Newsletter trimestral

CÁTEDRA

# iDANAE

INTELIGENCIA · DATOS · ANÁLISIS · ESTRATEGIA

## 3T25

# Computación cuántica: perspectivas estratégicas para los responsables de la toma de decisiones

POLITÉCNICA

UNIVERSIDAD POLITÉCNICA DE MADRID

Management Solutions
Making things happen

# Introducción a la computación cuántica

Entre las tecnologías emergentes, la computación cuántica (en inglés, *quantum computing*) destaca por las nuevas posibilidades que abre para abordar problemas complejos. Aunque todavía se encuentra en una fase inicial de desarrollo, su potencial para transformar sectores enteros es enorme, desde la optimización de la cadena de suministro hasta el diseño de nuevos fármacos, pasando por las comunicaciones seguras y la inteligencia artificial (IA).

Aunque aún no está madura para su uso generalizado en las empresas, la computación cuántica ya está marcando las tendencias en la innovación tecnológica. Al igual que la inteligencia artificial hace una década, sus primeros avances están generando un gran interés en todos los sectores. Por lo tanto, es esencial comprender tanto sus capacidades como sus limitaciones para anticipar su papel en el futuro.

En sus fundamentos, la computación cuántica se basa en los *qubits*[1], que difieren fundamentalmente de los bits clásicos. Los *qubits* aprovechan fenómenos físicos como la superposición[2] y el entrelazamiento[3], y se manipulan a través de puertas cuánticas[4] para la realización de operaciones. Estos mecanismos permiten procesar la información de formas que los ordenadores clásicos no pueden, lo que abre la puerta a resolver cálculos de optimización, simulación de sistemas y análisis de datos a una velocidad sin precedentes.

En combinación con arquitecturas especializadas, estos principios permiten a los ordenadores cuánticos abordar problemas de complejidad exponencial, como la factorización de números grandes o la simulación de sistemas moleculares. El algoritmo de Shor[5], por ejemplo, ilustra el impacto potencial en la criptografía al amenazar el cifrado basado en RSA[6], lo que subraya la urgencia de diseñar métodos resistentes a la computación cuántica. [1]

Desde una perspectiva empresarial, las implicaciones son significativas. En el ámbito financiero, la computación cuántica promete avances en la optimización de carteras y el análisis de riesgos. En el sector farmacéutico, acelera el descubrimiento de fármacos mediante simulaciones moleculares. En el ámbito energético, apoya la optimización dinámica de los sistemas de red y la asignación de recursos. [2]

Para preparar a las empresas y los negocios, los líderes deben evaluar la exposición de su sector a la disrupción cuántica y su nivel de preparación para la adopción. La previsión estratégica es clave: alinear la exploración con los objetivos empresariales, invertir en talento y colaborar con startups o socios de investigación proporciona una vía pragmática para la experimentación temprana. [3]

La computación cuántica ya no es una posibilidad lejana, sino una capacidad emergente que exige una atención informada. En una economía digital cada vez más compleja es fundamental que las organizaciones que desean seguir siendo competitivas comprendan tanto la mecánica de la computación cuántica como su potencial estratégico. [4]

[1] Un qubit (bit cuántico) es la unidad básica de información en la computación cuántica. A diferencia de los bits clásicos, que solo pueden tener dos estados (0 ó 1), los *qubits* pueden existir en una combinación de estados debido a la superposición. También pueden vincularse a través del entrelazamiento, lo que permite realizar cálculos más complejos y potentes.

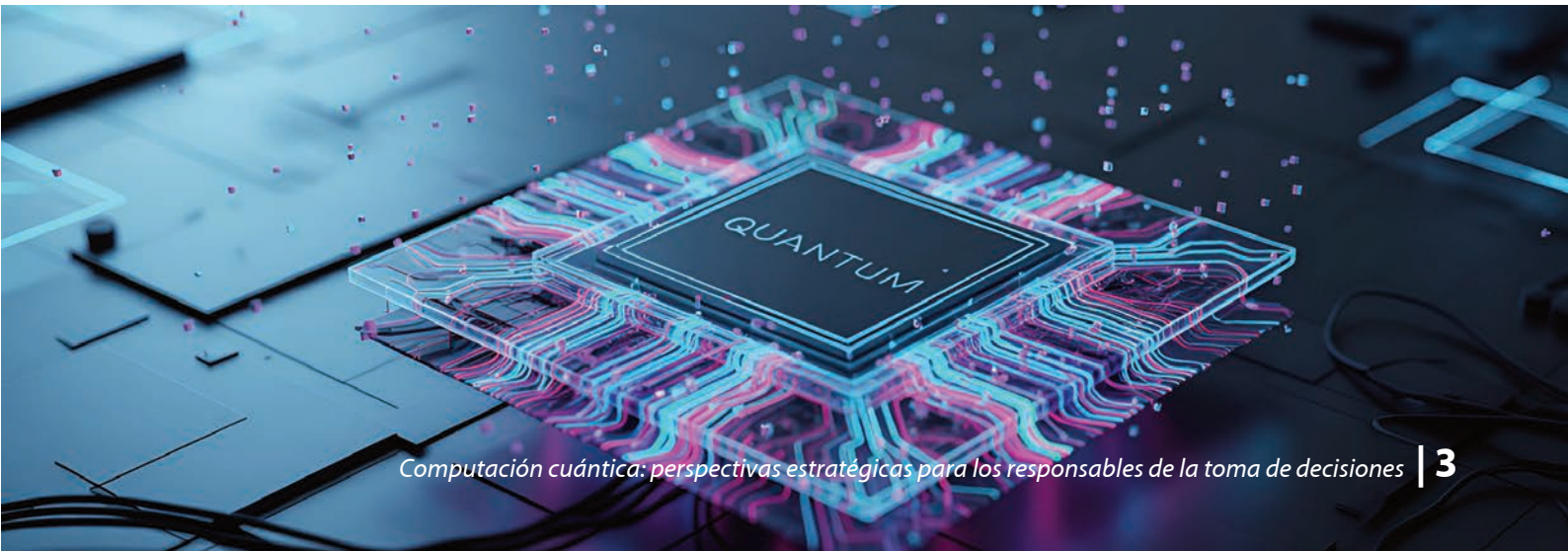
[2] Superposición: un qubit puede existir en una combinación de estados 0 y 1 simultáneamente, a diferencia de un bit clásico, que solo puede estar en el estado 0 ó 1 al mismo tiempo. Esto permite a los ordenadores cuánticos procesar múltiples posibilidades a la vez.

