

LA COMPUTACIÓN CUÁNTICA, RIESGOS ÉTICOS Y VACÍOS NORMATIVOS. UN ANÁLISIS MIXTO

GLADYS-INÉS BUSTAMANTE-CABRERA

Universidad Mayor de San Andrés. La Paz-Bolivia

CARMEN-ALICIA CARDOZO DE MARTÍNEZ

Universidad de Chile. Santiago de Chile

ZAIRA-RUTH ZUVIRÍA-LÓPEZ

Universidad Autónoma de Guadalajara. Guadalajara-México

BENJAMÍN BARÓN-VELANDIA

Corporación Universitaria Minuto de Dios-UNIMINUTO

Rectoría Bogotá y la Facultad de Educación de la Universidad de Missouri-Columbia

RESUMEN: La computación cuántica (CC) es una tecnología emergente con alto potencial de transformación en áreas como la criptografía, simulación de materiales y procesamiento de datos complejos. Sin embargo, no se abordan con suficiencia los problemas éticos y normativos que puede traer esta tecnología. El objetivo del estudio es analizar los riesgos éticos y vacíos normativos asociados a la computación cuántica (CC). Se realizó un estudio mixto secuencial exploratorio, revisando en una primera fase las patentes registradas de CC en el mundo. Además, se revisaron bases académicas en Google Scholar, Lens, Scopus y PubMed en el periodo de 2019 a 2024. Los artículos se analizaron con Atlas ti v25 y las patentes con SPSSv25 para el análisis exploratorio de correspondencias. Se identificaron 28494 solicitudes de patentes, de las cuales 17694 se encontraban activas. En la literatura revisada 19 documentos cumplían los requisitos de selección 2483. Luego de triangulación se obtuvieron 6 códigos emergentes, relacionados con riesgos potenciales, componentes éticos y legislación relacionados a privacidad, ciberseguridad, ruptura de algoritmos criptográficos, y vacíos regulatorios. La asociación más robusta se evidenció entre componentes éticos e interrupción del encriptamiento. Los resultados orientan la concentración de la discusión ética en ciberseguridad y protección de datos, con baja regulación normativa sobre el tema. Es necesario consiguientemente orientar investigaciones empíricas sobre riesgos emergentes.

PALABRAS CLAVE: Computación cuántica; ética; normas regulatorias; teoría cuántica; descripta-
miento; privacidad.

Quantum computing, ethical risks, and regulatory gaps. A mixed-methods analysis

ABSTRACT: Quantum computing (QC) promises transformations in various fields and raises ethical and regulatory challenges that need to be addressed. A mixed study was conducted, reviewing registered QC patents worldwide that reported emerging risks. In addition, 2,483 publications on the subject were reviewed in four databases. Nineteen academic disclosures met the search criteria. Of the 17,694 active CC patents, only 10% declared responsibilities. The articles were analyzed with Atlas ti v25, yielding six emerging codes related to potential risks, ethical components, and legislation. The concurrence of these codes indicated that CC posed greater risks than benefits and that ethical components should be considered for future regulations. The co-occurrence showed a

relationship between ethical components and encryption. The study concluded that there is a need to establish standards that minimize the ethical risks of CC use and ensure safety for humans and the environment.

KEY WORDS: Quantum computing; ethics; laws; quantum theory; decryption; privacy.

INTRODUCCIÓN

La computación cuántica (CC) es una tecnología con avance significativo en la última década y que cuenta con un potencial importante que promete la transformación en los campos de criptografía, la optimización computacional y procesamiento de datos complejos. A diferencia de la computación clásica, la CC utiliza los qubits^{1, 2} para ejecutar acciones como la superposición y entrelazamiento, con lo que amplía la capacidad para hacer cálculos de alta complejidad que abren nuevos espacios para los campos tecnocientíficos^{3, 4}. De esta manera, la CC es capaz de acelerar procesos de análisis, modelamiento de sistemas complejos en los que los sistemas tradicionales de informática tienen limitaciones.

Esta tecnología promete el avance en muchos campos del conocimiento. De esta forma la utilidad en el procesamiento de información para el desarrollo de nuevos materiales, simulaciones en estructuras químicas y biológicas, optimización de procesos industriales, modelización de riesgos en el área económica y financiera, predicción de escenarios, podrían aportar de manera significativa la toma de decisiones con un bajo margen de error⁵.

Sus beneficios potenciales se encuentran también en áreas como la energía, mejorando su eficiencia, la búsqueda de alternativas de uso sostenible de materiales, detección temprana de enfermedades en las plantas, mejora del cultivo y calidad de los alimentos, propuestas en el desarrollo de sistemas eficientes de atención en salud, industria farmacéutica entre algunos^{6, 7, 8}.

¹ Q. A. Memon, Al A. Mahmoud y M. Pecht, «Quantum Computing: Navigating the Future of Computation, Challenges, and Technological Breakthroughs», *Quantum Reports* 6, n.º 4 (2024): 627-630.

² V. Sood y R. P. Chauhan 2024. «Quantum computing: Impact on energy efficiency and sustainability», *Expert Systems with Applications* 255 (2024): 124401.

³ S. González Monserrate, «The Staggering Ecological Impacts of Computation and the Cloud», *The MIT Press Reader*, 2022. El autor realiza un informe sobre una investigación realizada por 5 años sobre los riesgos medioambientales del uso de la computación cuántica y los mecanismos de refrigeración utilizados.

⁴ E. Gonzáles, A. De La Pena, F. Cortés, D. Molano, B. Barón, N. Gualteros, J. Páez y C. Parra, «Robotic Theater: An Architecture for Competency Based Learning», *Advances in Intelligent Systems and Computing* (Berlín: Springer Verlag, 2019), 131-133.

⁵ *Ibid.*

⁶ Ch. D. Castillo Rosas, M. I. Díaz Tomás y A. C. Mendoza de los Santos, «El avance de la computación cuántica en la gestión de riesgos, una revisión sistemática», *Investigación y Ciencia Aplicada a la Ingeniería* 7, n.º 45 (2024): 23-24..

⁷ D. Silva y R. Núñez, «Exploración de las posibilidades de la computación cuántica para la criptografía», *CINTE* 1, n.º 2 (2023): 39 y 45.

⁸ R. Ur Rasool, H. F. Ahmad, W. Rafique, A. Qayyum, J. Qadir y Z. Anwar, «Quantum Computing for Healthcare: A Review», *Future Internet* 15, n.º 3 (2023): 3-8.

Sin embargo, estos potenciales beneficios también entrañan riesgos potenciales al medioambiente que no han sido declarados debidamente, al exponer de manera superficial la información sobre este tema y la presentación documental de datos relacionados exclusivamente a aspectos técnicos sobre la construcción de estos dispositivos tecnológicos. Es así, que existe, de manera aislada, información no explícita sobre cuáles serían los efectos sobre la salud humana y el medioambiente, así como sobre las regulaciones de su implementación, uso, manejo y residuos resultantes del deterioro de estas máquinas.

Una de las principales preocupaciones se relaciona al compromiso de los sistemas actuales de encriptación y seguridad informática sobre información sensible de los usuarios, ya que la CC presenta la probabilidad de vulneración de algoritmos criptográficos, por lo que la seguridad de confidencialidad institucional e informacional de los Estados podrían verse comprometidos^{9, 10}.

Este tema, ampliamente discutido en países desarrollados, ha expuesto igualmente las limitaciones de acceso a esta tecnología en países en vías de desarrollo, dejando espacios de vulnerabilidad de la información, así como el incremento en la brecha digital lo que empeoraría el marginamiento social y tecnológico^{11, 12}. De esta forma, la discusión de la CC no se limita a las capacidades operativas, sino que involucra el resguardo de derechos individuales, de autonomía, justicia y seguridad colectiva.

