



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

Análisis del uso de las tecnologías cuánticas en Defensa

Máster Universitario en Dirección TIC para la Defensa

ALUMNO: José Díaz Caro
DIRECTOR: Miguel Rodelgo Lacruz
CURSO ACADÉMICO: 2025-2026

Universida_{de}Vigo



Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

Análisis del uso de las tecnologías cuánticas en Defensa

Máster Universitario en Dirección TIC para la Defensa
Especialidad de Sistemas y Tecnologías de la Información

Universida_{de}Vigo

RESUMEN

Las tecnologías emergentes y disruptivas (EDT) son aquellas que provocan cambios radicales en el concepto y la operación de aplicaciones ya consolidadas, y las tecnologías cuánticas constituyen uno de los vectores más relevantes de esta transformación en el ámbito de la Defensa. Estas tecnologías introducen nuevas oportunidades operativas y, al mismo tiempo, riesgos significativos en un contexto de competencia estratégica entre estados y organismos supranacionales.

A medida que avanzan en su madurez tecnológica e industrial, se definen casos de uso más específicos y se clarifica su integración con capacidades ya en servicio, particularmente en Mando y Control (C2), Ciberdefensa, Guerra Electrónica e Inteligencia, Vigilancia y Reconocimiento (ISR). El trabajo analiza de forma estructurada la computación y las comunicaciones cuánticas utilizando los Niveles de Madurez Tecnológica (TRL) como marco para valorar su proximidad a la aplicación operativa.

Con el conocimiento actual, el TFM identifica qué capacidades militares pueden beneficiarse antes de las tecnologías cuánticas, incluyendo aplicaciones en optimización logística, simulación avanzada, análisis de grandes volúmenes de información, sincronización precisa de activos, distribución cuántica de claves (QKD) y transición hacia criptografía post-cuántica (PQC) resistente a ataques cuánticos. Asimismo, explora escenarios de integración híbrida cuántico-clásica y recoge casos de uso identificados en el contexto aliado, especialmente en la OTAN.

El objetivo final es aportar elementos para la definición de políticas y estrategias de adopción de tecnologías cuánticas en Defensa, con especial atención a la soberanía tecnológica, el desarrollo industrial nacional e internacional, los marcos de control de exportaciones y los planes de formación y capacitación del personal implicado en la concepción, despliegue y explotación de estas capacidades.

PALABRAS CLAVE

Tecnologías emergentes y disruptivas (EDT), Madurez tecnológica, Capacidades militares, Computación cuántica, Comunicaciones cuánticas

ÍNDICE DE CONTENIDO

Índice de Contenido.....	1
Índice de Figuras	4
Índice de Tablas.....	5
1 Introducción.....	7
1.1 Antecedentes y motivación	7
1.2 Tecnologías Emergentes y Disruptivas para Defensa.....	8
1.3 Madurez tecnológica	9
1.4 Capacidades militares	11
1.5 Oportunidades y riesgos de las tecnologías cuánticas	13
2 Ciencia y Tecnología Cuántica.....	15
2.1 Orígenes de la física cuántica.....	15
2.2 Principios fundamentales de las tecnologías cuánticas.....	16
2.2.1 La unidad de información cuántica, el qubit.....	16
2.2.2 Superposición y entrelazamiento	17
2.2.3 La medición cuántica y los teoremas de la no clonación y la no distribución.....	19
2.2.4 La coherencia cuántica.....	20
2.2.5 La teleportación cuántica.....	21
2.3 Las tecnologías cuánticas.....	22
2.3.1 Avances tecnológicos de la primera revolución cuántica.....	22
2.3.2 Avances tecnológicos de la segunda revolución cuántica	25
2.4 La información cuántica.....	25
2.5 La computación cuántica	27
2.5.1 Los ordenadores cuánticos.....	27
2.5.2 La complejidad computacional.....	30
2.5.3 Algoritmos cuánticos	34
2.5.4 La supremacía cuántica.....	37
2.5.5 NISQ versus FTQC.....	43
2.6 Las comunicaciones y las redes cuánticas	49
2.6.1 La distribución cuántica de clave (QKD)	50
2.6.2 La internet cuántica.....	56
3 Aplicación de las Tecnologías Cuánticas	61
3.1 Aplicaciones en sectores civiles.....	61

3.1.1 Aplicaciones de la computación cuántica.....	61
3.1.2 Aplicaciones de las comunicaciones cuánticas.....	62
3.2 Aplicación a las capacidades militares.....	63
3.2.1 Computación cuántica	65
3.2.2 Las comunicaciones cuánticas, la criptografía post-cuántica y los algoritmos de inspiración cuántica.....	68
3.2.3 Casos de uso militares en el ámbito OTAN.....	72
3.2.4 Operatividad militar de las tecnologías cuánticas.....	72
4 La Industria Cuántica	75
4.1 Asociaciones industriales	75
4.1.1 Asociación de la Industria Cuántica Europea (European Quantum Industry Consortium, QuIC).....	76
4.1.2 UKQuantum (Reino Unido)	76
4.1.3 Quantum Industry Canada, QIC (Canadá).....	76
4.1.4 Quantum Economic Development Consortium, QED-C (Estados Unidos).....	77
4.1.5 Quantum STRategic industry Alliance for Revolution, Q-STAR (Japón)	78
4.2 Industria internacional.....	78
4.2.1 Computación cuántica	78
4.2.2 Comunicaciones cuánticas	82
4.2.3 La industria China.....	85
4.3 Industria nacional	86
5 Políticas, Estrategias y Planes Cuánticos	91
5.1 La soberanía tecnológica e industrial.....	91
5.1.1 De la ciencia a la tecnología y de la innovación a la industria	91
5.1.2 Las tecnologías críticas.....	92
5.1.3 Los controles de exportación	93
5.2 La política industrial y tecnológica europea	95
5.2.1 Sectores críticos y su relevancia para la Seguridad y Defensa	95
5.2.2 La política industrial y tecnológica de defensa en Europa y España.....	95
5.3 La política de tecnologías cuánticas en Europa y en España	98
5.3.1 Iniciativas de la Comisión Europea en tecnologías cuánticas	98
5.3.2 Convocatorias y proyectos europeos en tecnologías cuánticas	100
5.4 La política de tecnologías cuánticas en otros países y organismos.....	101
5.4.1 Iniciativas del Reino Unido en tecnologías cuánticas	104
5.4.2 Iniciativas de Estados Unidos en tecnologías cuánticas	104

5.4.3 Actividades Chinas en tecnologías cuánticas	105
5.4.4 Actividades de la OTAN en tecnologías cuánticas.....	105
5.5 Estado de la cuántica en el mundo	107
5.5.1 Ciencia, tecnología e inversión [MIT 2025]	107
5.5.2 Formación y capacitación del personal.....	110
6 Conclusiones y acciones futuras.....	113
7 Bibliografía.....	117
8 Acrónimos	131

ÍNDICE DE FIGURAS

Figura 2-1 Representación gráfica de bits y qubits en la esfera de Bloch [adaptación de SB 2024].	18
Figura 2-2 Esquema básico de comunicación cuántica, usando pares entrelazados [SB 2024].	19
Figura 2-3 Pasos de la teleportación cuántica [Kimble 2008].	21
Figura 2-4 Diagrama esquemático de un sistema de comunicación general [Shannon 1948].	26
Figura 2-5 Clases de complejidad computacional [Hidary 2019].	33
Figura 2-6 Ejemplo de un circuito usado en el experimento de Sycamore de Google [Arute 2019].	38
Figura 2-7 Evolución del volumen cuántico con los diferentes procesadores de IBM.	39
Figura 2-8 Métrica volumétrica con circuitos de aplicación [Hashim 2025].	42
Figura 2-9 Principio del protocolo BB84 [BB 1984].	51
Figura 2-10 Red de comunicaciones cuánticas china [MERICS 2024].	54
Figura 2-11 Esquema de la infraestructura satélite LEO del EAGLE-1 y la red terrestre [Referencia 56].	55
Figura 2-12 Distribución de clave cuántica [WEH 2018].	57
Figura 2-13 Distribución de entrelazamientos [WEH 2018].	58
Figura 3-1 Esquema de un conflicto bélico empleando varios sistemas basados en tecnologías cuánticas [Krelina 2021].	64
Figura 5-1 Mapamundi de inversión en planes estratégicos en tecnologías cuánticas [FGCSIC 2025].	103
Figura 5-2 Patentes en tecnologías cuánticas por país, 2014-2024 [MIT 2025].	107
Figura 5-3 Porcentaje nacional de las publicaciones de investigaciones en computación cuántica, 2019-2023 [MIT 2025].	108
Figura 5-4 Porcentaje nacional de las publicaciones de investigaciones en comunicaciones cuánticas, 2019-2023 [MIT 2025].	109

ÍNDICE DE TABLAS

Tabla 1-1 TRL para hardware (adaptada de OSEA 2025).	10
Tabla 2-1 Ordenes de magnitud en complejidad computacional.	31
Tabla 2-2 Problema, O grande y clase de complejidad computacional.	32
Tabla 2-3 Fidelidad de circuitos cuánticos con la profundidad y el número de qubits.	44
Tabla 2-4 Número de qubits físicos y lógicos por aplicación.	46
Tabla 2-5 Comparación de los tres regímenes de computación cuántica.....	47
Tabla 2-6 Hitos de qubits físicos y de capacidad lógica efectiva.....	49
Tabla 3-1 Madurez y aplicación de las tecnologías cuánticas en Defensa.....	74
Tabla 4-1 Principales empresas de ordenadores cuánticos o QPU, tecnologías de los qubits y países de origen”.....	82
Tabla 5-1 Controles de exportación de tecnologías relacionadas con la cuántica [MERICS 2024].	94
Tabla 5-2 Principales iniciativas en tecnologías cuánticas a nivel mundial.....	102

1 INTRODUCCIÓN

1.1 Antecedentes y motivación

Los enfoques estratégicos de adopción de una tecnología emergente y disruptiva (*Emerging and Disruptive Technology*, EDT) son abstractos y a largo plazo, ya que implican explorar esas áreas emergentes todavía no consolidadas, definir casos de uso y anticipar retos futuros. Así, las estrategias de adopción de las tecnologías cuánticas se enfrentan al análisis, entendimiento e integración de tecnologías, proveedores, aplicaciones potenciales y posibles barreras, siendo una actividad compleja y poco tangible que demanda una visión futurista para entender cómo encajar las tecnologías cuánticas en una estructura organizacional, que la mayor parte de las ocasiones no está familiarizada con estas tecnologías.

Cuando se aborda una tecnología de uso en un sector, se pierde el hilo conductor de cuáles son los objetivos finales que llevan a su aplicabilidad operativa. En muchas ocasiones la complejidad y el detalle de los propios desarrollos científicos y tecnológicos centran el debate sin ahondar en otros aspectos como la disponibilidad de tecnologías habilitadoras, la capacidad de desarrollo y fabricación industrial, los marcos normativos, las políticas públicas que faciliten la transferencia tecnológica, o la formación especializada de recursos humanos.

Este trabajo pretende abordar de manera ordenada, metódica y consistente todos los aspectos a considerar en la evaluación y adopción de una tecnología emergente y disruptiva relevante para el sector de Defensa, como es la cuántica. La estructura y metodología de análisis de este trabajo es extrapolable a otras EDT (inteligencia artificial, sistemas autónomos, biotecnología, etc.) y a otros sectores (energía, salud, transporte). El objetivo principal del trabajo no es solamente desarrollar conocimiento especializado en profundidad sobre las tecnologías cuánticas, sino también establecer una metodología estructurada y replicable de cómo abordar y analizar otras tecnologías relevantes para el sector de Defensa.

Asimismo, el trabajo pretende concienciar sobre la criticidad de las políticas y planes a implementar, teniendo en cuenta que la complejidad y especialización de tecnologías como la cuántica requieren de la capacidad y dedicación adecuada de un número determinado de recursos con formación y conocimientos profundos en la materia. Sin una inversión estratégica en talento, infraestructura de investigación, colaboración público-privada y una gobernanza normativa, la adopción de estas tecnologías en defensa seguirá siendo aspiracional en lugar de operativa.

El Capítulo 1 presenta las tecnologías emergentes y disruptivas (EDT), explica el marco de madurez tecnológica (TRL), define las capacidades militares, e identifica las oportunidades y riesgos que introducen las tecnologías cuánticas en la competencia estratégica global.

El Capítulo 2 proporciona los fundamentos científicos y principios físicos de las tecnologías cuánticas, examina conceptos clave como el qubit, superposición, entrelazamiento y coherencia cuántica, y desarrolla dos de los dominios tecnológicos principales, la computación cuántica y las comunicaciones cuánticas.

El Capítulo 3 analiza las aplicaciones concretas de tecnologías cuánticas en los sectores civil y militar, y presenta los principales casos de uso identificados en el contexto de la OTAN en computación y comunicaciones cuánticas, contextualizando cada aplicación según su madurez tecnológica (TRL).

El Capítulo 4 analiza el ecosistema industrial cuántico internacional y nacional, identificando asociaciones industriales, principales actores en computación y comunicaciones cuánticas, y algunos de los principales proveedores.

El Capítulo 5 analiza políticas, estrategias y planes cuánticos en contextos europeo, nacional e internacional, examina la política industrial europea, y presenta una visión global mediante métricas de inversión pública, patentes, producción científica y formación de talento cuántico.

El Capítulo 6 presenta las conclusiones del trabajo.

1.2 Tecnologías Emergentes y Disruptivas para Defensa

Las tecnologías emergentes y disruptivas (*Emerging and Disruptive Technologies*, EDT) son innovaciones y avances tecnológicos con potencial para transformar industrias, mercados y sociedad. Mientras las tecnologías emergentes muestran un potencial relevante para impactar diferentes áreas, aunque todavía se encuentran en etapas iniciales de desarrollo y no han sido adoptadas de manera extensiva, las tecnologías disruptivas modificarán radicalmente la industria y el mercado desplazando a tecnologías, productos o servicios existentes. Ejemplos actuales de tecnologías emergentes son la inteligencia artificial, las tecnologías cuánticas y la biotecnología. Tecnologías disruptivas pasadas fueron internet o la telefonía móvil.

Las EDT traerán cambios radicales y presentarán riesgos y oportunidades en el campo de Defensa, y por ello las naciones, especialmente grandes potencias como Estados Unidos, China y Rusia, y otras organizaciones como la Unión Europea y la OTAN están embarcadas en una carrera tecnológica de desarrollo y adopción de EDT claves para las capacidades de la Defensa y la Seguridad.

La Organización del Tratado del Atlántico Norte (OTAN) ha identificado las EDT como un eje estratégico fundamental para preservar su ventaja operativa y responder a las amenazas globales. Las EDT están modificando profundamente las capacidades militares, y siendo consciente de que la superioridad tecnológica ha sido históricamente uno de sus pilares defensivos, ha adoptado una estrategia de innovación que combina el fomento de ecosistemas tecnológicos con la protección frente a amenazas derivadas del uso malicioso o no regulado de estas tecnologías. El Concepto Estratégico 2022 de la Alianza [NATO 2022] establece que las EDT constituyen tanto una oportunidad como un riesgo, y que su desarrollo debe estar guiado por principios de uso responsable, alineados con los valores democráticos y los derechos humanos. En este marco, la OTAN ha promovido iniciativas como el Acelerador de Innovación de Defensa para el Atlántico Norte (*Defence Innovation Accelerator for the North Atlantic*, DIANA)¹ y el Fondo de Innovación de la OTAN (*NATO Innovation Fund*, NIF)², con el objetivo de apoyar a startups y centros de investigación en el desarrollo de soluciones tecnológicas de doble uso, es decir, con aplicaciones tanto civiles como militares. Asimismo, la Alianza ha intensificado su cooperación con actores del sector privado, la academia y otras organizaciones internacionales, como la Unión Europea y las Naciones Unidas, para establecer estándares comunes, compartir buenas prácticas y evitar la fragmentación normativa en el desarrollo de tecnologías críticas. Esta cooperación se materializa en políticas específicas para cada área tecnológica prioritaria, así como en planes de adopción rápida que buscan reducir los ciclos de integración tecnológica en las fuerzas armadas aliadas.

Las actividades de innovación de la OTAN se centran actualmente en nueve áreas tecnológicas prioritarias³:

¹ <https://www.diana.nato.int/>

² <https://www.nif.fund/>

³ <https://www.nato.int/en/what-we-do/deterrence-and-defence/emerging-and-disruptive-technologies>

- Inteligencia Artificial (IA).
- Sistemas Autónomos.
- Tecnologías Cuánticas.
- Biotecnología y Tecnologías de Mejora de las Capacidades Humanas.
- Espacio.
- Sistemas Hipersónicos.
- Nuevos Materiales y Fabricación.
- Energía y Propulsión.
- Redes de Comunicaciones de Próxima Generación.

La Agencia Europea de Defensa (*European Defence Agency*, EDA) tiene identificadas seis EDT [Clapp 2022]:

- Inteligencia Artificial (IA).
- Tecnologías basadas en cuántica.
- Sistemas de armas robóticos y autónomos.
- Analítica de grandes datos.
- Sistemas de armas hipersónicas y tecnologías espaciales.
- Materiales avanzados.

La Estrategia de Tecnología e Innovación para la Defensa 2020 (ETID-2020)^{4,5} identifica las tecnologías emergentes y disruptivas como vectores de cambio, y también plantea una reflexión estratégica sobre su gobernanza, sus riesgos y su papel en la transformación de la defensa nacional. Propone aprovechar tecnologías maduras de forma innovadora y fomentar el desarrollo de aquellas aún incipientes, pero con alto impacto disruptivo. El documento menciona de manera no estructurada las siguientes tecnologías o innovaciones disruptivas:

- Sistemas aéreos remotamente tripulados (RPAS).
- Fabricación aditiva.
- Inteligencia artificial.
- Tecnologías cuánticas.
- Armas de energía dirigida.
- Biología sintética.
- Vehículos hipersónicos.

Se puede observar que en el contexto histórico de cada documento las tecnologías cuánticas aparecen en el listado de EDT.

1.3 Madurez tecnológica

Las organizaciones siempre se han enfrentado a las dificultades para evaluar de manera objetiva el grado de madurez de una tecnología, lo que generaba incertidumbre en la toma de decisiones, asignación de recursos y planificación estratégica. Las necesidades en el ámbito de la gestión tecnológica, especialmente en proyectos de innovación tecnológica de alto riesgo, trajeron el desarrollo y adopción del Nivel de Madurez Tecnológica (*Technology Readiness Level*, TRL).

El TRL es una herramienta desarrollada por la NASA en los años 70 para evaluar la madurez de tecnologías emergentes. Introducido por Stan Sadin (1974) y formalizado por John C. Mankins en la

⁴ <https://publicaciones.defensa.gob.es/estrategia-de-tecnologia-e-innovacion-para-la-defensa-etid-2020-libros-pdf.html>

⁵ En breve será publicada la última actualización de la ETID.

década de los 90 [Mankins 2009], ha sido adoptada por agencias como el Departamento de Defensa de Estados Unidos, la Agencia Espacial Europea (*European Spatial Agency*, ESA) y la Comisión Europea, formalizándose en un estándar ISO 16290:2013 para aplicaciones más allá del ámbito espacial [Héder 2017]. El TRL proporciona una escala estandarizada de nueve niveles, desde la observación científica básica (TRL 1) hasta la implementación operativa (TRL 9) (Tabla 1-1).

TRL	Definición	Descripción	Información de apoyo
TRL 1	Principios básicos observados	Se identifican los fundamentos científicos de la tecnología	Estudios teóricos, publicaciones científicas
TRL 2	Concepto tecnológico formulado	Se propone una aplicación basada en los principios observados, aunque aún es especulativa	Artículos, análisis preliminares del concepto
TRL 3	Prueba de concepto experimental	Se prueban partes clave de la tecnología en laboratorio.	Resultados de pruebas, modelos analíticos
TRL 4	Validación de componentes en laboratorio	Se construyen prototipos iniciales y se validan en condiciones controladas	Informes de pruebas de laboratorio, prototipos
TRL 5	Validación en entorno relevante	Se prueba el sistema en un entorno que simula condiciones reales	Datos de pruebas en campo simulado, informes técnicos
TRL 6	Demostración de sistema/subsistema	Se demuestra el funcionamiento del sistema completo o sus partes en un entorno relevante	Resultados de demostraciones, documentación técnica
TRL 7	Demostración en entorno operativo	El sistema se prueba en condiciones reales de operación	Informes de campo, validaciones operativas
TRL 8	Sistema completo certificado	El sistema está terminado y ha sido certificado para su uso	Certificaciones, documentación de calidad
TRL 9	Tecnología probada en operación real	El sistema ha sido utilizado con éxito en operaciones reales	Informes de uso operativo, retroalimentación de usuarios

Tabla 1-1 TRL para hardware (adaptada de OSEA 2025).

Esta estandarización ha sido clave para mejorar la comunicación entre actores del ecosistema tecnológico, como investigadores, ingenieros, gestores de proyectos, agencias financiadoras e inversores que comparten un lenguaje común, facilitando la colaboración interdisciplinar y la evaluación comparativa entre tecnologías. Además, el TRL ha contribuido significativamente a la reducción de riesgos tecnológicos, al permitir identificar tecnologías inmaduras que podrían comprometer el éxito de un proyecto, siendo especialmente útil en sectores de alta complejidad como el aeroespacial, la defensa, la energía y la salud, donde los fallos tecnológicos pueden tener consecuencias críticas. Ha permitido optimizar la asignación de recursos, ayudando a las organizaciones a decidir con mayor precisión dónde invertir tiempo, dinero y talento, priorizando aquellas tecnologías que están más cerca de su aplicación práctica. Ha facilitado la transferencia tecnológica, al indicar cuándo una innovación está lista para salir del laboratorio y ser comercializada

o licenciada. El TRL se ha convertido en una herramienta esencial en convocatorias de financiación pública, como las de la Comisión Europea en programas como Horizonte Europa, donde se exige que las propuestas tecnológicas indiquen su TRL para asegurar que los fondos se asignen de manera coherente con los objetivos del programa.

La Guía de Evaluación de la Madurez Tecnológica (*Technology Readiness Assessment*, TRA) de la Oficina del Secretario de Defensa para Adquisiciones de Estados Unidos (*Office of the Secretary of Defense for Acquisition*, OSEA) [OSEA 2025] evalúa la madurez tecnológica en sus programas de adquisición. Esta guía, que ha evolucionado en las versiones de 2009, 2011 y 2025, clarifica el papel crítico e independiente del TRA en la toma de decisiones estratégicas, especialmente en hitos donde se requiere que las tecnologías hayan sido demostradas en entornos relevantes, y donde se establecen criterios legales para la aprobación de programas de defensa. La guía enfatiza sobre los Elementos de Tecnología Críticos (*Critical Technology Element*, CTE), que son tecnologías esenciales para el éxito de un sistema, y que requieren de una identificación temprana y la asignación del TRL adecuado, diferenciando las definiciones para hardware y software. También hace hincapié en la importancia de contar con datos objetivos y expertos independientes para garantizar la credibilidad del análisis. Adicionalmente, la guía amplía el marco de evaluación incluyendo otros niveles de preparación como el Nivel de Madurez de Fabricación (*Manufacturing Readiness Level*, MRL), el Nivel de Madurez de Integración (*Integration Readiness Level*, IRL), el Nivel de Madurez del Sistema (*System Readiness Level*, SRL) y el Nivel de Madurez de Sostenimiento (*Sustainment Maturity Level*, SML), que amplían la evaluación en diferentes etapas del ciclo de vida de un sistema ofreciendo una visión más holística del riesgo técnico en programas complejos.

La guía TRA asegura una evaluación objetiva y estructurada del estado de las EDT, como es el caso de las tecnologías cuánticas, dando soporte a las decisiones estratégicas de desarrollo e incorporación a sistemas mayores. Se parte estableciendo un Plan de Evaluación y un equipo encargado de evaluar la madurez tecnológica. Seguidamente se identifican los elementos tecnológicos críticos (hardware, software, procesos) que son esenciales para el desempeño de la tecnología y que representan innovaciones o riesgos tecnológicos notables. Luego se evalúa y asigna el TRL a cada CTE definiendo el tipo de prueba y los entornos relevantes y operativos de las mismas. Se recopilan evidencias técnicas detalladas en cada etapa, incluyendo informes de pruebas, análisis, y comparación con objetivos técnicos, que justifiquen la asignación del TRL. Para tecnologías que estén en TRL bajos (1 a 3) o medios (4 a 6), se elabora un Plan de Maduración Tecnológica (*Technology Maturation Plan*, TMP) que detalla las actividades necesarias para alcanzar niveles más altos, mitigando riesgos de integración y operatividad. Dada la complejidad de las tecnologías cuánticas, la asignación correcta del TRL requiere de evaluaciones especializadas y de protocolos rigurosos de prueba en ambientes simulados o altamente controlados, así como de un juicio experto.

Para tecnologías suficientemente maduras se contempla incluir evaluaciones del MRL, IRL y SRL que actúan como indicadores críticos de viabilidad operativa y logística. El MRL identifica la capacidad de producir el sistema a escala y de forma asequible, el IRL mide la compatibilidad y fluidez de las interfaces entre distintos componentes, el SRL proporciona un índice compuesto que determina la madurez de todo el conjunto integrado, y el SML evalúa la capacidad de mantener, reparar y suministrar el sistema durante toda su vida útil. En conjunto, este enfoque multidisciplinar permite a los gestores de programas identificar cuellos de botella no solo en la innovación científica, sino también en la transición hacia la producción masiva y el despliegue en operaciones.

1.4 Capacidades militares

Las capacidades militares constituyen el elemento central del planeamiento estratégico de Defensa en el contexto internacional contemporáneo. La definición ampliamente adoptada en el contexto

internacional proviene de la OTAN⁶, “una capacidad es la habilidad que permite generar un efecto mediante el empleo de un conjunto integrado de aspectos clasificados como doctrina, organización, entrenamiento, material, desarrollo del liderazgo, personal, instalaciones e interoperabilidad”. Esta definición operacional establece que una capacidad militar no es un elemento aislado, como una plataforma de armamento, sino un sistema integral multidimensional que integra factores técnicos, humanos, organizacionales y doctrinales.

Los documentos sobre capacidad militares, en su mayoría, clasificados, se centran principalmente en capacidades militares convencionales y operacionales, tales como:

- Defensa aérea y antimisiles (sistemas integrados y multicapa).
- Sistemas de artillería y misiles de largo alcance.
- Movilidad estratégica (transporte aéreo y marítimo).
- Operaciones terrestres: fuerza y maniobra terrestre.
- Defensa marítima y control naval.
- Capacidades espaciales: comunicaciones, reconocimiento por satélite.
- Ciberdefensa y guerra electrónica.
- Inteligencia, Vigilancia y Reconocimiento (*Intelligence, Surveillance and Reconnaissance*, ISR).
- Sistemas de mando, control y comunicaciones integrados.
- Logística y sostenibilidad operativa.
- Capacidades de respuesta rápida (brigadas y fuerzas multinacionales).

A pesar de ello, las naciones y organismos multinacionales de Defensa consideran la importancia de la innovación tecnológica y las EDT como las tecnologías cuánticas, sobre todo en los ámbitos de sistemas de mando, control y comunicaciones, ciberdefensa y guerra electrónica e innovación tecnológica para potenciar capacidades futuras.

Uno de los documentos públicos recientes más relevantes sobre el tema es el “Libro Blanco Conjunto - Preparación en materia de defensa europea 2030” [CE 2025], de 19 de marzo, 2025. La Comisión Europea no ofrece una definición cerrada sobre las capacidades militares, pero de sus documentos estratégicos y normativos se entiende por capacidades militares las necesarias para planificar, ejecutar y sostener operaciones militares, incluyendo personal, equipos, infraestructura, sistemas de mando y control, y logística, desarrolladas de forma nacional o colaborativa por los Estados miembros. El documento identifica siete áreas prioritarias de capacidades militares que los Estados miembros deben desarrollar de forma colaborativa:

- Defensa aérea y antimisiles: Sistemas integrados y multinivel para proteger contra amenazas aéreas como misiles balísticos, hipersónicos, aviones y drones.
- Sistemas de artillería: Capacidades de fuego avanzado, incluyendo artillería moderna y sistemas de misiles de largo alcance para ataques precisos a distancia.
- Municiones y misiles: Creación de reservas estratégicas y aumento de la capacidad industrial para producir y reponer municiones y misiles de forma rápida y sostenida.
- Drones y sistemas antidrones: Desarrollo de vehículos no tripulados (aéreos, terrestres, marítimos y submarinos) y tecnologías para contrarrestarlos, con aplicaciones en vigilancia, reconocimiento y combate.
- Movilidad militar: Infraestructura y redes logísticas que permitan el transporte rápido y fluido de tropas y equipos dentro de la Unión Europea (UE) y hacia países socios.

⁶ <https://nso.nato.int/NATOTerm>

- Tecnologías avanzadas (IA, cuántica, ciberguerra y guerra electrónica): Aplicaciones militares de inteligencia artificial, tecnologías cuánticas, capacidades ofensivas y defensivas en el ciberespacio, y control del espectro electromagnético.
- Capacidades estratégicas y protección de infraestructuras críticas: Incluye reabastecimiento aéreo, inteligencia, vigilancia marítima, comunicaciones seguras, uso del espacio y protección de infraestructuras energéticas y logísticas.

Estas capacidades están alineadas con los objetivos de la Política Común de Seguridad y Defensa (*Common Security and Defence Policy*, CSDP)⁷ y buscan cerrar las brechas existentes en interoperabilidad, producción industrial, innovación tecnológica y preparación operativa. Las capacidades militares de la Unión Europea ya incluían anteriormente referencias explícitas a tecnologías cuánticas, especialmente en contextos de defensa, espacio, ciberseguridad y comunicaciones, abarcando la computación, los sensores, la criptografía y las comunicaciones cuánticas.

1.5 Oportunidades y riesgos de las tecnologías cuánticas

Las tecnologías cuánticas se están moviendo rápidamente de los laboratorios a los dominios estratégicos industriales y gubernamentales, afectando a la gestión de la información y teniendo efectos sobre los sectores de la Defensa y la Seguridad. La cuántica se encuentra en diferentes fases de madurez hacia el despliegue y operación de las soluciones aportadas. La gobernanza de la cuántica está emergiendo ahora, alentada por la supremacía estratégica que promete a las naciones punteras. Así, esta tecnología ha promovido políticas y estrategias, sobre todo estos últimos cinco años, y un creciente interés sobre el impacto sobre la paz y la seguridad global [TBP 2024, Krelina 2025_2].

Entre los beneficios está la detección de amenazas con mayor precisión, que podrían identificar materiales peligrosos (químicos, biológicos, nucleares), o modelos climáticos avanzados que podrían mejorar las predicciones sobre el cambio climático.

Pero existen riesgos emergentes que afectarían la estabilidad geopolítica y seguridad mundial. La computación cuántica podría poner en riesgo comunicaciones, transacciones digitales y datos personales, rompiendo los sistemas de cifrado que los protegen, o podría desarrollar nuevas moléculas que podrían emplearse como armas químicas o biológicas. Los sensores cuánticos desestabilizarían la disuasión nuclear estratégica al hacer detectables submarinos nucleares, silos de misiles y laboratorios secretos, y aportarían una ventaja táctica a los combatientes con capacidad de geoposicionamiento en entornos con el sistema de navegación global por satélite (*Global Navigation Satellite System*, GNSS) degradado o denegado. La carrera armamentista basada en tecnologías cuánticas llevará a conflictos asimétricos tecnológicamente, que pueden desembocar en una mayor riesgo y letalidad para los civiles. Otros riesgos son la sostenibilidad ambiental y los materiales críticos, ya que los ordenadores cuánticos demandan una gran cantidad de energía y requieren de materiales escasos como el helio-3 y las tierras raras.

La OTAN⁸ considera las implicaciones éticas de las EDT, como la IA, los sistemas autónomos y la biotecnología y el aumento de las capacidades humanas, pero también promueve garantizar que la innovación y adopción de las tecnologías cuánticas se realice de forma ética, segura y sostenible, anticipando riesgos antes de que se materialicen.

⁷ <https://eur-lex.europa.eu/ES/legal-content/summary/the-eu-s-common-security-and-defence-policy.html>

⁸ <https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/01/16/summary-of-natos-quantum-technologies-strategy>

La argumentación de los riesgos de las EDT no es nueva, todas las nuevas tecnologías proporcionan una ventaja táctica y estratégica a las naciones que disponen de ellas, y pueden ser empleadas de manera ilícita por terroristas y organizaciones criminales. Lo que está ocurriendo con tecnologías como la inteligencia artificial o la cuántica es que la dificultad de su interpretabilidad genera una brecha en la responsabilidad de sus decisiones, y que su capacidad de potenciar y acelerar el avance tecnológico en múltiples materias creará grandes diferencias entre las naciones con mayor capacidad en cuántica y tecnologías habilitadoras.

2 CIENCIA Y TECNOLOGÍA CUÁNTICA

El propósito del Capítulo 2 es proporcionar una comprensión de los fundamentos científicos, los principios físicos y la madurez tecnológica actual de las tecnologías cuánticas, estableciendo las bases conceptuales necesarias para analizar posteriormente sus aplicaciones militares y estratégicas. Para ello, el capítulo inicia con una revisión histórica de los orígenes de la física cuántica a finales del siglo XIX y principios del XX. A continuación, examina los principios fundamentales que subyacen a las tecnologías cuánticas: el qubit, la superposición, el entrelazamiento, la medición cuántica y el teorema de la no clonación, la coherencia cuántica y la teleportación cuántica. El capítulo diferencia entre la primera revolución cuántica (tecnologías pasivas basadas en comprensión de fenómenos cuánticos) y la segunda revolución cuántica (tecnologías activas que manipulan y controlan estados cuánticos). Finalmente profundiza en el dominio tecnológico de la computación cuántica, examinando las arquitecturas de ordenadores cuánticos, la complejidad computacional, los algoritmos cuánticos, y el concepto de supremacía cuántica, y en el dominio tecnológico de las comunicaciones cuánticas, analizando distribución cuántica de clave (QKD) como tecnología más madura y la visión emergente de internet cuántica como infraestructura global de comunicaciones híbrida clásica-cuántica.

2.1 Orígenes de la física cuántica

El origen de la física cuántica puede situarse a finales del siglo XIX, cuando la física clásica, particularmente la mecánica newtoniana y el electromagnetismo, demostraban ser insuficientes para explicar ciertos fenómenos a escalas atómicas y subatómicas tales como la radiación del cuerpo negro, el efecto fotoeléctrico y el espectro atómico [Ron 2025, Ron 2025_2].

El inicio crucial que marca el nacimiento formal de la teoría cuántica se sitúa en 1900, cuando Max Planck propuso que la energía no se emitía ni absorbía de manera continua, sino en unidades discretas denominadas “cuantos” [Planck 1900]. Su teoría fue decisiva para superar la llamada “catástrofe ultravioleta” en la radiación del cuerpo negro y sentó un nuevo paradigma en la física al introducir una constante fundamental, hoy conocida como la constante de Planck, que caracteriza la cuantización de la energía.

Cinco años después, en 1905, Albert Einstein explicó el efecto fotoeléctrico, un fenómeno que la física clásica no podía justificar. Einstein postuló la existencia de los “fotones”, partículas que transportan energía cuantizada. Con ello extendió la idea de Planck y propuso que la luz exhibe una dualidad onda-partícula, dependiendo del tipo de interacción que se observe. Posteriormente, en 1924, Louis de Broglie generalizaría la dualidad onda-partícula sugiriendo que no solo la luz, sino también la materia como los electrones, puede comportarse como onda y partícula⁹ [Broglie 1924].

En 1913, Niels Bohr desarrolló un modelo atómico que integraba la cuantización para explicar la estabilidad de los átomos de hidrógeno y sus espectros de emisión, formulando un esquema donde los electrones orbitaban en niveles discretos de energía [Kragh 2022]. Este modelo, aunque limitado para átomos complejos, representó un avance crucial para la aplicación de principios cuánticos a la estructura atómica.

La verdadera consolidación formal llegó en la década de 1920, cuando la mecánica cuántica fue completada mediante dos formulaciones equivalentes pero conceptualmente diferentes. En 1925,

⁹ C.J. Davisson y L.H. Germer [DG 1927], y G.P. Thomson [Thomson 1928] realizaron experimentos de difracción de electrones que confirmaron experimentalmente la dualidad de Louis de Broglie.

Werner Heisenberg propuso la mecánica matricial, un marco basado en cantidades observables [FJP 2009]. En 1926, Erwin Schrödinger presentó la mecánica ondulatoria, introduciendo la función de onda como entidad matemática clave para describir sistemas cuánticos y formulando la famosa ecuación de Schrödinger [Schrödinger 1926]. Max Born aportó en 1926 la interpretación de la función de onda como una función de probabilidad, sentando las bases para la naturaleza intrínsecamente probabilística de la mecánica cuántica [Born 1926]. Poco después, Paul Dirac formuló la ecuación de Dirac, que compatibiliza la mecánica cuántica con la relatividad especial, abriendo caminos hacia la física de partículas y la electrodinámica cuántica [Dirac 1927, Dirac 1928]. Estos desarrollos vinieron acompañados por el principio de incertidumbre de Heisenberg (1927), que estableció límites fundamentales en la precisión con que se pueden medir simultáneamente ciertas variables, como posición y momento, erosionando el determinismo clásico [Heisenberg 1927]. John von Neumann aportó el rigor matemático mediante los espacios de Hilbert, como base formal del análisis cuántico que unificaba la mecánica matricial y ondulatoria, y desarrolló la teoría de la medida cuántica (1932) [Neumann 1932].

2.2 Principios fundamentales de las tecnologías cuánticas

El cuerpo teórico de la física cuántica dio lugar a profundas discusiones filosóficas sobre la naturaleza de la realidad, la medición y la observación, evidenciadas en debates históricos entre figuras como Einstein y Bohr, que cuestionaron la interpretación de la teoría y la idea misma del determinismo en la naturaleza.

Las tecnologías cuánticas se basan en varios principios clave de la mecánica cuántica, entre los que destacan la superposición, el entrelazamiento, el principio de incertidumbre de Heisenberg, el efecto túnel cuántico y la interferencia cuántica. El principio de incertidumbre de Heisenberg, que establece los límites fundamentales en la precisión con la que se pueden conocer ciertas parejas de propiedades físicas, como posición y momento, influye en el diseño y la comprensión de dispositivos cuánticos. El efecto túnel cuántico, que permite que partículas atraviesen barreras energéticas que serían insuperables según la física clásica, es clave para sensores cuánticos y microscopios de alta resolución. La interferencia cuántica, que permite manipular los estados cuánticos mediante la superposición, es esencial para algoritmos cuánticos y control de qubits. Juntos, estos principios habilitan una gama amplia de tecnologías cuánticas que incluyen computación cuántica, comunicaciones cuánticas seguras y sensores cuánticos.

2.2.1 La unidad de información cuántica, el qubit

El concepto del qubit surgió gradualmente del desarrollo teórico de la computación cuántica durante la década de 1980, aunque su formalización conceptual ocurrió posteriormente.

Paul Benioff fue el primero en proponer ideas esenciales sobre computación cuántica (1980) imaginando una máquina de Turing tradicional que incorporaba principios de la mecánica cuántica y describiendo explícitamente una máquina de computación cuántica reversible [Benioff 1980]. Posteriormente, Richard Feynman (1981-1982) presentó su conocida ponencia titulada “Simulación de la física con computadoras” en la Primera Conferencia sobre Física de la Computación del MIT [Feynman 1982]. Feynman observó que ciertos fenómenos cuánticos no podían ser simulados eficientemente por computadoras clásicas y propuso utilizar precisamente esos fenómenos cuánticos para realizar cálculos complejos. David Deutsch describió el primer computador cuántico universal (1985), capaz de simular cualquier otro computador cuántico, y también fue el primero en formular un algoritmo cuántico y en exponer la idea de que un computador cuántico podría ejecutar diferentes algoritmos [Deutsch 1985].

El término “qubit” fue introducido por Benjamin Schumacher en un artículo publicado en *Physical Review* en 1995, en el que describió una forma de comprimir información cuántica en el número más pequeño de estados posibles, lo que se conoce como compresión de Schumacher [Schumacher 1995].

El qubit es la unidad de información cuántica, análoga al bit de la información clásica, en la que se codifican los estados cuánticos de cualquier partícula física (subatómicas, atómicas, fotones, iones, etc.). A diferencia de los bits clásicos, que pueden ser 0 o 1, los qubits pueden existir en múltiples estados simultáneamente gracias al principio de superposición (Figura 2-1).

Fue el descubrimiento del algoritmo de factorización de primos de Peter Shor [Shor 1999], presentado inicialmente en 1994 en una conferencia, lo que transformó la computación cuántica de una mera curiosidad teórica en un campo de investigación con aplicaciones potencialmente revolucionarias.

Uno de los retos principales de los ordenadores cuánticos es la ingeniería para materializar prácticamente los qubits. Las principales condiciones que se deben cumplir para conseguir una aplicación práctica de un qubit son, disponer de un sistema físico que tenga dos estados manipulables a los que se les pueda asignar los estados $|0\rangle$ y $|1\rangle$, y que se pueda aislar convenientemente de los efectos de decoherencia, para que la superposición de estados sea lo suficientemente estable.

En 1998 se demostró el primer algoritmo cuántico (versión más simple del algoritmo Deutsch-Jozsa) utilizando qubits efectivos de NMR, donde cada qubit corresponde al estado de espín nuclear de moléculas en solución, un modelo no direccionable individualmente y no escalable [CGK 1998]. En 1999 se realizó la primera implementación física de un qubit en el sentido moderno, un sistema de dos niveles coherente, controlable y físicamente aislado, basado en “caja de un solo par de Cooper” (*single-Cooper-pair box*) [NPT 1999]. Esta distinción refleja la diferencia fundamental entre un qubit efectivo, útil para demostraciones conceptuales, y un qubit físico, adecuado para arquitecturas escalables de computación cuántica.

2.2.2 Superposición y entrelazamiento

Las ideas sobre la superposición y el entrelazamiento cuántico surgieron en el contexto del desarrollo de la mecánica cuántica en las décadas de 1920 y 1930, en plena formación de esta nueva teoría que revolucionaba la física.

El concepto de superposición emerge con fuerza en la formulación ondulatoria de la mecánica cuántica, especialmente a partir del trabajo de Erwin Schrödinger en 1926 [Schrödinger 1926]. La función de onda que Schrödinger propuso describe un sistema cuántico no en un estado definido, sino como una combinación lineal de múltiples estados posibles, que sólo colapsa a un estado concreto al realizarse una medición. Este concepto desafió profundamente la intuición clásica, con Schrödinger expresando esta paradoja en su famoso “gato de Schrödinger”, un experimento mental para ilustrar cómo un sistema puede estar simultáneamente en dos estados opuestos hasta ser observado. La superposición se representa matemáticamente por la combinación lineal de sus estados individuales. Para el caso de dos estados en la base $\{|0\rangle, |1\rangle\}$:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

Hasta que se realiza una medida, la partícula se encuentra en esa superposición de estados con una probabilidad $\alpha^2 + \beta^2 = 1$, remarcando la naturaleza probabilística de los mismos. Al leer el qubit (medir el estado), éste se modifica y colapsa, pudiendo ser $|0\rangle$ con una probabilidad α^2 y $|1\rangle$ con una probabilidad β^2 . Sin embargo, antes de medirse no se tiene acceso a α o β con lo que los estados cuánticos desconocidos no son clonables o copiables.

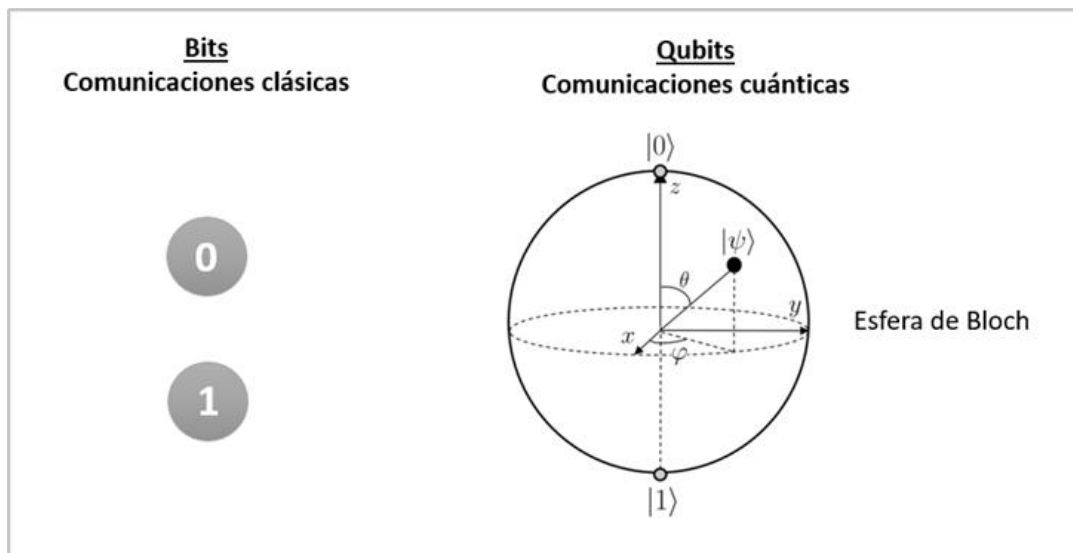


Figura 2-1 Representación gráfica de bits y qubits en la esfera de Bloch [adaptación de SB 2024].

El principio de superposición es fundamental para la computación cuántica, ya que permite procesar múltiples posibilidades a la vez y realizar cálculos paralelos.

El entrelazamiento cuántico es el fenómeno en el que dos o más partículas están correlacionadas de modo que el estado de una afecta instantáneamente al estado de la otra, independientemente de la distancia (Figura 2-2). Este fenómeno fue formalizado en 1935 por Albert Einstein, Boris Podolsky y Nathan Rosen en el artículo conocido como la paradoja EPR [EPR 1935]. Su objetivo era mostrar que la mecánica cuántica, con sus predicciones de correlaciones entre partículas separadas a distancia sin comunicación posible, era incompleta o debía ser revisada. Einstein tildó este fenómeno de “acción espeluznante a distancia”, porque parecía violar la causalidad relativista al implicar una conexión instantánea entre partículas separadas espacialmente. Ese mismo año, Erwin Schrödinger [Schrödinger 1935] introdujo el término entrelazamiento para describir esta propiedad fundamental de los estados cuánticos en los sistemas compuestos, enfatizando que las partículas entrelazadas forman un sistema unificado cuya descripción no puede factorizarse en estados individuales independientes.

El estado de dos qubits es la combinación lineal de todos los estados (2^2) de la base $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. Cuando dos partículas A y B interactúan y se entrelazan, el estado de una partícula está instantáneamente correlacionado con el estado de la otra de manera que sus estados cuánticos están ligados incluso cuando están separadas a largas distancias.

Durante décadas posteriores, estas ideas permanecieron en el ámbito teórico y fueron objeto de grandes debates. Sin embargo, el avance crucial llegó en 1964 cuando John Bell formuló matemáticamente las desigualdades que llevan su nombre [Bell 1964], demostrando que las correlaciones predichas por la mecánica cuántica y observadas en el entrelazamiento no admiten explicación mediante teorías clásicas basadas en variables ocultas locales. Bell demostró que, aunque las partículas entrelazadas muestran correlaciones muy fuertes cuando se miden en bases adecuadas, la violación de sus desigualdades es un fenómeno estadístico que solo se revela al comparar muchos resultados experimentales. Los experimentos realizados a partir de los años 70, y especialmente los de Alain Aspect¹⁰ en la década de 1980 [ADR 1982], confirmaron empíricamente estas predicciones, estableciendo el entrelazamiento como un fenómeno real y fundamental de la naturaleza cuántica. No

¹⁰ Algunas lagunas pendientes se cerraron experimentalmente en 2015 (<https://physicsworld.com/a/local-realism-is-dead-long-live-local-realism-exploring-loopholes-in-bell-tests/>)

obstante, durante décadas quedaron abiertas brechas o resquicios experimentales que se cerraron por tres grupos independientes en 2015 [Miller 2016].

Los cuatro estados de Bell, que representan las cuatro clases maximales de entrelazamiento bipartito, se formalizaron a partir del trabajo de John Bell en 1964 y se consolidaron como concepto estándar en la teoría de la información cuántica durante las décadas de 1980 y 1990: $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$; $|\Phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$; $|\Psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$; y el estado singlete $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$.

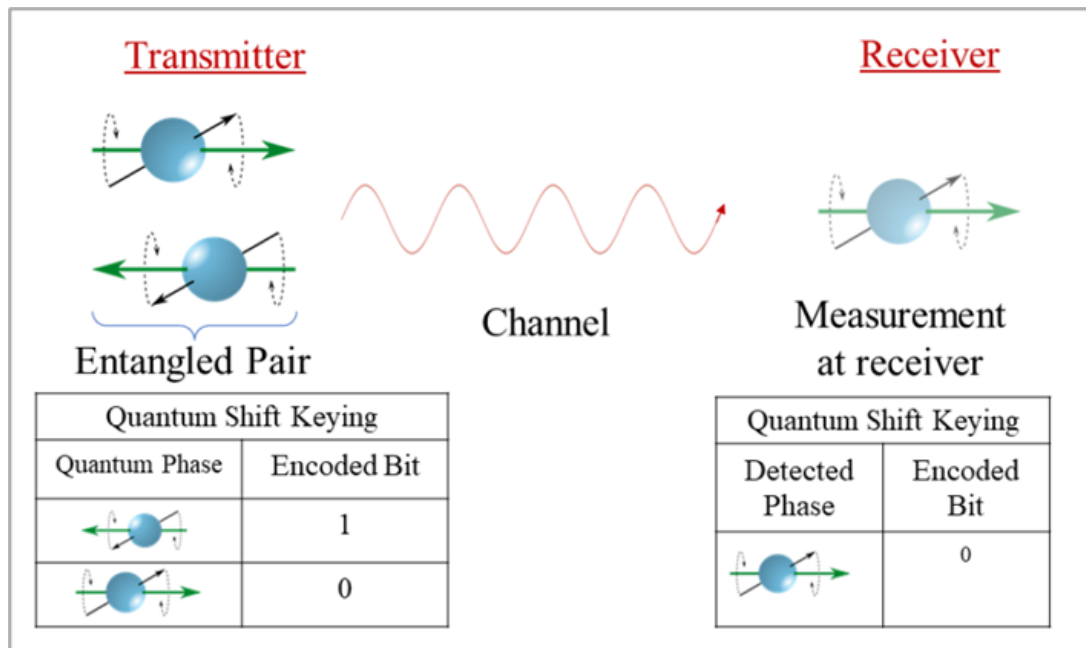


Figura 2-2 Esquema básico de comunicación cuántica, usando pares entrelazados [SB 2024].

El fenómeno de entrelazamiento interconecta los qubits no sólo de pares, sino de múltiples partículas, y su implicación sobre la computación y las comunicaciones cuánticas es la capacidad de procesar y transmitir en paralelo grandes cantidades de información. El entrelazamiento es la base de las comunicaciones cuánticas seguras y de varios protocolos de criptografía cuántica.

2.2.3 La medición cuántica y los teoremas de la no clonación y la no distribución

La medición en física clásica es un proceso aparentemente sencillo en el que el acto de medir no afecta al objeto que estamos midiendo. Podemos medir una propiedad de un sistema y a continuación, medir otra propiedad, y estar seguros de que la primera propiedad medida conserva su valor observado. Clásicamente, es fácil copiar información leyendo cada bit y escribiéndolo en otro sitio.

Éste no es el caso en la física cuántica en la que el acto de medición tiene un profundo efecto sobre la observación. Los qubits se encuentran en estados de superposición, y si los medimos, obtenemos $|0\rangle$ o $|1\rangle$ con cierta probabilidad. Por lo tanto, no se conoce el estado de superposición original porque la medida colapsa el estado a $|0\rangle$ o a $|1\rangle$, lo que significa que perdemos cualquier estado de superposición que tuviéramos originalmente, y con ella, cualquier entrelazamiento del que ese qubit pudiera ser parte. Por lo tanto, no es posible usar los mismos métodos conocidos y empleados en comunicaciones clásicas para el caso cuántico. La medición no solo revela información, sino que modifica el estado del sistema introduciendo la noción de colapso y de irreversibilidad en el proceso de observación. El

postulado de la proyección en mecánica cuántica establece que, tras una medición de un observable, el estado del sistema colapsa instantáneamente al autovector asociado al autovalor obtenido.

El Teorema de la no clonación establece que es imposible crear una copia de un estado cuántico desconocido, no siendo por tanto posible copiar los qubits ni usar los mismos mecanismos clásicos para amplificación de señal, retransmisión, etc. dado que están basados en la copia de datos.

El Teorema de la no distribución establece que los qubits no pueden ser distribuidos a múltiples receptores, aunque sí pueden ser transportados de un lugar a otro (a través de la teleportación cuántica).

2.2.4 La coherencia cuántica

La coherencia cuántica es una propiedad física fundamental de los sistemas cuánticos, que emerge del principio de superposición y se define formalmente como la capacidad de un sistema cuántico para mantener las relaciones de fase entre sus estados componentes durante un periodo de tiempo determinado. Los estados superpuestos mantienen una relación de fase específica que permite fenómenos de interferencia constructiva y destructiva, análogos a las ondas en un estanque que se alinean con precisión. Desde mediados de la década de 2010, la coherencia cuántica se ha formalizado rigurosamente dentro de la teoría de recursos cuánticos (*resource theory*). El trabajo fundacional de Baumgratz, Cramer y Plenio (2014) [BCP 2014] estableció las condiciones formales que deben satisfacer las medidas de coherencia.

La coherencia cuántica es inherentemente frágil ante las interacciones ambientales [Zurek 2003]. Los sistemas cuánticos reales no están aislados, sino que interactúan constantemente con su entorno (temperatura, vibraciones, campos externos) y estas perturbaciones externas inducen un proceso llamado decoherencia cuántica. La decoherencia opera a través de un mecanismo de entrelazamiento sistema-ambiente en el que una partícula cuántica coherente se acopla con partículas o campos ambientales, y la información sobre su estado cuántico se difunde hacia el entorno, propagándose a un vasto número de inaccesibles grados de libertad. El resultado es que la superposición colapsa, los patrones de interferencia desaparecen y el sistema cambia hacia un comportamiento puramente clásico. Las escalas temporales de este fenómeno son críticas, mientras que sistemas fotónicos pueden mantener coherencia durante segundos a minutos, los qubits superconductores típicamente mantienen coherencia entre 20 a 100 microsegundos, y los qubits de ión atrapado alcanzan de segundos a minutos (o incluso horas). Estos tiempos de coherencia representan actualmente el cuello de botella más restrictivo de los dispositivos cuánticos. La extensión y protección de la coherencia cuántica se ha convertido en el desafío central de la computación cuántica moderna. Para que un ordenador cuántico ejecute algoritmos útiles debe mantener la coherencia el suficiente tiempo que le permita realizar operaciones lógicas sin acumular errores ruidosos. Los fabricantes de tecnología cuántica trabajan en estrategias de mitigación de decoherencia, incluyendo aislamiento criogénico o blindaje electromagnético entre otras.

Más allá de la computación, la coherencia cuántica habilita aplicaciones en criptografía cuántica como la distribución cuántica de claves (QKD), basada en la imposibilidad de medir un sistema cuántico sin alterarlo, o los sensores y metrología cuántica, donde la sensibilidad extrema de las relaciones de fase coherentes permite detectar cambios ambientales minúsculos. Coherencia y entrelazamiento son operacionalmente equivalentes [SSDBA 2015, Zyga 2015], cualquier cantidad de coherencia puede convertirse en una cantidad igual de entrelazamiento mediante operaciones incoherentes. Esto significa que todo el conocimiento desarrollado sobre entrelazamiento puede aplicarse directamente al estudio de la coherencia.