[3] Entrelazamiento: fenómeno cuántico en el que dos o más *qubits* se vinculan de manera que el estado de uno afecta instantáneamente al estado del otro, independientemente de la distancia que los separe. Esto permite fuertes correlaciones que se utilizan en la computación y la comunicación cuánticas.

[4] Puertas cuánticas: operaciones que cambian el estado de los *qubits*, de forma similar a como las puertas lógicas clásicas manipulan los bits. Realizan transformaciones reversibles en los *qubits*, lo que permite el cálculo cuántico mediante la superposición y el entrelazamiento.

[5] Algoritmo de Shor: algoritmo cuántico diseñado para factorizar de manera eficiente números grandes en primos. A diferencia de la factorización clásica, que es lenta para números muy grandes, el algoritmo de Shor puede resolverlo en tiempo polinomial, lo que supone una amenaza para la criptografía clásica como RSA.

[6] Cifrado basado en RSA: método de criptografía de clave pública ampliamente utilizado que protege los datos basándose en la dificultad de factorizar números grandes. Su seguridad depende del hecho de que, con los ordenadores clásicos, factorizar el gran producto de dos números primos es computacionalmente difícil.



# Problemas que la computación cuántica pretende resolver

La computación cuántica está emergiendo como una herramienta transformadora en todos los sectores, abriendo nuevos enfoques para la optimización, la criptografía y el aprendizaje automático. [1]

La optimización es fundamental en sectores como la logística, las finanzas y la energía, donde el objetivo es identificar el mejor resultado entre innumerables variables. Los algoritmos cuánticos, como el algoritmo de optimización cuántica aproximada (quantum approximate optimization algorithm, o QAOA)[7], pueden evaluar muchas soluciones potenciales de forma más eficiente, lo que reduce los costes y el tiempo. Las aplicaciones van desde la optimización de las cadenas de suministro y las rutas de tráfico hasta la integración de las energías renovables. [5]

La criptografía, base de las comunicaciones digitales seguras, está a punto de sufrir una disrupción. Los ordenadores cuánticos amenazan los sistemas clásicos de clave pública, pero también introducen alternativas cuánticas seguras, como el cifrado basado en redes[8] y la distribución cuántica de claves[9] (quantum key distribution, o QKD), que aprovechan la incertidumbre cuántica para proporcionar comunicaciones teóricamente seguras. [1]

En el aprendizaje automático, los métodos mejorados por la computación cuántica aceleran ciertos cuellos de botella computacionales, como el procesamiento de datos de alta dimensión. Los modelos asistidos por la computación cuántica podrían permitir una detección más eficiente del fraude, conocimientos personalizados sobre la atención sanitaria y modelos de riesgo financiero. [2]

