procesamiento	Lineal (una operación por ciclo)	Exponencial (varias operaciones simultáneamente)
Velocidad de procesamiento	Limitada por la arquitectura	Mucho más rápida en problemas complejos
Seguridad en la información	Basada en criptografía clásica	Puede usar criptografía cuántica (QKD) para mayor seguridad

Nota. Mientras que la computación clásica se basa en bits y procesamiento lineal, la computación cuántica utiliza qubits y aprovecha la superposición y el entrelazamiento para ejecutar múltiples operaciones simultáneamente, ofreciendo ventajas significativas en seguridad y rendimiento.

Aplicaciones de la Computación cuántica

La computación cuántica no solo representa un avance en términos de capacidad de procesamiento, sino que también tiene aplicaciones prácticas en múltiples industrias:

La computación cuántica está transformando diversas áreas de la tecnología y la sociedad con su capacidad de procesamiento avanzado. En el ámbito de la ciberseguridad, representa una amenaza para los sistemas de cifrado tradicionales, como RSA y ECC, impulsando el desarrollo de criptografía post-cuántica (Shor, 1994). En respuesta, la Distribución Cuántica de Claves (QKD) permite generar claves seguras a nivel cuántico, garantizando la integridad de la comunicación (Morales & Ávila, 2025). En optimización y logística, los algoritmos cuánticos pueden resolver problemas de transporte, cadena de suministro y planificación con mayor eficiencia que los métodos clásicos. En la simulación de materiales y fármacos, la computación cuántica permite modelar moléculas complejas con una precisión sin precedentes, acelerando el desarrollo de nuevos materiales y medicamentos (Jaksch et al., 2000). Finalmente, en inteligencia artificial y machine learning, los algoritmos cuánticos pueden mejorar los procesos de aprendizaje automático, entrenando modelos con mayor velocidad y precisión que los sistemas actuales, sentando las bases para una revolución tecnológica en múltiples sectores.

Desafíos y Futuro de la Computación Cuántica

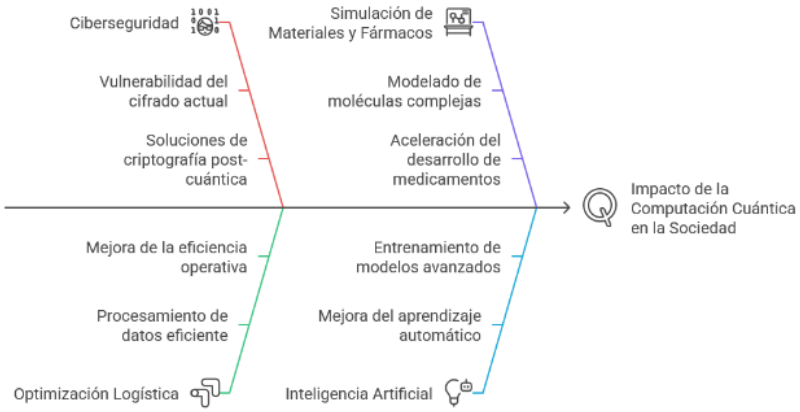
A pesar de su enorme potencial, la computación cuántica enfrenta varios desafíos:

Estabilidad y Decoherencia Cuántica: Los qubits son extremadamente sensibles a su entorno, lo que provoca errores en los cálculos si no se mantienen en condiciones específicas.
Costos de Implementación: La tecnología cuántica requiere temperaturas cercanas al cero absoluto (-273.15°C) para operar correctamente, lo que incrementa los costos y dificulta su adopción masiva.

Falta de Infraestructura y Estándares: Aún no existen estándares globales para la computación cuántica, lo que hace que su implementación en la industria sea un proceso complejo y lento.

A pesar de estos retos, empresas como Google, Microsoft e IBM están invirtiendo en el desarrollo de hardware cuántico, como el Chip Majorana 1, que promete avances en estabilidad y escalabilidad (PCWorld, 2025).

Ilustración 4. Impacto de la computación cuántica en el sector industrial



Elaborado con https://app.napkin.ai/

Concepto del Chip Majorana 1

El Majorana 1 es un chip cuántico desarrollado por Microsoft que representa un avance significativo en el campo de la computación cuántica.

Este procesador se basa en una arquitectura de núcleo topológico, utilizando partículas denominadas fermiones de Majorana para crear qubits más estables y menos propensos a errores. Este enfoque promete una mayor escalabilidad y fiabilidad en comparación con las tecnologías cuánticas tradicionales (Microsoft, 2025).