2.2.5 La teleportación cuántica

La teleportación cuántica [Bennet 1993] permite la transferencia de información cuántica a largas distancias sin mover físicamente los qubits, para ello se envían bits clásicos. En el corazón de la teleportación cuántica está el fenómeno del entrelazamiento. Es importante notar que la teleportación cuántica no permite la comunicación más rápida que la luz, ya que el paso de la comunicación clásica asegura este límite. El proceso de la teleportación cuántica implica los siguientes pasos (Figura 2-3):

- Se prepara previamente un par de qubits entrelazados en uno de los cuatro estados de Bell máximamente entrelazados. El qubit A permanece con Alice (emisor) y el qubit B se envía a Bob (receptor). Este entrelazamiento es el recurso fundamental que habilita la teleportación.
- Alice posee un tercer qubit P en un estado desconocido $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, donde los coeficientes α y β son completamente desconocidos. Este es el estado que Alice desea transferir a Bob.
- Alice realiza una medición proyectiva conjunta sobre sus dos qubits (A y P), colapsándolos a uno de los cuatro estados de Bell. Esto genera dos bits clásicos de información que codifican el resultado. El qubit original P se destruye por colapso del postulado de proyección, confirmando el Teorema de No-Clonación. Alice obtiene solo 2 bits de información, lo que le permite saber cuál de las 4 correcciones debe aplicar Bob, pero no le permite conocer el estado original de P.
- Alice envía los 2 bits resultantes a Bob mediante un canal clásico (radio, fibra óptica). Estos bits viajan a una velocidad menor o igual que la de la luz (c), respetando la relatividad especial. Bob no puede proceder a la siguiente etapa hasta recibir estos bits.
- Dependiendo de los 2 bits recibidos, Bob aplica una de cuatro operaciones unitarias a su qubit B. Si el resultado fue el estado de Bell $|\Phi^+\rangle$, Bob aplica la identidad I; si $|\Phi^-\rangle$, aplica la compuerta Pauli-Z; si $|\Psi^+\rangle$, aplica Pauli-X; si $|\Psi^-\rangle$, aplica Pauli-Y. Tras esta corrección, el qubit B se encuentra definitivamente en el estado original $|\psi\rangle$.

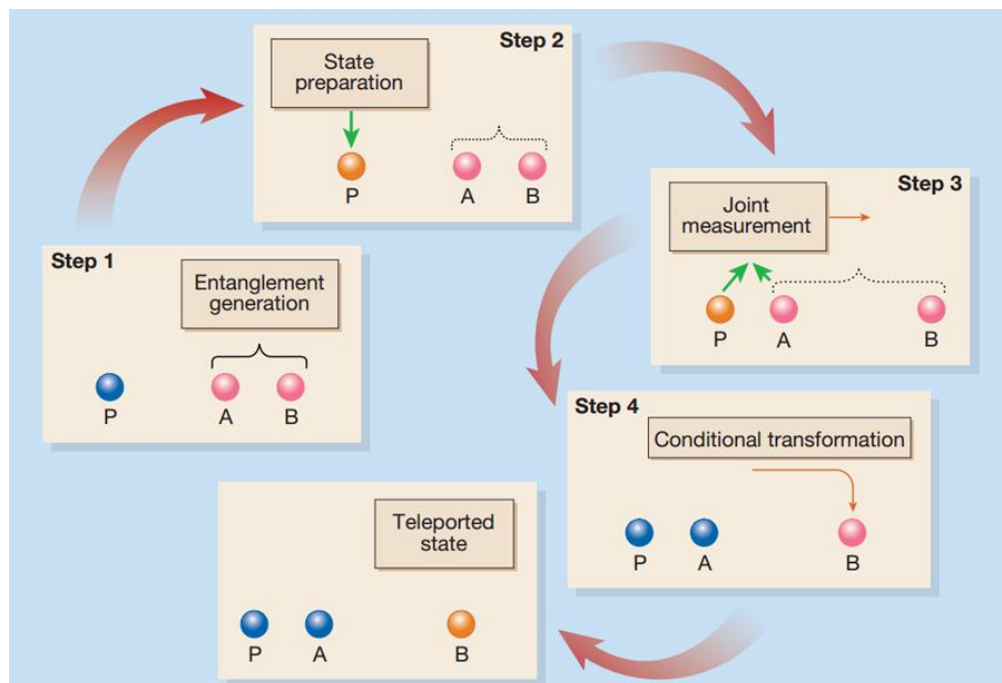


Figura 2-3 Pasos de la teleportación cuántica [Kimble 2008].

En resumen, la teleportación cuántica combina un qubit con el fenómeno del entrelazamiento y la transmisión de dos bits para transmitir la información del estado del qubit a otro lugar. Hay que tener en cuenta que α y β de la partícula P no se han medido nunca y que este qubit original desaparece del emisor y se transmite al receptor.

La teleportación cuántica puede usarse para establecer canales de comunicación seguros que son inmunes a la interceptación. Permite la creación de redes cuánticas distribuidas donde la información cuántica puede compartirse y procesarse en diferentes ubicaciones, pero requiere de repetidores cuánticos, que son necesarios para extender el alcance de las redes de comunicación cuántica.

2.3 Las tecnologías cuánticas

Los desarrollos científicos de la física cuántica, que se han gestado desde principios del siglo XX, han sido fundamentales para cambiar la comprensión de la naturaleza y han asentado las bases para numerosos desarrollos tecnológicos modernos.

Científicos y divulgadores contemporáneos que analizan la evolución histórica de la física cuántica y su impacto tecnológico han definido la existencia de dos revoluciones cuánticas [Latorre 2017]. Esta conceptualización ha emergido en las últimas dos décadas en el marco de la divulgación científica, la investigación aplicada y la planificación estratégica de la ciencia como forma de distinguir entre la revolución cuántica inicial (descubrimientos fundamentales y primeras aplicaciones), y la actual fase donde los avances permiten la explotación práctica y control experimental de propiedades cuánticas para una nueva generación de tecnologías.

2.3.1 Avances tecnológicos de la primera revolución cuántica

Los avances tecnológicos derivados de la primera revolución cuántica han sido decisivos para el progreso científico y tecnológico, y el desarrollo industrial del siglo XX. La descripción del mundo microscópico ha sido motor de una innovación tecnológica masiva, que ha moldeado desde la economía digital y la medicina, hasta la exploración espacial y la fabricación industrial cambiando la sociedad en pocas décadas.

La Primera Revolución Cuántica comenzó con los trabajos fundacionales de Max Planck, seguidos de los de Albert Einstein, Niels Bohr, Werner Heisenberg y Erwin Schrödinger que profundizaron en esta teoría quebrando el paradigma clásico a través de conceptos como la dualidad onda-partícula, la cuantización de la energía, la función de onda y el principio de incertidumbre. Esta primera revolución permitió comprender la estructura atómica, los espectros atómicos, y estableció las bases para una nueva rama de la física que describe el funcionamiento y las interacciones de la materia y la luz a escala microscópica. Este periodo sentó las bases para tecnologías innovadoras que emergieron más tarde, como los semiconductores y los transistores, los láseres, la microscopía electrónica, la Resonancia Magnética Nuclear (*Nuclear Magnetic Resonance*, NMR), los relojes atómicos, los superconductores y los supersólidos, la fotónica cuántica y las comunicaciones cuánticas, que han cambiado por completo la ciencia y la tecnología del siglo XX [Ron 2025, Ron 2025_2].

El entendimiento del comportamiento electrónico en sólidos y cristales a nivel cuántico fue fundamental para el desarrollo de semiconductores y transistores. La física cuántica explicó cómo los átomos se organizan en sólidos para formar bandas de energía, y cómo la existencia de la banda prohibida entre la banda de valencia y la banda de conducción determina la conductividad eléctrica de los materiales. Los semiconductores tienen una banda prohibida estrecha, lo que permite manipular su conductividad dopándolos con impurezas y de esa manera controlar el flujo de electricidad en los dispositivos [Kittel 1995]. John Bardeen, Walter Brattain y William Shockley (Laboratorios Bell) inventaron en 1947 el transistor de contacto puntual [BB 1948], un dispositivo semiconductor que

controlaba el flujo de corriente con un rendimiento superior y menor tamaño que las válvulas de vacío. El transistor revolucionó la electrónica, haciendo posible la miniaturización y creando la base para todos los dispositivos electrónicos modernos. Así tenemos el desarrollo del circuito integrado por Jack Kilby de Texas Instruments y Robert Noyce de Fairchild Semiconductor (1958) que integraba múltiples transistores en un solo chip, lo que permitió crear microprocesadores como el Intel 4004 (1971).

El diseño y funcionamiento de los láseres están directamente basados en la emisión estimulada, un fenómeno descrito por Einstein en su trabajo sobre la teoría cuántica de la radiación [Einstein 1917] y en la que describe los procesos de interacción de la luz con la materia: emisión espontánea, absorción y emisión estimulada. Durante las décadas siguientes, el conocimiento sobre la estructura atómica y la interacción luz-materia se profundizó, con experimentos que confirmaban estas predicciones teóricas. En 1950, Alfred Kastler propuso el método de bombeo óptico para lograr la inversión de población en un medio activo del láser [Kastler 1950], técnica que fue confirmada experimentalmente poco después. A principios de los años 50, los trabajos pioneros de Charles H. Townes y sus estudiantes consiguieron la primera generación y amplificación de radiación en microondas mediante emisión estimulada, creando el “máser” (*Microwave Amplification by Stimulated Emission of Radiation*) [GZT 1955]. En 1960, Theodore Maiman logró en los *Hughes Research Laboratories* (HRL) la primera emisión de luz láser utilizando un cristal de rubí como medio activo [Maiman 1960]. Posteriormente a comienzo y mediados de los años 60, técnicas como el “Q-switching” y el “mode-locking” permitieron obtener pulsos láser de nanosegundos y femtosegundos, abriendo su uso a múltiples aplicaciones. Los láseres se emplean en una inmensa variedad de aplicaciones, como las telecomunicaciones, la fabricación, la ciencia y la medicina, entre otras.

El concepto de dualidad onda-partícula fue clave para considerar a los electrones como “luz” de longitud de onda mucho menor que la luz visible, lo que implica mayor resolución en técnicas de microscopía electrónica frente a la óptica. En la década de 1930, investigadores como Ernst Ruska y Max Knoll desarrollaron el primer microscopio electrónico, empleando electrones acelerados para iluminar muestras bajo el fundamento teórico de que su longitud de onda dependía de su momento [RK 1932]. Ruska construyó el primer prototipo funcional, que fue mejorado con el tiempo para aumentar contraste y resolución hasta las escalas subnanométricas actuales. Los microscopios electrónicos han revolucionado la biología y la ciencia de materiales.

La Resonancia Magnética Nuclear (*Nuclear Magnetic Resonance*, NMR) se fundamenta en el comportamiento de los núcleos atómicos en campos magnéticos y la interacción de sus momentos magnéticos con ondas de radiofrecuencia. Isidor Isaac Rabi, en la década de 1930, fue pionero en medir el momento magnético de protones usando técnicas de resonancia magnética molecular [RZMK 1938]. En 1945, simultáneamente, pero de forma independiente, dos equipos dirigidos por Edward M. Purcell en Harvard [PTP 1946] y Felix Bloch en la Universidad de Stanford [BHP 1946] lograron observar la resonancia magnética de los protones en materiales sólidos y líquidos, respectivamente. El fenómeno, al que se dio el nombre de Resonancia Magnética Nuclear (MNR), representa un método para medir propiedades magnéticas nucleares con gran precisión. El desarrollo del espectrómetro de MNR permitió estudiar la estructura molecular detallada. Más adelante, en los años 70, Paul Lauterbur [Lauterbur 1973] y Peter Mansfield [Mansfield 1977] impulsaron el uso de la MNR para obtener imágenes médicas, dando origen a la resonancia magnética clínica, una técnica diagnóstica no invasiva de gran impacto en medicina.

La comprensión cuántica de las transiciones energéticas en átomos y sus propiedades magnéticas permitió diseñar dispositivos capaces de medir el tiempo y construir relojes atómicos con una exactitud sin precedentes. Isidor Isaac Rabi estableció con los trabajos en resonancia magnética nuclear (1930) el método experimental para medir las transiciones entre estados energéticos del núcleo atómico. En 1948, Harold Lyon construyó un primer reloj basado en las líneas de microondas del amoníaco (máser)

[Lombardi 2017], confirmando la utilidad de la vibración atómica para medir el tiempo, aunque con precisión limitada. Fue en 1955, cuando Louis Essen y Jack Parry diseñaron y construyeron el primer reloj atómico preciso basado en las transiciones del átomo de cesio-133 en el Laboratorio Nacional de Física (*National Physical Laboratory*, NPL) del Reino Unido [EP 1955]. Este reloj superó ampliamente la precisión de los relojes de cuarzo y cronometró la oscilación del átomo de cesio con una frecuencia exacta de 9.192.631.770 Hz. Este hito permitió redefinir el segundo en el Sistema Internacional de Unidades en 1967 basado en esta frecuencia atómica. Durante las décadas siguientes, se mejoraron los relojes atómicos utilizando otros elementos como rubidio e hidrógeno, logrando mayor estabilidad o menores consumos y tamaños. Más recientemente, se han desarrollado relojes atómicos de un solo ion [Rosenband 2008] y relojes ópticos basados en láser [Hinkley 2013, Brewer 2019], alcanzando precisiones de hasta un segundo en cientos de millones de años. En 2004, se creó un reloj atómico integrado en chip, con tamaño reducido y bajo consumo energético [Kitching 2018]. Los relojes atómicos son fundamentales para sistemas de navegación como el sistema de posicionamiento global vía satélite (*Global Positioning System*, GPS) y la sincronización global de redes de comunicación.

La primera revolución cuántica proporcionó el marco teórico fundamental para comprender fenómenos macroscópicos como la superconductividad, y más recientemente los supersólidos. En 1911, Heike Kamerlingh Onnes descubrió que, al enfriar mercurio a aproximadamente 4 K, la resistencia eléctrica desaparecía abruptamente [Bruyn 1997]. Esta transición marcó el comienzo del estudio del nuevo estado de la superconductividad al llegar a temperaturas del helio licuado. En 1933, Walther Meissner y Robert Ochsenfeld descubrieron que los superconductores expulsan el campo magnético interno cuando están en estado superconductor, fenómeno conocido como efecto Meissner [MO 1933]. Este hallazgo subrayó que la superconductividad es un nuevo estado termodinámico con propiedades físicas cuantificables distintas a las conductoras normales. La explicación cuantitativa completa no llegó hasta 1957 con la teoría BCS, propuesta por John Bardeen, Leon Cooper y Robert Schrieffer [BCS 1957], que explicó la superconductividad en términos de pares de electrones con interacción mediada por vibraciones de la red cristalina (pares de Cooper), formando un estado cuántico colectivo. La teoría BCS resolvió muchos enigmas y predijo la existencia de un gap energético superconductor visible en experimentos de túnel. Descubrimientos posteriores, como el efecto túnel Josephson (1962) [Josephson 1962] y el desarrollo de microscopios de efecto túnel [BR 1983], ampliaron las aplicaciones y la comprensión de los materiales superconductores. Aunque las teorías sobre supersólidos se han desarrollado desde hace décadas, el fenómeno en que un estado sólido exhibe propiedades superfluídicas (flujo sin viscosidad) a temperaturas extremadamente bajas, se ha demostrado recientemente [ZPM 2021]. Este fenómeno íntimamente relacionado con la mecánica cuántica y la condensación de Bose-Einstein tiene potenciales aplicaciones en tecnologías de energía, transporte magnético y computación cuántica.

El desarrollo de la fotónica cuántica surge como disciplina en la década de 1960 con la invención del láser por Theodore Maiman [Maiman 1960]. El láser permitió un haz de luz monocromática, coherente y de alta intensidad, ideal para la transmisión de información a largas distancias. El término “fotónica” empezó a usarse a finales de los 60 y se consolidó en las décadas siguientes como el estudio y aplicación de la manipulación de la luz para funciones electrónicas y de procesamiento de información. En la década de 1970, la invención del diodo láser [Hall 1962, Nathan 1962] y el desarrollo de fibras ópticas dopadas [KKM 1970] abrieron el camino para la transmisión de información mediante luz con pérdidas mínimas, revolucionando las telecomunicaciones. A partir de los años 80, se implementaron sistemas de comunicación óptica en redes de telecomunicaciones utilizando láseres y fibras ópticas¹¹. Se desarrollaron tecnologías tales como la multiplexación por división de longitud de onda (*Wavelength Division Multiplexing*, WDM) que permiten la transmisión

¹¹ <https://www.ebsco.com/research-starters/history/first-commercial-test-fiber-optic-telecommunications>

simultánea de múltiples canales en una fibra [Mur 2024]. La fotónica es la columna vertebral de las telecomunicaciones modernas mediante comunicaciones ópticas.

2.3.2 Avances tecnológicos de la segunda revolución cuántica

La Segunda Revolución Cuántica surgió cuando Richard Feynman propuso en 1982 la posibilidad de emplear los principios de la mecánica cuántica para la construcción de ordenadores y sistemas de computación [Feynman 1982]. Esta revolución, que comenzó a materializarse con los primeros qubits entre 1998 y 2001 y ha tenido un desarrollo notable la última década, se caracteriza por la capacidad de controlar y manipular estados cuánticos individuales y sistemas diminutos a nivel atómico y subatómico. La Segunda Revolución Cuántica ha implicado avances no solo teóricos sino también experimentales, facilitados por tecnologías que permiten la manipulación precisa de qubits, la creación y control de entrelazamiento cuántico y la coherencia cuántica. Esto ha abierto el camino al desarrollo de tecnologías cuánticas modernas como la computación cuántica, las comunicaciones cuánticas o los sensores cuánticos, entre otras [Acín 2018].

La segunda revolución representa la transición de la comprensión teórica a la manipulación tecnológica práctica de las propiedades cuánticas de la materia y energía, pero también encuentran su base teórica en la teoría de la información cuántica, que proporciona las herramientas para entender y maximizar el procesamiento y la transmisión de información en sistemas cuánticos [Wilde 2021, NC 2010]. La computación cuántica utiliza algoritmos que aprovechan la superposición y el entrelazamiento para resolver problemas fuera del alcance de la computación clásica. Las comunicaciones cuánticas permiten la transmisión segura de información mediante el uso de principios físicos frente a las amenazas de la criptografía convencional. Los sensores cuánticos mejoran la precisión y sensibilidad en mediciones físicas fundamentales. Los siguientes apartados profundizan en la teoría de la información cuántica, la computación cuántica y las comunicaciones cuánticas.

2.4 La información cuántica

Nuestra vida está inmersa en una presencia abrumadora de información que se transmite y almacena continuamente. En 1984, el tráfico global de Internet era apenas de 15 gigabytes por mes¹², mientras que en 2025 alcanza los 522 exabytes¹³ por mes¹⁴. La capacidad de almacenamiento instalada globalmente era en 1986 de 2,6 exabytes, mientras que en 2025 se estima en 10 zettabytes^{15,16}. Asimismo, la estimación de datos generados, capturados, replicados y consumidos en 2025 a escala global se considera en alrededor de 175 zettabytes [SI 2020]. Este crecimiento exponencial de la información disponible y almacenada plantea el desafío fundamental de formalizar cómo se cuantifica, se transmite y se interpreta la información en sistemas cada vez más complejos. La magnitud de datos que circula hoy día requiere de marcos conceptuales rigurosos que permitan distinguir entre datos brutos y contenido informativo real, así como optimizar los procesos de codificación y transmisión en infraestructuras globales de comunicación.

La teoría de la información propuesta por Claude Shannon en 1948 [Shannon 1948] formalizó el concepto de la información desde una perspectiva estadística, de utilidad en el tratamiento de la información en la ingeniería de los sistemas de computación y comunicaciones. La teoría establece el marco matemático para la codificación, transmisión y medición de la información (Figura 2-4).

¹² <https://blogs.cisco.com/sp/the-history-and-future-of-internet-traffic>

¹³ 10¹⁸ bytes (EB).

¹⁴ <https://www.ibisworld.com/united-states/bed/internet-traffic-volume/88089/>

¹⁵ 10²¹ bytes (ZB).

¹⁶ <https://rivery.io/blog/big-data-statistics-how-much-data-is-there-in-the-world/>

Shannon introdujo entre otros conceptos la entropía de la información como la medida de la incertidumbre o imprevisibilidad de un mensaje, permitiendo calcular el “valor informativo” del mensaje en función de su probabilidad de aparición: cuanto menos probable es un mensaje, mayor es su cantidad de información. Así, si un sistema puede recibir dos mensajes A y B, con una ocurrencia respectiva del 99% y del 1% de las veces, recibir el mensaje A no aporta valor informativo ya que es esperable, frente a B que es poco probable y aporta información que no se esperaba. La incertidumbre es máxima cuando todos los mensajes son igual de probables (50%), siendo el valor informativo por mensaje más alto que cuando uno de ellos es muy frecuente. Además, Shannon definió el bit como unidad elemental de información y demostró los límites teóricos en la capacidad de transmisión óptima en canales afectados por ruido, con el objetivo de lograr una comunicación eficiente y fiable.

Esta teoría (compresión de datos, capacidad de canal, entropía, etc.) tiene aplicaciones fundamentales en los sistemas de información y comunicaciones:

- La compresión de datos (ZIP, JPEG o MP3) codifica con menos bits los datos más frecuentes optimizando la transmisión y el almacenamiento.
- Los sistemas de comunicaciones (redes, telefonía o internet) transmiten información de la manera lo más eficientemente posible, acercándose al límite teórico de Shannon, usando menos recursos y afrontando el ruido de los canales.
- La criptografía y seguridad de la información codifica los datos con la máxima incertidumbre para dificultar su obtención por parte de terceros.
- Los algoritmos y modelos de la inteligencia artificial usan la teoría de la información para calcular la ganancia de información, seleccionar características y tomar decisiones óptimas en situaciones de incertidumbre.
- El concepto de información inspirado en la teoría de Shannon ha sido extensamente adoptado en biología para describir el “contenido de información” de los genes y del ADN, aunque su interpretación y alcance han sido objeto de debate [Segal 2015].

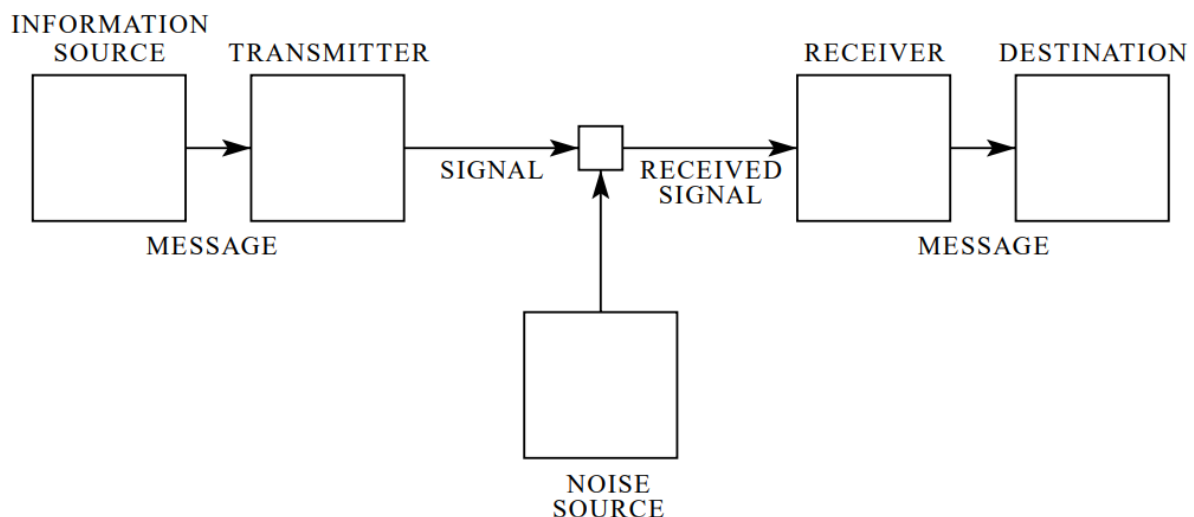


Figura 2-4 Diagrama esquemático de un sistema de comunicación general [Shannon 1948].

La ciencia de la información cuántica se ocupa de definir y tratar la información cuando está codificada, procesada y transmitida usando qubits cuánticos en vez de bits clásicos, e incorpora fenómenos, como la superposición, la interferencia y el entrelazamiento, que no tienen equivalente

clásico [Wilde 2021, NC 2010]. Así, la ciencia de la información cuántica tiene como objeto estudiar la naturaleza de la información a nivel cuántico combinando estos dos importantes desarrollos del siglo XX, la física cuántica y la teoría de la información. Benjamin Schumacher formuló en 1995 [Schumacher 1995] el primer teorema para sistemas cuánticos, análogo al de codificación de canal sin ruido de Shannon, en el que una fuente cuántica puede comprimirse de forma análoga a una fuente clásica pero con diferencias fundamentales en la representación de estados. El qubit y la entropía de von Neumann [Neumann 1932] cumplen roles equivalentes al bit y a la entropía de Shannon en la teoría clásica, aunque la teoría cuántica generaliza y modifica los conceptos clásicos apareciendo conceptos como la información mutua y la entropía condicional y coherente. La teoría cuántica desarrolla formalmente los sistemas cuánticos, los canales cuánticos, las mediciones irreversibles, la no-clonación, la capacidad de transmisión, la decoherencia, la codificación óptima y los límites fundamentales para transmisión y procesamiento de información usando medios cuánticos, así como los protocolos para corrección de errores, la protección frente a ataques externos y la transmisión fiable sobre canales cuánticos ruidosos, tomando como base las propiedades de la superposición y el entrelazamiento de la mecánica cuántica. Conceptualmente, existe una diferencia sustancial entre la información clásica (estudiada por Shannon) y la cuántica (estudiada por Schumacher y desarrollada en la llamada *Quantum Shannon Theory*). Cada una usa la entropía correspondiente (Shannon para clásica, von Neumann para cuántica), difiere en su tratamiento y representación, pero comparte el rigor formal, las herramientas matemáticas y la aspiración a definir límites y capacidades en sistemas físicos reales.

2.5 La computación cuántica

2.5.1 Los ordenadores cuánticos

Los ordenadores cuánticos son un ejemplo de cómo se implementan físicamente la manipulación de la información cuántica sobre máquinas reales. La computación cuántica, lejos de ser una única tecnología, abarca una diversidad de arquitecturas que reflejan distintas estrategias para manipular y procesar qubits. El ordenador cuántico integra la unidad de procesamiento cuántico (*Quantum Processing Unit*, QPU) o chip cuántico, que es el componente central que contiene los qubits y realiza las operaciones cuánticas, los sistemas de control y electrónica asociada, la infraestructura criogénica (si es necesaria), el software de control y programación, los interfaces de entrada/salida y en muchos casos, la integración con computación clásica. No obstante, los términos ordenador cuántico y QPU se usan a menudo de forma intercambiable en el contexto comercial y de difusión, y en ocasiones cuando mencionamos el *Nighthawk* de IBM lo llamamos ordenador cuántico o procesador cuántico en lugar de QPU.

Existen diversas implementaciones físicas de qubits que pueden dar soporte a diferentes arquitecturas de computación:

- Qubits superconductores: Utilizan circuitos de Josephson a temperaturas de milikelvins. Son rápidos (operan en nanosegundos) y escalables, pero sufren de tiempos de coherencia cortos (decenas de microsegundos) y problemas de escalabilidad por el cableado de control y la criogenia, aunque es probable que los qubits superconductores estén entre los primeros en alcanzar el umbral de corrección de errores que permita la computación cuántica escalable. Empresas que trabajan en esta tecnología son IBM, Google, D-Wave Systems, Quantum AI, IQM, Alice & Bob o la española Kilimanjaro siendo los tipos de qubits más utilizados.
- Qubits de iones atrapados: Emplean átomos cargados suspendidos en campos electromagnéticos, que son manipulados con láseres o microondas. Ofrecen tiempos de coherencia muy largos (segundos a horas) y fidelidades de puerta superiores al 99.9%, aunque

las operaciones son más lentas (microsegundos a milisegundos) y la escalabilidad es compleja. IonQ y Quantinuum comercializan este tipo de ordenadores.

- Qubits fotónicos: Usan fotones manipulados con óptica lineal (divisores de haz, desfases, detectores). Funcionan a temperatura ambiente a alta velocidad y son ideales para redes de fibra óptica. Implementar puertas de dos qubits es un reto técnico. Empresas en esta tecnología son PsiQuantum, Xanadu, Quandela y Quix Quantum.
- Qubits de átomos neutros (qubits de Rydberg): Utiliza átomos no cargados (rubidio y cesio) atrapados en pinzas ópticas, entrelazados mediante interacciones de Rydberg. Permite arquitecturas flexibles y escalables, aunque tiene complejidad técnica y debe mejorar la fidelidad de las puertas. En esta tecnología trabajan empresas como QuEra Computing y Pasqal.
- Qubits de espín en silicio y otros materiales: Usan espines de electrones o nucleares controlados por campos magnéticos y pulsos de microondas. Su principal ventaja es la compatibilidad con la tecnología CMOS (*Complementary Metal-Oxide-Semiconductor*), lo que permite una escalabilidad industrial, aunque aún existen desafíos en la uniformidad de fabricación y el escalado de la interacción de dos qubits. QuTech, Intel, Dirac y HRL trabajan con estas tecnologías.

Las principales modalidades y arquitecturas de ordenadores cuánticos¹⁷ están dominadas por los QPUs basados en puertas, seguidos de la computación tipo *annealing* o adiabática, aunque también existen otros tipos que se encuentran en un estado de madurez tecnológica más baja:

- La computación cuántica basada en puertas (*Gate-Based*)¹⁸.

La computación cuántica basada en puertas es el corazón de la visión moderna de una máquina cuántica universal, un procesador que no solo manipula ceros y unos, sino que explora simultáneamente múltiples posibilidades gracias a la superposición, el entrelazamiento y la interferencia. También llamado modelo de circuito cuántico o computación cuántica digital, es el equivalente cuántico de una computadora digital clásica que opera bajo las reglas de la mecánica cuántica. Cualquier operación o algoritmo cuántico puede descomponerse en una coreografía precisa de puertas unitarias, formando circuitos cuánticos. Es universal, con el conjunto adecuado de puertas, como Hadamard, T y CNOT, se puede construir cualquier operación cuántica imaginable, de manera análoga a las puertas NAND en la computación clásica. Además es reprogramable, cambiar el algoritmo no requiere modificar el hardware, solo la secuencia de puertas. Y es compatible con la corrección de errores cuánticos, que es una pieza clave para escalar hacia máquinas tolerantes a fallos.

Formalizado en los años 90 por DiVincenzo y Shor, el modelo de puertas ha sido el terreno fértil donde florecieron algoritmos como el de Shor y el de Grover, que prometen superar con creces las capacidades de los ordenadores clásicos. La teoría del modelo de puertas ha dado lugar a procesadores reales de diferentes modalidades físicas (superconductores, iones atrapados, fotones, átomos neutros, qubits en silicio) construidos por empresas como IBM, Google, IonQ y PsiQuantum, entre otras. Los qubits actuales son frágiles, sensibles al ruido y a la decoherencia, y la profundidad de los circuitos está limitada por el tiempo de coherencia y la corrección de errores.

La teoría de la tolerancia a fallos en computación cuántica es el marco que permite construir máquinas cuánticas fiables a partir de componentes intrínsecamente ruidosos y frágiles. Una máquina tolerante a fallos es capaz de detectar y corregir errores durante la ejecución de un algoritmo, sin perder la información cuántica. Para ello emplea codificación lógica, en la que

¹⁷ <https://postquantum.com/quantum-modalities/taxonomy-modalities/>

¹⁸ <https://postquantum.com/quantum-modalities/gate-based-universal-quantum/>

un qubit lógico se representa mediante muchos qubits físicos; la corrección activa de errores, mediante la realización de mediciones auxiliares que detectan errores sin colapsar el estado cuántico; y a través del establecimiento de umbrales de corrección, que determinan cuál es el error máximo admisible por operación (puerta lógica) que permite realizar cálculos arbitrariamente largos y precisos usando corrección de errores. Google y IBM emplean el código de superficie, que establece que se puede codificar un qubit lógico con un error suficientemente bueno (10^{-15}) para cálculos extendidos en una matriz 2D del orden de 1000 qubits físicos con umbrales de corrección menores al 1%.

- Computación cuántica por *Annealing* y computación cuántica adiabática¹⁹.

La computación cuántica por *annealing* u ordenadores *quantum annealing* (*Quantum Annealing Computing*, QAC) y la computación cuántica adiabática (*Adiabatic Quantum Computing*, AQC), que constituyen la categoría de ordenadores cuánticos analógicos, utilizan la evolución gradual de un sistema cuántico para resolver problemas de optimización. Ambos parten de un estado inicial simple y lo transforman lentamente en otro que codifica el problema, guiando al sistema hacia su estado de mínima energía según el teorema adiabático.

AQC es un modelo teórico universal, equivalente en capacidad al modelo de puertas. QAC es su versión práctica, implementada en dispositivos como los de D-Wave, orientados a problemas específicos como el de optimización binaria cuadrática sin restricciones (*Quadratic Unconstrained Binary Optimization*, QUBO) o los modelos de Ising (ver apartado 2.5.3). Aunque comparten fundamentos, difieren en su alcance: AQC asume sistemas ideales y sin ruido, mientras que QAC opera en condiciones reales con sistemas abiertos y temperaturas finitas. Esto hace que QAC sea más robusto pero menos preciso, pudiendo terminar en estados excitados. Además, QAC no es universal, ya que los dispositivos actuales solo permiten Hamiltonianos restringidos. Pese a estas limitaciones, QAC ha demostrado utilidad en planificación, logística y aprendizaje automático, especialmente en esquemas híbridos con algoritmos clásicos. Tanto QAC como AQC afrontan retos como la complejidad de la inserción de problemas y la falta de corrección de errores eficaz, pero ofrecen alternativas complementarias a la computación basada en puertas, con potencial también como simuladores cuánticos y herramientas de muestreo. Empresas como D-Wave lideran el desarrollo de hardware QAC.

- La computación cuántica topológica²⁰.

La computación cuántica topológica propone un enfoque distinto para procesar información cuántica. En lugar de aplicar corrección activa de errores, codifica los qubits en estados exóticos de la materia que son intrínsecamente resistentes al ruido. Un ejemplo son los modos cero de Majorana en superconductores topológicos, cuasipartículas predichas por Ettore Majorana en 1937 [Majorana 1937], cuyos estados de energía cero aparecen en pares en los extremos de nanohilos o en defectos del material.

La clave de estos qubits es que la información se codifica de forma no local entre pares de modos Majorana, lo que proporciona protección frente a perturbaciones locales. Las operaciones cuánticas se realizan mediante el entrelazamiento controlado de estos modos, donde el resultado depende únicamente del recorrido topológico y no de los detalles físicos del movimiento. Esta propiedad los convierte en una de las propuestas más prometedoras para lograr computación cuántica escalable y tolerante a fallos.

¹⁹ <https://postquantum.com/quantum-modalities/annealing-adiabatic/>

²⁰ <https://postquantum.com/quantum-modalities/topological-quantum-computing/>

Microsoft, a través de Station Q, ha invertido de forma destacada en esta línea, aunque aún no se ha demostrado de manera concluyente ni el entrelazamiento de Majoranas ni el funcionamiento completo de un qubit topológico. El grupo de Delft, apoyado por Microsoft, retractó en 2021 por falta de rigor su publicación de 2018 en Nature [Zhang 2018] sobre la observación definitiva de modos cero de Majorana. En 2024, investigadores de QuTech lograron generar Majoranas en un plano bidimensional [Haaf 2024]. Si su implementación se confirma, los qubits topológicos podrían reducir drásticamente la necesidad de corrección de errores, aunque su realización experimental sigue siendo uno de los mayores desafíos abiertos en física cuántica.

- La computación cuántica basada en medidas (*Measurement Based Quantum Computing*, MBQC)²¹.

La computación cuántica basada en medidas o computación cuántica unidireccional reemplaza las puertas lógicas por mediciones adaptativas realizadas sobre un estado de clúster previamente preparado. Este estado generado consiste en una gran red 2D de qubits entrelazados que actúa como un recurso universal, es decir, contiene en potencia cualquier computación cuántica. El cálculo se lleva a cabo midiendo secuencialmente qubits individuales. La base de cada medición se ajusta según los resultados anteriores, y estas mediciones “dirigen” la información a través del clúster, consumiendo el entrelazamiento como si fuera un recurso de un solo uso. De ahí el término unidireccional: una vez medido, el estado ya no puede reutilizarse.

MBQC es especialmente adecuada para sistemas fotónicos, donde los clústeres pueden generarse y medirse de forma natural, aunque también existen demostraciones en iones atrapados y qubits superconductores. Una ventaja importante es que separa la preparación del recurso entrelazado del proceso de cálculo, lo que permite generar el estado de clúster de forma anticipada (incluso con corrección de errores integrada) y ejecutar después el algoritmo mediante mediciones rápidas. Aunque MBQC es equivalente en poder computacional al modelo de puertas, su aplicación práctica está limitada por la dificultad de generar y mantener estados de clúster de gran tamaño.

El apartado 4.2.1 presenta una revisión de las principales empresas implicadas en el desarrollo de ordenadores cuánticos.

2.5.2 La complejidad computacional

Para entender cuándo la computación cuántica puede superar a la clásica, es esencial clasificar formalmente qué problemas son inherentemente difíciles y cómo los ordenadores cuánticos pueden resolverlos de una manera diferente a como lo hacen los ordenadores clásicos. Un problema computacional es una tarea o pregunta cuyo objetivo es obtener una solución, como ordenar una lista de números o determinar si un número es primo, mientras que un algoritmo es un procedimiento general y dependiente solo del método (no del hardware) para resolver dicho problema de forma sistemática. La implementación concreta de un algoritmo en un lenguaje de programación específico se realiza con un programa.

La complejidad computacional es el área de la computación que se encarga de estudiar y clasificar problemas según los recursos requeridos (principalmente tiempo y memoria) para solucionarlos con algoritmos sobre distintos modelos matemáticos de cómputo, como la máquina de Turing [Hidary 2019, Wong 2022]. La notación “O grande” es una herramienta matemática utilizada para describir cómo crece el tiempo de ejecución o el uso de recursos de un algoritmo en función del tamaño de la

²¹ <https://postquantum.com/quantum-modalities/measurement-based-mbqc/>

entrada n , especialmente cuando este tamaño se vuelve muy grande. n es la cantidad de datos que el algoritmo debe procesar. Por ejemplo, si un algoritmo ordena una lista, n sería el número de elementos en esa lista, y si el algoritmo opera sobre una matriz, n podría ser el número de filas o columnas. Por ejemplo, si un algoritmo de ordenamiento de una lista requiere a lo sumo $5n + 3$ operaciones para una lista de tamaño n , se dice que su complejidad es $O(n)$ ya que el término dominante es lineal en n . Formalmente decimos que una función $f(n)$ es $O(g(n))$, si existen constantes c y n_0 tales que $f(n) \leq c \cdot g(n)$ para todo $n \geq n_0$. Esto significa que para entradas suficientemente grandes, $f(n)$ no crece más rápido que una constante multiplicada por $g(n)$.

La notación “O grande” describe cómo crece el tiempo de ejecución o el uso de memoria del algoritmo a medida que n aumenta, permitiendo comparar la eficiencia de diferentes algoritmos de manera independiente de detalles específicos de implementación o hardware. Los órdenes de magnitud más comunes en complejidad computacional se pueden clasificar y comparar directamente. La Tabla 2-1 muestra cómo diferentes funciones “O grande” crecen conforme aumenta el tamaño de entrada n . Un problema $O(n^2)$ es manejable para $n = 1.000$, mientras que un problema $O(2^n)$ es imposible para $n > 30$ incluso en supercomputadoras.

Notación	Comportamiento	Ejemplo ($n = 1000$)
$O(1)$	constante	~1 operación
$O(\log n)$	logarítmico	~10 operaciones
$O(n)$	lineal	~1.000 operaciones
$O(n \log n)$	lineal-logarítmica	~10.000 operaciones
$O(n^2)$	cuadrático	~1 millón de operaciones
$O(n^3)$	cúbico	~mil millones de operaciones
$O(2^n)$	exponencial en base 2	~ 10^{300} operaciones
$O(e^n)$	exponencial en base e	~ 10^{434} operaciones
$O(n!)$	factorial	~ 10^{2568} operaciones

Tabla 2-1 Ordenes de magnitud en complejidad computacional.

Las clases de complejidad (Figura 2-5) permiten clasificar problemas como “fáciles” o “difíciles” para diferentes modelos de computación:

- Los problemas P (tiempo polinomial) pueden ser resueltos eficientemente por una computadora clásica en tiempo polinomial. Si el problema tiene tamaño n , existe un algoritmo que lo resuelve en tiempo proporcional a n^k para alguna constante k . Problemas P típicos son el ordenamiento de listas, la prueba de si un número es primo y la programación lineal, que tienen algoritmos conocidos de complejidad polinomial.
- Los problemas NP (tiempo polinomial no determinístico) son aquellos cuyas soluciones pueden ser verificadas eficientemente en tiempo polinomial, aunque encontrar la solución puede requerir mucho más tiempo. Si alguien propone una solución se puede verificar rápidamente si es correcta, pero es difícil encontrar esa solución de partida. Problemas de tipo NP son el

problema del viajante, Sudoku o la factorización de grandes números. Resolver la factorización de 2048 o un Sudoku es difícil, pero verificar si una solución conocida es correcta es muy fácil.

Todo problema resoluble es verificable ($P \subseteq NP$), pero se desconoce si $P = NP$.

- Los problemas NP-duros son aquellos a los que todos los problemas NP se pueden reducir en un tiempo polinomial. Si se puede resolver un problema NP-duro rápidamente, se podría resolver cualquier problema NP rápidamente.

Un problema NP-duro puede estar fuera de NP ($NP \subseteq \text{NP-duro}$), siendo potencialmente más difícil que cualquier problema en NP.

- Los problemas NP-completo cumplen dos condiciones:
 - Están en NP, ya que su solución puede verificarse en tiempo polinomial.
 - Es NP-duro, ya que todos los problemas en NP se pueden reducir a él.

Todos los problemas NP-completos son NP-duros, pero no al revés, y no todos los problemas NP-duros están en NP ($\text{NP-completo} = NP \cap \text{NP-duro}$).

- PSPACE (espacio polinomial) reúne los problemas que pueden resolverse usando solo una cantidad polinomial de memoria, sin restricción expresa sobre el tiempo. Un ejemplo es determinar la existencia de una estrategia ganadora en el ajedrez en un tablero grande.

Todo problema verificable cabe en memoria polinomial, y como ya sabemos todo problema resoluble es verificable ($P \subseteq NP \subseteq \text{PSPACE}$).

- BQP (tiempo polinómico cuántico con error acotado) representan los problemas que pueden ser resueltos eficientemente por una computadora cuántica en tiempo polinomial con un margen de error acotado. La factorización de números primos y de logaritmos discretos mediante el algoritmo de Shor es un ejemplo de problema en BQP, pues no se conocen algoritmos eficientes para resolver el problema en los ordenadores clásicos mientras en los cuánticos sí.

Se desconoce la posición de BQP (¿Es igual a NP? ¿Está dentro de PSPACE? ¿Se puede comparar?).

Problema	O grande	Clase de Complejidad
Ordenar listas de números	$O(\log n)$	P
Factorización de enteros	$O\left(\exp\left((c + o(1))(\log n)^{1/3}(\log \log n)^{2/3}\right)\right)$	NP
Problema del viajante (TSP) decisión	$O(n!)$ (algoritmo de fuerza bruta)	NP-completo
Determinación de estrategia ganadora en ajedrez	Tiempo no acotado polinomial, uso polinomial de espacio	PSPACE
Factorización con algoritmo cuántico de Shor	$O(n^3)$	BQP

Tabla 2-2 Problema, O grande y clase de complejidad computacional.

Para catalogar un determinado problema en una categoría de clase de complejidad computacional se sigue un proceso de pasos iterativos para comprobar si está en P, NP, NP-duro o NP-completo.

La notación “O grande” está directamente relacionada con las clases de complejidad, ya que la asignación de un problema a una clase computacional se basa en el análisis de la eficiencia de los algoritmos que lo resuelven expresada mediante “O grande” (Tabla 2-2). Por ejemplo, un problema pertenece a la clase P si existe un algoritmo que lo resuelve en tiempo polinomial respecto al tamaño de la entrada, es decir, su complejidad temporal es $O(n^k)$ para algún entero k . Esto incluye algoritmos con complejidad $O(n)$, $O(n^2)$, $O(n^3)$,... y también $O(\log n)$, $O(n \log n)$ o $O(1)$.

El problema de factorizar números enteros grandes en sus factores primos es un ejemplo clásico de problema en la clase NP. Si te proporcionan los factores, se puede verificar rápidamente (en tiempo polinomial) que su producto es el número original, pero no se conoce ningún algoritmo clásico eficiente para encontrar los factores en todos los casos. Los mejores algoritmos clásicos conocidos tienen una complejidad subexponencial, como es el caso del algoritmo de factorización general (*General Number Field Sieve*) que tiene una complejidad aproximada:

$$O\left(\exp\left((c + o(1))(\log n)^{1/3}(\log \log n)^{2/3}\right)\right),$$

donde n es el número a factorizar, c es una constante y $o(1)$ (“o pequeña”) es un término que tiende a cero a medida que n crece.

El algoritmo de Shor (espacio BQP) resolverá la factorización de enteros en tiempo polinomial $O(n^3)$ en un futuro ordenador cuántico tolerante a fallos con millones de qubits lógicos, donde n es el número de bits necesarios para representar el entero. Dado que la seguridad de la criptografía RSA reside en la dificultad clásica de factorizar enteros grandes, la computación cuántica constituye una amenaza estratégica para todos los sistemas basados en esta criptografía.

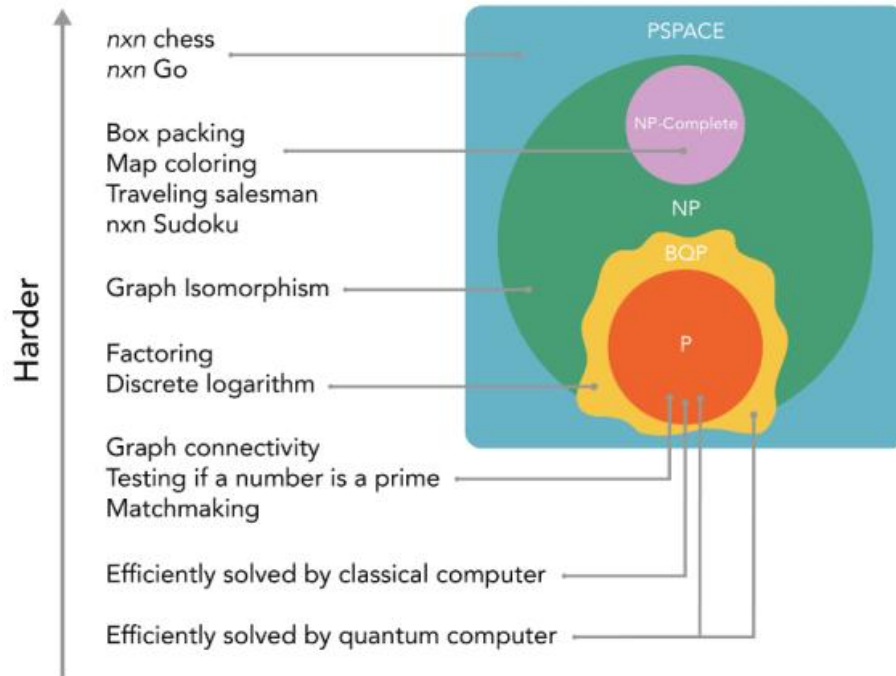


Figura 2-5 Clases de complejidad computacional [Hidary 2019].

El problema del viajante (*Traveling Salesman Problem*, TSP) consiste en encontrar el recorrido más corto en que visita una serie de ciudades exactamente una vez y regresa al punto de partida. La

complejidad computacional de este problema es $O(n!)$ en su versión clásica para un algoritmo de fuerza bruta donde n es el número de ciudades ($n!$ recorridos a considerar) o $O(2^n)$ para algunos algoritmos más avanzados. No se conoce ningún algoritmo clásico que lo resuelva en tiempo polinomial, aunque se puede verificar una solución propuesta (comprobar la longitud de un recorrido dado) en tiempo polinomial $O(n)$. El TSP se asigna a la clase NP-completo porque cumple con dos condiciones, su solución puede verificarse eficientemente, pero no se conoce un algoritmo eficiente para encontrarla en todos los casos, y su complejidad de tiempo crece mucho más rápido que cualquier polinomio en n .

Los ordenadores cuánticos no son universalmente más rápidos, sólo ofrecen ventajas para ciertos problemas específicos. Los ordenadores cuánticos superan exponencialmente a los clásicos en la brecha entre lo que es NP y lo que es BQP ($NP \cap BQP$), pero no existe evidencia de algoritmos capaces de resolver problemas NP-completos en tiempo polinomial.

2.5.3 Algoritmos cuánticos

Los ordenadores cuánticos aprovechan fenómenos como la superposición y el entrelazamiento para explorar simultáneamente múltiples soluciones o manipular información de manera no clásica. Son especialmente eficientes en problemas de factorización, búsqueda no estructurada y simulación de sistemas cuánticos, siempre que existan algoritmos cuánticos específicos que exploten la estructura del problema y permitan una reducción significativa en la complejidad computacional respecto a los métodos clásicos. Además, los ordenadores cuánticos pueden simular sistemas cuánticos naturales de manera mucho más eficiente que los clásicos, lo que es fundamental en química cuántica y física de materiales.

El algoritmo de Deutsch-Jozsa es uno de los primeros algoritmos cuánticos que demuestran una ventaja sobre los clásicos. Resuelve el problema de determinar si una función booleana es constante o balanceada, es decir, produce el mismo valor para todas las entradas o la mitad de las veces uno y la otra mitad cero. En un ordenador clásico se requieren hasta $2^{n-1} + 1$ consultas para estar seguro, mientras que el algoritmo cuántico lo resuelve con una sola consulta siendo su complejidad $O(1)$. Este algoritmo se ejecuta en ordenadores cuánticos universales, como los superconductores o de iones atrapados, y muestra una ventaja exponencial en la consulta al oráculo²², aunque el problema no es difícil en la práctica para grandes n .

El algoritmo de Shor puede factorizar números enteros grandes en sus factores primos en tiempo polinomial respecto al número de bits n con $O(n^3)$ o similar. Shor corre en ordenadores cuánticos universales y tiene aplicaciones directas en criptografía, ya que rompe sistemas como RSA. Es uno de los algoritmos que justifican el interés en la computación cuántica escalable. La factorización es un ejemplo de la clase BQP, problemas resolubles eficientemente por una computadora cuántica.

El algoritmo de Grover busca en una base de datos no ordenada. Clásicamente se requieren $O(n)$ consultas para encontrar un elemento especial entre n posibilidades, pero Grover lo logra en $O(\sqrt{n})$ consultas, lo que representa una ventaja cuadrática. Este algoritmo se ejecuta en ordenadores cuánticos universales y es útil para problemas de búsqueda y optimización. Aunque no resuelve problemas NP-completos en tiempo polinomial, sí acelera búsquedas exhaustivas.

El algoritmo de transformada de Fourier cuántica (*Quantum Fourier Transform*, QFT) es la versión cuántica de la transformada de Fourier discreta y se utiliza como subrutina en varios algoritmos, como el de Shor o la estimación de fase. Su implementación exacta requiere $O(n^2)$ puertas para n qubits, mientras que la transformada de Fourier clásica necesita $O(N \cdot \log N)$ operaciones para

²² Un oráculo es una función de caja negra que puede ser consultada pero cuya estructura interna no se conoce. En teoría de complejidad de consultas, la ventaja de un algoritmo se mide por el número de consultas al oráculo.

$N = 2^n$ puntos. El QFT puede ejecutarse en ordenadores cuánticos universales y constituye un componente esencial para algoritmos que explotan información de fase, aunque no sustituye a la FFT clásica en tareas de análisis espectral convencional.

El algoritmo de Bernstein-Vazirani busca una cadena secreta s tal que una función oráculo devuelve el producto escalar entre s y la entrada. Clásicamente, se requieren n consultas para encontrar s , pero el algoritmo cuántico lo logra con una sola consulta $O(1)$. Este algoritmo corre en ordenadores cuánticos universales y es relevante para problemas de búsqueda de patrones y criptografía. Aunque la mejora es polinomial, ilustra cómo la superposición cuántica permite extraer más información en menos pasos.

El algoritmo de Simon resuelve el problema de encontrar una cadena secreta s que enmascara las entradas de una función oráculo, donde $f(x) = f(y)$ si y solo si $x = y \oplus s$. Clásicamente se requieren $O(2^{n/2})$ consultas, pero el algoritmo cuántico lo resuelve en $O(n)$ consultas, logrando una ventaja exponencial. Corre en ordenadores cuánticos universales y fue el primer algoritmo en demostrar una separación exponencial entre la computación clásica y cuántica en la consulta al oráculo.

No se conoce ningún algoritmo cuántico que resuelva el problema del viajante (TSP) en tiempo polinomial. Sin embargo, el algoritmo de optimización aproximada cuántica (*Quantum Approximate Optimization Algorithm*, QAOA) [Hidary 2019, GPB 2023, Classic 2024] puede encontrar soluciones cercanas a la óptima mediante heurísticas aproximadas, aunque sin garantizar soluciones exactas polinomiales. Por tanto, aunque el TSP no tiene solución polinomial conocida en ordenadores cuánticos, sí puede beneficiarse de aceleraciones cuánticas mediante algoritmos aproximados. El QAOA consiste en un algoritmo variacional híbrido clásico-cuántico que es implementable en los ordenadores cuánticos NISQ²³ actuales. A diferencia de otros algoritmos que requieren corrección de errores completa, QAOA puede ejecutarse en máquinas cuánticas con cientos de qubits sin necesidad de emplear códigos de corrección sofisticados. El algoritmo se aplica a una amplia clase de problemas de optimización combinatoria NP-duros, incluyendo *MaxCut*, problemas de satisfactibilidad máxima (Max-SAT), programación cuadrática, problemas de grafos y desafíos logísticos, convirtiéndolo en una herramienta de propósito general. El algoritmo funciona alternando iterativamente dos operadores: uno que codifica la función objetivo del problema, y otro que permite explorar diferentes soluciones candidatas. El circuito se construye en capas sucesivas (controladas por un parámetro de profundidad p), donde cada capa está gobernada por parámetros ajustables que el optimizador clásico irá modificando. El optimizador clásico ajusta iterativamente estos parámetros mediante un ciclo que típicamente requiere entre cientos y miles de evaluaciones de la función de costo, dependiendo del método de optimización empleado. En cada iteración, el sistema cuántico es evaluado mediante mediciones y los resultados son procesados por el optimizador clásico para proponer nuevos parámetros que mejoren progresivamente la aproximación hacia la solución óptima. El algoritmo es teóricamente escalable en profundidad (el aumento del número de capas mejora la calidad de la solución), aunque en la práctica el ruido y la complejidad de los circuitos pueden limitar estas mejoras.