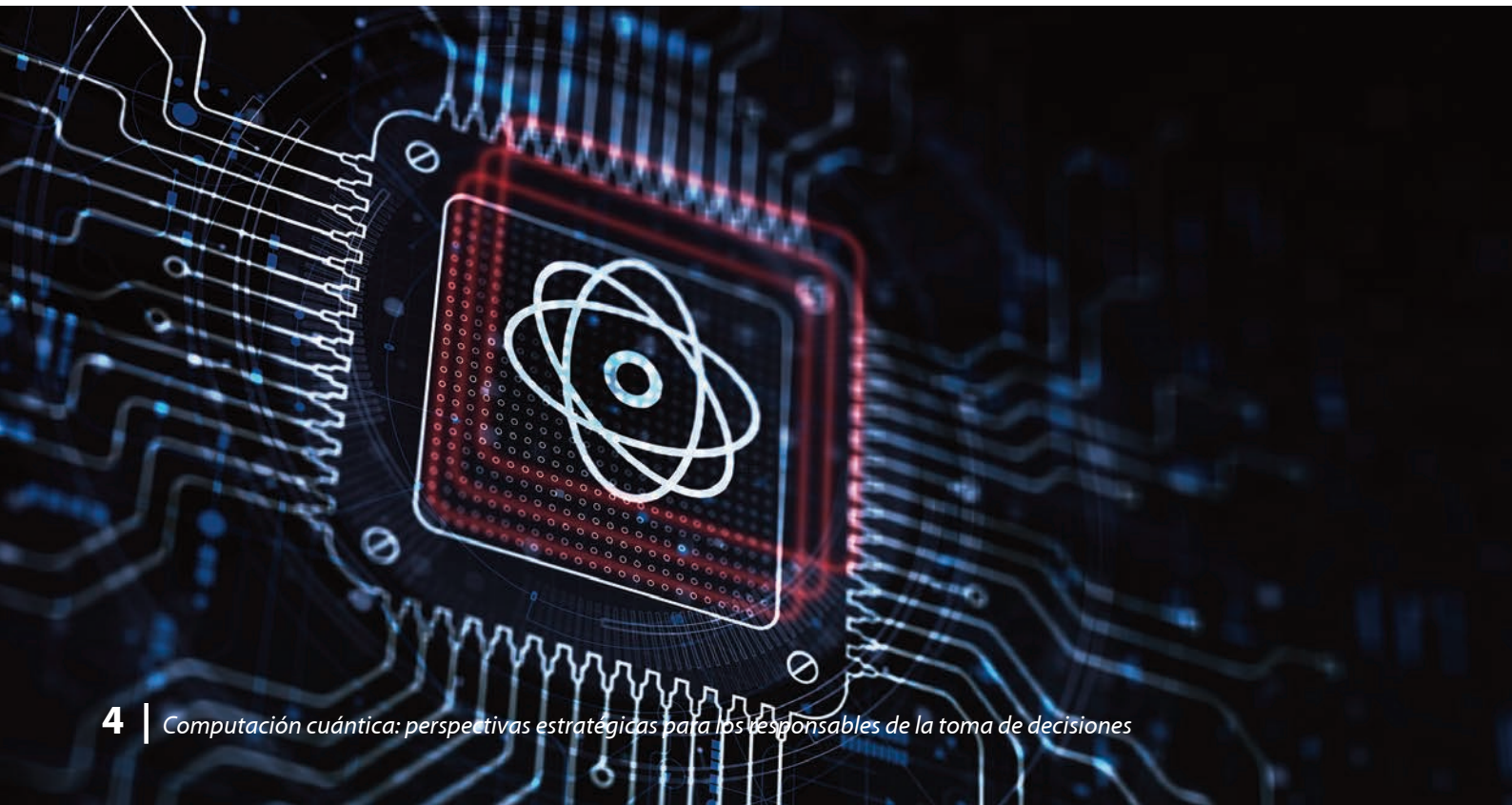
Estos avances no son meramente teóricos. Los proyectos piloto en el sector bancario están aplicando la computación cuántica al reequilibrio de carteras y a las simulaciones de riesgos; los consorcios farmacéuticos la están aprovechando para modelar el plegamiento de proteínas; y los proveedores de energía están probando optimizaciones basadas en la computación cuántica para la gestión de la red eléctrica. [6]

La computación cuántica no solo mejora los procesos existentes, sino que también transforma la propia toma de decisiones al permitir la modelización probabilística y la simulación de escenarios escalables. A medida que la tecnología madure, su papel en la planificación estratégica y la transformación operativa no hará más que profundizarse. [2]

[7] QAOA: algoritmo cuántico diseñado para encontrar soluciones aproximadas a problemas de optimización combinatoria.

[8] Cifrado basado en redes: un tipo de criptografía poscuántica que protege los datos utilizando estructuras matemáticas llamadas redes. Se considera resistente a los ataques de los ordenadores cuánticos.

[9] Distribución de claves cuánticas: método para compartir de forma segura claves de cifrado utilizando la mecánica cuántica. Aprovecha principios como la superposición y el entrelazamiento para detectar cualquier intento de espionaje: si un tercero intenta interceptar la clave, los estados cuánticos se alteran, revelando la intrusión.



# Retos a los que se enfrenta la computación cuántica

La computación cuántica se enfrenta a una serie de grandes obstáculos. Estos retos, que abarcan la fiabilidad técnica, la viabilidad económica y la preparación del ecosistema, deben abordarse antes de que la tecnología pueda tener un impacto real. [7]

## Fragilidad técnica: abordar los errores y la escalabilidad

Los sistemas cuánticos se basan en fenómenos únicos como la superposición y el entrelazamiento, que les permiten procesar múltiples posibilidades simultáneamente. Sin embargo, estas mismas propiedades también hacen que los sistemas cuánticos sean increíblemente sensibles a su entorno. [8]

Uno de los obstáculos más importantes es la alta tasa de error en las operaciones cuánticas. Los *qubits* son propensos a la decoherencia, lo que significa que pueden perder rápidamente su estado cuántico cuando se exponen a interferencias externas. Esta fragilidad dificulta la realización de cálculos largos y fiables. [8]

La escalabilidad es otro reto fundamental. La mayoría de los ordenadores cuánticos actuales contienen relativamente pocos *qubits*, lo que limita su capacidad computacional. A medida que los sistemas crecen, resulta cada vez más difícil gestionar las interacciones entre *qubits* y controlar las puertas cuánticas con la precisión necesaria para realizar cálculos exactos. La ampliación requerirá innovaciones en materiales, sistemas de control y corrección de errores. [9]

## Altos costes y retorno de la inversión incierto

El desarrollo y el funcionamiento del hardware cuántico es una tarea que requiere una gran inversión de capital. Ejemplos como la construcción de infraestructuras criogénicas, el aislamiento de los sistemas del ruido ambiental y la contratación de personal especializado conllevan costes considerables. Para muchas organizaciones, la justificación económica de la inversión en computación cuántica sigue sin estar clara. [10]

Además, el retorno de la inversión sigue siendo difícil de cuantificar. Si bien la computación cuántica promete beneficios a largo plazo en áreas como la optimización y la simulación, el plazo para obtenerlos es incierto. Las empresas deben sopesar los costes a corto plazo frente al potencial de resultados transformadores, a menudo sin tener muy claro cuándo se materializarán dichos resultados.