Con el fin de garantizar el ejercicio de los Derechos Humanos en la vida e individualidad de las personas y países, los Comités de Ética de la Investigación (CEI) deben ser partícipes activos en el planteamiento de procesos, procedimientos y normas de regulación ética claras para el uso de los avances tecnológicos, que incluyen de igual manera a los investigadores y desarrolladores en computación, asignándoles responsabilidades y sanciones en caso necesario. De ser así, los CEI, no tienen la tuición de ejecutar sanciones, por lo que las instituciones encargadas para ello deben organizar y delimitar leyes claras que penalicen acciones que conlleven los peligros antes mencionados.

La tecnología no puede ser preeminente en relación a los sentidos de vida y particularmente al actuar responsable de la comunidad de investigación y sus fuentes de financiación; ya lo mencionaba Hans Jonas desde 1991¹³ cuando formuló su

⁹ L. L. Enríquez Rodríguez y O. A. Mendoza Enríquez, *Desafíos del derecho a la protección de datos personales en la era digital. Una mirada desde América Latina* (Valencia: Tirant lo Blanch, 2024), 80-93.

¹⁰ O. E. Bernardi-Espín y M. A. Quimiz-Moreira, «Incidencia de la computación cuántica en los algoritmos criptográficos», *Código Científico Revista de Investigación* 5, n.º 1 (2024): 627-630 y 643.

¹¹ National Institute of Standards and Technology, Information Technology Laboratory, *Post-Quantum Cryptography* (Gaithersburg: NIST, 2024), 24-26. Revisión sistemática que pone de manifiesto los desafíos del uso de la CC en criptografía y el manejo de datos confidenciales, así como de la seguridad financiera.

¹² Rodríguez, A. 2024. Retos para la gobernanza de las tecnologías cuánticas en Europa. Los riesgos potenciales de la computación cuántica en el futuro inmediato y el riesgo en el desarrollo de este tipo de tecnologías que reciben grandes inversiones económicas de potencias mundiales.

¹³ Hans Jonas, filósofo alemán conocido por su obra *El principio de la responsabilidad*, donde realiza una crítica a la era de la tecnología y las consecuencias de esta sobre la humanidad, haciendo una reflexión moral sobre la creciente demanda y desarrollo de la tecnociencia y la responsabilidad del hombre sobre el medioambiente, y su deber con la protección de todos los seres vivos, pp. 195-203.

Principio de la Responsabilidad al hacer una crítica muy profunda de la ciencia moderna y del que llamó «su brazo armado: la tecnología» pidió a la comunidad reflexiva, promover el desarrollo de una ciencia consciente con una actuación con cautela y humildad frente al enorme y sobredimensionado poder de la tecnociencia. Desde entonces nos muestra la urgencia de mover la ética intersubjetiva que estaba ausente de la consideración externa a esa relación para redimensionar el alcance del actuar humano¹⁴.

Mientras se presentan beneficios potenciales de CC con mucho optimismo, las implicaciones éticas parecen ser abordadas de manera fragmentada, sobre todo en temas relacionados a la normatividad, regulación coordinada entre países, protección de derechos digitales y distribución equitativa de los beneficios, lo que limita la anticipación de riesgos emergentes.

La CC al desarrollarse principalmente en países con alta capacidad de inversión tecnológica y científica, la concentración del poder tecnológico rezaga el crecimiento de países con baja capacidad en tecnología y limitaciones económicas, lo que crearía una dependencia estructural manifiesta en regiones donde las normas específicas para su uso y aplicación no cuentan con normas específicas para el control social y jurídico¹⁵.

Con una mirada bioética la CC plantea la necesidad de reflexionar de manera profunda sobre las consecuencias futuras del poder tecnocientífico. Es así, que Hans Jonas, con el principio de responsabilidad, ofrece un marco pertinente para examinar tecnologías en fases emergentes, por las transformaciones en gran escala sobre la vida humana, los sistemas sociales y el entorno, al plantear la prudencia, anticipación y responsabilidad frente a innovaciones, que pueden tener consecuencias irreversibles.

Junto con los riesgos asociados a la seguridad de información y la privacidad individual y colectiva, así como a la desigualdad tecnológica, surgen interrogantes en dimensiones poco exploradas, como el consumo energético para el mantenimiento de infraestructuras cuánticas, el uso de materiales especializados para la fabricación de esta tecnología, la bioseguridad implicada en los procesos de desarrollo tecnológico y los efectos ambientales resultantes de su expansión.

Si bien estos temas no se analizan en la literatura especializada, su sola presencia resulta significativa y sugiere un punto de discusión de un dilema ético presente, por lo que es necesario evitar una fijación prematura de riesgos relacionada únicamente al plano criptográfico, existiendo impactos potenciales en la salud ocupacional, sostenibilidad ambiental y responsabilidad industrial.

En este escenario, también cobra importancia la participación de instancias de deliberación ética, académica e institucional que permitan acompañar críticamente el desarrollo de tecnologías emergentes. No se trata de frenar la innovación, sino de orientarla hacia marcos de responsabilidad, trazabilidad y protección de bienes fundamentales. La construcción de normas, políticas públicas y lineamientos éticos no puede quedar relegada a fases tardías del desarrollo tecnológico, cuando las

¹⁴ J. E. De Siqueira, «El Principio de Responsabilidad de Hans Jonas», *Acta Bioethica* 7, n.º 2 (2001): 277-285.

¹⁵ A. Auffèves, «Quantum Technologies Need a Quantum Energy Initiative», *PRX Quantum* 3, n.º 2 (2022): 020101-1-020101-12.

asimetrías de acceso, los vacíos regulatorios o los daños potenciales ya se encuentran consolidados. Por el contrario, la reflexión ética debe incorporarse desde las etapas tempranas del diseño, implementación y gobernanza de estas tecnologías, especialmente cuando sus efectos pueden proyectarse sobre la privacidad, la autonomía, la seguridad colectiva y el ambiente.

Pese a la relevancia creciente de esta discusión, la literatura sobre computación cuántica continúa dominada por enfoques técnicos, computacionales o experimentales, mientras que sus implicaciones éticas y normativas aparecen menos sistematizadas. En particular, persiste una insuficiente articulación entre el desarrollo de patentes, la expansión de aplicaciones tecnológicas y la producción académica que analiza críticamente sus riesgos, responsabilidades y vacíos regulatorios. Esta brecha hace necesario examinar no solo qué se está desarrollando en términos tecnológicos, sino también cómo se están representando los riesgos asociados a ese desarrollo y qué dimensiones permanecen subexploradas o invisibilizadas dentro del debate contemporáneo.

Por todo lo anterior, el presente estudio tuvo como objetivo analizar cómo las patentes activas entre 2019 a 2024 y la literatura académica reciente representan los riesgos éticos y los vacíos normativos asociados a la computación cuántica, con especial atención a la privacidad, la ciberseguridad, la protección de datos, la desigualdad de acceso y las referencias emergentes relativas a salud humana y medioambiente.

1. MATERIALES Y MÉTODOS

Se desarrolló una investigación mixta de tipo secuencial exploratorio con integración de procedimientos cualitativos y cuantitativos para analizar los riesgos éticos y normativos asociados a la CC. Este diseño se realizó con una aproximación documental e interpretativa de dos fuentes: las patentes relacionados con CC y publicaciones académicas especializadas. Posteriormente, se realizó la asociación de categorías emergentes identificadas.

La investigación se organizó en tres etapas complementarias:

- a. Primera etapa, revisión de patentes: se inició con la búsqueda de información documental, de patentes relacionadas al diseño o elaboración de computadoras cuánticas con el fin de identificar el volumen de registros, su distribución en áreas de desarrollo, su estado de actividad y presencia de menciones relacionadas con responsabilidad, seguridad y riesgos emergentes. Para ello se consultaron registros disponibles en LENS y WIPO, en el periodo comprendido entre enero de 2019 y diciembre de 2024.
- b. Segunda etapa, de análisis cualitativo de literatura académica, en el que se identificaron y analizaron diversas fuentes bibliográficas, siguiendo el método PRISMA, pero utilizando los siguientes criterios de búsqueda: artículos originales, reportes de caso, documentos normativos o informes técnicos completos en idioma inglés o español, de acceso abierto, publicados entre 2019 a 2024, en bases de Scopus, Google Scholar y PubMed, cuyo contenido

se refiera a riesgos éticos potenciales del uso de computadoras cuánticas, regulación, privacidad, seguridad y consideraciones normativas.

