

Libro Blanco de Ética y Regulación de las Tecnologías Cuánticas

Versión revisada para validación editorial

Fecha de corte: 27 de julio de 2026

1. Introducción

1.0. El reto

Durante el pasado siglo, la mecánica cuántica ha pasado de ser un conjunto de leyes físicas —quizás una de las conceptualizaciones más poderosas de la humanidad, cuyo centenario se celebró en 2025— a materializarse en usos e instrumentos decisivos para nuestra evolución tecnológica, del láser a los semiconductores. Hoy, el control deliberado de estados cuánticos permite explorar nuevas aplicaciones con potencial para contribuir a la transformación de la sociedad en los próximos años. Estamos, con toda probabilidad, en la «adolescencia» de estas tecnologías: una etapa exuberante, prometedora y todavía inestable. El entusiasmo debe convivir con el rigor: avanzar con ambición científica y, al mismo tiempo, con prudencia ante lo mucho que aún ignoramos. Esa prudencia es también una cuestión ética.

Este Libro Blanco se ocupa de las tecnologías cuánticas —computación, comunicaciones, sensórica y materiales— y de sus implicaciones éticas y regulatorias. La llamada «segunda revolución cuántica» alude al salto desde dispositivos cuyo funcionamiento emerge de principios cuánticos (p. ej., láseres, transistores o resonancia magnética) a sistemas que explotan deliberadamente la superposición y el entrelazamiento para el cómputo, las comunicaciones y la medida. Se trata de un continuo de evolución más que de una ruptura súbita, pero sus efectos pueden ser profundos si se logra que la delicada física de los qubits escale con fiabilidad. En todos los ámbitos de aplicación de estas tecnologías surgen dilemas éticos y de gobernanza diferenciados. Los principios éticos considerados se manifiestan en distintas dimensiones:

- **Computación cuántica:** Esta forma de computación, radicalmente distinta de la clásica, manipula amplitudes mediante superposición, interferencia y entrelazamiento. Puede ofrecer ventajas para determinadas clases de problemas y bajo supuestos concretos; no constituye una aceleración universal, y los costes de preparación de datos, corrección de errores y lectura pueden reducir o neutralizar la ventaja. Entre sus posibles aplicaciones figuran la simulación de fenómenos cuánticos, el descubrimiento de fármacos, el diseño de materiales avanzados y ciertos problemas de optimización. Ese potencial convive con riesgos sistémicos, desde la seguridad de la información hasta las asimetrías de poder derivadas de la «brecha cuántica». La pregunta ética no es solo «¿qué puede romper?», sino «¿quién controlará esta capacidad de cómputo y

bajo qué controles democráticos?» y «¿cómo encajará con las prioridades de la sociedad?».

- **Comunicaciones cuánticas:** Tecnologías como la distribución cuántica de claves (QKD) y las futuras redes cuánticas pueden reforzar la confidencialidad bajo determinados modelos de amenaza, siempre que su implementación, autenticación y operación sean seguras. Su despliegue plantea la necesidad de equilibrar esa protección con necesidades legítimas de seguridad y debido proceso, sin comprometer derechos fundamentales. Quienes dominen antes estas infraestructuras podrían obtener una ventaja estratégica frente a quienes mantengan sistemas criptográficos vulnerables.
- **Sensórica cuántica:** Desde la medicina de precisión hasta la navegación autónoma, los sensores cuánticos ofrecen mejoras reales, pero esa misma capacidad puede amplificar la vigilancia o habilitar usos militares sensibles. Una vez más, el acceso desigual a esta tecnología podría suponer una brecha tecnológica y acentuar diferencias entre países y sectores.
- **Materiales cuánticos:** El desarrollo de superconductores, nuevos compuestos y dispositivos diseñados mediante simulaciones cuánticas puede generar ventajas industriales significativas. El reto ético se centra en la concentración de poder, la dependencia y el acceso. ¿Cómo se gestionará, por ejemplo, la disponibilidad de una nueva generación de medicamentos hiperpersonalizados desarrollados gracias a estas capacidades?

El Libro Blanco dedica mayor detalle operativo a la computación y la ciberseguridad, por la inmediatez del riesgo criptográfico, y ofrece un tratamiento estratégico más breve de la sensorica y los materiales.

1.1. Propósito, enfoque y marco regulatorio de referencia

Este Libro Blanco se propone ofrecer una guía accionable para el ecosistema cuántico español —formado, en sentido amplio, por empresas, *startups*, responsables tecnológicos y de cumplimiento, inversores y reguladores—, integrando ética aplicada y Derecho positivo. Asumimos un principio metodológico clave: no hay vacío legal. Aunque no exista una *Lex Quantica* vertical, las tecnologías cuánticas pueden quedar sujetas a un marco horizontal y sectorial del Derecho de la Unión Europea, cuya aplicabilidad depende del producto, el rol, los datos, la finalidad, el sector y el territorio. Se trata de un marco denso y parcialmente solapado, lo que dificulta su aplicación coherente y puede afectar a la seguridad jurídica. En el diseño, la comercialización y el uso de estas tecnologías deben considerarse, entre otras normas, el Reglamento General de Protección de Datos («RGPD»), el Reglamento de Datos («Data Act»), el Reglamento de Inteligencia Artificial («RIA»), el Reglamento de Chips, la Directiva NIS2, el Reglamento DORA, el Reglamento de Ciberresiliencia («CRA»), el Reglamento eIDAS2, el Reglamento sobre productos de doble uso y la Directiva (UE) 2024/2853 sobre responsabilidad por los daños causados por productos defectuosos.

En un plano distinto del marco jurídico, el ecosistema español se apoya en políticas públicas y estrategias nacionales y europeas —p. ej., Quantum Technologies Flagship, EuroHPC o EuroQCI—. Estas iniciativas orientan la innovación y la inversión, pero no deben confundirse con obligaciones legales.

En vista del panorama descrito, la ética cuántica que proponemos no pretende reemplazar al Derecho, sino complementarlo dentro de un marco jurídico complejo y en constante evolución. Su finalidad es ofrecer principios orientadores y criterios de actuación que ayuden a interpretar las normas existentes, clarificar zonas grises y anticipar escenarios aún no previstos por el legislador. En un campo tan incipiente como el cuántico, este Libro Blanco sirve como marco orientativo para fomentar la innovación y la competencia sin menoscabo de los valores y derechos fundamentales de la Unión Europea.

1.1.1. Los cinco principios que estructuran el Libro Blanco

El Capítulo 2 expone los cinco principios rectores que articulan este Libro Blanco para guiar la toma de decisiones técnico-jurídicas en el ecosistema cuántico:

- **Libertad y autonomía.** Protege los derechos fundamentales, la privacidad y el control individual sobre la información, rechazando usos de vigilancia masiva y *social scoring*.
- **Justicia y equidad en el acceso a la tecnología.** Busca mitigar el *quantum divide* y promover el acceso equitativo a las capacidades cuánticas —como las infraestructuras EuroHPC o EuroQCI—, impulsando una verdadera soberanía digital europea.
- **Transparencia, explicabilidad e información responsable.** Reclama una documentación técnica trazable y una honestidad epistémica que permita comprender los límites de los sistemas. Cuando intervenga inteligencia artificial, debe garantizarse la supervisión humana que corresponda conforme al RIA.
- **Responsabilidad y rendición de cuentas.** Exige asignar funciones y responsabilidades, incorporar la seguridad por diseño cuando resulte aplicable y mantener evidencias que permitan una rendición de cuentas efectiva. Esto comprende la gestión de vulnerabilidades y, en el ámbito del CRA, la documentación de la lista de materiales de software («SBOM») y las notificaciones exigibles.
- **Sostenibilidad y desarrollo responsable.** Requiere evaluar el ciclo de vida de los sistemas cuánticos —energía, materiales y residuos— e integrar la información correspondiente en los informes corporativos de sostenibilidad cuando la entidad esté incluida en el ámbito aplicable de la Directiva de Información sobre Sostenibilidad Corporativa («CSRD») y los Estándares Europeos de Información sobre Sostenibilidad («ESRS»).

La privacidad y la seguridad operan, además, como exigencias transversales: el riesgo *harvest now, decrypt later* («HNDL») puede justificar una migración ordenada hacia la criptografía poscuántica («PQC»), mientras que la distribución cuántica de claves («QKD») es una tecnología complementaria que debe combinarse con un mecanismo de autenticación resistente al adversario previsto.

Estos principios no son abstractos: se operativizan como controles verificables y criterios de decisión que utilizaremos de forma repetida en las matrices de riesgo, las hojas de ruta de migración y las cláusulas contractuales descritas en los capítulos 4 a 7.

1.2. Ética de IA vs. ética de infraestructura cuántica (y su intersección)

Estamos en tiempo de fuerte *hype* sobre la inteligencia artificial, impulsado por su potencial poder transformador sobre nuestra sociedad. Este contexto marca también el marco de

reflexión sobre la siguiente frontera tecnológica: las tecnologías cuánticas. Distinguir ambos planos, el de la inteligencia artificial y el de la infraestructura cuántica, es esencial para evitar errores de diagnóstico y de interpretación de la regulación.

Partimos, por tanto, de dos visiones complementarias:

- La **ética de la IA** trata de sistemas que deciden, influyen en decisiones humanas o ejecutan acciones con distintos grados de autonomía. Sus ejes son los sesgos, la explicabilidad, el control humano efectivo y las prohibiciones y categorías de riesgo establecidas en el RIA.
- La **ética cuántica** se centra en infraestructuras que habilitan capacidades (computación, comunicaciones, sensórica, materiales) que pueden sustentar, entre otras cosas, aplicaciones de IA.

En la convergencia entre ambos planos —p. ej., en el *quantum machine learning*—, pueden concurrir ambos conjuntos de riesgos: los algorítmicos —transparencia, uso de datos y supervisión humana— y los infraestructurales —seguridad criptográfica, control de exportaciones y ciberresiliencia—.

Por ello, cuando una aplicación basada en tecnología cuántica constituya un sistema de IA y quede clasificada como de alto riesgo, deberá cumplir las obligaciones del RIA que correspondan a su categoría y al rol de cada operador. A su vez, la infraestructura subyacente deberá cumplir las obligaciones de RGPD, NIS2, DORA o CRA que resulten aplicables por su ámbito material y subjetivo.

Este enfoque por capas —quién decide, con qué datos, bajo qué garantías y sobre qué infraestructura— estructura los análisis sectoriales y las recomendaciones de cumplimiento de este Libro Blanco (véanse los capítulos 4 y 5).

1.3. El sentido de esta propuesta

Estamos, como decíamos, en una fase de adolescencia tecnológica, caracterizada por la búsqueda de coherencia, la corrección de errores y la necesidad de escalabilidad. No hay consenso sobre los plazos en los que, por ejemplo, estará disponible un equipo capaz de quebrar a escala la criptografía de clave pública vulnerable y, por prudencia, evitamos proyecciones enfáticas o especulativas.

Lo que sí existe hoy es el riesgo HNDL: los atacantes pueden interceptar y almacenar comunicaciones cifradas para descifrarlas en el futuro, cuando dispongan de capacidad suficiente. Esa posibilidad debe incorporarse al análisis de riesgos exigido, según el caso, por el RGPD, NIS2, DORA y el CRA. Atendiendo a la criticidad, la vida útil de la información, el estado de la técnica y el coste, dicho análisis puede conducir a inventariar activos criptográficos, planificar o ejecutar la migración hacia la PQC conforme a estándares técnicos aplicables y adoptar la cripto-agilidad como principio de diseño (véanse los capítulos 3.2 y 4.2–4.5).

Con la privacidad y la ciberseguridad como ejes, esta introducción sitúa el debate ético sin hipérboles: priorizamos controles verificables y criterios técnicos compatibles con el *hard law* vigente. Al mismo tiempo, anticipamos la necesidad de un marco especializado, proporcionado y pragmático.

Una regulación extensiva sin calibrar —p. ej., imponer requisitos de documentación o reproducibilidad desproporcionados respecto del riesgo y del rol del módulo cuántico— podría entorpecer la innovación sin mejorar las garantías reales (véase el capítulo 6).

Esta tensión entre proporcionalidad regulatoria y eficacia protectora atraviesa todo el Libro Blanco y se resuelve en clave empresarial y aplicada: mediante modelos de cumplimiento, ejemplos de controles y recomendaciones operativas diseñadas para entornos reales.

1.4. Cómo se conectan principios, Derecho y negocio (nuestra hoja de ruta)

Este Libro Blanco sigue una lógica deliberada: avanzar del principio al Derecho y del Derecho a la aplicación práctica. La estructura que proponemos refleja esa secuencia:

- **Cap. 2 (Principios):** detalla los cinco principios que consideramos clave, con su anclaje jurídico —Carta de Derechos Fundamentales; RGPD; RIA; CRA; NIS2; DORA; eIDAS2— y su traducción en criterios de diseño y controles.
- **Cap. 3 (Impactos éticos y técnicos):** prioriza la seguridad de la información —amenaza a la criptografía de clave pública; PQC y QKD en defensa en profundidad— y distingue riesgos por dominio —computación, comunicaciones, sensórica y materiales—.
- **Cap. 4 (Marco jurídico — *hard law* primero):** analiza la aplicabilidad del RGPD, el RIA, NIS2, DORA, el CRA, eIDAS2 y el régimen de control de productos de doble uso, con referencias a estándares —FIPS 203–205; ETSI/ISO/IEC para QKD y PQC— y responsabilidades por rol —fabricante, proveedor y usuario—.
- **Cap. 5 (Gobernanza, ética aplicada y cumplimiento):** explica cómo convertir principios y Derecho en operativa real y de gestión —sistema de gestión de calidad del RIA; SBOM y gestión de vulnerabilidades del CRA; planes de continuidad DORA; registro de incidencias vinculado a RGPD y NIS2—.
- **Cap. 6 (Riesgos normativos):** riesgos de incumplimiento y de fragmentación o sobreregulación; efectos financieros y reputacionales; PQC como medida razonable de diligencia; mitigaciones con plazos e indicadores.