También existe una creciente preocupación en torno a la preparación de personal cualificado. El talento en computación cuántica es limitado, y la formación de nuevos expertos requiere tiempo. Para que las empresas se beneficien de la computación cuántica, necesitan tanto las herramientas como las personas capaces de utilizarlas de forma eficaz. [10]

## Retos en el ecosistema: regulación, ética y normas

Más allá del laboratorio, la computación cuántica opera dentro de un ecosistema tecnológico y social más amplio. El panorama normativo de las tecnologías cuánticas sigue estando poco desarrollado. Los reguladores apenas están empezando a abordar cómo regular un campo que combina la física fundamental con la infraestructura digital. [11]

Las cuestiones éticas también están cobrando importancia. La computación cuántica tiene el potencial de romper muchos de los sistemas de cifrado actuales, lo que supone un riesgo para la privacidad de los datos y la ciberseguridad. Las organizaciones deben empezar a prepararse para un futuro en el que las protecciones criptográficas actuales puedan dejar de ser suficientes. [8]

La estandarización supone otro obstáculo. Sin unos parámetros técnicos y unos protocolos de interoperabilidad comunes, el sector corre el riesgo de fragmentarse. La creación de un lenguaje y un marco comunes para las tecnologías cuánticas será esencial para la colaboración global y la viabilidad comercial. [11]

# Cronología de la computación cuántica

La computación cuántica está evolucionando rápidamente, pero el ritmo de su impacto en el mundo real en todos los sectores sigue siendo incierto. En medicina, las tecnologías cuánticas ya están abriendo nuevos horizontes: los sensores cuánticos permiten la detección ultraprecisa de biomarcadores de enfermedades, mientras que los ordenadores cuánticos aceleran el análisis de vastos conjuntos de datos sanitarios y optimizan el modelado molecular para el desarrollo de fármacos y los ensayos clínicos. Se espera que la integración de herramientas cuánticas en áreas como el diagnóstico precoz, los tratamientos personalizados y el intercambio seguro de datos revolucione los modelos de atención sanitaria en la próxima década, pero su adopción satisfactoria dependerá de la superación de las barreras técnicas y la adquisición de experiencia clínica. [12]

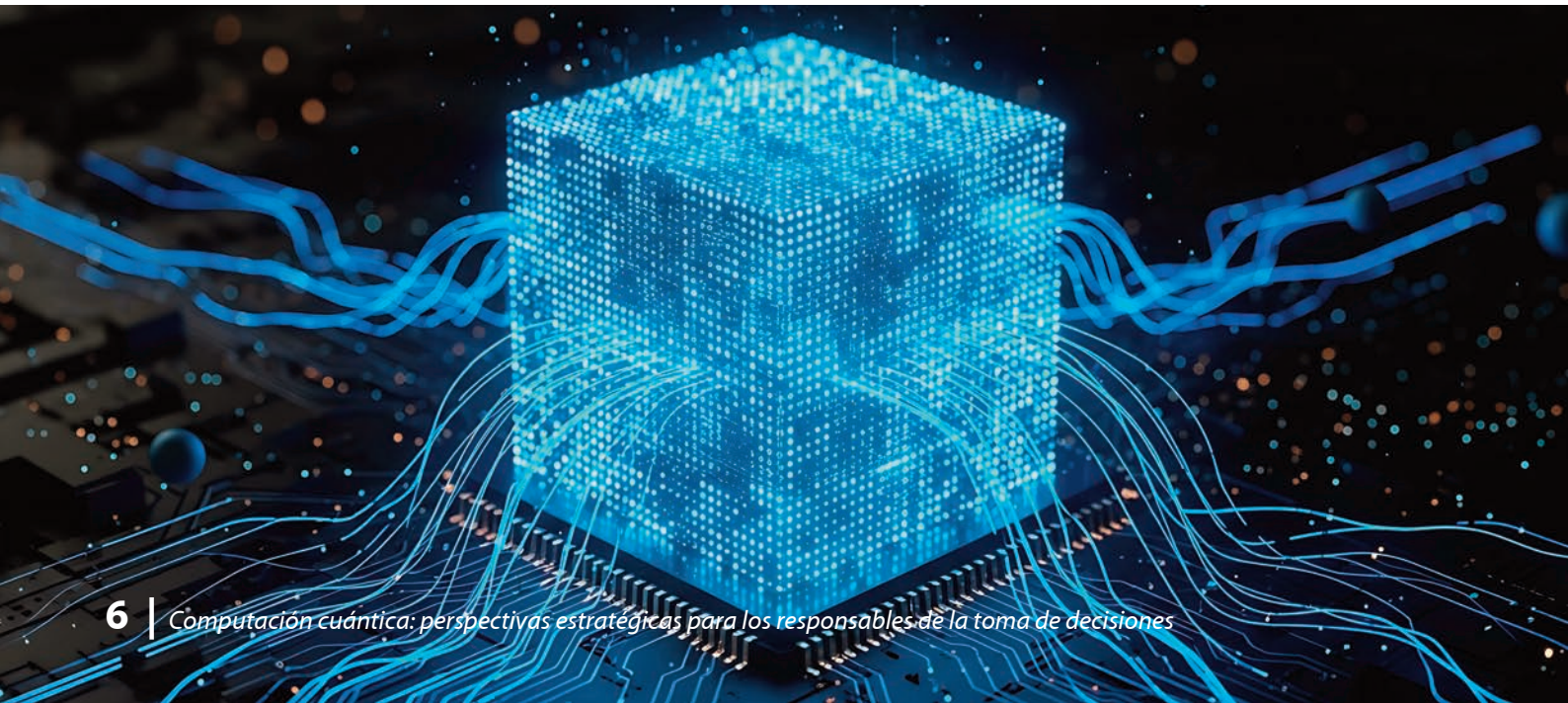
La investigación farmacéutica también se encuentra en la cúspide del cambio. Los ordenadores cuánticos ya han demostrado su potencial en la simulación de interacciones moleculares, lo que permite a los diseñadores de fármacos identificar y ajustar los candidatos prometedores más rápidamente que con los métodos tradicionales. Los principales modelos teóricos y los últimos artículos experimentales sugieren que la tecnología cuántica podría acortar en varios años los plazos de desarrollo de fármacos, especialmente en el caso de los fármacos biológicos y las terapias génicas, con un impacto a gran escala previsto a medida que surjan dispositivos cuánticos con corrección de errores durante la década de 2030. [13]