Los fermiones de Majorana son partículas que actúan como sus propias antipartículas, una propiedad que ha sido teorizada durante décadas pero que solo recientemente ha sido demostrada experimentalmente. La utilización de estas partículas permite la creación de qubits topológicos, que son inherentemente más resistentes a las perturbaciones ambientales, uno de los principales desafíos en la construcción de computadoras cuánticas prácticas (Microsoft, 2025).

La arquitectura de núcleo topológico del Majorana 1 facilita la integración de hasta un millón de qubits en un solo chip, lo que podría revolucionar la capacidad de procesamiento de las computadoras cuánticas y permitir la resolución de problemas complejos en campos como la criptografía, la simulación de materiales y la inteligencia artificial (Microsoft, 2025).

Este desarrollo es el resultado de casi dos décadas de investigación por parte de Microsoft, culminando en la creación de un material innovador conocido como "topoconductor", que es esencial para la manipulación efectiva de los fermiones de Majorana en el chip (Microsoft, 2025).

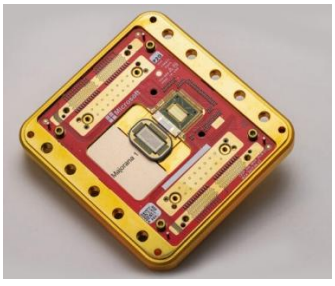


Imagen recuperada de: https://news.microsoft.com/source/latam/noticias-de-microsoft/microsoft-presenta-majorana-1-el-primer-procesador-cuantico-del-mundo-impulsado-por-qubits-topologicos/

Aplicaciones en Ciberseguridad

El impacto del chip Majorana 1 en la ciberseguridad es significativo. Su capacidad de procesar grandes volúmenes de información y ejecutar algoritmos de manera exponencialmente más rápida que las computadoras clásicas lo convierte en un aliado tanto para la ofensiva como para la defensiva en seguridad digital (Microsoft, 2025b).

- ✓ Criptografía Post-Cuántica: Una de las principales preocupaciones en ciberseguridad es que los algoritmos de cifrado actuales, como RSA o ECC, podrían volverse obsoletos debido a la capacidad de los ordenadores cuánticos de romper estas claves con el algoritmo de Shor. La tecnología de Majorana 1 puede ser utilizada para desarrollar algoritmos de criptografía post-cuántica, que sean resistentes a ataques de computadoras cuánticas (Arxiv, 2025).
- ✓ Distribución Cuántica de Claves (QKD): La QKD es un método de comunicación segura basado en principios cuánticos, que garantiza la detección de cualquier intento de interceptación. Con la estabilidad mejorada del chip Majorana 1, los sistemas de distribución de claves cuánticas pueden volverse más confiables y aplicables en infraestructuras críticas.
- ✓ Protección contra Ciberataques Cuánticos: A medida que la computación cuántica avanza, también lo hacen las amenazas. La criptografía basada en Majorana 1 puede proporcionar herramientas avanzadas para detectar y neutralizar ataques cibernéticos impulsados por algoritmos cuánticos maliciosos.
- ✓ Fortalecimiento de Infraestructuras Críticas: Sectores como el financiero, gubernamental y de telecomunicaciones podrían beneficiarse del Majorana 1 para proteger información sensible y transacciones digitales contra futuros ataques cuánticos. La implementación de estos sistemas permitiría garantizar la integridad de datos en redes altamente seguras y robustas.
- ✓ Autenticación Cuántica: La tecnología del chip Majorana 1 podría permitir sistemas avanzados de autenticación cuántica, eliminando por completo la posibilidad de suplantación de identidad o ataques de intermediario, asegurando la validez y veracidad de las credenciales digitales.

Desafíos y Futuro de Majorana 1

Aunque el chip Majorana 1 representa un avance significativo, aún existen desafíos en su implementación y escalabilidad. Algunos de estos incluyen:

- Infraestructura y costos: La computación cuántica requiere hardware altamente especializado y condiciones de operación extremadamente controladas, como temperaturas cercanas al cero absoluto para evitar la decoherencia (Microsoft, 2025b).
- Desarrollo de software cuántico: Si bien la arquitectura de Majorana 1 mejora la estabilidad de los qubits, aún es necesario desarrollar software optimizado que aproveche completamente esta tecnología.

Regulación y estándares: La adopción de la computación cuántica en ciberseguridad requiere la creación de estándares internacionales y regulaciones que aseguren su implementación de manera ética y segura (Microsoft, 2025c).