1.5. Principios como criterios operativos

La hoja de ruta anterior ordena el recorrido del Libro Blanco; este apartado concreta su primer eslabón y muestra cómo los principios se convierten en criterios que reaparecen en los capítulos jurídicos y operativos.

Para asegurar coherencia transversal, cada principio guía decisiones operativas y métricas:

- **Libertad y autonomía** → políticas de diseño que eviten usos intrusivos, límites a la inferencia de perfiles; EIDF/EIPD cuando proceda.
- **Justicia y equidad en el acceso a la tecnología** → acceso a capacidades (programas públicos, cooperación), cláusulas de no discriminación en licencias y SLAs.
- **Transparencia, explicabilidad e información responsable** → documentación técnica y supervisión humana en IA cuántica; honestidad epistémica —condiciones, tasas de error y ruido—.

- **Responsabilidad y rendición de cuentas** → asignación clara de roles; privacidad y seguridad por diseño; inventario criptográfico y migración proporcional al riesgo; gestión de vulnerabilidades y notificación; pruebas de resiliencia y gestión del riesgo de terceros cuando procedan. QKD, si se utiliza, debe contar con autenticación resistente al adversario previsto.
- **Sostenibilidad y desarrollo responsable** → evaluación del impacto energético y material y, cuando proceda, información conforme a CSRD/ESRS.

Estos ejes sustentan las matrices riesgo-norma-control, los marcos de migración a PQC y los ejemplos de cláusulas contractuales que se desarrollan en los capítulos siguientes.

1.6. Alcance: rigor, proporcionalidad y anti-hype

Este Libro Blanco parte de un principio de rigurosidad y proporcionalidad: distinguir la ciencia consolidada de las hipótesis o proyecciones especulativas. Explicitamos las incertidumbres que aún afectan a las tecnologías cuánticas (madurez, escalabilidad, reproducibilidad) y, como se ha anticipado, preferimos hablar de «ventaja cuántica» frente a términos más equívocos que, pese a su difusión mediática, pueden alejarse de una visión científica y jurídicamente rigurosa, como «supremacía cuántica».

Las referencias a escenarios controvertidos (p. ej., el «radar cuántico» o los cronogramas de ruptura criptográfica) se tratan como posibilidades bajo una alta incertidumbre, siempre priorizando la evidencia técnica disponible y su relevancia regulatoria.

El objetivo de este enfoque es ayudar a implementar con criterio los marcos y controles necesarios: qué medidas adoptar, en qué momento, con qué impacto y coste aproximado, y quién debe asumir el liderazgo y la responsabilidad en la adopción de unas tecnologías potencialmente disruptivas, en un momento en el que la inteligencia artificial ya se ha convertido en una fuerza transformadora de nuestra sociedad.

2. Principios Fundamentales para una Ética Cuántica

Los derechos fundamentales reconocidos por la UE y concretados en la legislación horizontal aplicable constituyen el primer nivel de referencia de una ética cuántica. A partir de ellos, proponemos cinco principios para orientar decisiones de diseño, despliegue y gobernanza.

2.1. Libertad y autonomía

El desarrollo de tecnologías cuánticas debe salvaguardar la autonomía individual y el control de las personas sobre sus datos y su privacidad. La autonomía personal no debe diluirse en arquitecturas que, por su capacidad de cómputo, medida o inferencia, desplacen el control humano. En cuántica, este principio opera en dos planos: (i) infraestructural —quién accede a capacidad de cómputo o medida, con qué límites y propósitos— y (ii) algorítmico, cuando hay convergencia con IA cuántica, donde importan la supervisión humana y la trazabilidad de los criterios de decisión. El potencial de ciertas aplicaciones para combinar o analizar datos exige

una aplicación estricta de los principios de protección de datos y de las garantías vinculadas al control de la propia información.

Anclaje jurídico y técnico del principio. Algunas bases normativas:

- **Derechos fundamentales:** La Carta de los Derechos Fundamentales de la UE garantiza el derecho a la protección de datos personales (art. 8) y el respeto a la vida privada (art. 7).
- **Limitación de la finalidad y minimización de datos (art. 5 RGPD):** Las capacidades de análisis de una aplicación cuántica no justifican un tratamiento para fines incompatibles con los inicialmente determinados ni un tratamiento excesivo.
- **Prevención del control desproporcionado:** La ética cuántica debe prevenir el uso de estas tecnologías para la vigilancia masiva o el control social. Cuando una aplicación constituya un sistema de IA, resultarán aplicables las prohibiciones del art. 5 del RIA en los supuestos y con el alcance definidos por esa norma, incluido el *social scoring* prohibido.
- **Seguridad del tratamiento (art. 32 RGPD):** El RGPD exige aplicar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, teniendo en cuenta, entre otros factores, el estado de la técnica. Ante la amenaza cuántica y el riesgo HNDL, el análisis puede justificar una adopción progresiva de criptografía resistente.
- **Gestión de riesgos de ciberseguridad (NIS2/DORA):** Las entidades incluidas en sus respectivos ámbitos deben gestionar los riesgos de ciberseguridad y aplicar medidas proporcionadas. La criticidad y la vida útil de la información pueden justificar planes de migración a PQC, sin que estas normas impongan por sí solas un mandato nominal y universal de adoptar una tecnología concreta.
- **Migración a PQC estandarizada:** Los estándares finalizados por el NIST son FIPS 203 (ML-KEM), FIPS 204 (ML-DSA) y FIPS 205 (SLH-DSA). Su adopción debe planificarse por riesgos, dependencias y casos de uso.
- **Cripto-agilidad (*crypto-agility*):** Es la capacidad de actualizar o sustituir algoritmos, protocolos y parámetros criptográficos sin rediseñar por completo el sistema. Debe incorporarse de forma proporcional a la criticidad y a la vida prevista de cada activo.

Para la práctica: en banca, salud o defensa, separar contractualmente «quién decide» —capa de IA o reglas— de «dónde se ejecuta» —infraestructura cuántica— y documentar la base jurídica del tratamiento cuando haya datos personales, manteniendo poder de control humano sobre resultados que afecten a derechos o riesgos operativos.

2.2. Justicia y equidad en el acceso a la tecnología

El acceso a los beneficios de las aplicaciones de las tecnologías cuánticas en general, y en particular a la computación, debe promoverse de manera equitativa para evitar la creación de una nueva brecha digital (*Quantum Divide*). La concentración actual de la investigación y desarrollo amenaza con generar desigualdades estructurales y dependencias tecnológicas críticas. Este principio opera fundamentalmente en el plano infraestructural: quién accede a capacidad de cómputo/medida, con qué límites y propósitos.

Anclaje estratégico y técnico:

- **Infraestructuras Públicas y Soberanía:** Para fomentar la equidad y la autonomía estratégica europea, es crucial promover el acceso a infraestructuras públicas. La iniciativa EuroHPC Joint Undertaking (Empresa Común Europea de Informática de Alto Rendimiento), que integra recursos de computación cuántica accesibles para la comunidad científica e industrial europea, es un mecanismo clave.
- **Cooperación Internacional y Desarrollo de Talento:** La inversión en programas de cooperación y la formación de talento especializado son esenciales para democratizar el acceso y fomentar un ecosistema diverso.

Para la práctica: diseñar políticas de acceso no discriminatorio, catálogos de servicio y esquemas de identidad/credenciales confiables (eIDAS2), priorizando casos de alto impacto social (p. ej., sensórica en salud o logística crítica) y una cadena de suministro abierta sin comprometer la seguridad.

2.3. Transparencia, explicabilidad e información responsable

La complejidad inherente a la computación cuántica plantea desafíos significativos para la transparencia y la explicabilidad, pero no exime del cumplimiento de las obligaciones legales de información, documentación y rendición de cuentas. La transparencia debe calibrarse según el destinatario: personas afectadas, usuarios profesionales, auditores, autoridades, compradores o financiadores no necesitan la misma información, aunque todos deben recibir la que resulte pertinente para comprender límites, riesgos y responsabilidades.

Anclaje Jurídico y Técnico:

- **Transparencia y supervisión humana (arts. 13 y 14 RIA):** Los sistemas de IA cuántica clasificados como de alto riesgo deben ser suficientemente transparentes para que los responsables del despliegue interpreten sus resultados y permitan una supervisión humana efectiva.
- **Decisiones exclusivamente automatizadas (art. 22 RGPD):** Cuando se cumplan sus presupuestos, el art. 22 limita las decisiones basadas únicamente en tratamientos automatizados que produzcan efectos jurídicos o afecten significativamente de modo similar. Deben observarse las excepciones y salvaguardas aplicables, junto con la información significativa exigida por los arts. 13 a 15.
- **Documentación técnica y honestidad epistémica (art. 11 RIA):** Cuando resulte aplicable, la normativa exige documentación sobre el rendimiento y las limitaciones del sistema. Esto requiere honestidad epistémica: reconocer y documentar los límites de validez, las incertidumbres del modelo, las tasas de error y el impacto del ruido cuántico.
- **Rigor Informativo:** Es necesario adoptar un enfoque realista, evitando expectativas exageradas (*anti-hype*) y garantizando una comunicación rigurosa para evitar alarmismos y desinformación pública.

Para la práctica: adaptar la documentación al destinatario e incluir las condiciones de validez, el dispositivo y la versión de *software*, la calibración, el número de ejecuciones, las tasas de error, la incertidumbre y la comparación con una referencia clásica. En aplicaciones de IA, añadir las instrucciones de uso y las medidas de supervisión exigibles según el RIA.

2.4. Responsabilidad y rendición de cuentas

Las entidades que desarrollan, comercializan, integran y utilizan tecnologías cuánticas deben asignar con claridad las responsabilidades de cada actor, prevenir daños previsibles y conservar evidencia de las decisiones adoptadas. La privacidad y la seguridad son exigencias transversales de esa rendición de cuentas. El riesgo HNDL (*harvest now, decrypt later*) convierte en presente un problema que algunos perciben como futuro: la posibilidad de capturar hoy datos cifrados vulnerables para leerlos mañana con un ordenador cuántico criptográficamente relevante (CRQC). El art. 32 RGPD y las obligaciones de gestión de riesgos de NIS2, DORA o el CRA, cuando resulten aplicables, pueden justificar medidas de inventario, cripto-agilidad y migración a PQC proporcionadas a la criticidad y a la vida útil de la información.

El carril técnico lo marcan FIPS 203 (ML-KEM), FIPS 204 (ML-DSA) y FIPS 205 (SLH-DSA). Su incorporación a PKI, HSM, certificados X.509 o servicios de confianza debe evaluarse conforme al caso de uso y a los perfiles normalizados disponibles, empleando, cuando convenga, esquemas híbridos durante la transición. QKD es un complemento —no un sustituto— para determinados escenarios de alta sensibilidad; no resuelve por sí sola la autenticación inicial y debe combinarse con un mecanismo resistente al adversario previsto, como PQC o, cuando sea viable, autenticación simétrica con claves precompartidas.

Anclaje Jurídico y Técnico:

- **Responsabilidad del fabricante y seguridad por diseño (CRA):** Cuando un producto cuántico quede comprendido en el ámbito del CRA, el fabricante y los demás operadores económicos deberán cumplir las obligaciones que correspondan a su rol. Entre ellas figuran la seguridad por diseño, la gestión de vulnerabilidades durante el periodo de soporte, la identificación y documentación de componentes mediante una SBOM en formato legible por máquina y las notificaciones exigibles.
- **Auditorías y notificación de incidentes (NIS2/DORA):** Las entidades incluidas en el ámbito de estas normas deben aplicar controles, pruebas y notificaciones de incidentes de acuerdo con su categoría, riesgo y régimen sectorial.
- **Control de exportaciones (Reglamento de Doble Uso):** Antes de exportar o transferir tecnología cuántica sensible debe comprobarse si el producto, *software* o asistencia técnica queda comprendido en una entrada de control y alcanza los umbrales o parámetros técnicos aplicables, así como el destino, usuario y uso final. El incumplimiento puede dar lugar a las sanciones previstas por el Derecho aplicable.

Para la práctica: asignar responsables mediante una matriz RACI; inventariar materiales criptográficos; priorizar secretos de larga vida —salud, defensa o finanzas—; y definir hitos de migración —p. ej., certificados híbridos, actualización de terminales o enclaves de alta criticidad—. El capítulo 6 detalla los riesgos y costes de una respuesta insuficiente.

2.5. Sostenibilidad y desarrollo responsable

La eficiencia de una solución cuántica no puede afirmarse de forma abstracta: debe compararse con la mejor alternativa clásica para una misma unidad funcional y a una precisión equivalente. Esa evaluación ha de abarcar el sistema completo —QPU, criogenia, láseres,

electrónica de control, computación clásica de apoyo, red, fabricación y materiales— y medir energía, emisiones y recursos por resultado útil. La sostenibilidad no es cosmética: es una decisión de diseño y, cuando la entidad esté incluida en el ámbito aplicable, una obligación de información bajo CSRD/ESRS. Para todo el ecosistema, el análisis de ciclo de vida, la reparabilidad y el reciclaje son criterios de aceptabilidad social y coste total de propiedad. En Europa, soberanía tecnológica y sostenibilidad se refuerzan mutuamente si la cadena de valor cuántica se construye con estándares compartidos y transparencia.

Anclaje jurídico y técnico:

- **Eficiencia energética y diseño ecológico:** Se debe priorizar la investigación en algoritmos y *hardware* eficientes, con métricas que incluyan todo el sistema y permitan comparaciones reproducibles por unidad funcional.
- **Información corporativa sobre sostenibilidad (CSRD):** Las entidades incluidas en su ámbito deberán informar conforme a la Directiva CSRD y a los ESRS en los términos y calendarios aplicables. El análisis puede comprender el consumo energético y la gestión de recursos materiales.

Para la práctica: definir una unidad funcional y un nivel de precisión comparables, medir QPU, criogenia, control, computación clásica de apoyo, red, fabricación y materiales, y contrastar el resultado con la mejor alternativa clásica disponible antes de afirmar una ventaja ambiental.