En el ámbito financiero, los bancos y las aseguradoras ya están llevando a cabo pruebas piloto con algoritmos cuánticos para el análisis de riesgos y la detección de fraudes, pero la mayoría de las hojas de ruta del sector (IBM y WEF) prevén un cambio significativo a nivel de producción más cerca de 2032-2035, dependiendo de la ampliación del hardware y el desarrollo de nuevas normas reguladoras. [14]

En cuanto a la logística y las cadenas de suministro globales, el Foro Económico Mundial informa de que se están realizando pruebas piloto con la computación cuántica para la optimización de rutas y la previsión de escenarios, y se espera una transformación de todo el sector a medida que el ecosistema madure entre 2030 y 2035. [15]

En cuanto a la ciberseguridad, se espera que en los próximos 10-15 años se disponga de un ordenador cuántico lo suficientemente grande como para romper el cifrado RSA. Las investigaciones de Google Quantum AI y los principales artículos académicos prevén un «Q-day» a principios o mediados de la década de 2030, lo que impulsará la migración urgente al cifrado cuántico seguro para todas las infraestructuras críticas. [16]

La inteligencia artificial y la computación cuántica están empezando a converger, ya que los enfoques híbridos de IA cuántica se muestran prometedores en el ámbito de la salud (diagnóstico, genómica) y el desarrollo de fármacos. Aunque la ventaja cuántica aún no es habitual fuera de los laboratorios de investigación, estudios científicos demuestran que el aprendizaje automático cuántico y el modelado molecular ya han superado a los enfoques clásicos en aplicaciones médicas especializadas, y es probable que su utilidad se amplíe a medida que ambos campos maduren. [12]



# Una oportunidad estratégica

El control de calidad sigue siendo una frontera muy prometedora en el ámbito tecnológico. Cada obstáculo supone una oportunidad para la innovación, la inversión y el liderazgo. Superarlos requerirá la colaboración entre disciplinas, sectores y regiones.

El camino hacia la ventaja cuántica no es lineal, pero es navegable. A medida que las organizaciones desarrollen su capacidad técnica, exploren casos de uso estratégicos y participen en la configuración de un ecosistema más amplio, contribuirán a liberar el poder transformador de la computación cuántica, no solo como herramienta, sino como catalizador de nuevas formas de pensar y resolver problemas.

## Comparación estratégica con la inteligencia artificial: evitar conceptos erróneos y ciclos en la computación cuántica

La computación cuántica está experimentando una ola de interés, marcada por hojas de ruta definidas e inversiones en crecimiento. Para comprender su trayectoria, resulta instructivo comparar la evolución de la computación cuántica con la historia de la inteligencia artificial:

- La computación cuántica se basa en teoremas matemáticamente demostrados, en particular el teorema del umbral, que establece que la corrección de errores cuánticos a gran escala es factible incluso cuando los *qubits* y las puertas son imperfectos, un resultado demostrado en el desarrollo de códigos de color topológicos[10] [17] [18]. Esto asimila su evolución a la de la IA, cuyos avances teóricos de los años sesenta y setenta solo tuvieron impacto una vez que el hardware alcanzó la madurez tecnológica necesaria décadas más tarde.
- Al igual que la IA, la computación cuántica está pasando ahora de la teoría a la ingeniería: se han establecido hitos teóricos, pero el valor práctico depende de un hardware robusto. Por ejemplo, el procesador Willow de Google Quantum AI logró operaciones por debajo del umbral de error cuántico[11], un avance confirmado en recientes publicaciones de Nature [19]. Esto significa que la ampliación de los sistemas cuánticos puede suprimir exponencialmente los errores, mejorando la fiabilidad computacional.
- Además, se ha logrado la validación experimental de la lógica cuántica robusta utilizando códigos de color topológicos en plataformas de átomos neutros[12], como se ha visto en trabajos recientes de Harvard, el MIT y QuEra [20], y desarrollado por primera vez en un experimento conjunto entre el grupo del profesor Martin-Delgado y los laboratorios de Innsbruck [21].