Conclusiones

El Majorana 1 marca un punto de inflexión en la computación cuántica, ofreciendo un enfoque innovador para resolver los problemas de estabilidad y escalabilidad que han frenado el desarrollo de esta tecnología. Su aplicación en ciberseguridad tiene el potencial de revolucionar la protección de datos y garantizar sistemas robustos contra amenazas futuras.

Microsoft ha apostado por un enfoque basado en qubits topológicos, que puede convertirse en la base para la próxima generación de ordenadores cuánticos seguros. Aunque aún queda camino por recorrer, el Majorana 1 representa un paso crucial hacia un futuro donde la computación cuántica sea una realidad accesible y aplicada en la protección de la información global (Microsoft, 2025a).

Canales de comunicación

El CSIRT Académico UNAD, actualmente cuenta con los siguientes canales de comunicación:

- Correo: csirt@unad.edu.co
- Página web: https://csirt.unad.edu.co

Referentes Bibliograficos

Dubey, V., Shende, P., Kumbhare, B., & Laxane, Y. B. (2025). Exploring AI Techniques for Quantum Threat Detection and Prevention. *Indian Journal of Computer Science and Technology, 4*(1), 8-12. https://doi.org/10.59256/indjcst.20250401002

Jaksch, D., Briegel, H.-J., Cirac, J. I., Gardiner, C. W., & Zoller, P. (2000). Entanglement of atoms via cold controlled collisions. *Physical Review Letters, 82*(9), 1975-1978. https://doi.org/10.1103/PhysRevLett.82.1975

Lara Pérez, M. L. (2019). *La computación cuántica y las implicaciones sobre la criptografía moderna*. Universidad Nacional Abierta y a Distancia.

Morales, G. N., & Ávila, M. (2025). Acerca de las compuertas lógicas cuánticas más rápidas y precisas. *Revista de Computación Cuántica, 10*(2), 45-59.

Sarma, S., & Hartmann, A. (2023). Quantum computing advances: Enhancing security with superconducting qubits. *Journal of Quantum Security, 15*(4), 112-126.

Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, 124-134.

Cinco Días. (2024, septiembre 25). *El CDTI adjudica a Sener un proyecto referente en seguridad cuántica para satélites*. Recuperado de https://cincodias.elpais.com/companias/2024-09-25/el-cdti-adjudica-a-sener-un-proyecto-referente-en-seguridad-cuantica-para-satelites.html

Infobae. (2024, diciembre 15). *Los misterios del mundo cuántico: cómo son los nuevos chips del futuro y qué problemas podrían resolver*. Recuperado de https://www.infobae.com/america/ciencia-america/2024/12/15/los-misterios-del-mundo-cuantico-como-son-los-nuevos-chips-del-futuro-y-que-problemas-podrian-resolver/

PCWorld. (2025, febrero 21). *Microsoft's new Majorana 1 chip is a quantum computing breakthrough*. Recuperado de https://www.pcworld.com/article/2616121/microsoft-makes-quantum-computing-breakthrough-with-new-majorana-1-chip.html

Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, 124-134.

The Times. (2024, agosto 15). *Battle begins to stop quantum computers smashing cyber defences*. Recuperado de https://www.thetimes.co.uk/article/battle-begins-to-stop-quantum-computers-smashing-cyber-defences-rzmlwqw7f

Microsoft. (2025, febrero 19). *Microsoft unveils Majorana 1, the world's first quantum processor powered by topological qubits*. Recuperado de https://azure.microsoft.com/en-us/blog/quantum/2025/02/19/microsoft-unveils-majorana-1-the-worlds-first-quantum-processor-powered-by-topological-qubits/

Microsoft. (2025a). *El chip Majorana 1 de Microsoft abre un nuevo camino para la computación cuántica*. Recuperado de https://news.microsoft.com/source/latam/features/ia/el-chip-majorana-1-de-microsoft-abre-un-nuevo-camino-para-la-computacion-cuantica/

Microsoft. (2025b). *Azure Quantum y el qubit topológico Majorana*. Recuperado de https://news.microsoft.com/source/features/innovation/azure-quantum-majorana-topological-qubit/

Microsoft. (2025c). *Microsoft unveils Majorana 1: The world's first quantum processor powered by topological qubits*. Recuperado de https://azure.microsoft.com/en-us/blog/quantum/2025/02/19/microsoft-unveils-majorana-1-the-worlds-first-quantum-processor-powered-by-topological-qubits/

Microsoft. (2025d). *Microsoft anuncia el nuevo chip Majorana 1 para impulsar la computación cuántica*. Recuperado de https://news.microsoft.com/azure-quantum/