Mapa principio–norma–riesgo (resumen)

Principio	Anclaje jurídico principal	Decisión clave de diseño	Riesgo si se ignora
Libertad y autonomía	Carta de los Derechos Fundamentales, arts. 7–8; RGPD arts. 5–6	Separar «quién decide» —IA— de «dónde se ejecuta» —infraestructura cuántica—; documentar la base jurídica y preservar el control humano	Pérdida de control humano; tratamientos ilícitos; decisiones opacas
Justicia y equidad en el acceso a la tecnología	Marco de acceso público —EuroHPC/EuroQCI—; eIDAS2	Acceso no discriminatorio, identidad y confianza federadas	Brecha cuántica, dependencia tecnológica, barreras a pymes
Transparencia, explicabilidad e información responsable	RIA arts. 11 y 13–14; RGPD arts. 13–15 y 22; eIDAS2	Documentación técnica, métricas reproducibles e información adaptada al destinatario	Auditorías fallidas; retirada de producto; litigios
Responsabilidad y rendición de cuentas	RGPD art. 32; NIS2; DORA; CRA; Reglamento (UE) 2021/821	RACI; privacidad y seguridad por diseño; hoja de ruta PQC proporcional al riesgo; QKD con autenticación resistente; gestión de vulnerabilidades y de exportaciones	Exposición HNDL; sanciones; interrupciones; costes de remediación
Sostenibilidad y desarrollo responsable	CSRD/ESRS, cuando resulten aplicables	Comparación por unidad funcional, análisis de ciclo de vida, eficiencia y reciclaje	Riesgo reputacional, costes operativos crecientes, barreras de mercado

Los riesgos normativos y las consecuencias del incumplimiento se analizan con detalle en el capítulo 6.

3. Impactos Éticos y Técnicos de las Tecnologías Cuánticas

En esta etapa aún adolescente de las tecnologías cuánticas —prometedora y frágil—, los impactos no se comprenden con hipérboles sensacionalistas, sino con una aproximación rigurosa y criterios verificables. Este capítulo presenta los efectos éticos y técnicos por

dominios —privacidad y seguridad de la información; ciberseguridad y respuesta PQC/QKD; IA cuántica; sectores críticos; equidad y soberanía digital; riesgos emergentes—, usando como brújula los cinco principios del capítulo 2 y anclando cada diagnóstico en el marco horizontal y sectorial potencialmente aplicable —RGPD, RIA, NIS2, DORA, CRA, eIDAS2 y régimen de doble uso—. No partimos de un vacío legal: el *hard law* es el suelo común, como se describe en el capítulo siguiente; la ética aplicada eleva el listón allí donde la norma ofrece opciones y ponderaciones.

Metodológicamente, distinguimos la infraestructura —computación, comunicaciones, sensórica y materiales— de la decisión algorítmica —IA— y, cuando convergen, separamos las capas de riesgo y garantías. Evitamos cronologías especulativas: en seguridad, el riesgo HNDL es presente y puede justificar, conforme al análisis de riesgos, una migración a PQC con cripto-agilidad; QKD aporta defensa en profundidad en determinados nichos y requiere un mecanismo de autenticación resistente al adversario previsto; la «ventaja cuántica» es el término operativo, no «supremacía». El objetivo es decidir qué riesgos priorizar, qué evidencias exigir y qué controles desarrollar en el capítulo 5.

La secuencia conecta los cinco principios con los impactos: la libertad y autonomía y la responsabilidad y rendición de cuentas guían la respuesta criptográfica de los apartados 3.1 y 3.2; la transparencia, explicabilidad e información responsable orientan el análisis de IA cuántica de 3.3; la justicia y equidad en el acceso a la tecnología informan los apartados sectoriales y de soberanía de 3.4 y 3.5; y la sostenibilidad y desarrollo responsable se integran en la evaluación de los riesgos emergentes de 3.6. La privacidad y la seguridad actúan en todos ellos como dimensiones transversales.

3.1. Impacto en la privacidad y la seguridad de los datos (La Amenaza)

Un ordenador cuántico tolerante a fallos y de escala suficiente alteraría de forma sistémica la seguridad de la información. El algoritmo de Shor permitiría resolver eficientemente la factorización de enteros y el logaritmo discreto, en los que se basan RSA, Diffie-Hellman y buena parte de la criptografía de curva elíptica. Esta amenaza se refiere a sistemas de clave pública vulnerables, no a toda la criptografía ni a toda forma de comunicación digital.

Definición de la Amenaza:

- **Ordenador cuántico criptográficamente relevante (CRQC):** La amenaza se materializará cuando exista un ordenador cuántico con suficiente escala y corrección de errores para ejecutar el algoritmo de Shor contra parámetros de uso real. En ese supuesto, los sistemas de clave pública vulnerables dejarán de ofrecer la seguridad prevista.
- **HNDL (*harvest now, decrypt later*):** La amenaza es presente por la posibilidad de «cosechar ahora y descifrar después». Los atacantes pueden interceptar y almacenar datos cifrados hoy para intentar descifrarlos en el futuro con un CRQC. Esto supone un riesgo inmediato y material para la información con una vida de confidencialidad larga, como archivos gubernamentales clasificados, secretos industriales y datos de salud, biométricos o financieros.

El escenario exige una respuesta coordinada para actualizar la infraestructura que dependa de algoritmos vulnerables. A efectos de cumplimiento, el patrón HNDL convierte la confidencialidad a largo plazo en un riesgo presente. Bajo el RGPD —arts. 25 y 32—, NIS2 o DORA, cuando resulten aplicables, las organizaciones deben evaluar ese riesgo y pueden tener que iniciar una transición planificada hacia esquemas resistentes, priorizando la información con mayor vida de confidencialidad.

Shor no es la única referencia relevante. En un modelo idealizado, el algoritmo de Grover reduce aproximadamente a la raíz cuadrada la complejidad de la búsqueda exhaustiva contra cifrados simétricos y funciones *hash*; este efecto suele mitigarse aumentando adecuadamente el tamaño de claves y salidas. Las firmas y los archivos que deban conservarse durante largos periodos requieren, además, políticas de preservación, renovación y prueba de validez.

3.2. Riesgos para la ciberseguridad y la respuesta a la amenaza cuántica (PQC y QKD)

La respuesta a la amenaza cuántica se articula en torno a dos enfoques tecnológicos distintos y complementarios: la criptografía poscuántica (PQC) y la distribución cuántica de claves (QKD). Es crucial comprender sus funciones, limitaciones e interdependencias.

Criptografía poscuántica (PQC): la respuesta principal y generalizable

- PQC se refiere a algoritmos criptográficos clásicos (ejecutables en hardware actual) diseñados para ser resistentes a ataques cuánticos.
- **Estandarización (NIST):** El NIST publicó FIPS 203 (ML-KEM, derivado de CRYSTALS-Kyber, para encapsulación de claves), FIPS 204 (ML-DSA, para firmas digitales) y FIPS 205 (SLH-DSA, para firmas digitales). FN-DSA, derivado de FALCON, se desarrolla separadamente como FIPS 206 y aún no es un estándar definitivo. En 2025, el NIST seleccionó HQC como algoritmo adicional de encapsulación de claves; su estándar tampoco está finalizado.
- **Prioridad estratégica:** La migración a PQC es la respuesta generalizable para los sistemas que dependen de criptografía de clave pública vulnerable. Las hojas de ruta deben priorizar el inventario criptográfico, la cripto-agilidad y, cuando proceda, los esquemas híbridos.

La hoja de ruta europea de aplicación coordinada, publicada en junio de 2025, establece una transición escalonada hasta 2035 según el nivel de riesgo. En la práctica, según el alcance y el plan de migración, puede ser necesario introducir requisitos de cripto-agilidad en la contratación, identificar equipos heredados incompatibles, programar su sustitución, reforzar la continuidad operativa y formar al personal; el seguro puede complementar, pero no sustituir, estas medidas.

La estrategia europea combina una transición prioritaria a PQC con QKD en determinados escenarios de alta sensibilidad. La conformidad debe apoyarse en evidencias técnicas y jurídicas adecuadas al régimen aplicable, como la gestión de vulnerabilidades del CRA o los servicios de confianza de eIDAS2 cuando correspondan.

Distribución cuántica de claves (QKD): un complemento especializado

- QKD es una técnica basada en hardware que utiliza principios de la física cuántica para distribuir claves criptográficas.
- **Seguridad teórica frente a seguridad práctica:** QKD ofrece garantías teóricas bajo modelos concretos, pero su seguridad práctica no es «inquebrantable». La implementación puede ser vulnerable a ataques contra dispositivos y canales laterales, así como a denegación de servicio.
- **Autenticación resistente:** QKD no resuelve por sí sola la autenticación inicial de los extremos. Debe combinarse con un mecanismo resistente al adversario previsto, como PQC o, cuando sea viable, autenticación simétrica con claves precompartidas.
- **Estandarización (ETSI):** ETSI está desarrollando normas técnicas para la interoperabilidad de QKD (p. ej., ETSI GS QKD 014 para interfaces API).
- **Limitaciones de despliegue:** Deben evaluarse la distancia y la tasa de generación de claves, la posible necesidad de nodos de confianza, la seguridad de los dispositivos, la resistencia frente a denegación de servicio, la interoperabilidad y la certificación.

Conclusión: QKD no sustituye a PQC, sino que puede actuar como capa complementaria de defensa en profundidad para casos de alta seguridad, siempre que la autenticación y la implementación respondan al modelo de amenaza.

3.3. Implicaciones en la inteligencia artificial y el análisis de datos (IA cuántica)

La convergencia de la computación cuántica con la inteligencia artificial, particularmente en el aprendizaje automático cuántico (*quantum machine learning* o QML), podría aportar ventajas en tareas concretas de análisis u optimización. No se ha demostrado una ventaja práctica general: cada propuesta debe evaluar la carga de datos, el coste de muestreo, el ruido, la escalabilidad y la comparación con el mejor método clásico disponible.

Desafíos éticos y regulatorios de la IA cuántica:

- **Análisis y vigilancia:** Si una aplicación llegara a acelerar determinadas inferencias o combinaciones de datos, podría potenciar usos de vigilancia o manipulación social, con riesgos para los derechos fundamentales y la protección de datos.
- **Opacidad y explicabilidad:** La incorporación de componentes cuánticos puede añadir complejidad técnica y dificultar la validación, sin eximir de los niveles de transparencia y documentación exigibles.
- **Cumplimiento del RIA:** Cuando una aplicación constituya un sistema de IA y quede clasificada como de alto riesgo, deberá cumplir las obligaciones que correspondan a su categoría y a cada rol, incluidas la documentación técnica —art. 11—, la transparencia —art. 13— y la supervisión humana —art. 14—. La mayor complejidad exige honestidad epistémica sobre las limitaciones del modelo, pero no determina por sí sola la clasificación.

En definitiva, el uso de infraestructura cuántica no activa por sí solo el RIA. Cuando concurren sus presupuestos, se aplicarán las obligaciones algorítmicas correspondientes; en paralelo, el RGPD, NIS2, DORA o el CRA regirán la infraestructura y las operaciones dentro de sus respectivos ámbitos. El capítulo 5 aborda esta coordinación.

3.4. Uso de la computación cuántica en sectores críticos (salud, defensa, finanzas)

La aplicación de la computación cuántica en sectores críticos puede generar oportunidades relevantes, pero también requiere identificar las obligaciones regulatorias aplicables a cada caso.

Algunos ejemplos:

Salud y Datos Sensibles:

- **Oportunidades:** Simulaciones moleculares avanzadas para el descubrimiento de fármacos y medicina personalizada.
- **Riesgos y regulación:** El tratamiento de datos de salud —categorías especiales de datos— exige una base jurídica conforme al art. 6 del RGPD y la concurrencia de una excepción del art. 9. El uso de tecnología cuántica no activa por sí solo una evaluación de impacto relativa a la protección de datos (EIPD); esta será obligatoria cuando sea probable que el tratamiento entrañe un alto riesgo conforme al art. 35. Cuando resulte aplicable, estos sistemas deben alinearse también con el Reglamento (UE) 2025/327 relativo al Espacio Europeo de Datos de Salud (EHDS), en vigor y con aplicación escalonada. La sensibilidad y los largos periodos de conservación de estos datos hacen especialmente relevante el riesgo HNDL.

Defensa y Seguridad Nacional (Doble Uso):

- **Oportunidades:** Criptoanálisis avanzado, desarrollo de nuevos materiales y sensores.
- **Riesgos y regulación:** El potencial de doble uso exige comprobar el Reglamento (UE) 2021/821 y su lista de control, actualizada por el Reglamento Delegado (UE) 2025/2003. La partida 4A506 incluye determinados ordenadores cuánticos y equipos conexos sujetos a parámetros técnicos; no todo *hardware*, *software* o asistencia cuántica requiere licencia. Deben verificarse el código y los umbrales, el destino, el usuario y el uso final antes de exportar o transferir.

Sector Financiero (Resiliencia y Estabilidad):

- **Oportunidades:** Mejora de la gestión del riesgo, optimización de carteras de inversión, detección avanzada de fraude.
- **Riesgos y regulación:** Según el caso de uso, pueden resultar aplicables MiFID II y el Reglamento sobre abuso de mercado a la negociación algorítmica, MiCA a los proveedores de servicios de criptoactivos, el Reglamento (UE) 2022/858 a infraestructuras de mercado basadas en DLT y DORA a la gestión del riesgo TIC y de terceros. El capítulo 4 desarrolla estas conexiones, incluida la migración criptográfica de las infraestructuras distribuidas.

3.5. Posibles desigualdades y soberanía digital

El riesgo de una brecha digital cuántica (*Quantum Divide*) es uno de los principales desafíos éticos y estratégicos. El dominio de estas tecnologías está actualmente concentrado debido a las altas barreras de entrada (inversión, infraestructura, talento especializado).

- **Dependencia Tecnológica:** Si no se establecen políticas de acceso equitativo e inversión estratégica, las naciones y empresas europeas podrían quedar rezagadas,

aumentando la dependencia tecnológica de terceros países y erosionando la soberanía digital de la UE.

- **Iniciativas estratégicas:** Iniciativas como EuroHPC —para computación— y EuroQCI —Infraestructura Europea de Comunicación Cuántica— pueden contribuir a mitigar este riesgo y favorecer una participación inclusiva y competitiva.