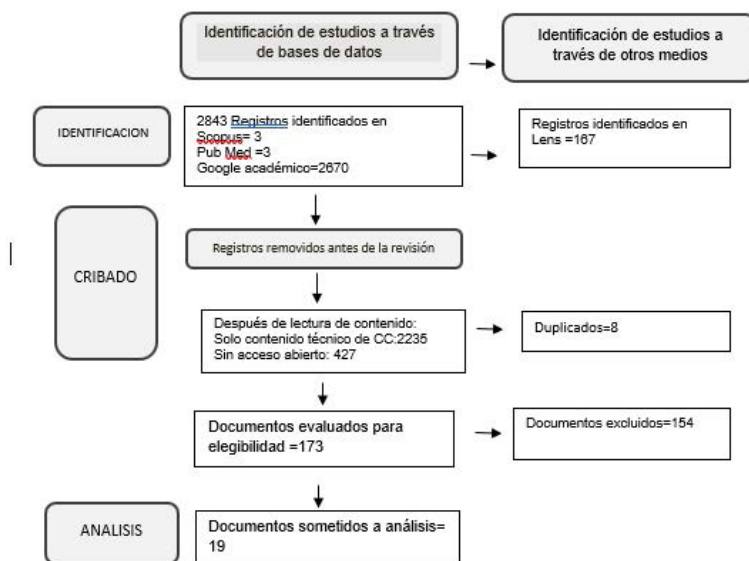
Esta revisión documental permitió conocer el estado del arte en el área y dio origen a categorías emergentes para hacer un primer análisis interpretativo. Los operadores claves de búsqueda fueron: [computación cuántica OR quantic computation] AND [[riesgos OR risk] OR [desventajas OR disadvantages] OR [impacto OR impact]] AND [[salud OR health]AND[privacidad OR privacy]AND[medioambiente OR environment]] encontrados en el título, resumen o texto de los documentos de revisión.

A partir de la revisión se identificaron las categorías orientadoras que fueron base para el análisis temático posterior y para la construcción del sistema de codificación axial abierta.

- c. Tercera etapa, análisis cualitativo y exploratorio cuantitativo: los documentos seleccionados fueron procesados en el software Atlas ti v25., organizándose en cuatro variables categóricas orientadoras o componentes, para realizar la matriz categorial, donde se encuentran: los cambios tecnológicos, ética, legislación y riesgos. Dentro de cada componente se identificaron expresiones recurrentes como: innovación tecnológica, dilemas éticos, brechas de datos sensibles, seguridad informática individual, ataque informático, interrupción del encriptamiento, dificultades generales, restricciones regulatorias, impacto en la seguridad global, vulnerabilidades en la explotación, imprevistos y bienestar social.

Figura 1

Diagrama de flujo de búsqueda sistemática de información



Fuente: elaboración propia, selección y cribado de documentos para análisis cualitativo.

La selección de documentos y depuración de duplicados se realizó mediante revisión manual asistida por gestor bibliográfico (Mendeley).

Los datos numéricos reportados en el análisis de coocurrencia, fueron organizados en el software SPSS v25, con el que se realizó un análisis de correspondencias con técnica exploratoria, para examinar la asociación entre componentes y categorías emergentes, así como la prueba de chi cuadrado de Pearson como estadístico de relación categorial y la reducción categorial consiguiente para el análisis de asociación e identificación de categorías prioritarias.

Por tratarse de un estudio documental basado en patentes y publicaciones académicas de acceso público no se requirió de aprobación por un Comité de Ética en Investigación.

2. RESULTADOS

Se encontraron 28494 solicitudes de patentes relacionadas con CC desde enero de 2019 a diciembre de 2024 de las cuales 22285 correspondían a EEUU, 3995 registradas en la Organización Mundial de Propiedad Intelectual (WIPO) y 2213 en Patentes Europeas. Del conjunto, 4835 tenían descargos de responsabilidad, concediéndose patentes a 18133 solicitudes, de las cuales 17694 se encuentran activas y 1686 fueron descontinuadas^{16, 17}.

Estos datos muestran un crecimiento sostenido en el desarrollo patentado en el área con presencia baja (10,85%) de menciones explícitas de responsabilidad (Tabla 1) o riesgos asociados a su uso (0, 60%) Figura 2.

Tabla 1

Patentes en Computación cuántica desde 2020 a 2025 y solicitantes anuales

Datos	Gráficos comparativos anuales	PATENTES EN COMPUTACION CUANTICA POR AÑO				
		2020	2021	2022	2023	2024
Patentes CC		6758	8256	8668	8989	10697
Patentes concedidas		2643	3049	5460	5336	3732
Descargo de responsabilidad			1137	1166	1063	1340
Solicitantes						
IBM		510	351	470	374	440
Intel		222	254	241	295	260
Google		209	139	163	157	188
Instituto Investig tecnológicas		175	139	110	103	
Microsoft		171	160	216	229	289
Pure				207	243	315
Huawei						410

Fuente: elaboración propia, elaborada de datos obtenidos en LENS y WIPO 2024.

¹⁶ LENS, «The Lens – Free & Open Patent and Scholarly Search», acceso el 24 de mayo de 2024.

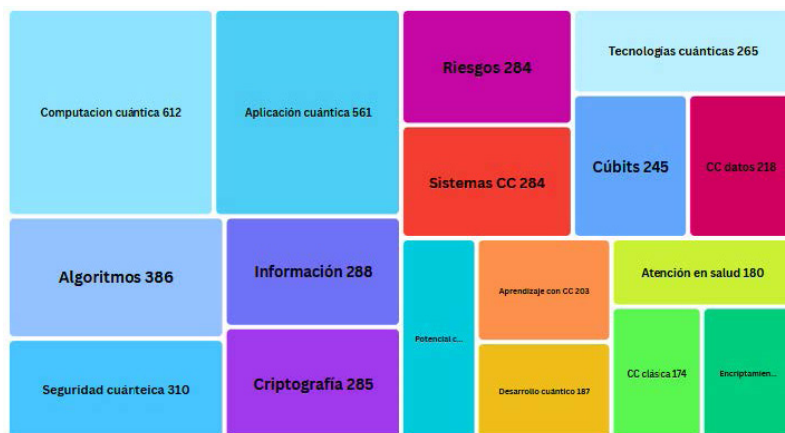
¹⁷ WIPO, «Search International and National Patent Collections», 2024.

Las patentes se concentraron principalmente en desarrollo computacional, destacándose aquellas que se refieren a seguridad e información y tratamiento de datos (Figura 2). Sobresalen solicitudes clasificadas bajo la categoría «computación cuántica» con 612 y «aplicación cuántica» con 561 peticiones respectivamente. Esta distribución confirma que el desarrollo tecnológico patentado privilegia componentes operativos y funcionales con énfasis en arquitectura computacional, procesamiento y protección de información.

Las publicaciones sobre CC, no tuvieron una frecuencia similar a la de las solicitudes de patentes en los últimos cinco años, existiendo 205 trabajos académicos, 97 de los cuales son trabajos científicos, sobre todo relacionados con procesadores y programación cuántica publicados en los periodos comprendidos en el estudio. Un trabajo hace mención a una patente y ninguno cuenta con citas académicas, encontrándose 19 publicaciones donde se exponen aspectos relacionados a riesgos o consideraciones éticas en su uso, que se limitan a exponer riesgos sobre protección de datos y ciberseguridad.

Del total cinco publicaciones fueron realizadas por el Consejo Superior de Investigaciones y el Centro Nacional de la Investigación, cuatro en el Instituto Nacional de Física Nuclear, tres en la Universidad de la Sorbona entre algunos centros de interés.