## Indicadores estratégicos: lecciones de la evolución de la IA

Se pueden utilizar algunos indicadores estratégicos para medir la evolución de la implementación de la computación cuántica:

- La utilidad funcional debe sustituir a la validación técnica pura: la ventaja cuántica, al igual que la IA, se medirá por los éxitos en problemas industriales y aplicaciones reales.
- Absorción del mercado y adopción empresarial: el impacto sostenible se producirá cuando las soluciones cuánticas impulsen los modelos de negocio y la integración operativa generalizada.
- Madurez del ecosistema y del talento: al igual que la IA, la cuántica requerirá de personal cualificado, la colaboración entre el mundo académico y la industria, y plataformas de software y hardware robustas.
- Inversión sostenida a largo plazo y gestión de las expectativas: evitar los ciclos de promesas excesivas y decepciones significa centrarse en el progreso sostenido a largo plazo, no en tendencias efímeras.
- Realismo de los medios de comunicación y las políticas: un discurso público y unas políticas cuidadosamente orientados pueden acelerar las expectativas realistas y el apoyo constructivo.

La trayectoria de la computación cuántica, al igual que la de la IA, dependerá de la investigación persistente, el progreso constante del hardware y la colaboración práctica entre disciplinas. El camino no es lineal, pero con los recientes hitos en la corrección de errores y la lógica escalable, el campo está posicionado para una transición de la investigación fundamental a la tecnología de impacto.

[10] Los códigos de color topológicos son una familia de códigos cuánticos de corrección de errores diseñados para proteger la información cuántica de los errores codificándola en las propiedades globales (topológicas) de una red de *qubits*, en lugar de en características locales. Funcionan disponiendo los *qubits* en redes específicamente coloreadas y altamente conectadas, a menudo en dos o tres dimensiones, de modo que el estado cuántico codificado sea resistente al ruido y las perturbaciones locales. Los códigos de color destacan por permitir una amplia gama de operaciones de puertas cuánticas tolerantes a fallos, llamadas puertas transversales, que se realizan de manera que los errores no se propaguen de forma incontrolada. Esta estructura convierte a los códigos de color en uno de los principales candidatos para la computación cuántica escalable y tolerante a fallos, y les permite alcanzar un nivel de computación por debajo del umbral de error necesario para obtener una ventaja cuántica práctica.

[11] El umbral de error cuántico es un valor teórico crítico en la computación cuántica que define la tasa de error máxima —como para operaciones, almacenamiento o mediciones de *qubits*— que se puede tolerar sin dejar de permitir una computación cuántica fiable a gran escala mediante la corrección de errores. Si las tasas de error físico de un procesador cuántico se mantienen por debajo de este umbral, los códigos de corrección de errores cuánticos pueden corregir los errores más rápido de lo que se producen, lo que permite escalar los cálculos indefinidamente sin pérdida de información. Alcanzar y mantenerse por debajo del umbral de error cuántico es esencial para construir ordenadores cuánticos prácticos y tolerantes a fallos, y es el objetivo fundamental del desarrollo moderno de hardware cuántico.

[12] Las computadoras cuánticas de átomos neutros son un tipo de plataforma de computación cuántica que utiliza átomos neutros individuales (en lugar de iones o circuitos superconductores) como *qubits*. Estos átomos se atrapan y se disponen en patrones precisos mediante láseres, formando a menudo grandes matrices regulares. La información cuántica se codifica en los estados internos de los átomos, y las operaciones entre *qubits* se realizan mediante pulsos láser que inducen interacciones o entrelazamientos. Las computadoras cuánticas de átomos neutros son prometedoras porque permiten arquitecturas altamente escalables y una reconfiguración flexible, y recientemente han demostrado una lógica tolerante a fallos y corrección de errores en grandes sistemas *multiqubit*.

# Aprender de la historia, liderar el futuro

La comunidad cuántica actual está trabajando para evitar ciclos de promesas excesivas y retrasos, centrándose en enfoques híbridos, aplicaciones a corto plazo y hardware que cumpla con los umbrales de corrección de errores. El optimismo sobre el futuro de la computación cuántica está justificado por los avances teóricos y experimentales, pero sigue siendo importante actuar con cautela: es esencial elaborar una hoja de ruta basada en resultados reales, y no solo en aspiraciones.

En última instancia, el destino de la computación cuántica reflejará las lecciones aprendidas de la IA: la persistencia, el progreso del hardware y el enfoque en casos de uso prácticos determinarán cuándo y cómo la promesa de la cuántica se convertirá en una realidad cotidiana.

## Marcos estratégicos para evaluar la preparación cuántica

Para abordar la adopción de la computación cuántica de forma inteligente, las organizaciones deben desarrollar marcos estructurados y criterios de decisión, evaluando la madurez tecnológica, la alineación con los objetivos empresariales, los plazos de inversión, sinergias con el talento y la infraestructura existentes dentro de la organización, y el entorno normativo. [7]

Por ejemplo, las aplicaciones de referencia en del sector financiero (modelización de riesgos, uso híbrido cuántico-clásico), farmacéutico (simulaciones moleculares, asociaciones tecnológicas) o energético (optimización de la red, sostenibilidad) pueden proporcionar una visión realista frente al entusiasmo exagerado.