3.6. Consecuencias no previstas y riesgos emergentes

La computación cuántica se encuentra en una etapa de desarrollo donde muchos de sus impactos a largo plazo son inciertos.

- **Impacto laboral:** Posibles cambios en tareas y perfiles altamente cualificados de áreas como la investigación química, las finanzas o la ciberseguridad, cuya magnitud y dirección son todavía inciertas.
- **Modelos predictivos y derechos fundamentales:** Los modelos predictivos que incorporen componentes cuánticos pueden afectar a derechos individuales y colectivos si no se gobiernan adecuadamente.
- **Gestión de riesgos emergentes:** La gestión de estos riesgos requiere mecanismos de supervisión ágiles y evaluaciones adaptadas al caso. La EIPD será obligatoria cuando sea probable que el tratamiento de datos personales entrañe un alto riesgo conforme al art. 35 del RGPD. La evaluación de impacto sobre los derechos fundamentales (EIDF) del art. 27 del RIA procederá para los responsables del despliegue y los sistemas de alto riesgo comprendidos en ese precepto, incluidos determinados organismos de Derecho público y entidades privadas que prestan servicios públicos.

El capítulo adopta una lógica preventiva: los impactos inciertos se abordan con evaluaciones de impacto cuando procedan, métricas de sostenibilidad pertinentes y pruebas de resiliencia proporcionadas al riesgo. El capítulo 5 desarrolla el detalle operativo y los indicadores.

Algunos ejemplos de coherencia «Riesgo → Norma → Control» (base para el capítulo 5)

Riesgo descrito en el cap. 3	Norma de referencia	Control/criterio para su gestión/supervisión
HNDL sobre datos de larga vida	RGPD 25/32; NIS2; DORA; CRA	Inventario criptográfico → evaluación y priorización → migración a PQC cuando el riesgo la justifique; cripto-agilidad, certificados híbridos, SBOM y notificación de vulnerabilidades.
QKD mal posicionado	ETSI/ISO QKD; eIDAS2 (traza)	QKD como complemento; autenticación resistente al adversario previsto; conformidad e interoperabilidad ETSI; evidencia firmada o sellada.
IA cuántica opaca	RIA arts. 11, 13, 14 y 17; RGPD 22	Documentación técnica y <i>model/risk cards</i> , límites y tasas de error, supervisión humana efectiva; traza jurídica eIDAS2 cuando proceda.
Fragmentación/lock-in	Data Act; eIDAS2; EuroHPC/EuroQCI	Portabilidad/switching, identidad y confianza federadas; uso de infraestructuras públicas.

4. Marco Jurídico y Regulatorio Aplicable (*hard law*)

Nos referimos en este capítulo al marco horizontal y sectorial potencialmente aplicable a la investigación, el desarrollo, la comercialización y el uso del *stack* cuántico en la UE: RGPD, Reglamento de IA, NIS2, DORA, CRA, eIDAS2 y el régimen de doble uso, entre otros. No hay un «vacío legal», pero tampoco una aplicación automática de todas estas normas por el solo

uso de tecnología cuántica. Las obligaciones dependen de la función asumida, el producto o servicio, los datos tratados, el sector, el territorio y el uso previsto. La ética aplicada (cap. 2) eleva el listón; aquí se identifica qué puede resultar obligatorio y para quién, con la vista puesta en la operativa (cap. 5) y los riesgos de incumplimiento (cap. 6).

4.1. Estado actual de la regulación cuántica: marco horizontal y sectorial potencialmente aplicable

Es un error asumir que las tecnologías cuánticas operan en un vacío legal por la ausencia de una legislación vertical específica (*Lex Quantica*). En la Unión Europea existe un marco tecnológico horizontal y sectorial que puede alcanzar actividades, productos y servicios cuánticos cuando concurren sus respectivos presupuestos de aplicación.

Conviene distinguir su naturaleza jurídica. Los reglamentos son obligatorios y directamente aplicables en las condiciones y desde las fechas previstas en cada texto; las directivas obligan en cuanto al resultado y requieren su transposición al Derecho nacional; y las normas técnicas o recomendaciones no son, por sí solas, legislación vinculante, aunque pueden adquirir relevancia contractual, supervisora o para la evaluación de conformidad. La neutralidad tecnológica —expresamente recogida, entre otros lugares, en el considerando 15 del RGPD— y el enfoque basado en el riesgo no sustituyen este análisis de ámbito.

Para evitar sobreafirmaciones, el Libro Blanco distingue entre **(O)** obligación normativa expresa, **(I)** interpretación jurídica basada en riesgo, **(S)** estándar técnico, **(R)** recomendación no vinculante y **(P)** propuesta de política o buena práctica.

El marco potencialmente aplicable incluye, entre otros:

- **Ciberseguridad y resiliencia:** NIS2 (Dir. (UE) 2022/2555), DORA (Reg. (UE) 2022/2554) y CRA (Reg. (UE) 2024/2847).
- **Protección de datos:** RGPD (Reg. (UE) 2016/679).
- **IA:** Reglamento de IA (Reg. (UE) 2024/1689), cuando la solución cuántica constituya o integre un sistema de IA comprendido en su ámbito.
- **Identidad y confianza:** eIDAS2 (Reg. (UE) 2024/1183).
- **Comercio estratégico:** régimen de doble uso (Reg. (UE) 2021/821 y actualización de su Anexo I).
- **Responsabilidad por productos:** Dir. (UE) 2024/2853.
- **Servicios financieros y criptoactivos:** DORA, MiCA (Reg. (UE) 2023/1114), régimen piloto DLT (Reg. (UE) 2022/858) y, cuando corresponda, MiFID II y MAR.
- **Estándares y orientación técnica:** FIPS 203-205 (PQC), ETSI/ISO/IEC y CEN-CENELEC.

La Estrategia para una Europa Cuántica (COM(2025) 363 final) es una iniciativa de política pública **(P)**. A fecha de cierre de esta edición, el denominado *Quantum Act* seguía figurando en la planificación de la Comisión: no se trata aquí como Derecho vigente ni como un régimen horizontal de clasificación de riesgos.

También debe seguirse la evolución del paquete Ómnibus Digital. A la fecha de corte, el Parlamento Europeo y el Consejo habían aprobado el texto legislativo PE 30/2026 REV 1 sobre simplificación del Reglamento de IA, todavía sin número definitivo de publicación en el *Diario*

Oficial. Ese texto desplaza la aplicación de las reglas de alto riesgo del anexo III al 2 de diciembre de 2027 y de las integradas en productos del anexo I al 2 de agosto de 2028. Otras modificaciones del acervo digital seguían en tramitación. Por ello, esta edición distingue el texto aprobado de las propuestas aún pendientes y recomienda verificar su publicación y aplicabilidad antes de usarlo como base de cumplimiento.

Riesgos si se ignora: según la norma y el supuesto concreto, pueden producirse multas, retirada o prohibición de productos, pérdida de certificaciones, responsabilidad civil y bloqueos de exportación, entre otras consecuencias; véase el cap. 6 para el detalle sancionador. A continuación se analiza la posible aplicación de cada pilar al ecosistema cuántico.

4.2. Ciberseguridad y Resiliencia (NIS2, DORA, CRA)

La legislación europea en materia de ciberseguridad y resiliencia es relevante para las tecnologías cuánticas tanto por el riesgo que pueden plantear para la criptografía actual como por los requisitos aplicables a determinadas entidades, productos y servicios.

4.2.1. Directiva NIS2 (Seguridad de las Redes y Sistemas de Información)

La Directiva (UE) 2022/2555 (NIS2) establece el marco de ciberseguridad para entidades de sectores críticos y otros sectores incluidos en sus anexos. Su aplicación efectiva debe examinarse junto con la legislación nacional de transposición.

Aplicabilidad a las Tecnologías Cuánticas:

- **Ámbito de aplicación:** NIS2 distingue entre entidades «esenciales» e «importantes». Los proveedores de servicios de computación en nube figuran entre los tipos de entidades cubiertos, pero alojar o prestar acceso a una plataforma cuántica no determina por sí solo la clasificación: deben verificarse la actividad, el tamaño, el establecimiento, las excepciones y la transposición nacional aplicable.
- **Gestión de riesgos (art. 21):** NIS2 exige medidas técnicas, operativas y organizativas adecuadas y proporcionadas. Entre las medidas mínimas figuran políticas y procedimientos sobre criptografía y, en su caso, cifrado. A la vista del riesgo *harvest now, decrypt later* (HNDL), la migración a PQC puede formar parte de las medidas exigibles **(I)** según el riesgo, el estado de la técnica y el calendario europeo aplicable; NIS2 no impone literalmente PQC a toda entidad.
- **Seguridad de la cadena de suministro:** Las entidades comprendidas deben gestionar los riesgos de sus proveedores y prestadores directos. Al contratar computación cuántica o adquirir componentes cuánticos, procede evaluar las prácticas de seguridad del proveedor en función de la relación y del riesgo, sin convertir al proveedor en sujeto de NIS2 por ese único hecho.

4.2.2. Reglamento DORA (Resiliencia Operativa Digital del Sector Financiero)

El Reglamento (UE) 2022/2554 (DORA) impone requisitos de resiliencia operativa digital a las entidades financieras comprendidas en su ámbito.

Aplicabilidad a las Tecnologías Cuánticas:

- **Gestión de riesgos TIC (arts. 6 y 9):** Las entidades financieras sujetas a DORA deben identificar y gestionar sus riesgos TIC. El riesgo de obsolescencia criptográfica y una eventual migración a PQC pueden integrarse en ese marco **(I)** cuando sean materiales para los activos, funciones y horizontes de confidencialidad de la entidad; DORA no prescribe de forma general un algoritmo poscuántico concreto.
- **Gestión de riesgos de terceros (Capítulo V):** El uso de una plataforma cuántica como servicio TIC debe incluirse, cuando proceda, en la gestión contractual y de concentración. Un proveedor no se convierte automáticamente en «proveedor tercero crítico»: la criticidad requiere la designación prevista en DORA conforme a sus criterios.
- **Pruebas de resiliencia (arts. 24-27):** Los escenarios de compromiso criptográfico pueden resultar pertinentes según el perfil de riesgo. Las pruebas avanzadas de penetración basadas en amenazas del art. 26 solo se exigen a las entidades identificadas para ese régimen, no a todas las entidades financieras ni a todo proveedor cuántico.

4.2.3. Reglamento de Ciberresiliencia (CRA)

El Reglamento (UE) 2024/2847 (CRA, *Cyber Resilience Act*) establece requisitos horizontales de ciberseguridad para los productos con elementos digitales comercializados en la UE cuya finalidad prevista o uso razonablemente previsible incluya una conexión de datos directa o indirecta, lógica o física, a un dispositivo o red.

Aplicabilidad a las Tecnologías Cuánticas:

- **Ámbito de aplicación:** Un hardware, una librería, un SDK u otro software cuántico quedará sujeto al CRA si encaja en la definición de «producto con elementos digitales», se introduce en el mercado y no concurre una exclusión. La etiqueta «cuántico» no basta: un sensor autónomo sin la conexión exigida, un servicio puro o una actividad de investigación no comercial requieren un análisis específico.
- **Requisitos esenciales (Anexo I):** Los productos incluidos deben cumplir requisitos de ciberseguridad por diseño y por defecto, proporcionados al riesgo, y gestionar sus vulnerabilidades durante el periodo de soporte. El uso de PQC o de mecanismos de cripto-agilidad puede ser una respuesta adecuada **(I)** cuando el análisis de riesgos y el estado de la técnica lo justifiquen; el CRA no impone PQC de forma universal.
- **Gestión de vulnerabilidades y SBOM (art. 13 y anexo I):** El fabricante debe identificar y documentar los componentes del producto, incluso mediante una lista de materiales de software (SBOM) en un formato de lectura mecánica de uso común. No existe una obligación general de publicar la SBOM ni de entregarla indiscriminadamente a todos los clientes, sin perjuicio del acceso que corresponda a las autoridades y de otros compromisos aplicables.
- **Notificación (art. 14):** Los fabricantes deben notificar vulnerabilidades explotadas activamente e incidentes graves que afecten a la seguridad del producto mediante los avisos y plazos escalonados establecidos en el artículo. El CRA será aplicable con

carácter general desde el 11 de diciembre de 2027; el art. 14 se aplica desde el 11 de septiembre de 2026 y el capítulo IV desde el 11 de junio de 2026.

4.3. Privacidad y Protección de Datos (RGPD)

El Reglamento (UE) 2016/679 (RGPD) es aplicable cuando una actividad cuántica implica tratamiento de datos personales y se cumplen sus criterios territorial y material. La computación cuántica puede ser relevante tanto para la seguridad de datos conservados a largo plazo como para determinados tratamientos avanzados.

Aplicabilidad a las Tecnologías Cuánticas:

Como riesgo para la seguridad de los datos:

- **Seguridad del tratamiento y PQC (arts. 5.1.f y 32):** El principio de integridad y confidencialidad y el art. 32 exigen un nivel de seguridad adecuado al riesgo, atendiendo, entre otros factores, al estado de la técnica, los costes, el contexto y las finalidades. El riesgo HNDL puede justificar una transición progresiva a PQC (I) para categorías de datos y horizontes de confidencialidad determinados; no convierte PQC en una obligación automática para todo tratamiento.
- **Protección de datos desde el diseño y por defecto (art. 25):** Deben adoptarse medidas técnicas y organizativas apropiadas desde el diseño. Según el caso, pueden incluir inventario criptográfico, cripto-agilidad o PQC, si resultan proporcionadas al riesgo y eficaces para aplicar los principios del RGPD.

Como medio o herramienta de tratamiento:

- **Principios del tratamiento y reidentificación (art. 5):** Una reidentificación efectiva podría afectar, según el tratamiento, a los principios de limitación de la finalidad, minimización de datos, exactitud e integridad y confidencialidad. La posibilidad de que técnicas cuánticas alteren la eficacia de una anonimización es una hipótesis que debe evaluarse con evidencia y atendiendo a los medios razonablemente utilizables; no cabe presumir que todo dato anonimizado se convierta por ello en dato personal.
- **Evaluación de impacto (EIPD) (art. 35):** La EIPD es obligatoria cuando sea probable que el tratamiento entrañe un alto riesgo para los derechos y libertades, incluidos los supuestos del art. 35.3 y los listados del art. 35.4. El uso de tecnología cuántica, incluso en salud o finanzas, no activa por sí solo la EIPD: deben examinarse finalidad, escala, categorías de datos, decisiones y demás criterios de riesgo.