Los algoritmos de simulación cuántica tienen aplicabilidad en sistemas cuánticos que son intratables clásicamente, como la simulación de reacciones químicas y dinámica molecular, el entendimiento de fenómenos biológicos, el diseño de fármacos y la búsqueda de nuevos materiales. Mientras que un ordenador clásico requeriría exponencialmente de más memoria y tiempo para simular sistemas cuánticos complejos, los ordenadores cuánticos pueden preparar y evolucionar directamente estados cuánticos. Los algoritmos de simulación cuántica (p.e. Trotter-Suzuki o simuladores variacionales) permiten modelar la evolución temporal de sistemas cuánticos bajo un

²³ Los ordenadores cuánticos NISQ (*Noisy Intermediate-Scale Quantum*) son procesadores de escala intermedia con entre decenas y cientos de qubits, que aún sufren ruido y carecen de corrección de errores completa, constituyendo la fase actual de desarrollo de la computación cuántica.

Hamiltoniano específico, resolviendo la ecuación de Schrödinger de manera más eficiente que los métodos clásicos. El método Trotter-Suzuki aproxima el operador de evolución temporal e^{-iHt} dividiéndolo en pequeños pasos secuenciales, aplicando exponenciales de términos individuales del Hamiltoniano de manera ordenada. Cada paso evoluciona el estado durante un tiempo $\Delta t = T/N$, y repitiendo este proceso N veces se aproxima la evolución completa. Por su parte, los simuladores variacionales como el solucionador variacional de autovalores cuántico (*Variational Quantum Eigensolver*, VQE) adoptan un enfoque híbrido clásico-cuántico donde un circuito cuántico parametrizado prepara un estado *ansatz*²⁴, se mide el valor esperado del Hamiltoniano, y un optimizador clásico ajusta iterativamente los parámetros para minimizar la energía. Ambos métodos son fundamentales en química cuántica y física de materiales, permitiendo simular estructuras electrónicas moleculares, transiciones de fase cuánticas y dinámicas de no-equilibrio con precisión que los ordenadores clásicos no pueden alcanzar.

Muchos problemas prácticos de optimización combinatoria NP-duros, como enrutamiento, logística o diseño de circuitos, pueden reformularse en un formato matemático especial llamado optimización binaria no restringida (*Quadratic Unconstrained Binary Optimization*, QUBO), o de forma equivalente en el modelo de Ising, originario de la física estadística. Esta reformulación es fundamental porque permite mapear problemas del mundo real a arquitecturas cuánticas especializadas y a algoritmos variacionales. En QUBO, el objetivo es asignar valores binarios (0 o 1) a un conjunto de variables para minimizar o maximizar una función que combina términos lineales e interacciones cuadráticas. El modelo de Ising describe la misma estructura desde una perspectiva física en la que una red de “spins” pueden estar en estado $+1$ o -1 e interactúan entre sí. Ambas formulaciones son matemáticamente equivalentes, QUBO es el lenguaje del optimizador y Ising el del físico. La equivalencia entre QUBO e Ising permite traducir un problema de optimización clásico a un formato procesable por dispositivos cuánticos. Habitualmente, el valor binario 0 se asocia al spin -1 y el valor 1 al spin $+1$, estableciendo un puente directo entre la optimización discreta y los modelos físicos. Los ordenadores *quantum annealing*, como los de D-Wave, trabajan directamente con el modelo de Ising. En lugar de puertas lógicas, codifican el problema como un paisaje energético cuya solución óptima corresponde al estado de mínima energía. El *annealer* evoluciona desde un estado inicial sencillo hacia configuraciones de spins de baja energía, aprovechando el efecto túnel cuántico para evitar quedar atrapado en óptimos locales. Los algoritmos variacionales en ordenadores cuánticos de puertas, como QAOA, también emplean formulaciones QUBO o Ising. En estos casos, el Hamiltoniano de costo se construye a partir del problema y el circuito cuántico explora el paisaje energético mediante iteraciones clásico-cuánticas. Así, tanto los *annealers* como los algoritmos variacionales comparten un mismo marco matemático donde QUBO e Ising proporcionan un lenguaje unificado para expresar problemas de optimización combinatoria en contextos cuánticos, ya sea en dispositivos de *annealing* o en máquinas de puertas.

Algoritmos como la versión cuántica de las Máquinas de Vectores de Soporte (*Quantum Support Vector Machines*, QSVM), la versión cuántica de las Máquinas de Boltzmann (*Quantum Boltzmann Machines*, QBM), la versión cuántica de las Redes Generativas Antagónicas (*Quantum Generative Adversarial Networks*, QGAN) y la versión cuántica de las Redes Neuronales Convolucionales (*Quantum Convolutional Neural Networks*, QCNN) son iniciativas emergentes dentro del aprendizaje automático cuántico que aprovechan las propiedades únicas de los sistemas cuánticos para mejorar y acelerar modelos tradicionales de aprendizaje máquina (*Machine Learning*, ML). Estos algoritmos se ejecutan preferentemente en ordenadores cuánticos universales, incluyendo plataformas superconductoras y de iones atrapados, que permiten la manipulación escalable y eficiente de qubits para implementar circuitos parametrizados de manera robusta. Aunque aún se encuentran en fase

²⁴ El estado *ansatz* (del alemán configuración inicial) es un estado cuántico parametrizado que restringe la búsqueda de la solución a un problema cuántico específico, a un subconjunto manejable de estados cuánticos definidos.

teórica y experimental, estos métodos remarcen el potencial de la computación cuántica para revolucionar el aprendizaje automático, proporcionando aceleraciones polinomiales o exponenciales y el análisis y la generación de datos complejos en determinadas tareas donde los métodos clásicos enfrentan limitaciones computacionales. La investigación evoluciona en algoritmos híbridos cuántico-clásicos y mejoras en la mitigación de ruido, apuntando a aplicaciones prácticas en visión por ordenador, procesamiento del lenguaje natural y química computacional.

2.5.4 La supremacía cuántica

No se trata solo de cuántos qubits tiene un ordenador cuántico, sino de qué tan bien puede usarlos en conjunto para ejecutar algoritmos complejos. Los qubits pueden ser propensos a errores y de corta duración, por lo que unos pocos qubits de alta fidelidad pueden ser más valiosos que muchos con ruido. La supremacía cuántica se define como el momento en que un ordenador cuántico logra realizar una tarea específica que ningún ordenador clásico puede resolver en un tiempo razonable. El ordenador cuántico resolvería un problema computacionalmente complejo en un tiempo superpolinomial con respecto al mejor algoritmo conocido de un ordenador clásico. Históricamente, los primeros demostradores de supremacía han utilizado tareas específicamente diseñadas para ser intratables clásicamente pero tratables cuánticamente, típicamente problemas sin aplicación práctica directa. A partir de 2024, la comunidad ha alcanzado la ventaja cuántica práctica en problemas del mundo real con valor científico o comercial documentable.

La demostración de esta supremacía y su benchmarking difieren según la arquitectura de computación empleada. En la computación cuántica digital (basada en puertas), la supremacía se ha evaluado inicialmente mediante problemas matemáticos abstractos diseñados para ser difíciles clásicamente, como el muestreo de circuitos aleatorios (*Random Circuit Sampling*, RCS), utilizando métricas de fidelidad estadística como la Métrica de la Entropía Cruzada (*Cross-Entropy Benchmarking*, XEB) o el Volumen Cuántico (*Quantum Volume*, QV). Por el contrario, en la computación cuántica analógica (basada en *annealing*), la ventaja se busca mediante la resolución directa de problemas de optimización o simulación física de gran escala inabordables para la supercomputación clásica.

La evaluación objetiva del rendimiento cuántico y la demostración de la supremacía cuántica han evolucionado principalmente durante la década de 2020, estableciendo marcos rigurosos para validar ventajas computacionales reales en optimización, simulaciones complejas y *quantum machine learning*²⁵. El desarrollo de métricas holísticas basadas en evidencias experimentales sólidas ha transformado el campo desde las demostraciones teóricas hasta el desarrollo de aplicaciones prácticas con impacto industrial. En los últimos 10 años, los *benchmarks* más relevantes han sido el muestreo de circuitos aleatorios (RCS) [Arute 2019] y el Volumen Cuántico (QV)²⁶ [CBSNG 2019, Wack 2021]. El RCS ejecuta circuitos cuánticos aleatorios y compara la distribución de resultados con lo que predice la mecánica cuántica, que se simula en una supercomputadora. El QV usa circuitos aleatorios para determinar el tamaño máximo de circuito que se puede ejecutar con fidelidad suficiente. El RCS se complementa con la Métrica de la Entropía Cruzada (XEB) [Arute 2019], que es una técnica estadística que mide la fidelidad comparando la distribución de probabilidad experimental con la ideal estimada por simulaciones clásicas.

Los circuitos cuánticos aleatorios (RCS) [BFNV 2018, Arute 2019, Mullane 2020] están diseñados para evaluar la capacidad de un sistema cuántico de generar distribuciones que son difíciles de simular clásicamente, evaluando así la supremacía cuántica. Los circuitos aleatorios permiten evaluar el rendimiento general del hardware y se pueden adaptar para probar diferentes aspectos del sistema,

²⁵ <https://postquantum.com/quantum-computing/quantum-computing-benchmarks/>

²⁶ <https://medium.com/qiskit/what-is-quantum-volume-anyway-a4dff801c36f>

como decoherencia, errores correlacionados, y capacidad de paralelización. Se diseñan y compilan específicamente en un entorno de software clásico (en las capas de control y programación del sistema cuántico) aplicando puertas cuánticas aleatorias sobre los qubits físicos del ordenador. Cada ciclo del circuito suele incluir una capa de puertas de un solo bit y una capa de puertas de dos qubits. La compilación transforma la descripción abstracta del circuito de esas puertas cuánticas aleatorias, en un conjunto de instrucciones específicas y compatibles con el hardware del ordenador cuántico. Una vez compilado, el circuito se envía al hardware cuántico para su ejecución física sobre los qubits.

El muestreo del circuito aleatorio (*random circuit sampling*, RCS) consiste en la medida del estado final varias veces para obtener una distribución de las cadenas de bits o secuencias binarias (*bitstrings*) (Figura 2-6). En un caso ideal (sin ruido), la distribución de probabilidad esperada de los *bitstrings* generados a la salida sigue una distribución exponencial típica de los sistemas caóticos (distribución de Porter-Thomas). El RCS establece si se ha cruzado el umbral de lo clásicamente simulable pero no ofrece soluciones aplicables, y además un dispositivo puede sobresalir en RCS, pero fallar en algoritmos estructurados. Adicionalmente, para verificar los resultados del RCS se requieren simulaciones clásicas intensivas.

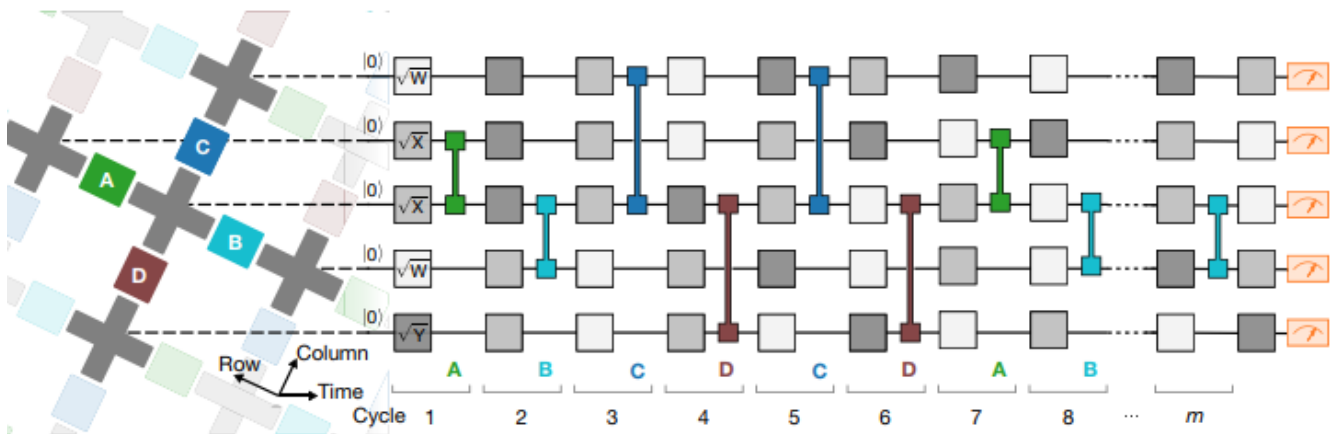


Figura 2-6 Ejemplo de un circuito usado en el experimento de Sycamore de Google [Arute 2019].

La técnica XEB²⁷ mide principalmente la fidelidad de circuitos cuánticos aleatorios [ZVBL 2020], es decir, qué tan cerca está la distribución de salida del circuito cuántico real respecto a la distribución ideal (teórica) que se espera del mismo circuito sin errores. Se ejecuta un circuito cuántico aleatorio en el dispositivo físico varias veces para obtener una colección de *bitstrings* (resultados de medición). Cuando es posible, se calcula la probabilidad ideal de cada bitstring usando simulación clásica y se compara con la frecuencia observada en el experimento. La fidelidad de XEB se define como $F_{XEB} = 2^n \langle P(x_i) \rangle_k - 1$, donde n es el número de qubits, $P(x_i)$ es la probabilidad de bitstring x_i calculada para un circuito cuántico ideal y el promedio se hace sobre los *bitstrings* observados. Si $F_{XEB} = 1$, las muestras provienen de un circuito cuántico ideal, sin errores, y si $F_{XEB} = 0$, equivale a valores puramente aleatorios, ruido blanco. Los valores de F_{XEB} entre 0 y 1 corresponden a probabilidades en que no haya habido errores mientras se ejecutaba el circuito, es decir no se comporta aleatoriamente. Valores de $F_{XEB} > 0,1\%$ en circuitos suficientemente complejos se consideran suficientes para demostrar la supremacía cuántica ya que indica que el procesador está generando distribuciones de salida que no pueden ser replicadas por simulaciones clásicas en tiempos razonables.

²⁷ <https://postquantum.com/quantum-computing/quantum-computing-benchmarks/>

En octubre de 2019, Google anunció que su procesador cuántico digital Sycamore²⁸, compuesto por 53 qubits superconductores, había alcanzado la llamada “supremacía cuántica” con un $F_{XEB} > 0,22\%$. El equipo de Google AI Quantum logró ejecutar una tarea RCS en solo 200 segundos, una operación que estimaron llevaría 10.000 años en el superordenador clásico más potente [Arute 2019]. Este experimento, validado por instituciones como NASA y Oak Ridge, demostró que un dispositivo cuántico programable puede superar a los algoritmos clásicos en una tarea específica, marcando un hito en la era NISQ. La técnica de verificación XEM permitió confirmar que Sycamore estaba generando *bitstrings* con una distribución estadística coherente con la interferencia cuántica esperada. Google cruzaba el umbral de la supremacía frente a otros sistemas de IBM, D-Wave y los ordenadores de iones atrapados que no lo habían logrado todavía. IBM cuestionó la magnitud del logro, proponiendo simulaciones clásicas más eficientes que reducían la duración a 2,5 días, aunque eso no negaba que el consenso de que Sycamore había demostrado una ventaja cuántica clara. En 2021, un equipo de la Universidad de Ciencia y Tecnología de China (*University of Science and Technology of China*, USTC) obtuvo un $F_{XEB} \approx 0,036\%$ para un ordenador superconductor de 60 qubits (Zuchongzhi 2.1) ejecutando circuitos aleatorios de 24 capas [Zhu 2021]. A pesar de esta pequeña fidelidad, se estimó que el supercomputador Sunway tardaría 10.000 años de computación frente a las 4 horas del ordenador cuántico.



Figura 2-7 Evolución del volumen cuántico con los diferentes procesadores de IBM²⁹.

El QV es una métrica holística del rendimiento de computadoras cuánticas de escala intermedia y ruidosa (NISQ) que engloba la mejor fidelidad de las operaciones de las puertas cuánticas, la mayor conectividad entre qubits y la mejor capacidad de los algoritmos de control y mitigación de ruido que

²⁸ <https://postquantum.com/industry-news/google-sycamore/>

²⁹ <https://www.ibm.com/quantum/blog/quantum-volume-256>

corrijan errores. Para llevar a cabo la medida QV se construyen circuitos modelo aleatorios de igual ancho en número de qubits m y profundidad en número de capas de puertas d ($m = d$) con puertas de dos qubits y permutaciones de qubits. Esto permite evaluar el rendimiento del sistema en condiciones donde la complejidad crece cuadráticamente, ya que más qubits implican más interacciones posibles.

La determinación del QV consiste en comparar los resultados de las simulaciones clásicas de un circuito ideal con los obtenidos del RCS. Para ello se simula el circuito idealmente (sin errores) y se calcula la distribución de probabilidad de todos los *bitstrings* posibles. Se determina el valor mediano de esas probabilidades y se define el conjunto de *heavy outputs* como aquellos *bitstrings* cuya probabilidad es mayor que la mediana. Posteriormente se ejecuta el circuito en el dispositivo real varias veces y se mide el estado final de todos los qubits obteniendo un *bitstring* como resultado. Si más de dos tercios de las salidas generadas se asemejan a las simuladas (*heavy output*), se considera estadísticamente que el dispositivo produce resultados más probables que la mediana esperada [Matteo 2025]. Se define el volumen cuántico como $V_Q = 2^{\min(m,d)} = 2^m$. Si un dispositivo puede ejecutar correctamente circuitos aleatorios de 5 qubits con profundidad 5, pero falla al intentar con 6 qubits y profundidad 6, entonces su volumen cuántico es $V_Q = 2^5 = 32$.

El QV es una forma práctica de comparar diferentes arquitecturas cuánticas y optimizar circuitos que ha sido adoptada como estándar por empresas como IBM, Honeywell (Quantinuum) e IonQ, que han reportado avances significativos en sus valores de QV como prueba de mejora tecnológica. IBM³⁰, por ejemplo, ha estado duplicando su Volumen Cuántico cada año (Figura 2-7) como parte de su hoja de ruta hacia la “ventaja cuántica”. El último ordenador cuántico en el que se ha medido el Volumen Cuántico ha sido el Quantinuum System Model H2, que alcanzó un QV récord³¹ de $2^{23} = 8.388.608$ en mayo de 2025 manteniendo alta fidelidad y conectividad total entre todos los qubits. La computadora cuántica Quantinuum System Model H2 actualmente cuenta con 56 qubits físicos basados en iones atrapados. Así, de los 56 qubits físicos disponibles, al menos 23 cumplieron las condiciones de baja tasa de error, coherencia y buena conectividad para ejecutar los circuitos aleatorios requeridos por el benchmark. El QV ha sido la métrica dominante para evaluar computadoras cuánticas durante la era NISQ, pero tiene los problemas de su dependencia de la simulación clásica y la limitación a circuitos aleatorios cuadrados (igual anchura y profundidad). Asimismo no proporciona una medida directa de la fidelidad como el XEB, sino de la superación de un umbral estadístico para ejecutar circuitos aleatorios con fidelidad suficiente, ni tiene en cuenta la velocidad de ejecución.

La simulación clásica de circuitos modelo aleatorios está directamente relacionada con la complejidad computacional que crece exponencialmente con el número de qubits y la profundidad del circuito, al necesitar almacenar 2^n amplitudes complejas. Clásicamente la simulación es $O(2^n)$, mientras que el ordenador cuántico puede ejecutarlos en tiempo polinomial. La métrica clave es comparar el tiempo de ejecución, si el ordenador cuántico completa la tarea en minutos y el clásico necesitaría miles de años se demuestra ventaja cuántica. Las simulaciones clásicas de circuitos cuánticos aleatorios llegan hasta unos 20-30 qubits de forma eficiente, y requieren mayores recursos de supercomputación a medida que aumenta el número de qubits siendo ~50 qubits el límite de capacidad práctica [Chen 2018, ZVBL 2020]. Simular un circuito de 50 qubits con profundidad 50 puede requerir petabytes de memoria y años de cómputo, incluso en supercomputadoras.

Estamos entrando en una fase de desarrollo de ordenadores cuánticos en la que la corrección de errores (*Quantum Error Correction*, QEC) permite construir ordenadores cuánticos tolerantes a fallos (*Fault-Tolerant Quantum Computing*, FTQC), capaces de ejecutar algoritmos complejos de forma estable y escalable. A medida que se ha ido entrando en la era QEC, métricas como RCS, QV o XEB han perdido relevancia. Empresas como IBM, IonQ, D-Wave Google o Microsoft y entidades

³⁰ <https://www.ibm.com/quantum/blog/quantum-volume-256>

³¹ <https://www.quantinuum.com/blog/quantum-volume-milestone>

académicas han propuesto diferentes métricas de rendimiento a nivel de sistema, orientadas a aplicaciones, volumétricas u holísticas y específicas de procesadores cuánticos tolerantes a fallos [MKG 2024, SEEAA 2025]. El grupo de trabajo IEEE P7131³² desarrolla activamente estándares para métricas de rendimiento de computación cuántica, cubriendo metodologías de evaluación tanto de hardware como de software. Estas iniciativas buscan establecer protocolos reproducibles a través de diferentes plataformas de computación cuántica. La maduración de la computación cuántica requiere de métricas de evaluación de múltiples facetas ampliando las métricas abstractas de fidelidad de los circuitos a las orientadas a la capacidad práctica de resolución de problemas.

Un circuito cuántico de alta fidelidad funciona correctamente y genera distribuciones cercanas a la ideal, y uno de baja fidelidad tiene errores acumulados por decoherencia, ruido en las puertas y lecturas imprecisas entre otras causas. La fidelidad decae exponencialmente con el número de qubits (cientos hasta ~1000 qubits) y la profundidad del circuito si no se aplica corrección de errores, aumentando el tiempo de resolución útil y proporcionando ventaja a los algoritmos clásicos que puedan simular eficientemente. La corrección de errores requiere de un número mínimo de qubits físicos (del orden de cientos a miles) para codificar un solo qubit lógico y fidelidades por debajo de ciertos umbrales (~0.1% de error por puerta) para que la corrección de errores sea efectiva [JNTM 2014]. La escalabilidad produce una transición entre la era sin corrección de errores (*Noisy Intermediate-Scale Quantum*, NISQ) y la era con corrección de errores (*Quantum Error Correction*, QEC) que extiende la ventaja cuántica y permite ejecutar algoritmos útiles y escalables (como Shor, simulación cuántica, etc.).

En 2020, IonQ propuso la métrica qubits algorítmicos³³ (*Algorithmic Qubits*, AQ) para evaluar cuántos qubits de un sistema cuántico pueden ser utilizados efectivamente en algoritmos reales, no solo en circuitos aleatorios. A diferencia del QV, que mide la capacidad general del hardware, AQ se enfoca en la utilidad práctica de los qubits requeridos para ejecutar algoritmos como la Transformada de Fourier Cuántica, Grover, simulaciones químicas o rutinas de optimización con alta fidelidad y resultados correctos. Por ejemplo, si un sistema tiene $AQ = 20$, significa que puede ejecutar algoritmos de 20 qubits con cientos de puertas entrelazadas y aún producir resultados confiables. Otras empresas cuestionan esta métrica como ajustada a la aplicación y más fácil de pasar que QV y la falta de estandarización y consenso sobre algoritmos y umbrales.

El propósito principal de las métricas de aplicación es medir la capacidad de la pila completa de un ordenador cuántico para ejecutar un caso de uso o algoritmo específico [Hashim 2025]. Algunas métricas de aplicación encapsulan aplicaciones de alto nivel, algoritmos variacionales y subrutinas claves. Algunas métricas de aplicación son SupermarQ, QASMBench y las desarrolladas por el *Quantum Economic Development Consortium* (QED-C). Todas se basan en ideas similares, pueden ser implementadas en ordenadores cuánticos de diferente arquitectura (basados en puertas, *quantum annealers*, etc.) y cubren un amplio rango de aplicaciones. La Figura 2-8 muestra la evaluación de las métricas SupermarQ y QED-C para una variedad de circuitos de aplicación de diferente anchura (número de qubits) y profundidad sobre un ordenador cuántico superconductor *ibm_guadalupe*. Cada punto representa la ejecución de una única métrica de aplicación y el color la puntuación alcanzada por la misma. El rendimiento cae con el número de qubits posiblemente porque el ordenador tiene una conectividad limitada.

Las métricas de aplicación cuántica representan una panorámica integral del potencial computacional de los ordenadores cuánticos, evaluando una diversidad notable de algoritmos que abarcan desde demostraciones teóricas clásicas hasta problemas prácticos de impacto real. Entre los mismos se encuentran los algoritmos tutoriales como el algoritmo de Deutsch-Jozsa y la Transformada

³² <https://standards.ieee.org/initiatives/quantum-standards-activities/>

³³ <https://postquantum.com/quantum-computing/quantum-computing-benchmarks/>

de Fourier Cuántica, que sirven como fundamentos educativos, junto con el histórico algoritmo de Shor, y algoritmos de optimización combinatoria como *MaxCut*, el problema del viajante y ajuste máximo en grafos. Paralelamente, la evaluación de simulación cuántica abarca sistemas fermiónicos complejos, modelos de Hubbard, simulaciones en física de materia condensada como el modelo BCS superconductor [BCS 1957], y aplicaciones en química cuántica que buscan calcular estados fundamentales de moléculas.

Complementando estas categorías clásicas, las métricas modernas incorporan algoritmos variacionales como QAOA para optimización, el algoritmo HHL [HHL 2009] para resolución de sistemas lineales, implementaciones de corrección cuántica de errores con códigos fase y mediciones intermedias, además de preparación de estados altamente entrelazados como estados GHZ y pruebas de desigualdades de Bell [GHZ 2007]. La métrica QED-C integra específicamente simulaciones de dinámicas de sistemas iónicos fermiónicos, problemas de grafos, sistemas lineales y factorización de números primos, proporcionando así una evaluación holística que integra la pila completa de software cuántico en problemas inspirados en aplicaciones reales. Esto permite comparar diferentes ordenadores cuánticos no solo en componentes aislados sino en su capacidad para resolver paradigmas computacionales. Para realizar comparaciones detalladas, las métricas de aplicación miden el tamaño o dimensión del problema a resolver, la fidelidad o precisión de la solución comparada con la ejecución cuántica ideal, el tiempo total de ejecución (*runtime*) y la escalabilidad o degradación del rendimiento con el aumento del tamaño del problema. La Figura 2-8 muestra la visualización aplicada a las métricas SupermarQ y QED-C en *ibmq_guadalupe*, donde los rectángulos coloreados representan directamente la puntuación lograda para diferentes métricas aplicadas a varios anchos (número de qubits) y profundidades (complejidad en número de operaciones) de circuito. El rendimiento se degrada claramente con el aumento del ancho del circuito debido a la conectividad limitada.

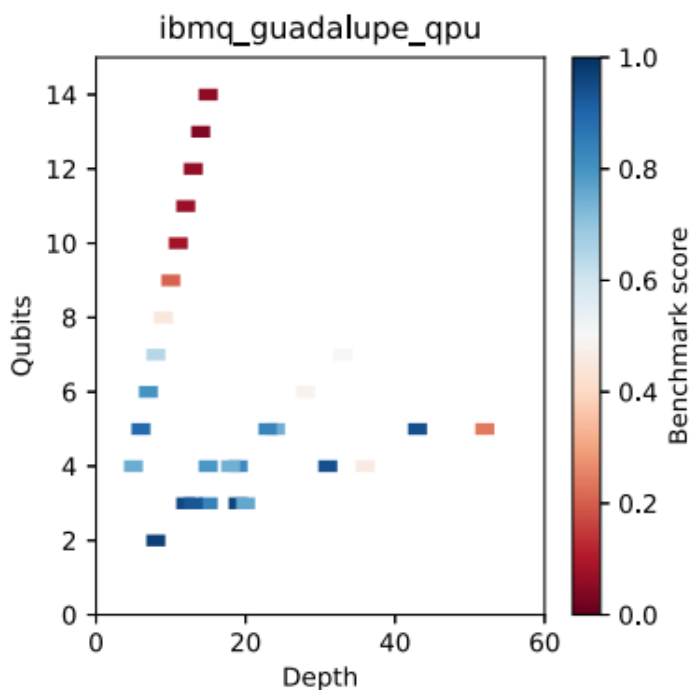


Figura 2-8 Métrica volumétrica con circuitos de aplicación [Hashim 2025].

Por otra parte, en el ámbito de la computación analógica, D-Wave ha logrado en 2025 un hito histórico al demostrar supremacía cuántica³⁴ en un problema útil y del mundo real, la simulación de materiales magnéticos complejos [King 2025]. Su ordenador cuántico de tipo *annealing* Advantage2 resolvió en minutos una simulación que requeriría cerca de un millón de años y más energía que el consumo anual global si se intentara con un superordenador clásico. El experimento consistió en simular dinámicas cuánticas relevantes para la investigación de nuevos materiales con aplicaciones en medicina, electrónica y redes eléctricas. Esta es la primera vez que se supera a un sistema clásico en un problema con valor práctico, no solo en tareas aleatorias sin utilidad directa.

Durante años, las métricas en computación cuántica prometían que los algoritmos cuánticos superarían a los correspondientes clásicos en tareas de predicción y optimización. Sin embargo, la literatura más reciente ha comenzado a matizar, incluso contradecir esas afirmaciones. A medida que los estudios se han vuelto más rigurosos y los dispositivos más accesibles, han surgido resultados que desafían el entusiasmo inicial. En 2025, un análisis exhaustivo de *benchmarks* [FKTH 2025] reveló que los métodos variacionales de aprendizaje automático cuántico (*Quantum Machine Learning*, QML) tienen por lo general, en el mejor de los casos, un rendimiento comparable al de modelos clásicos simples en una amplia gama de tareas de predicción. Esta afirmación, lejos de confirmar la superioridad cuántica, sugiere una paridad que obliga a replantear las expectativas. Más aún, los modelos cuánticos que sí logran destacar en rendimiento suelen hacerlo apoyándose en una cantidad considerable de parámetros entrenables clásicos. Esto ha llevado a algunos investigadores a preguntarse si los efectos cuánticos aportan realmente valor, o si el mérito recae en la parte clásica del sistema. A todo esto se suman las restricciones inherentes a los dispositivos NISQ en los que los qubits de calidad limitada, las interacciones ambientales y los efectos de muestreo finito siguen siendo obstáculos persistentes.

2.5.5 NISQ versus FTQC

La evolución de la computación cuántica digital o basada en puertas se estructura en dos grandes eras tecnológicas definidas por la capacidad de gestionar el ruido, la era actual NISQ (*Noisy Intermediate-Scale Quantum*) y la era futura FTQC (*Fault-Tolerant Quantum Computing*)³⁵. Mientras que el régimen NISQ (2020-presente) opera con un número limitado de qubits físicos (entre 50 y 500) vulnerables al ruido y sin corrección de errores, limitando su uso a demostraciones y casos específicos, la transición hacia la FTQC (estimada entre 2025-2035 para su fase temprana y más allá de 2035 para la madura) permitirá la ejecución de algoritmos universales complejos y escalables gracias a la implementación de la corrección de errores cuánticos (QEC).

Los dispositivos NISQ presentan restricciones inherentes significativas que limitan fundamentalmente su capacidad computacional. Estas limitaciones afectan tanto a la calidad individual de los qubits como a su comportamiento colectivo en circuitos complejos [Preskill 2018, Hashim 2025].

- Los qubits actuales sufren de coherencia limitada, caracterizada por dos tiempos fundamentales:
 - Tiempo de relajación T_1 : describe cuánto tiempo un qubit permanece en estado excitado antes de decaer al estado fundamental debido a relajación de energía. En qubits superconductores, oscila típicamente entre decenas y cientos de microsegundos. Este parámetro fija un límite superior absoluto para cualquier operación cuántica.

³⁴ <https://postquantum.com/industry-news/d-wave-quantum-advantage/>

³⁵ <https://postquantum.com/quantum-computing/nisq-ftqc-faq/>

- Tiempo de desfase T_2 : cuantifica cuánto tiempo un qubit en superposición puede mantener coherencia de fase antes de experimentar desfase puro. En la mayoría de los sistemas, $T_2 \leq 2T_1$, lo que refleja que la pérdida de energía (T_1) inevitablemente causa pérdida de fase.
- La fidelidad de los circuitos decae exponencialmente con profundidad y número de qubits según $F(d) \approx (1 - \epsilon)^{d \cdot n}$, donde d es la profundidad del circuito (número de capas de puertas), n es el número de qubits y ϵ es la tasa de error por puerta ($\sim 10^{-3}$ a 10^{-2} en dispositivos actuales). Esta relación exponencial es devastadora: un circuito con solo 100 puertas en 10 qubits con $\epsilon = 0,001$ produciría $F \approx (0,999)^{1000} \approx 0,37$, es decir, sólo un 37% de fidelidad. La fidelidad decae exponencialmente con el número de qubits (cientos hasta el orden de 1000 qubits) y la profundidad del circuito (Tabla 2-3) si no se aplica corrección de errores. Sin corrección de errores, la fidelidad se vuelve inutilizable rápidamente.
- Los dispositivos NISQ experimentan múltiples fuentes de error debido a interacciones ambientales y fuentes de ruido:
 - Ruido de amplitud (*amplitude damping*): pérdida espontánea de energía por emisión radiativa.
 - Ruido de desfase (*dephasing*): fluctuaciones de frecuencia aleatorias que destruyen la coherencia.
 - Ruido $1/f$: fluctuaciones lentas en parámetros de control que causan derivas temporales.
 - *Crosstalk*: acoplamientos indeseados entre qubits vecinos que generan errores correlacionados.
 - Fugas a estados superiores (*leakage*): excitación hacia niveles energéticos fuera del espacio computacional.
- Además del ruido físico, la medición cuántica introduce incertidumbre estadística $\sigma \sim 1/\sqrt{N}$, siendo N el número de muestras medidas de un circuito. Para obtener estimaciones confiables de probabilidades con error $< 1\%$, se requieren típicamente cientos a miles de muestras (shots) por circuito. Esta necesidad se multiplica al ejecutar múltiples circuitos en experimentos de *benchmarking*.
- El régimen NISQ está confinado a aproximadamente 50-500 qubits: 100-500 qubits superconductores prácticamente útiles, 10-100 qubits de iones atrapados (mejor coherencia, menos escalabilidad), 50-300 qubits de átomos neutros (prometedores, pero aún en desarrollo). La escalabilidad es el cuello de botella, cada qubit adicional incrementa el ruido global y hace más difícil mantener todo el sistema coherente simultáneamente.

Profundidad Circuito	10 Qubits	50 Qubits	100 Qubits
10 capas	$F \approx 90\%$	$F \approx 60\%$	$F \approx 37\%$
20 capas	$F \approx 81\%$	$F \approx 36\%$	$F \approx 13\%$
100 capas	$F \approx 37\%$	$F \approx 0.004\%$	$F \approx 0$

Tabla 2-3 Fidelidad de circuitos cuánticos con la profundidad y el número de qubits.

La combinación de estos factores crea lo que los investigadores llaman la “curva de la muerte”, que describe la degradación exponencial de la fidelidad con el aumento simultáneo del número de qubits y la profundidad del circuito. A partir de cierto punto, la fidelidad cae tan dramáticamente que los resultados se vuelven estadísticamente indistinguibles del ruido completamente aleatorio, haciendo

imposible extraer información útil del cálculo cuántico sin recurrir a mecanismos de corrección de errores.

La corrección de errores cuánticos (*Quantum Error Correction*, QEC) es el conjunto de técnicas que hacen posible la computación cuántica tolerante a fallos (*Fault-Tolerant Quantum Computing*, FTQC). Los códigos de corrección de errores hacen posible que los qubits puedan ejecutar algoritmos útiles durante el tiempo de coherencia [Preskill 2018, Hashim 2025]. La QEC representa la estrategia fundamental para transformar dispositivos NISQ ruidosos en computadores cuánticos confiables y escalables. Mientras que los dispositivos NISQ mitigan errores de forma pasiva, QEC introduce un mecanismo activo que consiste en codificar información lógica en múltiples qubits físicos para detectar y corregir automáticamente errores sin destruir la información cuántica.

- Más Qubits para Proteger Uno. A primera vista, QEC parece contradecir la intuición al necesitar 1,000 a 10,000 qubits físicos para proteger un único qubit lógico. La clave para entender esta aparente paradoja reside en tres mecanismos cuánticos fundamentales:
 - En ordenadores clásicos, la redundancia funciona por duplicación o copia de bits y comparación para detectar errores. Si los bits copiados difieren se corrige usando el valor en mayoría. En cuántica, esto es imposible por el Teorema de No-Clonación, no se pueden copiar los qubits para compararlos. QEC en lugar de copiar información, la distribuye de forma entrelazada entre múltiples qubits. Un qubit lógico puede estar representado muchos qubits físicos en códigos como el *Steane code* o el *Surface code* (malla 2D). Los estabilizadores son conjuntos de qubits vecinos cuya paridad se mide periódicamente. Mediante mediciones de paridad de estabilizadores, se puede extraer información sobre la presencia de errores (*bit-flip* X o *phase-flip* Z)³⁶ sin revelar la información lógica almacenada. El sistema usa esta información para corregir el error y mantener la coherencia del qubit lógico.
 - Los errores en cuántica siguen patrones matemáticos predecibles, denominados errores de Pauli que se propagan de forma determinista. Cuando un error ocurre en un qubit dentro de un circuito, su efecto sobre el resto del sistema se puede calcular de forma determinista usando las reglas de propagación de las puertas cuánticas (p.e. un error X antes de una puerta Hadamard se convierte en un error Z después de la puerta). La medida de los estabilizadores da como resultado un conjunto de bits denominados “síndrome de error”, que son una huella digital que indica qué tipo de error ocurrió y en qué lugar, sin revelar la información lógica. Un algoritmo clásico (decodificador) sobre un ordenador clásico interpreta estos síndromes y determina la corrección más probable a aplicar (p.e. aplicar X, Z o Y en ciertos qubits). En el *Surface Code*, se usan algoritmos como *Minimum Weight Perfect Matching*³⁷ para decidir cómo corregir los errores detectados.
 - A diferencia de sistemas clásicos, la redundancia cuántica es cuantitativa, no cualitativa (copia idéntica de bits). Los qubits físicos no son copias independientes, sino una distribución entrelazada donde ningún qubit individual contiene la información completa. Medir qubits individuales destruye la coherencia y colapsa el estado lógico. Para detectar errores no se mide cada qubit por separado, se miden combinaciones de qubits mediante los llamados estabilizadores (p.e. en el *Surface code*, se mide la paridad de cuatro qubits vecinos, si la paridad cambia significa que hubo un error en alguno de ellos).
- El Umbral de Tolerancia. El resultado teórico más importante en QEC es la existencia de un umbral de error $\varepsilon_{th} \approx 10^{-3}$ a 10^{-4} . Este número define una transición cualitativa en la que si la tasa de error individual de cada puerta cuántica desciende por debajo de este umbral,

³⁶ Operaciones de Pauli X ($|0\rangle \leftrightarrow |1\rangle$), Z ($|1\rangle \leftrightarrow -|1\rangle$), o Y (combinación de X y Z).

³⁷ Algoritmo clásico que empareja por parejas los defectos detectados en el “síndrome de error” minimizando la distancia total entre ellos, permitiendo identificar la corrección más probable en códigos cuánticos como el *Surface Code*.

entonces los errores acumulativos en un código QEC disminuyen exponencialmente con el número de qubits físicos. Por encima del umbral $\varepsilon > \varepsilon_{th}$ a más qubits, más errores totales. Actualmente se está en el límite bajo del umbral $\varepsilon = \varepsilon_{th}$ con $\varepsilon \approx 10^{-3}$ para dispositivos superconductores y $\varepsilon \approx 10^{-4}$ para iones atrapados. Por debajo del umbral $\varepsilon < \varepsilon_{th}$ a más qubits, los errores serán exponencialmente menores.

- Ciclos de corrección. En la práctica el QEC no es instantáneo sino que opera en ciclos repetidos. Cada ciclo típicamente dura de 100 a 500 nanosegundos en dispositivos superconductores. La detección de error (extracción del síndrome), decodificación clásica y aplicación de corrección debe ser inferior al tiempo de desfase $t_{ciclo} \ll T_2$. Si tenemos $T_2 = 100 \mu s$ y $t_{ciclo} = 100 ns$, hay 1000 ciclos antes de que la decoherencia sea irreversible.
- Código de superficie (*Surface code*). Entre todos los códigos cuánticos de corrección de errores propuestos, el código de superficie es actualmente el más prometedor para la implementación práctica. Requiere que los qubits interactúen solo con sus vecinos inmediatos en una red 2D, compatible con la mayoría de las arquitecturas actuales. Una red de $L \times L$ qubits produce una distancia de código $d = 2L - 1$, permitiendo escalabilidad indefinida. Tolera tasas de error individuales hasta del orden del 1%, casi 10 veces mejor que muchos otros códigos.
- *Overhead* Masivo. Una de las realidades más desafiantes del QEC es que la cantidad de qubits físicos necesarios escala dramáticamente con la demanda de fidelidad lógica para una determinada aplicación. La Tabla 2-4 pone de manifiesto que ejecutar el algoritmo de Shor para factorizar RSA-2048 exigiría del orden de 20 a 40 millones de qubits físicos cuando se utilizan códigos como el *surface code*. En contraste, los procesadores más avanzados disponibles en 2025 se sitúan en la horquilla de unos pocos cientos a alrededor de un millar de qubits físicos. Alcanzar las decenas de millones de qubits implica no solo multiplicar por varios órdenes de magnitud la escala de los dispositivos, sino también mantener o mejorar las tasas de error por puerta hasta situarlas cómodamente por debajo del umbral de tolerancia.

Aplicación	Número de qubits lógicos	Error lógico requerido	Número de qubits físicos por lógico	Número total de qubits físicos
Simulación Química (pequeña)	100-500	10^{-8}	~1.000	100.000-500.000
Factorización RSA-2048	2.000-4.000	10^{-15}	~10.000	20-40 millones
Optimización Combinatoria	1.000-10.000	10^{-6}	~1.000	1-10 millones
Comparación NISQ (sin QEC)	50-500	N/A (~0.01-0.1)	1	50-500

Tabla 2-4 Número de qubits físicos y lógicos por aplicación.

Un aspecto estratégico crucial es entender cuándo y cómo la computación cuántica tolerante a fallos (FTQC) supera ventajosamente a NISQ (Tabla 2-5). A día de hoy, el régimen NISQ puro utiliza 50-500 qubits físicos, es aplicable a circuitos de 100-1000 puertas máximo, y para $\varepsilon = 10^{-3}$ y 1000 puertas (capas $\times$ qubits) la fidelidad es $F = 37\%$. El régimen temprano de FTQC, estimado para 2025-

2035, requiere 1.000-100.000 qubits físicos, pero virtualmente tendrá todos los errores corregidos automáticamente alcanzando una fidelidad lógica $F \approx 0,99999999$ incluso para millones de puertas. Para problemas como la factorización de números primos (algoritmo de Shor) se requiere del orden de decenas de millones de puertas, siendo imposible en NISQ pero viable con FTQC maduro. Para problemas de optimización heurística (QAOA, VQE) el cruce es más gradual, pudiéndose usar NISQ para instancias pequeñas y siendo necesaria FTQC para instancias mayores.

Métrica	NISQ (Hoy)	FTQC Temprano	FTQC Maduro
Número de Qubits	50-500	1.000-100.000	10 millones+
Profundidad Útil	100-1.000	1.000-100.000	100 millones+
Error por Puerta	$\sim 10^{-3}$	$\sim 10^{-4}$ (bajo umbral)	$\sim 10^{-5}+$
Error Lógico Final	$\sim 0.01-0.1$ (inaceptable)	$\sim 10^{-6}$ a 10^{-8}	$\sim 10^{-15}$ (excelente)
Tipos de Problemas	Demostraciones, R&D	Simulación de moléculas, optimización	Factorización, búsqueda no estructurada, ML cuántico
Disponibilidad	2020-presente	2025-2035 (estimado)	2035+

Tabla 2-5 Comparación de los tres regímenes de computación cuántica.

En la Tabla 2-6 se compara la evolución de los ordenadores cuánticos de cuatro empresas representativas: IBM, Google, IonQ y Quantinuum. La tabla recoge el año de anuncio o despliegue aproximado y el número de qubits físicos y de qubits lógicos o qubits algorítmicos (AQ). En Google e IBM, los qubits lógicos son construidos mediante corrección de errores cuánticos (p.e. códigos de superficie). En el caso de IonQ, se emplea la métrica propia AQ. Esta métrica no es un conteo de qubits lógicos con corrección de errores completa, sino una medida del tamaño de un registro cuántico efectivamente utilizable en algoritmos prácticos, que combina fidelidad de las puertas, conectividad del hardware y profundidad de circuito alcanzable. En la tabla se representa AQ como si fuera un número de “qubits lógicos efectivos” con el fin de poder comparar de forma aproximada la capacidad de cómputo utilizable entre distintas tecnologías. En Quantinuum se representan tanto hitos en número de qubits físicos, como una demostración reciente de 4 qubits lógicos implementados con 32 qubits físicos con tasas de error lógicas hasta 800 veces menores que las físicas. Es importante subrayar que la comparación entre qubits lógicos con corrección de errores explícita (Google, Quantinuum, IBM) y qubits algorítmicos (AQ) debe hacerse con cautela, ya que se basan en criterios físicos y de ingeniería diferentes.

Empresa	Año ³⁸	Qubits físicos	Qubits lógicos / AQ	Comentario breve
IBM ^{39,40}	2016	5	-	Primer procesador de 5 qubits accesible en la nube (IBM Quantum Experience) ⁴¹
	2017	16	-	Procesador IBM Q de 16 qubits (familia anterior a Falcon/Hummingbird)
	2020	27	-	Procesador “Falcon”, 27 qubits superconductores
	2022	127	-	Procesador “Eagle”, 127 qubits
	2024	133	-	Procesador “Heron”, 133 qubits
	2025	120	-	Procesador “Nighthawk”, 120 qubits, mitigación de errores
	2029 ⁴²	—	200	Objetivo de hoja de ruta: ≈200 qubits lógicos “Starling” hacia FTQC
Google ⁴³	2019	53	-	Procesador “Sycamore”, 53 qubits, experimento de supremacía cuántica [Arute 2019]
	2023	49	1	Sycamore extendido con 49 qubits físicos para un qubit lógico de superficie
	2024	105	-	Chip “Willow”, 105 qubits, orientado a QEC y RCS
Quantinuum ⁴⁴	2021	12	-	Sistema H1-1 12 qubits totalmente conectados
	2022	20	-	Sistema H1-1 actualizado a 20 qubits totalmente conectados (<i>all-to-all</i>) ⁴⁵
	2024	56	-	Sistema H2-1 actualizado a 56 qubits atrapados totalmente conectados
	2024	32	4	Demostración de 4 qubits lógicos (generados mediante técnicas avanzadas de detección y corrección de errores)

³⁸ Anuncio o despliegue aproximado.

³⁹ <https://www.ibm.com/quantum/>

⁴⁰ [AbuGhanem 2024]

⁴¹ https://en.wikipedia.org/wiki/IBM_Quantum_Platform

⁴² Objetivo.

⁴³ <https://research.google/>

⁴⁴ <https://www.quantinuum.com/>

⁴⁵ <https://thequantuminsider.com/2022/06/14/quantinuum-completes-hardware-upgrade-achieves-20-fully-connected-qubits/>

Empresa	Año ³⁸	Qubits físicos	Qubits lógicos / AQ	Comentario breve
				<i>“better-than-break-even”</i> con 32 qubits físicos ⁴⁶
IonQ ⁴⁷	2020	11	-	IonQ Harmony: primer sistema comercial en la nube de 11 qubits físicos
	2022	32	29 (AQ)	IonQ Forte: sistema de 32 qubits físicos con AQ = 29 demostrado (benchmarking detallado)
	2024	32	35 (AQ)	IonQ Forte actualizado: milestone técnico AQ = 35, un año antes de lo previsto en <i>roadmap</i>

Tabla 2-6 Hitos de qubits físicos y de capacidad lógica efectiva.

2.6 Las comunicaciones y las redes cuánticas

Las comunicaciones y redes cuánticas representan un cambio fundamental en la transmisión segura de información y el procesamiento distribuido de datos. A diferencia de las redes clásicas que transmiten bits de información en estados binarios definidos, las redes cuánticas trabajan con las unidades de información cuántica, los qubits, que pueden existir en superposición de estados. La distribución cuántica de claves (QKD) surgió como la primera aplicación práctica que aprovecha los principios de la mecánica cuántica. La criptografía cuántica, con protocolos como BB84, ofrece una solución que no se basa en la complejidad matemática, sino en las leyes fundamentales de la física para garantizar que cualquier intento de interceptación sea detectado inmediatamente. Este concepto inicial ha evolucionado hacia una visión más amplia del “internet cuántico” [WEH 2018], red global que distribuye no solo claves sino estados cuánticos entrelazados entre nodos para computación distribuida y sincronización cuántica.

El desarrollo de las comunicaciones cuánticas ha progresado desde las demostraciones de laboratorio hasta implementaciones terrestres y satélite reales. Las redes QKD de primera generación ya están operativas en configuraciones metropolitanas y de larga distancia, utilizando repetidores confiables (nodos intermedios que descifran/cifran claves), pero sin repetidores cuánticos genuinos que extiendan el entrelazamiento sin exponer las claves. Estas redes representan la primera etapa del desarrollo del internet cuántico, donde la distribución de claves se realiza mediante nodos intermedios de confianza sin un verdadero entrelazamiento punto a punto. Paralelamente, se han desarrollado sistemas satelitales que superan las limitaciones de distancia de las fibras ópticas terrestres, donde las pérdidas exponenciales restringen las comunicaciones a centenares de kilómetros. El satélite chino Micius demostró en 2017 la viabilidad de QKD entre satélite y estaciones terrestres separadas más de 1.200 kilómetros [Liao 2017], abriendo la posibilidad de comunicaciones cuánticas intercontinentales (China y Austria) [Liao 2018]. Europa está desarrollando la iniciativa EuroQCI para desplegar infraestructura cuántica segura entre todos los estados miembros, con capacidad operativa inicial prevista para 2027⁴⁸. La tecnología QKD ha pasado de pruebas de laboratorio a implementaciones reales en instituciones financieras, redes gubernamentales y otras infraestructuras críticas, demostrando

⁴⁶ [Rattew 2024]

⁴⁷ <https://ionq.com/>

⁴⁸ <https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci>

su viabilidad operativa [SGUHF 2022]. Estas implementaciones prácticas coexisten con importantes esfuerzos de estandarización liderados por organismos como ITU-T⁴⁹, ETSI⁵⁰ e IETF⁵¹, aunque todavía no existe un marco completamente unificado.

2.6.1 La distribución cuántica de clave (QKD)

La Distribución Cuántica de Clave (*Quantum Key Distribution*, QKD) representa un cambio fundamental de paradigma en la criptografía contemporánea. A diferencia de los sistemas criptográficos clásicos, cuya seguridad se fundamenta en la dificultad computacional de ciertos problemas matemáticos, QKD basa su seguridad en los principios inviolables de la Mecánica Cuántica. Cuando dos partes legítimas Alice y Bob desean establecer una clave compartida mediante QKD, cualquier intento de interceptación (*eavesdropping*) por parte de un adversario Eve provoca perturbaciones detectables en el sistema cuántico, alertando a las partes legítimas de la presencia de vigilancia no autorizada. Esta distinción es crucial ante la inminente amenaza de los ordenadores cuánticos, que ponen en riesgo la mayoría de los esquemas de criptografía de clave pública actualmente desplegados.

Los protocolos fundamentales de QKD son:

- El BB84, desarrollado por Charles Bennett y Gilles Brassard en 1984 [BB 1984], constituye el primer esquema de distribución cuántica de clave demostrado y sigue siendo uno de los más simples y elegantes.

El protocolo BB84 (Figura 2-9) se basa en transmitir fotones individuales preparados en uno de cuatro estados de polarización, distribuidos en dos bases ortogonales previamente acordadas: la base Z (vertical/horizontal) y la base X (diagonal 45°/−45°). Para cada bit que desea enviar, Alice elige aleatoriamente una de estas dos bases y, dentro de la base seleccionada, prepara uno de sus dos estados posibles. A continuación, envía el fotón correspondiente a Bob a través del canal cuántico (fibra óptica o espacio libre). Bob, por su parte, mide cada fotón eligiendo también al azar entre las mismas dos bases. Una vez completada la transmisión, Alice y Bob anuncian públicamente qué bases utilizaron en cada posición, pero sin revelar los resultados de las mediciones. Esto les permite identificar los casos en los que ambos emplearon la misma base, que son precisamente aquellos en los que Bob obtiene el valor correcto con certeza. Los bits correspondientes a estas coincidencias forman la clave bruta preliminar, mientras que el resto se descarta.

La seguridad de BB84 se basa en que cualquier intento de Eve de obtener información sobre los fotones en tránsito obliga a que realice una medición. Debido al principio de proyección de la mecánica cuántica, si Eve mide un fotón en una base incorrecta altera su estado de forma inevitable e impredecible. Cuando Eve mide en la base correcta Bob solo tiene un 50% de probabilidad de usar esa misma base, pero cuando Eve se equivoca introduce errores adicionales que Bob podrá detectar más adelante. Para ello, Alice y Bob comparan públicamente una muestra de sus bits (sin revelar la clave completa) y calculan la tasa de error cuántico (*Quantum Bit Error Rate*, QBER). Si esta tasa supera un umbral seguro, concluyen que ha habido una intrusión. En esencia, la seguridad de BB84 combina el secretismo cuántico (la imposibilidad de copiar o medir sin perturbar) con la detección activa de *eavesdropping* mediante el análisis de errores.

⁴⁹ <https://www.itu.int/en/ITU-T/about/Pages/default.aspx>

⁵⁰ <https://www.etsi.org/>

⁵¹ <https://www.ietf.org/>

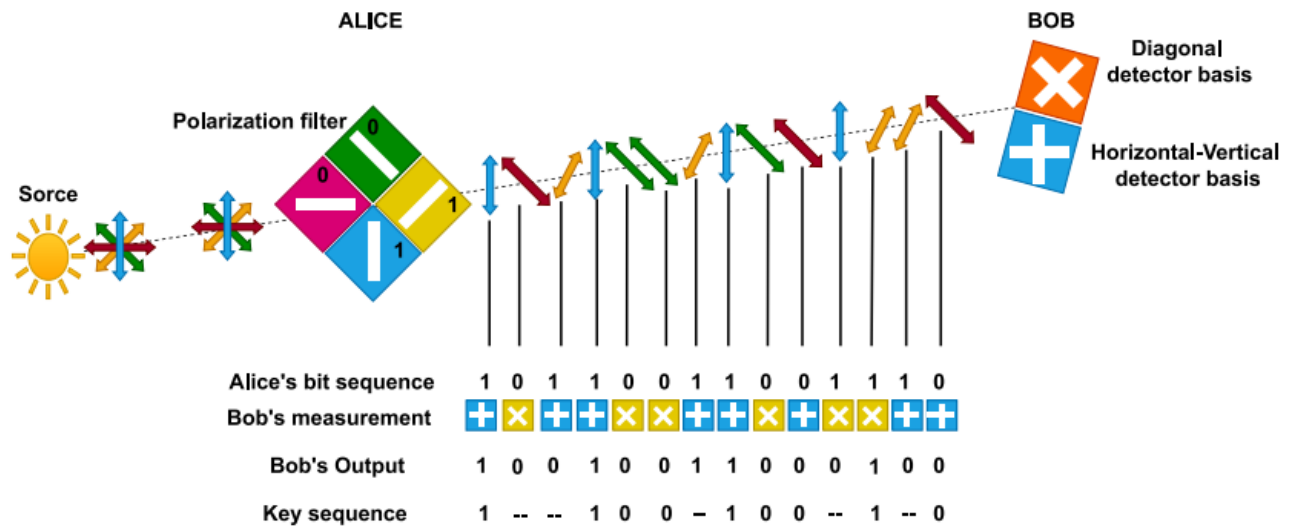


Figura 2-9 Principio del protocolo BB84 [BB 1984].