Figura 2
Número de solicitudes de patentes por área de desarrollo

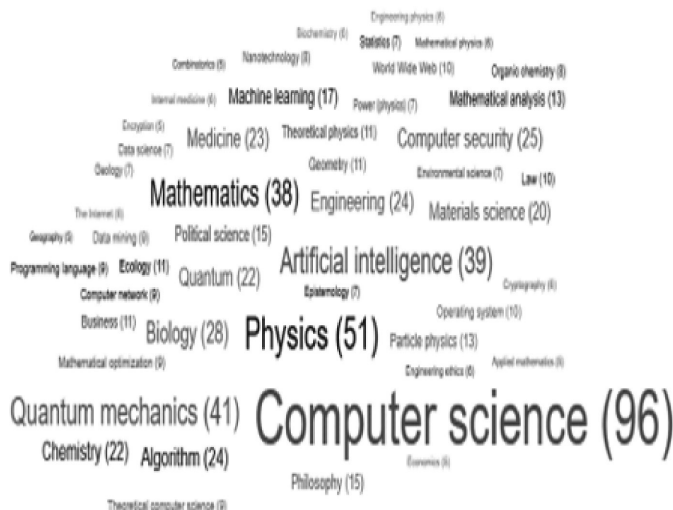


Fuente: elaboración propia basada en datos de LENS, 2024.

Las publicaciones sobre CC, no mostraron una frecuencia similar a la de las solicitudes de patentes en los últimos cinco años.

El análisis de frecuencia léxica de patentes y publicaciones mostró los términos recurrentes que se concentraron en ciencia computacional, física, mecánica cuántica, inteligencia artificial y matemática, observándose qué términos relacionados a ecología y filosofía fueron de mucha menor cuantía (Figura 3). Esta distribución sugiere que los aspectos técnicos de la CC predominan sobre un enfoque ético, social y ambiental.

Figura 3
Términos más frecuentes en documentos de patentes y publicaciones
sobre Computación Cuántica



Fuente: elaboración propia basada en datos de LENS.

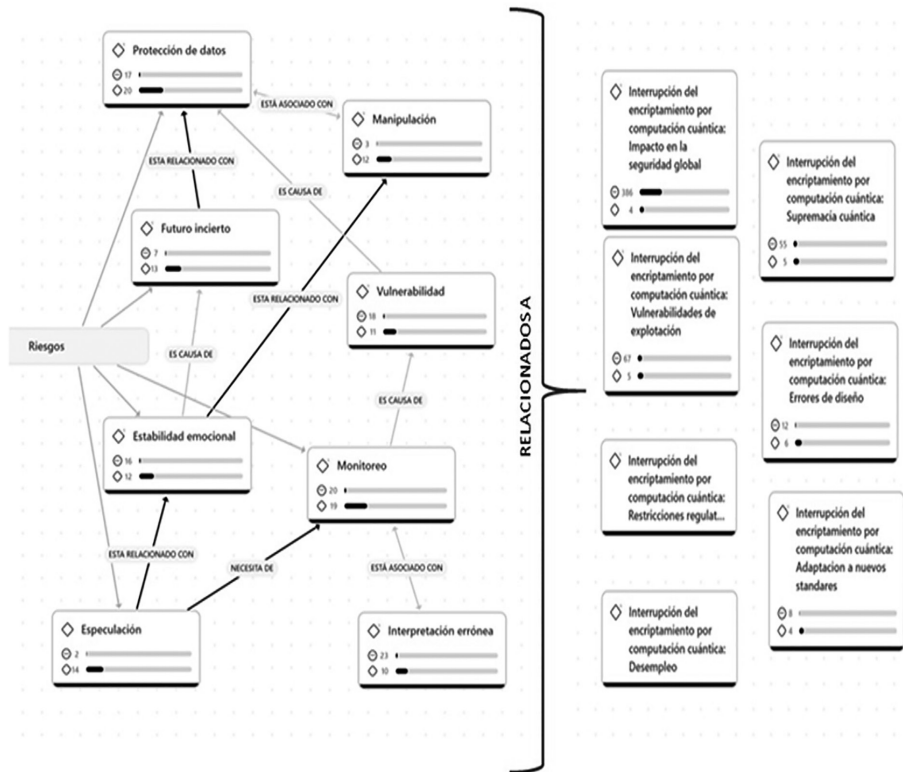
Los 19 documentos incluidos fueron analizados con Atlas ti v25, obteniéndose cuatro categorías orientadoras: cambios tecnológicos, componentes éticos, componentes de legislación, riesgos asociados a CC. Se obtuvieron 172 códigos que se sometieron a relaciones intercategoriales, a partir de la media de enraizamiento y densidad obtenidos del total de codificaciones, considerándose aquellos cuya media era igual o mayor a 22, lo que permitió delimitar un conjunto de categorías con relevancia analítica.

Dentro del componente cambios tecnológicos se identificaron seis códigos emergentes: análisis de datos, automatización, algoritmo criptográfico, colaboración científica, complejidad e innovación tecnológica. En el componente ético se reconocieron ocho códigos: bienestar social, ciberseguridad y privacidad, dilemas éticos, impacto económico, brecha digital y desigualdad, impacto social y desempleo, investigaciones éticas y conductas morales. En el componente de riesgos, se identificaron once códigos: interpretación errónea, brechas de datos sensibles, ruptura de algoritmos clásicos, cálculos rápidos y error, impacto en la seguridad global, restricciones regulatorias, supremacía cuántica, vulnerabilidad de explotación, limitaciones en monitoreo, riesgos imprevistos, riesgos generales. Finalmente, en el componente legislación se identificaron dos códigos: comunicación a la sociedad, políticas públicas. Estos hallazgos se muestran en la Figura 4.

El análisis de coocurrencia de las categorías orientadoras representado en el diagrama de Sankey mostró que, dentro del grupo de documentos, las menciones de riesgos y componentes éticos aparecieron con mayor densidad que las referencias

a beneficios sociales explícitamente problematizados (Figura 5). Este hallazgo no debe interpretarse como una medición objetiva del balance real entre riesgos y beneficios de la CC, sino como una característica del modo en que la literatura incluida representa y prioriza determinadas preocupaciones analíticas.

Figura 4
Red de la categoría riesgos



Fuente: elaboración propia.

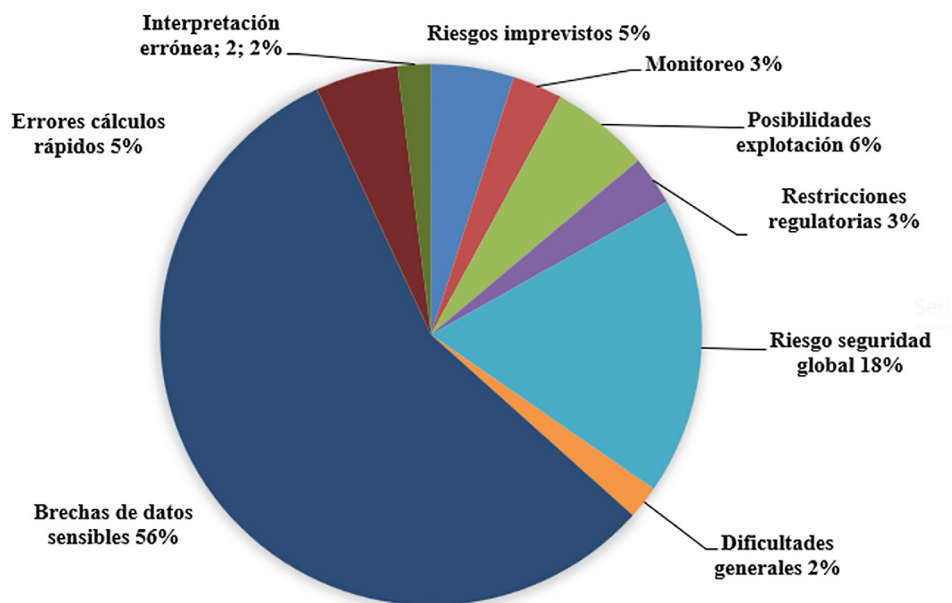
Figura 5
Diagrama de Sankey de coocurrencia de categorías orientadoras



Fuente: elaboración propia.