Muchas organizaciones e investigadores han desarrollado marcos estructurados para la preparación cuántica, como el Quantum Readiness Toolkit del Foro Económico Mundial [22] y los modelos de preparación organizativa destacados en la literatura científica. Estas herramientas ayudan a las organizaciones a evaluar su preparación, establecer prioridades para la adopción y evitar inversiones prematuras o la dependencia de un único proveedor. Como parte de esta planificación estratégica, los líderes tecnológicos deben reconocer que cualquier infraestructura o producto que dependa de RSA u otra criptografía de clave pública actual tendrá que migrar a algoritmos poscuánticos seguros en los próximos años, lo cual es una prioridad subrayada por las directrices oficiales del NIST y las normas definitivas para la criptografía poscuántica, que recomiendan comenzar esta transición ahora para garantizar la seguridad y el cumplimiento normativo en el futuro [23].

## Próximos pasos prácticos: desarrollo de la capacidad cuántica

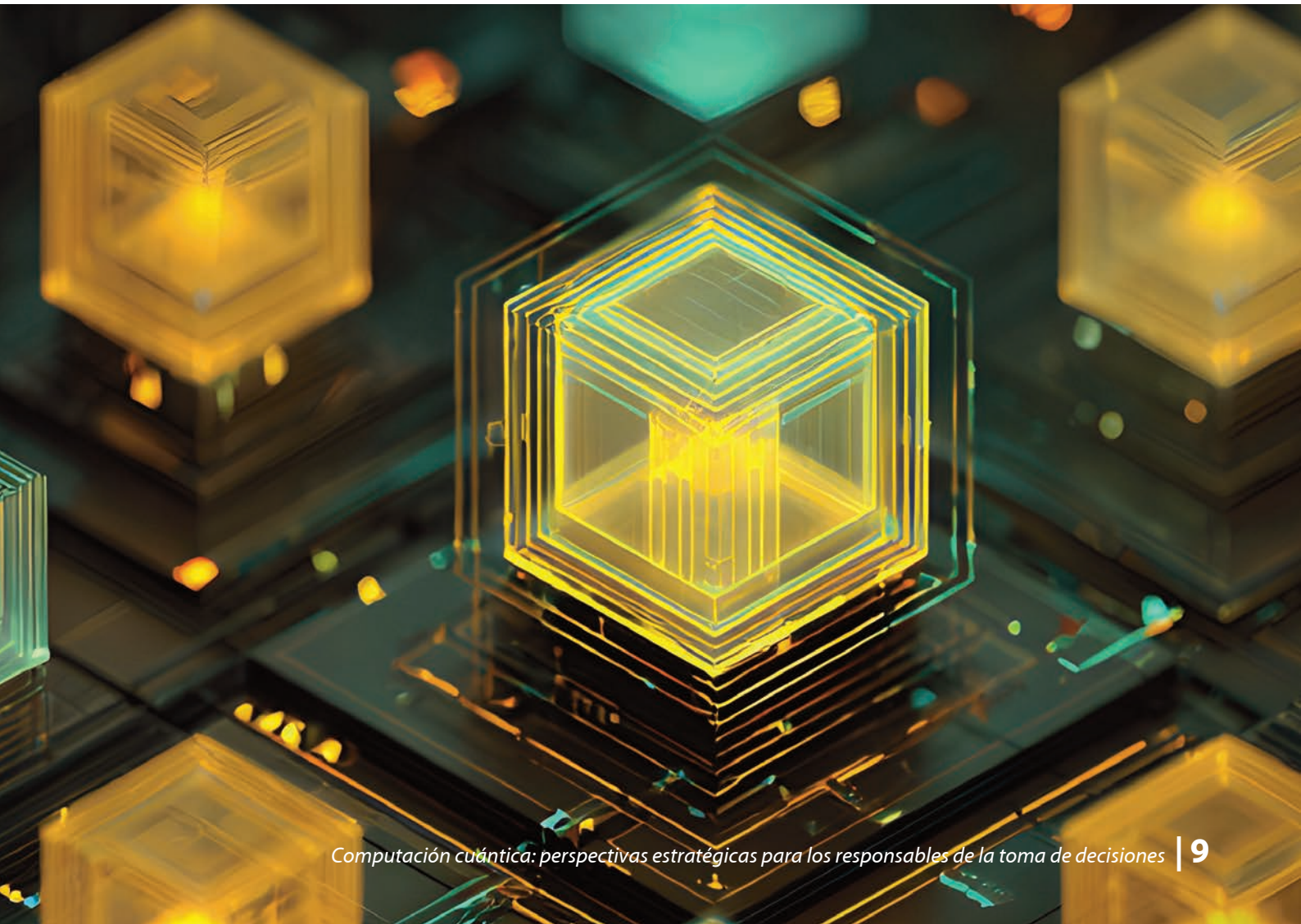
Se pueden considerar algunos pasos prácticos para desarrollar la capacidad cuántica en las organizaciones:

- Comenzar con proyectos piloto pequeños y cuantificables para comprobar la relevancia y la viabilidad de la aplicación de la computación cuántica.
- Aprovechar asociaciones con empresas emergentes, proveedores de servicios en la nube y laboratorios académicos para acceder a conocimientos especializados y crear prototipos rápidamente.
- Invertir en la formación tanto de directivos como de técnicos especializados, recurriendo a programas *online* accesibles y conferencias intersectoriales.
- Crear equipos multifuncionales que combinen conocimientos cuánticos y de negocio.
- Fomentar una cultura de experimentación, iteración y aprendizaje, no solo con la tecnología, sino también con los acuerdos entre empresas y los modelos de negocio. [7]

## Perspectiva final: previsión estratégica para la computación cuántica

La computación cuántica parece ahora más cercana que nunca, pero su calendario de adopción generalizada sigue siendo incierto. Al igual que con la inteligencia artificial, el potencial transformador no garantiza un impacto fácil o inmediato. Algunas industrias se enfrentarán a retos similares a los que se han planteado en el camino hacia la IA: escasez de especialistas altamente cualificados, pruebas poco claras de que la tecnología aporta más valor que las soluciones clásicas maduras y necesidades de inversión significativas para establecer la infraestructura adecuada e integrar nuevos flujos de trabajo. En este panorama, puede resultar difícil para las organizaciones distinguir entre las oportunidades reales y las tendencias efímeras, o identificar los casos de uso en los que las soluciones cuánticas realmente superarán a las herramientas existentes.