A pesar de su elegancia teórica, las implementaciones prácticas de BB84 se enfrentan a desafíos significativos. Los sistemas reales no utilizan fotones únicos perfectos sino pulsos débiles coherentes (*Weak-Coherent-Pulse*, WCP), que contienen ocasionalmente múltiples fotones. Esta multiplicidad introduce la vulnerabilidad conocida como ataque de división de número de fotones (*Photon-Number Splitting*, PNS), donde un atacante puede desviar preferentemente los fotones de multiplicidad hacia un sistema de almacenamiento para análisis posterior mientras los fotones únicos se propagan normalmente hacia Bob. Esta vulnerabilidad ha motivado el desarrollo del método de estado señuelo (*decoy-state*), que mitiga el ataque PNS mediante el envío de pulsos con diferentes intensidades de prueba [Hwang 2003, Wang 2005].

- El protocolo E91, propuesto por Artur Ekert en 1991 [Ekert 1991], adopta un enfoque distinto al de BB84 al basarse en el entrelazamiento cuántico. En este esquema, una fuente genera pares de fotones entrelazados en estados de Bell y envía uno a Alice y otro a Bob. Cada uno mide su fotón eligiendo al azar entre tres bases previamente acordadas: una de ellas se utiliza para generar la clave, mientras que las otras dos sirven para verificar la seguridad del sistema mediante un test de Bell. Cuando Alice y Bob eligen la misma base de generación de clave, sus resultados están perfectamente correlacionados y se emplean para formar la clave bruta, descartándose las mediciones realizadas en bases distintas. Por otro lado, cuando seleccionan bases diferentes, los resultados no se usan para la clave, sino para comprobar que las correlaciones observadas violan una desigualdad de Bell [Bell 1964], lo que garantiza que ningún intruso ha manipulado el canal o los dispositivos. Este mecanismo de verificación es el elemento distintivo de E91 y la base de su seguridad.

Esta característica hace que el protocolo E91 sea, en principio, compatible con el enfoque independiente del dispositivo (*Device-Independent QKD*, DI-QKD). En este marco, la seguridad no depende de conocer o confiar en el funcionamiento interno de los detectores, sino únicamente de comprobar experimentalmente que las correlaciones observadas violan una desigualdad de Bell. Sin embargo, para que esta independencia sea realmente válida, las pruebas de Bell deben realizarse sin brechas o resquicios experimentales, es decir, sin fallos técnicos ni limitaciones que un adversario pudiera explotar para reproducir las correlaciones mediante modelos clásicos. Durante décadas, lograr pruebas de Bell completamente libres de resquicios fue un desafío experimental, pero solo en tiempos recientes se han conseguido de

forma concluyente, lo que ha consolidado la viabilidad práctica del enfoque propuesto por Ekert [Miller 2016].

- El protocolo BBM92 [BBM 1992] representa una variante simplificada del esquema basado en entrelazamiento en el que sólo se requieren dos bases de medición para Alice y Bob, haciéndolo más práctico que E91 para implementaciones tempranas. Aunque BBM92 carece del mecanismo de prueba de Bell, mantiene la estructura de entrelazamiento que proporciona resiliencia frente a ciertos tipos de ataques.
- El protocolo B92, desarrollado por Charles Bennett en 1992 [Bennet 1992], utiliza solo dos estados cuánticos no ortogonales en lugar de los cuatro estados de polarización empleados en BB84. Esta reducción hace que el protocolo sea conceptualmente más sencillo y eficiente en términos de implementación, pero también lo vuelve más vulnerable a ciertos ataques. La información disponible para un posible *eavesdropper* es mayor al haber menos estados posibles, pudiéndola interceptar y reenviar.
- El protocolo SARG04 [SARG 2004] modifica la fase de post-procesamiento clásico del BB84 para reforzar la seguridad contra ataques PNS. En el BB84, Alice y Bob anuncian las bases de medida lo que facilita a un atacante explotar pulsos con múltiples fotones. En cambio, el SARG04 anuncia conjuntos de estados no ortogonales, de modo que incluso si un adversario obtiene más de un fotón no puede determinar con certeza el bit transmitido. El SARG04 es una variante más robusta frente a las vulnerabilidades en los canales con pérdidas del BB84, manteniendo la misma simplicidad en la preparación de estados.

Los protocolos BB84 y E91 comparten el objetivo de distribuir claves seguras y son equivalentes en seguridad cuando se implementan con qubits, pero se basan en principios conceptuales distintos. BB84 es un protocolo de tipo “prepara y mide”, en el que Alice prepara estados cuánticos en bases complementarias y Bob los mide. En contraste, E91 utiliza pares de fotones entrelazados generados por una fuente común, y su seguridad se fundamenta en la observación de correlaciones que violan desigualdades de Bell, lo que garantiza que un *eavesdropper* no pudo haber predeterminado los resultados [Scarani 2009]. Sin embargo, BB84 es más sencillo de implementar con la tecnología actual y ha sido ampliamente adoptado comercialmente, mientras que E91, aunque conceptualmente más cercano a esquemas independientes del dispositivo, requiere fuentes de entrelazamiento de alta calidad y verificación experimental de violaciones de Bell, lo que incrementa su complejidad práctica.

Las arquitecturas fundamentales de QKD son:

- La arquitectura de Distribución Cuántica de Clave Independiente del Dispositivo de Medición (*Measurement-Device-Independent* QKD, MDI-QKD) [LCQ 2012] elimina las vulnerabilidades de seguridad relacionadas con dispositivos de medición imperfectos. La QKD frecuentemente asume los fotodetectores como ideales, estando los componentes físicos reales sujetos a imperfecciones y fluctuaciones. Esta desconexión entre teoría e implementación ha permitido diversos ataques de canal lateral donde un adversario manipula los detectores para extraer información adicional.

MDI-QKD resuelve este dilema mediante una arquitectura tripartita. Alice y Bob envían qubits preparados en estados cuánticos predeterminados hacia un nodo central intermedio potencialmente no confiable. Este nodo intermedio realiza una medición conjunta denominada medición de Bell entre los dos qubits recibidos, sin conocer cuáles eran los estados preparados por Alice o Bob. El resultado clásico de la medición se comunica públicamente. Cuando la medición de Bell proyecta exitosamente ambos qubits hacia un estado de Bell determinado (particularmente el singlete que es el más fácil de identificar experimentalmente), Alice y Bob saben con certeza que sus qubits estaban entrelazados. Bajo estas condiciones, los resultados correlacionados constituyen claves seguras.

La ventaja de MDI-QKD es que la seguridad es completamente insensible a las propiedades del detector utilizado en el nodo intermedio. Incluso si los detectores están comprometidos o son de calidad baja, la seguridad de los bits clave se mantiene siempre que los qubits transmitidos por Alice y Bob sean legítimos. Adicionalmente, MDI-QKD proporciona robustez ante fluctuaciones de láser y otras imperfecciones del transmisor. La operación de interferencia de dos fotones en el nodo intermedio requiere que ambos qubits lleven la marca cuántica de forma que sobreviva a imperfecciones de transmisión. La implementación de MDI-QKD ha tenido mejoras significativas alcanzando tasas de clave segura de hasta 8 bits por segundo a 54 dB de pérdida de canal [Woodward 2021].

- La Distribución Cuántica de Clave de Campos Gemelos (*Twin-Field* QKD, TF-QKD) [LYDS 2018] surge de la limitación inherente a BB84 de que la tasa de clave segura disminuye linealmente con la transmitancia del canal cuántico. La tasa de claves escala aproximadamente como la transmitancia del canal multiplicada por funciones que también dependen de esta, limitado su uso a distancias metropolitanas típicamente de hasta 100 km de fibra óptica estándar. TF-QKD supera esta limitación mediante un mecanismo basado en interferencia de fotones únicos. Alice y Bob preparan y envían estados coherentes débiles con fases aleatorias hacia un nodo intermedio. En el nodo intermedio ambos estados se combinan en un divisor de haz y se realiza una medición proyectiva para detectar si ocurre interferencia constructiva o destructiva. Mediante un mecanismo de ajuste de fases, Alice y Bob pueden acordar cuándo sus estados interfirieron constructivamente. La tasa de clave en TF-QKD escala con la raíz cuadrada de la transmitancia en lugar de linealmente. Esta mejora es comparativa a los beneficios que proporcionarían los repetidores cuánticos, pero sin la complejidad de almacenar y reconectar estados entrelazados. Las implementaciones prácticas de TF-QKD han alcanzado distancias de 550 km de fibra óptica estándar. Una variante especialmente prometedora es el protocolo SNS (*Sending-Not-Sending*) TF-QKD, que simplifica los requisitos de control de fase.
- La Distribución Cuántica de Clave Completamente Independiente del Dispositivo (*Device-Independent* QKD, DI-QKD) [LPTRG 2013] introduce un protocolo en el que la seguridad de la clave cuántica no depende de la fiabilidad de los dispositivos empleados. Representa el grado máximo teórico de seguridad haciendo posible la distribución segura de claves incluso en presencia de canales altamente ruidosos o con grandes pérdidas. A diferencia de MDI-QKD, DI-QKD no hace ningún supuesto sobre la estructura interna de los dispositivos de Alice y Bob. La verificación de la legitimidad de todos los dispositivos se efectúa únicamente mediante pruebas estadísticas de violación de desigualdades de Bell. En el protocolo DI-QKD, Alice y Bob tienen respectivamente un dispositivo que produce una salida binaria cuando se proporciona una entrada de selección aleatoria. Miden repetidamente sus dispositivos con selecciones de entrada aleatorias e independientes y posteriormente analizan estadísticamente si los resultados conjuntos violan una desigualdad de Bell. Una violación significativa proporciona garantía de que la estadística observada no puede reproducirse mediante correlaciones clásicas locales. DI-QKD todavía está en una fase de investigación y requiere superar enormes retos técnicos y experimentales, como el entrelazamiento de muy alta calidad, violaciones de Bell amplias y significativas, y medidas casi perfectas con detectores de fotones con eficiencias casi perfectas (típicamente $> 90\%$).
- La Distribución Cuántica de Clave de Variables Continuas (*Continuum Variable* QKD, CV-QKD) [MPBP 2022] es una rama de QKD que utiliza variables continuas cuadráticas del campo electromagnético alternativamente a los esquemas de variable discreta. En CV-QKD, en lugar de codificar información en números de fotones discretos o polarizaciones, Alice modula los cuadrantes conjugados del campo electromagnético en amplitud y fase (X y P). Los cuadrantes están sujetos al principio de incertidumbre de Heisenberg proporcionando garantías

de seguridad en un régimen completamente diferente. Una ventaja significativa de CV-QKD radica en que los componentes ópticos necesarios (moduladores de fase, acopladores direccionales, detectores de fotodiodo) están disponibles comercialmente y se reutilizan en la infraestructura de telecomunicaciones ópticas moderna. Por consecuencia, CV-QKD es potencialmente más escalable y económicamente viable para despliegue en redes metropolitanas.



Figura 2-10 Red de comunicaciones cuánticas china [MERICS 2024].

Las implementaciones prácticas de QKD se enfrentan al dilema fundamental de que la generación determinista de fotones únicos es técnicamente compleja, mientras que el uso de pulsos coherentes débiles introduce la vulnerabilidad de división de número de fotones (PNS). El método del estado señuelo (*decoy-state*) propone una solución. Alice envía aleatoriamente pulsos en tres categorías, pulsos señal con intensidad nominal y pulsos de prueba o de estado señuelo con dos intensidades diferentes y conocidas. A partir de las tasas de error cuántica observadas para cada categoría, Alice y Bob pueden inferir estadísticamente cuántos fotones únicos fueron detectados exitosamente y cuántos fueron atacados por Eve, ajustando la tasa de clave final.

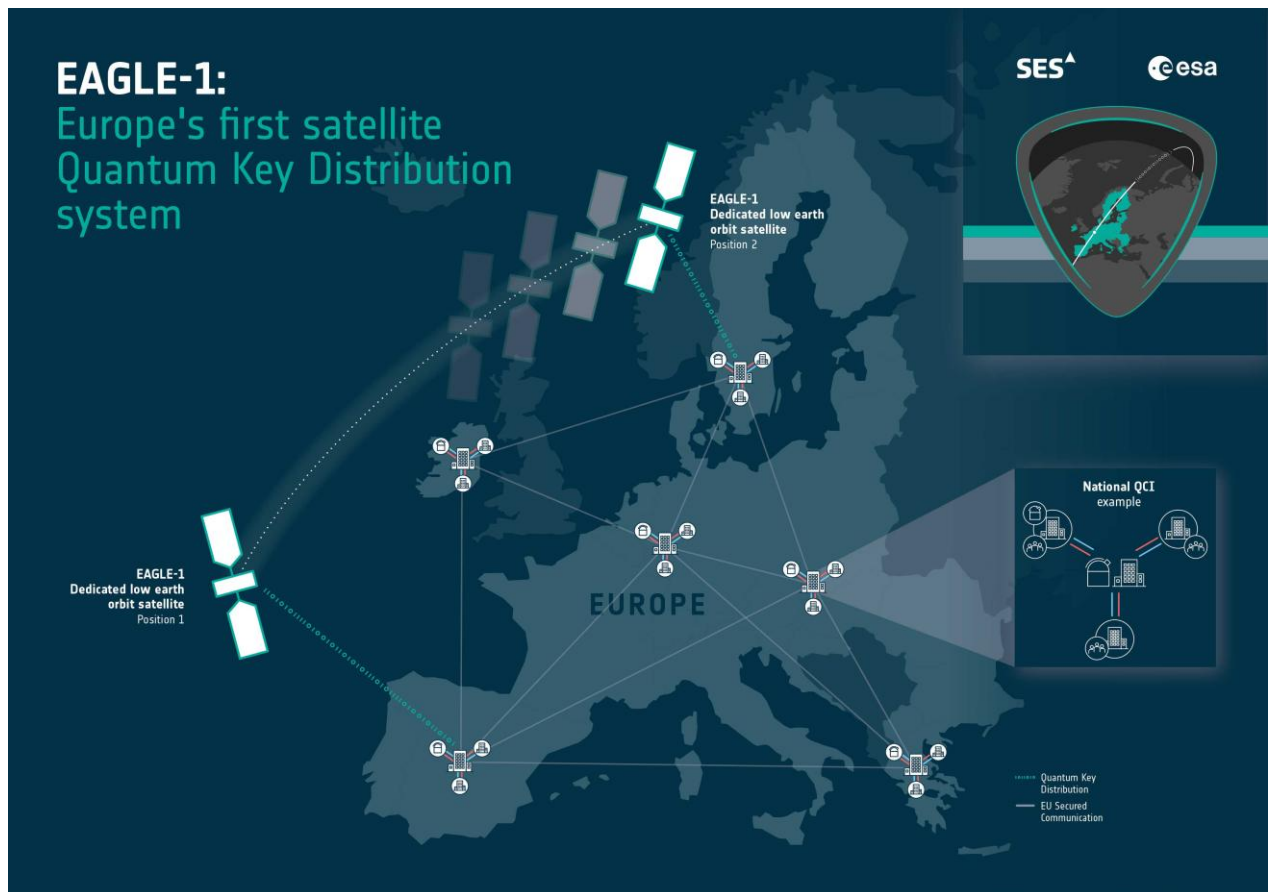


Figura 2-11 Esquema de la infraestructura satélite LEO del EAGLE-1 y la red terrestre [Referencia 56].

Los protocolos QKD fundamentales han sido demostrados exitosamente en laboratorio y la siguiente etapa es la integración de múltiples nodos QKD en redes metropolitanas y de mayor área. La iniciativa estratégica de la Comisión Europea de una Infraestructura de Comunicaciones Cuánticas Europea (*European Quantum Communication Infrastructure*, EuroQCI)⁵² representa uno de los esfuerzos más ambiciosos para el desarrollo de una infraestructura de comunicación cuántica segura que integre múltiples nodos QKD en redes metropolitanas y transnacionales para proteger las comunicaciones críticas de gobiernos e instituciones. China ha liderado la adopción de una red para comunicaciones cuánticas seguras que enlaza ciudades como Beijing, Shangai y Guangzhou con otras ciudades mediante múltiples nodos QKD alcanzando una longitud de 12.000 km [MERICS 2024] (Figura 2-10). Una limitación inherente de las redes terrestres es que la distancia máxima entre nodos está limitada por pérdidas de fibra óptica. Para lograr cobertura geográfica global, la investigación ha volcado esfuerzos significativos en la transmisión de fotones cuánticos a través de espacio libre. El satélite chino Micius, lanzado en 2016, realizó la primera demostración exitosa de distribución cuántica de clave tierra-satélite. La iniciativa europea QKDSat⁵³ de la Agencia Espacial Europea (*European Space Agency*, ESA) desarrolla una constelación de satélites de baja órbita (*Low Earth Orbit*, LEO) que busca la demostración en órbita y validación operacional pre-comercial de enlaces satélites QKD. El proyecto SAT-MQKD⁵⁴ de la ESA explora codificación multidimensional utilizando

⁵² <https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci>

⁵³

https://www.esa.int/Applications/Connectivity_and_Secure_Communications/Secure_communication_via_quantum_cryptography

⁵⁴ <https://connectivity.esa.int/projects/satmqkd>

pares de fotones hiperentrelazados, donde la información se codifica en polarización, tiempo de llegada, y frecuencia fotónica simultáneamente, proporcionando resiliencia mejorada contra turbulencia atmosférica. SAGA⁵⁵ e Eagle-1⁵⁶ (Figura 2-11) son iniciativas de QKD vía satélite que se integran dentro de la iniciativa EuroQCI.

2.6.2 La internet cuántica

La internet cuántica es una red de comunicación basada en principios de la mecánica cuántica que permite el intercambio de información cuántica entre múltiples nodos separados espacialmente⁵⁷. La internet cuántica permite la distribución de qubits entrelazados y estados cuánticos entre dispositivos distantes, lo que proporciona ventajas sin precedentes en criptografía (con seguridad garantizada por las leyes de la física), computación cuántica distribuida, metrología cuántica y sincronización de relojes de ultra-alta precisión. Su desarrollo implica la construcción de repetidores cuánticos y una compleja infraestructura de nodos que pueden preparar, almacenar, manipular y medir estados cuánticos con fidelidad extremadamente alta. Aunque actualmente se encuentra en etapas tempranas de implementación experimental, la internet cuántica representa uno de los objetivos más ambiciosos de la tecnología cuántica, con iniciativas globales como la *Quantum Internet Alliance*⁵⁸ de la Unión Europea que trabaja para demostrar redes cuánticas operacionales a escala regional en la próxima década.

El artículo relevante sobre la hoja de ruta hacia la internet cuántica fue escrito por Wehner et al. en 2018 [WEH 2018]. Establece seis etapas progresivas del desarrollo del internet cuántico, desde redes simples de repetidores de confianza hasta redes completamente funcionales con computadores cuánticos conectados. Cada etapa habilita nuevas aplicaciones y requiere capacidades tecnológicas incrementalmente más sofisticadas. A continuación se describe cada una:

- La etapa inicial, denominada de Redes de Repetidores de Confianza, no permite la transmisión de qubits de extremo a extremo. La red continúa transmitiendo solo información clásica. Sin embargo, lo puede hacer de forma más segura incorporando repetidores cuánticos a la infraestructura existente. Utiliza nodos repetidores intermediarios que deben ser confiables. Cada par de nodos adyacentes utiliza distribución cuántica de claves (QKD) para intercambiar claves de encriptación (Figura 2-12). Aunque tecnológicamente es un paso inicial, permite la implementación de infraestructura y desarrollo de ingeniería que puede ser actualizada posteriormente a verdaderos repetidores cuánticos.

Un mensaje clásico puede ser codificado, transmitido de forma segura a través de repetidores consecutivos, y decodificado en cada uno de ellos. Cada repetidor genera una nueva clave secreta, asegurando la transmisión segura del mensaje desde el origen hasta el destino. La seguridad de la transmisión depende de la confiabilidad de cada repetidor en la secuencia. El elemento clave es el repetidor de confianza sin preocupación por la interceptación de comunicaciones.

⁵⁵

https://www.esa.int/Applications/Connectivity_and_Secure_Communications/Advancing_Europe_s_quantum_secure_communications_from_space

⁵⁶ <https://www.ses.com/newsroom/eagle-1-advancing-europes-leadership-quantum-communications>

⁵⁷ <https://ndupress.ndu.edu/Media/News/News-Article-View/Article/2999147/the-quantum-internet-how-dod-can-prepare/>

⁵⁸ <https://quantuminternetalliance.org/>

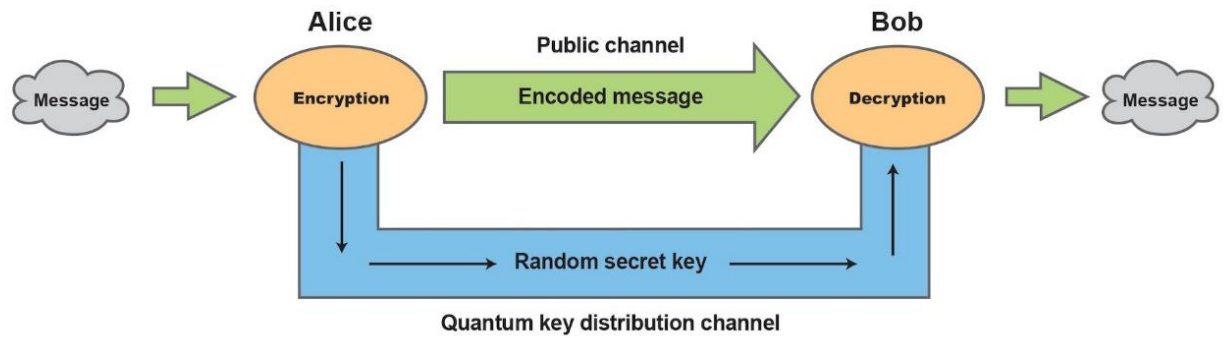


Figura 2-12 Distribución de clave cuántica [WEH 2018].

- La etapa de Redes de Preparación y Medición es la primera etapa que ofrece verdadera funcionalidad cuántica extremo a extremo, ya que permite la transmisión de información en forma de qubits. Cualquier nodo prepara un estado de un qubit y lo transmite a otro nodo, que posteriormente lo mide. La transmisión exitosa de qubits no es probable en esta etapa, y dado que es posible que se pierda un qubit el receptor debe detectar si el qubit se ha recibido antes de medirlo. Por lo tanto, todas las mediciones se “seleccionan posteriormente” en función del conocimiento de que el qubit se transmitió con éxito, y se puede ignorar cuando los qubits se pierden. Esta etapa habilita protocolos criptográficos como QKD segura entre puntos distantes sin necesidad de confiar en nodos intermedios, así como verificación segura de identidad y otras tareas de criptografía de dos partes.
- La etapa de Redes de Distribución de Entrelazamiento (Figura 2-13) permite la creación de entrelazamiento cuántico extremo a extremo de forma determinista o anunciada (probabilidad cercana a 1), junto con mediciones locales. Los nodos finales no requieren memoria cuántica en esta fase. Esta etapa es particularmente importante porque permite la implementación de protocolos independientes del dispositivo, donde los dispositivos cuánticos se modelan como cajas negras ampliamente no confiables. Esto incluye QKD independiente del dispositivo, proporcionando garantías de seguridad más fuertes. La red puede generar un par de qubits entrelazados al máximo y distribuirlos, uno al nodo A y otro al nodo B. Esta etapa podría implementarse utilizando verdaderos repetidores cuánticos, que reciben un qubit y lo entrelazan con otro que es el que difunden. Así se crea una conexión en cadena de qubits del nodo inicial al final.

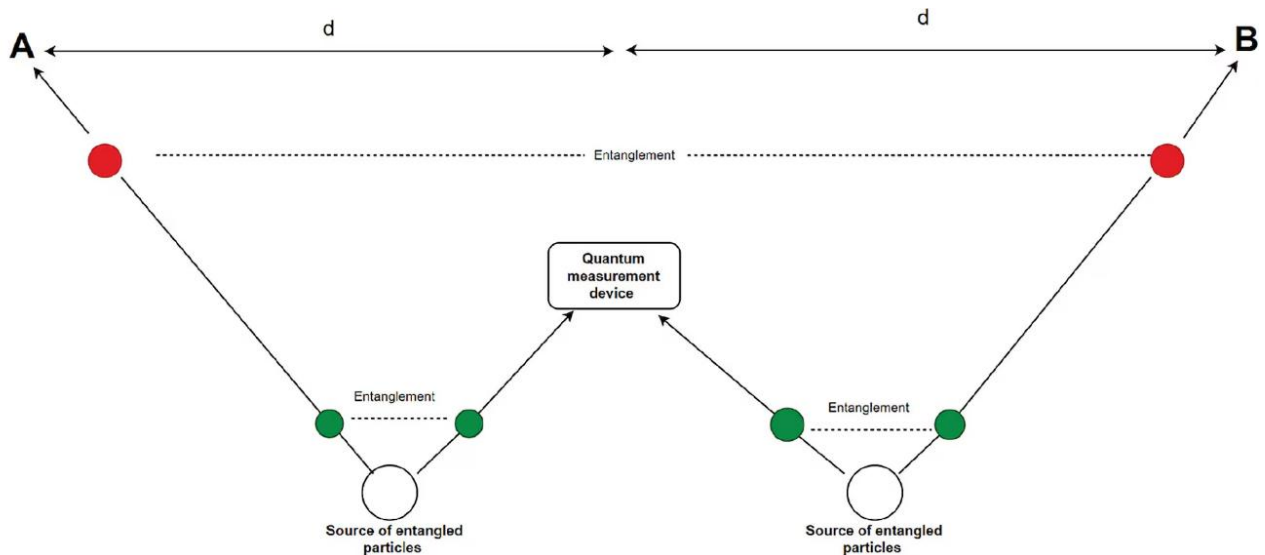


Figura 2-13 Distribución de entrelazamientos [WEH 2018].

- Las Redes de Memoria Cuántica se caracterizan por la capacidad de los nodos finales de tener memoria cuántica local con control universal simultáneo. Este enfoque hace posible el envío de estados cuánticos más grandes por teleportación cuántica, aumentando el volumen de información cuántica que se puede transmitir, y permitiendo implementar protocolos más complejos que requieren el almacenamiento temporal de un estado cuántico durante la comunicación cuántica o clásica. En esta etapa se pueden transferir qubits desconocidos de un nodo de red a otro mediante teleportación determinista (probabilidad cercana a 1). La memoria cuántica permite establecer un estado a la vez, almacenando los estados cuánticos a medida que se reciben de la red. La principal diferencia entre esta etapa y la anterior es que en esta nueva etapa varios qubits pueden moverse. Entre las aplicaciones destacadas se encuentran computación cuántica ciega o anónima (que permite a clientes usar computadores cuánticos remotos sin revelar información sobre el cálculo), intercambio de secretos cuánticos y sincronización mejorada de relojes atómicos.
- En la etapa de Redes Tolerantes a Fallos con Pocos Qubits, las operaciones locales pueden ejecutarse de forma tolerante a fallos. La tolerancia a fallos no es necesaria para muchos protocolos cuánticos conocidos, pero la disponibilidad de operaciones tolerantes a fallos permitiría la ejecución de cálculos cuánticos locales más complejos y la ampliación arbitraria de los tiempos de almacenamiento. El número de qubits permanece lo suficientemente pequeño para que los nodos finales puedan ser simulados efectivamente en computadores clásicos. La tolerancia a fallos implica que los parámetros de error puedan hacerse despreciables añadiendo más recursos. Las aplicaciones incluyen sincronización de relojes de mayor precisión y computación cuántica distribuida con pocos qubits.
- La etapa final de Redes de Computación Cuántica consiste en computadores cuánticos que pueden intercambiar comunicación cuántica arbitrariamente. A diferencia de las etapas anteriores que mejoran gradualmente la funcionalidad, esta etapa proporciona la capacidad fundamental de encontrar soluciones a problemas computacionales que no pueden resolverse eficientemente en computadores clásicos. El número de qubits lógicos es mayor que lo que puede simularse efectivamente en un computador clásico. En esta etapa se pueden realizar todos los protocolos de etapas anteriores.

El proyecto de comunicaciones y redes cuánticas del Instituto Nacional de Estándares y Tecnología estadounidense (*National Institute of Standards and Technology*, NIST)^{59,60} se centra en desarrollar dispositivos cuánticos avanzados para habilitar redes cuánticas funcionales y seguras. Su investigación aborda tecnologías clave como fuentes de fotones entrelazados, detectores de fotones individuales, memorias cuánticas ópticas e interfaces de transducción cuántica. Estas tecnologías permiten la creación, transmisión, almacenamiento y procesamiento de qubits ópticos, que son esenciales para establecer enlaces de comunicación cuántica entre nodos distantes. Se investiga el uso de materiales como el carburo de silicio (SiC), que ofrece propiedades ópticas no lineales y compatibilidad con procesos CMOS, para el desarrollo de dispositivos cuánticos integrados. El proyecto cierra el gap entre la teoría cuántica y las aplicaciones prácticas en tecnologías de la información, mediante la implementación de redes cuánticas reales. Para ello el NIST está construyendo el *NIST Gaithersburg Quantum Network* (NG-QNet) que consiste una serie de bancos de pruebas que permiten evaluar el rendimiento de componentes y protocolos en entornos de red reales. Estos bancos de pruebas incluyen plataformas para innovación en redes cuánticas, caracterización de componentes, sincronización temporal y estudio de nodos cuánticos de borde. El NIST participa en el consorcio entre diferentes agencias DC-QNet, que reúne a seis agencias federales para desarrollar una red cuántica regional no propietaria, orientada a aplicaciones como sensores distribuidos, comunicaciones seguras y computación cuántica en red y se ensayan arquitecturas, protocolos y estándares para una infraestructura cuántica interoperable y segura. Estas iniciativas buscan establecer estándares, mejores prácticas y herramientas de metrología para caracterizar redes cuánticas completas, no solo sus componentes individuales. Al integrar investigación fundamental con infraestructura experimental, el NIST contribuye al avance de redes cuánticas escalables, interoperables y robustas, sentando las bases para una futura internet cuántica. El programa *Quantum Augmented Network* (QuANET)⁶¹ de la Agencia de Proyectos de Investigación Avanzada de Defensa (*Defense Advanced Research Projects Agency*, DARPA)⁶² tiene como objeto desarrollar la primera red híbrida cuántico-clásica operativa, incorporando propiedades de seguridad y ocultamiento propias de la comunicación cuántica dentro de infraestructuras de red clásicas. Europa también trabaja en su internet cuántica a través de la iniciativa *Quantum Internet Alliance* (QIA)⁶³.

La visión a largo plazo de seguridad cuántica global requiere algo más ambicioso como el Internet Cuántico (*Quantum Internet*, QI), una red donde no solo las claves se distribuyen mediante QKD, sino donde los qubits mismos pueden ser procesados y teleportados cuánticamente entre ubicaciones distantes. Se requiere memoria cuántica de larga coherencia con tiempos de almacenamiento típicamente en microsegundos. Adicionalmente, se requieren operaciones con fidelidades superiores al 99%, un régimen aún no alcanzado en sistemas prácticos.

⁵⁹ <https://www.nist.gov/>

⁶⁰ <https://www.nist.gov/programs-projects/quantum-communications-and-networks>

⁶¹ <https://www.darpa.mil/research/programs/quantum-augmented-network>

⁶² <https://www.darpa.mil/>

⁶³ <https://quantuminternetalliance.org/>

3 APLICACIÓN DE LAS TECNOLOGÍAS CUÁNTICAS

El propósito del Capítulo 3 es identificar y analizar las aplicaciones concretas de las tecnologías cuánticas en sectores civiles y militares, demostrando cómo los fundamentos científicos y tecnológicos abordados en el Capítulo 2 se traducen en capacidades operativas y casos de uso reales. Para ello, el capítulo comienza examinando las aplicaciones de la computación cuántica y las comunicaciones cuánticas en sectores civiles, tales como la optimización industrial, el descubrimiento de fármacos, el modelado financiero, la criptografía y las comunicaciones seguras, que sirven como base para entender la traslación de estas tecnologías a contextos de defensa. A continuación, examina cómo la computación cuántica, las comunicaciones cuánticas, los sensores y metrología cuántica se aplican a capacidades militares específicas, evaluando su potencial para mejora de inteligencia, vigilancia y reconocimiento (ISR), sistemas de mando y control (C2), ciberdefensa y seguridad de comunicaciones, navegación independiente de sistemas satelitales, y optimización logística y operacional. El capítulo analiza casos de uso militares identificados en el contexto de la OTAN para computación cuántica y para comunicaciones y ciberseguridad cuántica, proporcionando ejemplos de la adopción de estas tecnologías en escenarios operativos. Finalmente, el capítulo contextualiza estas aplicaciones dentro de los horizontes de madurez tecnológica definidos en el Capítulo 1, identificando qué aplicaciones están próximas a demostración operativa en el corto plazo (TRL 6-7) y cuáles permanecen en fases de investigación y desarrollo a medio-largo plazo (TRL 3-5).

3.1 Aplicaciones en sectores civiles

3.1.1 Aplicaciones de la computación cuántica

La computación cuántica ha traído consigo nuevas formas de resolver problemas que resultan complejos para los ordenadores clásicos frente al volumen, velocidad y variedad de datos que generan las industrias modernas. Estos problemas están relacionados con la optimización, la simulación de sistemas complejos o la IA basada en cuántica. Algunos sectores en los que se han aplicado los algoritmos cuánticos han sido los sectores de la salud, financiero, logística, energía o telecomunicaciones⁶⁴ [CGM 2025, Bayerstadler 2021], entre otros.

En el ámbito de la salud, la revolución cuántica ha comenzado a transformar profundamente el análisis genómico y la medicina personalizada⁶⁵. En el campo de la genética, gracias a la capacidad de procesamiento acelerado y multidimensional, es posible analizar genomas completos en tiempos significativamente reducidos, descubrir relaciones que antes pasaban desapercibidas o analizar perfiles genéticos individuales, potenciando la medicina de precisión e individualizada. En el descubrimiento de nuevos fármacos, los algoritmos cuánticos permiten simular interacciones moleculares complejas y representar de manera más fiel de los sistemas biológicos, facilitando el diseño de tratamientos más eficaces. Además, el diagnóstico médico se beneficia de la detección automatizada de patrones en grandes volúmenes de imágenes clínicas, lo que mejora la precisión y reduce los errores humanos.

En el sector financiero, la computación cuántica está redefiniendo la detección de fraudes, la gestión de riesgos y la optimización de inversiones. Los portfolios pueden ahora ser analizados considerando múltiples variables y restricciones simultáneamente, lo que mejora la toma de decisiones

⁶⁴ https://www.meegle.com/en_us/topics/quantum-computing-applications/quantum-computing-for-big-data-analysis

⁶⁵ <https://standards.ieee.org/beyond-standards/how-can-quantum-computing-and-artificial-intelligence-transform-the-healthcare-industry/>

estratégicas. La detección de fraude se ha vuelto más eficiente gracias a la identificación de patrones anómalos en grandes volúmenes de transacciones, y la predicción de mercados se ha enriquecido con el análisis de correlaciones complejas en datos financieros. Por ejemplo, JP Morgan Chase⁶⁶ ha implementado algoritmos cuánticos para mejorar su análisis de riesgo, logrando una mayor precisión en sus modelos.

En el terreno de la logística y la optimización, los problemas complejos de mejora de rutas y reducción de costes encuentran soluciones innovadoras gracias a la computación cuántica. Volkswagen, por ejemplo, ha utilizado algoritmos cuánticos para optimizar el tráfico urbano, mejorando los tiempos de movilidad en ciudades congestionadas⁶⁷. Las cadenas de suministro se benefician de rutas más eficientes y una reducción significativa en los costos logísticos, mientras que la gestión energética se apoya en modelos predictivos para distribuir recursos y anticipar fallos. La evaluación paralela permite analizar en tiempo real millones de combinaciones simultáneamente, incluso con cambios o escalabilidad de las variables, dando soporte a la rápida toma de decisiones.

3.1.2 Aplicaciones de las comunicaciones cuánticas

Las comunicaciones cuánticas han comenzado a transformar fundamentalmente el panorama de la ciberseguridad y la protección de datos sensibles en la sociedad civil, aprovechando las garantías de seguridad proporcionadas por los principios inviolables de la mecánica cuántica. El desafío principal en la expansión de comunicaciones cuánticas en sectores civiles radica en superar las limitaciones técnicas actuales de alcance y velocidad de transmisión. Las redes de primera generación están restringidas a cientos de kilómetros debido a pérdidas en las fibras ópticas y las limitadas tasas de generación de claves seguras⁶⁸. Aunque suficientes para muchas aplicaciones, requieren de optimización para soportar volúmenes de tráfico comparables a las redes clásicas de alta velocidad. No obstante, el rápido progreso en fuentes de fotones entrelazados, detectores de alta eficiencia y repetidores cuánticos sugiere que estas limitaciones serán superadas en la próxima década, haciendo de las comunicaciones cuánticas un componente estándar de infraestructuras críticas globales.

En el sector financiero, las instituciones han reconocido la necesidad crítica de proteger transacciones de alto valor y datos de inteligencia de negocios contra amenazas cibernéticas emergentes. Bancos como JP Morgan Chase^{69,70} y fondos de inversión han iniciado proyectos piloto de QKD para proteger comunicaciones entre centros de datos, particularmente para transferencias internacionales y operaciones sensibles, reduciendo el riesgo de robo de identidades y fraude masivo y facilitando la implementación de acuerdos de confidencialidad entre instituciones financieras globales.

En las infraestructuras críticas, sectores como energía, transporte y agua han adoptado progresivamente tecnologías de comunicaciones cuánticas para proteger los sistemas de control supervisor y adquisición de datos (*Supervisory Control And Data Acquisition*, SCADA) [Biswas 2025]. Las redes cuánticas aseguran la integridad de comandos críticos que controlan plantas de energía, ferrocarriles y sistemas de distribución de agua, previniendo manipulaciones que podrían causar fallos en cascada catastróficos. Europa, a través de la iniciativa EuroQCI⁷¹, está integrando infraestructura de comunicaciones cuánticas directamente en las redes de control de infraestructuras críticas de los estados miembros, con validación operacional prevista a partir de 2026.

⁶⁶ <https://www.jpmorganchase.com/about/technology/news/jpmorganchase-qcware-evolve-hedging-for-a-quantum-future>

⁶⁷ <https://www.volkswagen-group.com/en/press-releases/volkswagen-optimizes-traffic-flow-with-quantum-computers-16995>

⁶⁸ <https://postquantum.com/post-quantum/quantum-key-distribution-qkd-cyber/>

⁶⁹ <https://www.jpmorgan.com/technology/news/firm-establishes-quantum-secured-crypto-agile-network>

⁷⁰ <https://wqs.events/case-study-how-jpmorgan-deployed-a-100-gb-s-qkd-secured-vpn-in-singapore/>

⁷¹ <https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci>

En el sector de telecomunicaciones, operadores como China Telecom⁷² y BT Group⁷³ han desplegado redes QKD metropolitanas que protegen las comunicaciones de sus clientes corporativos. Estas redes no solo garantizan confidencialidad, sino que también permiten ofrecer servicios de comunicaciones cuánticas como valor añadido diferencial en un mercado altamente competitivo.

En el sector de salud, la protección de datos de pacientes, registros médicos electrónicos y resultados de investigaciones clínicas ha adquirido importancia crítica. Hospitales⁷⁴ y organizaciones de investigación farmacéutica han comenzado a integrar QKD en sus infraestructuras de comunicación para garantizar la confidencialidad de información médica sensible.

Los sectores académico y de investigación, universidades y laboratorios científicos internacionales dependen de la transmisión segura de datos de investigación, resultados experimentales y colaboraciones intelectuales entre instituciones. La *Quantum Internet Alliance* (QIA)⁷⁵ en Europa ha fomentado la adopción de infraestructura cuántica en institutos de investigación, permitiendo que grupos científicos distribuidos globalmente colaboren sin riesgo de exposición de datos. Esta infraestructura es especialmente crítica para campos como la física de altas energías y la astrofísica, donde la replicación de experimentos depende de la autenticidad garantizada de los datos transmitidos.

En el contexto gubernamental, las administraciones públicas europeas han comenzado a desplegar infraestructura QKD para proteger comunicaciones administrativas sensibles, datos de ciudadanos e infraestructuras críticas, dentro del marco de la iniciativa paneuropea EuroQCI. En España, MadQCI, la mayor red de comunicaciones cuánticas de Europa, integra instituciones públicas, universitarias y de investigación en Madrid para validar casos de uso en sectores críticos⁷⁶. A nivel internacional, Corea del Sur⁷⁷, Austria⁷⁸ y Suiza⁷⁹ han implementado proyectos piloto demostrando la viabilidad de proteger servicios de gobierno digital con comunicaciones cuánticas.

3.2 Aplicación a las capacidades militares

Los ejércitos más poderosos aprovechan la ventaja del uso de las tecnologías más avanzadas. Para adoptar nuevas tecnologías en el sector de Defensa se deben tener en cuenta aspectos tales como las capacidades que proporcionarán y el impacto de estas, así como el horizonte temporal de madurez tecnológica hacia su integración en un sistema completamente operativo.

En el contexto militar, las tecnologías cuánticas no representan únicamente la aparición de una nueva familia de armas, sino que su relevancia radica en la capacidad de añadir nuevas funcionalidades a los sistemas existentes o transformar radicalmente la eficacia de operaciones clave [Krelina 2021, Krelina 2025_1, Krelina 2025_2] (Figura 3-1). La segunda revolución cuántica traerá consigo la mejora significativa en las capacidades militares que requieren del análisis de grandes volúmenes de datos; la modelización y la simulación; y la optimización, mejorando la gestión eficaz de recursos y suministros, la predicción de acciones del adversario y la toma de decisiones. La potencia de cálculo

⁷² <https://thequantuminsider.com/2025/05/20/china-telecom-launches-hybrid-quantum-safe-encryption-system-completes-1000-kilometer-secure-call/>

⁷³ <https://www.global.toshiba/ww/news/corporate/2022/04/news-20220427-01.html>

⁷⁴ <https://www.luxquanta.com/luxquanta-telefonica-vithas-and-qoolnet-shield-hospitals-against-quantum-attacks-n-72-en>

⁷⁵ <https://quantuminternetalliance.org/>

⁷⁶ <https://madqci.es/>

⁷⁷ <https://www.idquantique.com/quantum-safe-security/nation-wide-quantum-safe-key-distribution-network-in-south-korea/>

⁷⁸ <https://www.cancom.at/en/press/austria-is-a-pioneer-in-quantum-cryptography-for-protecting-data-critical-infrastructures>

⁷⁹ <https://www.businesswire.com/news/home/20251105758890/es>

proporcionada por los ordenadores y los algoritmos cuánticos permitirá resolver ciertos tipos de problemas complejos a velocidades inalcanzables por los ordenadores clásicos. El uso en la seguridad de la información permitirá que técnicas como la distribución cuántica de claves o el desarrollo de redes de comunicaciones cuánticas mejoren la confidencialidad de las comunicaciones militares. Por otro lado, el criptoanálisis de los datos y la identificación de las vulnerabilidades, con una rapidez sin precedentes, comprometerán la seguridad de las comunicaciones y los sistemas de información del adversario. La mayor precisión en la detección y medida de los sensores cuánticos mejorará las capacidades de vigilancia, detectando cambios mínimos y patrones en el entorno y anticipando las amenazas, y la navegación de alta precisión y resistente a interferencias incluso en entornos de degradación o denegación de GPS.

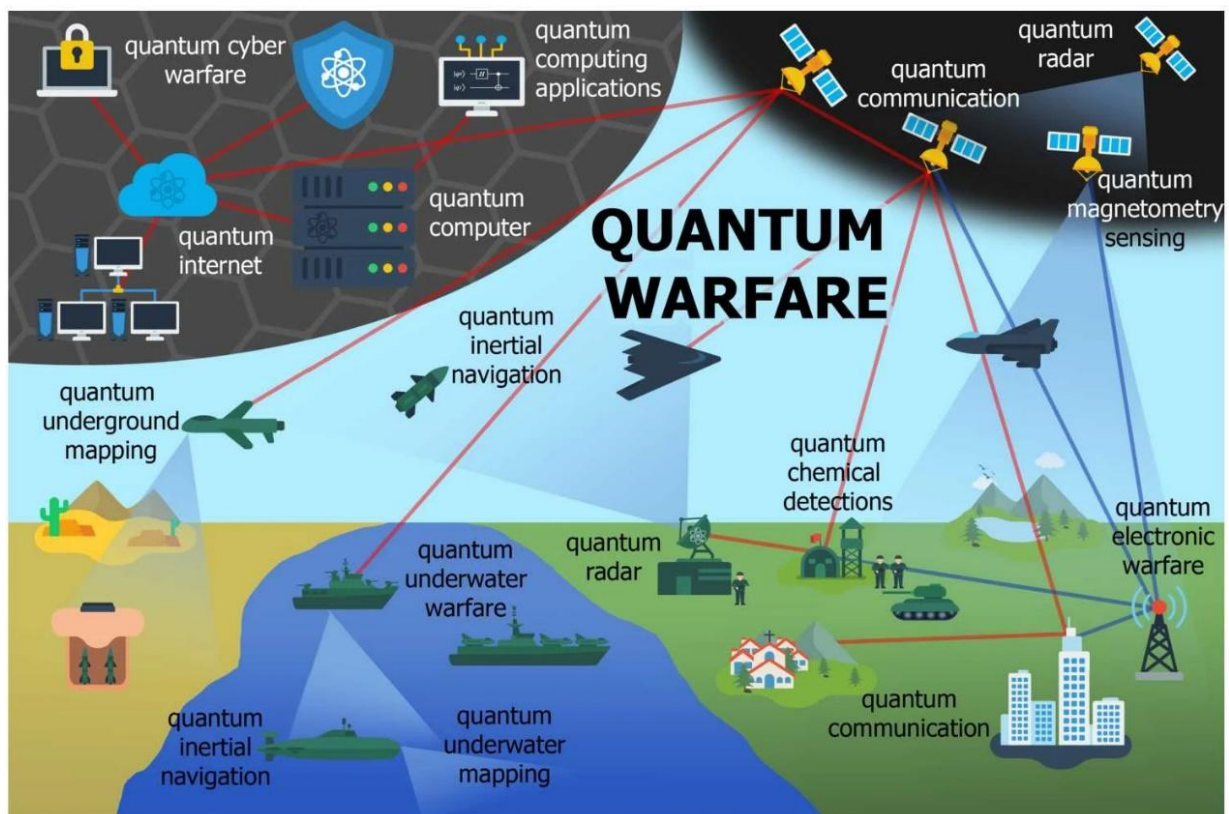


Figura 3-1 Esquema de un conflicto bélico empleando varios sistemas basados en tecnologías cuánticas [Krelin 2021].

Así, las tecnologías cuánticas afectarán a las capacidades militares de Mando y Control Integrado, Conocimiento de la Situación, Sostenimiento y Supervivencia y Protección.

Existen varias maneras de clasificación funcional y estratégica de las tecnologías cuánticas de aplicación a las capacidades militares. No son excluyentes, ya que una misma tecnología puede encajar en varios bloques o categorías. La clasificación más habitual en este tipo de tecnologías y sus potenciales aplicaciones son, entre otras:

- La computación cuántica: ordenadores cuánticos digitales y analógicos, circuitos cuánticos no programables o simuladores cuánticos, algoritmos cuánticos (optimización, modelización, simulación, IA basada en cuántica, etc.), y la integración de la computación cuántica y la clásica.

- Las comunicaciones cuánticas: distribución de clave cuántica, generadores de números aleatorios cuánticos y redes y comunicaciones cuánticas.
- Los sensores (y la metrología) cuánticos: magnetómetros y gravímetros; acelerómetros, giróscopos y sincronización del tiempo de alta precisión; o sensores radar y electroópticos cuánticos de baja relación señal-ruido (*Signal-to-Noise-Ratio*, SNR); así como otros sensores otros avanzados que explotan el entrelazamiento y la coherencia cuántica.
- Los algoritmos de inspiración cuántica sobre computación clásica y la criptografía post-cuántica o algoritmos seguros a la cuántica.

La clasificación estratégica según el impacto esperado en defensa sería:

- Tecnologías imprescindibles: criptografía post-cuántica.
- Tecnologías que aumentan la efectividad de las capacidades actuales: optimización cuántica o la inteligencia artificial cuántica.
- Tecnologías que incrementan la precisión de la medida: magnetometría, gravimetría, navegación inercial o sincronización del tiempo.
- Tecnologías que proporcionan capacidades completamente nuevas: radar cuántico, simulaciones químicas cuánticas, criptoanálisis cuántico o, distribución cuántica de claves.

Aunque la clasificación anterior incluye el dominio de los sensores y la metrología, el presente trabajo se centra esencialmente sobre las disciplinas de computación cuántica y comunicaciones cuánticas, y los algoritmos de inspiración cuántica sobre computación clásica y la criptografía post-cuántica o algoritmos seguros a la cuántica.

3.2.1 Computación cuántica

La arquitectura de la computación cuántica de uso en aplicaciones militares se divide principalmente en dos categorías fundamentales, los ordenadores cuánticos digitales y los analógicos. Los ordenadores cuánticos digitales, o de puertas lógicas, son sistemas universales y programables que utilizan qubits fijos manipulados mediante secuencias de puertas para ejecutar cualquier algoritmo cuántico disponible. Los ordenadores cuánticos digitales constituyen el modelo de computación cuántica con mayor potencial para aplicaciones militares de amplio espectro. En contraste, los ordenadores cuánticos analógicos, frecuentemente implementados mediante técnicas de *quantum annealing*, se especializan en la resolución de problemas de optimización guiando al sistema cuántico hacia su estado de menor energía. Adicionalmente, los simuladores cuánticos operan como circuitos no programables diseñados específicamente para replicar sistemas cuánticos naturales, especialmente moléculas e interacciones químicas complejas.

La integración de estas arquitecturas en Defensa no busca reemplazar a los sistemas clásicos, sino funcionar bajo un modelo híbrido en el que los ordenadores cuánticos trabajarían como aceleradores especializados para sub tareas específicas. En este modelo, los sistemas clásicos manejarían las funciones de control, entrada y salida de datos, y corrección de errores, mientras que los procesadores cuánticos se especializarían en tareas como simulación, optimización y ciertos algoritmos criptográficos [Pan 2025]. La implementación militar de esta arquitectura híbrida se visualiza a través de granjas de computación, que combinarían recursos clásicos y cuánticos donde un sistema operativo híbrido analizaría las tareas computacionales distribuyendo los cálculos entre recursos como CPU (*Central Processing Unit*), GPU (*Graphics Processing Unit*) y unidades de procesamiento cuántico (*Quantum Processing Units*, QPU).

La integración práctica de sistemas cuánticos y clásicos en entornos militares operativos presenta desafíos técnicos significativos. Los ordenadores cuánticos actuales requieren sistemas criogénicos para mantener la coherencia cuántica, lo que limita su implementación en plataformas móviles militares. Sin embargo, el desarrollo de qubits alternativos basados en fotónica, espín o centros de

nitrógeno-vacante en diamante, que pueden operar a temperatura ambiente, representa un área prioritaria de investigación para aplicaciones militares embarcadas [Ladd 2010]. Los chips cuánticos embarcados podrían realizar tareas analíticas simples u operaciones relacionadas con aplicaciones de redes cuánticas donde se requiere procesamiento directo de datos cuánticos.

Los principales dominios de aplicación y casos de uso de la computación cuántica serían:

- **Optimización Logística y Operativa:** Los problemas de logística militar, caracterizados por grandes volúmenes de datos, múltiples variables y restricciones dinámicas, superan a menudo la capacidad de respuesta de las herramientas digitales clásicas. Los ordenadores cuánticos, especialmente los *quantum annealers*, y los algoritmos de optimización como el Algoritmo de Optimización Aproximada Cuántica (*Quantum Approximate Optimization Algorithm*, QAOA) ofrecen capacidades superiores para abordar problemas combinatorios a gran escala. Los casos de uso incluyen la resolución eficiente de problemas como el del viajante (*Traveling Salesman Problem*, TSP) y el de rutas de vehículos (*Vehicle Routing Problem*, VRP). Esto se traduce operativamente en la asignación óptima de vehículos, personal y suministros en teatros de operaciones y la planificación de misiones complejas. En el corto plazo, los sistemas NISQ permiten abordar problemas de optimización específicos donde la ventaja cuántica es alcanzable antes de la corrección de errores completa. Estas aplicaciones incluyen además de la logística, la gestión de energía y el mantenimiento predictivo de plataformas, el análisis del espectro de radiofrecuencia y la programación de tareas satelitales (*satellite tasking*), optimizando recursos críticos en entornos operativos.
- **Modelización y Simulación Estratégica (“Wargaming”):** En el entorno estratégico, los decisores deben gestionar escenarios que integran factores diplomáticos, de información, militares, económicos, financieros, de inteligencia y de aplicación de la ley (marco DIMEFIL⁸⁰). Un escenario estratégico típicamente incluye cientos de variables interdependientes, retroalimentaciones dinámicas y efectos en cadena que cambian rápidamente a medida que se introducen nuevos datos (negociaciones diplomáticas, sanciones económicas, despliegues militares, campañas de información y amenazas cibernéticas). Los métodos clásicos de simulación, como los modelos basados en ecuaciones diferenciales, análisis de Monte-Carlo o juegos de simulación tradicionales, son capaces de tratar subconjuntos de este problema, pero rápidamente colapsan cuando el número de combinaciones posibles supera los límites computacionales. Sin embargo, la simulación cuántica puede representar de forma nativa sistemas con millones de grados de libertad, lo que reduce exponencialmente el número de operaciones frente a los métodos clásicos. Mediante algoritmos como Trotter-Suzuki o simuladores variacionales (*Variational Quantum Eigensolver*, VQE), es posible explorar simultáneamente miles de configuraciones de escenarios “qué pasaría si”. Esto facilita la actualización en tiempo real de los análisis estratégicos y la teoría de juegos, permitiendo respuestas rápidas ante eventos emergentes como ciberataques o cambios bruscos en la postura militar adversaria.
- **Simulación de Materiales y Amenazas QBRN:** La capacidad de simular sistemas moleculares complejos, inaccesibles para la computación clásica, habilita el desarrollo de nuevos materiales de defensa, como blindajes o explosivos, y la investigación avanzada en amenazas Químicas, Biológicas, Radiológicas y Nucleares (QBRN). Los simuladores cuánticos pueden modelar moléculas de tamaño medio con gran precisión, como por ejemplo la molécula del Sarín cuya simulación requeriría aproximadamente 250 qubits lógicos. Esta capacidad presenta una

⁸⁰ Instrumentos del poder nacional utilizados en los análisis en entornos estratégicos y militares: *Diplomacy* (Diplomacia), *Information* (Información), *Military* (Militar) y *Economic* (Económico), y adicionalmente, *Financial* (Financiero), *Intelligence* (Inteligencia) y *Law Enforcement* (Aplicación de la ley).

dualidad operativa, facilita el diseño de contramedidas y nuevos fármacos o antídotos, pero también plantea preocupaciones sobre el potencial desarrollo de nuevos agentes de guerra QBRN por parte de adversarios.