Los riesgos identificados con base en el enraizamiento y densidad observados en el gráfico 1, denotan que la CC abre brechas en datos sensibles, impacto en la seguridad global, vulnerabilidad de explotación e interrupción del encriptamiento. En contraste, los riesgos relativos a la salud humana o medio ambiente no alcanzaron presencia suficiente dentro de los documentos examinados, lo que sugiere que estas dimensiones no fueron suficientemente desarrolladas en la literatura revisada y deben ser entendidas en el presente estudio como vacíos de problematización más que como riesgos empíricamente establecidos.

Gráfico 1
Media de enraizamiento de los riesgos identificados de la CC
en la revisión de literatura



Fuente: elaboración propia.

Con los datos categoriales obtenidos, se realizó un análisis de coocurrencia, en el que se integraron 13 categorías con mayor sobresalencia porcentual, y cuatro componentes orientadores para el análisis de correspondencia cuantitativo en SPSS v25. La prueba de chi-cuadrado de Pearson mostró una relación estadísticamente significativa entre las necesidades categoriales identificadas y los componentes analíticos ($\chi^2=1561,523$; $q1=36$; $p=0,000$) como se presenta en la tabla 2. Este resultado indica que la distribución de las categorías no fue aleatoria dentro de los componentes definidos, sino que mostró patrones de agrupación relevantes para la interpretación documental.

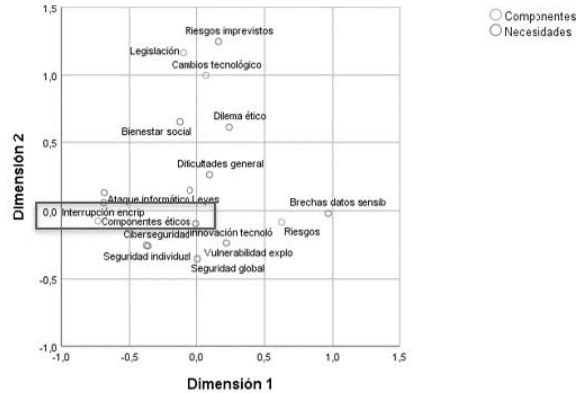
Tabla 2
Pruebas de chi-cuadrado de datos categoriales

	Valor	df	p
Chi-cuadrado de Pearson	1561,523a	36	0,000
Razón de verosimilitud	1669,170	36	0,000
Asociación lineal por lineal	281,165	1	0,000
N.º de casos válidos	8036		

Fuente: elaboración propia con datos de coocurrencia obtenidos de análisis con Atlas ti.

El análisis de correspondencias con normalización simétrica expuesta en el Gráfico 2, muestra una proximidad destacada entre el «componente ético» y la categoría «interrupción del encriptamiento». Al dicotomizar ambas variables se realizó una nueva prueba de chi-cuadrado, obteniéndose una asociación estadísticamente significativa ($\chi^2=691,047$; $q1=1$; $p=0,000$) lo que refuerza la consistencia interna de la esta relación (Tabla 3).

Gráfico 2
Simetría y normalización de necesidades y componentes CC



Fuente: elaboración propia datos de co-ocurrencia en SpSS.

Finalmente, la distribución porcentual mostró que la asociación entre componente ético e interrupción del encriptamiento fue de 46,9% del total de necesidades identificadas para este componente, frente al 19,5% observado en otros componentes. Este hallazgo sugiere que, dentro de la literatura incluida, la dimensión ética aparece estrechamente vinculada con la preocupación por la vulneración de sistemas de cifrado y exposición de datos sensibles, constituyéndose en el principal eje articulador de los riesgos relacionados a la CC (Tabla 4).

Tabla 3
Chi-cuadrado para Asociación entre componentes éticos e interrupción de encriptamiento

Pruebas de chi-cuadrado	Valor	df	Valor p	Significación exacta (bilateral)	Significación exacta (unilateral)
Chi-cuadrado de Pearson	691,047a	1	0,000		
Corrección de continuidad	689,769	1	0,000		
Razón de verosimilitud	692,058	1	0,000		
Prueba exacta de Fisher				0,000	0,000
Asociación lineal por lineal	690,961	1	0,000		
N.º de casos válidos	8036				

a. 0 casillas (0,0%) han esperado un recuento menor que 5. El recuento mínimo esperado es 1076,46.

b. Sólo se ha calculado para una tabla 2x2.

Fuente: elaboración propia con datos categóricos obtenidos de análisis con Atlas ti.

Tabla 4
Porcentaje de asociación entre componente ético en interrupción de encriptamiento, sobre otros componentes

		Componentes dicotomizados		Total
		Componente ético	Otros componentes	
Necesidades dicotomizadas	Interrupción de encriptamiento	1617	894	2511
		46,9%	19,5%	31,2%
Total	Otras necesidades	1828	3697	5525
		53,1%	80,5%	68,8%
		3445	4591	8036
		100,0%	100,0%	100,0%

Fuente: elaboración propia con datos categóricos obtenidos de análisis con Atlas ti.

3. DISCUSIÓN

Los hallazgos de este estudio no permiten cuantificar riesgos directos de la CC sobre la salud humana o el medioambiente, pero sí muestra diferencias en la producción de conocimiento, donde se enfatiza el desarrollo tecnológico con el registro progresivo de patentes orientados a seguridad en la criptografía, mientras que los impactos bioéticos y normas regulatorias sobre el uso de la CC son escasamente

documentados. En este sentido, el principal aporte del estudio no radica en demostrar daños ya consolidados, sino en mostrar que la discusión académica actual se concentra en algunos riesgos específicos relacionados con la privacidad, ciberseguridad e interrupción del encriptamiento, mientras las dimensiones de relevancia ética son todavía subexploradas.

La CC es una tecnología emergente que se incorpora de manera silente, pero constante en la vida cotidiana de las personas. Este instrumento informático, parece presentar múltiples ventajas vinculadas al manejo de grandes volúmenes de información, disminución en el tiempo del análisis de datos, sugiriendo al mismo tiempo la resolución de probables soluciones a problemas que actualmente impactan en nuestras vidas y nuestro entorno¹⁸. Memon, Mahmoud y Pecht describen a la CC como un avance tecnológico capaz de modificar de forma importante la computación contemporánea, mientras Sood y Chauhan destacan sus posibilidades en eficiencia, optimización y sostenibilidad tecnológica. En una línea similar, Ur Rassol et al. enfatizan el potencial de la CC en el sector de la salud y Castillo Rosas, Díaz Tomás y Mendoza de los Santos lo hace en relación a la modelización de riesgos y toma de decisiones complejas. El presente estudio no contradice dichas posturas, pero sí sugiere que existen problemas éticos y normativos que deben ser profundamente analizados, mucho más si se encuentran patentes activas sin descargos de responsabilidad y baja cantidad de publicaciones centradas en riesgos y regulación sobre su producción, aplicación y eliminación de residuos.

El predominio de patentes orientadas a la información, protección de datos y arquitectura computacional, confirma la expansión de la CC, centrando su atención en la tecnología y equipamiento, observación que acompaña lo señalado por Silva y Núñez y Bernardini-Espín y Quimiz Moreira, quienes consideran que la CC y la criptografía son los temas más visibles de preocupación. En la investigación realizada se encuentra una relación robusta entre el componente ético e interrupción del encriptamiento, visibilizando el problema ético en relación con sistemas de cifrado, exposición de datos sensibles y debilitamiento de la seguridad de la información. Este hallazgo es coherente con el énfasis regulatorio del NIST sobre criptografía postcuántica, que ha contribuido a instalar una agenda preventiva enfocada en la protección de información crítica.

Desde esta perspectiva, la discusión ética de la CC se encuentra enfocada a la privacidad y seguridad de datos, que está reforzada por los hallazgos de la investigación presentada, lo que orienta que el campo ético se configura principalmente en una ética de la información y seguridad más que en una ética integral con impacto social, laboral, ecológico y distributivo.