4.4. Inteligencia Artificial y Sistemas de Alto Riesgo (Reglamento de IA)

El Reglamento (UE) 2024/1689 (Reglamento de IA) adopta un enfoque basado en el riesgo. Solo será aplicable a una solución cuántica si esta constituye o integra un «sistema de IA» conforme a su definición y se cumplen los demás presupuestos de ámbito; la infraestructura o el cálculo cuántico no son IA por naturaleza.

Aplicabilidad a las Tecnologías Cuánticas (IA cuántica):

- **Clasificación de alto riesgo:** Una solución de IA cuántica será de alto riesgo cuando encaje en los criterios del art. 6 y, según corresponda, en el anexo I o en un caso de

uso del anexo III, teniendo también en cuenta las excepciones aplicables. La calificación crediticia, ciertos usos médicos o la gestión de infraestructuras críticas pueden requerir este análisis, pero el ámbito «crítico» o la tecnología cuántica no determinan automáticamente la clasificación.

- **Obligaciones para sistemas de alto riesgo (arts. 9-15):** Los proveedores de sistemas clasificados como de alto riesgo deben cumplir los requisitos correspondientes. La complejidad técnica («opacidad») de un modelo cuántico no exime de:
 - Sistema de gestión de riesgos continuo (art. 9).
 - Gobernanza de los datos de entrenamiento, validación y prueba (art. 10).
 - Documentación técnica detallada (art. 11).
 - Conservación de registros (art. 12).
 - Transparencia e información a los responsables del despliegue (art. 13).
 - Supervisión humana efectiva (art. 14).
 - Precisión, solidez y ciberseguridad (art. 15).
- **Honestidad epistémica y documentación:** Cuando sean exigibles la documentación técnica y el Anexo IV, deben reflejarse los límites de validez, las incertidumbres del modelo, el impacto del ruido cuántico y las tasas de error con el grado de detalle requerido.
- **Sistema de gestión de la calidad (QMS) (art. 17):** Los proveedores de sistemas de IA de alto riesgo deben implementar un QMS documentado que asegure el cumplimiento normativo durante todo el ciclo de vida.

4.5. Identidad Digital y Servicios de Confianza (eIDAS2)

El Reglamento (UE) 2024/1183 (eIDAS2) modifica y amplía el marco europeo de identidad digital y servicios de confianza. La amenaza cuántica puede afectar a la verificabilidad futura y a la preservación probatoria de firmas, sellos y evidencias electrónicas.

Aplicabilidad a las Tecnologías Cuánticas:

- **Validez, verificabilidad y conservación:** La obsolescencia futura de un algoritmo no invalida retroactivamente una firma o un sello que fuera válido al tiempo de su creación. Sí puede comprometer su verificabilidad futura y la preservación de su valor probatorio si no se aplican mecanismos adecuados de conservación, resellado y migración criptográfica.
- **Obligaciones de los QTSP:** Los prestadores cualificados de servicios de confianza deben gestionar el riesgo criptográfico y mantener los requisitos de seguridad y cualificación que les resulten aplicables. La transición concreta a PQC dependerá de los estándares, actos de ejecución, esquemas y calendarios aplicables; eIDAS2 no impone por sí solo un algoritmo PQC único e inmediato.
- **Cartera de Identidad Digital Europea (EUDI Wallet):** La cripto-agilidad y la preparación para algoritmos resistentes a ataques cuánticos son medidas prudentes (I/P) para preservar la confianza a largo plazo, sujetas a la arquitectura y especificaciones regulatorias aplicables.

4.6. Control de Exportaciones y Doble Uso (Reglamento (UE) 2021/821)

El Reglamento (UE) 2021/821 establece el régimen de la UE para el control de exportaciones, corretaje, asistencia técnica, tránsito y transferencia de productos de doble uso. Su Anexo I fue sustituido por el Reglamento Delegado (UE) 2025/2003.

Aplicabilidad a las Tecnologías Cuánticas:

- **Productos listados (Anexo I):** La entrada 4A506 comprende determinados ordenadores cuánticos y conjuntos electrónicos y componentes relacionados que alcancen sus parámetros técnicos. No toda tecnología cuántica está controlada: la clasificación exige comprobar la entrada, sus umbrales y notas técnicas, y puede alcanzar asimismo software o tecnología vinculados mediante sus entradas correspondientes.
- **Licencia y controles no listados:** La necesidad de autorización depende de la clasificación, la operación, el destino, el usuario y el uso final. Además de los productos listados, deben examinarse los controles *catch-all* y las medidas nacionales aplicables; no cabe inferir una licencia automática por la mera naturaleza cuántica del producto.
- **Tecnología y asistencia técnica:** El control puede extenderse a transferencias intangibles de tecnología, conocimiento técnico y asistencia técnica relacionadas con productos controlados, conforme a las definiciones y condiciones del Reglamento.

4.7. Normas y estándares técnicos internacionales (NIST, ETSI, CEN-CENELEC)

Los estándares técnicos desempeñan un papel fundamental en la implementación práctica de la regulación y la interoperabilidad, pero su fuerza jurídica debe distinguirse de la de una obligación legal expresa.

NIST (EE. UU.) — Criptografía poscuántica (PQC): En 2024, NIST publicó:

- **FIPS 203 (ML-KEM):** mecanismo de encapsulación de claves.
- **FIPS 204 (ML-DSA) y FIPS 205 (SLH-DSA):** esquemas de firma digital.

Estos estándares (**S**) son referencias técnicas de primer orden, pero no se convierten automáticamente en obligaciones de la UE. FALCON no corresponde a FIPS 204 ni a FIPS 205; cualquier referencia a FN-DSA/FIPS 206 debe ajustarse a su estado oficial en la fecha de consulta.

ETSI (Europa) - Comunicaciones Cuánticas (QKD): El Instituto Europeo de Normas de Telecomunicaciones (ETSI) desarrolla especificaciones para QKD.

ETSI GS QKD 014: define una interfaz API REST para la entrega interoperable de claves cuánticas.

CEN-CENELEC (Europa) - Componentes y Metrología: Estos organismos abordan la normalización técnica de componentes cuánticos y metrología.

Rol de los estándares armonizados: Una norma armonizada puede generar presunción de conformidad solo cuando haya sido adoptada y su referencia se haya publicado en el *Diario Oficial de la Unión Europea*, y únicamente dentro de su ámbito. Las especificaciones técnicas no armonizadas siguen siendo evidencia útil del estado de la técnica, pero no producen por sí solas esa presunción.

Iniciativas políticas de la UE: La Comisión publicó la Recomendación (UE) 2024/1101, de 11 de abril de 2024, relativa a una hoja de ruta de aplicación coordinada para la transición a la criptografía poscuántica. La hoja de ruta coordinada de 23 de junio de 2025, elaborada por el Grupo de Cooperación NIS, desarrolla prioridades e hitos comunes. Ambos instrumentos son orientación no vinculante **(R)** y no sustituyen el análisis de obligaciones aplicables a cada entidad.

4.8. Responsabilidad por productos defectuosos

La Directiva (UE) 2024/2853 incluye el software en el concepto de «producto» y contempla, entre otros elementos, la incidencia de las actualizaciones de seguridad y de la complejidad técnica en la prueba de la defectuosidad y la causalidad. Su aplicación a productos cuánticos debe analizarse junto con el CRA y con la normativa nacional de transposición.

No todo fallo, error de cálculo o vulnerabilidad cuántica determina por sí solo la existencia de un producto defectuoso. Deben examinarse la seguridad que legítimamente cabe esperar, la presentación y el uso razonablemente previsible, el momento de comercialización, la capacidad de actualización y las demás circunstancias del caso.

4.9. Servicios financieros, criptoactivos e infraestructuras DLT

El riesgo cuántico puede afectar a servicios financieros, criptoactivos e infraestructuras de mercado, pero el régimen aplicable depende del papel y la actividad de cada actor, no de una categoría jurídica autónoma de «QDLT».

- **MiCA (Reg. (UE) 2023/1114):** Puede resultar aplicable a emisores de criptoactivos y proveedores de servicios de criptoactivos comprendidos en su ámbito. La custodia de claves, la continuidad, la seguridad y la información al cliente deben analizarse conforme a la actividad concreta y a las exclusiones del Reglamento.
- **Régimen piloto DLT (Reg. (UE) 2022/858):** Se aplica a determinadas infraestructuras de mercado basadas en DLT para instrumentos financieros. Una adaptación criptográfica de la red debe preservar las condiciones de autorización, la integridad del mercado y la protección de participantes e inversores.
- **DORA, MiFID II y MAR:** DORA rige la resiliencia operativa digital de las entidades financieras incluidas; MiFID II y MAR pueden resultar aplicables según el instrumento, el servicio, la negociación y la conducta. Ninguno se activa automáticamente por incorporar tecnología cuántica.
- **Alcance técnico del riesgo:** Los algoritmos cuánticos afectan de forma asimétrica a firmas, intercambio de claves, cifrado simétrico y funciones hash; no implican la ruptura simultánea de toda cadena de bloques. La transición debe diseñarse según el protocolo, la custodia, la gobernanza, la interoperabilidad y el horizonte de riesgo de cada red **(I/P)**.

5. Gobernanza, Ética Aplicada y Cumplimiento

Tras analizar el marco jurídico vinculante (*hard law*) en la Sección 4, nos referimos a los mecanismos de gobernanza, los marcos de ética aplicada como la Investigación e Innovación Responsables (RRI), el papel del *soft law* y la implementación práctica de los requisitos de cumplimiento normativo y ético.

5.1. El papel de la gobernanza en la ética cuántica

La gobernanza de las tecnologías cuánticas comprende las estructuras, procesos y mecanismos —públicos y privados— destinados a dirigir, gestionar y supervisar su desarrollo y despliegue, de modo que se alineen con los valores éticos y con las normas que resulten aplicables según el producto, el rol, los datos, la finalidad, el sector y el territorio.

Gobernanza corporativa y cumplimiento (*hard law*)

La gobernanza debe ir más allá de los principios voluntarios o de los comités de ética consultivos. Cuando una organización quede incluida en el ámbito de una norma, debe poder acreditar responsabilidades, controles y evidencias proporcionados al riesgo.

- **Sistemas de gestión de la calidad (QMS):** Los proveedores de sistemas de IA de alto riesgo deben implantar el sistema de gestión de la calidad documentado previsto en el art. 17 del Reglamento de IA. La presencia de un componente cuántico no activa por sí sola esta obligación: primero debe existir un sistema de IA y concurrir la clasificación y el rol pertinentes.
- **Marcos de gestión de riesgos:** DORA (art. 6), NIS2 (art. 21) y el Reglamento de IA (art. 9) establecen, dentro de sus respectivos ámbitos, procesos de gestión de riesgos continuos e iterativos. La exposición cuántica debe integrarse cuando sea material por la criticidad del activo, la vida útil de la información, el estado de la técnica y el modelo de amenaza.

Gobernanza pública y estrategia nacional

Estrategia de Tecnologías Cuánticas de España 2025-2030: Aprobada por el Consejo de Ministros el 15 de abril de 2025, articula las áreas de computación, comunicaciones y sensórica cuánticas. Su presupuesto estimado asciende a 808 millones de euros, sujeto a las disponibilidades presupuestarias de cada ejercicio, con financiación prevista mediante fondos FEDER y el Plan de Recuperación, Transformación y Resiliencia. La alineación de las iniciativas sectoriales con esta estrategia debe combinar soberanía tecnológica, transferencia al mercado, talento, seguridad y evaluación ética.

5.2. Investigación e Innovación Responsables (RRI) como marco operativo

La RRI es un marco promovido por las instituciones europeas para alinear los procesos y resultados de investigación e innovación con los valores, necesidades y expectativas de la sociedad, especialmente útil en tecnologías emergentes.

- **Condiciones de financiación pública:** La RRI puede adquirir fuerza contractual cuando la convocatoria, el convenio o el acuerdo de subvención aplicable incorpore

obligaciones concretas de ética e integridad científica, ciencia abierta, igualdad, participación o gobernanza. No debe presumirse una obligación universal para todo proyecto cuántico financiado con fondos públicos. Cuando no exista una condición contractual verificable, la RRI opera como marco recomendado de buena gobernanza.

- **Dimensiones clave (Stilgoe et al., 2013):**
 - **Anticipación:** identificación temprana de posibles impactos sociales, éticos y ambientales.
 - **Reflexividad:** evaluación crítica de los compromisos y supuestos del proyecto.
 - **Inclusión:** participación proporcionada de los grupos de interés relevantes.
 - **Capacidad de respuesta (*responsiveness*):** adaptación de la innovación ante nueva evidencia, riesgos o preocupaciones sociales.

La aplicación sistemática y proporcionada de estas dimensiones desde las fases iniciales facilita la «ética desde el diseño» y deja evidencias útiles para la toma de decisiones.

5.3. El rol complementario del *soft law* y la autorregulación

El *soft law* —códigos de conducta, principios voluntarios y guías no vinculantes— desempeña un papel relevante en la ética cuántica, pero no sustituye a las obligaciones legales aplicables.

- **Prioridad del *hard law*:** La estrategia de cumplimiento debe partir del RGPD, el Reglamento de IA, NIS2, DORA, el Reglamento de Ciberresiliencia y las demás normas aplicables al caso.
- **Función complementaria:** El *soft law* permite desarrollar expectativas éticas más allá del mínimo legal, orientar la implementación sectorial y favorecer la armonización internacional. También puede informar el estándar de diligencia, sin convertirse por ello en una obligación autónoma.
- **Iniciativas relevantes:** Los Principios de Gobernanza de la Computación Cuántica del Foro Económico Mundial (2022), centrados en el bien común, la rendición de cuentas, la transparencia y la sostenibilidad, constituyen una referencia útil de autorregulación.