- **Inteligencia, Vigilancia y Reconocimiento (ISR):** La computación cuántica potencia el análisis de grandes volúmenes de datos heterogéneos y no estructurados provenientes de fuentes de inteligencia, vigilancia y reconocimiento (*Intelligence, Surveillance and Reconnaissance*, ISR), como IMINT (*Imagery Intelligence*), SIGINT (*Signals Intelligence*), OSINT (*Open Source Intelligence*) y GEOINT (*Geospatial Intelligence*). Aunque la implementación de la inteligencia artificial completamente cuántica presenta limitaciones significativas debido a la baja eficiencia en el procesamiento de datos clásicos, la inteligencia artificial mejorada cuánticamente (*Quantum Machine Learning*) ofrece ventajas sustanciales en tareas específicas [Biamonte 2017]. Algoritmos como las Máquinas de Vectores de Soporte Cuánticas (*Quantum Support Vector Machines*, QSVM) y las Máquinas de Boltzmann Cuánticas (*Quantum Boltzmann Machines*, QBM) proporcionan una aceleración significativa en el procesamiento de datos, la fusión de fuentes heterogéneas y la correlación de señales, lo que permitiría indexar bases de datos masivas, extraer correlaciones complejas, y detectar anomalías y patrones sutiles, optimizando la toma de decisiones en tiempo real. Asimismo, las Redes Generativas Antagónicas Cuánticas (*Quantum Generative Adversarial Networks*, QGAN) permiten crear datos sintéticos para entrenamiento, y las Redes Neuronales Convolucionales Cuánticas (*Quantum Convolutional Neural Networks*, QCNN) prometen procesar imágenes y vídeos ISR a velocidades sin precedentes.
- **Criptanálisis y Seguridad de la Información:** El avance de la computación cuántica plantea una amenaza existencial para la criptografía asimétrica tradicional. Un ordenador cuántico criptográficamente relevante podría ejecutar el algoritmo de Shor para romper cifrados RSA-2048 o ECC (*Elliptic Curve Cryptography*), exponiendo las comunicaciones y datos clasificados de los sistemas propios o adversarios. La computación cuántica también ofrece oportunidades, como la posibilidad de realizar pruebas avanzadas de seguridad, revelar vulnerabilidades en los sistemas de cifrado clásicos y mejorar la eficiencia de las operaciones de defensa y seguridad. A corto plazo, la realización de experimentos sobre hardware cuántico disponible, para evaluar el impacto real de la computación cuántica sobre la seguridad criptográfica militar incluye, evaluar la viabilidad de utilizar el algoritmo de Shor para romper cifrados RSA-2048 o ECC, implementar el algoritmo de Grover para analizar la resistencia de funciones hash y cifrados simétricos militares, y simular ataques de canal lateral asistidos por inteligencia artificial cuántica sobre hardware criptográfico militar. También se propone investigar el potencial de los algoritmos híbridos cuántico-clásicos para acelerar ataques contra sistemas criptográficos militares y comparar su rendimiento con los métodos clásicos. La amenaza de la computación cuántica criptográficamente relevante subraya el riesgo de estrategias adversarias de “cosechar ahora, descifrar después”, obligando a la transición inmediata hacia la criptografía post-cuántica. Desde un punto de vista defensivo, las redes neuronales cuánticas proporcionarán mayor capacidad y velocidad en el reconocimiento de patrones, siendo esenciales para el desarrollo de sistemas de ciberdefensa biomiméticos que protegerán las redes de forma análoga a como lo hacen los sistemas inmunológicos en los organismos biológicos.
- **Computación cuántica distribuida y en la nube:** La arquitectura en la nube emerge como un modelo particularmente relevante para aplicaciones militares, donde el acceso a recursos cuánticos especializados a través de redes seguras permite a las fuerzas militares aprovechar capacidades computacionales avanzadas sin requerir la implementación local de sistemas cuánticos complejos. Este modelo, conocido como computación cuántica como servicio (*Quantum Computing as a Service*, QCaaS), ya está comercialmente disponible y permite

acceso a cualquier persona interesada en computación cuántica. Para aplicaciones militares, este paradigma debe complementarse con protocolos de computación cuántica ciega [BFK 2009], que permiten la ejecución de algoritmos en ordenadores cuánticos remotos sin revelar el algoritmo, los datos de entrada o los resultados al proveedor del servicio.

Para que la computación cuántica pueda aplicarse eficazmente para resolver estos problemas es fundamental contar con datos operativos de alta calidad y codificados en formatos compatibles con la computación cuántica; la definición clara de los problemas, incluyendo todas las restricciones y objetivos, que aprovechen el potencial de la computación cuántica; la seguridad de los datos en entornos cuánticos e híbridos cuántico-clásico para la experimentación y el despliegue de estas tecnologías; y la integración e hibridación con las infraestructuras y sistemas actuales con una transición cuidadosa que no interrumpa los flujos operativos actuales.

Actualmente, la madurez tecnológica de los *quantum annealers* y simuladores se sitúa en un nivel de demostración relevante (TRL 5), mientras que los ordenadores cuánticos universales permanecen entre TRL 3 y 4. Las capacidades NISQ actuales son válidas para pequeños problemas de optimización combinatoria, simulación y *machine learning* cuántico, pero se requiere de FTQC con suficientes qubits lógicos para lograr un impacto operativo crítico y escalable en la próxima década.

3.2.2 Las comunicaciones cuánticas, la criptografía post-cuántica y los algoritmos de inspiración cuántica

La aplicación de las tecnologías cuánticas en el dominio de los sistemas de información no se limita exclusivamente al hardware cuántico, sino que abarca un espectro que va desde las redes de comunicaciones físicamente seguras hasta los algoritmos avanzados sobre hardware clásico.

- Comunicaciones Cuánticas y QKD: Las comunicaciones cuánticas combinan la Distribución de Clave Cuántica (QKD) y las redes cuánticas para ofrecer seguridad física garantizada por principios fundamentales cuánticos. La QKD permite generar y compartir claves simétricas donde cualquier intento de interceptación (*eavesdropping*) altera el estado cuántico, siendo detectado inmediatamente. La integración de los sistemas cuánticos con las infraestructuras convencionales militares demanda soluciones híbridas y protocolos estandarizados para garantizar la interoperabilidad. En contextos militares, la QKD es ideal para asegurar enlaces de mando y control (C2) entre centros de operaciones e inteligencia. La interoperabilidad con sistemas de Interconexión de Redes Privadas (*Private Network Interconnect*, PNI) y con las Infraestructuras de Clave Pública (*Public Key Infrastructure*, PKI) se logra integrando módulos de seguridad hardware (*Hardware Security Module*, HSM) con interfaces QKD, reforzando la resistencia ante la interceptación masiva. Esta integración permite que las claves generadas mediante QKD puedan utilizarse directamente en los mecanismos criptográficos existentes. Además de la seguridad en el cifrado, estas redes permiten la transferencia de tiempo y sincronización precisa, una capacidad crítica para coordinar sistemas radar, activos de guerra electrónica y plataformas distribuidas en entornos operativos.

La evolución de estas redes se estructura en tres generaciones:

- Primera Generación: Redes QKD operativas comercialmente que funcionan mediante enlaces ópticos dedicados a través de fibra óptica o canales de espacio libre, donde los estados cuánticos son generados, transmitidos y medidos para establecer una clave secreta común entre usuarios distantes. Estas redes presentan limitaciones significativas en términos de rango y escalabilidad, estando típicamente restringidas a distancias de aproximadamente 100 kilómetros debido a la pérdida de fotones en las fibras ópticas dedicadas. Para superar esta limitación de distancia las redes de primera generación emplean repetidores de confianza (*trusted nodes*), que son nodos intermedios que descifran

y vuelven a cifrar las claves cuánticas antes de reenviarlas. El protocolo MDI-QKD introduce nodos de medición independientes para conectar múltiples terminales sin exponer la clave, habilitando topologías de estrella y el primer atisbo de redes cuánticas escalables.

- Segunda Generación: Introduce repetidores cuánticos que extienden el entrelazamiento sin exponer la clave a nodos intermedios, superando las limitaciones de atenuación y decoherencia en enlaces más largos. Estas redes trascienden las limitaciones de la simple distribución de claves para permitir el entrelazamiento de sistemas cuánticos complejos distribuidos, incluyendo sensores cuánticos y computadoras cuánticas. Requieren componentes avanzados como memorias cuánticas, repetidores cuánticos genuinos, fuentes avanzadas de entrelazamiento, dispositivos de destilación de entrelazamiento y sistemas de transducción cuántica-clásica para la conversión entre diferentes modalidades físicas. Los repetidores cuánticos de segunda generación operan bajo principios fundamentalmente diferentes a los repetidores de confianza, utilizando el almacenamiento cuántico y la sincronización de fotones entrelazados a través de largas distancias. Estos dispositivos requieren memorias cuánticas capaces de almacenar y sincronizar información cuántica durante períodos prolongados. Las redes de segunda generación permiten la comunicación cuántica directa, la computación cuántica distribuida, las redes de sensores cuánticos y otros protocolos avanzados que van más allá de la simple distribución de claves.
- Tercera Generación: Representan la visión más ambiciosa de las comunicaciones cuánticas, aspirando a crear redes cuánticas globales que requieren tanto estandarización como interoperabilidad para asegurar que componentes de múltiples proveedores y múltiples generaciones de equipos puedan operar sin problemas como las redes clásicas globales actuales. Las tecnologías son actualmente experimentales, requiriendo avances significativos tanto en las tecnologías fundamentales como en la infraestructura de soporte. Estas redes necesitarán enlaces tanto terrestres como basados en satélites, sistemas de gestión de red altamente sofisticados y marcos de software robustos para la asignación de recursos, protocolos de enrutamiento e interfaces de aplicación.

Existe una correspondencia funcional directa entre las tres generaciones y las cinco etapas de la internet cuántica (apartado 2.6.2), donde la Primera Generación de redes implementa la Etapa 1 (Repetidores de Confianza), la Segunda Generación habilita las Etapas 3 y 4 (Distribución de Entrelazamiento y Memoria Cuántica), y la Tercera Generación materializa la Etapa 6 (Redes de Computación Cuántica).

- Generadores de Números Aleatorios Cuánticos (QRNG): Los Generadores de Números Aleatorios Cuánticos (QRNG) constituyen un componente fundamental que aprovecha fenómenos como la emisión de fotones o las fluctuaciones del vacío para generar entropía verdaderamente impredecible, en contraste con los generadores de números pseudoaleatorios clásicos que dependen de algoritmos deterministas y son vulnerables a la predicción adversaria o la ingeniería inversa.

Los QRNG se utilizan para generar claves criptográficas reforzando el cifrado de las VPN de alta seguridad y mejorando la autenticación multifactor mediante tokens basados en QRNG. Adicionalmente, los QRNGs facilitan el almacenamiento seguro de claves criptográficas cuántico-seguras que aseguran la transmisión y almacenamiento. En el ámbito militar, protegen las comunicaciones críticas y los datos militares clasificados de inteligencia, vigilancia y reconocimiento (*Intelligence, Surveillance and Reconnaissance*, ISR), inteligencia geoespacial (*Geospatial Intelligence*, GEOINT), inteligencia sobre señales (*Signals Intelligence*, SIGINT) e inteligencia sobre imágenes (*Imagery Intelligence*, IMINT), almacenados en redes tácticas en la nube y borde o transmitidos a través de las redes de misión. Los QRNG deben integrarse en

diferentes elementos de la infraestructura, como los módulos criptográficos militares, los sistemas de gestión de claves (*Key Management Systems*, KMS) y las Autoridades de Certificación (*Certificate Authority*, CA) militares para cifrado y autenticación de la infraestructura PKI. También en dispositivos tácticos en el borde, como radios definidas por software (*Software Defined Radios*, SDR), radios seguras y comunicaciones satélites (*Satellite Communications*, SATCOM) cifradas, así como infraestructura en la nube militar y redes de datos tácticas en el campo de operaciones.

La disponibilidad comercial actual de chips QRNG permite su integración inmediata en sistemas militares existentes, proporcionando beneficios de seguridad tangibles sin requerir el desarrollo de infraestructura cuántica completamente nueva. La naturaleza verificable de los QRNGs también proporciona ventajas operativas en entornos militares, donde la certificación de seguridad criptográfica (como NIST SP800-90B [NIST 2018]), que asegure la aleatoriedad libre de sesgos, y la validación de procedimientos criptográficos son requisitos críticos para el despliegue operacional. Los QRNGs pueden tener dificultades para producir números aleatorios a las altas tasas requeridas por aplicaciones como la computación en nube segura. La mitigación propuesta implica usar enfoques criptográficos híbridos que combinen QRNG con cifrado existente. La escalabilidad para redes federadas y de coalición presenta el desafío significativo de la interoperabilidad, por lo que se requiere el establecimiento de estándares QRNG dentro de los marcos de cifrado. La resistencia a intentos de hackeo cuántico constituye un riesgo adicional, requiriendo el despliegue de detección de amenazas impulsada por IA para el uso de claves criptográficas mejoradas con QRNG, mientras que la seguridad de la cadena de suministro de hardware QRNG debe asegurar la certificación mediante estándares militares aprobados.

- **Criptografía Post-Cuántica (PQC):** La Criptografía Post-Cuántica representa una iniciativa fundamental dentro de las comunicaciones cuánticas, que asegurará el cifrado de las comunicaciones militares de operaciones multidominio antes de que la QKD y las comunicaciones cuánticas seguras estén disponibles a gran escala. Ante la amenaza de que los futuros ordenadores cuánticos comprometan los esquemas actuales de clave pública (RSA, ECC, *Diffie-Hellman*), la Criptografía Post-Cuántica (PQC) se establece como una capacidad de defensa inmediata. Esta tecnología abarca algoritmos basados en retículos, criptografía isogénica, esquemas basados en hash, sistemas multivariados y criptografía basada en códigos. A diferencia de la Distribución de Clave Cuántica (QKD), que es probablemente segura desde una perspectiva matemática, todos los algoritmos de criptografía post-cuántica no son probablemente seguros y requieren procesos rigurosos de estandarización, análisis e implementación para evitar vulnerabilidades que podrían ser explotadas incluso por computadores clásicos.

En el ámbito de Defensa, la PQC es crítica para proteger las redes C4ISR (*Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance*), las comunicaciones tácticas y el Internet de Cosas Militares (*Internet of Military Things*, IoMT). Su implementación es urgente debido a la estrategia adversaria de “cosechar ahora, descifrar después” (*harvest now, decrypt later*), donde datos sensibles cifrados hoy podrían ser vulnerados en el futuro. Esta amenaza es particularmente crítica para los sectores militar, de inteligencia y gubernamental, donde secretos y datos confidenciales se intercambian o almacenan con períodos de clasificación que se extienden más allá del horizonte temporal esperado para la disponibilidad de computadores cuánticos criptográficamente relevantes.

La ventaja estratégica de la PQC radica en que es una solución de software desplegable sobre redes existentes, sin requerir una nueva infraestructura como la QKD o las comunicaciones cuánticas seguras, permitiendo asegurar las operaciones multidominio antes de que la

infraestructura cuántica física esté disponible a gran escala. Los desafíos de despliegue incluyen la integración y el rendimiento. La actualización de protocolos (TLS, IPsec, SSL, HTTPS, SSH, etc.) y dispositivos (servidores web, dispositivos de red, sistemas de autenticación, PKIs, sistemas de acceso remoto, plataformas en la nube, correo electrónico, etc.) no es una operación inmediata. Además, la implementación de los algoritmos PQC demandarán una mayor capacidad computacional, memoria y ancho de banda comparado con la criptografía clásica, al emplear algoritmos más complejos y tamaños de clave más grandes. Esto puede impactar en el cifrado en tiempo real en redes ISR de alta velocidad y comunicaciones de campo de operaciones. La solución propuesta implica optimizar las implementaciones PQC para sistemas embebidos de grado militar y aplicaciones de baja latencia. La gestión segura de claves para fuerzas desplegadas en entornos tácticos y móviles presenta otro desafío significativo. Los retos incluyen distribuir claves basadas en PQC a fuerzas desplegadas en entornos desconectados, requiriendo desarrollar sistemas de gestión de claves compatibles con PQC para operaciones militares distribuidas. Las contramedidas adversarias y ataques de canal lateral representan amenazas adicionales, ya que naciones hostiles pueden desarrollar contramedidas para atacar implementaciones PQC mediante ataques de canal lateral o manipulación física, requiriendo que se lleven a cabo evaluaciones continuas de vulnerabilidad y se implementen sistemas PQC resistentes a ataques físicos y cibernéticos. Un ejemplo de esta vulnerabilidad física se aborda en el proyecto SCA-QS (*Side-Channel Attacks with Quantum Sensing*)⁸¹, que investiga cómo la extrema sensibilidad de la magnetometría cuántica podría permitir nuevos vectores de ataque de canal lateral capaces de comprometer la seguridad de los microchips y el hardware criptográfico.

- Algoritmos de inspiración cuántica: Los algoritmos de inspiración cuántica representan un puente paradigmático entre la computación clásica y cuántica, surgiendo de la necesidad de aprovechar entendimientos derivados de principios cuánticos para resolver problemas complejos en sistemas computacionales convencionales. Estos algoritmos emergen cuando la comunidad científica observa que ciertas estrategias algorítmicas desarrolladas originalmente para computadores cuánticos pueden adaptarse para funcionar en hardware clásico, a menudo proporcionando mejoras computacionales sin requerir la infraestructura especializada que demandan los sistemas cuánticos reales. En optimización cuántica, métodos como QAOA han inspirado algoritmos clásicos que no requieren hardware cuántico, pero adoptan sus estrategias de exploración del espacio de soluciones.

En contextos militares, estos algoritmos híbridos encuentran aplicaciones inmediatas en la resolución de problemas complejos de logística, planificación de misiones, programación de juegos de guerra y la verificación y validación de sistemas militares. La naturaleza dual de estos algoritmos permite a las organizaciones militares beneficiarse de los entendimientos cuánticos sin las exigencias de los nuevos procesadores cuánticos.

Desde una perspectiva operativa, la madurez tecnológica varía significativamente. La QKD se encuentra en niveles TRL 8-9 con soluciones comerciales disponibles para protección de infraestructuras críticas, mientras los repetidores cuánticos necesarios para redes globales permanecen en fases de investigación (TRL < 5). Por su parte, PQC y QRNG alcanzan grados de disponibilidad comercial más avanzados, respectivamente entre TRL 7 a 8 y TRL 7 y 9, y están listos para su adopción en infraestructuras terrestres y satelitales, bancos de pruebas y sistemas de ciberdefensa, permitiendo una transición gradual hacia capacidades cuánticas completas. La experimentación de QKD englobaría las demostraciones de comunicaciones seguras, y pruebas de rendimiento y vulnerabilidad entre nodos a través de infraestructura terrestre y espacial, pero también en entornos

⁸¹ <https://www.cyberagentur.de/en/programs/sca-qs/>

tácticos a través de dispositivos portables. PQC y QRNG se emplearían en casos de uso análogos, adaptando algoritmos y generadores de claves a las diferentes infraestructuras y redes de comunicaciones de mando y control terrestres y SATCOM, entornos tácticos en operaciones militares, bancos de pruebas y sistemas de ciberdefensa.

3.2.3 Casos de uso militares en el ámbito OTAN

Como referíamos en el apartado 1.2, la OTAN identifica las Tecnologías Cuánticas como esenciales para preservar la superioridad estratégica y operacional. Consecuencia de ello ha sido la publicación de la primera estrategia en tecnologías cuánticas en enero de 2024 (apartado 5.4.4).

La *Science & Technology Organization* (STO)⁸² de la OTAN actúa como el centro científico-técnico de la Alianza para las tecnologías disruptivas, proporcionando investigación, análisis, experimentación y asesoramiento. La STO organiza simposios especializados, produce informes estratégicos y técnicos y analiza aplicaciones militares. Todo ello alimenta la estrategia cuántica de la OTAN y las decisiones informadas de defensa de los Aliados.

El *Allied Command Transformation* (ACT)⁸³ de la OTAN, como comando de desarrollo estratégico de capacidades de combate, examina la aplicación militar de las EDT. Con ese propósito, ACT selecciona y prioriza una serie de casos de uso destinados a validar su utilidad militar y en colaboración con la industria y la academia llega a la experimentación y la demostración de las soluciones más maduras. El principal objetivo de esos casos de uso militares es apoyar la supervisión, experimentación, evaluación comparativa e implantación oportuna de las EDT en las capacidades militares financiadas nacional o comúnmente por la OTAN

Los casos de uso identificados en el entorno OTAN relevantes para demostrar el impacto de las tecnologías cuánticas en las capacidades militares han sido, entre otros, la aplicación de la computación cuántica a la optimización logística y mantenimiento predictivo, a la simulación estratégica, a la criptografía o a la inteligencia artificial y *Machine Learning*; y el uso de las comunicaciones y ciberseguridad cuántica en comunicaciones seguras cuánticas, en procesos cuánticos de distribución segura de claves (*Quantum Key Distribution*, QKD) o en criptografía post-cuántica (*Post Quantum Cryptography*, PQC).

3.2.4 Operatividad militar de las tecnologías cuánticas

Como conclusión al análisis de las capacidades militares y su estado de desarrollo, resulta necesario correlacionar cada tecnología cuántica con su nivel de madurez (TRL) actual para definir una estrategia de adopción coherente. Esta clasificación permite distinguir claramente entre las soluciones de ciberseguridad y comunicaciones que se encuentran listas para un despliegue operativo inmediato o a corto plazo, y aquellas capacidades de computación y redes globales que, por su complejidad técnica, demandan una aproximación basada en la experimentación y la vigilancia tecnológica.

No obstante, según la metodología de Evaluación de la Madurez Tecnológica (TRA) descrita en el apartado 1.3, el despliegue efectivo de estas capacidades no depende únicamente de la validación experimental, sino que requiere avanzar en paralelo en otras dimensiones de madurez. Es fundamental ir considerando el Nivel de Madurez de Fabricación (MRL) para asegurar cadenas de suministro resilientes, el Nivel de Madurez del Sistema (SRL) para avalar soluciones completas, y el Nivel de Madurez de Integración (IRL) para garantizar la interoperabilidad con los sistemas y redes heredados.

⁸² <https://www.sto.nato.int/>

⁸³ <https://www.act.nato.int/>

De este modo, la estrategia de adopción no solo evaluaría el rendimiento técnico aislado, sino que integraría otros requisitos necesarios para transformar la tecnología en capacidad militar efectiva.

El verdadero impacto estratégico no provendrá de la tecnología cuántica de forma aislada sino del paradigma denominado “*Quantum + X*”, que define la convergencia de la cuántica con otras tecnologías emergentes para multiplicar el rendimiento operativo [Krelina 2025_2]. Esta integración permitirá potenciar las capacidades existentes en lugar de crear necesariamente nuevas clases de armas, destacando combinaciones como “*Quantum + IA*” para acelerar el reconocimiento de patrones y la toma de decisiones, “*Quantum + Espacio*” para enlaces satelitales seguros y conciencia situacional, y “*Quantum + Autonomía*” para la navegación de vehículos no tripulados en entornos sin GNSS. El objetivo final de esta convergencia es habilitar operaciones militares más rápidas, seguras y autónomas en todos los dominios.

A continuación, la Tabla 3-1 resume la hoja de ruta tecnológica para la Defensa, vinculando cada categoría con sus casos de uso principales y estableciendo el horizonte temporal y las acciones de ingeniería recomendadas.

Tecnología / categoría	Nivel TRL (madurez)	Casos de uso principales en Defensa	Horizonte / Acción recomendada
Criptografía post-cuántica (PQC)	TRL 7–8 (Validación operativa)	Mitigación contra amenazas “cosechar ahora, descifrar después”; protección de redes mediante actualización de protocolos (VPN, TLS, PKI); protección de IoMT	Prioridad Inmediata Certificación y migración escalonada: Planes nacionales y pruebas de interoperabilidad (2026); activos de alto riesgo (2030); migración completa (2035).
Generadores de números aleatorios (QRNG)	TRL 7–9 (Disponibilidad comercial)	Generación de claves criptográficas verdaderamente aleatorias; integración en comunicaciones en radios tácticas y enlaces SATCOM; autenticación multifactor y tokens seguros.	Despliegue Inmediato Integración (aumento de IRL) en sistemas actuales y certificación de aleatoriedad para reforzar la seguridad criptográfica.
Distribución cuántica de claves (QKD)	TRL 6–9 (Comercial / Integración)	Enlaces ultraseguros entre centros de mando y control; protección de infraestructuras y redes críticas terrestres y satelitales (EuroQCI); protección ciber contra interceptación activa.	Corto Plazo (Despliegue) Operatividad inicial (EuroQCI 2027); estandarización de interfaces para interoperabilidad en redes híbridas y validación de seguridad de dispositivos.
Computación analógica y simuladores	TRL 5 (Entorno relevante)	Optimización logística de rutas de vehículos y suministros en operaciones; simulación estratégica de escenarios (“ <i>Wargaming</i> ”) y toma de decisiones; simulación de materiales y amenazas QBRN.	Medio Plazo (Experimentación) Pruebas de concepto con datos operativos reales; benchmarking de algoritmos y verificación de ventaja práctica frente a soluciones clásicas.
Computación digital NISQ	TRL 3–4 (Laboratorio)	Machine Learning cuántico para detección de patrones en grandes volúmenes de datos ISR; problemas de optimización combinatoria a pequeña escala; “ <i>Quantum + X</i> ”	Medio Plazo (I+D) Desarrollo de algoritmos híbridos cuántico-clásicos; validación de mitigación de errores y evaluación de

Tecnología / categoría	Nivel TRL (madurez)	Casos de uso principales en Defensa	Horizonte / Acción recomendada
			rendimiento mediante métricas NISQ.
Computación digital FTQC	TRL < 3 (Concepto / Futuro)	Criptoanálisis y ruptura de cifrados asimétricos (RSA, ECC) mediante algoritmo de Shor; simulación avanzada para diseñar nuevos materiales y fármacos/antídotos; Análisis de inteligencia y descifrado masivo de datos históricos.	Largo Plazo (2030 - 2035+) Vigilancia tecnológica y escalado de MRL (fabricación); impacto estratégico profundo cuando se verifique la corrección de errores escalable.
Red Internet cuántica	TRL 3–5 (Investigación / Validación)	Interconexión de sensores, computadores y sincronismos distribuidos en la internet militar; comunicaciones cuánticas seguras.	Largo plazo (2030–2035+) Vigilancia tecnológica; desarrollo, pruebas, integración y validación de componentes (repetidores cuánticos; memorias cuánticas; destiladores de entrelazamiento; sincronización; interfaces cuántico telecomunicaciones); pilotos integrados; <i>testbeds</i> nacionales/internacionales.

Tabla 3-1 Madurez y aplicación de las tecnologías cuánticas en Defensa.

4 LA INDUSTRIA CUÁNTICA

El propósito del Capítulo 4 es analizar el ecosistema industrial de las tecnologías cuánticas a nivel internacional y nacional, identificando los principales actores, capacidades y cadenas de valor que condicionan su desarrollo y adopción en el ámbito de la Defensa. Para ello, el capítulo inicia presentando las asociaciones industriales cuánticas más relevantes, describiendo sus objetivos, miembros y papel en la coordinación sectorial. A continuación, examina la industria internacional de computación cuántica describiendo las tecnologías de qubits, las empresas líderes y los países de origen, y la industria de comunicaciones cuánticas analizando proveedores, soluciones comerciales emergentes e infraestructuras desplegadas. El capítulo dedica un apartado específico a la industria cuántica china evaluando su grado de integración vertical, sus inversiones estratégicas y su posicionamiento geopolítico, y concluye con el análisis de la industria cuántica nacional identificando empresas, capacidades tecnológicas, proyectos relevantes y su conexión con las cadenas de suministro europeas y globales.

4.1 Asociaciones industriales

Las asociaciones industriales cuánticas comparten una agenda común centrada en el desarrollo de estándares, la colaboración internacional, la formación de talento y la promoción de una economía cuántica global interoperable y segura. Todas ellas forman parte del *International Council of Quantum Industry Associations* (ICQIA), establecido formalmente en enero de 2023, que refleja una visión compartida de que la tecnología cuántica no es solo una competencia científica, sino una oportunidad económica y geopolítica. El ICQIA ha identificado y acordado una serie de temas prioritarios conjuntos, que incluyen:

- La colaboración internacional fomentando el diálogo y la cooperación entre regiones para evitar duplicidades y acelerar el progreso, y para alinear políticas públicas y estrategias nacionales que faciliten la interoperabilidad global.
- El desarrollo de estándares técnicos y métricas comunes para hardware, software, comunicaciones y protocolos cuánticos con objeto de normalizar rendimiento, calidad y seguridad para facilitar la adopción industrial.
- El fomento del talento y la fuerza laboral dada la escasez de profesionales capacitados en tecnologías cuánticas impulsando programas de formación, movilidad académica y certificación profesional.
- La construcción de cadenas de suministro resilientes identificando cuellos de botella en la cadena de valor cuántica (como criogenia, fotónica, materiales superconductores) y promoviendo la diversificación y colaboración entre proveedores globales.
- La seguridad cuántica y criptografía post-cuántica como acciones urgentes para preparar las infraestructuras digitales contra los ataques cuánticos, apoyando la transición hacia algoritmos criptográficos resistentes a la computación cuántica.
- La comercialización y adopción industrial mediante la aceleración de la transición de la investigación a productos y servicios reales en casos de uso en sectores como salud, energía, finanzas, defensa y logística.
- La promoción de políticas públicas favorables actuando como interlocutores entre la industria y los gobiernos, y asesorando sobre inversiones estratégicas, incentivos fiscales y regulación ética.

4.1.1 Asociación de la Industria Cuántica Europea (*European Quantum Industry Consortium*, QuIC)⁸⁴

El *European Quantum Industry Consortium* (QuIC) es una asociación industrial sin ánimo de lucro fundada en 2021, cuyo propósito es fortalecer y acelerar la competitividad y el crecimiento económico de la industria europea de tecnologías cuánticas, creando de valor en todo el continente. QuIC actúa como el principal catalizador y voz de la industria cuántica europea, promoviendo la colaboración entre grandes empresas, pymes, centros de investigación, universidades e inversores. Sus objetivos incluyen desarrollar y coordinar metas estratégicas y hojas de ruta para la investigación, innovación y despliegue de tecnologías cuánticas europeas; cooperar con las instituciones europeas y otros actores relevantes para posicionar a Europa como líder mundial en tecnologías cuánticas; fomentar el crecimiento industrial y la competitividad, estableciendo un ecosistema colaborativo y dinámico para la industria cuántica; impulsar la estandarización, la protección de la propiedad intelectual y la formación de talento especializado, alineando las necesidades de la industria con los perfiles profesionales requeridos; y promover productos y servicios cuánticos. QuIC está estrechamente vinculado al *Quantum Flagship* y participa en la coordinación de agendas estratégicas, proyectos piloto y actividades de transferencia tecnológica.

QuIC está conformado actualmente por más de 200 miembros, incluyendo grandes empresas, pymes y startups, agrupaciones empresariales, centros de investigación, universidades, inversores y organizaciones tecnológicas de toda Europa que tienen relación con las tecnologías cuánticas.

4.1.2 *UKQuantum* (Reino Unido)⁸⁵

UKQuantum es el consorcio industrial del Reino Unido dedicado a impulsar el desarrollo y la adopción de tecnologías cuánticas. Es una asociación industrial sin ánimo de lucro que representa los intereses del sector cuántico británico. Fundada en 2022, esta organización surgió como respuesta a la necesidad de articular una voz común para la industria, universidades y centros de investigación capaz de dialogar con el gobierno, influir en políticas públicas y fomentar la colaboración internacional. Mantiene una relación estratégica con el gobierno británico, especialmente con el Departamento de Ciencia, Innovación y Tecnología (*Department for Science, Innovation and Technology*, DSIT), participando activamente en la implementación de la *UK National Quantum Strategy* (2023), que contempla una inversión de 2500 millones de libras en diez años para posicionar al Reino Unido como líder mundial en tecnologías cuánticas.

Entre las decenas de miembros de UKQuantum se encuentran empresas líderes como Quantinuum (computación cuántica híbrida), ORCA Computing (fotónica cuántica), Riverlane (software y control cuántico) y Universal Quantum (procesadores escalables), instituciones académicas como la Universidad de Oxford, la Universidad de Cambridge y el Imperial College London, y centros de innovación como el National Quantum Computing Centre (NQCC) y el Quantum Technology Hub Network. UKQuantum apoya la participación en el *UK National Quantum Technologies Showcase*, el principal evento anual del sector cuántico británico que reúne a líderes del sector para debatir avances, políticas y oportunidades.

4.1.3 *Quantum Industry Canada*, QIC (Canadá)⁸⁶

El *Quantum Industry Canada* (QIC) es una organización sin ánimo de lucro, con sede en Toronto, fundada en 2019 como un consorcio empresarial con el objetivo de transformar la excelencia cuántica de Canadá en éxito comercial y liderazgo global, a través de la interconexión de la cadena de valor

⁸⁴ <https://www.euroquic.org/>

⁸⁵ <https://ukquantum.org/>

⁸⁶ <https://www.quantumindustrycanada.ca/>

cuántica nacional y su enlace con mercados globales. Está formado por empresas, institutos de investigación y socios estratégicos, y colabora activamente con el gobierno canadiense, que ha invertido directamente en el consorcio para fomentar la comercialización de tecnologías cuánticas en áreas como computación, sensores, comunicaciones seguras y materiales avanzados. Esta colaboración público-privada refleja el compromiso del Estado en posicionar a Canadá como líder mundial en el sector.

Entre los miembros más destacados del consorcio están Xanadu Quantum Technologies, pionera en computación cuántica fotónica, Zero Point Cryogenics, especializada en criogenia para sistemas cuánticos, Nord Quantique, desarrolladora de procesadores cuánticos superconductores, e instituciones académicas como el *Institute for Quantum Computing* de la Universidad de Waterloo y el *Perimeter Institute for Theoretical Physics*, que aportan talento e investigación de vanguardia en el campo.

Entre sus iniciativas más relevantes, QIC ha lanzado el primer portal de empleo dedicado exclusivamente al sector cuántico canadiense, facilitando la conexión entre talento y oportunidades laborales. QIC organizó el foro ejecutivo QUANTUM NOW / ICI QUANTIQUE (junio de 2025), que reunió a más de 375 líderes del sector tras la Cumbre del G7, donde se emitió la primera declaración de líderes sobre tecnologías cuánticas.

4.1.4 Quantum Economic Development Consortium, QED-C (Estados Unidos)⁸⁷

El QED-C nació con objeto de impulsar el desarrollo de la industria cuántica a nivel global a través de una infraestructura colaborativa que acelerara su desarrollo comercial. Está administrado por SRI International, una organización de investigación sin fines de lucro con sede en Arlington, Virginia, y respaldada por el NIST. QED-C fue creado como parte de la implementación de la *National Quantum Initiative Act* (2018), siendo oficialmente establecido en 2019. El QED-C fomenta la colaboración entre actores del ecosistema cuántico; impulsa la aplicación práctica de la tecnología cuántica en diferentes sectores; desarrolla una cadena de suministro sólida; facilita el acceso a financiación, recursos técnicos y oportunidades de negocio; y promueve políticas públicas y estándares.

El consorcio incluye más de 250 miembros de 19 países, siendo mayoritariamente estadounidenses (más de 130 empresas), agrupados en las categorías de empresas tecnológicas (desde startups a grandes empresas), universidades y centros de investigación, laboratorios gubernamentales, organizaciones sin fines de lucro e inversores y aceleradoras. Entre las corporaciones tecnológicas están IBM, Google Quantum AI, Microsoft, Intel, Amazon Web Services, D-Wave, IonQ y Rigetti Computing; instituciones académicas como MIT, Caltech y University of Chicago; laboratorios nacionales como Sandia National Laboratories y Los Alamos National Laboratory; y consultoras y proveedores industriales como Accenture, Deloitte, ExxonMobil, AT&T y Boeing. Resulta paradójico encontrar empresas e instituciones de investigación europeas asociadas a QED-C, a pesar de la política de soberanía tecnológica europea. Entre las empresas especializadas europeas participantes se encuentran Airbus (defensa); Oxford Instruments, Oxford Ionics y Nu Quantum del Reino Unido (tecnologías cuánticas especializadas); Alice&Bob y Quandela de Francia (computación cuántica); TOPTICA Photonics de Alemania (fotónica cuántica); y NKT Photonics de Dinamarca (componentes cuánticos). Esta presencia europea en un consorcio predominantemente estadounidense refleja tanto la apertura de la industria cuántica estadounidense como la complejidad del equilibrio entre competencia tecnológica y colaboración internacional en tecnologías críticas.

⁸⁷ <https://quantumconsortium.org/>

4.1.5 Quantum Strategic Industry Alliance for Revolution, Q-STAR (Japón)⁸⁸

Q-STAR (*Quantum Strategic Industry Alliance for Revolution*) es el consorcio industrial japonés creado para liderar la revolución cuántica del país transformando la ciencia cuántica en innovación comercial y desarrollo sostenible. Q-STAR fue fundado en septiembre de 2021 como parte de la implementación de la Estrategia de Tecnología e Innovación Cuántica del gobierno japonés (2020). Esta estrategia nacional identificó la necesidad de una colaboración estrecha entre industria, academia y gobierno para acelerar el desarrollo de tecnologías cuánticas aplicadas a la computación, las comunicaciones, los sensores y la criptografía. Q-STAR es una organización privada sin ánimo de lucro, pero con una relación directa y estratégica con el gobierno japonés a través del respaldo de la Oficina del Gabinete y el Ministerio de Economía, Comercio e Industria (METI), que la consideran un pilar clave para la competitividad tecnológica del país. Aunque no es una entidad estatal, actúa como brazo coordinador entre el sector público y privado.

Q-STAR está formado por más de 140 miembros, entre las que hay corporaciones tecnológicas como Fujitsu (especializada en computación cuántica y simulación), NTT (comunicaciones cuánticas), Hitachi, Toshiba y Mitsubishi Electric (hardware y sensores cuánticos). La institución académica más prominente es el RIKEN *Center for Quantum Computing* (RQC), que actúa como ancla científica del consorcio. Otras instituciones académicas incluyen *Keio University Quantum Computing Center*, *Tohoku University*, *Kyushu University (Institute of Mathematics for Industry)* y *Yokohama National University*.

Desde su establecimiento, Q-STAR ha participado activamente en iniciativas de colaboración internacional. En abril de 2025, Q-STAR firmó un Memorandum de Entendimiento con UKQuantum para fortalecer la colaboración UK-Japón en tecnologías cuánticas. Asimismo, Q-STAR es miembro fundador del *International Council of Quantum Industry Associations* (ICQIA), trabajando conjuntamente con los principales consorcios industriales de Europa (QuIC), Estados Unidos (QED-C) y Canadá (QIC) en la gobernanza internacional de tecnologías cuánticas.

4.2 Industria internacional

4.2.1 Computación cuántica

El panorama empresarial de la computación cuántica se caracteriza por una carrera intensiva entre gigantes tecnológicos multinacionales y startups especializadas de rápido crecimiento. A nivel global, existen más de 40 unidades procesadoras cuánticas comercialmente disponibles, con aproximadamente 160 adicionales en etapas de prototipado o planificación, desarrolladas por cerca de 80 fabricantes en 17 países. Los sistemas superconductores dominan el mercado comercial representando más del 40% de las QPU disponibles, aunque modalidades alternativas como fotónica, iones atrapados, y especialmente átomos neutros y espines de electrones, están ganando impulso [MIT 2025]. La Tabla 4-1 presenta un listado de las principales empresas con QPU completos o comerciales o con desarrollo de prototipos. Cada empresa ha definido estrategias claramente diferenciadas, con productos concretos ya operativos o próximos a comercializarse y roadmaps ambiciosos que proyectan hitos específicos hasta pasado 2030. Paralelo al desarrollo de QPU, el ecosistema de proveedores de materias primas y tecnologías habilitadoras ha emergido como pilar crítico para la viabilidad industrial de la computación cuántica. Este apartado presenta algunas empresas con QPU operativas y comerciales que han resuelto problemas relevantes frente a la supercomputación clásica y tienen actividad en defensa.

⁸⁸ <https://qstar.jp/en>

IBM Quantum ha desarrollado una estrategia de hardware escalable basada en procesadores superconductores, con la línea *Heron* (156 qubits) como arquitectura de referencia para aplicaciones de utilidad cuántica intermedia, complementada por el procesador *Condor* (1.121 qubits) para la exploración de los límites fundamentales de escalado de qubits⁸⁹. El procesador *Heron*, configurado con nuevas topologías y arquitecturas, logra tasas de error entre tres y cinco veces menores que la generación anterior *Eagle* (127 qubits), permitiendo ejecutar con precisión circuitos cuánticos que contengan hasta 5.000 operaciones de compuertas de dos qubits. En colaboración con Moderna, y con RIKEN y Cleveland Clinic, IBM desarrolló modelos y cálculos moleculares que han demostrado el potencial de reducción de ciclos de descubrimiento y desarrollo de nuevos fármacos⁹⁰. El *roadmap* público de IBM define hitos explícitos hacia computación cuántica tolerante a fallos con objeto de alcanzar para 2033 el sistema Blue Jay con 2.000 qubits lógicos realizando más de mil millones de operaciones⁹¹. En defensa y seguridad nacional, IBM ha avanzado a la Etapa B de la *Quantum Benchmarking Initiative* (QBI) de DARPA⁹². También ha identificado prioridades críticas para Departamento de Defensa estadounidense, como la transición de arquitecturas de seguridad criptográficas a algoritmos resistentes a la cuántica, la optimización de problemas logísticos de complejidad extrema que actualmente consumen recursos masivos de computación de alto rendimiento, y la simulación de materiales avanzados para desarrollo de armamentos de próxima generación.

Google Quantum AI ha desarrollado el procesador *Willow*⁹³, un chip superconductor de 105 qubits que representa un avance fundamental en la computación cuántica operativa. El procesador demuestra la reducción exponencial de errores conforme aumenta el número de qubits⁹⁴, resolviendo un desafío que ha perseguido al campo científico durante casi 30 años en materia de corrección de errores cuánticos. Específicamente, al aumentar las matrices de qubits codificados desde una configuración de 3×3 a 5×5 y luego a 7×7, la tasa de error codificada se reduce por un factor de aproximadamente 2 en cada paso. El chip demuestra ventaja cuántica verificable mediante el algoritmo *Quantum Echoes*⁹⁵, completando en menos de cinco minutos un cálculo de muestreo de circuitos aleatorios (RCS) que requeriría 10 septillones (10²⁵) de años en los supercomputadores clásicos más potentes disponibles. La implementación logra tiempos de coherencia (relajación T₁) mejorados de aproximadamente 68 microsegundos, representando una mejora respecto a la generación anterior Sycamore (~20 microsegundos), lo que permite alcanzar fidelidades de compuertas de qubit único superiores al 99,97% y fidelidades de compuertas de dos qubits del 99,88%. Google Quantum AI proyecta aplicaciones inmediatas en simulación molecular para el descubrimiento de fármacos, optimización logística, diseño de materiales avanzados y aceleración de algoritmos de inteligencia artificial. Ha establecido el objetivo de alcanzar una computadora cuántica útil con corrección de errores para 2029. En el contexto de defensa, Google Quantum AI ha sido seleccionado por DARPA⁹⁶ para participar en QBI.

IonQ ha desarrollado el procesador Forte Enterprise⁹⁷, un sistema de computación cuántica con 36 qubits basado en iones de iterbio atrapados y capaz de alcanzar conectividad entre todos los qubits (*all-to-all connectivity*), constituyendo una de las plataformas cuánticas más maduras comercialmente

⁸⁹ <https://tomorrowdesk.com/breakthrough/ibm-quantum-computing-4000-qubit>

⁹⁰ <https://intuitionlabs.ai/articles/ibm-quantum-drug-discovery>

⁹¹ <https://hightoweradvisors.com/blogs/well-th-blog/ibm-quantum-day-roadmap-and-scalability>

⁹² <https://www.darpa.mil/research/programs/quantum-benchmarking-initiative/>

⁹³ <https://blog.google/technology/research/google-willow-quantum-chip/>

⁹⁴ <https://research.google/blog/making-quantum-error-correction-work/>

⁹⁵ <https://blog.google/technology/research/quantum-echoes-willow-verifiable-quantum-advantage/>

⁹⁶ <https://www.techbuzz.ai/articles/google-quantum-ai-joins-darpa-s-2033-quantum-computing-push>

⁹⁷ <https://www.ionq.com/quantum-systems/forte>

disponibles. El sistema Forte se caracteriza por una fidelidad de compuertas de dos qubits de 99.99%⁹⁸, representando el error de compuerta más bajo logrado hasta la fecha por cualquier tecnología cuántica comercial. En colaboración con AstraZeneca, Amazon Web Services (AWS) y NVIDIA, IonQ demostró en junio de 2025 una ventaja cuántica verificable en simulación de reacciones químicas relevantes para desarrollo farmacéutico⁹⁹. El flujo de trabajo de química, acelerada cuánticamente, logró una mejora de más de 20 veces en tiempos de solución, mientras mantenía precisión computacional, para la reacción de Suzuki-Miyaura¹⁰⁰. La arquitectura de Forte, completamente configurable por software, permite que la topología de qubits, así como los sistemas de control óptico, se adapten dinámicamente a demandas computacionales específicas, distinguiendo el enfoque de iones atrapados de arquitecturas de conectividad limitada como superconductores. IonQ proyecta un *roadmap* acelerado, estructurado en hitos explícitos, con objeto de alcanzar sistemas modulares que escalen a más de 2 millones de qubits físicos, generando entre 40.000 y 80.000 qubits lógicos con tasas de error por debajo de 10^{-12} , para 2030¹⁰¹. El hito de obtener del orden de 1.600 qubits lógicos para 2028 adquiere relevancia criptográfica particular, ubicándolo en el rango de las estimaciones recientes de los qubits lógicos necesarios (1.000 a 1.400) para factorizar claves RSA-2048 en aproximadamente una semana¹⁰². IonQ ha establecido una entidad dedicada a integrar sus tecnologías de computación y redes cuánticas para el gobierno estadounidense y agencias aliadas. También ha sido seleccionado para la Etapa B de la *Quantum Benchmarking Initiative* de DARPA.

D-Wave Systems ha desarrollado el procesador Advantage2, un ordenador *quantum annealing* que contiene más de 4.400 qubits superconductores¹⁰³, representando la arquitectura más masiva de qubits comercialmente disponibles para problemas de optimización. Comparado con su predecesor Advantage, Advantage2 logra un aumento del 40% en escala de energía (determinando la precisión con la cual se especifican los parámetros de los problemas), duplicación del tiempo de coherencia (permitiendo resolver problemas más rápidamente) y reducción del 75% del ruido (mejorando la capacidad del sistema para distinguir entre soluciones con energías similares)¹⁰⁴. En marzo de 2025, D-Wave publicó la demostración de la supremacía cuántica computacional en un problema útil [King 2025]. Su computador Advantage2 completó una simulación de materiales magnéticos en minutos, una tarea que requeriría aproximadamente un millón de años y superaría el consumo anual de electricidad mundial si se ejecutara en el supercomputador Frontier¹⁰⁵. Estos problemas de simulación de materiales magnéticos tienen aplicaciones directas en descubrimiento de nuevos materiales. D-Wave ha servido a más de 100 clientes empresariales incluyendo Mastercard, Siemens Healthineers, NEC Corporation, DENSO, Lockheed Martin y Forschungszentrum Jülich, demostrando la validez comercial del *quantum annealing* para aplicaciones del mundo real¹⁰⁶. El roadmap público de D-Wave define evoluciones tecnológicas para los próximos años con el objeto de entregar en la Fase 5 (post-2030) un QPU general que combine múltiples unidades de lógica cuántica (Quantum Logic Unit, QLU) con memoria, registros, inicialización de estado y componentes de desplazamiento de datos¹⁰⁷. La empresa ha formado una unidad de negocios dedicada al gobierno estadounidense para desarrollar

⁹⁸ <https://www.ionq.com/news/ionq-advances-to-stage-b-of-darpas-quantum-benchmarking-initiative-qbi>

⁹⁹ <https://investors.ionq.com/news/news-details/2025/IonQ-Speeds-Quantum-Accelerated-Drug-Development-Application-With-AstraZeneca-AWS-and-NVIDIA/default.aspx>

¹⁰⁰ <https://thequantuminsider.com/2025/06/09/ionq-speeds-quantum-accelerated-drug-development-application-in-partnership-with-astrazeneca-aws-and-nvidia/>

¹⁰¹ <https://www.ionq.com/blog/ionqs-accelerated-roadmap-turning-quantum-ambition-into-reality>

¹⁰² <https://postquantum.com/quantum-computing-companies/ionq/>

¹⁰³ <https://support.dwavesys.com/hc/en-us/articles/32105885880087-D-Wave-s-Advantage2-Quantum-Computer-Now-Generally-Available>

¹⁰⁴ <https://www.dwavequantum.com/solutions-and-products/systems/>

¹⁰⁵ <https://thequantuminsider.com/2025/03/12/d-wave-stakes-claim-on-quantum-supremacy-for-real-world-problem/>

¹⁰⁶ <https://www.dwavequantum.com/company/newsroom/press-release/d-wave-deemed-awardable-vendor-for-us-department-of-defense-chief-digital-and-artificial-intelligence-office-s-tradewinds-solutions-marketplace/>

¹⁰⁷ https://www.dwavequantum.com/media/xvjpraig/clarity-roadmap_digital_v2.pdf

aplicaciones cuánticas dirigidas a logística y transporte militares. El computador Advantage2 ha sido desplegado operativamente para ejecutar problemas de misión crítica del gobierno estadounidense con acceso en tiempo real a través del servicio de nube *Leap* de D-Wave¹⁰⁸. AT&T ha demostrado mejoras de órdenes de magnitud en optimización de despacho de red y optimización de interrupciones del servicio usando *D-Wave Hybrid Solvers*¹⁰⁹, validando la aplicabilidad del *quantum annealing* a problemas logísticos de complejidad extrema relevantes a operaciones militares.

Tecnología	Empresa	País de Origen
Superconductores	Rigetti Computing	Estados Unidos
	Oxford Quantum Circuits (OQC)	Reino Unido
	Qilimanjaro Quantum Tech	España
	Google Quantum AI	Estados Unidos
	QuantWare	Países Bajos
	Alice & Bob	Francia
	IQM Quantum Computers	Finlandia
	D-Wave Quantum Inc.	Canadá
	IBM Quantum	Estados Unidos
	Anyon Systems	Canadá
	Fujitsu/RIKEN	Japón
	Quantum Circuits Inc.	Estados Unidos
	Microsoft	Estados Unidos
	SpinQ	China
	Nord Quantique	Canadá
Iones atrapados	IonQ	Estados Unidos
	Universal Quantum	Reino Unido
	eleQtron	Alemania
	Quantinuum	Reino Unido
	Alpine Quantum Technologies GmbH	Austria

¹⁰⁸ <https://www.dwavequantum.com/solutions-and-products/cloud-platform/>

¹⁰⁹ https://docs.dwavequantum.com/en/latest/industrial_optimization/leap_hybrid.html

Tecnología	Empresa	País de Origen
Átomos Neutros	Atom Computing	Estados Unidos
	Pasqal	Francia
	Infleqtion	Estados Unidos
	QuEra Computing Inc.	Estados Unidos
	Planqc (planqc GmbH)	Alemania
Silicio	Intel	Estados Unidos
	Photonic Inc.	Canadá
	Silicon Quantum Computing (SQC)	Australia
	SemiQon	Finlandia
	Dirac	Australia
Fotónica	PsiQuantum	Estados Unidos
	Quandela	Francia
	Xanadu Quantum Technologies	Canadá
	QBoson	China
	OptQC	Japón
	ORCA Computing	Reino Unido
	Aegiq	Reino Unido

Tabla 4-1 Principales empresas de ordenadores cuánticos o QPU, tecnologías de los qubits y países de origen^{110,111,112}.

4.2.2 Comunicaciones cuánticas

El sector de las comunicaciones cuánticas ha experimentado una transformación comercial acelerada, consolidando un ecosistema industrial global compuesto por fabricantes especializados de equipos QKD, integradores de redes terrestres y proveedores de infraestructuras satélite. Este panorama refleja la transición desde la investigación académica hacia despliegues operacionales de seguridad cuántica en infraestructuras críticas, telecomunicaciones comerciales y comunicaciones

¹¹⁰ <https://qir.mit.edu/>

¹¹¹ https://en.wikipedia.org/wiki/List_of_companies_involved_in_quantum_computing_communication_or_sensing

¹¹² <https://thequantuminsider.com/2025/09/23/top-quantum-computing-companies/>

gubernamentales. Este apartado presenta algunas empresas representativas del sector de las comunicaciones cuánticas.

Toshiba^{113,114,115,116,117} posiciona sus soluciones de QKD como su oferta más relevante en comunicaciones cuánticas, con raíces de investigación que se remontan a 1999 en su laboratorio de Cambridge. Su sistema QKD más avanzado implementa el protocolo TF-QKD basado en pares de fotones entrelazados, donde cualquier intento de interceptación altera los estados cuánticos y hace detectable la intrusión. En abril de 2025, Toshiba Europe alcanzó un hito significativo al transmitir mensajes cifrados cuánticamente a lo largo de 250 kilómetros sobre una red de fibra comercial en Alemania, sin necesidad de enfriamiento criogénico, validando por primera vez la viabilidad de infraestructura QKD estándar en telecomunicaciones convencionales. El sistema mantiene tasas de error cuántico de bit (QBER) bajas, críticas para la seguridad. Ese mismo año, Toshiba codesarrolló con *KDDI Research* y *NEC* una tecnología de multiplexado que permitió transmitir más de 30 Terabits por segundo con la distribución de claves secretas simultáneamente sobre una única fibra, reduciendo de forma notable los costes de introducción y operación. Además, Toshiba colabora en la iniciativa de una red fotónica total, denominada IOWN, para demostrar multiplexado de señales QKD y generación de claves en infraestructuras de próxima generación. Entre las aplicaciones demostradas destaca el proyecto conjunto con *Purdue University* y el *Oak Ridge National Laboratory*, donde sistemas QKD aseguraron la transmisión de datos desde un reactor nuclear, demostrando resiliencia en entornos críticos.

Fundada en 2001 en Suiza, ID Quantique^{118,119,120,121,122,123} se ha consolidado como líder global en soluciones de seguridad cuántica, destacando su línea *Clavis* como producto QKD más relevante. El sistema *Clavis XG* representa la generación más avanzada de la compañía, diseñado para producción comercial en infraestructuras de telecomunicación y centros de datos. En enero de 2025, *Clavis XG* alcanzó un hito histórico al convertirse en el primer producto QKD del mundo en recibir aprobación oficial de seguridad nacional por parte del Servicio de Inteligencia Nacional de Corea del Sur (*National Intelligence Service*, NIS). Esta certificación incluyó una evaluación rigurosa del sistema QKD y de la plataforma de gestión de claves cuánticas integrada (*QKMS Clarion KX*), realizada durante varios años con la participación de institutos de investigación, agencias de estándares técnicos y laboratorios de ciberseguridad. El protocolo BB84, empleado en *Clavis XG*, constituye el método de distribución de claves cuánticas con seguridad teóricamente demostrada en mecánica cuántica. La versión *Clavis XGR* está orientada a investigación académica, manteniendo las funcionalidades del sistema de producción mientras permite experimentación con parámetros y configuraciones avanzadas. La plataforma *Clarion KX* integrada con *Clavis* proporciona una suite completa para despliegues complejos de red. Además, ID Quantique y SK Telecom lideran los esfuerzos de estandarización global, habiendo publicado recientemente dos recomendaciones internacionales de la ITU-T (X.1710 y

¹¹³ <https://www.toshiba.eu/solutions/quantum/about/>

¹¹⁴ <https://www.toshiba.eu/newsroom/toshiba-breakthrough-brings-quantum-communications-to-existing-national-scale-telecommunications-infrastructure/>

¹¹⁵ <https://www.toshiba.eu/quantum/news/worlds-first-successful-demonstration-of-quantum-key-distribution-technology-for-multiplexing-over-30-tbps-of-high-capacity-data-and-secret-keys/>

¹¹⁶ <https://www.global.toshiba/ww/technology/corporate/rdc/rd/topics/25/2507-02.html>

¹¹⁷ <https://news.toshiba.com/press-releases/press-release-details/2025/Demonstration-of-Quantum-Secure-Communications-in-a-Reactor-Using-Quantum-Key-Distribution/default.aspx>

¹¹⁸ <https://www.idquantique.com/about-idq/company-profile/>

¹¹⁹ <https://www.idquantique.com/clavis-xg-series-qkd-obtains-national-security-certification/>

¹²⁰ <https://www.idquantique.com/quantum-safe-security/products/clarion-kx-platform/>

¹²¹ <https://www.idquantique.com/quantum-safe-security/products/clavis-xgr-qkd-system/>

¹²² <https://www.itu.int/rec/T-REC-X.1710/en>

¹²³ <https://www.itu.int/rec/T-REC-X.1714/en>

X.1714) que definen el marco de seguridad para redes QKD e híbridas que combinan claves cuánticas con otros métodos de intercambio.