Ahora bien, el hecho de que los riesgos asociados a salud humana y medioambiental no hayan alcanzado presencia suficiente dentro del corpus analizado no debe interpretarse como ausencia de problema, sino como un vacío relevante de investigación. Este punto es especialmente importante para evitar una lectura reductiva de los hallazgos. En la introducción del manuscrito ya se advertía, con apoyo en autores como Auffèves, Taranto et al. y Sood y Chauhan, que el desarrollo de

¹⁸ Castillo Rosas, Ch. D., Díaz Tomás y Mendoza de los Santos, «El avance de la computación cuántica», 23-24.

tecnologías cuánticas plantea interrogantes sobre consumo energético, enfriamiento extremo, sostenibilidad de infraestructuras y responsabilidad material de los sistemas tecnológicos. A ello pueden añadirse trabajos como el de Billat y Doeran sobre impactos ambientales de ordenadores cuánticos superconductores, así como reflexiones más amplias sobre la huella ecológica de la computación contemporánea, como las de Gonzáles Monserrate. En este contexto, los hallazgos del presente estudio sugieren no que tales riesgos hayan sido descartados, sino que la literatura revisada todavía no los ha incorporado de manera sistemática dentro de sus discusiones éticas y normativas.

Este resultado tiene implicaciones importantes. Una agenda ética excesivamente centrada en criptografía y ciberseguridad corre el riesgo de invisibilizar otras dimensiones del problema, como la procedencia y manejo de materiales especializados, las condiciones de bioseguridad implicadas en ciertos procesos industriales, los costos energéticos de mantenimiento de sistemas cuánticos o las consecuencias ambientales derivadas de la expansión de infraestructuras de alta exigencia técnica. En este punto, la observación de Auffèves sobre la necesidad de una «iniciativa energética cuántica» resulta especialmente pertinente, ya que desplaza la discusión desde la fascinación por la potencia tecnológica hacia la responsabilidad de pensar las condiciones materiales que hacen posible dicha innovación. Del mismo modo, Sood y Chauhan permiten contrastar el discurso optimista sobre sostenibilidad con la necesidad de examinar empíricamente cuándo, cómo y bajo qué condiciones la CC podría realmente traducirse en eficiencia energética y no en nuevas formas de presión material y ecológica.

Otro aspecto que emerge con fuerza es la dimensión geopolítica y distributiva del problema. La concentración de patentes y desarrollos en contextos con alta capacidad de inversión sugiere que la CC podría profundizar asimetrías ya existentes en infraestructura tecnológica, soberanía digital y acceso al conocimiento especializado. Esta preocupación es consistente con lo planteado por Rodríguez sobre la gobernanza de tecnologías cuánticas en Europa, así como con la propia configuración del corpus revisado, donde la discusión normativa aparece concentrada en espacios institucionales o científicos de países con mayores capacidades de desarrollo. En este escenario, la brecha digital ya no debe entenderse únicamente como diferencia de acceso a tecnologías disponibles, sino también como desigualdad en la capacidad de anticipar, regular y beneficiarse de tecnologías emergentes. La ética de la CC, por tanto, no se restringe a la protección de datos, sino que involucra preguntas más amplias sobre justicia distributiva, dependencia tecnológica y concentración del poder informacional.

En este marco, el principio de responsabilidad de Hans Jonas adquiere especial relevancia interpretativa. Tal como recuerda De Siqueira, la propuesta de Jonas obliga a considerar las consecuencias futuras del actuar tecnocientífico y a incorporar prudencia frente a innovaciones cuyo alcance puede exceder la capacidad inmediata de control social y normativo. Aplicado al campo de la CC, este enfoque sugiere que la ausencia actual de evidencia empírica robusta sobre algunos riesgos no justifica la omisión ética o regulatoria, sino que exige atención anticipatoria. La responsabilidad, en este caso, no consiste en frenar el desarrollo tecnológico, sino en impedir que la gobernanza llegue tarde a procesos de innovación que ya están

consolidando capacidades de enorme impacto sobre privacidad, infraestructura crítica y distribución global del poder tecnológico.

Desde una mirada institucional, esto implica reconocer que los comités de ética, los espacios académicos de deliberación y los organismos de formulación de políticas públicas pueden desempeñar un papel importante en la construcción de criterios de evaluación temprana. No obstante, a la luz de los hallazgos del estudio, conviene precisar que su rol no debe entenderse como sustitución de marcos jurídicos o regulatorios formales, sino como instancia de orientación ética, problematización anticipatoria y vigilancia crítica. Los resultados sugieren que la baja presencia de contenidos normativos en la literatura y en el desarrollo patentado no solo refleja una carencia documental, sino también una débil institucionalización del debate ético en torno a la CC. Por ello, la incorporación temprana de lineamientos de responsabilidad, trazabilidad y evaluación de impactos podría contribuir a evitar que la regulación siga un curso meramente reactivo.

Asimismo, la asociación observada entre componente ético e interrupción del encriptamiento permite una lectura más precisa del núcleo problemático actual. No se trata simplemente de una preocupación técnica sobre seguridad informática, sino de un punto de convergencia entre autonomía, confidencialidad, vulnerabilidad de individuos e instituciones y posibilidad de daño colectivo. En otras palabras, el encriptamiento aparece en el corpus no solo como infraestructura técnica, sino como soporte material de derechos, resguardo económico y estabilidad política. Esta constatación explica por qué la ética de la CC, en su estado actual de desarrollo documental, se organiza en torno a la protección de información sensible. Sin embargo, precisamente por esa centralidad, el debate corre el riesgo de estrecharse si no incorpora de forma progresiva otros ámbitos, como sostenibilidad, impactos laborales, responsabilidad industrial y desigualdad de acceso.

En relación con las repercusiones sociales y laborales, los datos del presente estudio no permiten afirmar de manera concluyente que la CC producirá desplazamientos masivos de profesiones o efectos inmediatos sobre el empleo. Sin embargo, sí permiten señalar que la literatura revisada incorpora preocupaciones prospectivas sobre desigualdad, concentración de capacidades y posibles reconfiguraciones en sectores intensivos en procesamiento de información. Esta lectura resulta más consistente metodológicamente que formular escenarios deterministas, y se alinea mejor con el carácter exploratorio del estudio. Por ello, más que anticipar consecuencias definitivas, corresponde señalar la necesidad de investigar de manera empírica cómo la convergencia entre computación cuántica, inteligencia artificial y automatización avanzada podría alterar estructuras laborales, circuitos de decisión y regímenes de acceso al conocimiento en distintos contextos nacionales.

Finalmente, los resultados muestran que la literatura sobre CC sigue dominada por enfoques técnicos y por narrativas de innovación, mientras las discusiones bioéticas y normativas permanecen menos sistematizadas y con baja densidad documental. Esta constatación refuerza la pertinencia del objetivo del estudio y confirma que existe una brecha entre el desarrollo tecnocientífico acelerado y la elaboración de marcos interpretativos y regulatorios suficientes. En consecuencia, una discusión madura sobre CC debería avanzar desde la mera problematización de la ciberseguridad hacia un enfoque integral que articule privacidad, justicia

distributiva, sostenibilidad, responsabilidad institucional y evaluación anticipatoria de impactos. Lejos de oponerse al desarrollo científico, esta ampliación del debate permitiría acompañarlo críticamente y dotarlo de mayor legitimidad social, previsión normativa y consistencia ética.

La carencia de información sobre estos temas, principalmente aquellos relacionados con bioseguridad en el manejo de los materiales de construcción de las computadoras cuánticas y la información sobre el desecho de los productos resultantes por daño o caducidad, la seguridad medioambiental referida a la implementación de espacios que alberguen la CC, los cuales requieren temperaturas inconcebibles para la supervivencia de especies animales o vegetales, así como la forma de extractivismo de materiales para su fabricación o la forma de manipulación de residuos tecnológicos, debe ser ampliamente discutida con el fin de establecer normas y seguridad, tanto como la continuidad en el manejo de estas tecnologías emergentes a partir de la apertura de más espacios de ciudadanía y de reflexión ética (Comités de convivencia, Comités de ética, Comités de integridad científica).