5.4. Ética, Privacidad y Seguridad desde el Diseño (*By Design*)

La «ética desde el diseño» propone incorporar las consideraciones éticas desde las primeras fases del desarrollo. Es un criterio de gobernanza; algunas de sus manifestaciones se traducen en obligaciones jurídicas concretas cuando concurre el ámbito de la norma correspondiente.

- **Protección de datos desde el diseño (art. 25 RGPD):** El responsable debe aplicar medidas técnicas y organizativas apropiadas para integrar los principios de protección de datos desde la concepción del tratamiento, atendiendo, entre otros factores, al estado de la técnica, los costes, la naturaleza del tratamiento y los riesgos.
- **Ciberseguridad desde el diseño (Reglamento de Ciberresiliencia):** Los fabricantes de productos con elementos digitales incluidos en su ámbito deben integrar los requisitos esenciales de ciberseguridad durante el ciclo de vida. La calificación no depende de que el producto sea «cuántico», sino de la definición legal, su finalidad o uso previsible, su conectividad, las exclusiones aplicables y el rol del operador.

5.5. Evaluaciones de Impacto (EIPD y EIDF)

La gestión proactiva de riesgos puede requerir evaluaciones de impacto, pero la tecnología cuántica no las activa automáticamente.

Evaluación de Impacto relativa a la Protección de Datos (EIPD o DPIA)

- **Cuándo procede (art. 35 RGPD):** La EIPD es obligatoria cuando, atendiendo a la naturaleza, el alcance, el contexto y los fines del tratamiento, sea probable que este entrañe un alto riesgo para los derechos y libertades, en particular en los supuestos del art. 35.3 y de las listas adoptadas conforme al art. 35.4. La escala, sensibilidad o combinación de datos de salud, biométricos o financieros puede hacer frecuente ese resultado, pero el uso de computación cuántica no basta por sí solo.
- **Contenido:** Debe describir el tratamiento, evaluar su necesidad y proporcionalidad, valorar los riesgos y concretar las medidas previstas. La cripto-agilidad o la PQC pueden formar parte de esas medidas cuando el riesgo, la vida útil de la confidencialidad y el estado de la técnica lo justifiquen.

Evaluación de Impacto sobre los Derechos Fundamentales (EIDF o FRIA)

- **Cuándo procede (art. 27 del Reglamento de IA):** Se exige, antes del despliegue, a los organismos de Derecho público y a las entidades privadas que prestan servicios públicos cuando utilicen sistemas de IA de alto riesgo, así como a los desplegados de los supuestos del Anexo III, puntos 5(b) y 5(c), relativos a evaluación de solvencia o puntuación crediticia y a evaluación de riesgos y fijación de precios en seguros de vida y salud. Debe verificarse siempre que exista un sistema de IA de alto riesgo y que el operador tenga el rol de desplegador previsto por la norma.
- **Contenido:** La EIDF identifica y evalúa los impactos sobre los derechos fundamentales en el contexto concreto de uso y define las medidas de mitigación, gobernanza y supervisión. Un componente cuántico se analiza solo en la medida en que afecte materialmente a esos riesgos.

5.6. Cooperación internacional e interoperabilidad técnica

Dada la naturaleza global de la ciencia y la tecnología cuántica, la cooperación internacional es esencial para abordar los desafíos éticos, garantizar la seguridad y evitar la fragmentación regulatoria.

- **Foros multilaterales y acuerdos:** La participación en la OCDE, la ONU y otros foros facilita la armonización de principios y el diálogo sobre doble uso y seguridad internacional. Cualquier propuesta de acuerdos vinculantes debe distinguirse de las obligaciones hoy vigentes.
- **Cooperación tecnológica europea:**
 - **EuroQCI:** despliegue de una infraestructura europea de comunicaciones cuánticas, combinando, cuando proceda, QKD con mecanismos criptográficos y de autenticación resistentes al adversario previsto.
 - **EuroHPC JU:** acceso paneuropeo a infraestructuras de supercomputación y computación cuántica.

- **Interoperabilidad y estándares:** La cooperación debe apoyar estándares de ISO, IEC, ETSI y CEN-CENELEC que permitan comparar prestaciones, evaluar seguridad e interoperar. Los estándares PQC del NIST son una referencia técnica relevante, pero su adopción debe integrarse en los perfiles europeos y sectoriales aplicables.

5.7. Estrategias de migración a PQC y cripto-agilidad

La transición a criptografía poscuántica es una acción prioritaria cuando existe exposición material a criptografía de clave pública vulnerable, especialmente respecto de información con larga vida de confidencialidad.

- **Marco europeo:** La Recomendación (UE) 2024/1101 de la Comisión, de 11 de abril de 2024, propuso una hoja de ruta coordinada para la transición a PQC. El Grupo de Cooperación NIS publicó el 23 de junio de 2025 la hoja de ruta correspondiente. Ambos instrumentos orientan principalmente a los Estados miembros y no constituyen, por sí solos, un mandato universal y directamente exigible a todas las empresas.
- **Estándares técnicos:** El NIST publicó en agosto de 2024 FIPS 203 (ML-KEM), FIPS 204 (ML-DSA) y FIPS 205 (SLH-DSA). La selección de algoritmos, perfiles híbridos y calendarios debe atender a la interoperabilidad, la madurez de las implementaciones y las guías aplicables.
- **Acciones clave:** inventario criptográfico; cripto-agilidad; priorización por criticidad, exposición, vida del dato y dependencia de terceros; y pruebas graduales de rendimiento, interoperabilidad y reversibilidad.

Hitos jurídico-operativos 2024-2035

Fecha	Hito	Naturaleza	Implicación operativa
11.04.2024	Recomendación (UE) 2024/1101 sobre transición a PQC	Recomendación no vinculante	Organizar la coordinación europea y preparar estrategias nacionales.
08.2024	Publicación de FIPS 203, 204 y 205	Estándares técnicos	Probar ML-KEM, ML-DSA y SLH-DSA en perfiles y productos adecuados.
23.06.2025	Hoja de ruta coordinada del Grupo de Cooperación NIS	Hoja de ruta no vinculante	Iniciar inventarios, gobernanza y planificación; los Estados miembros deberían comenzar la transición antes de finalizar 2026.
02.07.2025	Quantum Europe Strategy, COM(2025) 363	Estrategia de política pública	Coordinar investigación, infraestructuras, industria, doble uso y capacidades.
15.11.2025	Aplicación del Reglamento Delegado (UE) 2025/2003	Acto vinculante	Reclasificar productos y tecnología de doble uso con arreglo al Anexo I actualizado.
Final de 2030	Horizonte europeo para casos de alto riesgo e infraestructuras críticas	Objetivo de la hoja de ruta	Completar con prioridad las migraciones de mayor riesgo; no es una fecha universal de sanción para toda empresa.
Final de 2035	Horizonte para el resto de sistemas cuya migración sea viable	Objetivo de la hoja de ruta	Cerrar progresivamente la transición restante y documentar excepciones y riesgos residuales.

6. Riesgos Normativos

Las tecnologías cuánticas se desarrollan dentro de un marco horizontal y sectorial ya existente. El riesgo principal consiste tanto en incumplir una norma aplicable como en aplicar de forma automática obligaciones que dependen del producto, el rol, el dato, la finalidad, el sector o el

territorio. Para evitar contradicciones con el capítulo 4, esta sección resume cada cuestión en formato «riesgo → consecuencia → mitigación».

6.1. Riesgos de incumplimiento del *hard law*

Marco	Riesgo	Consecuencia	Mitigación proporcionada
RGPD	Tratar datos sin base jurídica, sin medidas adecuadas o sin EIPD cuando el tratamiento pueda entrañar alto riesgo. La reidentificación mediante técnicas cuánticas debe tratarse como una hipótesis a valorar, no como una capacidad general demostrada.	Medidas correctivas, prohibición o limitación del tratamiento, responsabilidad y multas de hasta 20 M€ o el 4 % del volumen de negocio mundial anual, según la infracción.	Clasificar tratamientos y datos; aplicar los arts. 25, 32 y 35 según el riesgo; evaluar HNDL y la vida de la confidencialidad; documentar la decisión de migrar o no a PQC. En una violación de seguridad, el responsable notifica a la autoridad, cuando proceda, dentro de las 72 horas desde que tenga constancia; la comunicación a los interesados, si existe alto riesgo, se realiza sin dilación indebida. El encargado informa al responsable sin dilación indebida.
Reglamento de IA	Tratar cualquier componente cuántico como sistema de IA o presumir que todo uso en un sector crítico es de alto riesgo; en sentido inverso, omitir obligaciones cuando sí concurren la definición, clasificación y rol legales.	Retirada o restricción del sistema, medidas de vigilancia y sanciones: hasta 35 M€ o 7 % por prácticas prohibidas; 15 M€ o 3 % por otras obligaciones; y 7,5 M€ o 1 % por información inexacta, incompleta o engañosa, con las reglas del art. 99.	Verificar definición, Anexo I o III y rol. Para sistemas de alto riesgo, mantener, entre otras evidencias, documentación técnica (art. 11), registros (art. 12), transparencia e información al desplegador (art. 13), supervisión humana (art. 14) y precisión, solidez y ciberseguridad (art. 15). Exigir transparencia suficiente según el riesgo, no una «explicabilidad completa».
Reglamento de Ciberresiliencia (CRA)	Presumir que todo hardware, software, sensor o servicio cuántico está incluido, o llegar tarde a seguridad, soporte, documentación de componentes y gestión de vulnerabilidades.	Restricciones de acceso al mercado, retirada o recuperación de productos, medidas correctivas y sanciones.	Clasificar el producto con elementos digitales, su conectividad, finalidad o uso previsible, exclusiones y rol de fabricante, importador o distribuidor. Documentar la SBOM en formato legible por máquina sin presumir su publicación general. Las obligaciones de notificación del art. 14 se aplican desde el 11 de septiembre de 2026 y las obligaciones principales, con carácter general, desde el 11 de diciembre de 2027.
NIS2	Incluir o excluir a una organización por la sola etiqueta «cuántica» y no gestionar incidentes conforme al régimen aplicable.	Supervisión, medidas correctivas y, para las categorías correspondientes, multas de hasta 10 M€ o 2 % y hasta 7 M€ o 1,4 %, sin perjuicio de la transposición nacional.	Comprobar categoría, tamaño, establecimiento y transposición. Una plataforma cuántica en nube puede estar incluida como proveedor <i>cloud</i> , pero la mera I+D cuántica no basta. Para incidentes significativos: alerta temprana en 24 horas, notificación en 72 horas, informe intermedio si lo solicita la autoridad e informe final, con carácter general, en un mes.
DORA	Considerar que cualquier proveedor cuántico es un proveedor tercero TIC crítico, que todas las entidades deben realizar TLPT o que existe un plazo general de notificación de un día hábil.	Requerimientos de supervisión, corrección de deficiencias, restricciones contractuales, sanciones nacionales y pérdida de clientes financieros.	Verificar si la entidad está incluida, si procede TLPT conforme al art. 26 y si el proveedor ha sido designado crítico según los criterios del marco. Notificar los incidentes TIC graves conforme a DORA y a sus normas técnicas aplicables; integrar la exposición cuántica en gestión de riesgo TIC, continuidad y terceros cuando sea material.
Responsabilidad por productos	Defectos de seguridad, falta de actualizaciones o reparto impreciso de responsabilidades entre fabricante, integrador, proveedor de software y servicio asociado.	Reclamaciones por daños y dificultades probatorias y causales, además de las medidas regulatorias del CRA.	Analizar la Directiva (UE) 2024/2853 y su transposición: incluye el <i>software</i> en el concepto de producto y considera la ciberseguridad y las actualizaciones entre los elementos relevantes para apreciar la defectuosidad. Definir contractualmente roles y conservar evidencia técnica.

Ninguno de estos marcos contiene, por el solo hecho de utilizar tecnología cuántica, un mandato nominal y universal de adoptar PQC. La transición puede resultar exigible o prudente según el riesgo, el estado de la técnica, los costes, la criticidad y la vida útil de la información.

6.2. Riesgos del control de doble uso

El Reglamento (UE) 2021/821, cuyo Anexo I fue actualizado por el Reglamento Delegado (UE) 2025/2003, incluye controles específicos sobre determinados ordenadores cuánticos y componentes en la partida 4A506. No todo ordenador, criostato, sensor, sistema QKD, algoritmo, software o asistencia técnica está controlado: deben comprobarse la partida, los umbrales, las notas técnicas, el destino, el usuario y el uso final.

Riesgo	Consecuencia	Mitigación
Clasificación por analogía o por número bruto de qubits, sin aplicar las definiciones y umbrales de la lista.	Licencias innecesarias o, en el extremo opuesto, exportaciones no autorizadas.	Clasificación documentada contra el Anexo I vigente, incluida 4A506 cuando proceda; dictamen especializado para supuestos dudosos.
Transferir equipos, software, tecnología o asistencia sin analizar el tipo de operación.	Paralización de entregas, sanciones administrativas o penales y pérdida de acceso a mercados.	Distinguir exportación fuera de la UE, transferencias intra-UE sujetas a control, intermediación, asistencia técnica, tránsito y controles <i>catch-all</i> ; tramitar autorizaciones antes de la operación.
No verificar destino, usuario final, uso final, sanciones o riesgo de desvío.	Uso militar o de proliferación no autorizado y daño reputacional grave.	Programa Interno de Cumplimiento, diligencia debida, cribado de sanciones, declaración de uso final, cláusulas de no reexportación y escalado de señales de alerta.
Aplicar controles de forma indiscriminada a la ciencia abierta.	Retrasos, fragmentación de la investigación y pérdida de competitividad sin mejora proporcional de seguridad.	Separar investigación básica de tecnología controlada, documentar las exclusiones aplicables y establecer un canal previo de revisión para colaboraciones internacionales.