Fundada en 2009 en China, QuantumCTek^{124,125,126} se ha consolidado como líder privado en distribución de claves cuánticas, con productos QKD ampliamente desplegados en infraestructuras de telecomunicación nacionales. Su portafolio incluye el sistema *QKD-PHA300*, diseñado para entornos de canales complejos y utilizado en múltiples implementaciones dentro de redes de telecomunicaciones chinas. La compañía ha participado en diversos proyectos de QKD en sectores gubernamentales, financieros y de telecomunicaciones. La infraestructura nacional china incluye el *backbone* cuántico Beijing–Shanghai, completado en 2017 y que representa la transición de la fase experimental a los servicios comerciales con 2.000 kilómetros de longitud, integrado posteriormente en la red nacional China de comunicaciones cuánticas (*China Quantum Communication Network*, CN-QCN) que alcanza los 12.000 kilómetros de longitud total e incluye 145 nodos backbone y 20 redes metropolitanas expandidas desde 2020. QuantumCTek contribuye al ecosistema mediante sistemas de generación y distribución de claves, plataformas de gestión de redes y equipamiento de comunicación cuántico-segura. Además, la empresa mantiene una intensa actividad en I+D para avanzar la tecnología QKD y ampliar sus aplicaciones. Sus sistemas han demostrado la integración de protocolos de autenticación con criptografía post-cuántica (PQC) en redes metropolitanas QKD, validando una arquitectura híbrida que ofrece redundancia dual donde, si una capa se ve comprometida, la otra mantiene la protección mediante seguridad basada en principios matemáticos distintos.

En mayo de 2025, China Telecom Quantum Group^{127,128} anunció el lanzamiento de lo que describe como el primer sistema de criptografía distribuida a nivel mundial resistente a ataques de ordenadores cuánticos, integrando tanto distribución de claves cuánticas (QKD) como criptografía post-cuántica (PQC) en una arquitectura de tres capas. El hito más destacado fue la realización de la primera llamada telefónica cifrada cuánticamente a lo largo de 1.000 kilómetros entre Beijing y Hefei, demostrando la viabilidad operacional de la tecnología a escala nacional. El sistema híbrido ofrece seguridad de extremo a extremo aplicable a mensajería cifrada, autenticación segura y protección de datos en tiempo real. Entre las plataformas lanzadas se incluyen *Quantum Secret* (colaboración y mensajería cifrada) y *Quantum Cloud Seal* (plataforma de flujo de trabajo digital seguro para aprobaciones, auditorías y gestión empresarial), ambas ya desplegadas en entornos comerciales y gubernamentales. La infraestructura subyacente comprende redes de comunicación cuántica en 16 centros urbanos chinos. En Hefei se encuentra actualmente la infraestructura metropolitana de comunicación cuántica más extensa del mundo, con 1.147 kilómetros de fibra QKD, ocho nodos centrales y 159 puntos de acceso que sirven a unas 500 agencias gubernamentales y 380 empresas estatales.

SpeQtral^{129,130,131} se ha posicionado como el actor más relevante en comunicaciones cuánticas basadas en satélites, siendo pionero en tecnologías comerciales de transmisión de entrelazamiento cuántico entre espacio y Tierra. La tecnología crítica consiste en la transmisión de pares de fotones entrelazados entre el espacio y la superficie terrestre, esencial para interconectar redes cuánticas

¹²⁴ <https://www.quantum-info.com/English/>

¹²⁵ <https://www.nature.com/articles/nature23655>

¹²⁶ <https://www.quantum-info.com/English/product/National/>

¹²⁷ <https://thequantuminsider.com/2025/05/20/china-telecom-launches-hybrid-quantum-safe-encryption-system-completes-1000-kilometer-secure-call/>

¹²⁸ <https://quantumcomputingreport.com/china-telecom-deploys-hybrid-quantum-safe-encryption-system-across-16-cities/>

¹²⁹ <https://speqtralquantum.com/>

¹³⁰ <https://www.thalesaleniaspace.com/en/press-releases/quantum-communications-satellite-speqtral-and-thales-alenia-space-launch-new>

¹³¹ <https://speqtralquantum.com/newsroom/speqtral-announces-speqtral-1-quantum-satellite-mission-for-ultra-secure-communications>

continentales. En asociación con Thales Alenia Space, *joint venture* de Thales (Francia) y Leonardo (Italia), desarrolla satélites dedicados como primeros demostradores de comunicaciones cuánticas comerciales. Según el acuerdo, SpeQtral opera los satélites y proporciona datos de coordinación incluyendo parámetros de apuntamiento y mediciones sincronizadas a bordo, mientras Thales Alenia Space gestiona las operaciones de estaciones terrenas y recopila mediciones locales sincronizadas para analizar críticamente el rendimiento de los enlaces cuánticos. El objetivo compartido es la experimentación y validación de los fundamentos técnicos de futuras redes cuánticas interoperables, así como explorar métodos para mejorar su desempeño. El *roadmap* contempla que Thales Alenia Space lance el satélite QINSAT antes de finalizar la década, capaz de distribuir pares de fotones entrelazados a estaciones terrenas, incluyendo las operadas por SpeQtral. Paralelamente, SpeQtral está forjando alianzas con gobiernos para llevar las comunicaciones cuánticas satelitales a aplicaciones operativas en 2026.

SK Telecom, compañía líder en telecomunicaciones de Corea del Sur, trabaja en el despliegue comercial de QKD y en la estandarización global de tecnologías cuánticas seguras. En colaboración con ID Quantique¹³², SK Telecom ha coeditado iniciativas de la ITU-T, como las recomendaciones internacionales X.1710 [ITUT 2020] y X.1714 [ITUT 2020_2], que establecen el marco de seguridad, amenazas, requisitos y métodos aplicables a redes QKD. La recomendación X.1710 define un marco integral que incluye amenazas de seguridad, requisitos de seguridad y métodos de seguridad para redes QKD complejas, abarcando aspectos tales como autenticación, control de acceso, confidencialidad, integridad de datos y disponibilidad frente a ataques de negación de servicio. La recomendación X.1714 especifica los requisitos de seguridad para métodos híbridos que combinan claves QKD con otras fuentes de intercambio de claves, así como la entrega segura de claves desde QKD hacia aplicaciones criptográficas, permitiendo arquitecturas de seguridad que combinan QKD con criptografía post-cuántica para proteger la cadena completa de comunicaciones contra ataques cuánticos. Además, SK Telecom impulsa la estandarización internacional de las tecnologías *quantum-safe* QRNG, habiendo contribuido también a la aprobación del primer estándar internacional X.1702 [ITUT 2019].

4.2.3 La industria China

A pesar de referencias frecuentes a decenas de empresas que trabajan en tecnología cuántica, solo catorce compañías privadas pueden identificarse como contribuyentes significativos a la innovación cuántica en China¹³³. Esta concentración es reflejo de las barreras de entrada como son la necesidad de talento especializado, equipamiento costoso y acceso a investigación académica de frontera. Las empresas se dividen en dos categorías:

- Nueve startups especializadas que impulsan innovación radical: Ciqtek, Kunfeng, Origin Quantum, Qasky, QuantumCTek, QuDoor, Shenzhou Quantum, SpinQ y TuringQ.
- Cinco grandes tecnológicas con divisiones cuánticas que aportan recursos y conexiones con mercados corporativos: Alibaba Quantum Lab, Baidu Quantum Lab, Huawei Quantum, Tencent y Zhongxing Telecommunication Equipment.

La geografía de la innovación cuántica se concentra en torno a la Universidad de Ciencia y Tecnología de China (USTC) que actúa como anclaje institucional. Aproximadamente veinte empresas cuánticas operan en una zona específica denominada Quantum Avenue, incluyendo cuatro de los nueve principales startups. Esta concentración geográfica genera compartición de talento, acceso a

¹³² <https://www.idquantique.com/id-quantique-and-sk-telecom-lead-international-standardization-of-quantum-safe-technology/>

¹³³ <https://itif.org/publications/2024/09/09/how-innovative-is-china-in-quantum/>

equipamiento especializado, y vínculos directos con investigación académica puntera. El vínculo institucional es el profesor de la USTC Guo Guangcan, que fundó el Departamento de Física Cuántica e Información Cuántica en 2001, y continúa en su discípulo Pan Jianwei. Esta genealogía institucional y de startups muestra un ecosistema cuántico creado mediante relaciones personales, lealtades académicas y transferencia sistemática de conocimiento desde universidad a industria.

Los cambios estructurales observados en 2023-2024 revelan una reorientación profunda de la estrategia cuántica estatal. Las dos mayores empresas tecnológicas Alibaba y Baidu cerraron sus divisiones cuánticas y transfirieron activos a instituciones estatales, Baidu a la Academia de Ciencias de Información Cuántica de Beijing y Alibaba a la Universidad de Zhejiang. No es una cuestión de rentabilidad, sino una estrategia del gobierno chino de consolidar el control de las tecnologías cuánticas en instituciones estatales y no dejarlas en manos de empresas privadas. Contrasta con la independencia empresarial y el objetivo de beneficio comercial de las empresas occidentales.

4.3 Industria nacional

La base tecnológica e industrial (BTI) cuántica nacional está a la altura internacional en sus campos de especialización. El ecosistema de tecnologías cuánticas en España ha experimentado un crecimiento relevante, configurando una red diversa de spin-offs universitarias, start-ups especializadas y empresas consolidadas que abarcan desde el desarrollo de hardware cuántico hasta soluciones de ciberseguridad cuántica, software y aplicaciones espaciales. El entramado de startups de tecnologías cuánticas junto con grandes empresas consolidadas y multinacionales conforma una cadena de valor completa desde la investigación fundamental hasta la operación de infraestructuras críticas, posicionando a España como referente estratégico en la implementación de comunicaciones cuánticas seguras a nivel europeo.

Qilimanjaro Quantum Tech es una empresa pionera en el desarrollo de computadores cuánticos basados en qubits superconductores que operan en arquitecturas tanto digitales como analógicas. La empresa está centrada en facilitar el acceso a la tecnología cuántica a través de su plataforma SpeQtrum (*Quantum-as-a-Service*, QaaS)¹³⁴, que proporciona acceso remoto a chips cuánticos alojados en centros de datos en la nube. Ha desarrollado el primer computador cuántico construido con tecnología 100% europea mediante una arquitectura abierta, integrando componentes de proveedores europeos como QuantWare. Fue instalado en el Barcelona Supercomputing Center (BSC), como parte del proyecto Quantum Spain, convirtiéndose en el primer computador cuántico operativo ubicado en territorio español. Qilimanjaro integra soluciones cuánticas con sistemas de computación de alto rendimiento (*High Performance Computing*, HPC), y ofrece servicios de consultoría especializada en algoritmos y aplicaciones cuánticas, permitiendo a empresas y centros de investigación identificar y desarrollar casos de uso cuánticos prácticos.

LuxQuanta es la apuesta española líder en distribución cuántica de claves (QKD), siendo spin-off del Instituto de Ciencias Fotónicas (ICFO). La empresa fue la primera proveedora europea de una tecnología innovadora capaz de integrarse en redes ópticas convencionales, convirtiéndose en pionera comercial de la solución QKD de variable continua (CV-QKD) basada en estados coherentes modulados gaussianos. Dispone de productos ya en el mercado para la securización de redes y centros de datos basados en su sistema NOVA LQ, que coexiste sin desplazamiento de datos en tráfico DWDM en banda C completamente ocupado, permitiendo una adopción rentable y escalable. LuxQuanta ha desarrollado un equipo multidisciplinar de ingenieros y profesionales con amplia experiencia en información cuántica experimental, telecomunicaciones, FPGA y desarrollo de

¹³⁴ Servicio en la nube que proporciona acceso remoto a procesadores y computadores cuánticos físicos alojados en centros de datos, permitiendo a usuarios ejecutar algoritmos cuánticos sin necesidad de poseer hardware cuántico propio.

software. Mantiene una integración técnica con el fabricante internacional ID Quantique, a través de la plataforma Clarion KX, para garantizar la interoperabilidad entre sistemas. La empresa recientemente ha sellado una alianza estratégica con GMV (noviembre 2025) para acelerar el despliegue de comunicaciones cuánticas seguras en Europa, combinando su tecnología QKD con el sistema de gestión de claves QuKee y la experiencia espacial de GMV en una solución diseñada en España y alineada con la iniciativa europea EuroQCI.

Quside es un fabricante especializado en generadores cuánticos de números aleatorios (QRNG) de ultra alta velocidad, componentes críticos para securizar infraestructuras de información y comunicaciones. La empresa desarrolló una arquitectura paralela innovadora que permitió generar números aleatorios cuánticos puros a velocidades sin precedentes (17 nanosegundos por bit), constituyendo el chip semiconductor más rápido del mercado con 1 Gb/s para aplicaciones de ciberseguridad crítica. Quside es una spin-off del Instituto de Ciencias Fotónicas (ICFO) que combina la experiencia en el desarrollo de tecnologías ópticas avanzadas con electrónica de alta frecuencia (GHz) e integración de FPGA, posicionándose como proveedor crítico para soluciones que requieren aleatoriedad cuántica certificada (SP800-90B del NIST y calificación ENS del CCN).

Multiverse Computing es líder en el desarrollo de algoritmos cuánticos diseñados para ejecutarse en hardware cuántico de terceros (IBM-Q, D-Wave) y en algoritmos de inspiración cuántica ejecutados en hardware clásico mediante técnicas de Tensor Networks. Su producto insignia, CompactifAI, es una herramienta de compresión y optimización de modelos neuronales que reduce el tamaño de los modelos hasta un 80%, disminuye el consumo energético aproximadamente un 50% y acelera la inferencia entre dos y ocho veces, manteniendo pérdidas mínimas de precisión. La empresa cuenta con software cuántico y algoritmos especializados para finanzas, energía, machine learning, defensa, aeroespacial y movilidad autónoma. Ha demostrado casos de uso comerciales reales en optimización de carteras de inversión, con datos de mercado en colaboración con BBVA, que permitirían maximizar rentabilidad en segundos frente a los dos días requeridos con métodos clásicos. Multiverse ha publicado resultados científicos que describen nuevos métodos para realizar cálculos de optimización dinámica de carteras que podrían acelerar significativamente los procesos financieros. La empresa cuenta con un equipo internacional de 184 profesionales (con más del 30% doctores en matemáticas, física e inteligencia artificial), respaldada por aceleradoras como el *Donostia International Physics Center* y el *Creative Destruction Lab* de Canadá, con participación en programas europeos estratégicos como FCAS (junto a Indra) en defensa, EPIIC (con Airbus) en sistemas de control avanzados, y colaboración con la OTAN en tecnologías emergentes.

QCentroid es una startup especializada en servicios de computación cuántica (*Quantum Computing as a Service*, QCaaS)¹³⁵ que ofrece QuantumOps, una plataforma empresarial integral para facilitar el acceso a la computación cuántica de forma accesible y económica. La plataforma permite la orquestación y optimización cuántica para aplicaciones en logística y optimización industrial, integrando mitigación de errores de Q-CTRL (especialista australiana en corrección de errores cuánticos) mediante Fire Opal, que puede mejorar el rendimiento de algoritmos cuánticos hasta 1000 veces. QCentroid ha desarrollado un enfoque sin código centrado en problemas, utilizando APIs, blockchain e IA generativa, con módulos especializados como Quantum Builder Suite (para orquestación y benchmarking), Quantum Studio (con asistentes de IA para descubrimiento de casos de uso) y Quantum Hub OS (para gestión de ecosistemas colaborativos), permitiendo que organizaciones de todos los tamaños ejecuten, comparen y distribuyan algoritmos cuánticos. La empresa ha establecido colaboraciones estratégicas con actores importantes como Mahou-San Miguel para

¹³⁵ Término amplio que engloba diversos servicios cuánticos en la nube, incluyendo acceso a hardware cuántico real, plataformas de orquestación, emuladores, simuladores cuánticos y herramientas de desarrollo para algoritmos cuánticos. Mientras que QaaS se emplea para el acceso a hardware real, QCaaS es más genérico y abarca cualquier servicio cuántico en la nube.

optimización logística y ha ganado el reto TrenLab VI de Renfe (2025) con un piloto para optimizar rutas, frecuencias y planificación resiliente de recursos ferroviarios. Además, ha desarrollado líneas de I+D especializadas en computación cuántica confidencial y Quantum Machine Learning para aplicaciones en finanzas (optimización de carteras y análisis de riesgo), energía, telecomunicaciones e I+D (materiales, química computacional), con despliegues ya en producción con clientes Fortune 500 y pilotos avanzados en hubs cuánticos europeos.

Inspiration-Q desarrolla algoritmos de inspiración cuántica que ofrecen las ventajas de la computación cuántica sin necesidad de hardware cuántico, ejecutándose en ordenadores ordinarios mediante infraestructura cloud (Azure y Hetzner). Como spin-off del Consejo Superior de Investigaciones Científicas (CSIC), la empresa se especializa en la adaptación a medida de algoritmos de inspiración cuántica para aplicación a problemas de optimización combinatoria con restricciones complejas, permitiendo resolver desafíos que requieren análisis de múltiples millones de opciones. Su portfolio de productos incluye iQ-Finance para construcción de carteras de inversión, modelado de series temporales financieras y detección de anomalías bursátiles; iQ-Xtreme para resolución de problemas complejos de optimización combinatoria matemática; e iQ-ML para entrenamiento de modelos de *machine learning* interpretables y causales. Inspiration-Q ha demostrado casos de uso comerciales reales con instituciones financieras como Bankia/CaixaBank, en el programa Insomnia, y con uno de los principales bancos españoles en un piloto de seguimiento de índices bursátiles. Como consecuencia, se ha madurado hasta la fase de precomercialización el producto iQ Index Tracking Plus, que probado con datos históricos de bolsa ha demostrado ser capaz de generar rendimientos superiores al índice Nasdaq 100, lo que valida su eficacia como herramienta de gestión de inversiones. La empresa cuenta con un equipo multidisciplinar de profesionales en computación, desarrollo, inteligencia artificial, ventas, finanzas y marketing, abordando desafíos de planificación industrial, logística, finanzas cuantitativas y *machine learning* interpretable.

La empresa G2-ZERO es un spin-off del Consejo Superior de Investigaciones Científicas (CSIC), fundada en 2020 con respaldo del programa NEOTEC. Está especializada en el desarrollo de fuentes de fotones individuales de alta calidad y otros componentes fotónicos cuánticos basados en semiconductores para aplicaciones en comunicaciones, computación y sensores cuánticos. Estos dispositivos son críticos para garantizar la seguridad de una comunicación cuántica extremo a extremo, siendo componentes esenciales en sistemas QKD confiables. G2-ZERO fue seleccionada en 2024 entre más de 1.300 candidatos para participar en el incubador Quantum DeepLab del programa DIANA de la OTAN, y en 2025 comienza su participación en el incubador de la Agencia Espacial Europea (ESA), evidenciando el reconocimiento internacional de su tecnología.

QDynamics es un spin-off del Laboratorio de Comunicaciones Cuánticas del CSIC especializado en el desarrollo de sistemas de distribución de claves cuánticas (QKD) en fibra óptica y espacio libre. La empresa ofrece soluciones CV-QKD basadas en protocolo GG02 para fibra óptica que operan en fibra monomodo estándar a 1550nm (banda C), utilizando la infraestructura de fibra actual con ensayos de campo exitosos que cubren distancias de hasta 50 km y pérdidas de canal de hasta 10 dB. El sistema incorpora innovaciones como coexistencia con datos clásicos en DWDM, generador cuántico de números aleatorios (QRNG) integrado, y una técnica patentada de frequency locking vía software que reduce los costes sin sacrificar rendimiento. Paralelamente, QDynamics desarrolla soluciones QKD en espacio libre basadas en protocolo BB84 con polarización y estaciones ópticas de tierra compactas y portátiles para enlaces con satélites LEO, facilitando la integración entre infraestructuras terrestres y espaciales cuánticas. El equipo técnico está liderado por profesionales en comunicaciones cuánticas del CSIC, incluyendo especialistas en CV-QKD, espacio libre, electrónica y seguridad. La empresa ha presentado un demostrador funcional en enero de 2025 y tiene previsto el lanzamiento de su primer sistema comercial para marzo de 2026.

QoolNet es un spin-off de la Universidad Politécnica de Madrid (UPM) especializado en soluciones de comunicación segura frente a amenazas cuánticas (Quantum-Safe Communication Solutions). Desarrollan plataformas de hardware y software avanzadas diseñadas para proteger infraestructuras críticas contra futuras amenazas cuánticas, mediante la integración de tecnologías de distribución cuántica de claves (QKD) con criptografía postcuántica (PQC) en sistemas híbridos. Sus soluciones se caracterizan por la integración sin fricción con infraestructuras de red existentes, versatilidad y escalabilidad en diversos medios de comunicación (fibra óptica, comunicaciones satelitales), y contribuciones activas a estándares europeos de telecomunicaciones, incluyendo una cartera significativa de patentes en tecnologías seguras a nivel cuántico. Ha participado activamente en proyectos como la implementación del primer enlace cuántico entre hospitales de Madrid en colaboración con Telefónica, Vithas y LuxQuanta, así como en demostraciones del Mobile World Congress 2025 sobre ciberseguridad cuántica aplicada al sector sanitario.

Paralelamente al ecosistema de startups y spin-offs cuánticos, las grandes empresas españolas consolidadas refuerzan la capacidad tecnológica nacional cuántica mediante soluciones integrales en los ámbitos de la ciberseguridad y espacial. El grupo empresarial OESIA, a través de sus filiales Tecnobit y Cypherbit, se posiciona como líder en el desarrollo de nodos cuánticos y soluciones de criptografía postcuántica, participando activamente en proyectos europeos estratégicos como Quarter y EuroQCI-Spain en tres ámbitos clave: formativo (capacitación en estándares cuánticos ETSI), de estandarización (implementación de funciones de seguridad en software y hardware a nivel EAL4+) e industrial (industrialización de nodos cuánticos a escala). Su fábrica de tarjetas electrónicas en Valdepeñas le posiciona como una de las pocas compañías en Europa con capacidad de fabricación a escala de soluciones cuánticas. EPICOM, empresa con participación pública, complementa este ecosistema ofreciendo soluciones de cifradores IP con calificación de seguridad hasta NATO SECRET basados en criptografía postcuántica, diseñadas para infraestructuras críticas y organismos gubernamentales. GMV, multinacional tecnológica con cuatro décadas de experiencia en ciberseguridad, cifrado y sistemas espaciales, ha emergido como actor clave en la integración de tecnologías cuánticas en el segmento espacial. Bajo su alianza estratégica con LuxQuanta (noviembre 2025), GMV aporta su vasta experiencia en misiones espaciales críticas como Galileo y su solución de gestión de claves (KMS) «QuKee» para orquestar el ciclo de vida completo de claves cuánticas en redes complejas, garantizando la seguridad redundante mediante la combinación de QKD y PQC en arquitecturas punto-multipunto. Telefónica actúa como integrador sistémico de tecnologías cuánticas en infraestructuras existentes, facilitando la adopción de soluciones de criptografía cuántica y postcuántica en colaboración con proveedores nacionales (LuxQuanta, QoolNet) como parte de MADQCI (Madrid Quantum Communications Infrastructure), además de aplicar algoritmia cuántica en optimización de tráfico de red y colaborar en estándares ETSI. Sener, con más de 23 años de experiencia en instrumentación óptica embarcada en satélites para navegación (Galileo) y observación terrestre, lidera el proyecto QKD-LEO como *prime contractor* junto a operadores satelitales españoles (Hispasat, Deimos) que potencialmente contribuirán a la constelación IRIS2 de la Unión Europea. Desarrolla instrumentación óptica de precisión de intercambio cuántico de claves para satélites LEO en asociación con actores del ecosistema cuántico nacional (Quside, LuxQuanta, ICFO).

Complementando la estructura industrial española, empresas multinacionales de tecnología, espacio y defensa, con operaciones consolidadas en territorio nacional aportan capacidades críticas en computación cuántica, ciberseguridad espacial y demostradores de alta complejidad. Eviden, filial de Atos especializada en soluciones de criptografía cuántica y postcuántica, desarrolla la plataforma integral Qaptiva™, un entorno de programación que permite escribir código una sola vez y ejecutarlo sin fricciones en diferentes hardware cuánticos (on-premise o cloud). Esta solución proporciona emuladores escalables de computadores cuánticos de hasta 41 qubits lógicos con capacidades open source para entrenamiento, y con su ecosistema de partners para integrar soluciones cuánticas en industrias críticas (automoción, defensa, energía, finanzas, ciencias de la vida, retail). Thales Alenia

Space, *joint venture* francoitaliana con operaciones consolidadas en España, participa como agente principal en el proyecto GARBO, el demostrador satelital más avanzado del mundo para intercambio de clave cuántica desde órbita geoestacionaria (QKD-GEO) financiado por el PERTE Aeroespacial europeo. Thales provee la carga útil integral del satélite (telescopio óptico de alta precisión, generador cuántico de números aleatorios, fuente de fotones polarizados, baliza láser, procesador de generación de claves) y sistemas de apuntamiento, con validación mediante ensayos de campo entre las islas canarias de La Palma y Tenerife (140 km) antes de implementación operativa en órbita. Cuenta con la participación de instituciones españolas (Instituto de Astrofísica de Canarias, Universidad Politécnica de Madrid) y actores financieros nacionales (Banco de Santander, BBVA, Telefónica, Cellnex). Telespazio Ibérica, filial de la italiana Telespazio (subsidiaria de Leonardo), desarrolla el componente crítico del enlace ascendente (*uplink*) en el proyecto QKD-LEO para la constelación de cubesats en órbita baja, permitiendo la transmisión de información cuántica desde estaciones terrestres. Estos componentes actúan como nodos de confianza (*trusted nodes*) que conectan con otras infraestructuras terrestres, facilitando la expansión y cobertura internacional de las redes de comunicaciones cuánticas globales a través de múltiples satélites.

5 POLÍTICAS, ESTRATEGIAS Y PLANES CUÁNTICOS

El propósito del Capítulo 5 es analizar las políticas, estrategias y planes relacionados con las tecnologías cuánticas en los ámbitos europeo, nacional e internacional, y evaluar cómo estos marcos condicionan su desarrollo tecnológico, industrial y su adopción en Defensa. Para ello, el capítulo inicia abordando los conceptos de soberanía tecnológica e industrial, las tecnologías críticas y los controles de exportación aplicables a tecnologías de doble uso, incluyendo la computación y las comunicaciones cuánticas. A continuación, examina la política industrial europea y su relevancia para la Seguridad y la Defensa, revisando sus instrumentos y como la cuántica se considera tecnología crítica y habilitadora. Posteriormente analiza las políticas específicas de tecnologías cuánticas en Europa y en España incluyendo iniciativas de la Comisión Europea, convocatorias y proyectos en tecnologías cuánticas y la Estrategia de Tecnologías Cuánticas de España. El capítulo estudia también las políticas de tecnologías cuánticas en otros países y organismos, como Reino Unido, Estados Unidos, China y la OTAN, describiendo sus estrategias nacionales, programas de financiación y enfoques de gobernanza. Finalmente, presenta una visión de conjunto del estado de la cuántica en el mundo, utilizando métricas como inversión pública, patentes, producción científica, y la formación y capacitación de la fuerza laboral cuántica, para contextualizar el posicionamiento global en la carrera por el liderazgo cuántico.

El Capítulo 5 analiza políticas, estrategias y planes cuánticos en contextos europeo, nacional e internacional, abordando soberanía tecnológica, tecnologías críticas y controles de exportación. Examina la política industrial europea, iniciativas españolas de tecnologías cuánticas, y las estrategias de Reino Unido, Estados Unidos, China y la OTAN, presentando finalmente una visión global mediante métricas de inversión pública, patentes, producción científica y formación de talento cuántico para contextualizar el posicionamiento en la carrera cuántica global.

5.1 La soberanía tecnológica e industrial

5.1.1 *De la ciencia a la tecnología y de la innovación a la industria*

La ciencia, la tecnología, la innovación y la industria han confluído como motores del crecimiento económico desde la Revolución Industrial. Las políticas internacionales de ciencia, tecnología e industria han ido convergiendo y evolucionado durante el siglo XX, creando las condiciones para promocionar activamente la investigación, el desarrollo tecnológico y la innovación empresarial. Las iniciativas estatales en ciencia, tecnología e industria tienen un impacto directo sobre el crecimiento económico y la estabilidad a largo plazo, pero también en la ventaja geoestratégica de unas naciones frente a otras.

En lo referente a la ciencia y a la innovación, a finales de la década de los 40 surgió el “modelo lineal de innovación”, que se presentaba como una secuencia de actividades o fases: investigación básica, investigación aplicada, desarrollo tecnológico, innovación y difusión [DJG 2011]. Se distinguía entre la libertad del científico para definir sus áreas de trabajo con objeto de aumentar el conocimiento y la explotación económica de ese conocimiento a través de la investigación aplicada desarrollada en los laboratorios de I+D empresariales. Sin embargo, el modelo ha sido cuestionado argumentando que un pequeño porcentaje de ciencia llegaba a innovaciones radicales, pero que la mayor parte de la innovación era más un proceso incremental de mejoras en productos y procesos existentes, liderado por investigadores y tecnólogos industriales. Así, se cuestionaba la dependencia del desarrollo tecnológico hacia la investigación, incluso se indicaba que podía ser que el flujo del modelo lineal fuera inverso. De esta manera, conviven los modelos agregados o lineales de innovación dirigidos a la

producción científica y los modelos dirigidos que se enfocan a la producción tecnológica [Saenz 2000].

Los conflictos bélicos y el posicionamiento comercial han sido claves para llevar a cabo la institucionalización de las políticas científicas, tecnológicas e industriales por parte de los Estados, creando para ello organismos públicos que priorizan, orientan y coordinan las actividades. En las naciones con mayores intereses económicos y geopolíticos, como es el caso entre otros de Estados Unidos, China y Rusia, las políticas, con un prominente control del Estado, siguen el modelo dirigido. El resto de las naciones pasan por posturas intermedias hasta ser más favorables a los modelos agregados, en muchos casos sin priorizar en ningún sector estratégico para la nación.

Los sectores prioritarios de innovación abarcan la salud, la energía, la aeronáutica y el espacio, las tecnologías de la información, la seguridad y la defensa, la automoción, los materiales y la fabricación avanzada, la agroindustria y el medio ambiente, siendo la preferencia de unos frente a otros en las naciones y dependiendo del contexto geoestratégico e histórico.

Con referencia al tipo de tecnologías, hay tecnologías que tienen un papel especial en el desarrollo económico porque no solo mejoran procesos específicos, sino que transforman múltiples sectores a la vez. Estas tecnologías, llamadas de propósito general¹³⁶ [BT 1992], se caracterizan porque se aplican de forma transversal en muchas industrias, tienen un potencial técnico que evoluciona con el tiempo, y generan nuevas oportunidades de innovación cuando se combinan con otras tecnologías o procesos. No obstante, en economías descentralizadas no siempre se aprovecha todo su potencial, porque los sectores que desarrollan la tecnología y los que la adoptan no necesariamente se coordinan. La computación cuántica se augura como una de las tecnologías de propósito general emergentes en el siglo XXI.

5.1.2 Las tecnologías críticas

El Observatorio Europeo de Tecnologías críticas (*Observatory of Critical Technologies*, OCT)¹³⁷ tiene por objeto la monitorización de las tecnologías críticas, los desarrollos relacionados y las cadenas de suministro. La Comisión publica periódicamente informes clasificados de la UE que ayudan a determinar los ámbitos que requieren actividades urgentes.

Una tecnología crítica, según la definición establecida por el Observatorio de Tecnologías Críticas de la Unión Europea, es aquella que reúne simultáneamente una serie de condiciones estratégicas y operativas esenciales. En primer lugar, implica una dependencia estratégica, ya que no existe una fuente de suministro dentro de la UE ni acceso sin restricciones desde proveedores externos, lo que la convierte en un riesgo potencial para la soberanía tecnológica. Además, su esencialidad radica en que es indispensable para sectores clave como el espacial, la seguridad o la defensa. Estas tecnologías se caracterizan también por su aplicabilidad múltiple, es decir, pueden utilizarse en diversos contextos o sectores, lo que amplifica su valor estratégico. Su nivel de integración suele ser bajo o medio, lo que significa que se trata de componentes, equipos, subsistemas, materiales, métodos, procesos o herramientas que son fundamentales para el funcionamiento de sistemas más complejos. Finalmente, deben tener una función claramente identificable y un rendimiento definido, lo que permite evaluar su impacto y utilidad de forma precisa dentro de las cadenas de valor tecnológicas y de defensa europeas.

En un mundo cada vez más volátil, incierto y tecnológicamente competitivo, la capacidad de un Estado para desarrollar, controlar y aplicar tecnologías críticas se ha convertido en un elemento esencial de su seguridad nacional. Distintos países y bloques estratégicos están abordando el desafío de garantizar su autonomía tecnológica en el ámbito de la defensa.

¹³⁶ Tecnologías de propósito general históricas fueron el motor de vapor, la electricidad o los circuitos integrados.

¹³⁷ https://defence-industry-space.ec.europa.eu/eu-space/eu-observatory-critical-technologies_en

5.1.3 Los controles de exportación

Las naciones avanzadas regulan las exportaciones de tecnologías y productos que puedan servir a fines tanto civiles como de seguridad y defensa.

El régimen jurídico común de la Unión Europea para el control de las exportaciones, el corretaje, la asistencia técnica, el tránsito y la transferencia de productos de doble uso viene establecido por el Reglamento (UE) 2021/821 [PECUE 2021], cuyo objetivo principal es garantizar que las exportaciones de estos productos no contribuyan a la proliferación de armas de destrucción masiva ni a violaciones de derechos humanos, al tiempo que se protege la competitividad de las empresas europeas. El documento contiene una serie de anexos, siendo el Anexo I la lista principal de bienes, software y tecnologías sujetos a control y el Anexo IV la lista de productos sensibles que requieren autorización para transferencias dentro de la Unión Europea, como las tecnologías criptográficas o las nucleares. Introduce controles específicos para productos no listados o de ciber-vigilancia que puedan ser utilizados en represión interna o violaciones graves del derecho internacional humanitario, y establece el principio de diligencia debida para los exportadores, quienes deben evaluar los riesgos de sus operaciones mediante programas internos de cumplimiento. Tras las últimas actualizaciones publicadas en septiembre/octubre de 2025, el Anexo I del Reglamento (UE) 2021/821 incluye apartados específicos sobre tecnologías cuánticas bajo la regulación de bienes y productos de doble uso, concretamente: ordenadores cuánticos, subsistemas y módulos de computadores cuánticos, circuitos de control y componentes electrónicos diseñados para operar a temperaturas criogénicas, amplificadores paramétricos, equipos de refrigeración criogénica y sondas de oblea para entornos de temperaturas extremadamente bajas. También establece requerimientos de licencia y supervisión en la exportación de productos, dispositivos y módulos destinados a la generación, transmisión o autenticación de claves mediante principios cuánticos, incluyendo tanto los equipos como sus componentes y el software asociado¹³⁸.

El Reglamento (UE) 2021/821 es directamente aplicable en el ordenamiento español, y se complementa con la Ley 53/2007, de 28 de diciembre, sobre el control del comercio exterior de material de defensa y de doble uso [BOE 2007], y el Real Decreto 679/2014, de 1 de agosto, por el que se aprueba el Reglamento de control del comercio exterior de material de defensa, de otro material y de productos y tecnologías de doble uso [BOE 2014]. El Real Decreto 679/2014 incluye productos y tecnologías adicionales sometidos a control específico a nivel nacional español.

Estados Unidos tiene leyes de control de exportaciones que se aplican a productos militares, a productos comerciales que tienen algún uso en el área militar o de inteligencia y a activos financieros. Las principales son el Reglamento de Tráfico Internacional de Armas (*International Traffic in Arms Regulations*, ITAR), que es administrado por el Departamento de Estado, y el Reglamento de Administración de Exportaciones (EAR), que es administrado por el Departamento de Comercio. Fabricantes, exportadores e intermediarios que pretendan exportar o importar artículos de defensa, servicios de defensa y otros datos técnicos relacionados incluidos en la lista USML¹³⁹ (*United States Munitions List*) están sujetos a la regulación ITAR. Análogamente, la regulación EAR cuenta con la lista CCL¹⁴⁰ (*Commerce Control List*). La USML no menciona específicamente en un listado detallado los elementos relacionados con tecnologías cuánticas, aunque se englobarían en las tecnologías, equipos y servicios destinados a aplicaciones militares o con capacidades críticas para defensa, por ejemplo, sensores cuánticos para sistemas de navegación, comunicaciones cuánticas encriptadas para

¹³⁸ <https://www.cuatrecasas.com/es/spain/gobierno-corporativo-compliance/art/tecnologias-doble-uso-listado-comunitario-actualizacion>

¹³⁹ <https://www.ecfr.gov/current/title-22/chapter-I/subchapter-M/part-121>

¹⁴⁰ <https://www.bis.doc.gov/index.php/documents/regulations-docs/2329-commerce-control-list-index-3/file>

uso estratégico o módulos integrados en sistemas de armas avanzados. CCL si incluye componentes, software y tecnologías relacionadas para ordenadores y criptografía cuánticos.

Varios países han añadido tecnologías relacionadas con la computación cuántica a sus catálogos de uso dual (Tabla 5-1) y requieren de permisos de exportación para ordenadores cuánticos y módulos y componentes electrónicos relacionados, para dispositivos de qubits, componentes de control cuántico y dispositivos de medición cuántica, y para circuitos de qubit que contengan o soporten “redes físicas de qubits”, es decir, infraestructuras tangibles y operativas que interconecten sistemas cuánticos permitiendo la comunicación y el procesamiento distribuido de información cuántica entre múltiples ubicaciones geográficas [MERICS 2024].

COUNTRY	DATE	SOFTWARE AND TECHNOLOGY; COMPLEMENTARY METAL-OXIDE-SEMICONDUCTORS	MATERIALS	CRYOGENIC COOLING SYSTEMS AND COMPONENTS
Netherlands and Spain	November 20, 2023	✗	✗	✗
France	February 2, 2024	✓	✗	✗
United Kingdom	April 2024	✓	✓	✓
Spain	May 26, 2024	✗	✗	✗
Finland*	June 18, 2024			
Canada	June 19, 2024	✓	✗	✗
Germany	July 22, 2024	✓	✗	✓
Italy	July 1, 2024	✓	✓	✓
Japan	July 8, 2024	✓	✗	✗
United States	September 6, 2024	✓	✓	✓
Netherlands	October 18, 2024	✓	✓	✓
Norway	November 3, 2024	✓	✓	✓

Tabla 5-1 Controles de exportación de tecnologías relacionadas con la cuántica [MERICS 2024].

China cuenta con legislación análoga como la Ley de Control de Exportaciones de la República Popular China, vigente desde diciembre de 2020¹⁴¹ y el Reglamento de Control de Exportaciones de Artículos de Doble Uso de China, efectivo desde diciembre de 2024¹⁴². Además, China ha efectuado un cambio estratégico limitando el nivel de colaboración internacional en investigación cuántica¹⁴³. El gobierno ha impuesto restricciones de colaboración internacional a sus instituciones estatales, y sólo permite coautorías con otras instituciones chinas. Este aislacionismo tiene el objetivo de proteger los secretos comerciales y de defensa limitando la difusión de conocimiento.

¹⁴¹ <https://spanish.people.com.cn/n3/2020/1202/c31621-9794868.html>

¹⁴² <https://www.china-briefing.com/news/china-issues-new-export-control-regulations/>

¹⁴³ <https://itif.org/publications/2024/09/09/how-innovative-is-china-in-quantum/>

5.2 La política industrial y tecnológica europea

5.2.1 Sectores críticos y su relevancia para la Seguridad y Defensa

Este apartado presenta la evolución estratégica y normativa de la Comisión Europea en lo referente a los sectores tecnológicos e industriales clave para el desarrollo económico de los países miembros, así como aquellas con influencia en las capacidades para la Seguridad y Defensa de la Unión Europea.

En 2022, la Comisión Europea presentó una hoja de ruta para reforzar la soberanía tecnológica de la Unión en seguridad y defensa [CE 2022], ante un contexto geopolítico complejo. El documento destaca que muchas tecnologías críticas provienen del ámbito civil, y que la rápida innovación difumina los límites entre usos militares y civiles. Para afrontar estos retos se propone integrar mejor las comunidades de investigación civil y militar, aprovechar instrumentos como el Fondo Europeo de Defensa (*European Defence Fund*, EDF) y reducir dependencias estratégicas en las cadenas de suministro. La estrategia se basa en cuatro ejes: impulsar tecnologías críticas mediante programas europeos, coordinar esfuerzos con Estados miembros y socios internacionales, fomentar la innovación entre pymes y startups, y crear un Observatorio de Tecnologías Críticas¹⁴⁴. Además, se priorizan sectores como la ciberseguridad, el espacio, los semiconductores y los sistemas autónomos, junto con medidas para fortalecer capacidades industriales, atraer inversión y proteger infraestructuras clave. Las tecnologías cuánticas quedan incluidas de manera implícita como tecnologías disruptivas y facilitadoras con relevancia transversal.

La Recomendación (UE) 2023/2113 [CE 2023], emitida por la Comisión Europea el 3 de octubre de 2023, busca reforzar la seguridad económica de la Unión Europea ante un entorno geopolítico y tecnológico cada vez más desafiante. Enmarcada en la Estrategia Europea de Seguridad Económica, se basa en tres pilares: competitividad, protección frente a riesgos y cooperación internacional. La Comisión identifica diez ámbitos tecnológicos críticos, de los cuales semiconductores avanzados, inteligencia artificial, tecnologías cuánticas y biotecnología requerían una evaluación de riesgos conjunta con los Estados miembros antes de finalizar 2023. Estos sectores fueron seleccionados por su potencial transformador, su posible uso dual (civil y militar) y el riesgo de ser utilizados para violaciones de derechos humanos. Las evaluaciones se realizarán bajo principios rectores que incluyen el análisis de vulnerabilidades sistémicas, el contexto geopolítico y la participación del sector privado, garantizando la confidencialidad de la información. Esta recomendación no implicaba medidas inmediatas, sino que establecía una base para futuras decisiones políticas proporcionales al nivel de riesgo. La Comisión continuará supervisando los avances tecnológicos y podrá ampliar la lista de tecnologías críticas si fuera necesario. Este documento menciona las tecnologías cuánticas como uno de los ámbitos tecnológicos más críticos y urgentes para ser evaluadas por su impacto potencial en la seguridad económica y su carácter transformador y dual.

5.2.2 La política industrial y tecnológica de defensa en Europa y España

La Unión Europea lleva dos décadas enfrentándose al reto de superar la fragmentación de su mercado de defensa. A pesar de contar con una industria potente y diversificada, la falta de coordinación entre los Estados miembros ha generado duplicidades, ineficiencias y problemas de interoperabilidad. El Libro Verde sobre los contratos públicos de defensa [CE 2004], publicado por la Comisión Europea en 2004, constataba que los contratos públicos de defensa estaban fuertemente compartimentados a nivel nacional, lo que generaba fragmentación, ineficiencia y altos costes para los contribuyentes, y la falta de coordinación impedía aprovechar economías de escala y limitaba la competitividad de la industria europea. Las especificidades de los contratos de defensa, como la confidencialidad, la seguridad de los aprovisionamientos, la complejidad técnica de los sistemas

¹⁴⁴ https://defence-industry-space.ec.europa.eu/eu-space/eu-observatory-critical-technologies_en

armamentísticos y el papel predominante de los Estados como clientes, reguladores y financiadores, así como el uso frecuente del artículo 346 del Tratado de la Unión Europea [UE 2010], que permite a los Estados miembros aplicar excepciones por razones de seguridad nacional, son impedimentos a un mercado europeo de Defensa más integrado, competitivo y eficiente, que refuerce la base industrial y tecnológica de defensa en Europa y contribuya al desarrollo de capacidades militares comunes en el marco de la Política Europea de Seguridad y Defensa.

Como consecuencia del Libro Verde se adoptó de la Directiva 2009/81/CE [PECUE 2009], que regula la contratación pública en los sectores de Defensa y Seguridad, introdujo procedimientos más transparentes y competitivos, adaptados a las especificidades del sector, como la confidencialidad, la seguridad de los suministros y la interoperabilidad. Su objetivo fue abrir el mercado entre Estados miembros, reduciendo la fragmentación y el uso excesivo de excepciones nacionales.

El Libro Verde también reforzó el papel de la Agencia Europea de Defensa (*European Defence Agency*, EDA)¹⁴⁵, creada en 2004, como actor clave en la coordinación en la investigación y desarrollo y adquisición de capacidades militares. La EDA se convirtió en un instrumento para fomentar la cooperación entre Estados miembros y avanzar hacia un mercado europeo de equipos de defensa.

En 2016, la UE estableció el Plan de Acción Europeo de la Defensa (*European Defence Action Plan*, EDAP) [CE 2016], para reforzar la autonomía estratégica de la industria de defensa. El plan se articula en torno a tres pilares principales: la creación de un Fondo Europeo de Defensa con dos secciones (una para investigación colaborativa en tecnologías militares y otra para el desarrollo conjunto de capacidades estratégicas); el impulso a las inversiones en las cadenas de suministro de defensa, especialmente en pymes y tecnologías de doble uso; y el refuerzo del mercado único de defensa mediante la aplicación efectiva de las directivas sobre contratación pública y transferencias intra-UE.

La EDAP ha dado lugar a los programas precursores del Fondo Europeo de Defensa (EDF)¹⁴⁶, la Acción Preparatoria de Investigación en Defensa (PADR)¹⁴⁷ con una financiación de 90 millones de euros de 2017 a 2019, y el Programa Europeo para el Desarrollo de la Industria de la Defensa (*European Defence Industrial Development Programme*, EDIDP)¹⁴⁸, con una financiación de 500 millones de euros entre 2019 y 2020.

El Fondo Europeo de Defensa (*European Defence Fund*, EDF)¹⁴⁹, con un presupuesto cercano a los 8.000 millones de euros para el período 2021–2027, establece el marco legal para financiar proyectos colaborativos transfronterizos de I+D en defensa con especial atención a las pymes y al desarrollo de tecnologías disruptivas. El Horizonte Europa¹⁵⁰ (2021–2027), aunque no exclusivo de defensa, es un programa marco de I+D+i que incluye líneas de investigación dual (civil-militar) y apoya tecnologías clave.

La Declaración de Versalles¹⁵¹ (marzo de 2022) marcó un punto de inflexión tras la invasión rusa de Ucrania. Los líderes europeos acordaron invertir más y mejor en defensa, fomentar la innovación tecnológica y fortalecer la industria de defensa europea. Otro aspecto era la reducción de dependencias estratégicas de energía, materias primas, semiconductores, salud, digitalización y alimentación.

¹⁴⁵ <https://eda.europa.eu/>

¹⁴⁶ https://defence-industry-space.ec.europa.eu/eu-defence-industry/european-defence-fund-edf-official-webpage-european-commission_en

¹⁴⁷ https://defence-industry-space.ec.europa.eu/eu-defence-industry/preparatory-action-defence-research-padr_en

¹⁴⁸ https://defence-industry-space.ec.europa.eu/eu-defence-industry/european-defence-industrial-development-programme-edidp_en

¹⁴⁹ https://defence-industry-space.ec.europa.eu/eu-defence-industry/european-defence-fund-edf-official-webpage-european-commission_en

¹⁵⁰ <https://www.horizonteeuropa.es/>

¹⁵¹ <https://www.consilium.europa.eu/en/press/press-releases/2022/03/11/the-versailles-declaration-10-11032022/>

La Brújula Estratégica para la Seguridad y la Defensa¹⁵² es el plan de acción concreto adoptado por la Unión Europea el 22 de marzo de 2022 en respuesta al contexto internacional marcado por amenazas crecientes como la competencia geopolítica, las tensiones económicas, la desinformación, el desarrollo tecnológico acelerado y la crisis climática, y tiene como propósito dotar a la UE de una visión común y objetivos concretos para reforzar su política de seguridad y defensa de aquí a 2030. Se estructura en torno a cuatro pilares fundamentales: Actuar, que refuerza la capacidad de la UE para intervenir en crisis globales, incluyendo el desarrollo de una Capacidad de Despliegue Rápido operativa en 2025, y nuevas misiones de apoyo internacional; Invertir, que promueve el aumento y la optimización del gasto en defensa con inversiones millonarias para fortalecer la industria y el desarrollo tecnológico europeo de defensa; Asegurar, que busca anticiparse a amenazas híbridas, cibernéticas y espaciales adoptando estrategias específicas en ciberresiliencia, seguridad marítima y defensa espacial, además de herramientas contra la manipulación informativa; Asociarse, que refuerza las alianzas con socios bilaterales, regionales y multilaterales incluyendo acuerdos con países no miembros de la UE, cooperación con la ONU y la OTAN. El pilar Invertir menciona explícitamente las tecnologías cuánticas, dentro del apartado de innovación, tecnologías disruptivas y reducción de dependencias estratégicas, como elemento clave en el aumento de capacidades en Seguridad y Defensa.

En marzo de 2024, la Comisión Europea presentó la Estrategia Industrial Europea de Defensa [CE 2024], orientada a reforzar la base industrial y tecnológica de defensa, fomentar la adquisición colaborativa de equipos (40% para 2030), aumentar el comercio intraeuropeo de defensa (35% del mercado para 2030), priorizar la contratación pública dentro de la UE (50% en 2030, 60% en 2035). Esta estrategia también promueve la cooperación con socios estratégicos y la integración de la preparación para la defensa en todas las políticas comunitarias.

El gasto en Defensa de los Estados Miembros¹⁵³ ha crecido los últimos 10 años hasta los 343.000 millones de euros en 2024, y se prevé que alcance los 381.000 millones de euros en 2025 (2,1% del PIB europeo). Los gastos europeos en I+D en Defensa ha alcanzado los 13.000 millones de euros en 2024, representando un 20% de incremento con respecto a 2023, y se espera que alcance los 17.000 millones de euros en 2025.¹⁵⁴

En junio de 2023, el Ministerio de Defensa aprobó la Estrategia Industrial de Defensa 2023 (EID 2023)¹⁵⁵, con el objetivo de fortalecer la autonomía estratégica de la Base Industrial y Tecnológica de Defensa (BITD), consolidar capacidades industriales clave, y fomentar la cooperación internacional dentro del marco nacional y europeo. La EID 2023 se complementa con la Estrategia de Tecnología e Innovación para la Defensa 2020 (ETID 2020)¹⁵⁶, publicada en diciembre de 2020, que orienta las actuaciones de I+D+i del departamento mediante la definición de objetivos tecnológicos de alto impacto y la excelencia en los procesos relacionados con la innovación en defensa. La ETID 2020 y la EID 2023 coinciden en el fortalecimiento de la autonomía de la base industrial nacional y el fomento de la cooperación tecnológica nacional e internacional, en apoyo de las capacidades militares y su libertad de acción operativa.

El Plan Industrial y Tecnológico para la Seguridad y la Defensa 2025¹⁵⁷ fue presentado y aprobado por el Consejo de Ministros de España el 22 de abril de 2025. Dotado con una inversión de 10.471

¹⁵² https://www.ceas.europa.eu/ceas/strategic-compass-security-and-defence-1_en

¹⁵³ <https://www.consilium.europa.eu/es/policies/european-defence-readiness/>

¹⁵⁴ <https://www.consilium.europa.eu/es/policies/defence-numbers/>

¹⁵⁵ <https://publicaciones.defensa.gob.es/estrategia-industrial-de-defensa-2023.html>

¹⁵⁶ <https://publicaciones.defensa.gob.es/estrategia-de-tecnologia-e-innovacion-para-la-defensa-etid-2020-libros-pdf.html>

¹⁵⁷ <https://www.lamoncloa.gob.es/consejodeministros/resumenes/Documents/2025/230425-plan-industrial-y-tecnologico-para-la-seguridad-y-la-defensa.pdf>

millones de euros para el año 2025, permite aumentar el gasto total en defensa y alcanzar el objetivo del 2% adquirido ante la Unión Europea y la OTAN. En el desglose, se establece que el 89% de los fondos se ejecutarán en territorio nacional favoreciendo a empresas españolas. La segunda partida del Plan se destinará a desarrollar y adquirir nuevas tecnologías de telecomunicación y ciberseguridad (31%).

El Ministerio de la Presidencia, Justicia y Relaciones con las Cortes publicó el Acuerdo del Consejo de Ministros para la creación del Comité Nacional de Seguridad y Soberanía Tecnológica [BOE 2025]. Con este Acuerdo, España ha dado un paso firme hacia la consolidación de su autonomía estratégica y la soberanía tecnológica en este momento histórico marcado por la aceleración tecnológica y los desafíos geopolíticos. El Comité nace como parte del ambicioso Plan Industrial y Tecnológico para la Seguridad y la Defensa 2025, con la intención de garantizar la correcta ejecución del Plan, fomentar la eficiencia del gasto en defensa, impulsar la transferencia tecnológica y coordinar sinergias entre organismos públicos y privados, promover la innovación en seguridad y defensa, atraer y retener talento, fortalecer el ecosistema emprendedor y reforzar las alianzas internacionales en el ámbito científico y tecnológico. El Comité Nacional se configura como un órgano colegiado adscrito a la Presidencia del Gobierno, presidido por el titular del Ministerio de Defensa e integrado por representantes de ministerios y organismos públicos clave. La Secretaría del Comité corresponde al titular de la Dirección General de Estrategia e Innovación de la Industria de Defensa (DIGEID). El Consejo Asesor canaliza las necesidades del sector privado, académico y sindical.

La industria de defensa española, compuesta mayoritariamente por pymes, tiene una clara orientación dual, especialmente en los sectores aeroespacial y aeronáutico, y una elevada tasa de exportación. Sin embargo, se enfrenta a los riesgos derivados de la baja inversión en defensa y de la participación de empresas extranjeras en su tejido industrial. El país tiene ante sí la oportunidad de fortalecer su soberanía tecnológica mediante una mayor inversión, la participación en programas europeos y el establecimiento de alianzas estratégicas.

5.3 La política de tecnologías cuánticas en Europa y en España

la UE ha identificado la cuántica como una tecnología crítica en su Estrategia de Seguridad Económica¹⁵⁸ y en el “Libro Blanco Conjunto - Preparación en materia de defensa europea 2030” [CE 2025].