Al igual que los proyectos de IA más exitosos, el progreso en la computación cuántica dependerá de que las organizaciones creen entornos en los que expertos de diversos ámbitos (técnicos y empresariales) puedan colaborar para identificar y abordar los retos más acuciantes. Será esencial crear equipos dedicados, diseñar nuevas formas de trabajar e integrar estrategias cuánticas en las operaciones diarias. Igualmente, será crucial que cualquier tecnología que se base en la criptografía RSA comience una migración cuidadosa y planificada hacia algoritmos seguros poscuánticos. Los responsables de la toma de decisiones deben evaluar activamente los riesgos cuánticos y actualizar su estrategia tecnológica para garantizar que sus sistemas sean seguros y estén preparados para el futuro. Solo aquellas organizaciones que combinen una visión realista con la creación de un ecosistema específico convertirán la promesa de la cuántica en resultados tangibles.



# Bibliografía


[1] Preskill, J.: Quantum Computing in the NISQ era and beyond (2018). https://arxiv.org/pdf/1801.00862.pdf.

[2] IBM Research: The Future of Computing: IBM Quantum Roadmap (2022).

[3] D-Wave Systems: Quantum Computing for Business: Practical Use Cases and Applications (2025).

[4] ibm.com/roadmaps/quantum/

[5] Quantum Computing Report: D-Wave Study Reports Over One-Quarter of Business Leaders Expect Quantum Optimization ROI of $5 Million or Higher (2025).

[6] https://arxiv.org/abs/1910.11333.

[7] Quantum Computing in 2025: Hype vs Reality. Supaboard.ai.

[8] Quantum Computing Future - 6 Alternative Views Of The Next Decade. Quantumzeitgeist.com.

[9] Quantum Leaders Tell FT: Scaling Challenges Still Loom. Thequantuminsider.com

[10] Quantum Computing in 2025: Milestones, Challenges, and What Lies Ahead. https://www.linkedin.com/pulse/quantum-computing-2025-milestones-challenges-what-lies-ilja-bele%C5%84ki-jjnyf

[11] State of Quantum 2025 - Third Edition. Meetiqm.com.

[12] Martín-Delgado, M., et al.: Informes anticipando tecnologías cuánticas en la medicina del futuro. Observatorio de tendencias. Fundación Instituto Roche (2024).

[13] Jeyaraman, N. et al.: Revolutionizing Healthcare: The Emerging Role of Quantum Computing in Enhancing Medical Technology and Treatment. National library of medicine (2024). doi: 10.7759/cureus.67486

[14] Yndurain, E. et al.: Exploring quantum computing use cases for financial services. IBM Institute for business value (2019).

[15] World Economic Forum: Quantum Economy Blueprint (2024).

[16] Quantum computers may crack RSA encryption with fewer *qubits* than expected. Phys.org (2025).

[17] Bombin, H., & Martin-Delgado, M.A.: Topological quantum distillation. Phys. Rev. Lett. 97, 180501 (2006).

[18] Bombin, H., & Martin-Delgado, M.A.: Topological computation without braiding. Phys. Rev. Lett. 98, 160502 (2007).

[19] Google Quantum AI (2025): Willow processor breakthrough. Nature.

[20] Sales Rodriguez, P., Robinson, J.M., Jepsen, P.N. et al. Experimental demonstration of logical magic state distillation. Nature 645, 620–625 (2025). https://doi.org/10.1038/s41586-025-09367-3.

[21] Nigg, D., et al.: Quantum computations on a topologically encoded qubit. Science (2014).

[22] World Economic Forum: Quantum Readiness Toolkit: Building a Quantum-Secure Economy (2023).

[23] Alagic, G. et al.: Status Report on the Fourth Round of the NIST Post-Quantum Cryptography Standardization Process. NIST IR 8545 (2025)

## Autores

Ernestina Menasalvas (UPM)
Manuel Ángel Guzmán (Management Solutions)
Rodrigo Lojero (Management Solutions)

UNIVERSIDAD POLITÉCNICA DE MADRID

La Universidad Politécnica de Madrid es una Entidad de Derecho Público de carácter multisectorial y pluridisciplinar, que desarrolla actividades de docencia, investigación y desarrollo científico y tecnológico.

**www.upm.es**

Management Solutions
Making things happen

Management Solutions es una firma internacional de consultoría, centrada en el asesoramiento de negocio, finanzas, riesgos, organización, tecnología y procesos, que opera en más de 50 países y con un equipo de 4.000 profesionales que trabajan para más de 2.200 clientes en el mundo.

**www.managementsolutions.com**

**Para más información visita**

**blogs.upm.es/catedra-idanae/**