La sociedad, que en este momento se ve impactada con los avances de la inteligencia artificial, no ha interiorizado aún la existencia de la CC como el siguiente paso del desarrollo digital, ni ha sido advertida o comunicada debidamente de los potenciales riesgos que este desarrollo tecnológico ofrece. La intención de este conocimiento, no es la de frenar el desarrollo, sino hacer del mismo una acción coherente, segura, respetuosa y accesible para todos, sin producir daño constante e irreversible al planeta y a los seres humanos.

Es comprensible entonces que las consideraciones éticas, sobre el diseño, manejo y aplicación de las CC, deben analizar cuestiones como la protección, solidaridad, justicia, la privacidad, la beneficencia y no maleficencia, para lograr avances científicos razonables y prudentes, enmarcados en la generación de acciones y acuerdos con el fin de establecer el cumplimiento de las escasas, pero vigentes normas sobre inteligencia artificial que previenen conductas inapropiadas en el uso de la CC.

La revisión de la literatura muestra la ausencia de estas consideraciones en la mayor parte de las publicaciones encontradas, que además corresponden a autores de países que no desarrollan CC, sin haber encontrado información orientadora sobre temas éticos o de políticas públicas que consideren una reglamentación clara para estas discusiones éticas emergentes.

La información disponible en las bases académicas advierten sobre las implicaciones en la ruptura criptográfica informática, poniendo en riesgo la seguridad individual, económica y financiera, incluyendo aquella sensible para los países y las personas, en la observancia de que algunos se verán favorecidos ante la ausencia de leyes o regulaciones locales o internacionales que limiten algunos aspectos de su manejo, para cometer actos indebidos. Estos vacíos legales, evidentes en varios países de América, deben ser resueltos por expertos en el área de políticas públicas, con la emisión de normas y leyes con el fin de evitar vulnerabilidades globales. Tómese en cuenta que, la información sobre aspectos de regulaciones específicas, limitaciones y riesgos no tiene la información suficiente para que se regule el uso de la CC y se eviten problemas éticos relacionados sobre todo a la salud y medioambiente.

Si la IA se observó como un riesgo en la continuidad laboral de algunas profesiones, la CC cerrará mayores espacios laborales, favoreciendo a las empresas económicamente poderosas para el manejo de información hasta hace poco clasificada o privada, marcándose con ello la supremacía cuántica, que aumentará las brechas de conocimiento y tecnología en las naciones con bajos índices de ingresos. El desempleo se hará más evidente y las consecuencias pueden ser nefastas. Si bien se darán espacios nuevos de conocimiento y de trabajo, la CC crea preocupaciones prospectivas de las profesiones que manejan información basada en datos, hablese de salud, economía, administración, educación, etc.

La investigación realizada muestra la escasez de información sobre temas álgidos relacionados a la protección de los individuos y del ecosistema y la ausencia de publicaciones referidas a estos temas relacionados con CC, evidenciando exploratoriamente que los componentes éticos deben ser considerados de manera importante en relación a variables de necesidad, y su asociación directa con el requerimiento de intervención en la interrupción del encriptamiento de datos.

CONCLUSIONES

Se concluye que la CC presenta grandes oportunidades en el manejo y análisis de datos, pero el estudio exploratorio realizado con la información de acceso sugiere que los riesgos regulatorios y éticos fueron más frecuentes que los beneficios sociales problematizados y requieren una urgente discusión ética sobre los principios básicos de respeto, igualdad, privacidad, justicia y consentimiento informado, ante la gran probabilidad de que esta tecnología pueda incurrir en el desciframiento de información de todo tipo, incluyendo datos sensibles y económicos, que ponen en riesgo la economía global y la seguridad individual.

Simultáneamente, la ausencia de estudios relacionados con el riesgo de uso de materiales especiales en la construcción de estas máquinas que afecten al ser humano o al ecosistema, así como la creciente disparidad tecnológica con países con economías bajas, debe llevar a realizar mayores investigaciones más allá de los daños ya demostrados, en búsqueda de riesgos emergentes y la construcción de marcos regulatorios proyectivos.

Consiguientemente, se propone que las políticas públicas de las naciones enfoquen su trabajo en la prevención oportuna, mediante el diseño de normas que regulen y limiten el uso, manipulación y desarrollo de tecnologías de este tipo, incluyendo la participación de los CEI como actores principales para la elaboración reglamentaria, previendo posibles intervenciones no regulables por el control humano.

REFERENCIAS BIBLIOGRÁFICAS

- Auffèves, Alexia. «Quantum Technologies Need a Quantum Energy Initiative». *PRX Quantum* 3, n.º 2 (2022): 020101-1-020101-12. <https://doi.org/10.1103/PRXQuantum.3.020101>.
- Bernardi-Espín, Oscar Eduardo y Mauricio Alexander Quimiz-Moreira. «Incidencia de la computación cuántica en los algoritmos criptográficos». *Código Científico Revista de Investigación* 5, n.º 1 (2024): 627-650. <https://doi.org/10.55813/gaea/ccri/v5/n1/401>.

- Billat, Arnaud y Doeran, Dimitri. «Environmental Impacts of a Superconducting Quantum Computer Based on a Life Cycle Assessment». Tesis de maestría. Universidad Católica de Lovaina, 2024. <https://thesis.dial.uclouvain.be/entities/masterthesis/f628a6f8-ab92-45f2-9198-8c5d464ab609>.
- Castillo Rosas, Charles Duck, Marcos Iván Díaz Tomás y Alberto Carlos Mendoza de los Santos. «El avance de la computación cuántica en la gestión de riesgos, una revisión sistemática». *Investigación y Ciencia Aplicada a la Ingeniería* 7, n.º 45 (2024): 22-27. <https://ojsincaing.com.mx/index.php/ediciones/article/view/358/536>.
- Canorea, Elena. «Quantum Computing: potencial y retos de futuro». *Plain Concepts*, 2024. <https://www.plainconcepts.com/es/quantum-computing-potencial-retos/>.
- Castro, Camilo. «Horizontes de innovación tecnológica en la industria de alimentos: datos sintéticos y computación cuántica para el futuro inmediato y a largo plazo». *Revista ION* 36, n.º 2 (2024): 101-107. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0120-100X2023000200101&lng=en&nrm=iso.
- Computer Security Division, Information Technology Laboratory. Post-Quantum Cryptography | CSRC | CSRC. CSRC | NIST. Gaithersburg: NIST, 2024. <https://csrc.nist.gov/Projects/post-quantum-cryptography>.
- De Siqueira, José Eduardo. «El Principio de Responsabilidad de Hans Jonas». *Acta Bioethica* 7, n.º 2 (2001): 277-285. <https://doi.org/10.4067/S1726-569X2001000200009>.
- Enríquez Rodríguez, Laura Lizette y Olivia Andrea Mendoza Enríquez. *Desafíos del derecho a la protección de datos personales en la era digital. Una mirada desde América Latina*. Valencia: Tirant lo Blanch, 2024. https://infocdmx.org.mx/images/biblioteca/2024/DesafiosDerecho-PDP_EraDigital.pdf.
- Garay, Jorge. «La computadora cuántica de Google acaba de ser humillada por una red de ordenadores convencionales chinos». *WIRED*, 2024. <https://es.wired.com/articulos/computadora-cuantica-de-google-humillada-por-ordenadores-convencionales>.
- González, Enrique, Andrés De La Peña, Felipe Cortés, Diego Molano, Benjamín Barón, Nicolás Gualteros, John Páez y Carlos Parra. «Robotic Theater: An Architecture for Competency Based Learning». *Advances in Intelligent Systems and Computing*. Berlín: Springer Verlag, 2019: 126-137. https://doi.org/10.1007/978-3-030-26945-6_12.
- González Monserrate, Steven. «The Staggering Ecological Impacts of Computation and the Cloud». *The MIT Press Reader*, 2022. <https://bit.ly/3ZRRY0S>.
- Gwenzi, Willis, Lynda Mangori, Concilia Danha, Nhamo Chaulkura, Nothando Dunjana y Edmond Sanganyado. «Sources, behaviour, and environmental and human health risks of high-technology rare earth elements as emerging contaminants». *Science of The Total Environment* 636 (2018): 299-313. <https://doi.org/10.1016/j.scitotenv.2018.04.235>.
- Hochberg, Eric J. y Michelle M. Gierach. «Missing the reef for the corals: Unexpected trends between coral reef condition and the environment at the ecosystem scale». *Frontiers in Marine Science* 8 (2021): 1-10. <https://doi.org/10.3389/fmars.2021.727038>.
- Jonas, Hans. *El principio de responsabilidad*. Herder, 2014. <https://etica.uazuay.edu.ec/sites/etica.uazuay.edu.ec/files/public/uazuay-etica-principio-de-la-responsabilidad-hans-jonas.pdf>.
- Larramendi Benítez, Elsa María, Gabriela Millán Verdecia y Mario Antonio Plana Castell. «Escasez y contaminación del agua, realidades del siglo XXI». 60, n.º 259 (2021): e854, 1-7. <https://www.medigraphic.com/pdfs/abril/abr-2021/abr21279n.pdf>.
- LENS. «The Lens – Free & Open Patent and Scholarly Search». Acceso el 24 de mayo de 2024. <https://www.lens.org/lens>.
- López, Juan Carlos. «Hay al menos una razón por la que merece la pena volver a la Luna: recoger su abundante helio-3 y usarlo en la fusión nuclear». *Xataka*, 2019. <https://www.xataka.com/investigacion/hay-al-razon-que-merece-pena-volver-a-luna-recoger-su-abundante-helio-3-usarlo-fusion-nuclear>.