5.3.1 Iniciativas de la Comisión Europea en tecnologías cuánticas

La Estrategia Cuántica Europea [CE 2025_2], presentada oficialmente por la Comisión Europea el 2 de julio de 2025, es una apuesta ambiciosa para convertir a Europa en líder mundial en tecnologías cuánticas antes de 2030. La Comisión Europea, consciente del potencial transformador de la física cuántica, ha articulado una hoja de ruta que abarca desde la investigación básica hasta la industrialización y la formación de talento especializado. El objetivo es construir un ecosistema robusto, competitivo y soberano, capaz de afrontar los retos tecnológicos y geopolíticos de la próxima década.

La estrategia se apoya en cinco grandes pilares: el impulso a la investigación e innovación, el despliegue de infraestructuras cuánticas, el refuerzo del ecosistema industrial y académico, la promoción de tecnologías espaciales y de doble uso, y el desarrollo de capacidades formativas y profesionales. Europa busca así consolidar clústeres de excelencia, fomentar la colaboración público-privada y proteger sus activos estratégicos frente a la competencia global. La industrialización de chips

¹⁵⁸ <https://www.consilium.europa.eu/es/policies/european-economic-security/>

cuánticos, la creación de una Academia Europea de Capacidades Cuánticas y la inversión en startups son algunos de los instrumentos clave para alcanzar estos objetivos. La estrategia reconoce el enorme potencial de las tecnologías cuánticas como herramientas de doble uso.

La Estrategia Cuántica de la Unión Europea se apoya en un Consejo Consultivo independiente que reúne a científicos y tecnólogos destacados y dispondrá de una Ley Cuántica para 2026.

Sin embargo, el asunto apremiante era que Europa tuviera una postura común sobre las medidas a adoptar de cara a la llegada de ese ordenador cuántico criptográficamente relevante capaz de vulnerar los sistemas de información y las comunicaciones.

El 11 de abril de 2024, la Comisión Europea emitió una recomendación a los Estados miembros de la Unión Europea sobre una hoja de ruta para llevar a cabo de manera coordinada la transición hacia una criptografía postcuántica (PQC) [CE 2024_2]. El objetivo es sincronizar los esfuerzos nacionales para diseñar y aplicar planes de transición, garantizando la interoperabilidad transfronteriza y la seguridad de las infraestructuras críticas y servicios digitales frente a las amenazas derivadas de la computación cuántica.

La Comisión recomienda que los Estados miembros definan una hoja de ruta común y coordinen sus acciones a través de un foro específico, aprovechando las estructuras existentes en ciberseguridad y creando un subgrupo especializado dentro del Grupo de Cooperación en Seguridad de Redes e Información (*Network and Information Systems*, NIS), con participación de agencias nacionales, ENISA y expertos en ciberseguridad. Asimismo, plantean que evalúen y seleccionen, con ayuda de expertos, los algoritmos de criptografía postcuántica más adecuados para la UE, y promuevan su adopción como normas comunes en toda la Unión, y adopten las medidas preparatorias adecuadas y proporcionadas para la transición, incluyendo la elaboración de planes nacionales alineados con la hoja de ruta europea.

El subgrupo sobre criptografía postcuántica debe coordinar el desarrollo de la hoja de ruta en un plazo de dos años desde la publicación de la recomendación, tras lo cual cada Estado miembro adaptará su propio plan nacional. También tiene encomendado intercambiar información con partes interesadas (sector público, industria, operadores) y colaborar con organismos como Europol y la OTAN para evitar duplicidades y garantizar un enfoque cohesivo.

El 11 de junio de 2025, el grupo de trabajo sobre PQC, subgrupo especializado creado dentro del Grupo de Cooperación en Seguridad de Redes e Información (NIS), publicó la hoja de ruta [NIS 2025], subrayando la urgencia de iniciar el proceso de migración, dada la posibilidad de ataques “cosechar ahora, descifrar después” (*harvest now, decrypt later*) y la longevidad de muchos sistemas críticos. El enfoque es progresivo y se articula en tres grandes hitos temporales:

- Para el 31 de diciembre de 2026, todos los Estados miembros deben haber iniciado planes nacionales de transición, identificado los actores relevantes, realizado inventarios de activos criptográficos y mapas de dependencias, involucrado la cadena de suministro, lanzado programas de concienciación y comenzando pilotos para casos de alto y medio riesgo.
- Para el 31 de diciembre de 2030, debe completarse la transición en los casos de alto riesgo, finalizar los pilotos y la planificación para los de riesgo medio, y habilitar por defecto actualizaciones de software y firmware seguras frente a amenazas cuánticas.
- Para el 31 de diciembre de 2035, la migración debe estar finalizada para los casos de riesgo medio y, en la medida de lo posible, para los de bajo riesgo, alineando el calendario europeo con los objetivos internacionales, como los de Estados Unidos y el Reino Unido.

El documento recomienda integrar el análisis de riesgo cuántico en la gestión habitual de riesgos, fomentar la agilidad criptográfica y coordinar esfuerzos a nivel europeo para garantizar la interoperabilidad y la seguridad de infraestructuras críticas. Además, se insta a los Estados miembros a

no esperar a completar cada fase antes de iniciar la siguiente, sino a avanzar en paralelo en todas las áreas posibles.

El Grupo de Cooperación NIS lanzó con posterioridad una consulta pública¹⁵⁹ para recoger opiniones y sugerencias. El objetivo de la encuesta es involucrar a todos los actores relevantes (proveedores de infraestructuras críticas, industria, academia y público general) en la mejora y adaptación de futuras versiones de la hoja de ruta, proponiendo soluciones sectoriales, herramientas de código abierto y pasos prácticos para facilitar la migración a sistemas criptográficos resistentes a la computación cuántica.

5.3.2 Convocatorias y proyectos europeos en tecnologías cuánticas

La Unión Europea ha establecido un marco integral de financiación y gobernanza para posicionar a Europa como líder global en tecnologías cuánticas, combinando investigación fundamental, desarrollo tecnológico e innovación industrial. Este ecosistema de apoyo se estructura a través de múltiples iniciativas estratégicas que operan de manera coordinada, desde programas de investigación de base amplia hasta infraestructuras especializadas y convocatorias temáticas orientadas a aplicaciones específicas. Incluye tanto las líneas de investigación civil del Horizonte Europa como las convocatorias temáticas del Fondo Europeo de Defensa (EDF), destinadas a fortalecer las capacidades de defensa y seguridad de la Unión Europea.

El programa Horizonte Europa¹⁶⁰ (2021-2027) ha lanzado varias convocatorias específicas en tecnologías cuánticas, principalmente a través de iniciativas como QuantERA¹⁶¹ y los programas de trabajo del cluster 4, digital, industria y espacio¹⁶². Estas convocatorias han financiado proyectos en áreas como comunicación cuántica, computación cuántica, simulación, sensores y metrología, y ciencia cuántica general.

El Quantum Flagship¹⁶³ es la gran iniciativa emblemática de la Unión Europea para el desarrollo de tecnologías cuánticas, lanzada en 2018 como parte de los programas de investigación e innovación. Su objetivo fue impulsar la investigación, la innovación y la industrialización en áreas como la computación, la comunicación, la simulación, los sensores y la metrología cuántica, con una financiación prevista de al menos 1.000 millones de euros a lo largo de 10 años. El Quantum Flagship reúne a universidades, centros de investigación, industria y startups para acelerar la transferencia de la ciencia cuántica al mercado y reforzar la soberanía tecnológica europea.

EuroQCI¹⁶⁴ (*European Quantum Communication Infrastructure*) es una iniciativa específica de la Comisión Europea, en colaboración con los Estados miembros y la Agencia Espacial Europea, para desplegar una infraestructura paneuropea de comunicaciones cuánticas ultraseguras. El EuroQCI combina redes terrestres de distribución de claves cuánticas (QKD) mediante fibra óptica y un segmento espacial basado en satélites, con el fin de proteger las comunicaciones gubernamentales, infraestructuras críticas y datos sensibles frente a amenazas actuales y futuras, incluidos los ordenadores cuánticos. Muchos de los proyectos piloto, prototipos y estándares que se están implementando en EuroQCI han surgido de la investigación financiada por el Quantum Flagship, como el proyecto OPENQKD.

¹⁵⁹ <https://digital-strategy.ec.europa.eu/en/news/survey-eu-roadmap-post-quantum-cryptography>

¹⁶⁰ https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en

¹⁶¹ <https://quantera.eu/>

¹⁶² https://research-and-innovation.ec.europa.eu/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe/cluster-4-digital-industry-and-space_en

¹⁶³ <https://qt.eu/>

¹⁶⁴ <https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci>

También el Quantum Flagship ha dado lugar a otra iniciativa estratégica como la **Quantum Internet Alliance (QIA)**¹⁶⁵, que desarrolla un plan hacia una internet cuántica paneuropea basada en entrelazamiento. La iniciativa en la que colaboran universidades, centros tecnológicos e industria pretende conectar redes metropolitanas a través de una red a larga distancia con una pila completa de control y comunicaciones con un sistema operativo propio.

La Ley Europea de los Chips [CE 2023_2] también promueve las tecnologías cuánticas mediante el apoyo a la creación de líneas piloto de chips cuánticos y una instalación de diseño cuántico, con el objetivo de transformar prototipos científicos en productos fabricables y así acelerar la industrialización cuántica europea. Por otra parte, la *Chips Joint Undertaking*¹⁶⁶ financia infraestructuras y proyectos que incluyen tecnologías cuánticas, como la integración de chips cuánticos en sistemas de computación de alto rendimiento (HPC) y la conexión de estos con supercomputadores europeos a través de EuroHPC JU. Se han destinado inversiones específicas para el desarrollo de chips cuánticos y la creación de un clúster de computación híbrida que conecte infraestructuras HPC con ordenadores y simuladores cuánticos en varios Estados miembros, incluyendo España.

El Fondo Europeo de Defensa ha incluido en algunas de sus convocatorias las temáticas de las tecnologías cuánticas. En la convocatoria de 2021¹⁶⁷ se solicitaron propuestas al *Topic EDF-2021-DIS-RDIS-QSENS: Quantum technologies for defence* y en 2024 al *Topic EDF-2024-LS-RA-DIS-QUANT-STEP: Quantum technologies*¹⁶⁸. Adicionalmente las convocatorias abiertas a las PYMES para la investigación de soluciones para defensa innovadoras y de futuro, y las de tecnologías disruptivas para defensa, han seleccionado muchas propuestas relacionadas con tecnologías cuánticas.

5.4 La política de tecnologías cuánticas en otros países y organismos

Las iniciativas gubernamentales en tecnologías cuánticas se iniciaron en 2013 con el *UK National Quantum Technologies Programme* del Reino Unido seguidas de otras hasta la recién publicada Estrategia de Tecnologías Cuánticas de España (2025). Hoy en día, las grandes potencias económicas disponen de estrategias en tecnologías cuánticas, realizando fuertes inversiones en su investigación, desarrollo e implementación industrial.

Históricamente, las naciones han ido promoviendo iniciativas estables (planes, programas y estrategias) con dotaciones económicas anuales o plurianuales (Tabla 5-2). En muchas de las iniciativas incluyendo la española, la tardía presentación de una Estrategia Nacional no ha implicado que se haya comenzado tarde, ya que en la mayoría de los casos ya existían programas disgregados que coordinaban y financiaban tecnologías cuánticas de manera aislada. Así, es difícil ordenar cronológicamente las primeras iniciativas: Reino Unido (2013), China (2016), Japón, Alemania, Unión Europea y Estados Unidos (2018), Francia, Canadá y Australia (2021), la India (2022), OTAN (2023) y España (2025).

El contenido de las estrategias de los diferentes países sigue un patrón común que incluye una declaración de intenciones como país, un marco regulatorio y sus líneas maestras principales. Integrado o separado de la estrategia está el plan nacional, que contiene de manera más pormenorizada y detallada cómo se desea alcanzar los objetivos de la estrategia.

¹⁶⁵ <https://quantuminternetalliance.org/>

¹⁶⁶ <https://www.chips-ju.europa.eu/>

¹⁶⁷ https://defence-industry-space.ec.europa.eu/edf-2021-call-topic-descriptions_en

¹⁶⁸ https://defence-industry-space.ec.europa.eu/document/download/77afc5d2-30b2-4f3f-917c-2c4368eb18e3_en?filename=EDF%202024%20Call%20Topic%20Descriptions.pdf

País/Organización	Iniciativa Principal
Reino Unido	<i>UK National Quantum Technologies Programme</i> ¹⁶⁹
China	Estrategia Cuántica Nacional ¹⁷⁰
Alemania	Tecnologías Cuánticas: desde lo básico hasta el mercado ¹⁷¹
Comisión Europea	<i>Quantum Flagship</i> ¹⁷² (iniciativa paneuropea de 10 años)
Estados Unidos	<i>National Quantum Initiative Act</i> ¹⁷³
Japón	<i>Quantum Technology Innovation</i> ¹⁷⁴
Francia	<i>La Stratégie Nationale Quantique</i> ¹⁷⁵
Canadá	<i>National Quantum Strategy</i> ¹⁷⁶
Australia	<i>National Quantum Strategy</i> ¹⁷⁷
India	<i>National Quantum Mission</i> ¹⁷⁸
OTAN	<i>NATO's Quantum Technologies Strategy</i> ¹⁷⁹
España	Estrategia de Tecnologías Cuánticas de España ¹⁸⁰
Comisión Europea	<i>Quantum Europe Strategy</i> ¹⁸¹

Tabla 5-2 Principales iniciativas en tecnologías cuánticas a nivel mundial.

Entre los contenidos más destacados que podemos encontrar en las diferentes estrategias está el refuerzo de la investigación básica y aplicada y el desarrollo tecnológico; el desarrollo de infraestructuras críticas de apoyo; el fomento de la participación industrial y colaboración público-privada; la coordinación de las hojas de ruta tecnológicas; la exploración de nuevas aplicaciones; la aceleración de investigaciones precompetitivas y la transferencia de tecnología; la potenciación de la competitividad de la industria nacional impulsando el crecimiento económico basado en la adopción y comercialización de productos y servicios basados en estas tecnologías; el desarrollo de una fuerza laboral cuántica; el aseguramiento del liderazgo, el cuidado de la soberanía tecnológica, la propiedad

¹⁶⁹ <https://uknqt.ukri.org/>

¹⁷⁰ <https://www.scquantum.org/news/chinese-national-quantum-strategy-2023>

¹⁷¹ <https://www.bmfr.bund.de/SharedDocs/Publikationen/DE/5/>

¹⁷² https://qt.eu/31432_Rahmenprogramm_Quantentechnologien.html?templateQueryString=2018+Quantentechnologien

¹⁷³ <https://www.quantum.gov/>

¹⁷⁴ <https://www8.cao.go.jp/cstp/english/quantum/index.html>

¹⁷⁵ <https://quantique.france2030.gouv.fr/>

¹⁷⁶ <https://ised-isde.canada.ca/site/national-quantum-strategy/en>

¹⁷⁷ <https://www.industry.gov.au/publications/national-quantum-strategy>

¹⁷⁸ <https://dst.gov.in/national-quantum-mission-nqm>

¹⁷⁹ [https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/01/16/summary-of-natos-](https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/01/16/summary-of-natos-quantum-technologies-strategy)

[quantum-technologies-strategy](https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2024/01/16/summary-of-natos-quantum-technologies-strategy)

¹⁸⁰ https://digital.gob.es/content/dam/portal-mtdfp/comunicacion/comunicacion_ministro/2025/04/

[2025-04-24/EstrategiaTecnologiasCuanticas_compressed_24_04.pdf](https://digital.gob.es/content/dam/portal-mtdfp/comunicacion/comunicacion_ministro/2025/04/2025-04-24/EstrategiaTecnologiasCuanticas_compressed_24_04.pdf)

¹⁸¹ <https://digital-strategy.ec.europa.eu/en/library/quantum-europe-strategy>

intelectual, los intereses económicos y la seguridad nacional; y el desarrollo de la cooperación internacional. Todas estas estrategias buscan reforzar la soberanía tecnológica, la competitividad industrial y la seguridad nacional, con inversiones públicas y privadas millonarias.

En todas las estrategias se propone una inversión multianual durante la duración de las mismas. Según datos de la Estrategia de Tecnologías Cuánticas de España (2025), actualmente se han invertido a nivel mundial 42.000 millones de dólares de fondos públicos y 8.500 millones de dólares en inversión de startups cuánticas, compitiendo con las startups de IA generativa. La previsión del mercado cuántico se estima 97.500 millones de euros para 2040 [FGCSIC 2025]. España tiene un presupuesto inicial de 808 millones de euros, pero se espera que el potencial de atraer inversiones públicas y privadas eleve la inversión total a aproximadamente 1.500 millones de euros. La Figura 5-1 muestra la inversión internacional en planes estratégicos en tecnologías cuánticas, pero no incluye la reciente Estrategia de Tecnologías Cuánticas de España.

Las estrategias crean la figura de un coordinador que actúe como punto focal, implemente, armonice y supervise el cumplimiento de la estrategia y sus planes, y consolide un ecosistema coordinado desde la investigación a la industria. Los coordinadores se rodearían de comités interdepartamentales o interministeriales para la armonización sectorial o regional, de consejos de expertos para asesoramiento y de grupos de trabajo temáticos específicos.

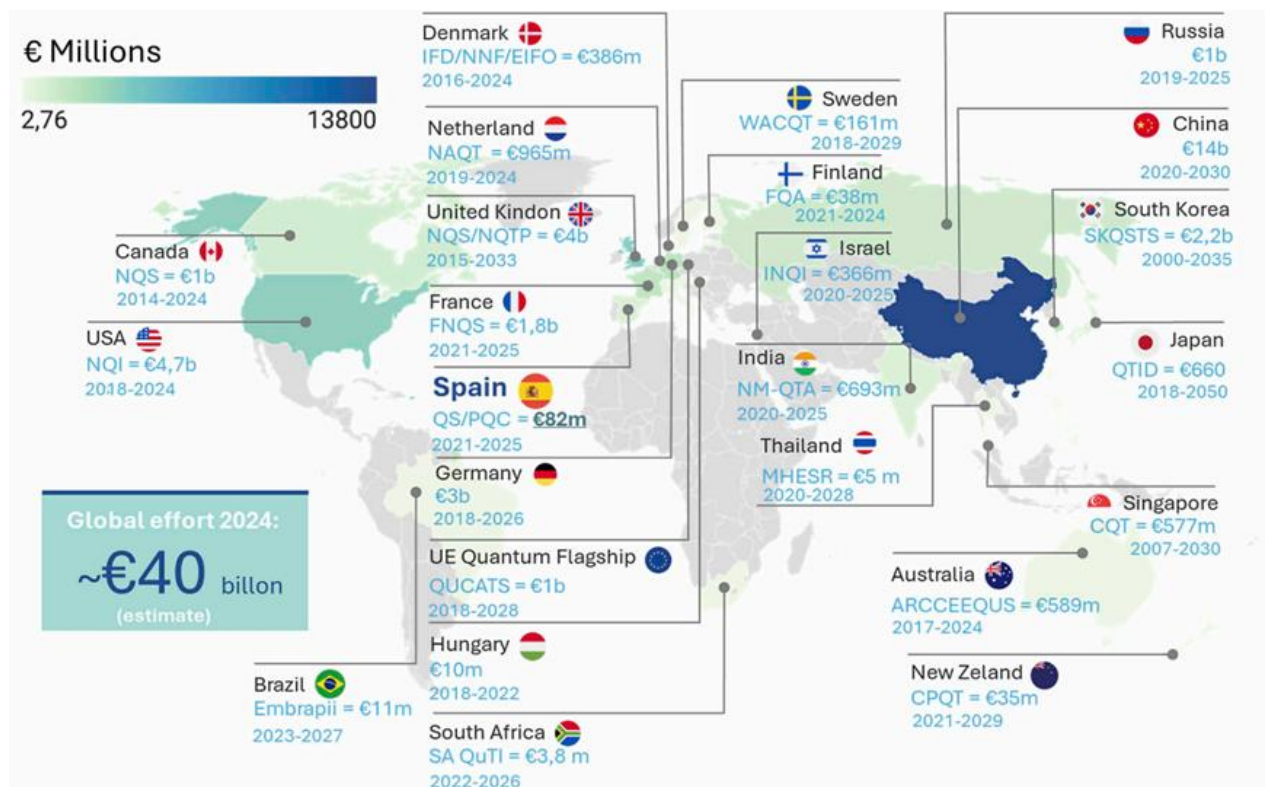


Figura 5-1 Mapamundi de inversión en planes estratégicos en tecnologías cuánticas [FGCSIC 2025].

La Organización de las Naciones Unidas (ONU) proclamó 2025 como el Año Internacional de la Ciencia y la Tecnología Cuánticas, en reconocimiento de los 100 años desde el desarrollo inicial de la mecánica cuántica, y con objeto de aumentar la conciencia pública sobre la importancia y el impacto de la ciencia cuántica y sus aplicaciones en todos los aspectos de la vida.

5.4.1 Iniciativas del Reino Unido en tecnologías cuánticas

El Reino Unido lanzó el UK National Quantum Technologies Programme en 2013, convirtiéndose en uno de los primeros países en establecer una hoja de ruta nacional para el desarrollo de tecnologías cuánticas. Este programa, con una inversión inicial de 270 millones de libras, se centró en la creación de hubs de investigación, la colaboración público-privada y la transferencia de tecnología a la industria, abarcando áreas como la computación, las comunicaciones, los sensores y la metrología cuántica.

La estrategia de 2023, denominada *UK National Quantum Strategy*, es una actualización y ampliación de la anterior, con una inversión pública comprometida de 2.500 millones de libras para la próxima década, y un enfoque más ambicioso en liderazgo internacional, aplicaciones industriales y competitividad global.

5.4.2 Iniciativas de Estados Unidos en tecnologías cuánticas

Estados Unidos no tiene una única estrategia centralizada como ocurre en Europa sino existe un conjunto de iniciativas que han ido evolucionando a lo largo del tiempo de acuerdo con la evolución de esta tecnología. El núcleo de las propuestas es la Iniciativa Nacional Cuántica (*National Quantum Initiative*, NQI)¹⁸² [USC 2018], lanzada en 2018 y reforzada en años posteriores con nuevos fondos y objetivos. Esta iniciativa busca posicionar a Estados Unidos como líder mundial en computación cuántica, comunicaciones cuánticas y sensores cuánticos, además de fomentar la formación de talento especializado.

A diferencia del enfoque europeo, que se basa en una coordinación política más estructurada desde la Comisión Europea, el modelo estadounidense se apoya en la colaboración entre agencias federales, como el Instituto Nacional de Estándares y Tecnología (*National Institute of Standards and Technology*, NIST)¹⁸³, el Departamento de Energía (*Department of Energy*, DOE)¹⁸⁴ y la Fundación Nacional de Ciencias (*National Science Foundation*, NSF)¹⁸⁵, junto con consorcios como el Consorcio de Desarrollo Económico Cuántico (*Quantum Economic Development Consortium*, QED-C). Esta red de actores impulsa la investigación, la estandarización y la transferencia tecnológica hacia el sector privado.

En el ámbito de Defensa, la Ley de Aceleración Cuántica para Defensa del Departamento de Defensa USA [USC 2024] establece iniciativas para acelerar la integración de la ciencia de la información cuántica (Quantum Information Science, QIS) en el Departamento de Defensa. También son de destacar las iniciativas de DARPA *Quantum Benchmarking Initiative* (QBI)¹⁸⁶ y *Quantum-Augmented Network* (QuANET)¹⁸⁷. El programa QBI es un programa lanzado en 2024 para evaluar rigurosamente si alguna arquitectura de computación cuántica puede alcanzar la escala útil (*utility-scale*) en 2033. La escala útil quiere decir que el valor computacional supere al coste. Su objetivo es verificar y validar enfoques hacia ordenadores cuánticos con corrección de errores y tolerancia a fallos que puedan ejecutar algoritmos de interés práctico con alto rendimiento y menor coste que las alternativas actuales. Uno de los programas que forman parte del QBI es el US2QC (*Underexplored Systems for Utility-Scale Quantum Computing*)¹⁸⁸ que explora arquitecturas de ordenadores cuánticos

¹⁸² <https://www.quantum.gov/>

¹⁸³ <https://www.nist.gov/>

¹⁸⁴ <https://www.energy.gov/>

¹⁸⁵ <https://www.nsf.gov/>

¹⁸⁶ <https://www.darpa.mil/research/programs/quantum-benchmarking-initiative>

¹⁸⁷ <https://www.darpa.mil/research/programs/quantum-augmented-network>

¹⁸⁸ <https://www.darpa.mil/research/programs/underexplored-systems-for-utility-scale-quantum-computing>

poco estudiadas. El programa QuANET busca integrar tecnologías de comunicación cuántica con infraestructuras clásicas para crear redes más seguras y resistentes frente a ciberataques.

Uno de los aspectos más distintivos de la estrategia estadounidense es su fuerte vínculo con la industria. Empresas como IBM, Google o D-Wave lideran el desarrollo de computadoras cuánticas y algoritmos, y atraen más del 50% del capital privado global destinado a estas tecnologías. Estados Unidos se apoya en la fuerza de su ecosistema científico-tecnológico, en el dinamismo de su sector privado, en su capacidad de innovación rápida y su aplicación en sectores estratégicos, incluyendo los sectores de Defensa, Aeronáutico y Espacial.

5.4.3 Actividades Chinas en tecnologías cuánticas

China considera la tecnología cuántica como un elemento central en la competencia científica y tecnológica global, especialmente frente a Estados Unidos, y está impulsando su desarrollo con una fuerte inversión pública estimada en unos 15.000 millones de dólares, comparado con aproximadamente los 3.800 millones de Estados Unidos. Desde 2022, China publica más artículos científicos sobre tecnología cuántica que cualquier otro país y lidera el despliegue de redes de comunicación cuántica con una extensión de 12.000 km y dos satélites (Micius y Jinan-1) dedicados a crear una infraestructura espacio-tierra de comunicaciones seguras. También desarrolla ordenadores cuánticos basados en procesadores fotónicos y superconductores, que progresan tanto en número de qubits como en estabilidad, aunque Estados Unidos mantiene liderazgo en muchos aspectos clave.

La innovación china en tecnologías cuánticas es fundamentalmente estatal con escasa inversión privada y una coordinación dirigida por el Partido Comunista y el gobierno, lo que supone una diferencia cultural y estratégica con los países occidentales [MERICS 2024]. Su intención es lograr aplicaciones militares, especialmente en criptografía, comunicaciones militares seguras y procesamiento avanzado de información. Los efectos de las restricciones a la exportación sobre componentes críticos, impuestas por países occidentales, han empujado a China a crear cadenas de suministro independientes y alcanzar la autosuficiencia tecnológica. La tecnología cuántica tendrá grandes implicaciones económicas, industriales, científicas y militares, y Europa debe mantener un papel activo en cooperación, gobernanza y estándares para no depender de normas y tecnología dictadas por potencias extranjeras, y para evitar una fragmentación global entre Estados Unidos y China.

La financiación de la innovación cuántica china presenta una asimetría fundamental respecto a Estados Unidos¹⁸⁹. Mientras que las startups estadounidenses reciben aproximadamente 1,28 billones de dólares en capital privado, las chinas reciben apenas 44 millones de dólares. Esta brecha estructural limita la inversión en talento, investigación y desarrollo y comercialización. Sin embargo, China lo ha compensado mediante un modelo alternativo de financiación estatal centralizada. La Fundación Nacional de Ciencias Naturales de China (NSFC) financia aproximadamente cincuenta por ciento de todas las publicaciones cuánticas chinas, proporcionando un flujo de capital predecible y coordinado que carece de equivalente en Estados Unidos, donde la financiación se fragmenta entre departamentos federales sin una coordinación central.

5.4.4 Actividades de la OTAN en tecnologías cuánticas

La OTAN publicó en enero de 2024 su primera estrategia sobre tecnologías cuánticas¹⁹⁰, aprobada por los ministros de Asuntos Exteriores de los países miembros en noviembre de 2023. El documento subraya como la transformación innovadora de estas tecnologías puede ser decisiva para la seguridad y la defensa moderna. La estrategia contempla aplicaciones en detección submarina, posicionamiento

¹⁸⁹ <https://itif.org/publications/2024/09/09/how-innovative-is-china-in-quantum/>

¹⁹⁰ <https://www.nato.int/en/news-and-events/articles/news/2024/01/17/nato-releases-first-ever-quantum-strategy>

preciso, navegación, comunicaciones seguras mediante criptografía resistente a la computación cuántica y sensores avanzados. Además, busca preparar a la Alianza frente al uso malicioso de estas capacidades y fomentar la cooperación con la industria para crear un ecosistema transatlántico en este ámbito.

Enmarcada dentro de la estrategia cuántica de la Alianza, el 2 de julio de 2024 se celebró en Bruselas la reunión inaugural del *Transatlantic Quantum Community* (TQC)¹⁹¹. La comunidad, presidida el primer año por Dinamarca, es una iniciativa impulsada por la OTAN para reforzar la cooperación aliada en el ámbito de las tecnologías cuánticas. El objetivo de la TQC es reunir a expertos de gobiernos, industria, academia y organismos de financiación para fomentar la innovación y mantener la ventaja tecnológica de la OTAN. Entre sus prioridades figuran abordar retos de financiación y desarrollo tecnológico, impulsar la formación de talento y explorar nuevas oportunidades de colaboración. Actualmente lidera el Reino Unido y España participa con el apoyo del ecosistema cuántico nacional.

El panel de Incubación de Tecnología y Ciencia (*Technology and Science Incubation*, TSI)¹⁹², de la Organización de Ciencia y Tecnología (*Science and Technology Organization*, STO) de la OTAN, surge con el objetivo de incubar temas emergentes que no estaban cubiertos por los programas tradicionales del Programa de Trabajo Colaborativo (*Collaborative Programme of Work*, CPoW). Su motivación principal es garantizar que la Alianza mantenga la ventaja científica y tecnológica y frente a amenazas y cambios rápidos en el entorno global. El enfoque del TSI se basa en ciclos de tres años, con la capacidad de cambiar de temática según las necesidades estratégicas, lo que permite mantener la relevancia y la innovación en defensa y seguridad. Actualmente se centra en dos áreas principales, tecnologías cuánticas y biotecnología. En el ámbito cuántico, se exploran aplicaciones como sensores, comunicaciones seguras, navegación y computación avanzada. En biotecnología, se abordan materiales innovadores, procesos industriales, biocomputación, sistemas bio-híbridos y soluciones para agricultura y medio ambiente. Además, se busca integrar estas disciplinas con otras tecnologías disruptivas como la inteligencia artificial, la robótica y la nanotecnología, creando sinergias que potencien la capacidad de respuesta de la OTAN frente a desafíos globales.

DIANA¹⁹³, la aceleradora de innovación de la OTAN, ha puesto en marcha varias iniciativas clave en torno a las tecnologías cuánticas. Entre ellas destaca la creación del Centro Cuántico DIANA de la OTAN (DIANAQ)¹⁹⁴, en la Universidad de Copenhague, concebido como un espacio seguro para reunir a emprendedores, inversores y científicos en el desarrollo de tecnologías cuánticas de doble uso. Además, DIANA ha impulsado programas de aceleración para startups llegando a diez empresas en la segunda fase del programa 2024, incluyendo la empresa española *Quside Technologies* que fabrica generadores cuánticos de números aleatorios. Otra iniciativa relevante ha sido el apoyo a proyectos pioneros, como la primera comunicación transatlántica cuántico-segura realizada en junio de 2025 por Quantropi Inc. y Alea Quantum Technologies. Este enlace conectó dos centros DIANA, el BioInnovation Institute en Copenhague y COVE en Halifax, demostrando la capacidad de la Alianza para garantizar comunicaciones resistentes a la computación cuántica. Asimismo, DIANA trabaja con más de 200 aceleradoras y unos 180 centros de prueba en toda la OTAN, ofreciendo espacios para validar y demostrar soluciones cuánticas en entornos operativos reales.

¹⁹¹ <https://www.nato.int/en/news-and-events/articles/news/2024/07/02/denmark-chairs-the-inaugural-meeting-of-natos-transatlantic-quantum-community>

¹⁹² <https://www.sto.nato.int/the-collaborative-programme-of-work-cpow/technology-and-science-incubation/>

¹⁹³ <https://www.diana.nato.int/>

¹⁹⁴ <https://dianaq.ku.dk/>

5.5 Estado de la cuántica en el mundo

5.5.1 Ciencia, tecnología e inversión [MIT 2025]

En el plano global, la carrera por el dominio de las tecnologías cuántica es muy intensa. Varios países han establecido estrategias nacionales integrales para desarrollar liderazgo en este campo, invirtiendo miles de millones de dólares y movilizandolos sus ecosistemas académicos, empresariales y gubernamentales. La distribución geográfica de estos esfuerzos refleja tanto las capacidades existentes como las ambiciones futuras de las principales potencias mundiales, con implicaciones profundas para la seguridad nacional, la competitividad económica y la estabilidad geopolítica.

El desarrollo cuántico se apoya en la colaboración estrecha entre corporaciones, universidades y gobiernos. Las universidades y centros académicos lideran la generación de conocimientos fundamentales e investigación básica, especialmente en publicaciones científicas, colaboraciones y desarrollo de teorías y algoritmos. Sin embargo, las investigaciones más influyentes suelen surgir de colaboraciones entre grandes grupos universitarios y empresas, como ocurre con Google, IBM, Microsoft y varias instituciones asiáticas. Estas alianzas permiten trasladar avances teóricos al mercado y acelerar la transferencia tecnológica. La relación entre el desarrollo cuántico corporativo y académico a nivel mundial se caracteriza por una fuerte interdependencia y cooperación, pero también por dinámicas específicas según región y tipo de tecnología. Los programas internacionales y nacionales suelen enfatizar la cooperación público-privada, especialmente en Europa y América del Norte, mientras que en China predomina un enfoque estatal y centralizado, aunque con participaciones empresariales significativas. Esta diferencia en modelos de gobernanza tiene implicaciones profundas para la velocidad de innovación, la distribución de capacidades y la seguridad de la cadena de suministro cuántica.

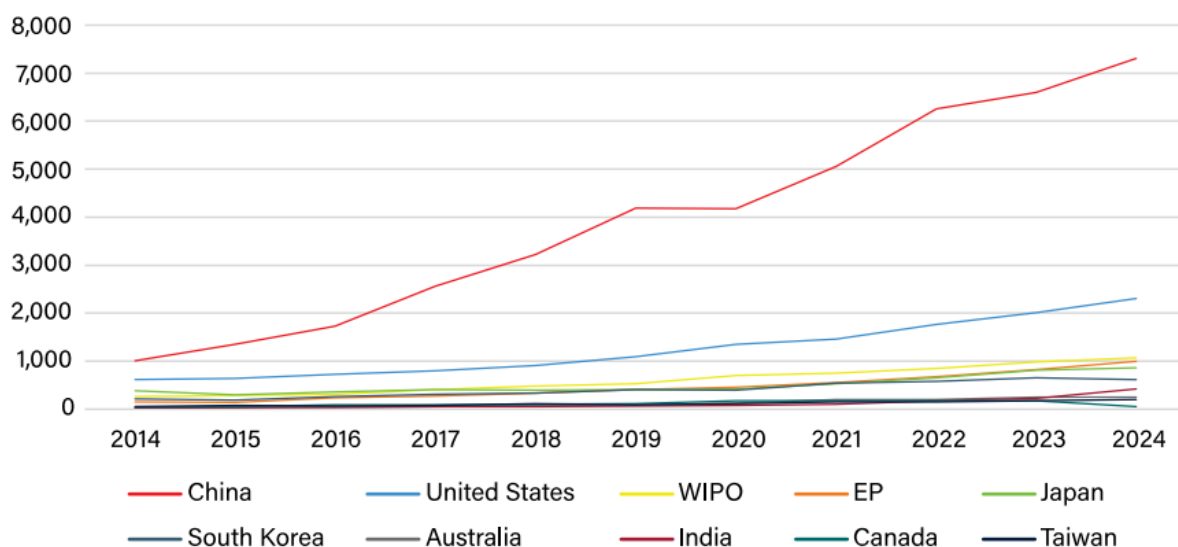


Figura 5-2 Patentes en tecnologías cuánticas por país, 2014-2024 [MIT 2025].

China ocupa una posición de liderazgo mundial en varias áreas de las tecnologías cuánticas, aunque presenta una especialización estratégica distinta respecto a otros países punteros como Estados Unidos y las potencias europeas. La estrategia china es eminentemente estatal, con énfasis en estándares propios y control de la cadena de valor, mientras que en Occidente predomina la colaboración internacional y público-privada. El gobierno chino ha destinado aproximadamente 15.000 millones de dólares (más del 50% de la inversión pública global) al desarrollo cuántico, superando con

crecen las cantidades invertidas por otras potencias. En el campo específico de comunicaciones cuánticas, China lidera claramente en cantidad de patentes y volumen de innovación, soportada por una inversión estatal masiva y una estrategia nacional orientada a la soberanía tecnológica y la seguridad. Instituciones como QuantumCTek, Ruban Quantum Technology y la Universidad de Pekín de Correos y Telecomunicaciones se encuentran entre los principales titulares de patentes en este dominio. La inversión China en estas tecnologías ha permitido hitos como el lanzamiento del primer satélite cuántico (Micius/QUESS en 2016) y la creación de la mayor red de comunicación cuántica del mundo, que se extiende más de 12.000 kilómetros. En hardware cuántico, China es el segundo país en cuanto a número y diversidad de unidades procesadoras cuánticas (QPU) disponibles comercialmente, después de Estados Unidos. Sin embargo, las QPU chinas tienden a ser de menor escala y prestaciones respecto a las estadounidenses y europeas.

Entre 2016 y 2021, las solicitudes de patentes en computación cuántica se incrementaron en más del 300%, y el total de patentes cuánticas creció cinco veces entre 2014 y 2024, demostrando la aceleración exponencial de la actividad innovadora en este campo. El 91% de las patentes en computación cuántica provienen de corporaciones (54%) y universidades (37%), lo que refleja que la innovación es impulsada fundamentalmente por estos dos sectores y suele estar muy concentrada en ellos. Los gobiernos y organizaciones sin ánimo de lucro tienen un papel minoritario en el volumen total de propiedad intelectual registrada. China es el país dominante en cuanto a patentes de tecnologías cuánticas. En 2024 tenía el 60% de todas las patentes globales en este sector, muy por delante de Estados Unidos (19%) y Japón, situado en tercera posición (Figura 5-2).

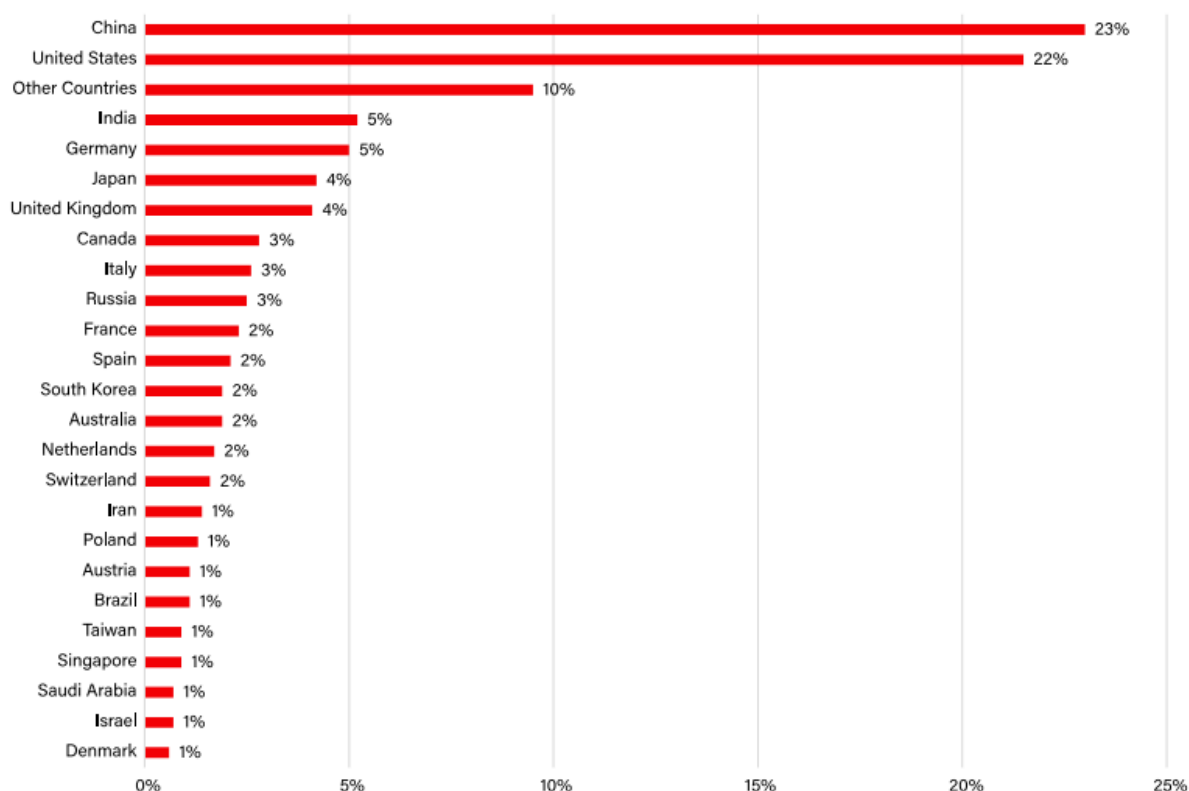


Figura 5-3 Porcentaje nacional de las publicaciones de investigaciones en computación cuántica, 2019-2023 [MIT 2025].

En publicaciones científicas sobre computación cuántica, China lidera el ranking en producción de artículos con el 23% del total global, seguida de cerca por Estados Unidos con el 22% (Figura 5-3). No

obstante, la investigación estadounidense es reconocida por su mayor índice de impacto (H-index de 104 frente a 61 de China) y la proporción de artículos altamente citados, lo que señala que, aunque China publica más, Estados Unidos produce trabajos de mayor influencia científica. En comunicaciones cuánticas, China es líder absoluto tanto en volumen (39% de las publicaciones) (Figura 5-4) como en calidad y citaciones, con un H-index de 51 que supera significativamente al de Estados Unidos (39). Esta fortaleza en investigación de comunicaciones cuánticas refleja una estrategia nacional deliberada y enfoque coordinado hacia el desarrollo de sistemas de comunicación ultra-seguros y redes de distribución de clave cuántica.

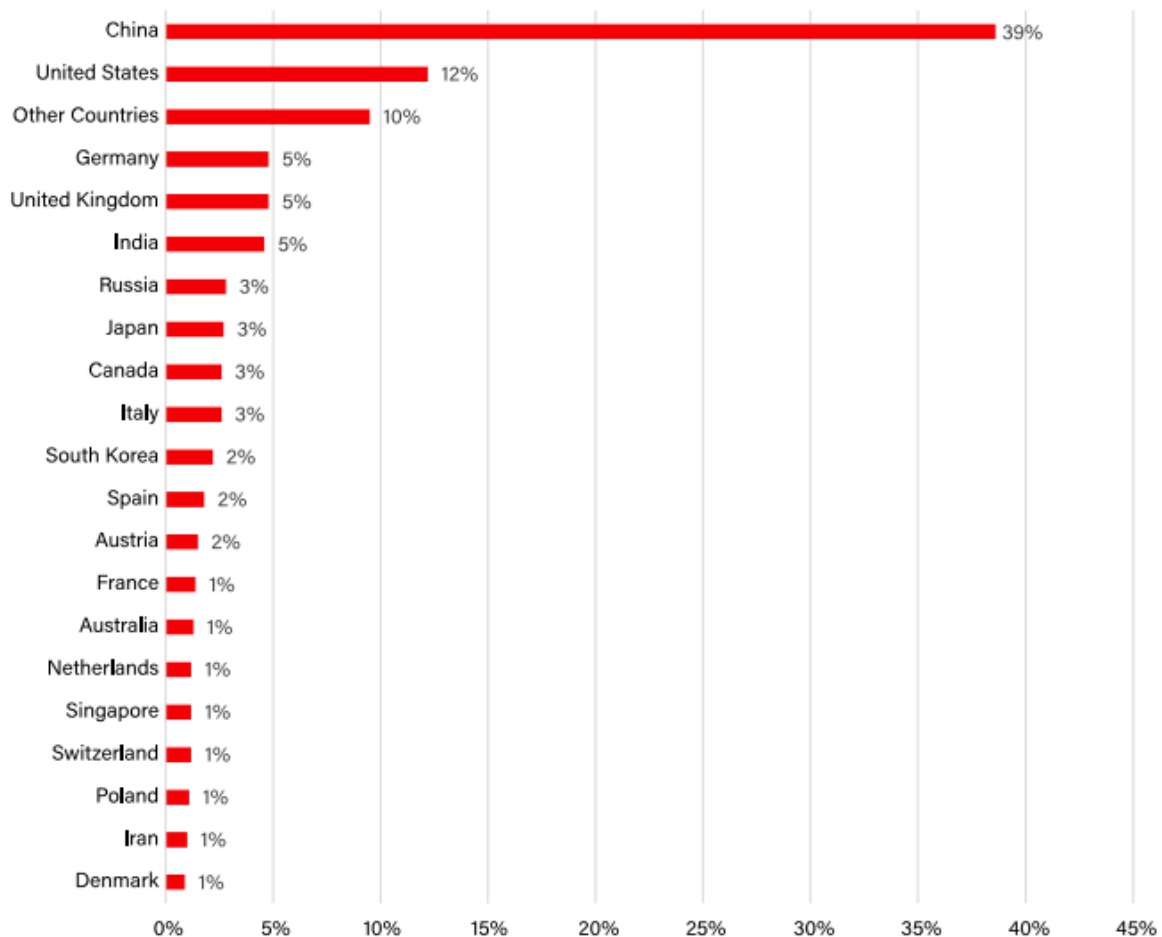


Figura 5-4 Porcentaje nacional de las publicaciones de investigaciones en comunicaciones cuánticas, 2019-2023 [MIT 2025].

Los fondos de capital riesgo se dirigen mayoritariamente a startups y empresas especializadas. En 2024, las compañías de computación cuántica captaron 1.600 millones de dólares en inversiones, mientras que el sector del software cuántico obtuvo 621 millones. El mayor impulso comercial corresponde a Estados Unidos y Reino Unido, que concentran el 60% de la inversión global, pero Europa y Asia también muestran un crecimiento robusto debido a estrategias multinacionales y apoyo estatal.

5.5.2 Formación y capacitación del personal

Se requiere desarrollar una fuerza laboral cuántica capaz de investigar, diseñar, fabricar, operar y mantener sistemas basados en tecnologías cuánticas. El sector de tecnologías cuánticas se enfrenta a un desajuste crítico entre la demanda creciente de profesionales especializados y la oferta limitada de candidatos formados. Como ha ocurrido con otras tecnologías, el sector privado de tecnología cuántica compite agresivamente por el talento especializado, ofreciendo salarios y beneficios que pueden exceder significativamente lo disponible en instituciones académicas y sector público. Una vez más los gobiernos deben implementar estrategias para retener profesionales cualificados en roles estratégicos, incluyendo flexibilidad en las estructuras de empleo público, colaboración industria-gobierno que permita la circulación del talento, y la creación de un rol profesional atractivo en la administración pública.

La demanda de competencias cuánticas en el mercado laboral estadounidense casi se ha triplicado desde 2018, mientras que el ritmo de formación de profesionales especializados ha sido insuficiente para cerrar esta brecha. El análisis de demanda en trabajos especializados en computación cuántica, ingeniería de sistemas cuánticos y ciberseguridad post-cuántica, revela que existe aproximadamente un candidato cualificado por cada tres posiciones especializadas disponibles. Este desajuste es particularmente acentuado en perfiles aplicados de ingeniería e integración de sistemas. Mientras que existen científicos en física cuántica y teoría de la computación cuántica, la escasez es más severa en ingenieros de software cuántico, y técnicos de operación y mantenimiento de hardware cuántico. El gobierno de Estados Unidos, a través de la Iniciativa Nacional Cuántica (*National Quantum Initiative*, NQI), ha puesto énfasis significativo en el desarrollo de la fuerza de trabajo, mientras que Canadá y Australia han lanzado estrategias nacionales cuánticas similares enfocadas en la expansión de la capacidad laboral [MIT 2025]. Europa, de manera análoga, ha lanzado la convocatoria DIGITAL-2025-SKILLS-08-QUANTUM-ACADEMY-STEP¹⁹⁵, para el establecimiento de una “Academia Digital de Habilidades Cuánticas” que proporcione formación especializada en tecnologías cuánticas y experiencia práctica en diferentes niveles de educación cuántica.

En educación formal en el panorama global muestra una expansión rápida pero aún insuficiente de programas especializados, así como en el número de graduados por año requeridos por la industria. Los programas de máster dedicados específicamente a tecnologías cuánticas están liderados por Alemania con 12, Reino Unido con 10 y Estados Unidos con 9, representando el 45% de todos los programas a nivel mundial. Francia y Holanda contribuyen con 6 programas cada uno [MIT 2025]. Estos programas combinan teoría cuántica fundamental con aplicaciones en ingeniería y ciencia de materiales.

La industria ha desempeñado un papel crucial en cerrar la brecha mediante programas de capacitación corporativa¹⁹⁶. IBM ofrece el *Qiskit Global Summer School*, que atrae a miles de participantes anuales y proporciona entrenamiento intensivo en programación cuántica y desarrollo de algoritmos. Microsoft ha desarrollado módulos de capacitación en su plataforma *Azure Quantum* que cubren entornos de desarrollo cuántico y programación híbrida clásico-cuántica. *D-Wave Systems* ofrece entrenamiento especializado en técnicas de *quantum annealing* y optimización, incluyendo cursos como “*Foundations for Quantum Programming*” diseñados para construir habilidades matemáticas y de programación previas a especializarse en computación cuántica. Estos programas corporativos enfatizan habilidades prácticas y aplicabilidad inmediata, complementando la formación académica más teórica

¹⁹⁵<https://digital-skills-jobs.europa.eu/en/opportunities/funding/digital-2025-skills-08-quantum-academy-step-sectoral-digital-skills-academies>¹⁹⁶<https://www.spinquanta.com/news-detail/quantum-computing-courses-building-the-quantum-workforce-of-tomorrow>

La educación cuántica se expande en todos los niveles, mostrando la importancia de la formación académica adaptada a la demanda corporativa y científica. Universidades y empresas colaboran en la creación de cursos y materiales, y en programas de doctorado y formación especializada, lo que facilita la movilidad de talento entre ambos mundos. Existen hubs, programas de formación conjunta, y plataformas de acceso a computadoras cuánticas (*quantum-as-a-service*, QaaS) que permiten a estudiantes y empresas experimentar e innovar [MIT 2025].

A nivel de educación primaria y secundaria, se han lanzado iniciativas para introducir conceptos cuánticos y generar talentos desde edades tempranas. En Estados Unidos, la *National Q-12 Education Partnership*, creada como parte de la NQI, desarrolla materiales educativos y herramientas interactivas para estudiantes desde primaria hasta secundaria. La Unión Europea, a través de su programa *Quantum Flagship*, ha integrado temas de tecnología cuántica en currículos de educación secundaria en múltiples estados miembros. El *Coding School*, en colaboración con IBM, el Instituto Tecnológico de Massachusetts (*Massachusetts Institute of Technology*, MIT) y la Universidad de California en Berkeley, ha capacitado desde 2020 a más de 18,000 estudiantes de secundaria en fundamentos de computación cuántica, demostrando que conceptos cuánticos complejos pueden ser accesibles a audiencias jóvenes [MIT 2025].

La adopción exitosa de sistemas cuánticos en defensa requiere, más allá de los desarrolladores de tecnología y equipos, que el personal civil y militar responsable de la especificación, adquisición, operación y mantenimiento desarrolle competencias en tecnologías cuánticas. Este personal no necesita ser experto en mecánica cuántica o algoritmos cuánticos complejos, pero debe comprender suficientemente los principios, capacidades, limitaciones y requisitos operacionales de estos sistemas. La Academia de la Fuerza Aérea de Estados Unidos (*United States Air Force Academy*, USAFA) ha desarrollado una especialización académica secundaria en tecnologías cuánticas¹⁹⁷ para oficiales de la rama aérea, que proporciona formación integral en principios cuánticos, aplicaciones militares y consideraciones de integración de sistemas.

Un aspecto estratégico emergente y de urgencia inmediata es la migración masiva de la infraestructura criptográfica de gobiernos, defensa y sectores críticos a algoritmos criptográficos resistentes a ataques cuánticos (*post-quantum cryptography*, PQC). La capacitación del personal en ciberseguridad cuántica no solo afecta a personal técnico especializado, sino requiere que los funcionarios responsables de los servicios y operaciones de sistemas de información y ciberseguridad, comprendan las características operacionales, los requisitos de integración y las limitaciones de rendimiento.

¹⁹⁷ <https://www.usafa.edu/academic/quantum-technologies/>

6 CONCLUSIONES Y ACCIONES FUTURAS

La segunda revolución cuántica, enfocada en el control y la ingeniería directa de sistemas cuánticos, ha evolucionado desde los conceptos teóricos hacia las tecnologías tangibles con aplicación dual crítica. El presente trabajo ha establecido una metodología estructurada y replicable para analizar estas Tecnologías Emergentes y Disruptivas (EDT) en el ámbito de la Defensa. A través del recorrido realizado, desde los fundamentos científicos del Capítulo 2 y las aplicaciones operativas del Capítulo 3, hasta el mapeo industrial del Capítulo 4 y el análisis político-estratégico del Capítulo 5, se concluye que la computación y las comunicaciones cuánticas representan tanto oportunidades transformadoras como riesgos geopolíticos para las capacidades militares de Mando y Control, ISR, ciberdefensa y logística.

En el contexto actual, marcado por el desarrollo del ordenador cuántico y estrategias como “cosechar ahora, descifrar después”, este análisis sugiere a los responsables de los Sistemas de Información y Telecomunicaciones (CIS/TIC) del Ministerio de Defensa tomar como referencia los plazos y acciones detallados en la Tabla 3-1 para definir su estrategia y plan de acción específico. La anticipación en la implementación de estas medidas constituye un factor clave para garantizar la confidencialidad de la información clasificada a largo plazo frente a la evolución de las capacidades ofensivas.

Para garantizar la superioridad en el espectro de la información y la soberanía tecnológica, se propone una hoja de ruta articulada en los siguientes ejes de acción:

- **Capacitación y Formación del Personal:** La adopción exitosa de estas capacidades requiere trascender la mera adquisición de equipos para abordar el desafío estratégico del capital humano, mitigando la brecha crítica global entre la demanda exponencial de perfiles cualificados y la oferta limitada de talento mediante una estrategia de formación escalonada. Se propone dotar al personal especialista de los cuerpos de ingenieros y TIC de conocimientos técnicos relevantes a través de programas de posgrado y másteres especializados, enfocándose no solo en la física teórica sino en la ingeniería de sistemas y mantenimiento necesarios para operar estas tecnologías. Simultáneamente, resulta vital implementar un programa corporativo de concienciación básica para el personal de estado mayor y operativo, para que los responsables de la planificación comprendan las limitaciones físicas y los conceptos operacionales sin necesidad de ser expertos. También se debe incluir la instrucción específica de los responsables CIS en la migración urgente a la Criptografía Post-Cuántica (PQC), para gestionar la transición durante el periodo híbrido.
- **Identificación de aplicaciones militares:** Se requiere implementar un proceso sistemático de traducción tecnológica que convierta la factibilidad detectada en verdadera capacidad militar, cubriendo el vacío existente entre la disponibilidad comercial y la utilidad táctica. Esta actividad debe centrarse en la definición y la evaluación de casos de uso operativos específicos, tales como la optimización logística en zona de operaciones, la simulación estratégica o la protección de enlaces de mando y control, analizando no solo la madurez tecnológica (TRL), sino también los niveles de madurez de integración (IRL) y de sistema (SRL) necesarios para garantizar su interoperabilidad con la infraestructura heredada. Este enfoque permitirá adecuar las soluciones duales emergentes a los requisitos singulares de Defensa, priorizando la adopción de arquitecturas híbridas y el paradigma “*Quantum + X*” que aporten una ventaja tangible y evitando la inversión en tecnologías que, aunque científicamente viables, carezcan de relevancia operativa inmediata para las Fuerzas Armadas.