6.3. Riesgos de sobrerregulación y fragmentación

Riesgo	Consecuencia	Mitigación
Extender RGPD, Reglamento de IA, NIS2, DORA o CRA por la mera presencia de un componente cuántico.	Costes desproporcionados, incertidumbre y desincentivo a la innovación.	Aplicar una ficha de subsunción por producto, rol, dato, finalidad, sector, tamaño y territorio; distinguir obligación expresa, interpretación basada en riesgo, estándar, recomendación y propuesta.
Imponer soluciones técnicas únicas o fechas universales antes de disponer de perfiles maduros.	Bloqueo tecnológico, dependencia de proveedor y migraciones inseguras.	Usar requisitos funcionales y basados en riesgo, pruebas piloto, interoperabilidad y revisiones periódicas.
Confundir trazabilidad jurídica con observación física de estados cuánticos internos.	Exigencias imposibles y falsa oposición entre cumplimiento y física cuántica.	Asegurar reproducibilidad estadística y procedimental: versión de circuito y compilador, calibración, dispositivo, número de ejecuciones, distribución de resultados e intervalos, incertidumbre, verificación clásica o cruzada y umbral de confianza proporcionado al daño potencial.
Requisitos divergentes entre Estados, sectores o compradores.	Duplicación de pruebas, barreras de mercado y menor escalabilidad.	Favorecer estándares europeos e internacionales, reconocimiento mutuo, documentación reutilizable y coordinación entre supervisores, industria y comunidad científica.

6.4. Estrategias transversales de mitigación

- **Cumplimiento desde el diseño:** Someter cada proyecto a una revisión temprana de aplicabilidad y riesgo. Las EIPD o EIDF se realizan cuando concurren sus presupuestos legales; otras evaluaciones pueden utilizarse voluntariamente como buena práctica.
- **Hoja de ruta PQC basada en riesgo:** Completar el inventario criptográfico, establecer una línea base, priorizar datos de larga vida y sistemas críticos, probar esquemas híbridos cuando proceda y aprobar metas internas por el órgano competente. Los

horizontes europeos de 2026, 2030 y 2035 son referencias de coordinación, no sanciones automáticas ni fechas universales para todas las empresas.

- **QKD como defensa en profundidad:** Utilizarla solo cuando el caso de uso, la infraestructura, los costes y el modelo de amenaza lo justifiquen. QKD no autentica por sí sola los extremos; debe combinarse con un mecanismo resistente al adversario previsto, como PQC en despliegues de clave pública o, cuando sea viable, autenticación simétrica con claves precompartidas.
- **Contratos y cadena de suministro:** Incluir roles, soporte, SBOM cuando proceda, gestión de vulnerabilidades, cripto-agilidad, continuidad, auditoría, control de exportaciones y uso final. Los plazos contractuales más estrictos deben presentarse como acuerdos, no como plazos legales generales.
- **Gobernanza y controles internos:** Asignar la supervisión al nivel directivo adecuado, mantener un registro de decisiones, validar de forma cruzada los resultados de alto impacto y comunicar límites, incertidumbres y condiciones de validez.

Cada acción debe asociarse a un responsable, una fecha interna, una evidencia y un indicador de resultado. El objetivo no es acumular controles, sino reducir exposición verificable sin asfixiar la innovación.

7. Recomendaciones y Pasos Futuros

Planteamos algunas recomendaciones estratégicas y pasos operativos necesarios para implementar una gobernanza ética y un marco regulatorio eficaz para las tecnologías cuánticas en la Unión Europea y España. El objetivo es pasar del análisis a la acción, priorizando el cumplimiento normativo y la implementación de buenas prácticas.

7.1. Fomento de la Educación, el Talento Multidisciplinar y la Concienciación

El desarrollo de un ecosistema cuántico responsable y competitivo depende críticamente de la disponibilidad de talento especializado y de una concienciación pública adecuada.

Recomendaciones:

- **Formación de profesionales híbridos:** Fomentar programas educativos universitarios y de formación profesional que integren la ética de la tecnología y el Derecho digital de la UE en los currículos STEM (Ciencia, Tecnología, Ingeniería y Matemáticas). Es esencial formar profesionales cuánticos con sensibilidad ética y jurídica —ingenieros, físicos, juristas y filósofos trabajando conjuntamente— capaces de implementar los principios de ética, privacidad y seguridad desde el diseño.
- **Capacitación regulatoria y técnica especializada:** Desarrollar programas de formación continua para profesionales de la ciberseguridad sobre PQC y cripto-agilidad, y para responsables de cumplimiento normativo y auditores sobre la aplicación del Reglamento de IA (RIA), el CRA, DORA y el régimen de doble uso a casos cuánticos concretos.
- **Divulgación rigurosa y conciencia pública:** Promover iniciativas de divulgación basadas en el principio de información responsable: evitar expectativas exageradas

(*anti-hype*) y comunicar con claridad beneficios, límites, incertidumbres y riesgos reales —como HNDL— para fomentar un debate público de calidad.

7.2. Fortalecimiento de la Gobernanza Institucional y la Supervisión

En lugar de proponer la creación de nuevos organismos de supervisión *ad hoc*, se recomienda un enfoque pragmático y eficiente: integrar la dimensión cuántica en los mandatos de los organismos de supervisión existentes en la UE y a nivel nacional, reforzando sus capacidades técnicas.

Recomendaciones:

- **Integración en organismos existentes de la UE:** Reforzar las capacidades técnicas de las agencias, autoridades y organismos ya competentes para que puedan abordar los riesgos cuánticos dentro de sus respectivos mandatos:
 - **ENISA (Agencia de la UE para la Ciberseguridad):** Apoyo técnico a la transición coordinada a PQC, en línea con la Recomendación (UE) 2024/1101 y la hoja de ruta europea de 2025, y asistencia al ecosistema NIS2 y CRA.
 - **Oficina de IA de la UE:** Desarrollo y coordinación del marco del RIA para los sistemas comprendidos en sus competencias, incluida la orientación sobre documentación, transparencia y supervisión humana cuando exista IA cuántica.
 - **CEPD y autoridades de protección de datos:** Consideración del riesgo cuántico en la interpretación de la seguridad del tratamiento —art. 32 RGPD— y de las EIPD —art. 35 RGPD—, dentro de sus competencias.
 - **Autoridades Europeas de Supervisión (EBA, ESMA y EIOPA):** Integración proporcionada del riesgo cuántico en la supervisión de la resiliencia operativa bajo DORA cuando sea material para las entidades y funciones supervisadas.
- **Coordinación nacional:** Reforzar la coordinación entre los organismos competentes. En España, el Centro Criptológico Nacional (CCN) puede seguir impulsando orientación técnica sobre transición criptográfica, mientras que las autoridades de ciberseguridad, protección de datos, supervisión financiera y control de exportaciones conservan sus competencias propias.

7.3. Integración de la Ética y el Cumplimiento en la Estrategia Tecnológica

La ética y el cumplimiento normativo (*hard law*) deben ser elementos centrales e integrados en las estrategias de desarrollo tecnológico, tanto a nivel corporativo como nacional.

Recomendaciones:

- **Estrategia de Tecnologías Cuánticas de España 2025-2030:** Alinear las iniciativas sectoriales con la estrategia aprobada en 2025. El documento estima un presupuesto aproximado de **808 millones de euros**, procedente principalmente del PRTR y FEDER, pero somete su ejecución a las disponibilidades presupuestarias de cada ejercicio y aclara que su aprobación no constituye por sí sola un compromiso financiero.
- **Quantum Europe Strategy:** La Comunicación COM(2025) 363 articula cinco áreas conectadas: (i) investigación e innovación; (ii) infraestructuras cuánticas; (iii)

fortalecimiento del ecosistema cuántico y su industrialización; (iv) espacio y tecnologías cuánticas de doble uso, seguridad y defensa; y (v) capacidades y talento cuánticos. Estas prioridades deben coordinarse con EuroHPC, EuroQCI y las políticas nacionales sin confundirse con obligaciones jurídicas individuales.

- **Estado del futuro *Quantum Act*:** A 27 de julio de 2026, el rastreador oficial de la Comisión seguía clasificándolo como iniciativa «planificada», no como norma adoptada o vigente. Debe mantenerse una vigilancia regulatoria fechada, sin atribuirle todavía obligaciones de cumplimiento.
- **Implementación proporcionada de RRI:** Traducir los principios de Investigación e Innovación Responsables (RRI) en condiciones de financiación, contratación y evaluación cuando el programa o proyecto correspondiente así lo prevea, evitando presentarlos como una obligación legal universal.
- **Cumplimiento desde el diseño (*Compliance by Design*):** Integrar desde las fases iniciales los requisitos que resulten aplicables por producto, actividad y rol —p. ej., QMS del RIA o seguridad y gestión de vulnerabilidades del CRA—, conservando evidencia de las decisiones de ámbito y proporcionalidad.

7.4. Promoción de Buenas Prácticas y Aseguramiento del Cumplimiento (*hard law*)

La promoción de buenas prácticas debe centrarse en la implementación efectiva de las obligaciones legales y los estándares técnicos críticos.

Recomendaciones Técnicas (Seguridad - Prioridad Crítica):

- **Priorizar la migración a PQC y la cripto-agilidad según el riesgo:** Elaborar planes basados en inventario, criticidad, vida de confidencialidad, dependencias y capacidad de sustitución. FIPS 203-205 son estándares técnicos relevantes, no obligaciones automáticas de la UE ni una orden de migración inmediata para toda infraestructura.
- **Inventario criptográfico:** Las organizaciones expuestas al riesgo deben identificar algoritmos, protocolos, claves, certificados, proveedores, datos de larga confidencialidad y equipos heredados. El inventario debe conducir a prioridades verificables, no limitarse a un registro documental.
- **Posicionamiento de QKD (defensa en profundidad):** Evaluar QKD como complemento especializado para casos de alta sensibilidad, atendiendo a distancia, tasa de claves, nodos de confianza, dispositivos, disponibilidad e interoperabilidad. QKD requiere autenticación resistente al adversario previsto, que puede basarse en PQC o, cuando resulte viable, en mecanismos simétricos con claves precompartidas; no depende exclusivamente de PQC.

Recomendaciones Regulatorias (IA y Control de Exportaciones):

- **Aplicación del RIA por ámbito y rol:** Comprobar primero si la solución constituye o integra un sistema de IA y después su categoría y el rol de cada operador. Cuando resulte aplicable, deberán respetarse las prohibiciones del art. 5 y las obligaciones correspondientes, sin tratar todo componente cuántico como IA o como sistema de alto riesgo.
- **Gestión proactiva del doble uso:** Implantar programas internos de cumplimiento proporcionados a la exposición real bajo el Reglamento (UE) 2021/821 y su Anexo I

actualizado, con clasificación técnica, revisión de destino, usuario y uso final, control de transferencias intangibles y escalado de dudas antes de exportar.

7.5. Evaluación Continua y Definición de KPIs Éticos y de Cumplimiento

Para garantizar la rendición de cuentas (*accountability*) y la mejora continua, es necesario pasar de una evaluación cualitativa a una monitorización objetiva basada en métricas.

Recomendaciones:

- **Evaluación iterativa y gestión de riesgos:** Implementar procesos continuos a lo largo del ciclo de vida, aplicando el art. 9 del RIA, el art. 6 de DORA o el art. 21 de NIS2 únicamente cuando la organización, el sistema y el riesgo estén comprendidos en sus respectivos ámbitos.
- **Indicadores de resultado:** Combinar indicadores de ejecución con métricas que muestren reducción efectiva del riesgo y efectos sobre las personas y el ecosistema. Entre otras:
 - Porcentaje de información de larga confidencialidad que continúa protegida exclusivamente con criptografía de clave pública vulnerable, ponderado por criticidad.
 - Reducción de vulnerabilidades críticas explotables fuera del plazo interno de remediación y tasa de reincidencia tras actualizaciones.
 - Cumplimiento de objetivos de recuperación en pruebas e incidentes, tiempo medio de recuperación y afectación real a funciones críticas.
 - Riesgo residual y número de impactos adversos sobre derechos tras las medidas definidas en EIPD o EIDF, solo cuando dichas evaluaciones sean exigibles.
 - Evolución de la concentración de acceso a capacidad cuántica —p. ej., utilización por pymes, centros públicos y territorios— y resultados obtenidos por unidad de recurso.
 - Energía, emisiones, materiales y residuos por resultado útil, comparados con la mejor alternativa clásica disponible a precisión equivalente.
- **Auditoría, aprendizaje y transparencia:** Revisar periódicamente las métricas, causas raíz y eficacia de las medidas, evitando premiar el mero volumen de documentación. Solo las entidades incluidas en el ámbito de la CSRD deberán integrar la información material exigible en sus informes de sostenibilidad; las demás podrán comunicarla voluntariamente, identificando con claridad su naturaleza y metodología.