- Ma, Shunrong y Guilin Han. «Rare earth elements reveal the human health and environmental concerns in the largest tributary of the Mekong River, Northeastern Thailand». *Environmental Research* 252, n.º 3 (2024): 118968. <https://doi.org/10.1016/j.envres.2024.118968>.
- Márquez, Javier. «IBM ha construido el refrigerador de dilución más grande del mundo. Su misión: enfriar ordenadores cuánticos». *Xataka*, 2022. <https://www.xataka.com/investigacion/ibm-ha-construido-refrigerador-dilucion-grande-mundo-su-mision-enfriar-ordenadores-cuanticos>.
- Maturana Romesín, Humberto y Bernhard Pörksen. «Autopoiesis de lo vivo». En *Del ser al hacer. Los orígenes de la biología del conocer*, editado por J. C. Sáez, 51-56. Santiago de Chile: Comunicación Noreste, 2010. <https://bit.ly/3WCOVYS>.
- Meier, Florian y Hayata Yamasaki. «Energy-Consumption Advantage of Quantum Computation». *arXiv*, 2025. <https://doi.org/10.48550/arXiv.2305.11212>.
- Memon, Qurban A., Al Ahmad Mahmoud y Michael Pecht. «Quantum Computing: Navigating the Future of Computation, Challenges, and Technological Breakthroughs». *Quantum Reports* 6, n.º 4 (2024): 627-663. <https://doi.org/10.3390/quantum6040039>.
- Naciones Unidas. *Pacto internacional de Derechos Civiles y Políticos*. Nueva York: OHCHR, 1996. <https://www.ohchr.org/es/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>.
- Naciones Unidas. *Resolución aprobada por el Consejo de Derechos Humanos el 26 de septiembre de 2019*. 2019. <https://docs.un.org/es/A/HRC/RES/42/15>.
- Rodríguez, Andrea. «Retos para la gobernanza de las tecnologías cuánticas en Europa». *IDEES*, 2024. <https://revistaidees.cat/es/reptes-per-a-la-governanca-de-les-tecnologies-quantiques-a-europa/>.
- Rodríguez Heredia, Dunia. «Intoxicación ocupacional por metales pesados». *MEDISAN* 21, n.º 12 (2017): 7003-7016. <https://medisan.sld.cu/index.php/san/article/view/1089>.
- Rosales Rodríguez, Amán. «El determinismo tecnológico y la "dialéctica de la historia"». *Crítica: Revista Hispanoamericana de Filosofía* 34, n.º 100 (2002): 3-31. <https://doi.org/10.22201/iifs.18704905e.2002.953>.
- Silva, Davide y Rosa Núñez. «Exploración de las posibilidades de la computación cuántica para la criptografía». *CINTE* 1, n.º 2 (2023): 35-53. <https://cienciainteligente.com/index.php/CIN/article/view/16/16>.
- Singh, Ankit. «The Role of Quantum Technology in Sustainable Development». *AZOQuantum*, 2024. <https://www.azoquantum.com/Article.aspx?ArticleID=556>.
- Sood, Vaishali y Rishi Paul Chauhan. «Quantum computing: Impact on energy efficiency and sustainability». *Expert Systems with Applications* 255 (2024): 124401. <https://doi.org/10.1016/j.eswa.2024.124401>.
- Tan, Jia, Jiabin Li, Bojun Cao, Junxiang Wu, Dinghao Luo, Zhaoyang Ran, Liang Deng, Xiaoping Li, Wembo Jiang, Kai Xio, Lei Wang y Yongqiang Hao. «Niobium promotes fracture healing in rats by regulating the PI3K-Akt signalling pathway: An in vivo and in vitro study». *Journal of Orthopaedic Translation* 37 (2022): 113-125. <https://doi.org/10.1016/j.jot.2022.08.007>.
- Taranto, Philip, Faraj Bakhshinezhad, Andreas Bluhm, Ralph Silva, Nicolai Friis, Maximilian P. E. Lock, Giuseppe Vitagliano, Felix C. Binder, Tiago Debarba, Emanuel Schwarzhans, Fabien Clivaz y Marcus Huber. «Landauer Versus Nernst: What is the True Cost of Cooling a Quantum System?». *PRX Quantum* 4 (2023): 1-61. <https://doi.org/10.1103/PRXQuantum.4.010332>.
- UN Water. «Progresos en la calidad de las aguas ambientales. Novedades sobre el indicador mundial 6.3.2 y necesidades de aceleración. Resumen ejecutivo 2021». Naciones Unidas, 2021. <https://bit.ly/4gr3d68>.
- Ur Rasool, Raihan, Hafiz Farooq Ahmad, Wajid Rafique, Adnan Qayyum, Junaid Qadir y Zahid Anwar. «Quantum Computing for Healthcare: A Review». *Future Internet* 15, n.º 3 (2023): 1-36. <https://doi.org/10.3390/fi15030094>.

WIPO. «Search International and National Patent Collections». 2024. https://patentscope.wipo.int/search/en/result.jsf?_vid=P10-M5OFUE-75240.

Wood, Georgia. «Seguridad de cifrado para un mundo postcuántico». *CSIS Strategic Technologies Blog*, 2022. <https://www.csis.org/blogs/strategic-technologies-blog/encryption-security-post-quantum-world>.

Docente investigador emérito
Universidad Mayor de San Andrés. La Paz- Bolivia
gibustamante@umsa.bo
dra.gbustamante@gmail.com
<https://orcid.org/0000-0002-2275-4386>

GLADYS-INÉS BUSTAMANTE-CABRERA

Docente investigador en Investigación Clínica
Universidad de Chile. Santiago de Chile
carmenaliciacardozo@unal.edu.co
carmen_aliciademartinez@yahoo.co.uk
<https://orcid.org/0000-0001-8705-8958>

CARMEN-ALICIA, CARDOZO DE MARTÍNEZ

Profesor investigador
Universidad Autónoma de Guadalajara. Guadalajara-México
zzuviria@edu.uag.mx
<https://orcid.org/0000-0001-9127-7432>

ZAIRA-RUTH ZUVIRÍA-LÓPEZ

Investigador asociado al CIIDE (Centro Internacional de Investigación para el Desarrollo de la Educación) Corporación Universitaria Minuto de Dios-UNIMINUTO
Rectoría Bogotá y la Facultad de Educación de la Universidad de Missouri-Columbia
bbaron@uniminuto.edu
benjaminbv@gmail.com
<https://orcid.org/0000-0002-4968-6336>

BENJAMÍN BARÓN-VELANDIA

[Artículo aprobado para publicación en diciembre de 2025]