- **Vigilancia Tecnológica e Industrial:** España y Europa se enfrentan una dependencia estratégica crítica que se ve acentuada por el endurecimiento de los controles de exportación sobre tecnologías de doble uso. El mercado global está polarizado entre la innovación en hardware de computación liderada por el capital privado de Estados Unidos (IBM, Google) y el dominio estatal de China en patentes y despliegue de infraestructuras de comunicaciones. Ante la heterogeneidad del panorama tecnológico, la madurez industrial y su potencial aplicación operativa en Defensa, se recomienda la creación de un Grupo de Trabajo específico para tecnologías con TRL > 5 (disponibilidad a corto y medio plazo, 2-5 años). Este grupo debe centrarse en la validación de productos comerciales ya existentes en QKD y QRNG para su integración operativa, dejando la vigilancia de la computación cuántica tolerante a fallos (FTQC), cuyo horizonte de madurez (TRL < 5) se proyecta más allá de 2030, bajo la competencia de los departamentos de prospectiva básica e I+D.
- **Planes tecnológicos e industriales:** La estrategia nacional debe priorizar pragmáticamente los nichos donde la Base Industrial y Tecnológica de Defensa (BITD) española ya posee capacidad competitiva probada y reconocimiento internacional, como las infraestructuras QKD (LuxQuanta, QDynamics), el QRNG de alta velocidad (Quside), los simuladores cuánticos (Qilimanjaro) y los algoritmos PQC. Estas capacidades deben coordinarse bajo el paraguas de la Estrategia de Tecnología e Innovación para la Defensa (ETID 2020) y la Estrategia Industrial de Defensa (EID 2023), ejecutándose a través del Plan Industrial y Tecnológico 2025. Se recomienda que el recién creado Comité Nacional de Seguridad y Soberanía Tecnológica asuma la gobernanza de esta hoja de ruta, definiendo hitos operativos claros y asegurando su alineación con iniciativas europeas clave como EuroQCI y el Fondo Europeo de Defensa (EDF), y realizando una evaluación continua de la cadena de suministro para identificar componentes críticos y puntos únicos de fallo.
- **Experimentación y despliegue en Entornos Tácticos:** Se debe priorizar la transición desde la validación en laboratorio hacia la experimentación operativa de soluciones de comunicaciones seguras, integrando la Criptografía Post-Cuántica (PQC), los Generadores Cuánticos de Números Aleatorios (QRNG) y la Distribución Cuántica de Claves (QKD). Estas tecnologías han alcanzado niveles de madurez TRL 6-9 con soluciones comerciales disponibles para su despliegue inmediato. El objetivo final es asegurar una capacidad de comunicación y sincronización instantánea, resiliente, de alta capacidad y teóricamente no interceptable en entornos tácticos multidominio. Para ello, es esencial colaborar estrechamente con el ecosistema industrial nacional, aprovechando proyectos piloto que evalúen e integren soluciones de alta madurez y potencial operatividad en los sistemas de información y comunicaciones actuales.
- **Liderazgo en Estandarización e Internacionalización:** España debe asumir un rol proactivo y de liderazgo en los procesos de Pruebas, Evaluación, Verificación y Validación (TEVV), así como en la certificación e interoperabilidad, garantizando que los nuevos desarrollos sean seguros, fiables y compatibles con las infraestructuras heredadas y los estándares aliados. Esto implica intensificar la participación en la OTAN a través de la *Transatlantic Quantum Community* (TQC), la *Science & Technology Organization* (STO) y el *Allied Command Transformation* (ACT), capitalizando el éxito de la industria nacional en el acelerador DIANA (como G2-Zero y Quside) para posicionar las tecnologías de doble uso. Asimismo, es fundamental alinear las capacidades nacionales con la base industrial europea mediante la colaboración con la Agencia Europea de Defensa (EDA) y el seguimiento activo de programas del Fondo Europeo de Defensa (EDF) y la iniciativa EuroQCI, asegurando la integración en las cadenas de suministro críticas y evitando la fragmentación tecnológica en el desarrollo de futuras redes de comunicaciones seguras.
- **Ampliación del Alcance:** Finalmente, aunque este análisis se ha centrado en la computación y las comunicaciones cuánticas, la metodología estructurada debe incorporar el dominio de los

sensores y la metrología cuántica, cerrando el círculo de la adaptación de la Defensa a la era cuántica. Dentro de las tecnologías cuánticas, los sensores cuánticos ofrecen una madurez tecnológica superior y una factibilidad de adopción más inmediata, permitiendo su integración progresiva como cargas de pago en plataformas y sistemas heredados sin requerir una sustitución completa de la infraestructura. Estas tecnologías son críticas para garantizar la independencia operativa en entornos degradados, proporcionando capacidades de navegación y posicionamiento de alta precisión (PNT) independientes del GNSS, así como mejoras sustanciales en la detección de amenazas submarinas y subterráneas mediante gravimetría y magnetometría avanzada. Por tanto, futuros trabajos deben aplicar rigurosamente los criterios de madurez tecnológica (TRL) y de integración (IRL) a esta disciplina para completar la estrategia de adaptación de la Defensa a la era cuántica, asegurando que no se ignoren ventajas tácticas que ya están técnicamente al alcance.

7 BIBLIOGRAFÍA

En este capítulo figuran todas las referencias citadas en el trabajo en el estilo IEEE. Todos los enlaces a sitios web y recursos en línea incluidos en este listado y en las notas a pie de página han sido consultados y verificados durante el segundo semestre de 2025.

- [AbuGhanem 2024] M. AbuGhanem, “IBM Quantum Computers: Evolution, Performance, and Future Directions,” arXiv preprint arXiv:2410.00916, Sep. 2024. [En línea]. Disponible en: <https://arxiv.org/html/2410.00916v1>
- [Acín 2018] A. Acín et al., “The quantum technologies roadmap: a European community view,” *New Journal of Physics*, vol. 20, no. 8, p. 080201, Aug. 2018, doi: 10.1088/1367-2630/aad1ea.
- [ADR 1982] A. Aspect, J. Dalibard, and G. Roger, “Experimental test of Bell’s inequalities using time-varying analyzers,” *Physical Review Letters*, vol. 49, no. 25, pp. 1804–1807, Dec. 1982, doi: 10.1103/physrevlett.49.1804.
- [Arute 2019] F. Arute et al., “Quantum supremacy using a programmable superconducting processor,” *Nature*, vol. 574, no. 7779, pp. 505–510, Oct. 2019, doi: 10.1038/s41586-019-1666-5.
- [Bayerstadler 2021] A. Bayerstadler et al., “Industry quantum computing applications,” *EPJ Quantum Technology*, vol. 8, no. 1, Nov. 2021, doi: 10.1140/epjqt/s40507-021-00114-x.
- [BB 1948] J. Bardeen and W. H. Brattain, “The Transistor, a Semi-Conductor triode,” *Physical Review*, vol. 74, no. 2, pp. 230–231, Jul. 1948, doi: 10.1103/physrev.74.230.
- [BB 1984] C. H. Bennett and G. Brassard, “Quantum Cryptography: Public Key Distribution and Coin Flipping,” in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, India, 1984.
- [BBM 1992] C. H. Bennett, G. Brassard, and N. D. Mermin, “Quantum cryptography without Bell’s theorem,” *Phys. Rev. Lett.*, vol. 68, no. 5, pp. 557–559, Feb. 1992, doi: 10.1103/PhysRevLett.68.557.
- [BCP 2014] T. Baumgratz, M. Cramer, and M. B. Plenio, “Quantifying Coherence,” *Physical Review Letters*, vol. 113, no. 14, p. 140401, Sep. 2014. doi: 10.1103/PhysRevLett.113.140401.
- [BCS 1957] J. Bardeen, L. N. Cooper, and J. R. Schrieffer, “Theory of superconductivity,” *Physical Review*, vol. 108, no. 5, pp. 1175–1204, Dec. 1957, doi: 10.1103/physrev.108.1175.
- [Bell 1964] J. S. Bell, “On the Einstein Podolsky Rosen paradox,” *Physics Physique Fizika*, vol. 1, no. 3, pp. 195–200, Nov. 1964, doi:

- 10.1103/physicsphysiquefizika.1.195.
- [Benioff 1980] P. Benioff, “The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines,” *Journal of Statistical Physics*, vol. 22, no. 5, pp. 563–591, May 1980, doi: 10.1007/BF01011339.
- [Bennet 1992] C. H. Bennett, “Quantum cryptography using any two nonorthogonal states,” *Phys. Rev. Lett.*, vol. 68, no. 21, pp. 3121–3124, May 1992, doi: 10.1103/PhysRevLett.68.3121.
- [Bennet 1993] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, “Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels,” *Physical Review Letters*, vol. 70, no. 13, pp. 1895–1899, Mar. 29, 1993, doi: 10.1103/PhysRevLett.70.1895.
- [BFK 2009] A. Broadbent, J. Fitzsimons, and E. Kashefi, “Universal blind quantum computation,” *arXiv preprint arXiv:0807.4154*, 2009. doi: 10.48550/arXiv.0807.4154.
- [BFNV 2018] A. Bouland, B. Fefferman, C. Nirkhe, and U. Vazirani, “On the complexity and verification of quantum random circuit sampling,” *Nature Physics*, vol. 15, no. 2, pp. 159–163, Oct. 2018, doi: 10.1038/s41567-018-0318-2.
- [BHP 1946] F. Bloch, W. W. Hansen, and M. Packard, “The nuclear induction experiment,” *Physical Review*, vol. 70, no. 7–8, pp. 474–485, Oct. 1946, doi: 10.1103/physrev.70.474.
- [Biamonte 2017] J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe, and S. Lloyd, “Quantum machine learning,” *Nature*, vol. 549, no. 7671, pp. 195–202, Sep. 2017, doi: 10.1038/nature23474.
- [Biswas 2025] H. Biswas, “Power Networks SCADA Communication Cybersecurity, A Qiskit Implementation,” *arXiv:2503.20365 [quant-ph]*, Mar. 2025. doi: 10.48550/arXiv.2503.20365
- [BOE 2007] Jefatura del Estado, “Ley 53/2007, de 28 de diciembre, sobre el control del comercio exterior de material de defensa y de doble uso.” *Boletín Oficial del Estado*, no. 312, 29 dic. 2007. [En línea]. Disponible en: <https://www.boe.es/eli/es/l/2007/12/28/53/con>
- [BOE 2014] Ministerio de la Presidencia, “Real Decreto 679/2014, de 1 de agosto, por el que se aprueba el Reglamento de control del comercio exterior de material de defensa, de otro material y de productos y tecnologías de doble uso.” *Boletín Oficial del Estado*, no. 207, sec. I, pp. 68148–68300, 26 ago. 2014. [En línea]. Disponible en: <https://www.boe.es/eli/es/rd/2014/08/01/679>
- [BOE 2025] Ministerio de la Presidencia, Justicia y Relaciones con las Cortes, “Orden PJC/809/2025, de 23 de julio, por la que se publica el Acuerdo del Consejo de Ministros de 24 de junio de 2025, por el que se crea el Comité Nacional de Seguridad y Soberanía Tecnológica, se establece su composición y funcionamiento, y se regula su Consejo Asesor.” *Boletín Oficial del Estado*, no. 178, sec. III, pp. 100360–100365, 25 jul. 2025. [En línea]. Disponible en:

<https://www.boe.es/eli/es/o/2025/07/23/pjc809>

- [Born 1926] M. Born, “Zur Quantenmechanik der Stoßvorgänge,” *The European Physical Journal A*, vol. 37, no. 12, pp. 863–867, Dec. 1926, doi: 10.1007/bf01397477
- [BR 1983] G. Binnig and H. Rohrer, “Scanning tunneling microscopy,” *Surface Science*, vol. 126, no. 1–3, pp. 236–244, Mar. 1983, doi: 10.1016/0039-6028(83)90716-1.
- [Brewer 2019] S. M. Brewer et al., “Al⁺27 Quantum-Logic Clock with a Systematic Uncertainty below 10,” *Physical Review Letters*, vol. 123, no. 3, Jul. 2019, doi: 10.1103/physrevlett.123.033201.
- [BT 1992] T. Bresnahan and M. Trajtenberg, “General purpose technologies “Engines of growth?,”” Aug. 1992. doi: 10.3386/w4148.
- [Broglie 1924] L. De Broglie, “XXXV. A tentative theory of light quanta,” *The London Edinburgh and Dublin Philosophical Magazine and Journal of Science*, vol. 47, no. 278, pp. 446–458, Feb. 1924, doi: 10.1080/14786442408634378.
- [Bruyn 1997] R. De Bruyn Ouboter, “Heike Kamerlingh Onnes’s Discovery of Superconductivity,” *Scientific American*, vol. 276, no. 3, pp. 98–103, Mar. 1997, [En línea]. Disponible en: <https://www.jstor.org/stable/24993663>
- [CBSNG 2019] A. W. Cross, L. S. Bishop, S. Sheldon, P. D. Nation, and J. M. Gambetta, “Validating quantum computers using randomized model circuits,” *Physical Review. A/Physical Review, A*, vol. 100, no. 3, Sep. 2019, doi: 10.1103/physreva.100.032328.
- [CE 2004] Comisión Europea, “Libro verde: Los contratos públicos de defensa,” COM(2004)608 final, 23 Sep. 2004. [En línea]. Disponible en: <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2004:0608:FIN:ES:PDF>
- [CE 2016] Comisión Europea, “Comunicación de la Comisión al Parlamento Europeo, al Consejo Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: Plan de Acción Europeo de la Defensa,” COM(2016) 950 final, 30 nov. 2016. [En línea]. Disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:52016DC0950>
- [CE 2022] Comisión Europea, “Comunicación de la Comisión al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: Hoja de ruta sobre tecnologías críticas para la seguridad y la defensa,” COM(2022) 61 final, 15 Feb. 2022. [En línea]. Disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52022DC0061>
- [CE 2023] Comisión Europea, “Recomendación (UE) 2023/2113 de la Comisión, de 3 de octubre de 2023, sobre ámbitos tecnológicos críticos para la seguridad económica de la UE con vistas a realizar evaluaciones de riesgos adicionales conjuntamente con los Estados miembros,” 2023/2113, 3 Oct. 2023. [En línea]. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:L_202302113
- [CE 2023_2] Parlamento y Consejo Europeos, “Reglamento (UE) 2023/1781 del

Parlamento Europeo y del Consejo de 13 de septiembre de 2023 por el que se establece un marco de medidas para reforzar el ecosistema europeo de semiconductores y por el que se modifica el Reglamento (UE) 2021/694 (Reglamento de chips),” 2023/1781, 13 Sep. 2023. [En línea]. <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32023R1781&qid=1760215187922>

- [CE 2024] Comisión Europea y Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad, “Comunicación Conjunta al Parlamento Europeo, al Consejo, al Comité Económico y Social Europeo y al Comité de las Regiones: Estrategia para una Europa Cuántica: Una nueva Estrategia Industrial de Defensa Europea: lograr la preparación en materia de defensa de la UE a través de una industria de defensa europea resiliente y con capacidad de respuesta,” JOIN/2024/10 final, 5 mar. 2024. [En línea]. Disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A52024JC0010&qid=1757200201531>
- [CE 2024_2] Comisión Europea, “Recomendación (UE) 2024/1101 de la Comisión, de 11 de abril de 2024, sobre una hoja de ruta para llevar a cabo de manera coordinada la transición hacia una criptografía postcuántica,” 2024/1101, 11 Abr. 2024. [En línea]. https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:L_202401101
- [CE 2025] Comisión Europea, “Libro Blanco Conjunto. Preparación en materia de defensa europea 2030,” Diario Oficial de la Unión Europea, JOIN(2025) 120 final, 19 mar. 2025. [En línea]. Disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52025JC0120>
- [CE 2025_2] Comisión Europea, “Comunicación de la Comisión al Parlamento Europeo y al Consejo: Estrategia para una Europa Cuántica: una Europa cuántica en un mundo cambiante,” Diario Oficial de la Unión Europea, COM(2025) 363 final, 2 jul. 2025. [En línea]. Disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A52025DC0363>
- [CGK 1998] I. L. Chuang, L. M. K. Vandersypen, X. Zhou, D. W. Leung, and S. Lloyd, “Experimental realization of a quantum algorithm,” *Nature*, vol. 393, pp. 143–146, 1998. doi: 10.1038/30181
- [CGM 2025] A. Ciacco, F. Guerriero, and G. Macrina, “Review of quantum algorithms for medicine, finance and logistics,” *Soft Computing*, Feb. 2025, doi: 10.1007/s00500-025-10540-z.
- [Chen 2018] Z.-Y. Chen, Q. Zhou, C. Xue, X. Yang, G.-C. Guo, and G.-P. Guo, “64-qubit quantum circuit simulation,” *Science Bulletin*, vol. 63, no. 15, pp. 964–971, Jun. 2018, doi: 10.1016/j.scib.2018.06.007.
- [Clapp 2022] S. Clapp, “Emerging disruptive technologies in defence,” *European Parliament*, PE 733.647, Sep. 2022. [En línea]. Disponible en: [https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/733647/EPRS_ATA\(2022\)733647_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/733647/EPRS_ATA(2022)733647_EN.pdf)
- [Classic 2024] Classiq Technologies, “Quantum Approximate Optimization Algorithm (QAOA),” Classiq, 22-feb-2024. [En línea]. Disponible en:

<https://www.classiq.io/algorithms/quantum-approximate-optimization-algorithm-qaoa>

- [Deutsch 1985] D. Deutsch, “Quantum theory, the Church-Turing principle and the universal quantum computer,” *Proc. R. Soc. London A*, vol. 400, no. 1818, pp. 97–117, 1985, doi: 10.1098/rspa.1985.0070.
- [DG 1927] C. Davisson and L. H. Germer, “Diffraction of electrons by a crystal of nickel,” *Physical Review*, vol. 30, no. 6, pp. 705–740, Dec. 1927, doi: 10.1103/PhysRev.30.705.
- [Dirac 1927] P. A. M. Dirac, “The quantum theory of the emission and absorption of radiation,” *Proceedings of the Royal Society of London Series a Containing Papers of a Mathematical and Physical Character*, vol. 114, no. 767, pp. 243–265, Mar. 1927, doi: 10.1098/rspa.1927.0039.
- [Dirac 1928] P. A. M. Dirac, “The quantum theory of the electron,” *Proceedings of the Royal Society of London Series a Containing Papers of a Mathematical and Physical Character*, vol. 117, no. 778, pp. 610–624, Feb. 1928, doi: 10.1098/rspa.1928.0023.
- [DJG 2011] I. F. De Lucio, J. V. Jurado, and A. G. Gracia, “Ciencia e Innovación. Una relación compleja y evolutiva,” *Arbor*, vol. 187, no. 752, pp. 1077–1089, Dec. 2011, doi: 10.3989/arbor.2011.752n6005
- [Einstein 1917] A. Einstein, “Zur Quantentheorie der Strahlung,” *Physikalische Zeitschrift*, vol. 18, pp. 121–128, 1917.
- [Ekert 1991] A. K. Ekert, “Quantum cryptography based on Bell’s theorem,” *Physical Review Letters*, vol. 67, no. 6, pp. 661–663, Aug. 1991.
- [EP 1955] L. Essen and J. V. L. Parry, “An atomic standard of frequency and time interval: a caesium resonator,” *Nature*, vol. 176, no. 4476, pp. 280–282, Aug. 1955, doi: 10.1038/176280a0.
- [EPR 1935] A. Einstein, B. Podolsky, and N. Rosen, “Can Quantum-Mechanical description of physical reality be considered complete?,” *Physical Review*, vol. 47, no. 10, pp. 777–780, May 1935, doi: 10.1103/physrev.47.777.
- [Feynman 1982] R. P. Feynman, “Simulating physics with computers,” *International Journal of Theoretical Physics*, vol. 21, no. 6–7, pp. 467–488, Jun. 1982, doi: 10.1007/bf02650179.
- [FGCSIC 2025] Fundación General CSIC, “De bits a qubits: Radiografía de la Innovación Cuántica,” Unidad de Vigilancia Estratégica de la FGCSIC, 2025. [En línea]. Disponible en: https://fgcsic.es/wp-content/uploads/2025/04/FGCSIC_Informe_VT_Tecnologias_Cuanticas.pdf
- [FJP 2009] W. A. Fedak and J. J. Prentis, “The 1925 Born and Jordan paper “On quantum mechanics,”” *American Journal of Physics*, vol. 77, no. 2, pp. 128–139, Jan. 2009, doi: 10.1119/1.3009634.
- [FKTH 2025] T. Fellner, D. Kreplin, S. Tovey, y C. Holm, “Quantum vs. classical: A comprehensive benchmark study for predicting time series with variational

- quantum machine learning,” arXiv:2504.12416v1 [quant-ph], 16 Apr. 2025.
- [GHZ 2007] D. M. Greenberger, M. A. Horne, and A. Zeilinger, “Going beyond Bell’s theorem,” arXiv:0712.0921 [quant-ph], Dec. 2007, doi: 10.48550/arXiv.0712.0921.
- [GPB 2023] C. Grange, M. Poss, y E. Bourreau, “An introduction to variational quantum algorithms for combinatorial optimization problems,” 4OR, vol. 21, pp. 363–403, 2023. [En línea]. Disponible en: <https://arxiv.org/abs/2212.11734>. doi: 10.1007/s10288-023-00549-1
- [GZT 1955] J. P. Gordon, H. J. Zeiger, and C. H. Townes, “The Maser—New type of microwave amplifier, frequency standard, and spectrometer,” Physical Review, vol. 99, no. 4, pp. 1264–1274, Aug. 1955, doi: 10.1103/physrev.99.1264.
- [Haaf 2024] S. L. D. T. Haaf et al., “A two-site Kitaev chain in a two-dimensional electron gas,” Nature, vol. 630, no. 8016, pp. 329–334, Jun. 2024, doi: 10.1038/s41586-024-07434-9.
- [Hall 1962] R. N. Hall, G. E. Fenner, J. D. Kingsley, T. J. Soltys, and R. O. Carlson, “Coherent light emission from GAAS junctions,” Physical Review Letters, vol. 9, no. 9, pp. 366–368, Nov. 1962, doi: 10.1103/physrevlett.9.366.
- [Hashim 2025] A. Hashim, L. B. Nguyen, N. Goss, B. Marinelli, R. K. Naik, T. Chistolini, J. Hines, J. P. Marceaux, Y. Kim, P. Gokhale, T. Tomesh, S. Chen, L. Jiang, S. Ferracin, K. Rudinger, T. Proctor, K. C. Young, I. Siddiqi, and R. Blume-Kohout, “Practical Introduction to Benchmarking and Characterization of Quantum Computers,” PRX Quantum, vol. 6, no. 3, p. 030202, Aug. 2025, doi: 10.1103/PRXQuantum.6.030202.
- [Héder 2017] M. Héder, “From NASA to EU: the evolution of the TRL scale in Public Sector Innovation,” The Innovation Journal, vol. 22, no. 2, pp. 1-23, 2017, ISSN 1715-3816, https://eprints.sztaki.hu/9204/1/Heder_1_3269345_ny.pdf
- [Heisenberg 1927] W. Heisenberg, “Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik,” The European Physical Journal A, vol. 43, no. 3–4, pp. 172–198, Mar. 1927, doi: 10.1007/bf01397280.
- [HHL 2009] A. W. Harrow, A. Hassidim, and S. Lloyd, “Quantum algorithm for solving linear systems of equations,” Physical Review Letters, vol. 103, no. 15, p. 150502, Oct. 2009, doi: 10.1103/PhysRevLett.103.150502.
- [Hidary 2019] J. D. Hidary, Quantum Computing: an Applied Approach. Springer Cham, 2019. doi: 10.1007/978-3-030-23922-0.
- [Hinkley 2013] N. Hinkley et al., “An Atomic Clock with 10^{-18} Instability,” Science, vol. 341, no. 6151, pp. 1215–1218, Aug. 2013, doi: 10.1126/science.1240420.
- [Hwang 2003] W.-Y. Hwang, “Quantum key distribution with high loss: Toward global secure communication,” Physical Review Letters, vol. 91, p. 057901, 2003, doi: 10.1103/PhysRevLett.91.057901.
- [ITUT 2019] ITU-T, “Quantum noise random number generator architecture,”

- Recommendation ITU-T X.1702, Nov. 2019. Disponible en: https://www.itu.int/rec/dologin_pub.asp?lang=s&id=T-REC-X.1702-201911-I!!PDF-E&type=items
- [ITUT 2020] ITU-T, “Security framework for quantum key distribution networks,” Recommendation ITU-T X.1710, Oct. 2020. Disponible en: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1710-202010-I!!PDF-E&type=items
- [ITUT 2020_2] ITU-T, “Key combination and confidential key supply for quantum key distribution networks,” Recommendation ITU-T X.1714, Oct. 2020. Disponible en: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-X.1714-202010-I!!PDF-E&type=items
- [JNTM 2014] P. Jouzdani, E. Novais, I. S. Tupitsyn, and E. R. Mucciolo, “Fidelity threshold of the surface code beyond single-qubit error models,” *Physical Review A*, vol. 90, no. 4, Oct. 2014, doi: 10.1103/physreva.90.042315.
- [Josephson 1962] B. D. Josephson, “Possible new effects in superconductive tunnelling,” *Physics Letters*, vol. 1, no. 7, pp. 251–253, Jul. 1962, doi: 10.1016/0031-9163(62)91369-0.
- [Kastler 1950] A. Kastler, “Quelques suggestions concernant la production optique et la détection optique d’une inégalité de population des niveaux de quantification spatiale des atomes. Application à l’expérience de Stern et Gerlach et à la résonance magnétique,” *Journal De Physique*, vol. 11, no. 6, pp. 255–265, Jan. 1950, doi: 10.1051/jphysrad:01950001106025500.
- [Kimble 2008] H. J. Kimble, “The quantum internet,” *Nature*, vol. 453, pp. 1023–1030, Jun. 2008, doi: 10.1038/nature07127
- [KKM 1970] F. P. Kapron, D. B. Keck, and R. D. Maurer, “Radiation Losses in Glass Optical Waveguides,” *Applied Physics Letters*, vol. 17, no. 10, pp. 423–425, Nov. 1970, doi: 10.1063/1.1653255.
- [King 2025] A. D. King et al., “Beyond-classical computation in quantum simulation,” *Science*, Mar. 2025, doi: 10.1126/science.ado6285.
- [Kitching 2018] J. Kitching, “Chip-scale atomic devices,” *Applied Physics Reviews*, vol. 5, no. 3, p. 031302, Aug. 2018, doi: 10.1063/1.5026238.
- [Kittel 1995] C. Kittel, *Introduction to Solid State Physics*, 7th edition. John Wiley & Sons, 1995. ISBN-13 978-0471111818
- [Kragh 2022] H. Kragh, Ed., *Niels Bohr: On the constitution of atoms and molecules*. Birkhäuser Cham, 2022. doi: 10.1007/978-3-030-97664-4.
- [Krelina 2021] M. Krelina, “Quantum technology for military applications,” *EPJ Quantum Technology*, vol. 8, no. 1, Nov. 2021, doi: 10.1140/epjqt/s40507-021-00113-y.
- [Krelina 2025_1] M. Krelina, “An introduction to military quantum technology for policymakers,” Mar. 2025. doi: 10.55163/drdq1599.

- [Krelina 2025_2] M. Krelina, “Military and security dimensions of quantum technologies: A primer,” Jul. 2025. doi: 10.55163/zvttl1529.
- [Ladd 2010] T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe, and J. L. O’Brien, “Quantum computers,” *Nature*, vol. 464, no. 7285, pp. 45–53, 2010. doi: 10.1038/nature08812.
- [Latorre 2017] J. I. Latorre Sentís, *Cuántica: Tu futuro en juego*. Editorial Ariel, 2017. ISBN-13 978-8434425392
- [Lauterbur 1973] P. C. Lauterbur, “Image formation by induced local interactions: Examples employing nuclear magnetic resonance,” *Nature*, vol. 242, no. 5394, pp. 190–191, Mar. 1973, doi: 10.1038/242190a0.
- [LCQ 2012] H.-K. Lo, M. Curty and B. Qi, “Measurement-device-independent quantum key distribution,” *Physical Review Letters*, vol. 108, p. 130503, 2012, doi: 10.1103/PhysRevLett.108.130503.
- [Liao 2017] S.-K. Liao et al., “Satellite-to-ground quantum key distribution,” *Nature*, vol. 549, pp. 43–47, 2017, doi: 10.1038/nature23655.
- [Liao 2018] S.-K. Liao et al., “Satellite-relayed intercontinental quantum network,” *Physical Review Letters*, vol. 120, no. 3, p. 030501, 2018, doi: 10.1103/PhysRevLett.120.030501.
- [Lombardi 2017] M. A. Lombardi, “A Historical Review of U.S. Contributions to the Atomic Redefinition of the SI Second in 1967,” *Journal of Research of the National Institute of Standards and Technology*, vol. 122, Jun. 2017, doi: 10.6028/jres.122.029.
- [LPTRG 2013] C. C. W. Lim, C. Portmann, M. Tomamichel, R. Renner, and N. Gisin, “Device-Independent Quantum Key Distribution with Local Bell Test,” *Physical Review X*, vol. 3, no. 3, p. 031006, Jul. 2013. doi:10.1103/PhysRevX.3.031006
- [LYDS 2018] M. Lucamarini, Z. Yuan, J. F. Dynes y A. J. Shields, “Overcoming the rate–distance limit of quantum key distribution without quantum repeaters,” *Nature*, vol. 557, pp. 400–403, 2018. [En línea]. Disponible en: <https://www.nature.com/articles/s41586-018-0066-6>
- [Maiman 1960] T. H. Maiman, “Stimulated optical radiation in Ruby,” *Nature*, vol. 187, no. 4736, pp. 493–494, Aug. 1960, doi: 10.1038/187493a0.
- [Majorana 1937] E. Majorana, “Teoria simmetrica dell’elettrone e del positrone,” *Il Nuovo Cimento*, vol. 14, pp. 171–184, 1937.
- [Mankins 2009] J. C. Mankins, “Technology readiness assessments: A retrospective,” *Acta Astronautica*, vol. 65, no. 9–10, pp. 1216–1223, Apr. 2009, doi: 10.1016/j.actaastro.2009.03.058.
- [Mansfield 1977] P. Mansfield, “Multi-planar image formation using NMR spin echoes,” *Journal of Physics C Solid State Physics*, vol. 10, no. 3, pp. L55–L58, Feb. 1977, doi: 10.1088/0022-3719/10/3/004.

- [Matteo 2025] O. Di Matteo, “Quantum volume,” PennyLane Demos, Jul. 11, 2025. https://pennylane.ai/qml/demos/quantum_volume
- [MERICS 2024] J. Groenewegen-Lau and A. Hmadi, “MERICS China Tech Observatory Quantum Report 2024,” Mercator Institute for China Studies (MERICS), Dec. 2024. [En línea]. Disponible en: <https://merics.org/sites/default/files/2024-12/MERICS%20China%20Tech%20Observatory%20Quantum%20Report%202024.pdf>
- [Miller 2016] J. L. Miller, “Three groups close the loopholes in tests of Bell’s theorem,” Physics Today, Jan. 2016, doi: 10.1063/PT.3.3039.
- [MIT 2025] Ruane, J., Kiesow, E., Galatsanos, J., Dukatz, C., Blomquist, E., Shukla, P., “The Quantum Index Report 2025”, MIT Initiative on the Digital Economy, Massachusetts Institute of Technology, Cambridge, MA, May 2025.
- [MKG 2024] P. Malhotra, A. Kumar, and S. Garhwal, “A Systematic Review of Quantum BenchMarking,” International Journal of Theoretical Physics, vol. 63, no. 11, Oct. 2024, doi: 10.1007/s10773-024-05811-8.
- [MO 1933] W. Meissner and R. Ochsenfeld, “Ein neuer Effekt bei Eintritt der Supraleitfähigkeit,” The Science of Nature, vol. 21, no. 44, pp. 787–788, Nov. 1933, doi: 10.1007/bf01504252.
- [MPBP 2022] A. G. Mountogiannakis, P. Papanastasiou, B. Braverman, y S. Pirandola, “Composably secure data processing for Gaussian-modulated continuous-variable quantum key distribution,” Physical Review Research, vol. 4, no. 1, p. 013099, Feb. 2022, doi: 10.1103/PhysRevResearch.4.013099.
- [Mullane 2020] S. Mullane, “Sampling random quantum circuits: a pedestrian’s guide,” alphaXiv, Jul. 2020, [En línea]. Disponible en: <https://www.alphaxiv.org/es/overview/2007.07872v1>
- [Mur 2024] J.-M. Mur, Redes de fibra óptica: Conceptos fundamentales. Ediciones ENI, 2024. ISBN 978-2-409-04726-8
- [Nathan 1962] M. I. Nathan, W. P. Dumke, G. Burns, F. H. Dill, and G. Lasher, “Stimulated Emission of Radiation from Gaas P-N Junctions,” Applied Physics Letters, vol. 1, no. 3, pp. 62–64, Nov. 1962, doi: 10.1063/1.1777371.
- [NATO 2022] North Atlantic Treaty Organization (NATO), “NATO 2022 Strategic Concept,” Jun. 2022. [En línea]. <https://www.nato.int/content/dam/nato/webready/documents/publications-and-reports/strategic-concepts/2022/290622-strategic-concept.pdf>
- [NC 2010] M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information. Cambridge, UK: Cambridge University Press, 2010. doi: 10.1017/CBO9780511976667.
- [Neumann 1932] J. von Neumann, Mathematical Foundations of Quantum Mechanics. Princeton, NJ, USA: Princeton University Press, Oct. 1996. ISBN 0691028931.

- [NIS 2025] NIS Cooperation Group, “A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography,” Part 1, Version: 1.1, EU PQC Workstream, 11 Jun. 2025. [En línea]. Disponible en: <https://ec.europa.eu/newsroom/dae/redirection/document/117507>
- [NIST 2018] M. S. Turan, E. Barker, J. Kelsey, K. A. McKay, M. L. Baish, and M. Boyle, Recommendation for the Entropy Sources Used for Random Bit Generation, NIST Special Publication 800-90B, Jan. 2018. doi: 10.6028/NIST.SP.800-90B.
- [NPT 1999] Y. Nakamura, Yu. A. Pashkin, and J. S. Tsai, “Coherent control of macroscopic quantum states in a single-Cooper-pair box,” *Nature*, vol. 398, pp. 786–788, 1999. doi: 10.1038/19718
- [OSEA 2025] Office of Systems Engineering and Architecture, Technology Readiness Assessment Guidebook. Office of the Under Secretary of Defense for Research and Engineering, 2025. [Digital version]. Disponible en: <https://www.cto.mil/wp-content/uploads/2025/03/TRA-Guide-Feb2025-Cleared.pdf>
- [Pan 2025] B. Pan, “Hybrid Quantum-Classical Computing for Physical Problems: Architectures, Algorithms, and Applications in the Networked Era,” *Journal of Network Computing and Applications*, vol. 10, no. 1, pp. 70–80, 2025. DOI: 10.23977/jnca.2025.100109.
- [PECUE 2009] Parlamento Europeo y Consejo de la Unión Europea, “Directiva 2009/81/CE del Parlamento Europeo y del Consejo, de 13 de julio de 2009, sobre coordinación de los procedimientos de adjudicación de determinados contratos de obras, de suministro y de servicios en los ámbitos de la defensa y la seguridad, y por la que se modifican las Directivas 2004/17/CE y 2004/18/CE,” *Diario Oficial de la Unión Europea*, L 216, pp. 76–136, 20 ago. 2009. [En línea]. Disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32009L0081>
- [PECUE 2021] Parlamento Europeo y Consejo de la Unión Europea, “Reglamento (UE) 2021/821 del Parlamento Europeo y del Consejo de 20 de mayo de 2021 por el que se establece un régimen de la Unión de control de las exportaciones, el corretaje, la asistencia técnica, el tránsito y la transferencia de productos de doble uso (versión refundida),” *Diario Oficial de la Unión Europea*, L 206, pp. 1–119, 11 jun. 2021. [En línea]. Disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32021R0821>
- [Planck 1900] M. Planck, “Zur Theorie des Gesetzes der Energieverteilung im Normalspektrum,” *Verhandl. Dtsch. phys. Ges.* 2 (1900) 237.
- [Preskill 2018] J. Preskill, “Quantum Computing in the NISQ era and beyond,” *Quantum*, vol. 2, p. 79, Aug. 2018, doi: 10.22331/q-2018-08-06-79.
- [PTP 1946] E. M. Purcell, H. C. Torrey, and R. V. Pound, “Resonance absorption by nuclear magnetic moments in a solid,” *Physical Review*, vol. 69, no. 1–2, pp. 37–38, Jan. 1946, doi: 10.1103/physrev.69.37.
- [Rattew 2024] A. G. Rattew, “Quantum Approximate Optimization Algorithm: A Short

- Survey,” arXiv:2406.02666 [quant-ph], Jun. 4, 2024. [En línea]. Disponible en: <https://arxiv.org/abs/2406.02666>
- [RK 1932] M. Knoll and E. Ruska, “Das Elektronenmikroskop,” The European Physical Journal A, vol. 78, no. 5–6, pp. 318–339, May 1932, doi: 10.1007/bf01342199.
- [Ron 2025] J. M. S. Ron, Historia de la física cuántica. Volumen I: El periodo fundacional: Origen y desarrollo de la cuantización de Planck (1860-1924). Editorial Crítica, 2025. ISBN-13 978-8491997252
- [Ron 2025_2] J. M. S. Ron, Historia de la física cuántica. Volumen II: La creación e interpretación de la mecánica cuántica: De Heisenberg al gato de Schrödinger (1925-1935). Editorial Crítica, 2025. ISBN-13 978-8491997795
- [Rosenband 2008] T. Rosenband et al., “Frequency ratio of AL + and HG + Single-Ion optical clocks; metrology at the 17th decimal place,” Science, vol. 319, no. 5871, pp. 1808–1812, Mar. 2008, doi: 10.1126/science.1154622.
- [RZMK 1938] I. I. Rabi, J. R. Zacharias, S. Millman, and P. Kusch, “A new method of measuring nuclear magnetic moment,” Physical Review, vol. 53, no. 4, p. 318, Feb. 1938, doi: 10.1103/physrev.53.318.
- [Saenz 2000] J. F. Saenz, “Evolución del sistema ciencia, tecnología e industria en el mundo y en la UE,” Lull: Revista de la Sociedad Española de Historia de las Ciencias y de las Técnicas, vol. 23, no. 47, pp. 399–430, 2000. [En línea]. Disponible en: <https://dialnet.unirioja.es/download/articulo/62252.pdf>
- [SARG 2004] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, “Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations,” Phys. Rev. Lett., vol. 92, no. 5, p. 057901, Feb. 2004, doi: 10.1103/PhysRevLett.92.057901.
- [SB 2024] R. Singh and R. M. Bodile, “A Quick Guide to Quantum Communication,” arXiv preprint arXiv:2402.15707, Feb. 2024. [En línea]. Disponible en: <https://doi.org/10.48550/arXiv.2402.15707>
- [Scarani 2009] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus and M. Peev, “The security of practical quantum key distribution,” Reviews of Modern Physics, vol. 81, no. 3, pp. 1301–1350, 2009, doi: 10.1103/RevModPhys.81.1301.
- [Schrödinger 1926] E. Schrödinger, “An undulatory theory of the mechanics of atoms and molecules,” Physical Review, vol. 28, no. 6, pp. 1049–1070, Dec. 1926, doi: 10.1103/physrev.28.1049.
- [Schrödinger 1935] E. Schrödinger, “Die gegenwärtige Situation in der Quantenmechanik,” The Science of Nature, vol. 23, no. 48, pp. 807–812, Nov. 1935, doi: 10.1007/bf01491891.
- [Schumacher 1995] B. Schumacher, “Quantum coding,” Physical Review A, vol. 51, no. 4, pp. 2738–2747, Apr. 1995, doi: 10.1103/physreva.51.2738.
- [SEEAA 2025] H. Soubra, H. Elsayed, Y. Elbrolosy, Y. Adel, and Z. Attia, “Comprehensive

- review of metrics and measurements of quantum systems,” *Metrics*, vol. 2, no. 2, p. 9, Jun. 2025, doi: 10.3390/metrics2020009.
- [Segal 2015] J. Segal, “The notion of information in biology, an appraisal,” *BIO Web of Conferences*, vol. 4, p. 00017, jan. 2015, doi: 10.1051/bioconf/20150400017.
- [SGUHF 2022] M. Stanley, Y. Gui, D. Unnikrishnan, S. R. G. Hall and I. Fatadin, “Recent progress in quantum key distribution network deployments and standards,” *Journal of Physics: Conference Series*, vol. 2416, no. 1, p. 012001, 2022, doi: 10.1088/1742-6596/2416/1/012001.
- [Shannon 1948] C. E. Shannon, “A mathematical theory of communication,” *Bell System Technical Journal*, vol. 27, no. 3, pp. 379–423, Jul. 1948, doi: 10.1002/j.1538-7305.1948.tb01338.x.
- [Shor 1999] P. W. Shor, “Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,” *SIAM Rev.*, vol. 41, no. 2, pp. 303–332, 1999, doi: 10.1137/S0036144598347011.
- [SI 2020] IDC and Seagate, “Rethink Data: Put More of Your Business Data to Work,” Seagate Technology, 2020. [En línea]. Disponible en: <https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf>
- [SSDBA 2015] A. Streltsov, U. Singh, H. S. Dhar, M. N. Bera, and G. Adesso, “Measuring Quantum Coherence with Entanglement,” *Physical Review Letters*, vol. 115, no. 2, pp. 020403, Jul. 2015. [En línea]. Disponible en: <https://doi.org/10.1103/PhysRevLett.115.020403>
- [TBP 2024] M. Taddeo, A. Blanchard, and K. Pundyk, “Consider the ethical impacts of quantum technologies in defence — before it’s too late,” *Nature*, vol. 634, no. 8035, pp. 779–781, Oct. 2024, doi: 10.1038/d41586-024-03376-4.
- [Thomson 1928] G.P. Thomson, “Experiments on the diffraction of cathode rays,” *Proceedings of the Royal Society A*, vol. 117, no. 778, pp. 600–609, 1928, <https://doi.org/10.1098/rspa.1928.0022>
- [UE 2010] Unión Europea, “Versiones consolidadas del Tratado de la Unión Europea y del Tratado de Funcionamiento de la Unión Europea,” 2010/C 083/01, Mar. 2010. doi: 10.3000/1725244X.C_2010.083.spa.
- [USC 2018] U.S. Congress, “National Quantum Initiative Act,” Public Law No. 115–368, 21 Dec. 2018. [En línea]. Disponible en: <https://www.congress.gov/bill/115th-congress/house-bill/6227/text>
- [USC 2024] U.S. Congress, “H.R.7935 – Defense Quantum Acceleration Act of 2024,” 118th Congress, Introduced in House, Apr. 10, 2024. [En línea]. Disponible en: <https://www.congress.gov/bill/118th-congress/house-bill/7935/text>
- [Wack 2021] A. Wack et al., “Quality, Speed, and Scale: three key attributes to measure the performance of near-term quantum computers,” *arXiv (Cornell University)*, Jan. 2021, doi: 10.48550/arxiv.2110.14108.
- [Wang 2005] X.-B. Wang, “Beating the photon-number-splitting attack in practical

- quantum cryptography,” *Physical Review Letters*, vol. 94, p. 230503, 2005, doi: 10.1103/PhysRevLett.94.230503.
- [WEH 2018] S. Wehner, D. Elkouss, and R. Hanson, “Quantum internet: A vision for the road ahead,” *Science*, vol. 362, no. 6412, p. eaam9288, Nov. 2018, doi: 10.1126/science.aam9288.
- [Wilde 2021] M. M. Wilde, “Quantum Information Theory,” 2nd ed., Cambridge University Press, Baton Rouge, Louisiana, USA, Dec. 2021, [En línea]. Disponible en: <https://www.markwilde.com/git-notes.pdf>
- [Wong 2022] T. G. Wong, “Introduction to Classical and Quantum Computing,” Rooted Grove, Omaha, Nebraska, 2022. [En línea]. Disponible: <https://www.thomaswong.net/introduction-to-classical-and-quantum-computing-1e4p.pdf>
- [Woodward 2021] R. I. Woodward, Y. S. Lo, M. Pittaluga, M. Minder, T. K. Paraíso, M. Lucamarini, Z. L. Yuan, y A. J. Shields, “Gigahertz measurement-device-independent quantum key distribution using directly modulated lasers,” *npj Quantum Information*, vol. 7, art. 58, 2021. [En línea]. Disponible en: <https://www.nature.com/articles/s41534-021-00394-2>
- [Zhang 2018] H. Zhang et al., “RETRACTED ARTICLE: Quantized Majorana conductance,” *Nature*, vol. 556, no. 7699, pp. 74–79, Mar. 2018, doi: 10.1038/nature26142.
- [Zhu 2021] Q. Zhu, S. Cao, F. Chen, M.-C. Chen, X. Chen, T.-H. Chung, H. Deng, Y. Du, D. Fan, M. Gong, C. Guo, C. Guo, S. Guo, L. Han, L. Hong, H.-L. Huang, Y.-H. Huo, L. Li, N. Li, S. Li, Y. Li, F. Liang, C. Lin, J. Lin, H. Qian, D. Qiao, H. Rong, H. Su, L. Sun, L. Wang, S. Wang, D. Wu, Y. Wu, Y. Xu, K. Yan, W. Yang, Y. Yang, Y. Ye, J. Yin, C. Ying, J. Yu, C. Zha, C. Zhang, H. Zhang, K. Zhang, Y. Zhang, H. Zhao, Y. Zhao, L. Zhou, C.-Y. Lu, C.-Z. Peng, X. Zhu, y J.-W. Pan, “Quantum Computational Advantage via 60-Qubit 24-Cycle Random Circuit Sampling,” *arXiv:2109.03494v2 [quant-ph]*, Sep. 2021.
- [ZPM 2021] Y.-C. Zhang, T. Pohl, and F. Maucher, “Phases of supersolids in confined dipolar Bose-Einstein condensates,” *Physical Review. A/Physical Review, A*, vol. 104, no. 1, Jul. 2021, doi: 10.1103/physreva.104.013310.
- [Zurek 2003] W. H. Zurek, “Decoherence, einselection, and the quantum origins of the classical,” *Reviews of Modern Physics*, vol. 75, no. 3, pp. 715–775, 2003. [En línea]. Disponible en: <https://doi.org/10.1103/RevModPhys.75.715>
- [ZVBL 2020] A. Zlokapa, B. Villalonga, S. Boixo, and D. A. Lidar, “Boundaries of quantum supremacy via random circuit sampling,” *arXiv (Cornell University)*, May 2020, doi: 10.1038/s41534-023-00703-x.
- [Zyga 2015] L. Zyga, “Physicists find quantum coherence and quantum entanglement are two sides of the same coin,” *Phys.org*, Jun. 25, 2015. [En línea]. Disponible en: <https://phys.org/news/2015-06-physicists-quantum-coherence-entanglement-sides.html>

8 ACRÓNIMOS

ACT	<i>Allied Command Transformation</i>
ADN	<i>Ácido desoxirribonucleico</i>
AQ	<i>Algorithmic Qubits</i>
AQC	<i>Adiabatic Quantum Computing</i>
BITD	<i>Base Industrial y Tecnológica de Defensa</i>
BTI	<i>Base Tecnológica e Industrial</i>
CA	<i>Certificate Authoritie</i>
CCN	<i>Centro Criptológico Nacional</i>
CMOS	<i>Complementary Metal-Oxide-Semiconductor</i>
CN-QCN	<i>China Quantum Communication Network</i>
CPoW	<i>Collaborative Programme of Work</i>
CPU	<i>Central Processing Unit</i>
CSDP	<i>Common Security and Defence Policy</i>
CTE	<i>Critical Technology Element</i>
CV-QKD	<i>Continuum Variable QKD</i>
C2	<i>Command and Control</i>
C4ISR	<i>Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance</i>
DARPA	<i>Defense Advanced Research Projects Agency</i>
DIANA	<i>Defence Innovation Accelerator for the North Atlantic</i>
DIMEFIL	<i>Diplomatic, Information, Military, Economic, Financial, Intelligence, Law</i>
DI-QKD	<i>Device-Independent QKD</i>
DOE	<i>Department of Energy</i>
DSIT	<i>Department for Science, Innovation and Technology</i>
ECC	<i>Elliptic Curve Cryptography</i>
EDA	<i>European Defence Agency</i>
EDAP	<i>European Defence Action Plan</i>
EDF	<i>European Defence Fund</i>

EDIDP	<i>European Defence Industrial Development Programme</i>
EDT	<i>Emerging and Disruptive Technology</i>
ENS	Esquema Nacional de Seguridad
ESA	<i>European Spatial Agency</i>
ETID	Estrategia de Tecnología e Innovación para la Defensa
EuroQCI	<i>European Quantum Communication Infrastructure</i>
FPGA	<i>Field-Programmable Gate Array</i>
FTQC	<i>Fault-Tolerant Quantum Computing</i>
GEOINT	<i>Geospatial Intelligence</i>
GNSS	<i>Global Navigation Satellite System</i>
GPS	<i>Global Positioning System</i>
GPU	<i>Graphics Processing Unit</i>
HPC	<i>High Performance Computing</i>
HRL	<i>Hughes Research Laboratories</i>
HSM	<i>Hardware Security Module</i>
HTTPS	<i>Hypertext Transfer Protocol Secure</i>
IA	Inteligencia Artificial
ICQIA	<i>International Council of Quantum Industry Associations</i>
IMINT	<i>Imagery Intelligence</i>
IoMT	<i>Internet of Military Things</i>
IPsec	<i>Internet Protocol Security</i>
IRL	<i>Integration Readiness Level</i>
ISO	<i>International Standardization Organization</i>
ISR	<i>Intelligence, Surveillance and Reconnaissance</i>
ITU	<i>International Telecommunication Union</i>
ITU-T	<i>ITU Telecommunication Standardization Sector</i>
KMS	<i>Key Management Systems</i>
LEO	<i>Low Earth Orbit</i>
MBQC	<i>Measurement Based Quantum Computing</i>
MDI-QKD	<i>Measurement-Device-Independent QKD</i>

MIT	<i>Massachusetts Institute of Technology</i>
ML	<i>Machine Learning</i>
MRL	<i>Manufacturing Readiness Level</i>
NASA	<i>National Aeronautics and Space Administration</i>
NATO	<i>North Atlantic Treaty Organization (OTAN)</i>
NG-QNet	<i>NIST Gaithersburg Quantum Network</i>
NIF	<i>NATO Innovation Fund</i>
NIS	<i>National Intelligence Service / Network and Information Systems</i>
NISQ	<i>Noisy Intermediate-Scale Quantum</i>
NIST	<i>National Institute of Standards and Technology</i>
NMR	<i>Nuclear Magnetic Resonance</i>
NPL	<i>National Physical Laboratory</i>
NQCC	<i>National Quantum Computing Centre</i>
NQI	<i>National Quantum Initiative</i>
NSF	<i>National Science Foundation</i>
OCT	<i>Observatory of Critical Technologies</i>
ONU	<i>Organización de las Naciones Unidas</i>
OSEA	<i>Office of the Secretary of Defense for Acquisition</i>
OSINT	<i>Open Source Intelligence</i>
OTAN	<i>Organización del Tratado del Atlántico Norte (NATO)</i>
PADR	<i>Preparatory Action on Defence Research</i>
PKI	<i>Public Key Infrastructure</i>
PIB	<i>Producto Interior Bruto</i>
PNI	<i>Private Network Interconnect</i>
PNT	<i>Positioning, Navigation and Timing</i>
PNS	<i>Photon Number Splitting</i>
PQC	<i>Post-Quantum Cryptography</i>
PYMES	<i>Pequeñas y Medianas Empresas</i>
QAC	<i>Quantum Annealing Computing</i>
QaaS	<i>Quantum as a Service</i>

QAOA	<i>Quantum Approximate Optimization Algorithm</i>
QBER	<i>Quantum Bit Error Rate</i>
QBI	<i>Quantum Benchmarking Initiative</i>
QBM	<i>Quantum Boltzmann Machines</i>
QBRN	Químicas, Biológicas, Radiológicas y Nucleares
QCaaS	<i>Quantum Computing as a Service</i>
QCNN	<i>Quantum Convolutional Neural Networks</i>
QEC	<i>Quantum Error Correction</i>
QED-C	<i>Quantum Economic Development Consortium</i>
QFT	<i>Quantum Fourier Transform</i>
QGAN	<i>Quantum Generative Adversarial Networks</i>
QI	<i>Quantum Internet</i>
QIA	<i>Quantum Internet Alliance</i>
QIS	<i>Quantum Information Science</i>
QKD	<i>Quantum Key Distribution</i>
QLU	<i>Quantum Logic Unit</i>
QML	<i>Quantum Machine Learning</i>
QPU	<i>Quantum Processing Unit</i>
QRNG	<i>Quantum Random Number Generator</i>
Q-STAR	<i>Quantum Strategic Industry Alliance for Revolution</i>
QSVM	<i>Quantum Support Vector Machines</i>
QuANET	<i>Quantum Augmented Network</i>
QUBO	<i>Quadratic Unconstrained Binary Optimization</i>
QV	<i>Quantum Volume</i>
RCS	<i>Random Circuit Sampling</i>
RNG	<i>Random Number Generator</i>
RPAS	Sistemas aéreos remotamente tripuladas
RSA	<i>Rivest – Shamir – Adleman</i>
SATCOM	<i>Satellite Communications</i>
SCADA	<i>Supervisory Control And Data Acquisition</i>

SIGINT	<i>Signals Intelligence</i>
SML	<i>Sustainment Maturity Level</i>
SNR	<i>Signal-to-Noise Ratio</i>
SRL	<i>System Readiness Level</i>
STO	<i>Science and Technology Organization</i>
TEVV	<i>Test and Evaluation, Verification and Validation</i>
TF-QKD	<i>Twin-Field QKD</i>
TIC	Tecnologías de la Información y las Comunicaciones
TLS	<i>Transport Layer Security</i>
TMP	<i>Technology Maturation Plan</i>
TQC	<i>Transatlantic Quantum Community</i>
TSI	<i>Technology and Science Incubation</i>
TSP	<i>Traveling Salesman Problem</i>
TRA	<i>Technology Readiness Assessment</i>
TRL	<i>Technology Readiness Level</i>
TSP	<i>Traveling Salesman Problem</i>
UE	Unión Europea
UK	<i>United Kingdom</i>
US	<i>United States</i>
USAFA	<i>United States Air Force Academy</i>
USTC	<i>University of Science and Technology of China</i>
US2QC	<i>Underexplored Systems for Utility-Scale Quantum Computing</i>
VPN	<i>Virtual Private Network</i>
VQE	<i>Variational Quantum Eigensolver</i>
VRP	<i>Vehicle Routing Problem</i>
WCP	<i>Weak-Coherent-Pulse</i>
XEB	<i>Cross-Entropy Benchmarking</i>