8. Bibliografía y Fuentes de Referencia

Derecho de la Unión Europea

- Unión Europea. Reglamento (UE) 2016/679, Reglamento General de Protección de Datos (RGPD). EUR-Lex
- Unión Europea. Reglamento (UE) 2023/2854 sobre normas armonizadas para un acceso justo a los datos y su utilización (Reglamento de Datos o *Data Act*). EUR-Lex

- Unión Europea. Reglamento (UE) 2024/1689 por el que se establecen normas armonizadas en materia de inteligencia artificial (Reglamento de IA). EUR-Lex
- Unión Europea (2026). Texto legislativo PE 30/2026 REV 1 sobre simplificación del Reglamento de IA, aprobado por el Parlamento Europeo y el Consejo y pendiente, a la fecha de corte, de número definitivo de publicación. EUR-Lex
- Unión Europea. Reglamento (UE) 2023/1781 por el que se establece un marco de medidas para reforzar el ecosistema europeo de semiconductores (Reglamento de Chips). EUR-Lex
- Unión Europea. Directiva (UE) 2022/2555 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (NIS2). EUR-Lex
- Unión Europea. Reglamento (UE) 2022/2554 sobre la resiliencia operativa digital del sector financiero (DORA). EUR-Lex
- Unión Europea. Reglamento (UE) 2024/2847 relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales (CRA). EUR-Lex
- Unión Europea. Reglamento (UE) 2024/1183 por el que se modifica el Reglamento (UE) 910/2014 en lo que respecta al establecimiento del marco europeo de identidad digital (eIDAS2). EUR-Lex
- Unión Europea. Reglamento (UE) 2021/821 por el que se establece un régimen de control de las exportaciones, el corretaje, la asistencia técnica, el tránsito y la transferencia de productos de doble uso. EUR-Lex
- Comisión Europea. Reglamento Delegado (UE) 2025/2003 por el que se modifica el Reglamento (UE) 2021/821 en lo que respecta a la lista de productos de doble uso. EUR-Lex
- Unión Europea. Directiva (UE) 2024/2853 sobre responsabilidad por los daños causados por productos defectuosos. EUR-Lex
- Comisión Europea. Recomendación (UE) 2024/1101, de 11 de abril de 2024, relativa a una hoja de ruta de aplicación coordinada para la transición a la criptografía poscuántica. EUR-Lex
- Unión Europea. Reglamento (UE) 2025/327 relativo al Espacio Europeo de Datos de Salud (EHDS). EUR-Lex
- Unión Europea. Reglamento (UE) 2023/1114 relativo a los mercados de criptoactivos (MiCA). EUR-Lex
- Unión Europea. Reglamento (UE) 2022/858 sobre un régimen piloto de infraestructuras del mercado basadas en la tecnología de registro descentralizado. EUR-Lex
- Unión Europea. Directiva 2014/65/UE relativa a los mercados de instrumentos financieros (MiFID II). EUR-Lex
- Unión Europea. Reglamento (UE) 596/2014 sobre el abuso de mercado (MAR). EUR-Lex
- Unión Europea. Directiva (UE) 2022/2464 sobre información corporativa en materia de sostenibilidad (CSRD). EUR-Lex

Política pública y hojas de ruta

- Gobierno de España (2025). *Estrategia de Tecnologías Cuánticas de España 2025-2030*. Documento oficial

- Comisión Europea (2025). *Quantum Europe Strategy*, COM(2025) 363, 2 de julio de 2025. Shaping Europe's Digital Future
- Comisión Europea. *One Europe, One Market roadmap*, rastreador oficial que mantiene el *Quantum Act* entre las iniciativas planificadas; última actualización consultada: 20 de julio de 2026. Comisión Europea
- Grupo de Cooperación NIS y Comisión Europea (2025). *A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography*, 23 de junio de 2025. Shaping Europe's Digital Future

Estándares y fuentes técnicas

- National Institute of Standards and Technology (NIST) (2024). FIPS 203, *Module-Lattice-Based Key-Encapsulation Mechanism Standard* (ML-KEM). NIST CSRC
- NIST (2024). FIPS 204, *Module-Lattice-Based Digital Signature Standard* (ML-DSA). NIST CSRC
- NIST (2024). FIPS 205, *Stateless Hash-Based Digital Signature Standard* (SLH-DSA). NIST CSRC
- NIST (2025). *NIST Selects HQC as Fifth Algorithm for Post-Quantum Encryption*. NIST
- NIST (2025). *FIPS 206: FN-DSA (Falcon)*, presentación de la sexta conferencia de estandarización PQC. NIST CSRC
- European Telecommunications Standards Institute (ETSI) (2019). ETSI GS QKD 014 V1.1.1, *Quantum Key Distribution; Protocol and data format of REST-based key delivery API*. ETSI

Ética, RRI y gobernanza de tecnologías cuánticas

- World Economic Forum (2022). *Quantum Computing Governance Principles*. Informe
- Bengoetxea, Juan Bautista y Mitcham, Carl (2010). *Ética e ingeniería*. Valladolid: Universidad de Valladolid.
- Coenen, Christopher y Grunwald, Armin (2017). "Responsible research and innovation (RRI) in quantum technology". *Ethics and Information Technology*, 19, 277-294. DOI
- Cortina, Adela (1996). "El estatuto de la ética aplicada. Hermenéutica crítica de las actividades humanas". *Isegoría*, 13, 119-127. DOI
- Kop, Mauritz (2021). "Establishing a Legal-Ethical Framework for Quantum Technology". *Yale Journal of Law & Technology*. Texto
- Ménissier, Thierry (2022). "The ethics of quantum technologies: a problematic formulation". *QuantAlps Days*. HAL
- Possati, Luca M. (2023). "Ethics of Quantum Computing: an Outline". *Philosophy & Technology*, 36(48). DOI
- Stahl, Bernd Carsten; Timmermans, Job y Flick, Catherine (2017). "Ethics of Emerging Information and Communication Technologies: On the implementation of responsible research and innovation". *Science and Public Policy*, 44(3), 369-381. DOI
- Stilgoe, Jack; Owen, Richard y Macnaghten, Phil (2013). "Developing a framework for responsible innovation". *Research Policy*, 42(9), 1568-1580. DOI

8.1. Glosario de Conceptos Clave

A. Términos Técnicos y Conceptos Cuánticos

Computación cuántica: Paradigma de computación que procesa información mediante sistemas cuánticos y explota fenómenos como superposición, interferencia y entrelazamiento. Puede ofrecer ventajas para determinadas clases de problemas y bajo condiciones concretas; no constituye una aceleración universal frente a la mejor alternativa clásica.

Cripto-agilidad (*crypto-agility*): Capacidad organizativa y técnica para descubrir dónde se usa criptografía y actualizar o sustituir de forma controlada algoritmos, protocolos, claves, certificados y parámetros, preservando seguridad, interoperabilidad y continuidad. No presupone que el cambio sea automático ni que pueda hacerse sin adaptar la arquitectura.

Criptografía de clave pública o asimétrica: Familia de mecanismos que emplean una clave pública y una clave privada para funciones como establecimiento de claves y firma digital. Un CRQC capaz de ejecutar Shor a escala relevante comprometería mecanismos basados en factorización o logaritmo discreto, como RSA, Diffie-Hellman y ECC.

Criptografía poscuántica (PQC): Algoritmos criptográficos clásicos diseñados para resistir ataques de ordenadores clásicos y cuánticos conforme a los modelos y parámetros evaluados. Pueden ejecutarse en infraestructura convencional, aunque su integración requiere analizar rendimiento, claves, protocolos e interoperabilidad. NIST publicó FIPS 203 —ML-KEM—, FIPS 204 —ML-DSA— y FIPS 205 —SLH-DSA—.

CRQC (ordenador cuántico criptográficamente relevante): Ordenador cuántico tolerante a fallos con escala y recursos suficientes para ejecutar un ataque criptográficamente relevante contra parámetros de uso real, por ejemplo mediante Shor frente a determinados sistemas de clave pública.

Distribución cuántica de claves (QKD): Técnica basada en hardware que utiliza propiedades cuánticas para establecer material de clave entre extremos bajo un modelo de seguridad definido. Sus garantías prácticas dependen de dispositivos, canales, protocolos y operación. Requiere autenticar los extremos mediante un mecanismo resistente al adversario previsto, que puede ser PQC o, cuando sea viable, autenticación simétrica con claves precompartidas.

HN DL (*harvest now, decrypt later* / cosechar ahora, descifrar después): Patrón de amenaza en el que un atacante intercepta y conserva información cifrada para intentar descifrarla en el futuro. Convierte la confidencialidad a largo plazo en un riesgo presente, aunque todavía no exista un CRQC operativo para el ataque considerado.

IA cuántica (*quantum AI*): Área que estudia la integración de componentes cuánticos con sistemas de IA, incluido el aprendizaje automático cuántico. La combinación no implica por sí sola una ventaja práctica ni convierte toda infraestructura cuántica en un sistema de IA.

Qubit (bit cuántico): Unidad básica de información cuántica cuyo estado puede ser una superposición coherente respecto de una base de medida y que puede entrelazarse con otros sistemas cuánticos. Su medición produce un resultado clásico con probabilidades determinadas por el estado y la medición.

B. Términos Jurídicos, Regulatorios y Éticos

Control de exportaciones de doble uso: Régimen establecido en la UE por el Reglamento (UE) 2021/821 y su lista actualizada, que puede someter a autorización determinadas operaciones sobre productos, *software* y tecnología de uso civil y militar. No toda tecnología cuántica está controlada: deben comprobarse clasificación, umbrales, operación, destino, usuario y uso final.

Ética desde el diseño (*ethics by design*): Enfoque de gobernanza que integra valores, impactos y participación desde las fases iniciales del ciclo de vida. No constituye por sí solo una obligación jurídica universal, aunque puede apoyar el cumplimiento de obligaciones específicas de privacidad, seguridad o gestión de riesgos desde el diseño.

Evaluación de Impacto sobre los Derechos Fundamentales (EIDF / FRIA): Evaluación estructurada exigida por el art. 27 del RIA a los responsables del despliegue y sistemas de alto riesgo comprendidos en ese precepto. No se exige a todo responsable ni a todo sistema de alto riesgo; su alcance incluye determinados organismos de Derecho público, prestadores privados de servicios públicos y ciertos casos específicos.

Evaluación de Impacto relativa a la Protección de Datos (EIPD / DPIA): Proceso previo exigido por el art. 35 RGPD cuando sea probable que un tratamiento entrañe un alto riesgo para los derechos y libertades de las personas físicas. El mero uso de tecnología cuántica no activa automáticamente esta obligación.

Hard law / soft law: El *hard law* comprende normas jurídicamente vinculantes; en la UE, los reglamentos son directamente aplicables en sus condiciones y las directivas requieren transposición. El *soft law* comprende recomendaciones, guías y otros instrumentos sin fuerza vinculante directa, aunque pueden orientar interpretación, supervisión, contratos o diligencia.

Honestidad epistémica: Criterio ético y técnico consistente en reconocer y documentar límites de validez, incertidumbres, tasas de error y condiciones de funcionamiento. No es un término jurídico autónomo del RIA, pero puede contribuir a satisfacer requisitos de documentación, transparencia y gestión de riesgos cuando resulten aplicables.

Investigación e Innovación Responsables (RRI): Enfoque que busca alinear procesos y resultados de investigación e innovación con valores, necesidades y expectativas sociales mediante prácticas como ética de la investigación, ciencia abierta, participación, igualdad y gobernanza. Su exigibilidad depende del programa, contrato o norma aplicable.

Lista de materiales de software (SBOM): Inventario estructurado y legible por máquina de los componentes de *software* de un producto. En el CRA, el fabricante debe identificar y documentar componentes, incluso mediante una SBOM; ello no equivale a una obligación general de publicarla o entregarla indiscriminadamente.

Privacidad desde el diseño (*privacy by design*): Obligación del art. 25 RGPD que exige al responsable aplicar medidas técnicas y organizativas apropiadas para integrar eficazmente los principios de protección de datos y las garantías necesarias, atendiendo al riesgo y a los demás factores previstos en el precepto.

Seguridad desde el diseño (*security by design*): Enfoque consistente en integrar requisitos de seguridad durante diseño, desarrollo, mantenimiento y soporte. El CRA lo concreta para los productos con elementos digitales comprendidos en su ámbito mediante requisitos esenciales y gestión de vulnerabilidades basada en el riesgo.

Sistema de gestión de la calidad (QMS): Sistema documentado exigido por el art. 17 del RIA a los proveedores de sistemas de IA de alto riesgo para asegurar el cumplimiento del Reglamento durante el ciclo de vida.

8.2. Relación de Acrónimos y Siglas

Normativa de la Unión Europea

AI Act: Denominación inglesa del Reglamento de IA; véase RIA.

CRA: Cyber Resilience Act (Reglamento de Ciberresiliencia de la UE).

CSRD: Corporate Sustainability Reporting Directive (Directiva (UE) 2022/2464 sobre sostenibilidad corporativa).

DORA: Digital Operational Resilience Act (Reglamento (UE) 2022/2554 sobre resiliencia operativa digital del sector financiero).

eIDAS2: Reglamento (UE) 2024/1183 (Marco Europeo de Identidad Digital y servicios de confianza).

EHDS: European Health Data Space (Reglamento (UE) 2025/327 relativo al Espacio Europeo de Datos de Salud).

MiFID II: Markets in Financial Instruments Directive (Directiva 2014/65/UE sobre mercados de instrumentos financieros).

MiCA: Markets in Crypto-Assets Regulation (Reglamento (UE) 2023/1114 relativo a los mercados de cryptoactivos).

NIS2: Directiva (UE) 2022/2555 (Medidas para un elevado nivel común de ciberseguridad en la Unión).

RIA: Reglamento de Inteligencia Artificial (Reglamento (UE) 2024/1689).

RGPD: Reglamento General de Protección de Datos (Reglamento (UE) 2016/679).

Términos Técnicos, Éticos y Estándares

CRQC: Cryptographically Relevant Quantum Computer (ordenador cuántico criptográficamente relevante).

DPIA: Data Protection Impact Assessment (véase EIPD).

ECC: Elliptic Curve Cryptography (Criptografía de Curva Elíptica).

EIPD: Evaluación de Impacto relativa a la Protección de Datos.

EIDF: Evaluación de Impacto sobre los Derechos Fundamentales.

ETSI: European Telecommunications Standards Institute (Instituto Europeo de Normas de Telecomunicaciones).

FIPS: Federal Information Processing Standards (Estándares Federales de Procesamiento de la Información, EE.UU.).

FRIA: Fundamental Rights Impact Assessment (véase EIDF).

HNDL: Harvest Now, Decrypt Later (cosechar ahora, descifrar después).

PQC: Post-Quantum Cryptography (Criptografía poscuántica).

QKD: Quantum Key Distribution (Distribución de Claves Cuánticas).

QMS: Quality Management System (Sistema de Gestión de la Calidad).

QTSP: Qualified Trust Service Provider (Prestador Cualificado de Servicios de Confianza).

RRI: Responsible Research and Innovation (Investigación e Innovación Responsables).

RSA: Algoritmo criptográfico de clave pública (Rivest-Shamir-Adleman).

SBOM: Software Bill of Materials (Lista de Materiales de Software).

Instituciones e Iniciativas

CCN: Centro Criptológico Nacional (España).

CEPD: Comité Europeo de Protección de Datos.

ENISA: Agencia de la Unión Europea para la Ciberseguridad.

EuroHPC JU: European High-Performance Computing Joint Undertaking (Empresa Común Europea de Informática de Alto Rendimiento).

EuroQCI: European Quantum Communication Infrastructure (Infraestructura Europea de Comunicación Cuántica).

NIST: National Institute of Standards and Technology (Instituto Nacional de Estándares y Tecnología, EE.UU.).